COPYRIGHT
Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

TRADEMARK ATTRIBUTIONS
Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.
Preface

Contents

1 Introduction

2 User interface

3 System configuration
4 Proxies

Configure proxies .................................................. 66
Explicit proxy mode .................................................. 66
  Configure the explicit proxy mode ............................... 67
Transparent Proxy settings ........................................ 68
Proxy HA settings .................................................. 73
Best practices - Configuring the Proxy HA mode ................. 74
  Configure the Proxy HA mode .................................... 76
  Resolving issues with a Proxy HA configuration .................. 77
Best practices - High Availability configuration size limits ......... 78
Best practices - Configuring the explicit proxy mode with WCCP .. 79
  Configure use of the WCCP protocol ............................ 81
  Settings for a WCCP service ..................................... 81
  Troubleshooting WCCP-related issues ......................... 83
Transparent router mode .......................................... 84
  Configure the transparent router mode ......................... 85
  Configure nodes in transparent router mode ................. 85
Transparent Router settings ...................................... 88
Transparent bridge mode .......................................... 90
  Configure the transparent bridge mode ....................... 90
  Configure nodes in transparent bridge mode .................. 91
  Best practices - Fine-tuning a transparent bridge configuration ... 94
  Transparent Bridge settings ................................... 95
Packet size handling ............................................. 97
Secure ICAP ......................................................... 97
SOCKS proxy ....................................................... 98
  Configuring a SOCKS proxy ..................................... 98
  Using properties and an event in rules for a SOCKS proxy ... 98
  Configure SOCKS proxy settings ................................. 99
  Using UDP under SOCKS ......................................... 100
  SOCKS Proxy rule set ........................................ 101
Instant messaging .................................................. 101
XMPP proxy ......................................................... 105
Configure common proxy settings ................................ 106
Proxies settings ................................................... 106
  Network Setup .................................................. 106
  HTTP Proxy ..................................................... 106
  FTP Proxy ....................................................... 107
  ICAP Server ...................................................... 109
6 Rules

Rule flexibility .................................. 173
About filtering .................................. 174
    Filtering cycles .................................. 175
    Process flow ................................ 175
Rule elements .................................. 177
    Rule format on the user interface .......... 178
    Complex criteria .............................. 179
Rule representation in the documentation text ..................... 179
Rule sets .................................... 181
Rule set system ................................. 182
Rule set library .................................. 183
Rule Sets tab .................................. 184
Create a rule ................................... 186
    Name and enable a rule ....................... 186
    Working with the Add Criteria window ...... 187
    Add the rule criteria ........................ 189
    Add the rule action .......................... 190
    Add a rule event ................................ 191
Create a rule set ................................ 191
Import a rule set ................................ 193
Best practices - Rule configuration .......................... 194
    Using rules and rule sets in appropriate cycles ..... 194
    Using expensive properties at the end of the filtering process ..... 195
    Using not more than two properties in the criteria of a rule ........ 196
Restrict access to configuration items ......................... 198

7 Lists

List types .................................... 200
Lists tab .................................... 202
Access a list ................................... 203
    Access a list on the Lists tab .......... 204
    Access a list in a rule .................. 204
Create a list ................................... 204
    Add a new list ............................. 205
    Fill a list with entries ................. 205
Work with different types of lists ........................... 205
    Add a wildcard expression to a global whitelist for URLs ........ 206
    Add a URL category to a blocking list .... 207
    Add a media type to a media type filter list .... 207
Subscribed lists ................................... 208
    Create a subscribed list .................. 208
    Settings for subscribed lists content .... 209
    Updating subscribed lists .............. 210
    Creating a content file for a customer-maintained list .......... 211
    Best practices - Working with a McAfee-maintained subscribed list ...... 213
External lists ................................... 214
    Use of external list data in rules .......... 216
    Substitution and placeholders ............ 216
    Configure the External Lists module .... 217
    External Lists module settings ........... 218
    Configure general settings for external lists ...... 224
    External Lists system settings .......... 224
Map Type lists .................................. 225
    Create a Map Type list .................. 225
    Using properties to work with Map Type lists .......... 226
Retrieving map data from external and subscribed lists .......................................................... 227
Common Catalog ......................................................................................................................... 228
Prepare the use of Common Catalog lists .................................................................................. 229
Set up a user account for Common Catalog lists ...................................................................... 229
Set up an administrator account for Common Catalog lists ..................................................... 230
Enable use of the REST interface for Common Catalog lists .................................................... 230
Sample settings for registering Web Gateway on a McAfee ePO server .................................. 231
JavaScript Object Notation data .................................................................................................. 231

8 Settings ..................................................................................................................................... 237
Types of settings ......................................................................................................................... 237
Settings tab .................................................................................................................................. 239
Access settings ............................................................................................................................. 240
  Access action and module settings on the Settings tab ............................................................. 240
  Access action and module settings in a rule .............................................................................. 240
  Access system settings ............................................................................................................. 241
Create action and module settings .............................................................................................. 241

9 Authentication ............................................................................................................................ 243
Authenticating users ..................................................................................................................... 244
LDAP digest authentication ......................................................................................................... 245
Configure authentication ............................................................................................................. 246
Configure the Authentication module .......................................................................................... 247
Authentication settings .................................................................................................................. 247
Implement a different authentication method ............................................................................... 258
Using system settings to configure authentication ...................................................................... 258
  Kerberos Administration settings ............................................................................................ 258
  Join the appliance to a Windows domain .................................................................................. 259
  Windows Domain Membership settings ................................................................................. 260
Best practices - Configuring authentication for deployment types .............................................. 261
  Authentication for the explicit proxy mode .......................................................................... 262
  Authentication for transparent modes ..................................................................................... 264
  Authentication for the explicit proxy mode with WCCP ......................................................... 267
Best practices - Configuring LDAP authentication ...................................................................... 268
  Configure the LDAP method for authenticating a user ........................................................... 269
  Configure the settings for the LDAP authentication method ............................................... 270
  Configure queries for user and group attributes ................................................................... 271
  Storing an attribute in a separate property ............................................................................ 272
  Storing the original user name for logging .......................................................................... 273
  Testing and troubleshooting LDAP authentication ................................................................. 274
Instant messaging authentication ................................................................................................. 276
  Configure instant messaging authentication ........................................................................... 277
  Configure the Authentication module for instant messaging authentication ........................ 278
  Configure the File System Logging module for instant messaging authentication ............... 279
  IM Authentication rule set ....................................................................................................... 279
One-time passwords ...................................................................................................................... 281
  Configure one-time passwords for authenticating users ...................................................... 282
  Configure one-time passwords for authorized overriding .................................................... 282
  Configure the settings for one-time passwords ................................................................... 283
Authentication Server (Time/IP Based Session with OTP) rule set ........................................... 283
Authorized Override with OTP rule set ..................................................................................... 286
Authentication Server (Time/IP Based Session with OTP and Pledge) rule set ........................ 288
Authorized Override with OTP and Pledge rule set .................................................................. 290
Client Certificate authentication ................................................................................................. 292
  Use of certificates for Client Certificate authentication .......................................................... 293
  Rule sets for Client Certificate authentication ....................................................................... 293
Redirecting requests to an authentication server ........................................ 294
Implement Client Certificate authentication ........................................... 295
Import the Authentication Server (for X509 Authentication) rule set .......... 296
Modify a rule set to configure the use of server certificates .................. 296
Modify a rule set to configure the use of certificate authorities ............... 297
Configure a listener port for incoming requests on the appliance ............ 298
Import the Cookie Authentication (for X509 Authentication) rule set ......... 299
Modify a rule set to change the listener port for incoming requests ........... 299
Import a client certificate into a browser ........................................... 300
Administrator accounts ........................................................................ 302
Add an administrator account ............................................................... 302
Edit an administrator account ............................................................... 302
Delete an administrator account ........................................................... 303
Administrator account settings ............................................................. 303
Manage administrator roles ................................................................... 304
Administrator role settings ................................................................... 304
Configure external account management ............................................ 305

10 Quota management ........................................................................... 307
   Imposing quotas and other restrictions on web usage ......................... 307
   Time quota ...................................................................................... 310
      Configure time quotas ................................................................ 310
      Time Quota settings .................................................................. 311
      Time Quota rule set .................................................................. 311
   Volume quota .................................................................................. 313
      Configure volume quotas ............................................................ 314
      Volume Quota settings ............................................................... 314
      Volume Quota rule set ............................................................... 315
   Coaching ...................................................................................... 317
      Configure coaching .................................................................. 318
      Coaching settings .................................................................... 318
      Coaching rule set .................................................................... 318
   Authorized override ......................................................................... 320
      Configure authorized overriding ................................................. 320
      Authorized Override settings .................................................... 321
      Authorized Override rule set ..................................................... 321
   Blocking sessions ........................................................................... 323
      Configure blocking sessions ....................................................... 323
      Block Session settings ............................................................. 324
      Blocking Sessions rule set ........................................................ 324
   Quota system settings ...................................................................... 325

11 Web filtering .................................................................................... 327
   Virus and malware filtering .............................................................. 327
      Configure key elements for virus and malware filtering ................ 329
      Key elements for virus and malware filtering .............................. 329
      Configure virus and malware filtering using the complete rules view . 330
      Configure settings for the Anti-Malware module ............................ 331
      Change the module combination for scanning web objects ............. 331
      Anti-Malware settings ................................................................ 333
      Gateway Anti-Malware rule set .................................................... 337
      Media stream scanning ............................................................... 339
      Anti-malware queue .................................................................. 340
   URL filtering ................................................................................... 341
      Configure key elements for URL filtering ................................... 343
      Key elements for URL filtering ................................................... 343
#12 Supporting functions

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring the use of Advanced Threat Defense</td>
<td>417</td>
</tr>
<tr>
<td>Gateway ATD settings</td>
<td>418</td>
</tr>
<tr>
<td>Advanced Threat Defense rule set</td>
<td>420</td>
</tr>
<tr>
<td>ATD - Offline Scanning with Immediate File Availability rule set</td>
<td>421</td>
</tr>
<tr>
<td>Data loss prevention</td>
<td>423</td>
</tr>
<tr>
<td>Configure data loss prevention</td>
<td>427</td>
</tr>
<tr>
<td>Configure data loss prevention using default classifications</td>
<td>428</td>
</tr>
<tr>
<td>Configure data loss prevention using dictionary entries</td>
<td>428</td>
</tr>
<tr>
<td>Data Loss Prevention (Classifications) settings</td>
<td>430</td>
</tr>
<tr>
<td>Data Loss Prevention (Dictionaries) settings</td>
<td>431</td>
</tr>
<tr>
<td>Data Loss Prevention rule set</td>
<td>432</td>
</tr>
<tr>
<td>Preventing data loss using an ICAP server</td>
<td>434</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Progress indication</td>
<td>437</td>
</tr>
<tr>
<td>Configure progress indication</td>
<td>438</td>
</tr>
<tr>
<td>Configure the progress indication modules</td>
<td>439</td>
</tr>
<tr>
<td>Progress Page settings</td>
<td>439</td>
</tr>
<tr>
<td>Data Trickling settings</td>
<td>440</td>
</tr>
<tr>
<td>Progress Indication rule set</td>
<td>441</td>
</tr>
<tr>
<td>Bandwidth throttling</td>
<td>441</td>
</tr>
<tr>
<td>Bandwidth throttling rules</td>
<td>442</td>
</tr>
<tr>
<td>Configure bandwidth throttling</td>
<td>443</td>
</tr>
<tr>
<td>Web caching</td>
<td>444</td>
</tr>
<tr>
<td>Verify the enabling of the web cache</td>
<td>444</td>
</tr>
<tr>
<td>Web Cache rule set</td>
<td>444</td>
</tr>
<tr>
<td>Next-hop proxies</td>
<td>446</td>
</tr>
<tr>
<td>Next-hop proxy modes</td>
<td>446</td>
</tr>
<tr>
<td>Configure next-hop proxies</td>
<td>448</td>
</tr>
<tr>
<td>Add a next-hop proxy to a list</td>
<td>449</td>
</tr>
<tr>
<td>Configure the Next Hop Proxy module</td>
<td>449</td>
</tr>
<tr>
<td>Configure next-hop proxy stickiness</td>
<td>450</td>
</tr>
<tr>
<td>Next-hop proxies for SOCKS traffic</td>
<td>450</td>
</tr>
<tr>
<td>Best practices - Troubleshooting next-hop proxy issues</td>
<td>454</td>
</tr>
<tr>
<td>Next Hop Proxy settings</td>
<td>457</td>
</tr>
<tr>
<td>Add Next Hop Proxy settings</td>
<td>457</td>
</tr>
<tr>
<td>Protocol Detector settings</td>
<td>458</td>
</tr>
<tr>
<td>Next Hop Proxy rule set</td>
<td>459</td>
</tr>
</tbody>
</table>

#13 User messages

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending messages to users</td>
<td>461</td>
</tr>
<tr>
<td>Edit the text of a user message</td>
<td>463</td>
</tr>
<tr>
<td>Authenticate settings</td>
<td>464</td>
</tr>
<tr>
<td>Block settings</td>
<td>464</td>
</tr>
<tr>
<td>Redirect settings</td>
<td>465</td>
</tr>
<tr>
<td>Templates tab</td>
<td>467</td>
</tr>
<tr>
<td>Template Editor</td>
<td>467</td>
</tr>
</tbody>
</table>

#14 Cloud single sign-on

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How cloud single sign-on is configured</td>
<td>473</td>
</tr>
<tr>
<td>SSO process in proxy and non-proxy modes</td>
<td>474</td>
</tr>
<tr>
<td>Supported authentication methods</td>
<td>475</td>
</tr>
<tr>
<td>SSO Catalog of supported cloud services</td>
<td>477</td>
</tr>
<tr>
<td>Viewing the SSO Catalog</td>
<td>477</td>
</tr>
<tr>
<td>SSO Catalog in the user interface</td>
<td>478</td>
</tr>
<tr>
<td>SSO Catalog as a service</td>
<td>479</td>
</tr>
</tbody>
</table>
15 Cloud storage encryption
Encrypting and decrypting cloud storage data ............................................. 549
Configure encryption and decryption of cloud storage data .......................... 552
Configure the settings for encrypting and decrypting data ............................. 552
Cloud Storage Encryption settings .................................................................. 553
Cloud Storage Encryption Support settings ................................................... 553
Decrypt cloud storage data manually ............................................................. 554
Cloud Storage Encryption rule set .................................................................. 554

16 Hybrid solution
Working with the hybrid solution .................................................................. 557
Restrictions of the hybrid solution .................................................................. 558
Configure a hybrid solution ............................................................................ 560
Configure settings for the hybrid solution ...................................................... 560
Select a rule set for the hybrid solution ......................................................... 561
Perform synchronization manually ................................................................. 562
Web Hybrid settings ...................................................................................... 562
Legacy hybrid solution ................................................................................... 563
Synchronizing settings for the legacy hybrid solution ...................................... 564
Web filtering settings for synchronization .................................................... 564
Configure synchronization settings ............................................................... 565
Web Hybrid Legacy settings ........................................................................... 565

17 Monitoring
Dashboard ...................................................................................................... 567
Access the dashboard ...................................................................................... 568
Alerts tab ........................................................................................................ 568
Charts and Tables tab ..................................................................................... 571
Logging .......................................................................................................... 578
Administer logging ......................................................................................... 579
View log files ................................................................................................ 579
Log file types .................................................................................................. 580
Configure log file settings .............................................................................. 581
Log File Manager settings .............................................................................. 582
File System Logging settings ......................................................................... 584
Create a log ..................................................................................................... 585
Create a log handler ....................................................................................... 586
Elements of a logging rule ............................................................................. 586
Best practices - Adding a log file field ......................................................... 587
Best practices - Creating a log ........................................................................ 588
Access log rule set ........................................................................................ 594
Found Viruses Log rule set ........................................................................... 594
Error handling ............................................................................................... 595
Error handling using error IDs ....................................................................... 595
Error handling using incident information .................................................... 595
Configure error handling ............................................................................... 596
View the error handling rule sets .................................................................... 597
Best practices - Working with the Error Handler ......................................... 597
Default error handler rule set ....................................................................... 600
Performance measurement ............................................................................ 607
View performance information ..................................................................... 608
Configure performance measurement ........................................................... 608
Using properties in rules to log performance information ............................... 609
Using events in rules to measure rule set processing time ............................. 610
Event monitoring with SNMP ....................................................................... 611
Configure the SNMP settings ....................................................................... 611
### SNMP settings

SNMP settings

### Transferring data for McAfee ePO monitoring

Transferring data for McAfee ePO monitoring

- Configure the ePolicy Orchestrator settings
- ePolicy Orchestrator settings
- Bypass ePO Requests rule set

### Best practices - Sending access log data to a syslog server

Best practices - Sending access log data to a syslog server

- Add a rule for sending access log data
- Adapt the rsyslog.conf system file for sending access log data
- Resolving issues with sending access log data

### Sending syslog data to McAfee Enterprise Security Manager

Sending syslog data to McAfee Enterprise Security Manager

- Configure the sending of syslog data
- Adapt the rsyslog system file for the data transfer
- Fine-tuning the collection and evaluation of syslog data
- Resolving issues with the transfer of syslog data

### Troubleshooting

**18 Troubleshooting**

Troubleshooting methods

- Rule tracing
  - Debug rule processing issues using rule tracing
  - Rule tracing panes
  - Use rule tracing to find out why a request was blocked
  - Best practices - Find out why a web page displays no images
  - Restore removed rule traces to the rule tracing panes
  - Delete rule traces
  - Create a feedback file
  - Enable the creation of core files
  - Enable the creation of connection tracing files
  - Create a packet tracing file
  - Work with system and network tools
  - Restart a service of the operating system
  - Display running AV threads
  - Back up and restore an appliance configuration
  - Troubleshooting settings

### Configuration lists

**A Configuration lists**

List of actions

- List of actions
- List of block reason IDs
- List of error IDs
- List of events
- List of incident IDs
- List of properties
  - Properties - A
  - Properties - B
  - Properties - C
  - Properties - D
  - Properties - E
  - Properties - F
  - Properties - G
  - Properties - H
  - Properties - I
  - Properties - J
  - Properties - L
  - Properties - M
  - Properties - N
  - Properties - P
  - Properties - Q
Contents

B  REST interface 755
  Prepare use of the REST interface 755
  Enable use of the interface 756
  Give permission to access the interface 756
  Working with the REST interface 756
    Using curl as the data transfer tool 757
    Authenticating to the interface 759
    Requesting resources 760
    Performing basic activities 761
    Working on individual appliances 763
    Working with system files 764
    Working with log files 765
    Working with files uploaded for troubleshooting 766
    Working with lists 767
  Sample scripts for working with the REST interface 771

C  Third-party software 775
  Third-party software list 775

Index 783
Preface

This guide provides the information you need to work with your McAfee product.

About this guide
This information describes the guide’s target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience
McAfee documentation is carefully researched and written for the target audience. The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions
This guide uses these typographical conventions and icons.

- **Book title, term, emphasis**
  - Title of a book, chapter, or topic; a new term; emphasis.

- **Bold**
  - Text that is strongly emphasized.

- **User input, code, message**
  - Commands and other text that the user types; a code sample; a displayed message.

- **Interface text**
  - Words from the product interface like options, menus, buttons, and dialog boxes.

- **Hypertext blue**
  - A link to a topic or to an external website.

- **Note**: Additional information, like an alternate method of accessing an option.

- **Tip**: Suggestions and recommendations.

- **Important/Caution**: Valuable advice to protect your computer system, software installation, network, business, or data.

- **Warning**: Critical advice to prevent bodily harm when using a hardware product.

What's in this guide
This guide is organized to help you find the information you need. The McAfee Web Gateway appliance is introduced with overviews of main functions, deployment options, system architecture, and administrator activities. This is followed by an explanation of how to setup the appliance and complete first steps up to the point where you configure proxy, authentication, and web filtering functions.
Configuration of these main functions is explained in separate chapters.

It is also explained how to configure functions of the appliance system, such as domain name services, port forwarding, or static routes, and how to set up an appliance as a node in a Central Management configuration.

Chapters on monitoring and troubleshooting are provided at the end of the guide.

An appendix contains lists of important configuration elements, such as actions, events, properties, and others.

**Find product documentation**

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

**Task**

1. Go to the Knowledge Center tab of the McAfee ServicePortal at [http://support.mcafee.com](http://support.mcafee.com).

2. In the Knowledge Base pane, click a content source:
   - Product Documentation to find user documentation
   - Technical Articles to find KnowledgeBase articles

3. Select Do not clear my filters.

4. Enter a product, select a version, then click Search to display a list of documents.
# Introduction

The McAfee® Web Gateway (Web Gateway) appliance ensures comprehensive web security for your network.

It protects your network against threats arising from the web, such as viruses and other malware, inappropriate content, data leaks, and related issues. It also ensures regulatory compliance and a productive work environment.

## Contents

- Filtering web traffic
- Main functions of the appliance
- Main components of the appliance
- Deployment of the appliance
- High-level administration activities

## Filtering web traffic

The appliance is installed as a gateway that connects your network to the web and filters the traffic that goes out and comes in.

Following the implemented web security rules, it filters the requests that users send to the web from within your network and the responses that are sent back from the web. Embedded objects sent with requests or responses are also filtered.

Malicious and inappropriate content is blocked, while useful matter is allowed to pass through.

![Diagram of filtering web traffic](image)

**Figure 1-1 Filtering web traffic**

1 – Your network  
2 – Web Gateway  
3 – Web  
1 – Sends request to the web.  
2 – Filters requests and responses.  
3 – Sends responses to your network.
Main functions of the appliance

Filtering web traffic is a complex process. The main functions of the appliance contribute to it in different ways.

**Filtering web objects**

Special anti-virus and anti-malware functions on the appliance scan and filter web traffic and block web objects if they are infected.

Other functions filter requested URLs, using information from the Global Threat Intelligence™ system, or perform media type and application filtering.

They are supported by functions that do not filter themselves, but complete such jobs as counting user requests or indicating the progress made in downloading web objects.

**Filtering users**

Authentication functions of the appliance filter users, using information from internal and external databases and methods such as NTLM, LDAP, RADIUS, Kerberos, and others.

In addition to filtering normal users, the appliance also gives you control over administrator rights and responsibilities.

**Intercepting web traffic**

This is a prerequisite for any filtering of web objects or users. It is achieved by the proxy functions of the appliance, using different network protocols, such as HTTP, HTTPS, FTP, Yahoo, ICQ, Windows Live Messenger, XMPP, and others.

The appliance can run in explicit proxy mode or in transparent bridge or router mode.

**Monitoring the filtering process**

The monitoring functions of the appliance provide a continuous overview of the filtering process.

They include a dashboard, which displays information on alerts, web usage, filtering activities, and system behavior. Logging and tracing functions are also available, as well as options to forward data to an McAfee ePolicy Orchestrator™ (McAfee ePO) server or do event monitoring with an SNMP agent.
Main components of the appliance

The McAfee Web Gateway appliance uses several subsystems to provide filtering and other functions, based on its operating system.

Appliance subsystems

The subsystems of the appliance and their modules do the following:

- **Core subsystem** — Provides a proxy module for intercepting web traffic and a rule module for processing the filtering rules that make up your web security policy.

  This subsystem furthermore provides the modules (also known as engines) that complete special jobs for the filtering rules and can be configured by you, for example, the Anti-Malware module, the URL Filter module, or the Authentication module.

  A flow manager module ensures efficient cooperation between the modules.

- **Coordinator subsystem** — Stores all configuration data processed on the appliance

  This subsystem also provides update and Central Management functions.

- **Configurator subsystem** — Provides the user interface (internal subsystem name is *Konfigurator*)

Figure 1-2  Appliance subsystems and modules

Operating system

The subsystems of the appliance rely on the functions of its operating system, which is MLOS2 (McAfee Linux Operating System version 2).

This version is also used by other Linux-based McAfee security products, for example, by McAfee Email Gateway, which reduces your learning effort if you are the administrator for two or more of these products.
The operating system provides functions for executing the actions that the filtering rules trigger, file and network reading and writing, and access control.

A configuration daemon (sysconfd daemon) implements changed configuration settings in the operating system.

Deployment of the appliance

Before you set up the McAfee Web Gateway appliance, consider how you want to use it. You can run it on different platforms and configure different modes of network integration. You can also set up and administer multiple appliances as nodes in a Central Management configuration.

Platform

You can run the appliance on different platforms.

- **Hardware-based appliance** — On a physical hardware platform
- **Virtual appliance** — On a virtual machine

Network integration

In your network, the appliance can intercept, filter, and transmit web traffic in different modes.

- **Explicit proxy mode** — The clients that the appliance communicates with are aware of it. You must configure them “explicitly” to direct their traffic to the appliance.
- **Transparent modes** — The clients are not aware of the appliance.
  - **Transparent bridge** — The appliance acts as an “invisible” bridge between its clients and the web. You need not configure the clients for this.
  - **Transparent router** — The appliance routes traffic according to a routing table, which you need to fill out.

Administration and updates

You can administer the appliance and have updates distributed in different ways.

- **Standalone** — Administer the appliance separately and let it not receive updates from other appliances.
- **Central Management** — Set up the appliance as a node in a complex configuration and administer other nodes on its user interface, including the distribution of updates.

You can then administer the appliance on other nodes and let it receive updates from them.

High-level administration activities

Administering the appliance includes different activities, depending on the requirements of your network.

The following are recommended high-level administration activities.
Task

1. Perform the initial setup.
   The setup procedure includes the initial configuration of system parameters, such as host name and IP address, implementing an initial system of filtering rules, and licensing.
   Two wizards are available in this phase: one for the initial configuration, another for the filtering rules.

2. Configure the proxy functions.
   After the initial setup, explicit proxy mode and the HTTP protocol are preconfigured on the appliance.
   You can modify this setup and also configure other network components that the appliance communicates with.

3. Consider implementing authentication.
   Authentication is not implemented on the appliance by default.
   If you want to implement it, you can choose from a number of different authentication methods, including NTML, LDAP, Kerberos, and others.

4. Configure web filtering.
   You can review the rules that have been implemented during the initial setup for virus and malware filtering, URL filtering, media type filtering, and other filtering-related processes.
   You can finetune these rules and adapt them to the needs of your network.
   Working on the filtering rules includes maintaining the lists that the rules use and configuring the settings for rule actions and the modules that are involved in the filtering process.

5. Monitor the appliance behavior.
   When you have configured the appliance according to your requirements, you can monitor it to see how it performs the filtering process.
   You can also monitor system functions, such as CPU and memory usage, number of active connections, and others.

For more information on these activities, see the sections that deal with them, for example, under Setup, Authentication, or Web filtering.
Introduction
High-level administration activities
User interface

The user interface allows you to work with rules, lists, settings, accounts, and other items for administering Web Gateway. It provides information on key filtering and system parameters and enables you to perform troubleshooting measures.

Contents
- Main elements of the user interface
- Supporting configuration functions
- Configuring a web security policy on the user interface
- Administering Web Gateway without the user interface

Main elements of the user interface

The main elements of the user interface can be seen in the following sample screen.

![User interface screenshot]

Figure 2-1. User interface

The table below describes the main elements of the user interface.
### Table 2-1 Main elements of the user interface

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>System information line</td>
<td>Displays system and user information.</td>
</tr>
<tr>
<td>User Preferences</td>
<td>Opens a window to let you configure settings for the user interface and change your password.</td>
</tr>
<tr>
<td>Logout</td>
<td>Logs you off from the user interface.</td>
</tr>
<tr>
<td>Help icon</td>
<td>Opens the online Help. You can browse through its pages or navigate on a tree structure and perform a full text search or search for index terms.</td>
</tr>
<tr>
<td>Top-level menu bar</td>
<td>Lets you select one of the following menus:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dashboard</strong> — For viewing information on events, web usage, filtering activities, and system behavior</td>
</tr>
<tr>
<td></td>
<td>• <strong>Policy</strong> — For configuring your web security policy</td>
</tr>
<tr>
<td></td>
<td>• <strong>Configuration</strong> — For configuring the system settings of the appliance</td>
</tr>
<tr>
<td></td>
<td>• <strong>Accounts</strong> — For managing administrator accounts</td>
</tr>
<tr>
<td></td>
<td>• <strong>Troubleshooting</strong> — For solving problems on the appliance</td>
</tr>
<tr>
<td>Search</td>
<td>Opens a window with the following search options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Search for objects</strong> — Lets you search for rule sets, rules, lists, and settings. Typing a search term in the input field displays all objects with names matching the search term.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Search for objects referring to</strong> — Lets you select a list, property, or settings and displays all rules that use the selected item.</td>
</tr>
<tr>
<td>Save Changes</td>
<td>Saves your changes.</td>
</tr>
<tr>
<td>Tab bar</td>
<td>Provides the tabs of the currently selected top-level menu.</td>
</tr>
<tr>
<td></td>
<td>The top-level menus have the following tabs:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dashboard</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Alerts</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Charts and Tables</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policy</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Rule Sets</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Lists</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Settings</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Templates</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Configuration</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Appliances</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>File Editor</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Accounts</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Administrator Accounts</strong></td>
</tr>
<tr>
<td></td>
<td>The <strong>Troubleshooting</strong> top-level menu has no tabs.</td>
</tr>
<tr>
<td>Toolbar (on tab)</td>
<td>Provides varying tools (depending on the selected tab).</td>
</tr>
</tbody>
</table>
Table 2-1 Main elements of the user interface (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigation pane</td>
<td>Provides tree structures of configuration items, such as rules, lists, and</td>
</tr>
<tr>
<td></td>
<td>settings.</td>
</tr>
<tr>
<td>Configuration pane</td>
<td>Provides options for configuring the item that is currently selected on the</td>
</tr>
<tr>
<td></td>
<td>navigation pane.</td>
</tr>
</tbody>
</table>

Supporting configuration functions

The user interface provides several functions to support your configuration activities.

Table 2-2 Supporting administration functions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yellow triangle</td>
<td>Appears attached to the name of a list that is still empty and needs to be filled by you. Some filter lists are created, but not filled by the policy configuration wizard because they are too sensitive.</td>
</tr>
<tr>
<td>Yellow text insert</td>
<td>Appears when you move your mouse pointer over an item on the user interface providing information on the meaning and usage of the item.</td>
</tr>
<tr>
<td>OK icon</td>
<td>Appears in a window when the input you entered is valid.</td>
</tr>
<tr>
<td>False icon</td>
<td>Appears in a window when the input you entered is invalid.</td>
</tr>
<tr>
<td>Message text</td>
<td>Appears with the False icon, providing information on your invalid input.</td>
</tr>
<tr>
<td>Light red color of input field</td>
<td>Indicates an invalid entry.</td>
</tr>
<tr>
<td>Save Changes</td>
<td>The button turns red when you change an item.</td>
</tr>
<tr>
<td></td>
<td>It turns gray again when you have saved your changes.</td>
</tr>
<tr>
<td>Red triangle</td>
<td>Appears attached to tabs, icons, and list entries when you have changed an item and not yet saved. For example, when you have changed a rule, the red triangle appears:</td>
</tr>
<tr>
<td></td>
<td>• In the row of the rule entry on the settings pane</td>
</tr>
<tr>
<td></td>
<td>• On the rule set icon</td>
</tr>
<tr>
<td></td>
<td>• On the projection of the Rule Sets tab</td>
</tr>
<tr>
<td></td>
<td>• On the Policy icon of the top-level menu bar</td>
</tr>
</tbody>
</table>

Discarding changes

When you have been performing administrator activities on the user interface, you can discard changes you have made instead of saving them.

One option to discard changes is a positive answer when prompted at logoff whether you really want to do it with unsaved changes.

Another option is to discard changes and reload configuration data.

Reloading configuration data restores the configuration that existed after it was last saved, which can have been done by you or another administrator. If no changes have been saved yet after the initial setup of the appliance, the initial setup configuration is restored.
Discard changes by reloading data

You can discard changes you have configured on the user interface by reloading the existing configuration data.

**Task**

1. Click the small black triangle next to the *Save Changes* button.

   An insert reading *Reload Data from Backend* appears.

2. Click the insert.

   Pending changes are discarded and the configuration data is reloaded.

---

Configuring a web security policy on the user interface

On the user interface, you can configure a web security policy for your network.

A web security policy is implemented on Web Gateway by various rules, which are grouped into rule sets. The rules in a rule set usually deal with a particular field of web security. For example, there can be a rule set with rules for anti-malware filtering, for URL filtering, for media type filtering, and so on.

You can view these rules and rule sets on the user interface, edit them, delete them, and also create new rules and rule sets.

A rule contains several elements. For example, a URL filtering rule could contain a list of categories for URLs, a block action, and other elements. When a user sends a request for web access, the rule would block this request if a URL is submitted with it that falls into one of these categories.

By including this rule in your web security policy, you can make sure that users cannot access, for example, websites that fall into the categories *Online Shopping, Entertainment, or Drugs*, from within your network.

**Policy tabs**

The user interface provides three tabs for configuring a web security policy.

- **Rule Sets tab** — On this tab, you can perform all activities for configuring web security rules.
  
  You can also work with the lists and settings that are used in rules on this tab.

  For more information about working with rules, see the *Rules* chapter.

- **Lists tab** — This tab provides an alternative method of access to the lists that are used in rules.
  
  You can select lists from the lists tree and configure them.

  For more information about working with lists, see the *Lists* chapter.

- **Settings tab** — This tab provides an alternative method of access to the settings that are used in rules. You can select settings from the settings tree and configure them.

  In rule configuration on Web Gateway, the term *settings* is used to refer to a group of parameters that are set to particular values. There are two kinds of settings:

  - Settings for the modules (also known as *engines*) that perform jobs in rule processing, for example, for the Anti-Malware module, which scans web objects for infections by viruses and other malware
  
  - Settings for the actions that are executed by rules, for example, for the *Block* action
There can be various settings for a module or action. This way a module can perform its job in different ways or an action can be executed in different ways, depending on which of the various settings are configured for a module or action.

For more information about working with settings, see the Settings chapter.

- **Templates tab** — This tab allows you to work with templates that are used for configuring messages to users of Web Gateway.

  For more information about working with templates, see the User messages chapter.

**Working with the Rule Sets tab**

On the Rule Sets tab, you can select a rule set, for example, the URL Filtering rule set, and configure its rules.

Two different rule set views are available, which allow you to work with:

- **Key elements of rules** — This rule set view shows key elements of the rules in a particular rule set, but not the complete rules with all elements that might be configured.

  Key elements are the elements that you will most likely want to modify when you are configuring your web security policy. This rule set view allows you to focus your attention on working with these elements.

  This rule set view appears when you:
  - Select a default rule set
  - Import some rule sets from the rule set library

  | Some library rule sets do not appear in this view.

  This rule set view does not appear for rule sets that you have created on your own.

  The following is an example of a key element that can be configured in this view.

  ![Figure 2-2  Sample key element - URL whitelist](URL whitelist)

  **Figure 2-2  Sample key element - URL whitelist**

  A URL whitelist is an element, for example, of a rule for URL filtering.

  Click **Edit** to open the list for editing.
• **Complete rules** — This rule set view shows complete rules, and shows all the rules that are contained in a particular rule set. You can select individual elements from these rules, including the key elements, and configure them. You can also create new rules in this view or delete rules.

When you select a default rule set or a library rule set for which both views are provided, you need to leave the key elements view before you can work with the complete rules view. After leaving the key elements view, you cannot return to this view unless you discard all changes or re-import the rule set.

The URL whitelist example is a key element of a rule for URL filtering, which looks as follows when it is displayed in the complete rules view.

![Sample element within a complete rule - URL whitelist](image)

**Figure 2-3  Sample element within a complete rule - URL whitelist**

Click **URL WhiteList** to open the list for editing.

**See also**

- [Key elements view on page 28](#)
- [Complete rules view on page 30](#)

**Key elements view**

The key elements view shows key elements of the rules in a rule set and allows you to configure them.

![Key elements view](image)

**Figure 2-4  Key elements view**

**Options of the key elements view**

The following table describes the options of the key elements view.
Table 2-3 Options of the key elements view

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule set name field</td>
<td>Shows the default name of the rule set that key elements are displayed for and lets you edit this name.</td>
</tr>
<tr>
<td>Rule set description field</td>
<td>Shows the default description of the rule set that key elements are displayed for and lets you edit this description.</td>
</tr>
<tr>
<td>Enable</td>
<td>When selected, the rule set with the key elements you are currently configuring is enabled.</td>
</tr>
<tr>
<td>Unlock View</td>
<td>Leaves the key elements view and displays the corresponding complete rules view.</td>
</tr>
<tr>
<td></td>
<td>A confirmation message appears. Be aware that after leaving the key elements view, you cannot return to it unless you discard all changes or re-import the rule set.</td>
</tr>
<tr>
<td></td>
<td>On the rule sets tree, icons before the rule set name show which of the two views is currently enabled.</td>
</tr>
<tr>
<td></td>
<td>Rule set in key elements view</td>
</tr>
<tr>
<td></td>
<td>Rule set in complete rules view</td>
</tr>
<tr>
<td></td>
<td>• To work with nested rule sets, click Unlock View for the nesting rule set.</td>
</tr>
<tr>
<td></td>
<td>The nested rule sets appear on the rule sets tree, with the complete rule sets view enabled for each of them.</td>
</tr>
<tr>
<td></td>
<td>• To display the nested rule sets of the default Common Rules rule set, expand this rule set.</td>
</tr>
<tr>
<td></td>
<td>The complete rules view is already enabled for the last of the nested rule sets, while the others are still displayed in the key elements view.</td>
</tr>
<tr>
<td></td>
<td>You can use the Unlock option of the rule set context menu to leave the key elements view for one or more rule sets at once.</td>
</tr>
<tr>
<td></td>
<td>1 Select one rule set or several rule sets at once, then right-click and select Unlock.</td>
</tr>
<tr>
<td></td>
<td>You can also expand a rule set that includes nested rule sets and select one or more nested rule sets.</td>
</tr>
<tr>
<td></td>
<td>2 Confirm that you want to leave the key elements view.</td>
</tr>
<tr>
<td></td>
<td>The complete rules view is enabled for all selected rule sets.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Opens a window for configuring who is allowed to access the rule set with the key elements you are currently configuring.</td>
</tr>
<tr>
<td>Key elements for a rule set</td>
<td>The key elements vary for each rule set.</td>
</tr>
<tr>
<td></td>
<td>Key elements for related functions are displayed in a group. Each group is preceded by a group header.</td>
</tr>
<tr>
<td></td>
<td>For example, on the key elements view for URL filtering, key elements are displayed in the groups Basic Filtering, SafeSearch, and others.</td>
</tr>
<tr>
<td></td>
<td>These groups contain key elements for basic URL filtering, for additionally using SafeSearch functions in the filtering process, and for other functions.</td>
</tr>
</tbody>
</table>
Configure a key element

The following is a sample task for configuring a key element of a web security rule.

A URL is entered into a URL whitelist. This whitelist is a key element of a rule in the default URL Filtering rule set.

When a request for access to a web object is received on Web Gateway, the rule lets the request skip URL filtering if the URL that is submitted with the request is on the whitelist. This reduces filtering effort and time for requests to access "allowed" web objects.

The URL entry in the sample is http://www.mcafee.com/*. Due to the wildcard element (*), all requests with URLs that match this entry, for example, http://www.mcafee.com/us/products/web-gateway.aspx, will skip URL filtering.

Task

2. On the rule sets tree, select the URL Filtering rule set.
   Key elements of the rules in this rule set appear in the configuration pane.
3. Under Basic Filtering, click Edit next to URL Whitelist.
   The Edit List window opens.
4. Enter a URL into the whitelist.
   a. Under List content, click the Add icon.
      The Add Wildcard Expression window opens.
   b. In the Wildcard Expression field, type http://www.mcafee.com/*.
   c. Click OK.
      The Add Wildcard Expression window closes, and the URL appears in the list of the Edit List window.
5. Click OK.
   The Edit List window closes.
6. Click Save Changes.

Complete rules view

The complete rules view shows the complete rules that are contained in a rule set. It allows you to work with their elements, including the key elements.

You can edit and delete rules and create rules of your own. You can also edit, delete, and create rule sets. New rule sets can be filled with existing rules, as well as with rules of your own.
You can also import rule sets from a rule set library on Web Gateway and from an online rule set library. You can then work with these rule sets and their rules in the same way as with any other rules and rule sets.

Figure 2-5 Complete rules view
For more information about the complete rules view, see the Rules chapter.

Configure a rule element in the complete rules view
The following is a sample task for configuring an element of a web security rule in the complete rules view.

A URL is entered into a URL whitelist. This whitelist is an element of a rule in the default URL Filtering rule set. The steps for accomplishing this are almost the same as for completing this task in the key elements view. Only the way the URL whitelist is accessed is different.

When a request for access to a web object is received on Web Gateway, a rule lets the request skip URL filtering if the URL that is submitted with the request is on the whitelist. This reduces filtering effort and time for requests to access "allowed" web objects.

The URL entry in the sample is http://www.mcafee.com/*. Due to the wildcard element (*), all requests with URLs that match this entry, for example, http://www.mcafee.com/us/products/web-gateway.aspx, will skip URL filtering.

Task

2. On the rule sets tree, select the URL Filtering rule set.
   Key elements of the rules in this rule set appear in the configuration pane.

3. Click Unlock View to leave the key elements view.
   A message asks you to confirm that you want to leave the key elements view, and also warns you that you cannot return to this view.
4 Click Yes.

The complete rules view appears.

5 In the rule Allow URLs that match in URL WhiteList, click URL WhiteList.

The Edit List window opens.

6 Enter a URL into the whitelist.
   a Under List content, click the Add icon.

      The Add Wildcard Expression window opens.
   b In the Wildcard Expression field, type, for example, http://www.mcafee.com/*.
   c Click OK.

      The Add Wildcard Expression window closes, and the URL appears in the list of the Edit List window.

7 Click OK.

The Edit List window closes.

8 Click Save Changes.

For more information about working with rules and rule sets, see the Rules chapter.

---

**Administering Web Gateway without the user interface**

An additional interface is provided that allows you to administer Web Gateway without being logged on to its standard user interface. This alternative interface is referred to as REST (Representational State Transfer) interface.

Using the REST interface, you can perform administration activities on a particular Web Gateway appliance and on others that are connected to it, for example, turn off an appliance, restart it, work with lists and settings, or trigger updates.

For an introduction to the REST interface that explains basic methods of working with it and provides sample script lines for communicating with the interface, see the REST interface section in the appendix of this guide.
System configuration

The appliance system provides basic functions that are used by other functions, such as web filtering, authentication, or quota management. You can configure this system to adapt it to the requirements of your network.

When configuring the appliance system, you are dealing mainly with:

- **System settings** — Are configured for network interfaces, DNS servers, proxies, Central Management, and other components and methods that are related to the appliance system
- **System files** — Contain settings for functions of the appliance system that can be modified using the File Editor
- **Database updates** — Ensure that relevant information is made available to the filtering functions of an appliance

System configuration is in part performed during the initial setup of an appliance. After this setup, you can complete further configuration activities for the appliance system.

Contents

- Initial setup system settings
- System configuration after the initial setup
- Configure the system settings
- Appliances tab
- System settings for general appliance functions
- System settings for network functions
- Network interface bonding
- Source-based routing
- System files
- File Editor tab
- Cache volume resizing
- Database updates
- Closed network updates

Initial setup system settings

Performing the initial setup of an appliance includes configuring some of its system settings.

You can leave the initial settings at their default values or implement your own settings. Later on, you can still modify these settings.

The following table shows the settings that are configured at the initial setup and their default values.
Table 3-1 Initial setup system settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary network interface</td>
<td>eth0</td>
</tr>
<tr>
<td>Autoconfiguration with DHCP</td>
<td>yes</td>
</tr>
<tr>
<td>Host name</td>
<td>mwgappl</td>
</tr>
<tr>
<td>Root password</td>
<td>&lt;none&gt;</td>
</tr>
<tr>
<td>Remote root logon with SSH</td>
<td>on</td>
</tr>
<tr>
<td>Default gateway</td>
<td>&lt;configured by DHCP&gt;</td>
</tr>
<tr>
<td>DNS server</td>
<td>&lt;configured by DHCP&gt;</td>
</tr>
</tbody>
</table>

System configuration after the initial setup

All settings for the appliance system can be configured after its initial setup. This includes the modification of the settings that were configured during this setup.

Settings for the appliance system can be configured in different fields.

System settings for general functions

Some system settings are configured for functions of the appliance system that provide general services, such as licensing or date and time on an appliance.

See also
License settings on page 37
Telemetry settings on page 38
Date and Time settings on page 40
File Server settings on page 41
User Interface settings on page 42

Network system settings

Network system settings are configured to integrate the appliance system into the network.

Some network system settings are already configured at the initial setup, including settings for the primary network interface of an appliance and the DNS server that is used by an appliance.

Later on, you can also configure settings for the proxy functions, port forwarding, static routes, and other network-related functions.

See also
Network Interfaces settings on page 46
Domain Name Service settings on page 123
Network Protection settings on page 49
Port Forwarding settings on page 50
Static Routes settings on page 51
Proxies settings on page 106

Authentication and quota system settings

Authentication and quota system settings are configured to implement methods for authenticating users on an appliance and imposing restrictions on their web usage.

Configuring authentication and quotas is mainly done on an appliance by working with rules in authentication and quota rule sets.
However, a few authentication functions are configured as settings of the appliance system, including settings for the Kerberos authentication method and for Windows domain membership.

Some quota parameters are also configured as system settings.

**See also**
- Kerberos Administration settings on page 258
- Windows Domain Membership settings on page 260
- Quota system settings on page 325

**Web filtering system settings**
Web filtering system settings are configured to implement functions for filtering web objects on an appliance.

Web filtering configuration is mainly done on an appliance by working with rules in web filtering rule sets, such as the Gateway Antimalware or the URL Filter rule set.

However, a few web filtering functions are configured as settings of the appliance system, for example, the anti-malware queue, which collects web objects in a queue to limit work load for the scanning modules of an appliance.

**See also**
- Anti-Malware system settings on page 340

**Central Management system settings**
Central Management system settings are configured when you are running multiple appliances as nodes in a common configuration.

In a Central Management configuration, you can also configure system settings for other nodes from the node you are logged on to.

**See also**
- Central Management settings on page 161

**System settings for logging and troubleshooting**
System settings for logging and troubleshooting are configured to control the log file manager on an appliance and also for using external components to record log data.

Use of external components includes forwarding data to a McAfee ePO server and monitoring events with an SNMP agent.

**See also**
- Log File Manager settings on page 582
- ePolicy Orchestrator settings on page 615
- SNMP settings on page 612

**Configure the system settings**
You can configure settings for the appliance system to adapt it to the requirements of your network.

**Task**
1. Select Configuration | Appliances.
2. On the appliances tree, select an appliance and click the system settings you want to configure.
Configure these settings as needed.

Click Save Changes.

See also
System configuration after the initial setup on page 34

### Appliances tab

Use the Appliances tab to configure system settings on an appliance.

![Figure 3-1 Appliances tab](image)

#### Main elements of the Appliances tab

The following table describes the main elements of the Appliances tab.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliances toolbar</td>
<td>Toolbar with items for adding appliances to a Central Management configuration, removing them, and updating them all at once</td>
</tr>
<tr>
<td>Appliances tree</td>
<td>Tree structure of appliances with the system settings for each appliance</td>
</tr>
<tr>
<td>Appliance toolbar (appears when an appliance is selected on the appliances tree)</td>
<td>Toolbar with items for working with a selected appliance</td>
</tr>
<tr>
<td>Appliance settings</td>
<td>System settings for the selected appliance</td>
</tr>
</tbody>
</table>

#### Appliances toolbar

The appliances toolbar provides the following options.
## System settings for general appliance functions

Some system settings are configured for functions that provide general services of the appliance system.

Settings for general appliance functions include:

- License settings
- Date and Time settings
- File Server settings
- User Interface settings

### License settings

The License settings are used for importing a license to an appliance. Information about the license is shown together with these settings, and options for reviewing the agreements on license and data usage.

### License Administration

Settings for importing a license
### Table 3-5 License Administration

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import license</td>
<td>Provides the options that are required for importing a license.</td>
</tr>
<tr>
<td>I have read and accept the end user license agreement</td>
<td>Provides a link to the End User License Agreement and a checkbox to select after reading the document.</td>
</tr>
<tr>
<td></td>
<td>To import a license, the checkbox must be selected, otherwise the import options remains grayed out.</td>
</tr>
<tr>
<td>License file</td>
<td>Shows the name and path of the license file that has been selected after browsing the local file system.</td>
</tr>
<tr>
<td></td>
<td>When the name and path appear in this field, more license information is shown under License information.</td>
</tr>
<tr>
<td></td>
<td>The license is activated by clicking <strong>Save Changes</strong>.</td>
</tr>
<tr>
<td>Browse</td>
<td>Opens the local file system to let you browse for a license file.</td>
</tr>
</tbody>
</table>

### License Information

Information about an imported license and an option for reviewing the Data Usage Statement

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Shows the name of a license file.</td>
</tr>
<tr>
<td>Creation</td>
<td>Shows the date when a license file was created.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Shows the date when a license file expires.</td>
</tr>
<tr>
<td>License ID</td>
<td>Shows the ID of a license.</td>
</tr>
<tr>
<td>Customer</td>
<td>Shows the name of the license owner.</td>
</tr>
<tr>
<td>Customer ID</td>
<td>Shows the ID of the license owner.</td>
</tr>
<tr>
<td>Seats</td>
<td>Shows the number of workplaces in the license owner’s organization that the license is valid for,</td>
</tr>
<tr>
<td>Evaluation</td>
<td>Shows whether the license has been evaluated.</td>
</tr>
<tr>
<td>Features</td>
<td>Lists the features of Web Gateway that are covered by the license.</td>
</tr>
<tr>
<td>I have read and understood the data usage statement</td>
<td>Provides a link to the Data Usage Statement.</td>
</tr>
</tbody>
</table>

### Telemetry settings

The Telemetry settings are used for configuring the collection of feedback data about web objects that are potentially malicious, as well as about policy configuration.

### Feedback Settings

Settings for collecting feedback data

- You can separately enable or disable each of the following options.
Table 3-7 Feedback Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send feedback to McAfee about system information and suspicious URLs</td>
<td>When selected, feedback data is collected and sent to special McAfee feedback servers. McAfee collects this data to analyze it and improve the threat prediction and protection features of Web Gateway. For more information, see the Data Usage Statement.</td>
</tr>
<tr>
<td>to improve its threat prediction and protection services</td>
<td></td>
</tr>
<tr>
<td>Send feedback to McAfee about potentially malicious websites</td>
<td>When selected, relevant data for virus and malware filtering is collected and sent to a special McAfee feedback server.</td>
</tr>
<tr>
<td>Send feedback to McAfee about dynamically classified websites</td>
<td>When selected, relevant data for classifying websites is collected and sent to a special McAfee feedback server.</td>
</tr>
<tr>
<td>Send feedback to McAfee about policy configuration to improve the</td>
<td>When selected, relevant data for policy configuration is collected and sent to a special McAfee feedback server.</td>
</tr>
<tr>
<td>product</td>
<td></td>
</tr>
</tbody>
</table>

Further Information

Link to the Data Usage Statement

Table 3-8 Further Information

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Usage Statement</td>
<td>Provides a link to the data usage statement, which explains:</td>
</tr>
<tr>
<td></td>
<td>• What McAfee uses collected feedback data for</td>
</tr>
<tr>
<td></td>
<td>• What data is collected</td>
</tr>
<tr>
<td></td>
<td>• How data collection can be turned off for different types of data</td>
</tr>
<tr>
<td></td>
<td>The data usage statement has also been presented to you at the initial setup of the appliance.</td>
</tr>
</tbody>
</table>

Advanced Settings

Advanced settings for collecting feedback data

Table 3-9 Advanced Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use upstream proxy</td>
<td>When selected, a proxy server is used to send feedback data to McAfee.</td>
</tr>
<tr>
<td>IP or name of the proxy</td>
<td>Specifies the IP address or host name of the proxy server.</td>
</tr>
<tr>
<td>Port of the proxy</td>
<td>Specifies the port number of the port on the proxy server that listens for requests to send feedback data. The port number can range from 1 to 65635. The default port number is 9090.</td>
</tr>
<tr>
<td>User name</td>
<td>Provides the user name that is required for logging on to the proxy server.</td>
</tr>
<tr>
<td>Password</td>
<td>Provides the password that is required for logging on to the proxy server. Clicking Set opens a window for setting the password.</td>
</tr>
<tr>
<td>Choose feedback server</td>
<td>When selected, an IP address and port number can be configured for the server that feedback data is sent to.</td>
</tr>
<tr>
<td>IP of the server</td>
<td>Specifies the IP address of the feedback server.</td>
</tr>
</tbody>
</table>
Table 3-9  Advanced Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port of the server</td>
<td>Specifies the port number of the port on the feedback server that listens for requests to send data.</td>
</tr>
<tr>
<td></td>
<td>The port number can range from 1 to 65635.</td>
</tr>
<tr>
<td></td>
<td>The default port number is 443.</td>
</tr>
<tr>
<td></td>
<td>When selected, feedback-sending activities are logged.</td>
</tr>
</tbody>
</table>

Date and Time settings

The Date and Time settings are used for configuring the time servers that synchronize date and time of the appliance system. They also allow you to set the system time manually.

Date and Time

Settings for date and time of the appliance system

Table 3-10  Date and Time

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable time synchronization with NTP servers</td>
<td>When selected, the appliance uses time servers under the NTP (Network Time Protocol) for time synchronization.</td>
</tr>
<tr>
<td></td>
<td>The system time of the appliance is then synchronized with the time on the NTP servers. This will fail, however, if the delta between both times is too big.</td>
</tr>
<tr>
<td></td>
<td>We therefore recommend that you restart the appliance after configuring time synchronization with NTP servers. When the appliance restarts, it sets system time to the time on the NTP servers.</td>
</tr>
<tr>
<td>NTP server list</td>
<td>Provides a list for entering the servers that are used for time synchronization under the NTP protocol.</td>
</tr>
<tr>
<td></td>
<td>The list elements are as follows:</td>
</tr>
<tr>
<td></td>
<td>• String — Specifies the name of an NTP server.</td>
</tr>
<tr>
<td></td>
<td>• Comment — Provides a plain-text comment on an NTP server.</td>
</tr>
<tr>
<td>Select time zone</td>
<td>Provides a list for selecting a time zone.</td>
</tr>
<tr>
<td></td>
<td>Time synchronization performed by the NTP servers or manually set time refer to the time zone that you select here</td>
</tr>
</tbody>
</table>

Set System Time Manually

Settings for configuring time and date on the appliance system manually
Table 3-11 Set System Time Manually

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current date and time</td>
<td>Provides items for setting date and time of the appliance system.</td>
</tr>
<tr>
<td></td>
<td>• Date — Enables you to enter a date by typing it in the field or using a calendar.</td>
</tr>
<tr>
<td></td>
<td>• Calendar icon — Opens a calendar for selecting a date.</td>
</tr>
<tr>
<td></td>
<td>After selecting a date on the calendar and clicking <strong>OK</strong>, the date appears in the date field.</td>
</tr>
<tr>
<td></td>
<td>• Time — Lets you specify a time by typing it.</td>
</tr>
<tr>
<td></td>
<td>The system time of an appliance is then synchronized with the time on the NTP servers. This will fail, however, if the delta between both times is too big.</td>
</tr>
<tr>
<td></td>
<td>We therefore recommend that you restart the appliance after configuring time synchronization with NTP servers. When the appliance restarts, it sets system time to the time on the NTP servers.</td>
</tr>
<tr>
<td>Set now</td>
<td>Sets the date and time you have entered into the corresponding fields.</td>
</tr>
</tbody>
</table>

File Server settings

The File Server settings are used for configuring dedicated file server ports on an appliance to enable, for example, the downloading of files by clients.

HTTP Connector Port

Settings for dedicated file server ports on an appliance

Table 3-12 HTTP Connector Port

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable dedicated file server port over HTTP</td>
<td>When selected, the dedicated HTTP file server ports configured below are enabled.</td>
</tr>
<tr>
<td>HTTP connector</td>
<td>Specifies the port number of the dedicated HTTP file server port.</td>
</tr>
<tr>
<td></td>
<td>You can enter more than one port number here, separating them by commas. The allowed range is 1024 to 65335.</td>
</tr>
<tr>
<td></td>
<td>You can set up a port forwarding rule if you want to forward requests to ports 1–1023.</td>
</tr>
<tr>
<td></td>
<td>Instead of entering a port number alone, you can enter it with an IP address. This means connecting to an appliance over this port is only allowed when using the specified address.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>An appliance has two interfaces with IP addresses as follows:</td>
</tr>
<tr>
<td></td>
<td>eth0: 192.168.0.10, eth1: 10.149.110.10</td>
</tr>
<tr>
<td></td>
<td>You enter the following under HTTP connector:</td>
</tr>
<tr>
<td></td>
<td>4711, 192.168.0.10:4722</td>
</tr>
<tr>
<td></td>
<td>Then connecting to the appliance over port 4711 is allowed using both IP addresses, whereas connecting over port 4722 requires that IP address 192.168.0.10 is used.</td>
</tr>
<tr>
<td></td>
<td>Restricting connections in the latter way can be used for setting up an intranet.</td>
</tr>
</tbody>
</table>
Table 3-12 HTTP Connector Port (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable dedicated file server port over HTTPS</td>
<td>When selected, a dedicated HTTPS file server port is enabled.</td>
</tr>
</tbody>
</table>
| HTTPS connector | Specifies the port number of the dedicated HTTPS file server port.  
You can enter more than one port number here, separating them by commas. The allowed range is 1024 to 65335.  
Entering an IP address with a port number can be done in the same way as for the HTTP connector and has the same meaning.  
You can set up a port forwarding rule if you want to forward requests to ports 1–1023. |

User Interface settings

The User Interface settings are used for configuring elements of the local user interface of an appliance. These elements include ports, the logon page, a certificate for SSL-secured communication, and other items.

UI Access

Settings for configuring the way that the user interface of an appliance can be accessed

Table 3-13 UI Access

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| HTTP connector | Provides options for configuring access to the user interface under the HTTP protocol.  
• Enable local user interface over HTTP — When selected, you can connect to the user interface under the HTTP protocol.  
• HTTP connector — Specifies a port for connecting to the user interface under HTTP.  
• Enable REST interface over HTTP — When selected, you can connect to the REST interface under the HTTP protocol. |
| HTTPS connector | Provides options for configuring access to the user interface under the HTTPS protocol.  
• Enable local user interface over HTTPS — When selected, you can connect to the user interface under the HTTPS protocol.  
• HTTPS connector — Specifies a port for connecting to the user interface under HTTPS.  
• Enable REST interface over HTTPS — When selected, you can connect to the REST interface under the HTTPS protocol. |
**Table 3-13  UI Access (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS client certificate connector</td>
<td>Provides options for configuring a client certificate connector.</td>
</tr>
<tr>
<td></td>
<td>• Enable client certificate authentication — When selected, client certificate authentication can be performed.</td>
</tr>
<tr>
<td></td>
<td>• HTTPS connector for client certificate authentication — Specifies a port for connecting to the user interface when client certificate authentication is performed.</td>
</tr>
<tr>
<td></td>
<td>• Redirect target after authentication — When selected, a request is redirected after client certificate authentication has successfully been performed.</td>
</tr>
<tr>
<td></td>
<td>• Redirection host and port — Specifies the host system and the port on this system that requests are redirected to.</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Provides miscellaneous options for configuring access to the user interface.</td>
</tr>
<tr>
<td></td>
<td>• Session timeout — Limits the time (in minutes) that elapses before a session on the user interface is closed if no activities occur.</td>
</tr>
<tr>
<td></td>
<td>The range for the session timeout is 1–99,999 minutes.</td>
</tr>
<tr>
<td></td>
<td>The timeout is 30 minutes by default.</td>
</tr>
</tbody>
</table>

**Login Page Options**

Settings for the page that is used to log on to the user interface of an appliance

**Table 3-14  Login Page Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow browser to save login credentials</td>
<td>When selected, credentials submitted by a user for logging on to an appliance are saved by the browser.</td>
</tr>
<tr>
<td>Restrict browser session to IP address of user</td>
<td>When selected, a session for working with the user interface is only valid as long as the IP address of the client that the user started this session from remains the same.</td>
</tr>
<tr>
<td>Let user decide to restrict session for IP address or not</td>
<td>When selected, it is up to the user who started a session for working with the user interface whether it should be valid only for the IP address of the client that the session was started from.</td>
</tr>
<tr>
<td>Allow multiple logins per login name</td>
<td>When selected, more than one user can log on to the user interface using the same user name and password.</td>
</tr>
<tr>
<td>Use HTTPOnly session cookies (applet loading may take longer)</td>
<td>When selected, HTTPOnly cookies are used for a session with the user interface.</td>
</tr>
<tr>
<td>Maximum number of active applet users</td>
<td>Limits the number of users that can be logged on to the user interface of an appliance at the same time.</td>
</tr>
<tr>
<td></td>
<td>The maximum number of users is 20 by default.</td>
</tr>
<tr>
<td>Login message</td>
<td>Provides the following options for displaying an additional message on the page used for logging on to the user interface.</td>
</tr>
<tr>
<td></td>
<td>You can work with these options if you want to display a message, for example, to comply with internal policies or external regulations.</td>
</tr>
<tr>
<td></td>
<td>• Show on login page — When selected, the text that you type in the HTML message field, appears on the logon page.</td>
</tr>
<tr>
<td></td>
<td>• HTML message — The text that you type in this field appears on the logon page.</td>
</tr>
</tbody>
</table>
User Interface Certificate

Settings for a certificate that is used in SSL-secured communication over the HTTPS port for the user interface

Table 3-15  User Interface Certificate

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject, Issuer, Validity, Extensions</td>
<td>Provide information about the certificate that is currently in use.</td>
</tr>
<tr>
<td>Import</td>
<td>Opens the Import Certificate Authority window for importing a new certificate.</td>
</tr>
<tr>
<td>Certificate chain</td>
<td>Displays a certificate chain that is imported with a certificate.</td>
</tr>
</tbody>
</table>

Import Certificate Authority window

Settings for importing a certificate that is used in SSL-secured communication

Table 3-16  Import Certificate Authority window

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>Specifies the name of a certificate file.</td>
</tr>
<tr>
<td></td>
<td>The file name can be entered manually or by using the Browse button in the same line.</td>
</tr>
<tr>
<td>Browse</td>
<td>Opens the local file manager to let you browse for and select a certificate file.</td>
</tr>
<tr>
<td>Private key</td>
<td>Specifies the name of a private key file.</td>
</tr>
<tr>
<td></td>
<td>The file name can be entered manually or by using the Browse button in the same line.</td>
</tr>
<tr>
<td></td>
<td>Only keys that are AES-128-bit encrypted or unencrypted keys can be used here.</td>
</tr>
<tr>
<td>Browse</td>
<td>Opens the local file manager to let you browse for and select a private key file.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets a password that allows the use of a private key.</td>
</tr>
<tr>
<td>Import</td>
<td>Opens the Import Certificate Authority window for importing a new certificate.</td>
</tr>
<tr>
<td>OK</td>
<td>Starts the import process for the specified certificate.</td>
</tr>
<tr>
<td>Certificate chain</td>
<td>Specifies the name of a certificate chain file.</td>
</tr>
<tr>
<td></td>
<td>The file name can be entered manually or by using the Browse button in the same line.</td>
</tr>
<tr>
<td>Browse</td>
<td>Opens the local file manager to let you browse for and select a certificate chain file. After importing a certificate with a certificate chain, the certificate chain is displayed in the Certificate chain field of the User Interface Certificate settings.</td>
</tr>
</tbody>
</table>

Memory Settings

Settings for the memory that is available when working with the user interface of an appliance
### Table 3-17 Memory Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount of maximum memory available for GUI applet</td>
<td>Limits the amount of memory (in MiB) that is available for the user interface applet. The range for the available maximum is 100–999 MiB. The available maximum is 512 MiB by default.</td>
</tr>
<tr>
<td>Amount of maximum memory available for MWG UI backend</td>
<td>Limits the amount of memory (in MiB) that is available for the user interface backend. The range for the available maximum is 100–9999 MiB. If no value is specified here, the default maximum of 512 MiB is configured.</td>
</tr>
</tbody>
</table>

### REST Settings

Settings for configuring use of the REST interface to work with an appliance

### Table 3-18 REST Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size of a REST request</td>
<td>Limits the size (in MiB) of a request that is sent to the REST interface. The maximum amount of memory that is available when working with the REST interface is 200 MiB. The maximum size of a request is 2 MiB by default.</td>
</tr>
<tr>
<td>Maximum memory per REST session</td>
<td>Limits the amount of memory (in MiB) that is available for a session when working with the REST interface. The maximum amount of memory that is available when working with the REST interface is 200 MiB. The maximum amount of memory for a session is 10 MiB by default.</td>
</tr>
<tr>
<td>Maximum number of active REST users</td>
<td>Limits the number of users that can work with the REST interface at the same time. The maximum number of users is 20 by default.</td>
</tr>
</tbody>
</table>

### System settings for network functions

Some system settings are configured for functions that integrate the appliance system into your network.

System settings for network functions include proxy settings and the following settings:

- Network Interfaces settings
- Domain Name Service settings
- Network Protection settings
- Static Routes settings
- Port Forwarding settings

See also

*Proxies settings on page 106*
Network Interfaces settings

The Network Interfaces settings are used for configuring the network interfaces of an appliance.

Network Interface Settings

Settings for network interfaces

Table 3-19  Network Interface Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Host name / Fully qualified domain name | Specifies the host name of an appliance.  
The name must be specified as fully qualified domain name. |
| Default gateway (IPv4)          | Specifies the default gateway for web traffic under IPv4.                   |
| Default gateway (IPv6)          | Specifies the default gateway for web traffic under IPv6.                   |
| Enable these network interfaces | Provides a list of network interfaces that are available for being enabled or disabled.  
The eth0 network interface is by default included in the list and enabled. |
| IPv4                            | Provides options for configuring network interfaces under IPv4.  
The options are provided on a separate tab. |
| IPv6                            | Provides options for configuring network interfaces under IPv6.  
The options are provided on a separate tab. |
| Advanced                        | Provides options for configuring additional media and a bridge for a network interface.  
The options are provided on a separate tab. |
| Add VLAN                        | Opens a window for adding a network interface for VLAN traffic.             |
| Delete                          | Deletes a selected network interface for VLAN traffic.                      |

The following tables describe the options on the IPv4, IPv6, and Advanced tabs.

**IPv4**

Tab for configuring network interfaces under IPv4
Table 3-20 IPv4

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP settings</strong></td>
<td>Lets you select a method to configure an IP address for a network interface.</td>
</tr>
<tr>
<td>• Obtain automatically (DHCP) — The IP address is automatically obtained, using the Dynamic Network Host Protocol (DHCP).</td>
<td></td>
</tr>
<tr>
<td>• Configure manually — The IP address is configured manually.</td>
<td></td>
</tr>
<tr>
<td>• Disable IPv4 — IPv4 is not used for this interface.</td>
<td></td>
</tr>
<tr>
<td><strong>IP address</strong></td>
<td>Specifies the IP address of a network interface (manually configured).</td>
</tr>
<tr>
<td><strong>Subnet mask</strong></td>
<td>Specifies the subnet mask of a network interface (manually configured).</td>
</tr>
<tr>
<td><strong>Default route</strong></td>
<td>Specifies the default route for web traffic using the network interface (manually configured).</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>Limits the number of bytes in a single transmission unit to the specified value.</td>
</tr>
<tr>
<td><strong>IP aliases</strong></td>
<td>Provides a list of aliases for the IP address.</td>
</tr>
<tr>
<td>• Add alias — Opens the Input window for adding an alias.</td>
<td></td>
</tr>
<tr>
<td>• Delete — Deletes a selected alias.</td>
<td></td>
</tr>
</tbody>
</table>

IPv6

Tab for configuring network interfaces under IPv6

Table 3-21 IPv6

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP settings</strong></td>
<td>Lets you select a method to configure an IP address for a network interface.</td>
</tr>
<tr>
<td>• Obtain automatically (DHCP) — The IP address is automatically obtained, using the Dynamic Network Host Protocol (DHCP).</td>
<td></td>
</tr>
<tr>
<td>• Solicit from router — The IP address is obtained from a router.</td>
<td></td>
</tr>
<tr>
<td>• Configure manually — The IP address is configured manually.</td>
<td></td>
</tr>
<tr>
<td>• Disable IPv6 — IPv6 is not used for this interface.</td>
<td></td>
</tr>
<tr>
<td><strong>IP address</strong></td>
<td>Specifies the IP address of a network interface (manually configured).</td>
</tr>
<tr>
<td><strong>Default route</strong></td>
<td>Specifies a default route for web traffic using the network interface (manually configured).</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>Limits the number of bytes in a single transmission unit to the specified value.</td>
</tr>
<tr>
<td><strong>IP aliases</strong></td>
<td>Provides a list of aliases for the IP address.</td>
</tr>
<tr>
<td>• Add alias — Opens a window for adding an alias.</td>
<td></td>
</tr>
<tr>
<td>• Delete — Deletes a selected alias.</td>
<td></td>
</tr>
</tbody>
</table>

Advanced

Tab for configuring advanced network interface functions.

The tab provides different options when the currently selected network interface is a bonding interface. These options are described in a second table.
Table 3-22 Advanced

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>Lets you select additional media for use with a network interface.</td>
</tr>
<tr>
<td></td>
<td>• Automatically detect — Media for use with a network interface are automatically detected if available in the network environment of an appliance.</td>
</tr>
<tr>
<td></td>
<td>• 1000Base-T-FD, 1000Base-HD, ... — The selected media item is used with a network interface.</td>
</tr>
<tr>
<td>Bridge enabled</td>
<td>When selected, web traffic is routed through a network interface in transparent bridge mode.</td>
</tr>
<tr>
<td></td>
<td>• Name — Specifies the name of the transparent bridge.</td>
</tr>
<tr>
<td>Bond enabled</td>
<td>When selected, the currently selected network interface, for example, eth2, is configured as a bonded interface that is subordinated to a bonding interface.</td>
</tr>
<tr>
<td></td>
<td>• Name — Specifies the name of the bonding interface.</td>
</tr>
</tbody>
</table>

The following table describes the options provided on the Advanced tab when a bonding interface is selected.
### Advanced

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bonding</td>
<td>Provides options for a bonding interface.</td>
</tr>
<tr>
<td>options</td>
<td>• <strong>Mode</strong> — Specifies the mode used to let the bonded network interfaces in</td>
</tr>
<tr>
<td></td>
<td>the bonding configuration become active.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active/Passive</strong> — When selected, only one bonded interface is active</td>
</tr>
<tr>
<td></td>
<td>at any time. A different bonded interface becomes active only if the active</td>
</tr>
<tr>
<td></td>
<td>bonded interface fails. The MAC address of the bonding interface is only</td>
</tr>
<tr>
<td></td>
<td>visible externally on one port, which avoids address confusion for a network</td>
</tr>
<tr>
<td></td>
<td>switch. The mode is referred to in some system messages as <em>mode 1</em>.</td>
</tr>
<tr>
<td></td>
<td>The mode is selected by default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>802.3ad/LACP</strong> — When selected, all bonded interfaces in the bonding</td>
</tr>
<tr>
<td></td>
<td>configuration are active. The bonded interface for outgoing traffic is</td>
</tr>
<tr>
<td></td>
<td>selected according to the configured hash policy. When this mode is selected,</td>
</tr>
<tr>
<td></td>
<td>the <strong>LACP rate</strong> and <strong>Hash policy</strong> options become accessible.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Miimon</strong> — Sets the time interval (in milliseconds) for sending the</td>
</tr>
<tr>
<td></td>
<td>polling messages of the MII monitoring program. The default interval is</td>
</tr>
<tr>
<td></td>
<td>100 milliseconds.</td>
</tr>
<tr>
<td></td>
<td>• <strong>LACP rate</strong> — Sets the transmission rate for sending LACP-DU data</td>
</tr>
<tr>
<td></td>
<td>packets in 802.3ad mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Slow</strong> — When selected, data packets are sent every 30 seconds.</td>
</tr>
<tr>
<td></td>
<td>This transmission rate is selected by default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fast</strong> — When selected, data packets are sent every second.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hash policy</strong> — Determines the way that a hash value is calculated for</td>
</tr>
<tr>
<td></td>
<td>a bonding configuration.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Layer2</strong> — When selected, a combination of layer 2 values is used to</td>
</tr>
<tr>
<td></td>
<td>calculate the hash. The values that are included in this combination are</td>
</tr>
<tr>
<td></td>
<td>hardware MAC addresses and packet type ID addresses. This hash policy is</td>
</tr>
<tr>
<td></td>
<td>selected by default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Layer2+3</strong> — When selected, a combination of layer 2 and layer 3</td>
</tr>
<tr>
<td></td>
<td>protocol information is used to calculate the hash.</td>
</tr>
</tbody>
</table>

### Network Protection settings

The Network Protection system settings are used for configuring protective rules for traffic coming in to an appliance from your network.

### Network Protection Rules

Settings for configuring network protection rules
Table 3-24  Network Protection Rules

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable network protection</td>
<td>When selected, the settings configured in the following for network protection are enabled.</td>
</tr>
<tr>
<td>Input policy</td>
<td>Lets you select the action taken on incoming traffic.</td>
</tr>
<tr>
<td></td>
<td>Incoming traffic can either be dropped or accepted.</td>
</tr>
<tr>
<td>Allow Ping requests</td>
<td>When selected, the appliance accepts and answers Ping requests.</td>
</tr>
<tr>
<td>Exceptions from default policy</td>
<td>Provides a list for entering the network devices that send traffic to an appliance.</td>
</tr>
<tr>
<td></td>
<td>Traffic from these devices is not handled according to the rules that are currently implemented. When these rules drop incoming traffic, traffic sent from the devices listed here is accepted and vice versa.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the list of exceptions from the default policy.

Table 3-25  Exceptions from default policy – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Specifies the name of a network device that sends traffic to the appliance.</td>
</tr>
<tr>
<td></td>
<td>Typing * or no input means all devices are covered.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specified the protocol used for sending traffic.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies the IP address or address range of the network device or devices that send traffic to the appliance.</td>
</tr>
<tr>
<td>Destination port</td>
<td>Specifies the port on an appliance that is the destination of network traffic.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on an exception.</td>
</tr>
</tbody>
</table>

Port Forwarding settings

The Port Forwarding settings are used for configuring rules that let an appliance forward web traffic sent from a port on a particular host to another port.

Port Forwarding

Settings for configuring port forwarding rules

Table 3-26  Port Forwarding

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port forwarding rules</td>
<td>Provides a list of port forwarding rules.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the list of port forwarding rules.

Table 3-27  Port forwarding rules – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source host</td>
<td>Specifies the IP address of a host that is the source of web traffic in a port forwarding rule.</td>
</tr>
<tr>
<td>Bind IP</td>
<td>Specifies the bind IP address.</td>
</tr>
<tr>
<td>Target port</td>
<td>Specifies the port that web traffic from the source host is forwarded to.</td>
</tr>
<tr>
<td>Destination host</td>
<td>Specifies the IP address of the host that is the destination of web traffic sent from the source host.</td>
</tr>
</tbody>
</table>
Table 3-27 Port forwarding rules – List entry (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination port</td>
<td>Specifies the port on the destination host used for listening to web traffic coming in from the source host.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a port forwarding rule.</td>
</tr>
</tbody>
</table>

The Port Forwarding settings continue as follows.

Table 3-28 Port Forwarding (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable extended connection logging</td>
<td>When selected, all logs for port forwarding are stored on the appliance system under /var/log/mwg_fwd.log.  The logging options that you configure here apply to all port forwarding that performed under the configured port forwarding rules. The stored log files can also be viewed on the user interface under the Troubleshooting top-level menu. Select the appliance that you want to view log files for, then select Log files and open the system folder.</td>
</tr>
<tr>
<td>Customize extended logging fields</td>
<td>When selected, the input fields for configuring the type of data that should be logged become accessible.</td>
</tr>
<tr>
<td>Log on success</td>
<td>Lets you enter the type of data to be logged when web traffic is successfully forwarded. You can enter one or more of the following data types by typing them in capital letters, separated by commas: PID, HOST, USERID, EXIT, DURATION, TRAFFIC.</td>
</tr>
<tr>
<td>Log on failure</td>
<td>Lets you enter the type of data to be logged when forwarding web traffic failed. You can enter one or more of the following data types by typing them in capital letters, separated by commas: HOST, USERID, ATTEMPT. HOST data is logged by default.</td>
</tr>
</tbody>
</table>

Static Routes settings

The Static Routes settings are used for configuring routes that always use the same gateway and interface on this gateway when web traffic is routed from an appliance to a particular host.

Static Routes

Settings for static routes under IPv4 or IPv6

Table 3-29 Static Routes

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static routes list</td>
<td>Provides a list of static routes for transmitting web traffic under IPv4 or IPv6.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the list of static routes.

Table 3-30 Static routes list – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Specifies the IP address and (optionally) net ask of the host that is the destination of a static route.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Specifies the IP address of the gateway for routing web traffic from the appliance to a host.</td>
</tr>
<tr>
<td>Device</td>
<td>Specifies the interface used on a gateway for a static route.</td>
</tr>
</tbody>
</table>
### Table 3-30 Static routes list – List entry (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Provides a plain-text description of a static route.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a static route.</td>
</tr>
</tbody>
</table>

### Source-based routing

Settings for source-based routing under IPv4 or IPv6

#### Table 3-31 Source-based routing

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source-based routing for IPv4</td>
<td>When selected, source-based routing is performed under IPv4.</td>
</tr>
<tr>
<td>Source-based routing for IPv6</td>
<td>When selected, source-based routing is performed under IPv6.</td>
</tr>
<tr>
<td>Static source routing table number</td>
<td>Provides a list of entries for source routing tables that are used to route the traffic that is sent and received through the management user interface.</td>
</tr>
<tr>
<td>Source-based routing list for IPv4</td>
<td>Provides a list of routing entries for the traffic that is sent and received through the management user interface. These routing entries are for a network where IPv4 is followed.</td>
</tr>
<tr>
<td>Source-based routing list for IPv6</td>
<td>These routing entries are for a network where IPv6 is followed.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the list for static source routing tables.

#### Table 3-32 Static source routing table number – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source information to look up routing table</td>
<td>Specifies the source IP address of the traffic that is routed according to the configured static source routing table.</td>
</tr>
<tr>
<td>Routing table number</td>
<td>Specifies the number of the routing table for routing the traffic that is sent and received through the management user interface.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a static source routing table.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the list for source-based routing under IPv4.

#### Table 3-33 Source-based routing list for IPv4 – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Specifies the IP address range (in CIDR notation) for the destinations of the traffic that is sent through the management network interface.</td>
</tr>
<tr>
<td>Routing table number</td>
<td>Specifies the number of the routing table for routing the traffic that is sent and received through the management user interface.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Specifies the IP address of the gateway for the traffic that is sent and received through the management network interface.</td>
</tr>
<tr>
<td>Device</td>
<td>Specifies the name of the network interface that is configured as the management network interface.</td>
</tr>
<tr>
<td>Source IP</td>
<td>Specifies the IP address of the network interface that is configured as the management network interface. This address is the source IP address of the traffic that is routed according to the routing table.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on an entry for source-based routing.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the list for source-based routing under IPv6.
Table 3-34  Source-based routing list for IPv6 – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Specifies the IP address range (in CIDR notation) for the destinations of the traffic that is sent through the management network interface.</td>
</tr>
<tr>
<td>Routing table number</td>
<td>Specifies the number of the routing table for routing the traffic that is sent and received through the management user interface.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Specifies the IP address of the gateway for the traffic that is sent and received through the management network interface.</td>
</tr>
<tr>
<td>Device</td>
<td>Specifies the name of the network interface that is configured as the management network interface.</td>
</tr>
</tbody>
</table>
| Source IP         | Specifies the IP address of the network interface that is configured as the management network interface.  
                      This address is the source IP address of the traffic that is routed according to the routing table. |
| Comment           | Provides a plain-text comment on an entry for source-based routing. |

Network interface bonding

Bonding two or more network interfaces enables them to act as one while increasing bandwidth and providing High Availability.

The network interfaces on Web Gateway, for example, the eth2 and eth3 interfaces, can be bound together to form a single channel. A bonding kernel module is created this way and made accessible through a common network interface, which is referred to as the bonding interface.

The network interfaces that are bound together under the bonding interface are referred to as the bonded interfaces. These interfaces can be provided by different NICs.

The terms "master" and "subordinate" are also used to refer to a bonding and a bonded interface, respectively. In some system messages, you will also see the term "slave" used for a bonded interface.

With regard to the components and processes that are involved, network interface bonding is also known as NIC bonding, ethernet bonding, or channel bonding.

You can configure network interface bonding on the user interface of Web Gateway. To verify that a bonding interface has successfully been configured, you can run some suitable commands from a system console.

A VLAN can be configured on a bonding interface in the same way as on an ordinary network interface, using the relevant configuration options of the user interface.

When the transparent bridge or router mode are configured for a network, network interface bonding cannot be implemented.
Configure network interface bonding

To configure network interface bonding, create a bonding interface and configure parameters for this interface and the bonding configuration.

**Task**

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure network interface bonding on and click Network Interfaces.

   The Network Interfaces settings appear in the configuration pane.

3. Create a bonding interface.
   
   a. Under Enable these network interfaces, select a network interface that you want to run as a bonded interface, for example, eth2.
   
   b. On the Advanced tab, select Bond enabled and in the Name field type the name of the bonding interface that you want to create, for example, bond1.

   Repeat substeps a and b for another network interface that you want run as a bonded interface under this bonding interface.

   You can also add further network interfaces as bonded interfaces and have more than two network interfaces in the bonding configuration.

   c. Click Save Changes.

   d. Log out and log on again.

      After the logon, the new bonding interface appears in the list under Enable these network interfaces.

4. Configure parameters for the bonding interface.

   a. Select the bonding interface and click the IPv4 or IPv6 tab, according to the protocol version that is used in your network.

   b. Select Configure manually and under IP address and subnet mask type an IP address and the values for a subnet mask.

      You can leave the default value under MTU, which specifies the maximum number of bytes in a single transmission unit, as it is.

5. Configure parameters for the bonding configuration.

   a. Select the bonding interface and click the Advanced tab.

   b. Under Mode, select one of the following bonding modes.

      • Active/Passive — In this mode, only one bonded interface in the bonding configuration is active at any time. A different bonded interface becomes active only if the active bonded interface fails.

      The MAC address of the bonding interface is only visible externally on one port, which avoids address confusion for a network switch.

      This mode is referred to in some system messages as mode 1.

      The mode is selected by default.
• **802.3ad/LACP** — In this mode, all bonded interfaces in the bonding configuration are active. The bonded interface for outgoing traffic is selected according to the configured hash policy.

  This mode is referred to in some system messages as **mode 4**.

  When this mode is selected, the **LACP rate** and **Hash policy** options become accessible.

c Under **Miimon**, configure monitoring for the bonding interface.

  The value that you configure here sets the time interval (in milliseconds) for sending the polling messages of the MII monitoring program.

  The default interval is 100 milliseconds.

d If you have selected **802.3ad/LACP** as bonding mode, select options that are specific to this mode.

  Under **LACP rate**, select the transmission rate for the LACP-DU data packets that are exchanged between bonding and bonded network interfaces.

  • **Slow** — With this transmission rate, data packets are sent every 30 seconds.

    This transmission rate is selected by default.

  • **Fast** — With this transmission rate, data packets are sent every second.

  Under **Hash policy**, select one of the following options.

  • **Layer2** — This policy uses a combination of layer 2 values to calculate the hash. The values that are included in this combination are hardware MAC addresses and packet type ID addresses.

    This hash policy is selected by default.

  • **Layer2+3** — This policy uses a combination of layer 2 and layer 3 protocol information to calculate the hash.

  6 Click **Save Changes**.

  **See also**
  
  Network Interfaces settings on page 46

**Checking the bonding configuration**

You can verify that you have successfully configured a bonding network interface from a system console.

To verify that the bonding configuration runs with the parameters that you have configured, you can use a suitable network script. An additional command enables you to check the status of the bonding interface and the network interfaces that are bound to it.

**Verifying the configuration parameters**

The **ifcfg** network script allows you to verify that the network interfaces of the bonding configuration are running with the configured parameters, such as the bonding mode or the IP address of the bonding interface.

To view the parameters for the bonding interface, for example, **bond 1**, run the network script using the following command:

```bash
cat /etc/sysconfig/network-scripts/ifcfg-bond1
```
The command returns, for example, the following lines.

```
### BEGIN AUTOGENERATED CONFIG
BONDING_OPTS='mode=1 miimon=600'
BOOTPROTO='none'
DEVICE='bond1'
IPADDR='10.11.12.12'
...
```

To view the parameters for a bonded interface, for example, `eth2 1`, run the following command:

```
cat /etc/sysconfig/network-scripts/ifcfg-bond1
```

The command returns, for example, the following lines.

```
### BEGIN AUTOGENERATED CONFIG
BOOTPROTO='none'
MASTER='bond1'
SLAVE='yes'
DEVICE='eth2'
...
```

**Checking the network interface status**

You can check whether the bonded network interfaces are running properly under the bonding interface and which of the bonded interfaces is currently in active (slave) status.

Run the following command, for example, if the bonding interface is `bond1`:

```
cat /proc/net/bonding/bond1
```

The command returns, for example, the following lines.

```
### Ethernet Channel Bonding Driver: v. 3.7.1 (April 27, 2015)
Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
MII Status: up
MII Polling Interval (ms): 600
Up Delay (ms): 0
Down Delay (ms): 0
Slave Interface: eth2
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW Addr: 00:0c:29:e0:a7:37
Slave Queue ID: 0
Slave Interface: eth3
MII Status: up
...
```

**Source-based routing**

When configuring routing for traffic in your network, you can let routing decisions be based on the source IP address. This routing method is known as source-based routing.

Using this method you can separate the management traffic that an administrator creates when accessing the user interface of a Web Gateway appliance from the traffic that the administrator or end users create when accessing the web. The two kinds of traffic can also be protected by a separate firewall for each of them.
To implement the method, you allow administrator access to the user interface only through a particular network interface on the appliance. This network interface is the management network interface, while a different network interface is configured for access to the web.

You can also configure that monitoring information, for example, SNMP messages, must access the appliance through the management network interface.

After passing through the management interface, traffic can be identified for further routing by its source IP address, which is the address of the management interface.

Configuring the routing for this traffic includes two main steps:

- Configuring a routing table
- Configuring a route within this table

The source IP address is specified in both steps to ensure that traffic with this address is routed according to a particular table and route.

Different routing tables can be configured and entered in a list on Web Gateway while different routes can be configured for each table.

You can configure routes for use under IPv4 or IPv6, depending on which version of this protocol is followed within your network.

### Configure source-based routing for a management network interface

Configure source-based routing to separate other traffic from traffic that has a management network interface as its source.

#### Task

1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to configure source-based routing on.
3. Configure use of the management network interface for administrator access to the user interface.
   a. Click User Interface.
   b. Under HTTP Connector, proceed as follows.
      i. Make sure Enable local user interface over HTTP is selected.
      ii. In the HTTP connector field, type the IP address and listener port of the management network interface.
4. Configure use of the management network interface for SNMP messages.
   a. Click SNMP.
   b. Under SNMP Port Settings, click the Add icon on the toolbar of the Listener address list.
      The Add SNMP Listeners window opens.
   c. In the Listener address field, type the IP address and listener port of the management network interface.
   d. Click OK.

The window closes and the listener address appears in the list.
5 Configure source-based routing for traffic that is sent and received through the management network interface.
   a Click Static Routes.
   b Under Source-based routing, select Source-based routing for IPv4 or Source-based routing for IPv6, depending on the IP version used in your network.

   Two lists for configuring source-based routing appear.
   c On the toolbar of the Static source routing table number list, click the Add icon.

   The Add ApplianceSourceBasedRoutingTable window opens.
   d Configure an entry for the routing table as follows.
      • In the Source information to look up routing table field, type the IP address of the management network interface.
      • In the Routing table number field, type the number of the routing table for the traffic that is sent and received through the management network interface.
   e Click OK.

   The window closes and the routing table entry appears in the list.
   f On the toolbar of the Source-based routing list for IPv4 (or the list for IPv6), click the Add icon.

   The Add ApplianceSourceBasedRoutingIPv4 window (or the window for IPv6) opens.
   g Configure a routing entry as follows.
      • In the Destination field, type the IP address range in CIDR notation for the destinations of the traffic that is sent through the management network interface.
      • In the Routing table number field, type the number of the routing table for the traffic that is sent and received through the management network interface.
      • In the Gateway field, type the IP address of the gateway for the traffic that is sent and received through the management network interface.
      • In the Device field, type the name of the network interface that you want to configure as the management network interface.
      • In the Source IP field, type the IP address of the network interface that you want to configure as the management network interface.
   h Click OK.

   The window closes and the routing entry appears in the list.

6 Click Save Changes.

See also
Static Routes settings on page 51
System files

System files contain settings for functions of the appliance system. You can edit these settings using the File Editor.

The settings that are stored in system files include settings of parameters the appliance system uses for network communication, for example, IP addresses, the maximum message size, or the maximum number of messages in a queue.

Other settings are used to configure functions of the appliance system such as logging, access restrictions, and others.

An example for a system file is the `/etc/hosts` file, which contains entries for IP addresses and host names, including the local IP address and host name of the appliance itself.

The File Editor allows you to edit the settings in these files. It is accessible on a tab of the user interface.

To edit system files, only use the File Editor. If you open these files outside the File Editor to edit them manually, your changes will be overwritten when an upgrade to a new version of Web Gateway is performed.

See also

`File Editor tab` on page 59

File Editor tab

The `File Editor` tab allows you to edit system files on an appliance.

Main elements of the File Editor tab

The following table describes the main elements of the `File Editor` tab.
### Table 3-35  Main elements of the File Editor tab

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files</td>
<td>Tree structure of appliances with the system files for each appliance</td>
</tr>
<tr>
<td>Editor</td>
<td>Toolbar with items for editing a system file and content pane for displaying the file entries (appears when a system file is selected under Files)</td>
</tr>
</tbody>
</table>

### Editor toolbar

The Editor toolbar provides the following options.

### Table 3-36  File Editor toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Opens a menu with options for editing the text in system file entries.</td>
</tr>
<tr>
<td></td>
<td>• Cut — Cuts out selected text</td>
</tr>
<tr>
<td></td>
<td>• Delete — Deletes selected text</td>
</tr>
<tr>
<td></td>
<td>• Copy — Copies selected text</td>
</tr>
<tr>
<td></td>
<td>• Select All — Selects the complete text</td>
</tr>
<tr>
<td>Paste</td>
<td>Paste copied or cut-out text</td>
</tr>
<tr>
<td>Discard changes</td>
<td>Discards text changes. A window opens to let you confirm the discarding.</td>
</tr>
</tbody>
</table>
When the `yum upgrade` command is used to set up an appliance, the wizard must also be started manually.

The path and file name for the main log that records the activities of the wizard are `/var/log/resize-cache.log`.

If the resizing has already been performed on an appliance, the wizard displays a corresponding message.

If you still need to resize the appliance volumes, contact McAfee support.

---

**Database updates**

Information retrieved from external databases for use in the filtering process must be updated from time to time.

Web objects are filtered on an appliance in a rule-based process. The filtering rules need information on these objects to know whether they should trigger actions, such as blocking access to an object or allowing it. They rely for this information on special modules (also known as *engines*).

For example, a virus and malware filtering rule relies on the Anti-Malware module (engine) to find out whether an object is virus-infected, or a URL filtering rule relies on the URL Filter module (engine) for URL category information.

The modules retrieve this information, for example, virus signatures stored in DAT files, from external databases. The database updates on an appliance apply to this information.

You can update database information on an appliance using different methods.

- **Manual engine update** — You can manually update database information for the modules of the appliance you are currently logged on to.

- **Automatic engine update** — You can also configure automatic updates in regular intervals for the modules of the appliance you are currently logged on to.

  These updates can retrieve information:

  - **From the internet** — Information is then downloaded from the relevant external databases. Database information is for the first time updated in this way immediately after the initial setup of an appliance.

  - **From other nodes in a Central Management configuration** — Information is then downloaded from these nodes. For every node, you can in turn configure whether uploading information from it to other nodes is allowed.

    You can configure these updates when you set up a Central Management configuration, specifying for each node how it should behave with regard to automatic updates.

---

**Update database information manually**

You can update database information for the modules of an appliance manually. The update applies to the modules of the appliance you are logged on to and to those of other appliances that you have included as nodes in a Central Management configuration.
Task
1 Select Configuration | Appliances.
2 On the appliances toolbar, click Manual Engine Update.
   The update is performed.

Schedule automatic engine updates
You can schedule automatic updates of database information for the modules of an appliance.
When you are running multiple appliances as nodes in a Central Management configuration, you can
schedule updates for the modules (also known as engines) on the nodes as part of configuring settings
for this configuration.

Task
1 Select Configuration | Appliances.
2 On the appliances tree, select the appliance you want to schedule automatic updates on and click
   Central Management.
3 Scroll down to Automatic Engine Updates and configure update settings as needed.
4 Click Save Changes.

Closed network updates
Web Gateway appliances can be operated and updated in networks that have no internet connectivity
for security or other reasons. These networks are also known as "closed" or "isolated" networks.
When appliances that run in these networks need to be updated, they cannot connect to the usual
McAfee update servers. An offline update procedure must be performed instead.

You can select and download an update package from a McAfee portal that is provided for this
purpose, store it on portable media and use this media to apply the update package to one or more
appliances in a closed network.

Update packages contain updated information for modules (engines) and malware patterns used in the
filtering process on an appliance. Only full updates (as opposed to incremental updates) are made
available on the portal.

After entering the portal, you need to submit the version number of Web Gateway on the appliance
you want to update, and are provided with a list of features that updated information is currently
available for.

According to your selection, an update package including all files required for the update is created in
zipped format for downloading.
Update an appliance in a closed network

To update an appliance in a network with no internet connectivity, download an update package, store it on portable media, and use the media to perform the update.

**Task**

1. Download an update package.
   a. Use a browser to go to the update page of the Content & Cloud Security at:
      https://contentsecurity.mcafee.com/update
   b. On the update page, enter the version number for an appliance you want to update.
      A list of features that updated information is available for appears.
   c. Select the features you want to update.
      An update package is created according to your selection.
   d. Download the update package to your system.

2. Use portable media, for example, a USB drive, to transfer the update package from the system you used for the download to your administration system in the closed network.

3. For each appliance in the closed network that you want to update, perform the following steps:
   a. Select Configuration | Appliances.
   b. Click Update Engines, then select Upload Update File.
      The Engine Update by File Upload window opens.
   c. Click Browse, go to the location on the administration system where you stored the update package, and select the update package file.
   d. Click Update.
      The appliance is updated using the information from the update package.
   e. Click Close to close the window.
The appliance uses its proxy functions to intercept web traffic and transmit it if this is allowed by the filtering rules. You can configure these functions to meet the requirements of your network.

The following are key settings for proxies:

- **Network mode** — Explicit proxy mode or a transparent mode
  
  Specific settings can be configured for each of these modes.

- **Network protocol** — HTTP, HTTPS, FTP, ICAP, and instant messaging protocols
  
  Protocol settings are common proxy settings that can be configured for each of the network modes.

You can configure other common proxy settings and also implement special proxy solutions, for example, reverse HTTPS proxy or proxy auto-configuration.

**Contents**

- Configure proxies
- Explicit proxy mode
  - Best practices - Configuring the Proxy HA mode
  - Best practices - High Availability configuration size limits
  - Best practices - Configuring the explicit proxy mode with WCCP
- Transparent router mode
- Transparent bridge mode
- Packet size handling
- Secure ICAP
- SOCKS proxy
- Instant messaging
- XMPP proxy
- Configure common proxy settings
- Proxies settings
  - Controlling outbound source IP addresses
  - Using WCCP to redirect FTP traffic
  - Using the Raptor syntax for FTP logon
  - Node communication protocols
  - Using DNS servers according to domains
  - Using DXL messages to exchange web security information
  - Best practices - Working with the user-agent header
  - Bypassing for Office 365 and other Microsoft services
  - Reverse HTTPS proxy
  - Proxy auto-configuration
  - Using the Helix proxy
Configure proxies

You can configure the proxy functions of the appliance as is appropriate for your network. Complete the following high-level steps.

**Task**

1. **Review the proxy settings.**
   - The following key settings are configured by default:
     - Network mode: Explicit proxy
     - Network protocol: HTTP

2. **Modify these settings as needed.**
   - You can, for example, do the following:
     - Configure a different network mode.
       - You can choose one of the following:
         - Explicit proxy mode with High Availability functions
         - Transparent router mode
         - Transparent bridge mode
     - Configure a different network protocol.
       - You can add one or more of the following to HTTP (or add them and disable HTTP):
         - HTTPS
         - FTP
         - IFP
         - ICAP
         - Instant messaging protocols: Yahoo, ICQ, Windows Live Messenger, XMPP (for Jabber and other services)
     - Modify other proxy settings, for example, timeouts or the maximum number of client connections.

3. **Configure a special proxy solution if needed,** for example, reverse HTTPS proxy or proxy auto-configuration.

4. **Save your changes.**

**Explicit proxy mode**

In explicit proxy mode, the clients that have their web traffic filtered on the appliance “know” they are connected to it. They must explicitly be configured to direct their web traffic to the appliance. If this is ensured, it is less important where the appliance is deployed within your network. Typically, it is placed behind a firewall and connected to its clients and the firewall by a router.
The following diagram shows a configuration in explicit proxy mode.

![Diagram of explicit proxy mode](image)

**Figure 4-1  Explicit proxy mode**

**Configure the explicit proxy mode**

You can configure the proxy functions of an appliance in explicit proxy mode, which is the default mode for these functions.

**Task**

1. Select **Configuration | Appliances**.

2. On the appliances tree, select the appliance you want to configure the explicit proxy mode for and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.

3. Under **Network Setup**, select one of the two options for the explicit proxy mode.
   - **Proxy** — For the explicit proxy mode
     
     *This is the default proxy mode.*
     
     When it is selected, specific settings for configuring transparent features of the explicit proxy mode appear below the **Network Setup** settings.
   - **Proxy HA** — For an explicit proxy mode with High Availability functions
     
     After selecting this option, specific **Proxy HA** settings appear below the **Network Setup** settings.

4. Configure specific and common settings for the selected option as needed.

5. Click **Save Changes**.

**See also**

- [Packet size handling](#) on page 97
- [Best practices - Configuring the Proxy HA mode](#) on page 74
- [Transparent Proxy settings](#) on page 68
- [Proxy HA settings](#) on page 73
- [Proxies settings](#) on page 106
Transparent Proxy settings
The Transparent Proxy settings are used for configuring transparent features of the explicit proxy mode.

Transparent Proxy
Settings for configuring the explicit proxy mode with transparent features

Table 4-1  Transparent Proxy

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported client redirect methods</td>
<td>Provides methods for intercepting web traffic and directing it to an appliance.</td>
</tr>
<tr>
<td></td>
<td>• WCCP — When selected, HTTP client requests sent to web servers under the IPv4 protocol are intercepted by an additional network device and directed to the appliance using the WCCP protocol.</td>
</tr>
<tr>
<td></td>
<td>The clients are not aware of the redirection, it remains transparent for them.</td>
</tr>
<tr>
<td></td>
<td>In the same way as for client requests, responses from web servers are directed back to the appliance.</td>
</tr>
<tr>
<td></td>
<td>When using the WCCP redirection method, you need to configure one or more WCCP services on the appliance to let them perform the redirection.</td>
</tr>
<tr>
<td></td>
<td>You also need to configure the network device that intercepts the client requests and server responses. This device can be configured as a router or switch with routing functions.</td>
</tr>
<tr>
<td></td>
<td>After selecting this option, the <strong>WCCP Services</strong> inline list appears for configuring and adding WCCP services.</td>
</tr>
<tr>
<td></td>
<td>• L2 transparent — When selected, client requests sent to a web server under the IPv4 and IPv6 protocols are intercepted by an additional network device and directed to the appliance using the Layer 2 redirection method.</td>
</tr>
<tr>
<td></td>
<td>Under this method, client requests are accepted on the appliance even if their destination IP addresses are not addresses of the appliance. The redirection is transparent to the clients.</td>
</tr>
<tr>
<td></td>
<td>You need to enter the original ports for those client requests that are to be intercepted and redirected in a list on the appliance together with the ports that these requests are redirected to.</td>
</tr>
<tr>
<td></td>
<td>The additional network device must be configured accordingly.</td>
</tr>
<tr>
<td></td>
<td>When this option is selected, requests can not be transmitted using a connection in active FTP mode. Only the passive FTP mode is then available.</td>
</tr>
<tr>
<td></td>
<td>After selecting this option, the <strong>Port Redirects</strong> inline list appears for entering ports.</td>
</tr>
</tbody>
</table>

The following two tables describe list entries in the lists of WCCP services and port redirects.

Table 4-2  WCCP Services – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service ID</td>
<td>Identifies a service that directs web traffic to an appliance under the WCCP protocol.</td>
</tr>
<tr>
<td>WCCP router definition</td>
<td>Specifies the Multicast IP address and DNS name of a router (or switch with routing functions) that uses a WCCP service to direct web traffic to an appliance.</td>
</tr>
<tr>
<td></td>
<td>You can configure multiple routers here, separating entries by commas.</td>
</tr>
<tr>
<td>Ports to be redirected</td>
<td>Lists the ports, for example, on web servers, that data packets must have in their address information to be redirected.</td>
</tr>
<tr>
<td></td>
<td>You can specify up to eight port numbers here, separated by commas.</td>
</tr>
</tbody>
</table>
### Table 4-2 WCCP Services – List entry (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports to be redirected are source ports</td>
<td>Specifies whether the ports that are to be redirected are source ports. When configuring a WCCP service, you need to select this option if the service is used to redirect responses from web servers back to the appliance.</td>
</tr>
<tr>
<td>Proxy listener IP address</td>
<td>Specifies the IP address of an appliance when serving client requests.</td>
</tr>
<tr>
<td>Proxy listener port</td>
<td>Specifies a port for listening to client requests. The default port number is 9090.</td>
</tr>
<tr>
<td>MD5 authentication key</td>
<td>Sets a password used under the MD5 algorithm for signing and verifying control data packets. The <strong>Set</strong> button opens a window for setting the password. The password can have up to eight characters.</td>
</tr>
<tr>
<td>Assignment method</td>
<td><em>This main item does not appear in the list, but is visible in the Add and Edit windows. The following two elements are related to it, specifying the assignment method.</em></td>
</tr>
<tr>
<td></td>
<td>• Assignment by mask — When selected, masking of the source or destination IP addresses is used for load distribution.</td>
</tr>
<tr>
<td></td>
<td>• Assignment by hash — When selected, a hash algorithm is used for load distribution.</td>
</tr>
</tbody>
</table>
Table 4-2  WCCP Services – List entry (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Input for load distribution**       | This main item does not appear in the list, but is visible in the Add and Edit windows. The following elements are related to it, specifying what is used in a data packet as the criteria for load distribution. Different elements are provided, depending on whether you have selected assignment by mask or hash. When running multiple appliances, load distribution can be configured for the proxies on them. Data packets can be distributed to these proxies based on their source or destination IP addresses and port numbers. When source or destination IP addresses are used for load distribution, they can be masked or a hash algorithm can be applied to them, see the options under Assignment method. When source or destination ports are used, only the hash algorithm method can be selected. **Load distribution options for assignment by mask:**  
  - **Source IP mask** — Specifies the mask for a source IP address. The default mask value is `0x15`.  
  - **Destination IP mask** — Specifies the mask for a destination IP address. The default mask value is `0x15`. The maximum mask length is 4 digits, for example, `0xa000`. For both masks together, 6 bit can be set as a maximum. If a mask is set to `0x0`, it does not influence load distribution. So, if you want to use, for example, only source IP addresses for load distribution, you need to set the mask for destination IP addresses to this value. **Load distribution options for assignment by hash:**  
  - **Source IP** — When selected, load distribution is based on source IP addresses.  
  - **Destination IP** — When selected, load distribution is based on destination IP addresses.  
  - **Source port** — When selected, load distribution is based on source port numbers.  
  - **Destination port** — When selected, load distribution is based on destination port numbers. When configuring one WCCP service for handling client requests and another for handling web server responses, you need to select Source IP and Destination IP in a "crosswise" corresponding manner. This means that if you select Source IP for the client requests service, you must select Destination IP for the web server responses service. If you select Source IP for the web server responses service, you must select Destination IP for the client requests service, and so on. The same applies when selecting Source port and Destination port. |
| **Assignment weight**                 | Sets a value to determine how much load is assigned to a proxy. Use this value to assign more load to a proxy on an appliance that has more CPU capacity. 0 means no load is distributed to a proxy. |
Table 4-2  WCCP Services – List entry (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding</td>
<td>This main item does not appear in the list, but is visible in the Add and Edit windows. The following two elements are related to it, specifying the forwarding method.</td>
</tr>
<tr>
<td>method</td>
<td></td>
</tr>
<tr>
<td>• GRE-encapsulated</td>
<td>— When selected, data packets are encapsulated by the router before being redirected.</td>
</tr>
<tr>
<td>• L2-rewrite to local NIC</td>
<td>— When selected, data packets are redirected to the appliance by replacing the MAC address of the next device (on the route to the web server) with that of the appliance.</td>
</tr>
<tr>
<td>L2-redirect target</td>
<td>Specifies a network interface on an appliance that data packets are redirected to</td>
</tr>
<tr>
<td>Magic (Mask assignment)</td>
<td>Lets you set an unknown field in the mask that an appliance sends to the router. This setting is needed for ensuring compatibility with different versions of the vendor’s operating system, which is used for the router.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a WCCP service.</td>
</tr>
</tbody>
</table>

Table 4-3  Port redirects – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original destination port</td>
<td>Specifies the port that the data packets belonging to a client request were originally directed to.</td>
</tr>
<tr>
<td>Destination proxy port</td>
<td>Specifies a port that data packets are redirected to.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a port redirect.</td>
</tr>
</tbody>
</table>

Advanced Outgoing Connection Settings

Settings specifying methods for handling information contained in client requests sent to web servers that are requirements for the network environment of the appliance
### Table 4-4 Advanced Outgoing Connection Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| IP spoofing (HTTP, HTTPS, FTP) | When selected, the appliance keeps the client IP address that is contained in a client request as the source address and uses it in communication with the requested web server under various protocols.  
When WCCP services are used for intercepting web traffic and directing it to the appliance, you need to configure two services for each port on the appliance that listens to client requests: one for the requests that come in from the clients, and one for responses to these requests that are sent by the web servers.  
When this option is not selected, the appliance chooses a source port and uses it in this communication.  
- **IP spoofing for explicit proxy connections** — When selected, client addresses are kept in explicit proxy mode, in which web traffic is not intercepted by an additional device.  
- **Use same source port as client for IP spoofing** — When selected, client source ports are kept and used in addition to client source addresses for communication with web servers.  
  When this option is not selected, the appliance chooses a random source port and uses it in this communication. |
| HTTP: Host header has priority over original destination address (transparent proxy) | When selected, the destination address that is provided in the HOST header part of a client request under the HTTP protocol is used for communication with the requested web server.  
In a transparent proxy configuration, communication with a web server could also use the destination address that is specified under the TCP protocol for the connection that serves to transmit a client request. This address is also known as the original destination address.  
Both methods of communication are available to a transparent proxy on an appliance that intercepts client requests or to a WCCP service that intercepts requests and redirects them to an appliance.  
Using the HOST header destination address is the preferred method, however, for some configurations it can be necessary to deselect this option and use the original destination address for communication with a web server.  
- If web traffic is processed on multiple appliances with transparent proxies running on them and client requests are routed to them according to destination addresses, it must be ensured that the proxies use the original destination addresses when connecting to web servers.  
- This applies also if a WCCP service intercepts client requests and redirects them to multiple appliances, using destination addresses for load distribution. |

#### Sample WCCP service settings for IP spoofing

Sample settings for configuring WCCP services with IP spoofing

> Configure these settings only if you want to perform IP spoofing. It is usually not required that you configure two services for redirecting web traffic to the appliance under the WCCP protocol.

You can use IP spoofing in a configuration with WCCP services that intercept web traffic and direct it to the appliance. In this case, you need to configure two services for all ports on the appliance that listen.

One of these services is for the requests that come in from the clients and another one for the responses to these requests that are sent by the web servers.

The following table shows sample parameter values for these services.
Table 4-5 Sample parameter values for two WCCP services configured with IP spoofing

<table>
<thead>
<tr>
<th>Option</th>
<th>Service for client requests</th>
<th>Service for web server responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service ID</td>
<td>51</td>
<td>52</td>
</tr>
<tr>
<td>WCCP router definition</td>
<td>10.150.107.254</td>
<td>10.150.107.254</td>
</tr>
<tr>
<td>Ports to be redirected</td>
<td>80, 443</td>
<td>80, 443</td>
</tr>
<tr>
<td>Ports to be redirected are source ports</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>Proxy listener IP address</td>
<td>10.150.107.251</td>
<td>10.150.107.251</td>
</tr>
<tr>
<td>Proxy listener port</td>
<td>9090</td>
<td>9090</td>
</tr>
<tr>
<td>MD5 authentication key</td>
<td>* * * * *</td>
<td>* * * * *</td>
</tr>
<tr>
<td>Input for load distribution</td>
<td>This main item does not appear in the settings list, but is visible in the Add and Edit windows. The following four elements are related to it</td>
<td></td>
</tr>
<tr>
<td>Source IP</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>Destination IP</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>Source port</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>Destination port</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>Assignment method</td>
<td>This main item does not appear in the settings list, but is visible in the Add and Edit windows. The following four elements are related to it</td>
<td></td>
</tr>
<tr>
<td>Assignment by mask</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>Assignment by hash</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>Assignment weight</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Forwarding method</td>
<td>This main item does not appear in the settings list, but is visible in the Add and Edit windows. The GRE-encapsulated and L2-rewrite to local NIC elements are related to it</td>
<td></td>
</tr>
<tr>
<td>GRE-encapsulated</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>L2-rewrite to local NIC</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>L2-redirect target</td>
<td>eth1</td>
<td>eth1</td>
</tr>
<tr>
<td>Magic (Mask assignment)</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>Comment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Proxy HA settings**

The Proxy HA settings are used for configuring the proxy functions of the appliance in explicit proxy mode with High Availability functions.

**Proxy HA**

Settings for the explicit proxy mode with High Availability functions
Table 4-6 Proxy HA

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port redirects</td>
<td>Provides a list for entering the ports that requests sent by users are redirected to.</td>
</tr>
</tbody>
</table>
| Director priority   | Sets the priority (ranging from 0 to 99) that an appliance takes in directing data packets.  
|                     | The highest value prevails. 0 means the appliance never directs data packets, but only filters them.  
|                     | In a High Availability configuration, two appliances are typically configured as director nodes with a priority higher than zero to direct data packets, providing fail-over functions for each other.  
|                     | The remaining nodes are configured with zero priority (also known as scanning nodes).  
|                     | The priority value is set on a slider scale.                                  |
| Management IP       | Specifies the source IP address of an appliance that directs data packets when sending heartbeat messages to other appliances. |
| Virtual IPs         | Provides a list of virtual IP addresses.                                     |

The following two tables describe entries in the list of port redirects and the list of virtual IP addresses.

Table 4-7 Port redirects – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol name</td>
<td>Specifies the name of the protocol used for data packets coming in when a user sends a request.</td>
</tr>
<tr>
<td>Original destination ports</td>
<td>Specifies the ports that redirected data packets were originally sent to.</td>
</tr>
<tr>
<td>Destination proxy port</td>
<td>Specifies the port that data packets sent to the above ports originally are redirected to.</td>
</tr>
<tr>
<td>Optional 802.1Q VLANs</td>
<td>Lists the IDs of the network interfaces for VLAN traffic that are configured.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a port redirect.</td>
</tr>
</tbody>
</table>

Table 4-8 Virtual IPs – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual IP address</td>
<td>Specifies a virtual IP address (in CIDR notation).</td>
</tr>
<tr>
<td>Network interface</td>
<td>Specifies a network interface on an appliance used for heartbeats under VRRP (Virtual Router Redundancy Protocol).</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a virtual IP address.</td>
</tr>
</tbody>
</table>

Best practices - Configuring the Proxy HA mode

The Proxy HA network mode that can be configured on Web Gateway is an explicit proxy mode with High Availability functions. It allows you to perform failover and load balancing without using external load balancers.

We recommend that you only use this setup for networks with up to 1000 Web Gateway users. For larger networks, we recommend external load balancing devices.
**Director node and scanning nodes**

One of the appliances in a Proxy HA configuration is configured as the director node. The other appliances are then configured as scanning nodes. The role is assigned to each appliance by configuring a priority value.

The director node performs load balancing within the High Availability cluster by distributing load to the scanning nodes. Usually, the director node also acts as a scanning node. The scanning nodes can act as backup nodes to replace a failed director node. You can also configure a node as a simple scanning node that does not perform backup functions.

The node that has the director role at a given point in time is known as the *active director*. The active director uses a virtual IP address (VIP) as an alias IP address on its interface for communication with the clients.

We recommend that you also configure the appliances you want to include in the Proxy HA configuration as members of a Central Management configuration.

These configurations do not depend on each other for running successfully. But if the appliances are not controlled and synchronized by Central Management, each appliance might follow different web security rules after some time.

**Load balancing**

Load balancing in a Proxy HA configuration takes into account resource usage and active number of connections. So, if one scanning node is overloaded, others get more traffic to compensate.

When load balancing is performed, requests from the same client usually go to the same scanning node.

**Failover**

If the director node fails, the backup node with the highest priority takes over the director role. When the original director node returns to active status, it takes over the director role again.

To verify that nodes are available, VRRP (Virtual Router Redundancy Protocol) is used for health checks. You must configure the following for VRRP on each appliance to enable the health checks: A VRRP interface and a virtual router ID that is the same for all members of the High Availability cluster.

Each node sends a multicast packet per second to IP address 224.0.0.18. If no multicast packet from the active director is seen for 3–4 seconds, a failover is performed. The failover lets the backup node with the highest priority become the director node. This node takes on ownership of the virtual IP address of the High Availability cluster and informs the other nodes about its new director role.

*Gratuitous ARP* (Address Resolution Protocol) messages are used to update the ARP tables of participating clients and routers. Each time the common virtual IP address changes ownership (a failover occurs), the new director node sends a gratuitous ARP message. Subsequent TCP/IP packets can then reach this node.

**See also**

*Best practices - High Availability configuration size limits on page 78*
**Configure the Proxy HA mode**

Configure the Proxy HA mode to perform load balancing and failover without using external load balancers.

**Task**

1. Select **Configuration | Appliances**.

2. On the appliances tree, select an appliance that you want to include in the Proxy HA configuration, then click **Proxies (HTTP, HTTP(S), FTP, SOCKS, ICAP ...)**.

3. Under **Network Setup**, select **Proxy HA**.

   The **Proxy HA** settings appear immediately below the **Network Setup** settings.

4. Configure Web Gateway the following for each appliance in the Proxy HA configuration:

   a. **Port redirects** — Add an entry with the following parameters in the list of port redirects.
      - **Protocol name** — HTTP
      - **Original destination ports** — Proxy port that the users of your network select in their browsers
      - **Destination proxy port** — Proxy port used by Web Gateway

      The proxy port that the users select in their browsers and the proxy port that Web Gateway uses can be the same, for example, **9090**.

      In this case, enter a port redirect into the list that redirects, for example, port 9090 to port 9090.

   b. **Director priority** — Set a numerical value for the priority in taking the director role.
      - Highest priority, for example, **99** — For the director node
      - Lower priority, must be higher than **0**, for example, **89** — For a backup node

      A backup node can perform a failover to replace the director node when that node fails and no other node with a higher priority is available. Otherwise the backup node works as a scanning node.
      - **0** — For a node that only acts as a scanning node

   c. **Management IP** — Specify the local IP address of the appliance.

      This IP address is used to auto-discover the scanning nodes. All nodes must be on the same subnet to be auto-discovered.

   d. **Virtual IPs** — Specify the shared IP address for the High Availability cluster.

      This address is owned by the active director and must be the same on all nodes. Your users must select this address in their browsers.
Configure the settings for the VRRP health checks.

- **Virtual router ID** — ID used for the VRRP health checks
  
  This ID must be the same on all nodes. It is 51 by default.
  
  You can leave the default ID, unless you are already using VRRP elsewhere in your network with ID 51. Then change it here to make it unique for the Proxy HA configuration.

- **VRRP interface** — Interface used by VRRP for the health checks

  This interface is `eth0` by default.

  You can leave the default interface, unless you are not using the `eth0` interface on your appliances at all or want to use multiple interfaces.

5. Click **Save Changes**.

When the size of data packets is handled in a flexible manner between a Web Gateway appliance and its clients, using the method known as **Path MTU discovery**, an additional configuration effort is required for the Proxy HA mode.

**See also**

- Packet size handling on page 97
- Proxy HA settings on page 73

## Resolving issues with a Proxy HA configuration

Several measures can be taken when trying to resolve issues with a Proxy HA configuration.

### Look up VRRP health check messages

Messages about the VRRP health checks are logged on an appliance system under:

```
/var/log/messages
```

These messages also inform you about whether an appliance is in director or backup node status.

### Find out which node blocked a request

To find out which of the nodes in a High Availability cluster blocked a request, edit the user message template for Block actions. Insert the `System.HostName` property.

### Test a specific node

To test the behavior of a particular node, enter a new proxy port in the port redirect list only on that node, for example, 9091.

Then point the browser on the client system that you are using to test the node to `<IP address of Web Gateway>:9091`.

### Identify the active director

To identify the active director node that owns the virtual IP address of the High Availability cluster, set up an SSH session with each node. Then run the `ip addr show` command on each of them.
Inspect failure to distribute web traffic

If all web traffic is processed on the director node or another single node instead of being distributed to other nodes, it could have these reasons:

- No port redirects are configured on the director node. If there are no port redirects, the director node will not redirect traffic to other nodes, but handle it locally.
- The director node does not know about any other nodes because they are configured with IP addresses that do not belong to the same subnet.
- All traffic is coming from the same source IP address because there is a downstream proxy or a NAT device in place. Then the usual behavior for load balancing is to direct this traffic to the same node again and again.

Best practices - High Availability configuration size limits

When configuring the Proxy HA (High Availability) network mode, you need to consider the number of Web Gateway appliances to include in the configuration.

In most cases, multiple appliances are run in a network and configured as nodes that are administered using Central Management functions.

Usually, one of these nodes is configured as the director node that directs incoming web traffic to the other nodes, which are termed scanning nodes since their job is to scan this traffic.

On a particular appliance, network interfaces are usually configured in a two-leg solution, which uses separate interfaces for incoming and outgoing web traffic, or in a three-leg solution, which uses an additional interface for Central Management communication.

Considering a network that is configured in this way, the following should be taken into account:

- The number of scanning nodes must be chosen in a way that lets their added maximum throughput not exhaust or exceed the maximum throughput that can be achieved by the director node, which is 1 gigabit per second by default.

  This value results from the following internal restrictions: The network interface that the director node uses by default is limited to processing a data volume of 1 gigabit per second.

  Also, the kernel-mode driver of the MLOS operating system, which runs on a Web Gateway appliance, only allows a scaling of up to 1 gigabit per second.

- We recommend that you leave a clear safety margin when configuring the number of scanning nodes that would theoretically be possible under these conditions.

  - For example, with a throughput of 100 megabits per second for a scanning node, ten nodes would be possible, but we recommend five.
  
  - With a throughput of 300 megabits per second, three nodes would be possible, but we recommend two.

The maximum throughput on a scanning node varies with the appliance model that is used as a node and how a node is configured, for example, whether anti-malware filtering or the web cache are enabled or not. To find this value for a node, you can use a sizing calculator.

Calculations look different if a 10G network interface is used by a director node instead of the default 1G network interface or if IP spoofing is enabled in a configuration. This is explained in the following.
**10G network interfaces**

When a 10G network interface is installed on an appliance that is configured as the director node, the maximum throughput for this node is increased. However, the scaling limit of the MLOS kernel-mode driver must still not be exhausted or exceeded.

- For example, with a throughput of 100 megabits per second for a scanning node, more than five nodes are possible, but we still recommend not to extend their number to ten.

- With a throughput of 300 megabits per second, three nodes are possible, we recommend not to use more.

**IP spoofing**

When IP spoofing is configured, data packets pass through the director node twice, once when the director node directs them to the scanning nodes and a second time when they are returned from the scanning nodes to the director node, as this node forwards the data packets to their original IP addresses.

This means the maximum throughput is only 500 megabits per second on the director node if a 1G network interface is used while the scaling limit of the MLOS kernel-mode driver remains the same.

The number of scanning nodes must be adapted accordingly.

- For example, with a throughput of 100 megabits per second for a scanning node and a director node that uses a 1G network interface, the number of scanning nodes must be less than five.

  If a 10G network interface is used, the number of scanning nodes can be higher, but we still recommend five.

- With a throughput of 300 MBit/s for a scanning node and a director node that uses a 1G network interface, there should be only one scanning node.

  If a 10G network interface is used, we recommend not to configure more than three scanning nodes.

**See also**

*Best practices - Configuring the Proxy HA mode on page 74*

---

**Best practices - Configuring the explicit proxy mode with WCCP**

When implementing the explicit proxy mode on a Web Gateway appliance, you can configure the redirection of web traffic to Web Gateway under WCCP (Web Cache Communication Protocol). Use of this protocol considerably enhances the capabilities for load balancing and failover.

To enable redirection under WCCP, a suitable router must be placed between the client systems of the users in your network and the web. The router redirects requests for web access from the clients that are directed to particular ports to the Web Gateway appliance.

The router is also referred to as the WCCP device. Instead of a router, you can also use a switch as WCCP device.

On the appliance, you must configure a WCCP service. When configuring this service, you specify a service ID, the IP address of the router, the ports that requests are redirected from, and other information.

Multiple appliances can connect to the same router under WCCP for load balancing and failover. The appliances must be configured as nodes in a Central Management configuration and a WCCP service must be configured on each of them.
The redirection happens transparently, which means users are not aware that their requests are redirected. When the response to a request is received from a web server, Web Gateway forwards it to the client, using (spoofing) the IP address of the web server.

To start working with the router, Web Gateway subscribes to it. The router is not aware of Web Gateway until the subscription happens. No settings must be configured on the router to inform it about Web Gateway.

**Communication between Web Gateway and the router**

Under WCCP, data packets are exchanged to subscribe, negotiate settings, and as health checks. Web Gateway sends a "Here I Am" packet to the router and forwards the configured settings. These settings include the ports for redirection, the ID of the WCCP service, the IP address that traffic should be redirected to, and other information.

The router acknowledges with an "I See You" packet that the subscription has been successful and includes the router ID, which is the highest interface IP address on the router.

If a router does not receive a "Here I Am" packet over more than 25 seconds, it sends a removal query, requesting that Web Gateway respond immediately. If no response is received within another 5 seconds, Web Gateway is considered offline and removed from the pool of WCCP partners.

**Load balancing and failover**

In a WCCP configuration with multiple Web Gateway appliances, the first appliance that connects to the router distributes workload to the other appliance. Portions of workload that are distributed are also known as "buckets" in WCCP terminology.

When an appliance goes offline or returns, buckets are immediately reassigned. If the appliance that is currently assigning buckets goes offline, another appliance takes over its role.

We do not recommend using WCCP when the router, client systems, or the Web Gateway appliances are separated by a device that uses the method known as source NATing to handle client traffic. This method impacts the performance of load balancing under WCCP. It also prevents you from configuring rules for user authentication based on time or client IP addresses.

**Fail-open and fail-closed strategies**

If use of the WCCP protocol is configured on the router and no Web Gateway appliance is available, the router lets requests for web access pass through without redirection. This behavior follows a strategy known as *fail-open strategy*.

If you have a firewall in your network, you must configure it to allow requests for web access with any source IP addresses to enable this strategy. Requests can then go out to the web directly.

Under a *fail-close strategy*, requests are blocked if no Web Gateway appliance is available to redirect them to. For this strategy to work, you must configure the firewall to allow only requests with source IP addresses belonging to Web Gateway.

**Using WCCP only or as fallback solution**

You can use the explicit proxy mode with WCCP as your only network mode solution, which means all web traffic is handled in this mode. You can also use it as a fallback solution for special use cases in an explicit proxy configuration, for example, to deal with applications that do not recognize proxy settings. Another use case would be handling web traffic in a Wi-Fi network segment where users can bring their own devices.
As best practice, we recommend using two different proxy ports. Configure one for handling web traffic in explicit proxy mode with WCCP, and one for handling it without WCCP. Following this practice allows you to use the property for proxy ports in the criteria of web security rules.

**Configure use of the WCCP protocol**

To configure use of the WCCP protocol, configure a router and one or more Web Gateway appliances for handling web traffic according to this protocol.

**Task**

1. Configure a router for handling web traffic according to the WCCP protocol.
   Configuring the router mainly includes specifying the ID of the WCCP service. For more information, see the router documentation.

2. Configure a Web Gateway appliance for handling web traffic according to the WCCP protocol.
   Configuring the appliance mainly includes setting up a WCCP service on it.
   a. Select Configuration | Appliances.
   b. Select the appliance that you want to configure for use of the WCCP protocol and click Proxies (HTTPS, FTP, SOCKS, ICAP ...).
   c. Under Network Setup make sure that Proxy (optional WCCP) is selected. Under Transparent Proxy select WCCP.
      The WCCP services list appears.
   d. On the list toolbar, click the Add icon.
      The Add WCCP Service window opens.
   e. To add a service, provide values for the service parameters. When you are done, click OK.
      The new service appears in the WCCP services list.
   f. Click Save Changes.

You can include more than one appliance in a WCCP configuration. Configure a WCCP service on every appliance that you want to include.

When configuring the explicit proxy mode with WCCP after using a different network mode before (Proxy HA mode, transparent router or bridge mode), you must restart the appliance.

The restart unloads the network driver that handles the transparent interception and redirection of web traffic. Restarting is only required once. Later on you can enable and disable use of the WCCP protocol without restarting.

**See also**

*Settings for a WCCP service on page 81*

**Settings for a WCCP service**

When configuring the settings for a WCCP service, you specify values for several service parameters. Regarding these parameters, consider the best-practice information that is provided in the following.
**Service ID**

The service ID identifies the WCCP service. The service is also included in the configuration of the router, where the ID for this service must be the same.

Service IDs 0–50 are static under WCCP and reserved for *well known services* with standard configurations. Service IDs 51–255 are dynamic and involve negotiation between the partners in the WCCP configuration. For the WCCP service that you configure, we recommend using a value from 51 to 98.

**WCCP router definition**

The IP address of the router that is used in the WCCP configuration is specified in the router definition. Alternatively, you can specify the name that this IP address is resolved to by a domain name server.

You can configure multiple routers by specifying an IP address or DNS name for each of them or by using a multicast IP address. The use of an IP address as multicast IP address for multiple routers is indicated in the configuration of the respective routers by specifying the keywords `group-address` and `group-listen`.

**Ports to be redirected**

The ports that web traffic is redirected from to the Web Gateway proxy port are listed here.

The redirection works for traffic under the HTTP protocol and also under HTTPS. Redirection of FTP traffic or traffic under any other protocol is not supported. This means that all ports that you list here must be ports for HTTP and HTTPS traffic. Port 80 for HTTP traffic and port 443 for HTTPS traffic are by default included in the list.

If you add more ports for HTTPS traffic, you must also add them as ports that are to be treated as SSL within the HTTP proxy configuration.

*If version 1 of WCCP is used, only traffic for port 80 is redirected. You cannot add any other ports for redirection.*

**Proxy listener address**

The proxy listener address is the physical IP address of the network interface card on a Web Gateway appliance that web traffic is redirected to.

**Proxy listener port**

The proxy listener port is the port on Web Gateway that listens to the redirected requests.

For the redirection to work, you must bind the proxy listener port to the IP address 0.0.0.0. For example, if you are using the default port 9090, bind it by specifying 0.0.0.0:9090.

You must not bind the port (by specifying `localhost`) to the IP address of the appliance that you are working on, nor to any other IP address. Otherwise the redirection will not work and traffic will not be processed.

**Assignment method**

The assignment method is the method for assigning buckets (processing jobs) under WCCP to different Web Gateway appliances when a configuration consists of more than one appliance. The method can be assignment by mask or hash. Some routers only support the mask assignment method. For more information, see the router documentation.
**Input for load distribution**

Load distribution can be based on the source or destination IP address or the source or destination port of a request. We recommend configuring load distribution based on the source IP address. This ensures that the same appliance is always used for the requests that a user submits from a particular client system. Breaking sessions is avoided this way.

**Assignment weight**

The assignment weight is used to assign traffic load to different Web Gateway appliances in a WCCP configuration. If the default value 1000 is configured on all appliances, the load is distributed equally.

If an appliance in the configuration performs better than the others, you can configure a higher value on this appliance and lower values on the others. If all appliances perform equally well, we recommend leaving the default value on each of them.

**GRE-encapsulated**

When the Generic Routing Encapsulation (GRE) method is used for sending data packets, an original data packet is encapsulated inside a new packet with additional headers. The new packet is then sent from the router to Web Gateway over a connection that is known as a GRE tunnel. This method requires more overhead, but has the advantage of working across subnets.

**L2-rewrite to local NIC**

When the L2-rewrite (Layer 2 rewrite) method is used for sending data packets, the destination MAC address is rewritten to the MAC address of the proxy. The packets are then redirected to a network interface on an appliance. This method works only if the router and the appliance are on the same subnet.

**L2-redirect target**

The target for redirecting data packets under the L2-rewrite method is the network interface of a NIC on the appliance that you are working on. The interface name, for example, `eth0`, is selected to specify this interface.

**Troubleshooting WCCP-related issues**

You can review WCCP-related information on the appliance dashboard or retrieve it running suitable commands on the command line of a system console that is connected to the appliance.

**Review WCCP-related information on the dashboard**

Review WCCP-related information on the dashboard, to see whether troubleshooting activities are required.

**Task**

1. Select Dashboard | Charts and Tables.

2. On the navigation pane, click System Summary and scroll down to the WCCP Service Current Status Report table.

The table shows values for several WCCP parameters, such as the ID of the WCCP service that the appliance has subscribed to, the IP address of the router, forwarding and return methods, and assigned buckets.

It also shows the time stamps of the latest "Here I Am" and "I See You" data packets, which allows you to verify that the health check is working.
Retrieving WCCP-related information on the command line

You can use several commands to retrieve WCCP-related information on the command line. Enter the following command to see if web traffic is redirected to the configured port on a Web Gateway appliance.

```
iptables -t mangle -L
```

You will see, for example, an entry for the chain WCCP0 with a line containing `redirect 10.10.73.72:9090`.

10.10.73.72 is the IP address of the network interface of the NIC on the Web Gateway appliance that you configured as destination of the redirected traffic. 9090 is the configured port.

You can check whether the appliance sends "Here I Am" and "I See You" data packets. Enter the following command:

```
tcpdump -npi eth0 port 2048
```

Within the data packets that are displayed, verify that the following applies:

- The IP address shown for the web cache is the IP address of the Web Gateway appliance.
- The bucket assignment method is the method that is also configured for Web Gateway.
- The redirect method is the method that is also configured for Web Gateway.

You can check whether the GRE-encapsulated or L2-rewritten data packets are received on the Web Gateway appliance.

- For GRE-encapsulation, enter the following command:
  ```
tcpdump -npi eth0 ip proto 47
  ```
  Verify that the source IP address of the data packets is the IP address that is configured for the router on Web Gateway.

- For L2-rewriting, enter the following command:
  ```
tcpdump -npi eth0 not host <IP address of the Web Gateway appliance
  ```
  Verify that the source IP address of the data packets is the IP address of the client that sent the request.

To check that redirected data packets are received on Web Gateway, you can also enter the `ifconfig` command.

Transparent router mode

The transparent router mode is one of the two transparent modes you can configure for the proxy functions of a Web Gateway appliance if you do not want to use an explicit mode.

In transparent router mode, the clients are unaware of the appliance and need not be configured to direct their web traffic to it.

The appliance is placed as a router immediately behind a firewall. A switch can be used for connecting the appliance to its clients. A routing table is used to direct the traffic.
Director and scanning nodes

If you are running several appliances as nodes within a complex configuration, for example, in a Central Management cluster, one node is usually configured as director, while the other nodes are configured as scanning nodes.

The director node receives web traffic from the clients and distributes it to the scanning nodes, which perform filtering activities on the traffic according to the rules that are implemented. Further handling of the traffic by the director or scanning nodes differs depending on what is configured.

The director node can also perform filtering activities. We recommend to configure at least two director nodes to avoid problems in case one of them goes offline.

Configure the transparent router mode

To configure the proxy functions of an appliance in transparent router mode, complete the following high-level steps.

Task

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure the transparent router mode for and click Proxies (HTTP(S), FTP, ICAP, and IM).

   
   After selecting this mode, specific Transparent Router settings appear below the Network Setup settings.
   
   Common settings follow the specific settings, including settings for configuring the HTTP, FTP, and other network protocols.

4. Configure specific and common settings as needed.

5. Click Save Changes.

When running several appliances as nodes in a Central Management configuration, you can configure the transparent router mode on each of them.

Configure nodes in transparent router mode

You can configure the transparent router mode for two or more appliances that are nodes in a Central Management configuration. One of the nodes takes the director role, which means it directs data packets, while the scanning nodes filter them.

Node configuration includes configuring network and proxy settings.
Tasks

- **Configure network settings for a director node in transparent router mode on page 86**
  To configure a director node in transparent router mode, configure network interfaces for inbound and outbound web traffic.

- **Configure proxy settings for a director node in transparent router mode on page 86**
  To configure proxy settings for a director node in transparent router mode, configure the director role for this node, as well as port redirects and proxy ports.

- **Configure a scanning node in transparent router mode on page 87**
  To configure a scanning node in transparent router mode, configure at least one network interface for outbound traffic. Configure the proxy settings in the same way as for a director node in this mode, except for the scanning role.

### Configure network settings for a director node in transparent router mode

To configure a director node in transparent router mode, configure network interfaces for inbound and outbound web traffic.

**Task**

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance you want to configure as a director node and click **Network interfaces**.
3. Configure network interfaces as is suitable for your network.
   - You need at least one interface for inbound and one for outbound web traffic.
4. Click **Save Changes**.
   - You are logged off and logged on to the appliance again.

### Configure proxy settings for a director node in transparent router mode

To configure proxy settings for a director node in transparent router mode, configure the director role for this node, as well as port redirects and proxy ports.

The director role is configured by giving the node a priority value > 0.

**Task**

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance you want to configure as a director node and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.
3. Under **Network Setup**, select **Transparent Router**.
   - Specific **Transparent Router** settings appear below the **Network Setup** settings.
4. Configure one or more port redirects that let requests sent from clients of Web Gateway be redirected to a particular port.
   a. Under **Port redirects**, click **Add**.
   
      The **Add Port Redirects** window opens.
Configure the following for a new port redirect that applies to connections under HTTP or HTTPS:

- **Protocol name** — http
  
  http covers connections under both HTTP and HTTPS.

- **Original destination ports** — 80, 443
  
  These are the default destination ports. They cover connections under both HTTP and HTTPS.
  
  If you also want to filter HTTPS traffic, enable the SSL Scanner rule set, which is by default provided on the rule sets tree, but not enabled.

- **Destination proxy port** — 9090
  
  9090 is the default proxy port on an appliance.
  
  If you need to use other ports due to the requirements of your network, change these settings as needed.
  
  To configure a port direct for connections under FTP, select this protocol. Default ports are then preconfigured, which you can change as needed.

5. Set **Director priority** to a value > 0.

6. In the **Management IP** field, type an IP address for each of the scanning nodes that the director should be able to connect to.

7. Under **Virtual IPs**, configure virtual IP addresses for the inbound and outbound network interfaces, using free IP addresses for this purpose.

8. Leave the number under **Virtual router ID** as it is.

9. From the **VRRP interface** list, select the interfaces for heartbeats under this protocol.

10. Configure IP spoofing as needed.

11. Under **HTTP proxy port**, make sure **Enable HTTP proxy** is selected.

   The setting is selected by default. An entry for port 9090 is also configured by default on the **HTTP Port Definition List**.

   - You can change this port as needed. Clicking **Add** opens the **Add HTTP Proxy Port** window, which allows you to add more proxy ports.

   - To configure one or more FTP proxies, select **Enable FTP Proxy** under **FTP Proxy**. An entry for FTP control port 2121 and FTP data port 2020 is then preconfigured on the **FTP Port Definition List**

12. Click **Save Changes**.

**Configure a scanning node in transparent router mode**

To configure a scanning node in transparent router mode, configure at least one network interface for outbound traffic. Configure the proxy settings in the same way as for a director node in this mode, except for the scanning role.

The scanning role is configured by giving the node 0 as the priority value.

**Task**

1. Select **Configuration | Appliances**.

2. On the appliances tree, select the appliance you want to configure as a scanning node and click **Network interfaces**.
3 Configure network interfaces as is suitable for your network. You need at least one interface for outbound web traffic.

4 Click Save Changes.

5 You are logged off and logged on to the appliance again.

6 On the appliances tree, select the appliance you want to configure as a scanning node and click Proxies (HTTP(S), FTP, SOCKS, ICAP ...).

7 Under Network Setup, select Transparent Router. Specific Transparent Router settings appear below the Network Setup settings.

8 Configure the same port redirects as for the director node.

9 Set Director priority to 0.

10 Configure IP spoofing in the same way as for the director node.

11 Configure the same HTTP and FTP proxy ports as for the director node.

12 Click Save Changes.

To run more than one scanning node in transparent router mode, configure additional appliances in the same way.

**Transparent Router settings**
The Transparent Router settings are specific settings for configuring the proxy functions of an appliance in transparent router mode.

**Transparent Router**
Settings for configuring the transparent router mode

**Table 4-9  Transparent Router**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port redirects</td>
<td>Provides a list for entering the ports that requests for web access sent by users of your network are redirected to.</td>
</tr>
<tr>
<td>Director priority</td>
<td>Sets the priority (ranging from 0 to 99) that an appliance takes in directing the data packets that are sent in a request.</td>
</tr>
<tr>
<td></td>
<td>When several appliances are run as nodes in a complex configuration, for example, a Central Management cluster, the node with the highest value is the director node, while the other nodes are scanning nodes that only perform filtering activities.</td>
</tr>
<tr>
<td></td>
<td>The director node receives data packets, distributes them to the other nodes for filtering, and forwards the data packets that have passed the filtering to the web.</td>
</tr>
<tr>
<td></td>
<td>In a complex configuration, set the director node to a value higher than zero, and set the scanning nodes to zero.</td>
</tr>
<tr>
<td>Management IP</td>
<td>Specifies the source IP address of an appliance that directs data packets when sending heartbeat messages to other appliances.</td>
</tr>
<tr>
<td>Virtual IPs</td>
<td>Provides a list for entering virtual IP addresses.</td>
</tr>
<tr>
<td>Virtual router ID</td>
<td>Identifies a virtual router.</td>
</tr>
</tbody>
</table>
### Table 4-9 Transparent Router (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP interface</td>
<td>Specifies the network interface on an appliance for sending and receiving heartbeat messages.</td>
</tr>
</tbody>
</table>
| IP spoofing (HTTP, HTTPS) | When selected, the appliance keeps the client IP address that is sent with a request as the source address and uses it in communication with the requested web server under various protocols.  
The appliance does not verify whether this address matches the host name of the request. |
| IP spoofing (FTP)    | When selected, the appliance communicates with a file server under the FTP protocol in the same way as under the HTTP or HTTPS protocol to perform IP spoofing.  
For active FTP, this option must be enabled. |

The following two tables describe entries in the list of port redirects and the list of virtual IP addresses.

### Table 4-10 Port redirects – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol name</td>
<td>Specifies the name of the protocol used for sending and receiving requests.</td>
</tr>
<tr>
<td>Original destination ports</td>
<td>Specifies the ports that requests must originally be sent to if they are to be redirected.</td>
</tr>
<tr>
<td>Destination proxy port</td>
<td>Specifies the port that requests are redirected to.</td>
</tr>
</tbody>
</table>
| Source IP based exceptions | Excludes requests that have been received from clients with the specified IP addresses from redirecting.            
  • For each IP address, a net mask must also be specified.  
  • When a request is excluded from redirecting, it is not processed by any of the filtering rules that are implemented.  
  • You can configure redirection exceptions in this way to let requests received from trusted sources skip further processing on Web Gateway or for troubleshooting connection problems. |
| Destination IP based exceptions | Excludes requests that are sent to a destination with the specified IP address from redirecting.                     
  • For each IP address, a net mask must also be specified.  
  • When a request is excluded from redirecting, it is not processed by any of the filtering rules that are implemented.  
  • You can configure redirection exceptions in this way to let requests sent to trusted destinations skip further processing on Web Gateway or for troubleshooting connection problems. |
| Optional 802.1Q VLANs | Lists the IDs of the network interfaces for VLAN traffic that are configured.                                        |
| Comment              | Provides a plain-text comment on a port redirect.                                                                  |
Table 4-11  Virtual IPs – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual IP address</td>
<td>Specifies a virtual IP address (in CIDR notation).</td>
</tr>
<tr>
<td>Network interface</td>
<td>Specifies a network interface on an appliance that the virtual IP address configured here is assigned to.</td>
</tr>
<tr>
<td></td>
<td>This virtual IP address is only assigned to the interface if the current node takes the role of an active director.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a virtual IP address.</td>
</tr>
</tbody>
</table>

Transparent bridge mode

The transparent bridge mode is one of the transparent modes you can configure for the proxy functions of the appliance if you do not want to use an explicit mode.

In this mode, the clients are unaware of the appliance and need not be configured to direct their web traffic to it. The appliance is usually placed between a firewall and a router, where it serves as an invisible bridge.

The following diagram shows a configuration in transparent bridge mode.

![Transparent bridge mode diagram](image)

Figure 4-2  Transparent bridge mode

Configure the transparent bridge mode

To configure the proxy functions of an appliance in transparent bridge mode, complete the following high-level steps.

Task

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure the transparent bridge mode for and click Proxies (HTTP(S), FTP, ICAP, and IM).


   After selecting this mode, specific Transparent Bridge settings appear below the Network Setup settings.

   Common settings follow the specific settings, including settings for configuring the HTTP, FTP, and other network protocols.

4. Configure specific and common settings as needed.
5  Restart the appliance.

The restart includes the reloading of network drivers, which ensures that the appropriate drivers for this network mode are applied.

We also recommend restarting the appliance after switching from the transparent bridge mode to another network mode.

6  Click Save Changes.

When running several appliances as nodes in a Central Management configuration, you can configure the transparent bridge mode on each of them.

When the size of data packets is handled in a flexible manner between a Web Gateway appliance and its clients, using the method known as Path MTU discovery, an additional configuration effort is required for the transparent bridge mode.

See also
Packet size handling on page 97
Transparent Bridge settings on page 95

Configure nodes in transparent bridge mode
You can configure the transparent bridge mode for two or more appliances that are nodes in a Central Management configuration. One of the nodes takes the director role, which means it directs data packets, while the scanning nodes filter them.

Node configuration includes configuring network, Central Management, and proxy settings.

Tasks
- Configure network and Central Management settings for a director node in transparent bridge mode on page 91
  To configure a director node in transparent bridge mode, configure a network interface for the transparent bridge functions and let its IP address be used for Central Management communication.

- Configure proxy settings for a director node in transparent bridge mode on page 92
  To configure proxy settings for a director node in transparent bridge mode, configure the director role for it, as well as port redirects and proxy ports.

- Configure a scanning node in transparent bridge mode on page 93
  To configure a scanning node in transparent bridge mode, configure the same settings as for a director node in this mode, except for the scanning role.

Configure network and Central Management settings for a director node in transparent bridge mode
To configure a director node in transparent bridge mode, configure a network interface for the transparent bridge functions and let its IP address be used for Central Management communication.

Task
1  Select Configuration | Appliances.

2  On the appliances tree, select the appliance you want to configure as a director node and click Network interfaces.
3 Prepare the network interface for the transparent bridge functions.
   a Select a still unused network interface of the appliance, but do not enable it yet.
   b On the Advanced tab, select Bridge enabled.
   c In the Name field, type ibr0 as the name of the interface.
   d On the IPv4 tab, under IP Settings, select Disable IPv4.
   e Click Save Changes.
   You are logged off and logged on to the appliance again.

4 Configure the network interface for the transparent bridge functions.
   a Select Configuration | Appliances. Then select the appliance again, and click Network interfaces.
      An additional network interface named ibr0 is now available.
   b Select the ibr0 interface.
   c On the IPv4 tab, configure an IP address, a subnet mask, and a default route for this interface.
   d Select the checkbox next to the interface to enable it.

5 Configure the network interface that is currently used to access the appliance as the network interface for the transparent bridge functions.
   a Select the network interface that is currently used to access the appliance.
   b On the Advanced tab, select Bridge enabled.
   c In the Name field, type ibr0 as the name of the interface.
   d On the IPv4 tab, under IP Settings, select Disable IPv4.

6 Enable the ibr0 network interface that you selected in step 3 from the until now unused network interfaces.

7 Configure Central Management settings.
   a Select Central Management.
   b Under Central Management Settings, add the IP address you configured for the ibr0 network interface to the list that is provided.

8 Click Save Changes.

If you want to use more than one network interface for the transparent bridge mode, configure more unused network interfaces of an appliance in the same way.

**Configure proxy settings for a director node in transparent bridge mode**
To configure proxy settings for a director node in transparent bridge mode, configure the director role for it, as well as port redirects and proxy ports.

The director role is configured by giving the node a priority value > 0.

**Task**
1 Select Configuration | Appliances.
2 On the appliances tree, select the appliance you want to configure as a director node and click Proxies (HTTP(S), FTP, ICAP, and IM).
3 Under **Network Setup**, select **Transparent Bridge**.
Specific **Transparent Bridge** settings appear below the **Network Setup** settings.

4 Configure one or more port redirects that let requests sent from clients of Web Gateway be redirected to a particular port.
   a Under **Port redirects**, click **Add**.
   b Configure the following for a new port redirect that applies to connections under HTTP or HTTPS:
      • **Protocol name** — http
         *http* covers connections under both HTTP and HTTPS.
      • **Original destination ports** — 80. 443
         These are the default destination ports. They cover connections under both HTTP and HTTPS.
         If you want to filter also HTTPS traffic, you need to enable the SSL Scanner rule set, which is by default provided on the rule sets tree, but not enabled.
      • **Destination proxy port** — 9090
         9090 is the default proxy port on an appliance.
         If you need to use other ports due to the requirements of your network, change these settings as needed.
         To configure a port direct for connections under FTP, select this protocol. Default ports are then preconfigured, which you can change as needed.

5 Set **Director priority** to a value > 0.

6 In the **Management IP** field, type the IP address you specified for ibr0 when configuring the network settings.

7 Configure IP spoofing as needed.

8 Under **HTTP proxy port**, make sure **Enable HTTP proxy** is selected.
   The setting is selected by default. An entry for port 9090 is also configured by default on the **HTTP Port Definition List**.
      • You can change this port as needed. Clicking **Add** opens the **Add HTTP Proxy Port** window, which allows you to add more proxy ports.
      • To configure one or more FTP proxies, select **Enable FTP Proxy** under **FTP Proxy**. An entry for FTP control port 2121 and FTP data port 2020 is then preconfigured on the **FTP Port Definition List**.

9 Click **Save Changes**.

**Configure a scanning node in transparent bridge mode**
To configure a scanning node in transparent bridge mode, configure the same settings as for a director node in this mode, except for the scanning role.
The scanning role is configured by giving the node 0 as the priority value.

**Task**
1 Select **Configuration | Appliances**.
2 On the appliances tree, select the appliance you want to configure as a scanning node and click **Proxies (HTTP(S), FTP, SOCKS, ICAP ...)**.
3. Under **Network Setup**, select **Transparent Bridge**.
   Specific **Transparent Bridge** settings appear below the **Network Setup** settings.

4. Configure the same port redirects as for the director node.

5. Set **Director priority** to 0.

6. Configure IP spoofing in the same way as for the director node.

7. Configure the same HTTP and FTP proxy ports as for the director node.

8. Click **Save Changes**.

To run more than one scanning node in transparent bridge mode, configure additional appliances in the same way.

**Best practices - Fine-tuning a transparent bridge configuration**

When configuring Web Gateway in transparent bridge mode, you can complete several activities in addition to the basic steps to improve the configuration.

These activities include the following:

- Configuring port redirects
- Setting up more than one appliance
- Appropriate handling of the STP protocol

**Configuring port redirects**

Web Gateway is by default configured to scan and filter requests for web access arriving on ports 80 and 443. All requests arriving on other ports are passed on to the web unfiltered unless you specify additional ports.

You can configure port redirects as exceptions for requests coming from a particular client IP address or going to a particular destination IP address. These exceptions are also passed on to the web unfiltered.

**Setting up more than one appliance**

When configuring Web Gateway in transparent bridge mode, we recommend setting up more than one appliance.

When a Web Gateway appliance is configured in this mode, it is implemented in an in-line position within your network. This means that all traffic is physically passing through the appliance, even if no ports are configured to receive the traffic and enable its filtering. Setting up only one appliance would therefore make it a single point of failure.

If you set up at least one other appliance, it can serve as a failover device. Another appliance will, however, not only perform failover functions, but also load balancing, receiving, and processing web traffic.

**Avoiding a port shutdown under STP**

When the Web Gateway appliances in your network are directly connected to switches that use the Spanning Tree Protocol (STP), ports needed for load balancing communication might be shut down under this protocol.

On most network switches, STP is used to avoid loops and ensure a single path of communication, shutting down redundant ports that cause such loops.
The protocol is also used, however, when two or more Web Gateway appliances are configured in transparent bridge mode. One of the appliances then takes the director role, in which it directs the web traffic that occurs to the other appliance or appliances for processing.

STP is used to communicate this role and the load balancing measures between the appliances.

If network switches with STP are directly connected to the Web Gateway appliances, it is highly likely that ports needed for this load balancing communication are shut down.

You can proceed in one of the following ways to avoid a shutdown:

- Disable STP on every switch that is directly connected to a Web Gateway appliance.

  Do not use this method if other components of your network rely on these switches and STP.

- Install a second switch without STP between every Web Gateway appliance and every switch with STP that the appliance would be connected to.

  Setting up your network in this way ensures that load balancing on the Web Gateway appliances and other network components that rely on switches with STP are not impacted.

See also
Configure the transparent bridge mode on page 90

Configure port redirects for the transparent bridge mode
Configure port redirects for the transparent bridge mode to pass on particular requests to the web unfiltered.

Task
1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure port redirects on and click Proxies (HTTP(S), FTP, SOCKS, ICAP ...).


   The Transparent Bridge settings appear below the Network Setup settings.

4. In the list under Port redirects, specify an IP address and subnet mask for every port redirect that you want to configure.

5. Click Save Changes.

Transparent Bridge settings
The Transparent Bridge settings are specific settings for configuring the proxy functions of an appliance in transparent bridge mode.

Transparent Bridge
Settings for configuring the transparent bridge mode
Table 4-12  Transparent Bridge

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port redirects</td>
<td>Provides a list for entering the ports that requests for web access sent by users of your network are redirected to.</td>
</tr>
<tr>
<td>Director priority</td>
<td>Sets the priority (ranging from 0 to 99) that an appliance takes in directing the data packets that are sent in a request.</td>
</tr>
<tr>
<td></td>
<td>The highest value prevails. 0 means an appliance is what is known as a scanning node, which never directs data packets, but only filters them.</td>
</tr>
<tr>
<td></td>
<td>You can use this option only to configure a node as a scanning node (priority = 0) or a director node (priority &gt; 0).</td>
</tr>
<tr>
<td></td>
<td>Differences in node priorities greater than 0 are not evaluated. After configuring node priorities greater than 0 for multiple appliances in</td>
</tr>
<tr>
<td></td>
<td>transparent bridge mode, you need to watch their behavior to find out which one has actually become the director node that directs data packets.</td>
</tr>
<tr>
<td>Management IP</td>
<td>Specifies the source IP address of an appliance that directs data packets when sending heartbeat messages to other appliances.</td>
</tr>
<tr>
<td>IP spoofing (HTTP, HTTPS)</td>
<td>When selected, the appliance keeps the client IP address that is sent with a request as the source address and uses it in communication with</td>
</tr>
<tr>
<td></td>
<td>the requested web server under various protocols. The appliance does not verify whether this address matches the host name of the</td>
</tr>
<tr>
<td></td>
<td>request.</td>
</tr>
<tr>
<td>IP spoofing (FTP)</td>
<td>When selected, the appliance communicates with a file server under the FTP protocol in the same way as under the HTTP or HTTPS protocol to</td>
</tr>
<tr>
<td></td>
<td>perform IP spoofing. For active FTP, this option must be enabled.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the list of port redirects.

Table 4-13  Port redirects – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol name</td>
<td>Specifies the name of the protocol used for sending and receiving requests.</td>
</tr>
<tr>
<td>Original destination ports</td>
<td>Specifies the ports that redirected requests must originally be sent to if they are to be redirected.</td>
</tr>
<tr>
<td>Destination proxy port</td>
<td>Specifies the port that requests are redirected to.</td>
</tr>
<tr>
<td>Source IP based exceptions</td>
<td>Excludes requests that have been received from clients with the specified IP addresses from redirecting.</td>
</tr>
<tr>
<td></td>
<td>• For each IP address, a net mask must also be specified.</td>
</tr>
<tr>
<td></td>
<td>• When a request is excluded from redirecting, it is not processed by any of the filtering rules that are implemented.</td>
</tr>
<tr>
<td></td>
<td>• You can configure redirection exceptions in this way to let requests received from trusted sources skip further processing on Web Gateway or for troubleshooting connection problems.</td>
</tr>
</tbody>
</table>
Table 4-13  Port redirects – List entry (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Destination IP based exceptions | Excludes requests that are sent to a destination with the specified IP address from redirecting.  
  • For each IP address, a net mask must also be specified.  
  • When a request is excluded from redirecting, it is not processed by any of the filtering rules that are implemented.  
  • You can configure redirection exceptions in this way to let requests sent to trusted destinations skip further processing |
| Optional 802.1Q VLANs          | Lists the IDs of the network interfaces for VLAN traffic that are configured. |
| Comment                       | Provides a plain-text comment on a port redirect.                           |

Packet size handling

When communication between Web Gateway on an appliance and its clients requires that the size of data packets is handled in a flexible manner, only the explicit proxy mode can be configured as usual. The following modes require an additional configuration effort in this case:

• Proxy HA (High Availability) mode
• Transparent router mode
• Transparent bridge mode

The size of data packets is measured by the MTU (Maximum Transmission Unit) parameter, which limits the number of bytes that can be sent in one packet.

The method of negotiating the value for this parameter between communication partners is known as Path MTU Discovery. It is not available for the three modes listed above.

For example, when Web Gateway sends a data packet to a client that it connects to through a VPN (Virtual Private Network) tunnel, the MTU that the VPN tunnel can handle might be 1412, whereas the MTU of the data packets is 1500.

The VPN gateway then sends a message under the ICMP protocol to inform its partner about the required size, but this message cannot be processed unless the configured network mode is the explicit proxy mode.

To solve this problem for the other modes, reduce the MTU parameter value for the network interface on Web Gateway that is used for the communication, in this case, for communication with clients behind a VPN tunnel. Set the parameter to the value that is required, for example, to 1412.

The MTU parameter is configured on the user interface as part of the Network Interfaces settings for the IPv4 or IP6 protocol, which can be accessed under Configuration | Appliances.

Secure ICAP

When an appliance takes the roles of server and client under the ICAP protocol, communication can be performed in SSL-secured mode.

To use this mode, you need to import a server certificate for each ICAP port on the appliance that will receive SSL-secured requests from its clients. The clients are not required to submit certificates.
Requests that are directed from the appliance in its role as an ICAP client to the ICAP server must include ICAPS as a specification in the server address to enable SSL-secured communication with that server.

The appliance does not send a client certificate to the ICAP server.

**SOCKS proxy**

You can configure Web Gateway to run as a proxy that forwards web traffic under the SOCKS (Sockets) protocol.

When web traffic goes on under the SOCKS protocol, it also follows an embedded protocol, which can be, for example, HTTP or HTTPS.

The embedded protocol can be detected on Web Gateway, and if filtering is supported for web traffic under this protocol, the configured filtering rules can be processed for this traffic. If filtering is not supported, the traffic can be blocked by a suitable rule.

There are some restrictions to using the SOCKS protocol for the proxy functions on Web Gateway:

- The SOCKS protocol version must be 5, 4, or 4a.
- The BIND method is not supported for setting up connections under the SOCKS protocol.

Web traffic that is forwarded by a next-hop proxy under the SOCKS protocol can be protected using level 1 or 2 of the Kerberos authentication method.

In this case, encryption that would also make this traffic SSL-secured cannot by applied, so SSL scanning is not required. The default SSL Scanner rule set therefore includes a criteria part that lets this traffic skip SSL scanning.

**Configuring a SOCKS proxy**

To configure Web Gateway as a SOCKS proxy, you need to complete several activities.

- Enable the SOCKS proxy.
- Specify one or more proxy ports that listen to the SOCKS proxy clients when they send requests to Web Gateway.
  
  These ports are specified as part of the common proxy settings on Web Gateway.
- Create rules that control the behavior of the SOCKS proxy.

These settings are configured as part of the common proxy settings on Web Gateway.

**Using properties and an event in rules for a SOCKS proxy**

Two properties and an event are available to create rules for controlling the behavior of Web Gateway when it runs as a SOCKS proxy.

There is no preconfigured SOCKS proxy rule set available in the default rule set system or the rule set library. If you want to use such rules, you need to create them and insert them in an existing rule set or create a rule set for them.
• *ProtocolDetector.DetectedProtocol* — This property can be used to detect the embedded protocol that is followed in web traffic under the SOCKS protocol, for example, HTTP or HTTPS.

  Its value is the protocol name in string format. When the embedded protocol cannot be detected, the string is empty.

• *ProtocolDetector.ProtocolFilterable* — This property can be used to find out whether filtering is supported for web traffic following the embedded protocol that has been detected.

  Its value is *true* if this traffic is filterable and *false* otherwise.

  If this property is processed in a rule, the *ProtocolDetector.DetectedProtocol* property is also filled with a value. If this value is an empty string for the latter property, which means no the embedded protocol could not be detected, the value of the *ProtocolDetector.ProtocolFilterable* property is, consequently, set to *false*.

• *ProtocolDetector.ApplyFiltering* — This event can be used to enable processing of other rules that are configured on Web Gateway for filtering web traffic under the protocol that has been detected.

Accordingly, the following rule enables processing of other rules for filtering web traffic under the SOCKS protocol if an embedded protocol has been detected that is filterable.

**Name**

*Enable filtering for SOCKS traffic following an embedded protocol that is filterable*

**Criteria**

*ProtocolDetector.ProtocolFilterable is true*  

**Action**  

StopCycle

**Event**

*ProtocolDetector.ApplyFiltering*

The following rule blocks SOCKS traffic if no embedded protocol is detected.

**Name**

*Block SOCKS traffic if no embedded protocol can be detected*

**Criteria**

*ProtocolDetector.DetectedProtocol equals " "*

**Action**

Block

If no rule is configured that would enable the filtering of SOCKS traffic or block it if no embedded protocol is detected, this traffic is allowed.

This means that if a request for web access is received from a SOCKS client on Web Gateway, it is forwarded to the requested web server without any further processing.

### Configure SOCKS proxy settings

You can configure settings for a SOCKS proxy as part of the common proxy settings on Web Gateway.

**Task**

1. Select Configuration | Appliances .

2. On the appliances tree, select the appliance you want to configure as a SOCKS proxy, then click Proxies (HTTP(S), FTP, ICAP, and IM).

   The settings for configuring proxy functions appear in the configuration pane.

3. Scroll down to the SOCKS Proxy settings.
Configure these settings as needed.

Click Save Changes.

See also
Proxies settings on page 106

Using UDP under SOCKS
You can configure UDP (User Datagram Protocol) when Web Gateway is running as a proxy under the SOCKS protocol.

When traffic going on under the SOCKS protocol is processed by the proxy functions on Web Gateway, traffic that follows UDP can also be detected and forwarded. This traffic is not filtered, but forwarded as it is.

To allow the handling of UDP traffic in this way, you must complete the following configuration activities.

• Set the range of ports that listen to UDP traffic.
• Set a timeout on connections for UDP traffic.

You need not explicitly enable the handling of UDP traffic in addition to configuring these settings, as it is basically enabled by default.

When a client of Web Gateway sends a request for setting up a connection that follows UDP under SOCKS, the command name sent with the request is stored as the value of a property.

The name of the property is Command.Name and its value is SOCKSUDPASSOCIATE then. You can use this property in a rule for monitoring or other purposes.

You can also use this property in a rule to disable processing of UDP traffic on Web Gateway.

Use of UDP is also monitored and shown on the dashboard under SOCKS Traffic Summary.

Configure settings for UDP under SOCKS
Configure settings for UDP to enable filtering of traffic that is going on under this protocol when Web Gateway is running as a proxy under the SOCKS protocol.

Task

1 Select Configuration | Appliances.

2 On the appliances tree, select the appliance you want to configure UDP settings on and click Proxies (HTTP(S), FTP, SOCKS, ICAP ...).

3 In the configuration pane, scroll down to SOCKS Proxy. Under Port range for UDP, set the range of ports that listen to UDP traffic.

4 Scroll further down to Timeouts for HTTP(S), FTP, ICAP, SOCKS, and UDP. Under UDP timeout, set the timeout on connections for UDP.

5 Click Save Changes.
SOCKS Proxy rule set

The SOCKS Proxy rule set is a library rule set for filtering traffic that is going on under the SOCKS protocol.

<table>
<thead>
<tr>
<th>Library rule set – SOCKS Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM) and responses</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.

**Filter traffic under the SOCKS protocol with filterable embedded protocol**


The rule uses the `ProtocolDetector.ProtocolFilterable` property to check whether the protocol that is embedded in the SOCKS traffic is filterable on Web Gateway. Filterable protocols are HTTP and HTTPS.

If either of these two protocols is detected, filtering is enabled by the rule event. If no embedded protocol is detected, the rule does not apply and processing continues with the second rule.

**Block traffic under the SOCKS protocol if no embedded protocol is detected**

`ProtocolDetector.ProtocolFilterable <Protocol Detector Settings> equals " "` → Block <Default>

The rule blocks requests if no embedded protocol is detected.

**Block traffic under the SOCKS protocol if detected protocol is not on whitelist**

`ProtocolDetector.DetectedProtocol <Protocol Detector Settings> is not in list Protocol Whitelist` → Block <Default>

The rule blocks requests if an embedded protocol is detected, but is not on a particular whitelist.

The rule is not enabled by default.

---

**Instant messaging**

Instant messaging proxies can be set up on an appliance to filter instant messaging (IM) chat and file transfer.

When users of your network participate in instant messaging communication, they send, for example, chat messages to an instant messaging server, receive responses to their messages, or send and receive files. An instant messaging proxy on an appliance can intercept and filter this traffic according to the implemented filtering rules. For this purpose, instant messaging traffic is redirected to the appliance.

The following network components are involved in the filtering process:

- **Instant messaging proxies** — Proxies can be set up on an appliance to filter instant messaging under different protocols, for example, a Yahoo proxy, a Windows Live Messenger proxy, and others.

- **Instant messaging clients** — These clients run on the systems of the users within your network to enable communication with instant messaging servers.
• **Instant messaging servers** — These are the destinations that are addressed by client from within your network.

• **Other components of your network** — Other components involved in instant messaging filtering can be, for example, a firewall or a local DNS server that redirects instant messaging traffic to an appliance.

When configuring instant messaging filtering, you need to complete configuration activities for the instant messaging proxy or proxies to ensure they intercept and filter the instant messaging traffic.

You also need to ensure that the instant messaging traffic is redirected to the instant messaging proxies. However, configuration activities for this are not performed on the clients, but on other components of your network. For example, DNS redirects or firewall rules are configured in a suitable manner.

An instant messaging proxy on an appliance is mainly intended to be used together with vendor IM client software that is provided, for example, by Yahoo, Microsoft, ICQ, or Google. But this client software can still change its behavior, for example, use a new logon server, without advance warning after a hidden update.

When using third-party client software, you should generally be aware that logon servers, protocol versions, or authentication methods could have been modified in comparison to those of the original client software, which can prevent an instant messaging proxy on an appliance from intercepting and filtering instant messaging traffic.

### Configuring an instant messaging proxy

To configure an instant messaging proxy on an appliance, you need to configure the relevant parts of the **Proxies** settings of the **Configuration** top-level menu.

These are mainly settings for:

• Enabling an instant messaging proxy

• IP address and ports for listening to requests sent by instant messaging clients

• Settings for instant messaging servers

• Timeouts for instant messaging communication

Default values are preconfigured for all these settings after the initial setup of an appliance.

Instant messaging going on under the following protocols can be filtered:

• Yahoo

• ICQ

• Windows Live Messenger

• XMPP, which is the protocol used for Google Talk, Facebook Chat, Jabber, and other instant messaging services

The rules that are processed on an appliance for filtering instant messaging traffic are those that have **Requests (and IM)** configured as the processing cycle in the settings of their rule sets.

However, the **Responses** cycle can also be involved when instant messaging under the Yahoo protocol is filtered. Under this protocol, a requested file is transferred to a client in a response of the same kind as a response used for transferring files in normal web traffic. The file is stored on a server and retrieved by the client under HTTP, for example, using a suitable URL.
When problems arise in the communication between instant messaging client and proxy under a particular protocol, the client can also switch to using a different protocol and bypass the proxy this way. The client can even use a protocol for normal web traffic. On the dashboard of an appliance, this would result in a decrease of the IM traffic and an increase of the web traffic that is displayed.

**Session initialization**

During initialization of an instant messaging session between client and server, client requests can only be received on an appliance, but no responses can be sent back. As long as this is the case, the `IM.Message.CanSendBack` property will have `false` as its value when used in a rule.

We recommend that you do not implement any blocking rules with regard to session initialization, unless you want to block instant messaging traffic completely. You should also allow required helper connections, which are typically DNS requests or HTTP transfers.

Restrictions that you implement, for example, allowing only authenticated users, should rather apply to traffic going on during the session itself, such as chat messages and file transfers.

**Configuring other network components for instant messaging filtering**

The purpose of configuring other network components for instant messaging filtering is to redirect the instant messaging traffic that is going on between clients and servers to an appliance that has one or more instant messaging proxies running.

For example, under the ICQ protocol, clients send their requests to a server with the host name `api.icq.net`. For instant messaging filtering, you need to create a DNS redirecting rule that lets this host name be resolved not to the IP address of the ICQ server, but to that of the appliance.

In a similar way, firewall rules can be created to direct instant messaging traffic to an appliance rather than to an instant messaging server.

**Filtering instant messaging traffic under Windows Live Messenger**

When configuring the filtering of instant messaging traffic that is going on under the Windows Live Messenger protocol, the following is useful to know.

The host name of the instant messaging server is `messenger.hotmail.com`. This is the host name that must be resolved in a redirecting rule by the IP address of an appliance with an instant messaging proxy.

Sometimes a client connects to the server without requesting the host name to be resolved in a DNS lookup. In this case, it can help to find and remove the following registry entry within the client settings:

```
geohostingserver_messenger.hotmail.com:1863, REG_SZ
```

For a successful logon to a server, the following URL must be accessible to a client without authentication:

```
http://login.live.com
```

For this reason, you need to insert this URL in the whitelists that are used by the implemented web filtering rules on an appliance.

**Filtering Instant messaging traffic under ICQ**

When configuring the filtering of instant messaging traffic that is going on under the ICQ protocol, the following is useful to know.
The host names of the instant messaging servers are as follows:

- `api.icq.net` (Service request server: new since parting from AOL)
- `ars.icq.com` (File transfer proxy: new since parting from AOL)
- `api.oscar.aol.com` (Old service request server)
- `ars.oscar.aol.com` (Old file transfer proxy)
- `login.icq.com` (For new logon procedure)
- `login.oscar.aol.com` (For old logon procedure)

ICQ clients log on to a server in an encrypted process that cannot be intercepted by the instant messaging proxy on an appliance.

But after this, an ICQ client asks the service request server for information about the session server, using the magic token received after the logon. Here the instant messaging proxy intercepts. The filtering process then uses another logon procedure after the client name has been announced in the communication with the session server.

In contrast to the vendor Yahoo client, the vendor ICQ client ignores any Internet Explorer connection settings.

**Filtering instant messaging traffic under Yahoo**

When configuring the filtering of instant messaging traffic that is going on under the Yahoo protocol, the following is useful to know.

The list of instant messaging servers that requests are sent to can be very long. The following is a list of the host names of servers that are or have been in use. New servers can have appeared by now that would have to be added to the list.

- `vcs.msg.yahoo.com`
- `vcs1.msg.yahoo.com`
- `vcs2.msg.yahoo.com`
- `scs.yahoo.com`
- `cs.yahoo.com`
- `relay.msg.yahoo.com`
- `relay1.msg.dcn.yahoo.com`
- `relay2.msg.dcn.yahoo.com`
- `relay3.msg.dcn.yahoo.com`
- `mcs.msg.yahoo.com`
- `scs.msg.yahoo.com`
- `scsa.msg.yahoo.com`
- `sces.msg.yahoo.com`
- `scsh.msg.yahoo.com`
- `scsb.msg.yahoo.com`
- `scs.msg.yahoo.com`
- `scs-fooa.msg.yahoo.com`
- `scs-foob.msg.yahoo.com`
- `scs-fooc.msg.yahoo.com`
- `scs-food.msg.yahoo.com`
- `scs-fooe.msg.yahoo.com`
- `scs-foof.msg.yahoo.com`
- `scsd.msg.yahoo.com`
- `relay1.msg.dcn.yahoo.com`
- `relay2.msg.dcn.yahoo.com`
- `relay3.msg.dcn.yahoo.com`
- `mcs.msg.yahoo.com`
- `scs.msg.yahoo.com`
- `scs-fooa.msg.yahoo.com`
- `scs-foob.msg.yahoo.com`
- `scs-fooc.msg.yahoo.com`
- `scs-food.msg.yahoo.com`
- `scs-fooe.msg.yahoo.com`
- `scs-foof.msg.yahoo.com`
- `scsd.msg.yahoo.com`
- `relay1.msg.dcn.yahoo.com`
- `relay2.msg.dcn.yahoo.com`
- `relay3.msg.dcn.yahoo.com`
- `mcs.msg.yahoo.com`
- `scs.msg.yahoo.com`
- `scs-fooa.msg.yahoo.com`
- `scs-foob.msg.yahoo.com`
- `scs-fooc.msg.yahoo.com`
- `scs-food.msg.yahoo.com`
- `scs-fooe.msg.yahoo.com`
- `scs-foof.msg.yahoo.com`
- `scsd.msg.yahoo.com`
For a successful logon to a server, the following URLs must be accessible to a client without authentication:

- http://vcs1.msg.yahoo.com/capacity
- http://vcs2.msg.yahoo.com/capacity

For this reason, you need to insert these URLs in the whitelists that are used by the implemented web filtering rules on an appliance.

Even if the option Connect directly to the Internet has been enabled within the settings on a Yahoo client, it might still use Internet Explorer connection settings. This can cause the logon to fail in a later stage of the process. Therefore, we recommend that you also insert the URL *login.yahoo.com* in a whitelist.

### Issues with instant messaging filtering

Issues with instant messaging filtering can involve, for example, the connection between client and server or the application of the implemented filtering rules.

Keep-alive data packets are sent in regular intervals as part of the instant messaging traffic to indicate the communication partners are still connected and responsive. Intervals vary between 20 and 80 seconds, depending on the IM protocol and client software. These data packets are not processed by the filtering rules that are implemented on an appliance.

If you detect such data packets in a troubleshooting situation, you can use rule engine tracing to see which rules are still executed.

When a client sends a request for logon to the server, it is redirected to the appliance if you have configured the appropriate settings. However, a client can at the same time try to log on to another server that requires SSL-secured authentication. If this fails, the client can also drop the connection to the appliance.

Some clients also provide options for performing basic troubleshooting tests after a failure to log on to the server.

---

**XMPP proxy**

When filtering instant messaging communication on an appliance, one of the methods you can use is to set up a proxy under the XMPP (Extensible Messaging and Presence Protocol).

This protocol is also known under the name of Jabber. It is used, for example, to participate in Facebook chats or Google talk going on between an XMPP client and server.

You can configure settings for the XMPP proxy on the user interface under **Configuration | Proxies**.

When the SSL Scanner rule set is not enabled on an appliance, traffic going on between an XMPP client and this appliance is not encrypted, but filtered by all rules that are enabled on the appliance. If the client does not accept unencrypted traffic, the connection is closed.

When the SSL Scanner rule set is enabled, traffic is encrypted and inspected using SSL scanning to make it available for filtering by other rules on the appliance.
Configure common proxy settings

You can configure common proxy settings in addition to the specific settings for a network mode. Common proxy settings include settings for the different types of proxies that can be configured on Web Gateway.

**Task**

1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to configure common proxy settings for and click Proxies (HTTP(S), FTP, ICAP, and IM).
3. Configure these settings as needed.
4. Click Save Changes.

Proxies settings

The Proxies settings are used for configuring specific parameters for the different network modes that can be implemented on Web Gateway, as well as common parameters that apply for any of these modes. A periodic triggering of the rule engine can also be configured.

**Network Setup**

Settings for implementing a network mode

When a network mode is selected, specific settings for this mode appear below these settings.

**Table 4-14** Network Setup

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy (optional WCCP)</td>
<td>When selected, the explicit proxy mode is used and WCCP services can redirect web traffic to an appliance.</td>
</tr>
<tr>
<td>Proxy HA</td>
<td>When selected, the explicit proxy mode with High Availability functions is used.</td>
</tr>
<tr>
<td>Transparent router</td>
<td>When selected, the transparent router mode is used.</td>
</tr>
<tr>
<td>Transparent bridge</td>
<td>When selected, the transparent bridge mode is used.</td>
</tr>
</tbody>
</table>

**HTTP Proxy**

Settings for running a proxy on an appliance under the HTTP protocol

This protocol is used for transferring web pages and other data (also providing SSL encryption for enhanced security).

**Table 4-15** HTTP Proxy

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable HTTP proxy</td>
<td>When selected, a proxy is run on an appliance under the HTTP protocol.</td>
</tr>
<tr>
<td>HTTP Port Definition list</td>
<td>Provides a list for entering the ports on an appliance that listen to client requests.</td>
</tr>
<tr>
<td>Anonymous login for FTP over HTTP</td>
<td>Specifies the user name for logging on as an anonymous user when requests are transmitted to an FTP server by an HTTP proxy on an appliance.</td>
</tr>
<tr>
<td>Password for anonymous login for FTP over HTTP</td>
<td>Sets a password for a user name.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add Via HTTP header</td>
<td>When selected, a Via HTTP header is added to a request that is processed on an appliance. This option is selected by default.</td>
</tr>
<tr>
<td>Adjust content-type header for requests to archives (depending on the content encoding)</td>
<td>When selected, a content-type header in a request for access to an archive file is adjusted if this header does not match the content encoding that was detected for the archive.</td>
</tr>
<tr>
<td>Host header has priority over original destination address (transparent proxy)</td>
<td>When selected, requests that are sent to the proxy on an appliance in transparent proxy mode are recognized as traffic in explicit proxy mode and processed accordingly. Requests can, for example, be received on an appliance in transparent mode when they have been forwarded by a load balancer. If the proxy does not recognize the requests as traffic in explicit proxy mode, they will be forwarded to the web without filtering. This option is only available if the explicit proxy mode is not already configured on an appliance. If the option is available, it is selected by default.</td>
</tr>
</tbody>
</table>

**FTP Proxy**

Settings for running a proxy on an appliance under the FTP protocol

This protocol is used for transferring files, using separate connections for control functions and data transfer.

When a file is uploaded to the web from an FTP client and processed on Web Gateway, you can send progress indicators to the client by inserting the **FTP Upload Progress Indication** event into a suitable rule.

This will prevent a timeout on the client when processing takes more time, for example, due to scanning the file for infections by viruses and other malware.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable FTP proxy</td>
<td>When selected, a proxy is run on an appliance under the FTP protocol.</td>
</tr>
<tr>
<td>FTP port definition list</td>
<td>Provides a list for entering the ports on an appliance that listen to client requests.</td>
</tr>
<tr>
<td>Allow character @ in FTP server user name (Authentication using USER ftpserveruser@ftpserver)</td>
<td>When selected, this character is allowed in a user name.</td>
</tr>
<tr>
<td>Enable authentication using USER proxyuser@ftpserver@ftpserver</td>
<td>When selected, this syntax is allowed for a user name.</td>
</tr>
<tr>
<td>Enable authentication using USER ftpserveruser@proxyuser@ftpserver</td>
<td>When selected, this syntax is allowed for a user name.</td>
</tr>
</tbody>
</table>

---

**Table 4-16 FTP Proxy**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable FTP proxy</td>
<td>When selected, a proxy is run on an appliance under the FTP protocol.</td>
</tr>
<tr>
<td>FTP port definition list</td>
<td>Provides a list for entering the ports on an appliance that listen to client requests.</td>
</tr>
<tr>
<td>Allow character @ in FTP server user name (Authentication using USER ftpserveruser@ftpserver)</td>
<td>When selected, this character is allowed in a user name.</td>
</tr>
<tr>
<td>Enable authentication using USER proxyuser@ftpserver@ftpserver</td>
<td>When selected, this syntax is allowed for a user name.</td>
</tr>
<tr>
<td>Enable authentication using USER ftpserveruser@proxyuser@ftpserver</td>
<td>When selected, this syntax is allowed for a user name.</td>
</tr>
</tbody>
</table>
Table 4-16  FTP Proxy (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable customized welcome message</td>
<td>When selected, you can edit the welcome message that is shown to a user who sends a request for web access under the FTP protocol. Type the welcome message into the Customized welcome message text field, using the appropriate values for the variables that are contained in the message.</td>
</tr>
<tr>
<td>Select the command to be used for next-hop proxy login</td>
<td>Allows you to select the command that Web Gateway sends for logon when connecting to a next-hop proxy under the FTP protocol. The following commands can be selected: • SITE • OPEN • USER@Host</td>
</tr>
</tbody>
</table>

The following table describes an entry in the FTP port definition list.

Table 4-17  FTP port definition list – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listener address</td>
<td>Specifies the IP address and port number for a port that listens to FTP requests.</td>
</tr>
<tr>
<td>Data port</td>
<td>Specifies the port number of a port that is used for handling data transfer under the FTP protocol.</td>
</tr>
<tr>
<td>Port range for client listener</td>
<td>Configures a range of numbers for ports that listen to FTP requests received from clients. The range is configured by specifying port numbers for its beginning and end.</td>
</tr>
<tr>
<td>Port range for server listener</td>
<td>Configures a range of numbers for ports that listen to FTP responses received from web servers that requests were forwarded to.</td>
</tr>
<tr>
<td>Allow clients to use passive FTP connections</td>
<td>When selected, requests can be sent from clients using passive connections under the FTP protocol.</td>
</tr>
<tr>
<td>McAfee Web Gateway uses same connections (active/passive) as clients does</td>
<td>When selected, Web Gateway uses the same type for forwarding web traffic as a client that sent a request to Web Gateway.</td>
</tr>
<tr>
<td>McAfee Web Gateway uses passive FTP connections</td>
<td>When selected, Web Gateway can forward web traffic using passive connections under the FTP protocol.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a port that listens to FTP requests.</td>
</tr>
</tbody>
</table>
ICAP Server

Settings for running an ICAP server on an appliance that modifies requests and responses in communication with ICAP clients

Table 4-18 ICAP Server

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ICAP server</td>
<td>When selected, an ICAP server is run on an appliance.</td>
</tr>
<tr>
<td>ICAP Port Definition list</td>
<td>Provides a list for entering the ports on an appliance that listen to requests from ICAP clients. When multiple ICAP servers are configured on different appliances within your network, requests coming in from ICAP clients are distributed among these servers in round-robin mode.</td>
</tr>
</tbody>
</table>

IFP Proxy

Settings for running a proxy on an appliance under the IFP protocol

This protocol is used for transferring web pages.

Table 4-19 IFP Proxy

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IFP proxy</td>
<td>When selected, a proxy is run on an appliance under the IFP protocol.</td>
</tr>
<tr>
<td>IFP port definition list</td>
<td>Provides a list for entering the ports on an appliance that listen to client requests for the IFP proxy.</td>
</tr>
<tr>
<td>Maximum number of concurrent IFP requests allowed</td>
<td>Limits the number of IFP requests that are processed at the same time to the specified value. You can use this setting to prevent an overloading of the IFP proxy.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the IFP port definition list.

Table 4-20 IFP port definition list – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listener address</td>
<td>Specifies the IP address and port number for a port that listens for IFP requests.</td>
</tr>
<tr>
<td>Send error message as redirect</td>
<td>When set to true, a user who sent a request is informed, for example, about a blocking of the request, by redirecting the request to an error message page. Otherwise the relevant information is sent as a normal message under the IFP protocol.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a port that listens to IFP requests.</td>
</tr>
</tbody>
</table>

SOCKS Proxy

Settings for running a proxy on an appliance under the SOCKS (sockets) protocol

Table 4-21 SOCKS Proxy

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SOCKS proxy</td>
<td>When selected, a proxy is run on an appliance under the SOCKS protocol.</td>
</tr>
<tr>
<td>SOCKS port definition list</td>
<td>Provides a list for entering the ports on an appliance that listen to client requests for the SOCKS proxy.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the SOCKS port definition list.
### Table 4-22  SOCKS port definition list – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listener address</td>
<td>Specifies the IP address and port number of a port that listens for SOCKS requests.</td>
</tr>
<tr>
<td>Port range for UDP</td>
<td>Sets the range of ports used for listening to requests sent under the UDP protocol when a SOCKS proxy is configured.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a port that listens to SOCKS requests.</td>
</tr>
</tbody>
</table>

### Data Exchange Layer

Settings for using the DXL (Data Exchange Layer) technology to exchange information between different security products

#### Table 4-23  Data Exchange Layer

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription Topics</td>
<td>Provides a list of topics that a security product can subscribe to in order to receive messages about these topics.</td>
</tr>
<tr>
<td>Services</td>
<td>Provides a list of services that send messages about topics to security products.</td>
</tr>
</tbody>
</table>

The following tables describe entries in the Subscription Topics and Services lists.

#### Table 4-24  Subscription Topics – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Specifies the name of a topic.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a topic.</td>
</tr>
</tbody>
</table>

#### Table 4-25  Services – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Specifies the name of a service that sends messages about topics.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a service.</td>
</tr>
</tbody>
</table>

### Web Cache

Setting for enabling the web cache on an appliance

In addition to enabling the web cache, you need to implement a rule set to control reading from and writing to the cache.

#### Table 4-26  Web Cache

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable cache</td>
<td>When selected, the web cache is enabled on an appliance.</td>
</tr>
</tbody>
</table>
Timeouts for HTTP(S), FTP, ICAP, SOCKS, and UDP
Settings for timeouts on connections for communication under the HTTP, HTTPS, FTP, ICAP, SOCKS, and UDP protocols

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial connection timeout</td>
<td>Sets the time (in seconds) that is allowed to elapse before a newly opened connection is closed if no request is received.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Sets the time (in seconds) that is allowed to elapse before a connection is closed if a client or web server remains inactive during an uncompleted connection request communication.</td>
</tr>
<tr>
<td>Client connection timeout</td>
<td>Sets the time (in seconds) that is allowed to elapse between one request and the next before a connection from an appliance to a client is closed.</td>
</tr>
<tr>
<td>Maximum idle time for unused HTTP server connections</td>
<td>Sets the time (in seconds) that is allowed to elapse between one request and the next before a connection from an appliance to a server under the HTTP protocol is closed.</td>
</tr>
<tr>
<td>UDP timeout (inactivity timeout)</td>
<td>Sets the time (in seconds) that is allowed to elapse between one request and the next before a connection from an appliance to a client under the UDP protocol is closed.</td>
</tr>
</tbody>
</table>

DNS Settings
Settings for communication with a domain name system server

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP protocol version preference</td>
<td>Lets you select the version of the IP protocol that is used for communication.</td>
</tr>
<tr>
<td></td>
<td>• (Version options)</td>
</tr>
<tr>
<td></td>
<td>• Same as incoming connection — When selected, the protocol version is used that is already in use on the incoming connection.</td>
</tr>
<tr>
<td></td>
<td>• IP4 — When selected, version 4 of the IP protocol is used.</td>
</tr>
<tr>
<td></td>
<td>• IP6 — When selected, version 6 of the IP protocol is used.</td>
</tr>
<tr>
<td></td>
<td>• Use other protocol version as fallback — When selected, the other protocol version is used if one of the two versions is not available.</td>
</tr>
<tr>
<td>Minimal TTL for DNS cache</td>
<td>Sets a minimum time (in seconds) that must have elapsed before data stored in the cache is deleted.</td>
</tr>
<tr>
<td>Maximal TTL for DNS cache</td>
<td>Limits the time (in seconds) that elapses before data stored in the cache is deleted to the specified value.</td>
</tr>
</tbody>
</table>

Yahoo
Settings for running an instant messaging proxy under the Yahoo protocol on an appliance

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Yahoo proxy</td>
<td>When selected, a proxy for instant messaging under the Yahoo protocol is run on an appliance.</td>
</tr>
<tr>
<td>Listener address</td>
<td>Specifies the IP address of a proxy and the number of the port that listens to client requests.</td>
</tr>
<tr>
<td>Support file transfer over 0.0.0.0:80</td>
<td>When selected, requests for file transfers can use this IP address and port.</td>
</tr>
</tbody>
</table>
### Table 4-29 Yahoo (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login server</td>
<td>Specifies the host name and port number of the server that users log on to before sending requests.</td>
</tr>
<tr>
<td>Relay server (Japan)</td>
<td>Specifies the host name and port number of the server used as a relay station for transferring files.</td>
</tr>
<tr>
<td>Yahoo client connection timeout</td>
<td>Limits the time (in seconds) that elapses before an inactive connection from an instant messaging proxy to a client is closed to the specified value.</td>
</tr>
<tr>
<td>Yahoo server connection timeout</td>
<td>Limits the time (in seconds) that elapses before an inactive connection from an instant messaging proxy to a server is closed to the specified value.</td>
</tr>
</tbody>
</table>

### ICQ

Settings for running an instant messaging proxy under the OSCAR (Open System for Communication in Real Time) protocol on an appliance

### Table 4-30 ICQ

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ICQ proxy</td>
<td>When selected, a proxy for instant messaging under OSCAR is run on an appliance.</td>
</tr>
<tr>
<td>Login and file transfer proxy port</td>
<td>Specifies the IP address of an appliance that an instant messaging proxy is run on and the number of the port for handling logon and file transfer.</td>
</tr>
</tbody>
</table>
  - Enable additional file transfer proxy port — When selected, an additional port can be used for handling file transfers. |
  - Additional file transfer proxy port — Specifies the additional IP address and port number for handling file transfers. |
| BOS listener port       | Specifies the IP address of an appliance that an instant messaging proxy is run on and the number of the port that listens to BOS (Basic OSCAR Service) requests. These requests are requests for sending chat messages, as opposed to, for example, requests for file transfers. |
| ICQ login server        | Specifies the host name and port number of the server that users log on to before sending requests. |
| ICQ service request server | Specifies the host name and port number of the server that handles requests.                        |
| ICQ file transfer proxy | Specifies the host name and port number of the server that handles file transfers.                  |
| ICQ client connection timeout | Limits the time (in seconds) that elapses before an inactive connection from the instant messaging proxy to a client is closed to the specified value. |
| ICQ server connection timeout | Limits the time (in seconds) that elapses before an inactive connection from the instant messaging proxy to a server is closed to the specified value. |
Windows Live Messenger
Settings for running an instant messaging proxy under the Windows Live Messenger protocol on an appliance

Table 4-31  Windows Live Messenger

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Windows Live Messenger proxy</td>
<td>When selected, a proxy for instant messaging under Windows Live Messenger is run on an appliance</td>
</tr>
<tr>
<td>Windows Live Messenger NS proxy listener 1</td>
<td>Specifies the IP address of an appliance that an instant messaging proxy is run on and the number of the first port that listens to client requests in NS (Notification Server) mode.</td>
</tr>
<tr>
<td>Windows Live Messenger NS proxy listener 2</td>
<td>Specifies the IP address of an appliance that an instant messaging proxy is run on and the number of the second port that listens to client requests in NS (Notification Server) mode.</td>
</tr>
<tr>
<td>Windows Live Messenger SB proxy port</td>
<td>Specified the IP address of an appliance that an instant messaging proxy is run on and the number of the port that listens to client requests sent in SB (Switchboard) mode.</td>
</tr>
<tr>
<td>Windows Live Messenger client connection timeout</td>
<td>Limits the time (in seconds) that elapses before an inactive connection from the instant messaging proxy to a client is closed to the specified value.</td>
</tr>
<tr>
<td>Windows Live Messenger server connection timeout</td>
<td>Limits the time (in seconds) that elapses before an inactive connection from the instant messaging proxy to a server is closed to the specified value.</td>
</tr>
</tbody>
</table>

XMPP
Settings for running an instant messaging proxy under the XMPP protocol on an appliance
This is the protocol used for several instant messaging services including Jabber, Google Talk, Facebook Chat, and others.

Table 4-32  XMPP

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable XMPP proxy</td>
<td>When selected, a proxy for instant messaging under the XMPP protocol is run on an appliance</td>
</tr>
<tr>
<td>Proxy port</td>
<td>IP address of an appliance that an instant messaging proxy is run on and port number for the port that listens to requests sent under the XMPP protocol</td>
</tr>
<tr>
<td>Client connection timeout</td>
<td>Limits the time (in seconds) that elapses before an inactive connection from the instant messaging proxy to a client is closed to the specified value.</td>
</tr>
<tr>
<td>Server connection timeout</td>
<td>Limits the time (in seconds) that elapses before an inactive connection from the instant messaging proxy to a server is closed to the specified value.</td>
</tr>
</tbody>
</table>
## Advanced Settings

Settings for advanced proxy functions

### Table 4-33  Advanced Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum number of client connections</strong></td>
<td>Limits the number of connections between a proxy on an appliance and its clients. Specifying 0 means that no limit is configured.</td>
</tr>
<tr>
<td><strong>Compress content to client</strong></td>
<td>Provides options for compressing the content in the body of a response from a web server that is forwarded to a client by Web Gateway.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Never</strong> — The content is never compressed when the response of the server is forwarded to the client.</td>
</tr>
<tr>
<td></td>
<td>• <strong>If server's response is compressed</strong> — The content is compressed if the content was already compressed in the response of the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>If client supports compression</strong> — The content is only compressed if the client that it is forwarded to supports compression.</td>
</tr>
<tr>
<td><strong>Handle compressed requests from client</strong></td>
<td>Provides options for handling requests that were received in compressed format from a client of Web Gateway.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ignore</strong> — The compressed content is not extracted and filtered, and the request is forwarded to the web server in compressed format.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Extract</strong> — The compressed content is extracted, so it can be filtered, but not compressed again before it is eventually forwarded to the web server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Extract and compress again</strong> — The compressed content is extracted, so it can be filtered, and compressed again before it is eventually forwarded to the web server.</td>
</tr>
<tr>
<td><strong>Number of working threads</strong></td>
<td>Specifies the number of threads used for filtering and transmitting web objects when a proxy is run on an appliance.</td>
</tr>
<tr>
<td><strong>Number of threads for AV scanning</strong></td>
<td>Specifies the number of threads used to scan web objects for infections by viruses and other malware when a proxy is run on an appliance.</td>
</tr>
<tr>
<td><strong>Use TCP no delay</strong></td>
<td>When selected, delays on a proxy connection are avoided by not using the Nagle algorithm to assemble data packets. This algorithm enforces that packets are not sent before a certain amount of data has been collected.</td>
</tr>
<tr>
<td><strong>Maximum TTL for DNS cache in seconds</strong></td>
<td>Limits the time (in seconds) that host name information is stored in the DNS cache.</td>
</tr>
</tbody>
</table>
### Table 4-33 Advanced Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Timeout for errors for long running connections** | Sets the time (in hours) that a long-running connection to another network component is allowed to remain inactive before Web Gateway closes the connection.  
  The default time is 24 hours.  
  This setting prevents the performance of a Web Gateway appliance from being impacted by long-running connections that run extremely long.  
  Time is measured as follows for the different connection protocols to determine whether the timeout has been reached.  
  - HTTP, HTTPS (with content inspection), ICAP, and similar protocols: Time is measured for every request that is sent on a connection.  
  - SOCKS (when the embedded protocol is not followed), tunneled HTTP, HTTPS (without content inspection), and similar protocols: Time is measured for a connection as a whole.  
  - FTP: Time is measured for the control connection.  
  When the connection is closed, an error is generated, which can be handled by the rules in an Error Handler rule set. |
| **Check interval for long running connections** | Sets the time (in minutes) that elapses between check messages sent over a long-running connection. |
| **Maximum amount of data per connection or request** | Sets the amount of data (in MB) that can be sent on a long-running connection to another network component before Web Gateway closes the connection.  
  The default amount is 10,240 MB.  
  This setting prevents the performance of a Web Gateway appliance from being impacted by long-running connections that carry a very high data load.  
  Data load is measured as follows for the different connection protocols to determine whether the maximum amount has been reached.  
  - HTTP, HTTPS (with content inspection), ICAP, and similar protocols: Data load is measured for every request that is sent on a connection.  
  - SOCKS (when the underlying protocol is not followed), tunneled HTTP, HTTPS (without content inspection), and similar protocols: Data load is measured for a connection as a whole.  
  - FTP: Data load is measured for the data connection.  
  When the connection is closed, an error is generated, which can be handled by the rules in an Error Handler rule set.  
  The following properties are then set to the value of the measured data to be available for the error handling rules: Bytes.ToClient, Bytes.ToServer, Bytes.FromClient, Bytes.FromServer. |
<p>| <strong>Volume interval for connections</strong> | Sets the volume interval for long-running connections. |
| <strong>Internal path ID</strong> | Identifies the path an appliance follows to forward internal requests (not requests received from clients), for example, requests for style sheets used to display error messages. |
| <strong>Bypass RESPmod for responses that must not contain a body</strong> | When selected, responses sent in communication under the ICAP protocol are not modified according to the RESPMOD mode if they do not include a body. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call log handler for progress page updates</td>
<td>When selected, the rules in the log handler rule set that is implemented on the appliance are processed to deal with the specified updates and objects.</td>
</tr>
<tr>
<td>and objects embedded in error templates</td>
<td></td>
</tr>
<tr>
<td>Allow connections to use</td>
<td>When selected, local ports can be used for requests on an appliance that a proxy is run on.</td>
</tr>
<tr>
<td>local ports using proxy</td>
<td></td>
</tr>
<tr>
<td>Use virtual IP as the Proxy.IP property value</td>
<td>When selected, the value for the Proxy.IP property in High Availability mode is a virtual IP address for all nodes in a configuration.</td>
</tr>
<tr>
<td></td>
<td>It is the virtual IP address that is used by clients to connect to the proxy.</td>
</tr>
<tr>
<td></td>
<td>When the director node redirects a request sent from a client to a scanning node, this address is the value of the Proxy.IP property also on the scanning node (not the physical address of the scanning node).</td>
</tr>
<tr>
<td>HTTP(S): Remove all hop-by-hop headers</td>
<td>When selected, hop-by-hop headers are removed from requests received on an appliance that an HTTP or HTTPS proxy is run on.</td>
</tr>
<tr>
<td>HTTP(S): Inspect via headers to detect proxy loops</td>
<td>When selected, via headers in requests received on the appliance that an HTTP or HTTPS proxy is run on are inspected to detect loops.</td>
</tr>
<tr>
<td>HTTP(S): Host from absolute URL has priority over host header</td>
<td>When selected, the host names corresponding to absolute URLs in requests received on an appliance that an HTTP or HTTPS proxy is run on are preferred to the host names contained in the request headers.</td>
</tr>
<tr>
<td>Encode own IP address in progress page ID to enable non-sticky load balancers</td>
<td>When selected the own IP address is encoded in the progress page ID.</td>
</tr>
<tr>
<td>HTTP(S): Maximum size of a header</td>
<td>Sets a limit to the size (in MB) for the header of a request or response sent in HTTP(S) traffic.</td>
</tr>
<tr>
<td></td>
<td>The default size is 10 MB.</td>
</tr>
<tr>
<td>Listen backlog</td>
<td>Specifies a value for the listen backlog.</td>
</tr>
<tr>
<td></td>
<td>The default value is 128.</td>
</tr>
<tr>
<td>Limit for working threads doing IO in web cache</td>
<td>Sets a limit to the number of working threads for the web cache.</td>
</tr>
<tr>
<td></td>
<td>The default number is 25.</td>
</tr>
<tr>
<td>Progress page limit</td>
<td>Sets a limit to the size (in KB) of the progress page.</td>
</tr>
<tr>
<td></td>
<td>The default size is 40,000 KB.</td>
</tr>
</tbody>
</table>
Table 4-33 Advanced Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable TCP window scaling</td>
<td>When selected, the window for receiving data packages at the TCP communication level is increased by the scaling factor that you specify under TCP window scale.</td>
</tr>
<tr>
<td></td>
<td>This option is enabled by default. If you disable the option, it means that there is no window scaling. Disable the option only if you really want to configure the receive window in this way.</td>
</tr>
<tr>
<td>TCP window scale (format: 0-14)</td>
<td>Sets the size of the window for receiving data packages on the TCP communication level.</td>
</tr>
<tr>
<td></td>
<td>The initial size of the receive window can be scaled using a scaling factor that is calculated by taking base 2 to the power of the value that you specify here.</td>
</tr>
<tr>
<td></td>
<td>For example, if you specify 1, the scaling factor is (2^1 = 2), which means the window size is doubled.</td>
</tr>
<tr>
<td></td>
<td>The range of values that you can specify is 0–14.</td>
</tr>
<tr>
<td></td>
<td>If you specify 0, it yields 1 as the scaling factor. It means that you want to leave the initial size of your receive window as it is.</td>
</tr>
<tr>
<td></td>
<td>It still allows, however, the use of window scaling for the receive window of the communication partner.</td>
</tr>
<tr>
<td></td>
<td>The default value is 2.</td>
</tr>
</tbody>
</table>

Periodic Rule Engine Trigger List
Settings for connecting to web servers, calling the rule engine, and downloading data

Table 4-34 Periodic Rule Engine Trigger List

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Periodic Rule Engine Trigger List</td>
<td>When selected, connections to the web servers specified in list called URL definition list are set up in regular intervals.</td>
</tr>
<tr>
<td></td>
<td>The interval for each web server connection is also specified on the list.</td>
</tr>
<tr>
<td></td>
<td>When the interval has elapsed, the rule processing module (rule engine) on an appliance is called, a connection to the web server is set up, and data is downloaded from the web server and passed on to the rule engine for processing.</td>
</tr>
<tr>
<td></td>
<td>Data is only downloaded under the HTTP and HTTPS protocols.</td>
</tr>
<tr>
<td></td>
<td>Web servers that connections are set up to in this way include next-hop proxy servers and other servers used for providing particular services in the web.</td>
</tr>
<tr>
<td>URL definition list</td>
<td>Provides a list of web servers that a connection can be set up to.</td>
</tr>
</tbody>
</table>

The following table describes a list entry in the URL definition list.

Table 4-35 URL definition list – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Specifies the IP address and port number or the URL of a web server that a connection can be set up to.</td>
</tr>
<tr>
<td>Trigger interval</td>
<td>Specifies the interval (in seconds) that elapses before the next attempt to set up a connection to a web server.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a web server connection.</td>
</tr>
</tbody>
</table>
Controlling outbound source IP addresses

Using different source IP addresses for outbound connections from Web Gateway to web servers or next-hop proxies can lead to connection problems. To avoid these problems, you can replace these addresses with a single address.

Different source IP addresses might be used, for example, when load balancing is configured for multiple Web Gateway appliances. Load balancing can lead to connection problems on the side of the involved web servers or next-hop proxies. Problems can, for example, arise when source IP addresses change during a session period.

To avoid these problems, you can configure a rule that replaces changing source IP addresses with a single address.

This single address does not have to be fixed. You can set up a list of IP addresses and let the rule select an address in a particular position on the list. The address that replaces other addresses then varies according to what you have entered in that position.

Network setups for controlling outbound source IP addresses

Controlling outbound source IP addresses is supported for network setups with:

- IPv4 or IPv6
- HTTP, HTTPS, FTP, or SOCKS proxy
  
  Instant messaging is not supported.
- Proxy (with optional WCCP) mode
  
  The transparent router mode is supported if the source IP addresses that are used for replacing other addresses are configured as aliases.

  The Proxy HA and transparent bridge modes are not supported.

Periodic rule engine triggering is also possible when control of outbound source IP addresses is implemented.

Sample rule for controlling outbound source IP addresses

A rule that replaces outbound source IP addresses by a single address, for example, when connections to next-hop proxies are set up, could look as follows:

Name

Use proxy depending on the destination

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL.Destination.IP is in range list Next Hop Proxy IP Range List</td>
<td>Continue</td>
<td>Enable Next Hop Proxy &lt;Internal Proxy&gt;</td>
</tr>
<tr>
<td>OR</td>
<td>Enable Outbound Source IP Override(Proxy.OutboundIP(2))</td>
<td></td>
</tr>
<tr>
<td>URL.Destination.IP is in list Next Hop Proxy IP List</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The criteria of the rule specifies when a next-hop proxy is used. The first of the two events sets up a connection to a next-hop proxy.

The second event, Enable Outbound Source IP Override, is for controlling outbound source IP addresses. It replaces ("overrides") any source IP address that is submitted with a request by an IP address that is taken from a list.
An event parameter, which is itself a property, specifies the IP address. The name of the property is `Proxy.OutboundIP`. Its value is the IP address in the list position determined by the property parameter.

**List of IP addresses for controlling outbound source IP addresses**

The list of IP addresses that you can use to replace outbound source IP addresses is part of the `Proxies` settings. You can find it there under *Advanced Outgoing Connection Settings*. Its name is *Outbound Source IP list*.

The following applies regarding the position of an IP address in the list:

- The list index starts from 0. If you specify, for example, 2, as the parameter of the `Proxy.OutboundIP` property to determine a position, the third IP address on the list is selected.

- If you specify a parameter value that is higher than the number of list entries, the position is determined by calculating `<parameter-value> modulo <number-of-list-entries>`.

  For example, if you specify 5 for a list that has only three list entries, the result of the modulo calculation is 2. The third IP address on the list is then selected.

**Network routing and IP address spoofing**

The IP addresses that are inserted into data packets by the *Enable Outbound Source IP Override* event are non-local source IP addresses. You must therefore configure network routing in a suitable way.

Data packets that are sent back from a web server to a client must be routed to the proxy on Web Gateway. You can, for example, use static routes to route the data packets.

When the *Enable Outbound Source IP Override* event is triggered and you have IP address spoofing enabled, the event also overrides this setting.

**Logging the use of outbound IP source addresses**

Several properties are available for logging data about outbound connections, including the source IP address and port that Web Gateway uses when connecting to web servers or next-hop proxies.

These properties are set to particular values, regardless of whether you have configured a single source IP address, using the *Enable Outbound Source IP Override* event. But you can also use them in this case.

- `Proxy.Outbound.IP` — Stores the source IP address that Web Gateway uses when connecting to web servers and next-hop proxies.

  Do not confuse this property with *Proxy.OutboundIP*, which has no dot before *IP* and is used together with the *Enable Outbound Source IP Override* event to select a single source IP address from a list.

- `Proxy.Outbound.Port` — Stores the source port that is used by Web Gateway when connecting to web servers or next-hop proxies.

- `Proxy.Outbound.IPLList` — Stores the list of source IP addresses that Web Gateway can select an address from when connecting to web servers and next-hop proxies.

  The list is configured as part of the `Proxies` settings under *Advanced Outgoing Connection Settings*. Its name is *Outbound Source IP list*. When a single source IP address for outbound connections is configured, it is taken from this list.
Configure control of outbound source IP addresses
Replace different outbound source IP addresses with a single address to avoid connection problems.

Task
1. Select Configuration | Appliances.
2. Select an appliance for configuring the replacement of IP addresses, then select Proxies (HTTP(S), FTP, SOCKS, ICAP ...) and scroll down to Advanced Outgoing Connection Settings.
3. Under Outbound source IP list, add one or more IP addresses to the list of source IP addresses for outbound requests.
4. Add the following event to an existing rule for connections to web servers or next-hop proxies: Enable Outbound Source IP Override with Proxy.OutboundIP property as a parameter.

The rule now uses the list that you have configured to select an IP address for replacing different outbound source IP addresses.

Using WCCP to redirect FTP traffic
Requests that clients of Web Gateway send to servers under the FTP protocol can be redirected to Web Gateway using the WCCP (Web Cache Control Protocol) redirection method.

To send a request to a server under the FTP protocol, a client of Web Gateway opens the initial FTP connection. The client uses the IP address of the server for this connection. To let Web Gateway act as a proxy, the request is redirected to the IP address of the appliance that Web Gateway runs on.

Under the default settings, the client considers this redirection as a security risk and does therefore not continue with opening the FTP data connection. When redirection is performed using the WCCP protocol, you can solve this problem by modifying the settings as follows:

- Using the active FTP mode for the connection from the client to the proxy
  Clients are by default allowed to use the passive FTP mode. You can enforce the active FTP mode by disabling an option of the proxy settings on the user interface of Web Gateway.

- Configuring a port for redirection to the proxy
  This port must be entered in the list of ports that are redirected under WCCP.

- Letting the proxy use the IP address of the FTP server instead of its own IP address
  Setting a particular parameter ensures that the proxy uses this address.

After modifying the settings in this way, a client uses the active FTP mode. It sends the proxy an IP address and a port number to connect to. The proxy returns a synchronization message. In this message, the IP address of the FTP server is used as the source IP address of the proxy. The port number is 21 or 2020.

The client responds with the IP address of the FTP server as its destination IP address and the same port number. Requests from the client to the FTP server are then redirected to the proxy, using WCCP as the redirection method.

The WCCP redirection method cannot be used for FTP traffic in transparent bridge or router mode.
Configure the use of WCCP for redirecting FTP traffic

To enable the use of the WCCP redirection method for requests that clients send to servers under the FTP protocol, configure the proxy settings as follows.

Task

1. Enforce use of the active FTP mode by clients.
   a. Select Configuration | Appliances.
   b. On the appliances tree, select the appliance that you want to enable use of the WCCP redirection method for, then click Proxies (HTTP(S), FTP, SOCKS, ICAP ...).
   c. Scroll down to FTP Proxy and make sure that Enable FTP proxy is selected.
   d. Select an entry in the FTP port definition list, click Edit, and under FTP Proxy Port, deselect Allow clients to use passive connections.
      Repeat this substep for all entries in the list.

2. Add ports 21 and 2020 to the ports that are used for redirection under WCCP.
   a. Within the Proxies settings, scroll to Transparent Proxy, and under Supported redirection methods, make sure that WCCP is selected.
   b. Select an entry in the WCCP services list, click Edit, and under Ports to be redirected type 21,2020.
      Repeat this substep for all entries in the list.

3. Click Save Changes.

4. Within the relevant settings, set the ftp.match.client.data parameter to yes.

   This setting ensures that Web Gateway uses the IP address that it received from the client as its source IP address when responding to the client.
   
   This address is the IP address of the FTP server in question, not the IP address of the Web Gateway appliance. The client does therefore not suspect a security risk.

   Requests sent from a client to a server under the FTP protocol are now redirected to Web Gateway, using the WCCP redirection method, and processed without problems.

Using the Raptor syntax for FTP logon

When Web Gateway is configured to run as an FTP proxy, the Raptor syntax can be used for logging on to an FTP server with Web Gateway as a proxy.

To perform this logon, the user who wants to access the FTP server can run the USER, PASS, and ACCEPT commands from a suitable FTP client. Using these commands, the FTP server is specified together with user names and passwords for both the FTP server and the Web Gateway proxy.

The command syntax is as follows:

USER <ftpuser>@<ftpserver> <proxyuser>
PASS <ftpuserpass>
ACCT <proxyuserpass>

The following table describes the meanings of the command parameters.
Table 4-36 Command parameter for FTP logon

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftpserver</td>
<td>FTP server that access is requested to</td>
</tr>
<tr>
<td>ftpuser</td>
<td>User name on the FTP server</td>
</tr>
<tr>
<td>ftpuserpass</td>
<td>Password for the FTP server</td>
</tr>
<tr>
<td>proxyuser</td>
<td>User name on the Web Gateway proxy</td>
</tr>
<tr>
<td>proxyuserpass</td>
<td>Password for the Web Gateway proxy</td>
</tr>
</tbody>
</table>

Node communication protocols

When Web Gateway appliances run as director and scanning nodes in a Central Management configuration, communication between the nodes uses the Virtual Router Redundancy Protocol (VRRP) and MWG Management Protocol.

Use of the protocols depends on the proxy settings that you have configured on the appliances that run as nodes. The protocols differ with regard to the activities of director and scanning nodes that are covered by them.

Virtual Router Redundancy Protocol

The Virtual Router Redundancy Protocol is used when you have configured Web Gateway as a proxy in transparent router mode or High Availability proxy mode.

Under this protocol, virtual IP addresses are assigned to active director nodes and backup director nodes. The protocol also determines which director node takes the active director role.

MWG Management Protocol

The MWG Management Protocol is used in transparent router, transparent bridge, and High Availability proxy mode. Under this protocol, scanning nodes are identified that are available for processing web traffic.

The node that takes the active director role sends out broadcast messages to the scanning nodes, using the IP address that you have configured as its source IP address under the Management IP option of the respective proxy settings.

The protocol lets scanning nodes that are available within the same network segment respond in regular intervals to the discovery messages of the director node.

Security considerations

The security features of the Virtual Router Redundancy Protocol and MWG Management Protocol are similar to that of the Address Resolution Protocol (ARP).

The Virtual Router Redundancy Protocol uses multicast with an IP address that is not routed beyond the local broadcast domain. MWG Management Protocol uses broadcast messages.

A malicious node on the same network segment might send VRRP messages and hence impersonate itself as the active director node holding the respective virtual IP address. If that node decides to drop all data packets it receives for the virtual IP address, network connectivity stops for the clients that are connected to the Web Gateway proxy.

To prevent malicious nodes from harming operation of the Web Gateway proxy, we recommend that you use IP addresses from a protected network segment when configuring proxy settings according to the Virtual Router Redundancy Protocol and the MWG Management Protocol.
Using DNS servers according to domains

The use of DNS (Domain Name System) servers to resolve domain information provided in URLs into IP addresses when requests for web access are processed on Web Gateway can be configured according to the domains of the requested destinations.

This use of DNS servers is also known as conditional DNS forwarding.

Domains, for example, testnet.webwasher.com, are entered into a list together with the IP address of the DNS server that is used to resolve the URL information. More than one DNS server can be specified this way for a domain.

When a request to a particular destination on the web is sent to Web Gateway, it is forwarded to a DNS server according to this list.

The use of a particular DNS server can be configured dynamically with DHCP (Dynamic Host Configuration Protocol). This is also the default setting after the initial setup of a Web Gateway appliance.

If both configuration with DHCP and conditional DNS forwarding are configured, DHCP takes precedence and conditional DNS forwarding is bypassed.

If a BIND server is configured as a DNS server, the DNS server settings that are stored in a configuration file on Web Gateway will be overwritten. To keep these settings for domain name resolving, you need to enter them manually again.

Configure the use of DNS servers according to domains

To enable the use of DNS servers according to the domains of destinations in the web, configure the Domain Name Service settings in a suitable manner.

Task

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure the use of DNS servers for and click Domain Name Service.

3. Configure the settings in the Conditional DNS Forwarder Configuration section as needed.

4. Click Save Changes.

Domain Name Service settings

The Domain Name Service settings are used for configuring DNS servers, including the use of DNS servers according to particular domains, which is also known as conditional DNS forwarding.

Domain Name Service Settings

Settings for DNS servers

Table 4-37  Domain Name Service Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary domain name server</td>
<td>Specifies the IP address of the first server.</td>
</tr>
<tr>
<td>Secondary domain name server</td>
<td>Specifies the IP address of the second server.</td>
</tr>
<tr>
<td>Tertiary domain name server</td>
<td>Specifies the IP address of the third server.</td>
</tr>
</tbody>
</table>
Conditional DNS Forwarder Configuration

Settings for using DNS servers according to domains

Table 4-38 Conditional DNS Forwarder Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable conditional</td>
<td>When selected, a DNS server from the Conditional Forwarder List resolves domain information sent in a request to Web Gateway into an IP address.</td>
</tr>
<tr>
<td>forwarding</td>
<td>• A DNS server is selected from the list according to the domain of the requested destination.</td>
</tr>
<tr>
<td></td>
<td>• A DNS server is specified in the list by its IP address.</td>
</tr>
<tr>
<td></td>
<td>• Up to 5 DNS servers can be specified for a domain.</td>
</tr>
<tr>
<td></td>
<td>If this option is enabled, the following five options become accessible.</td>
</tr>
<tr>
<td>Default resolver(s)</td>
<td>Specifies the IP addresses of the DNS server or servers that are by default used for resolving domain information.</td>
</tr>
<tr>
<td></td>
<td>IP addresses for up to 5 DNS servers can be specified here.</td>
</tr>
<tr>
<td>TTL for positive answer</td>
<td>Limits the time (in seconds) that positive answers are cached for conditional DNS forwarding to the specified value.</td>
</tr>
<tr>
<td></td>
<td>• The allowed time range is 1 to 604800 seconds.</td>
</tr>
<tr>
<td></td>
<td>• The default time is 604800 seconds.</td>
</tr>
<tr>
<td>TTL for negative answer</td>
<td>Limits the time (in seconds) that negative answers are cached for conditional DNS forwarding to the specified value.</td>
</tr>
<tr>
<td></td>
<td>• The allowed time range is 1 to 604800 seconds.</td>
</tr>
<tr>
<td></td>
<td>• The default time is 10800 seconds.</td>
</tr>
<tr>
<td>Conditional Forwarder</td>
<td>Contains entries for domains and IP addresses of DNS servers that are involved in conditional forwarding.</td>
</tr>
<tr>
<td>List</td>
<td>Conditional Forwarder Reverse Lookup List Contains entries for domains and IP addresses of DNS servers that are involved when a reverse lookup is performed in conditional forwarding.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the Conditional Forwarder List.

Table 4-39 Conditional Forwarder List – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward zone</td>
<td>Specifies a domain name. When a request for a destination within a particular domain is sent to Web Gateway, the DNS server or servers are used for a lookup that have been specified for this domain.</td>
</tr>
<tr>
<td>DNS server(s)</td>
<td>Specifies a DNS server or several DNS servers by their IP addresses. IP addresses for up to five DNS servers can be specified here.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on the conditional DNS forwarding that is configured by this list entry.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the Conditional Forwarder Reverse Lookup List.
Table 4-40 Conditional Forwarder Reverse Lookup List – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward zone</td>
<td>Specifies the IP address of a domain.</td>
</tr>
<tr>
<td></td>
<td>• The IP address is specified in CIDR notation.</td>
</tr>
<tr>
<td></td>
<td>• When a reverse lookup is performed for an IP address, the DNS server or servers are used that have been specified for this address.</td>
</tr>
<tr>
<td>DNS server(s)</td>
<td>Specifies a DNS server or several DNS servers by their IP addresses. IP addresses for up to five DNS servers can be specified here.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on the conditional DNS forwarding that is configured by this list entry.</td>
</tr>
</tbody>
</table>

Using DXL messages to exchange web security information

You can use the DXL technology to send and receive information to and from web security products that are connected to Web Gateway in a common security architecture.

McAfee® Data Exchange Layer (DXL) is a messaging technology for real-time information exchange. The technology is used to exchange security-related information, for example, file reputation scores between Web Gateway and other web security products that are connected to it.

This kind of information exchange is part of a security architecture that is provided by McAfee and is also known as Security Connected.

You can exchange information under DXL in two main scenarios: One is publishing a message about a security topic in an event and receiving this message after subscribing for the topic. The other is sending a query for information about a security topic to a service and receiving a response from this service.

The web security products that are connected to each other, including Web Gateway, take the various roles that belong to these scenarios. Products can be publishers and subscribers, they can send queries and also act as services that queries are sent to.

When a publisher sends DXL messages to the subscribers, they send no responses. When a DXL message is sent as a query for security-related information to a service, the service sends a response, providing information about the topic that was specified in the query.

Web Gateway supports the sending of DXL messages in events and as queries to a service. It can also receive DXL messages and act as a service that provides information on a web security topic.

Configuring settings for the exchange of web security information

To enable the exchange of information about web security topics on Web Gateway, you must configure several settings. Credentials for a McAfee ePO server must be configured, as parts of the DXL architecture are managed by this administration product.

Topics and services are configured as part of the settings for the proxy functions of Web Gateway.

DXL messages can also be traced for troubleshooting after enabling the relevant option of the Troubleshooting settings.

Sample rule for sending a DXL message in an event

The following sample rule uses an event to send a message about a topic to the subscribers.
The message is sent when processing a request for web access from a client of Web Gateway shows that the requested URL belongs to a bad category. The event then sends the IP address of the client to all that have subscribed to the "Bad Client" topic to receive information about bad clients.

The event **DXL.Event** is provided for creating a rule like this. The event has two parameters, which are a topic and information that is in some way related to the topic.

The rule looks as follows.

**Name**

Use an event to send a DXL message to the subscribers

**Criteria**

URL.Categories<Default> at least one in list Bad Categories

**Action**

Continue

**Event**

DXL.Event ("Bad Client", "IP.ToString(Client.IP))

**Sample rule for sending a DXL message as a query to a service**

The following sample rule retrieves the reputation score for a requested file and blocks the request if the reputation score has a particular value.

The rule uses the **DXL.Query** property in its criteria. This property provides a reputation score that was retrieved by sending a DXL message as a query to a service. The web security product that takes the role of the service is a McAfee® Threat Intelligence Exchange (TIE) server.

One of the property parameters is the topic that the query is about. The other parameter is the information about the topic that was the query retrieved. This information was received as response from the service that the query was sent to.

If a query is sent to a TIE server, the **TIE.Filereputation** property is used to store the information that is retrieved as response from this server.

The rule looks as follows.

**Name**

Send a DXL message as a query to a service

**Criteria**

DXL.Query ("File Reputation", TIE.Filereputation) matches *reputation=15*

**Action**

Block <FileReputation>

**Configure the settings for information exchange with DXL**

To enable information exchange with DXL, configure credentials for communication with a McAfee ePO server and the topics and services that you want to include in DXL messages.

**Task**

1. Configure the credentials that Web Gateway submits when connecting to a McAfee ePO server to enable DXL messaging.
   a. Select **Configuration | Appliances**.
   b. On the appliances tree, select the appliance that you want to configure the information exchange on and click **ePolicy Orchestrator**.
   c. Under **ePO DXL Settings**, configure a host name, user account, and password for use by Web Gateway when connecting to a McAfee ePO server.

2. Click **Proxies (HTTP(S), FTP, SOCKS, ICAP ...)** and on the configuration pane scroll down to **Data Exchange Layer**.
3 Configure topics for DXL messages:
   a. On the toolbar of the Subscription Topics list, click the Add (or Multiple Add) icon.
   b. In the window that opens, type a topic name (or multiple names separated by commas), then click OK.
      The window closes and the topics appear in the list.

4 Configure the following for each service that you want to receive DXL messages:
   a. On the toolbar of the Services list, click the Add icon. The Add DXL Service window opens.
   b. Type a service name in the Service field.
   c. On the toolbar of the Topics list, click the Add (or Multiple Add) icon.
   d. In the window that opens, type the name of a topic (or multiple names separated by commas) that the service is to send information about, then click OK.
      The window closes and the topics appear in the list.
   e. Click OK to close the Add DXL Service window.
      The service appears in the list.

5 Click Save Changes.

**Configure settings for information exchange using a TIE server**

Configure settings to use a TIE server for providing web security information that is collected on this server. The web security information that Web Gateway can retrieve from a TIE server is file reputation scores.

**Task**

1. Select Policy | Settings.

2. On the Engines branch of the settings tree, select TIE Filter and click Add. An Add Settings window opens.

3. In the Name field, type a name for the settings.

4. Under Product Priorities, select one of the following.
   - **Use default product priority order**
     The default order is to use information from the TIE server first for sending in an event. If this information is not available, the lowest reputation score that a connected product sent is retrieved.
     After selecting this option, continue with step 6.
   - **Customize product priority order**
     After selecting this option, continue with step 5.
5 Customize the product priority order.
   a On the toolbar of the product list, click the Add icon.
   b In the Product ID field of the window that opens, type a comma-separated list of product IDs in
      the order that you want to use information from these products.
      Typing an asterisk as a list element means that the lowest reputation score sent by a product is
      used.
      In the Comment field, you can optionally type an explanation for each product ID.
   c Click OK.
      The window closes and each product ID appears in a separate line of the list.
6 Click OK to close the Add Settings window.
      The window closes and the new settings appear under TIE Filter on the settings tree.
7 Click Save Changes.

Best practices - Working with the user-agent header

The user-agent header is a header in a request for web access sent under the HTTP protocol. This
header identifies the software program that was used to send the request. You can work with this
header to create a rule that performs a particular action on a request that contains this header.

The software used on a client for sending a request can be a browser, a media player, or a similar
program. If you find, for example, that requests sent with a particular browser cause issues with user
authentication on Web Gateway, you can create a rule that skips authentication for these requests or
blocks them.

The rule contains the value of the user-agent header in the criteria for the action that is performed.
When a request is processed on Web Gateway, this value is retrieved from the request to see whether
it is the one for the software program that causes issues.

If not only one program causes issues or you expect that more will be found, you can also work with a
list of user-agents. The value of the user-agent header within a request is then compared to the list
entries to see whether it matches any of them.
Finding the user-agent

To create a rule with an action for a request that caused issues due to its user-agent, you must know which user-agent it is. There are several ways to find this out.

- **Access log** — You can inspect the access log that is maintained on Web Gateway. The data that this log records includes the user-agent header of a request by default.

- **Online resources** — You can find information about browsers, media players, and similar programs that run as user-agents on client systems using online resources, for example, performing an online search. Websites are available that support your search for information, for example, by listing and describing the most common user-agents or by identifying the browser that is currently in use on a client.

- **TCP dump** — You can create a TCP dump of the request processing that Web Gateway performs, using the troubleshooting functions on the user interface. For more information about these functions, see the *Troubleshooting* chapter.

When a TCP dump has been created, you can work with a packet tracing tool, for example, Wireshark, to follow the TCP stream. You can select a GET request sent for web access and inspect the data packets of this request with its headers.

If you already have some information about the user-agent that causes issues, you can filter the output in Wireshark accordingly. Entering, for example, the following line returns all data packets that contain the text string "Mozilla".

```
http.user_agent matches "Mozilla"
```

Most user-agent headers for browsers begin with the text string "Mozilla". This does not necessarily mean that the user-agent is the Mozilla Firefox browser. It could be Firefox or a different browser.

Common user-agent headers

The following list provides information about some user-agent headers for software programs that are often found when TCP dumps created on Web Gateway are inspected.

Codes lines from the Wireshark packet tracing tool showing the relevant information are added for each user-agent header.

- **Firefox** — A user-agent header for a Mozilla Firefox browser contains the text string "Firefox/" followed by the version number.

```
Mozilla/6.0 (Windows NT 6.2; WOW64; rv:16.0.1) Gecko/20121011 Firefox/16.0.1
```

- **Internet Explorer** — A user-agent header for a Microsoft Internet Explorer browser contains the text string "MSIE" followed by the version number.

```
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
```

- **Chrome** — A user-agent header for a Google Chrome browser contains the text string "AppleWebKit".

```
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.22 (KHTML, like Gecko) Chrome/25.0.1364.172 Safari/537.22
```

Do not confuse a header like this with a user-agent header for the Apple iPhone smartphone.
• **Windows Media Player** — A user-agent header for Windows Media Player contains the two text strings shown in this sample code block.

```
Windows-Media-Player/10.0.0.xxxx
NSPlayer/10.0.0.xxxx WMFSDK/10.0
```

• **iTunes** — A user-agent header for an Apple iTunes media player contains the text string "iTunes/" followed by the version number.

```
Mozilla/6.0 (Windows NT 6.2; WOW64; rv:16.0.1) Gecko/20121011 Firefox/16.0.1
```

• **Safari on iPhone** — A user-agent header for an app that runs on an iPhone, for example, the Apple Safari browser, contains the text string "iPhone".

```
Mozilla/6.0 (Windows NT 6.2; WOW64; rv:16.0.1) Gecko/20121011 Firefox/16.0.1
```

**Sample rule for working with the user-agent header**

In a rule that performs an action on a request with a user-agent header for a particular software program, the user-agent is included in the rule criteria. If the rule is to apply for more than one user-agent, you can work with a list of user-agents.

> We recommend using a list, even if you are presently interested in a particular user-agent only. Using a list makes it easier to modify the rule when more user-agents must be addressed in the future.

The rule criteria contains a property that is set to the value for the user-agent in the user-agent header when the rule is processed. The rule applies if this value matches one of the entries in a list of user-agents or a single user-agent if you have configured the rule this way.

The list might, for example, contain the entry "MSIE 10" for version 10 of the Microsoft Internet Explorer. If a request includes a user-agent header for this browser, the rule criteria matches, as the string that you entered in the list is also contained in the user-agent header.

The property that is used to retrieve the value for the user-agent from the user-agent header in a request is `Header.Request.Get()` To use the property for retrieving this value, you configure the string "User-Agent" as a parameter of the property.

The purpose of the sample rule is to let a request skip SSL scanning. It looks as follows.

<table>
<thead>
<tr>
<th>Name</th>
<th>Skip SSL Scanner for user-agents in list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Header.Request.Get(&quot;User-Agent&quot;) matches in list User Agent Whitelist</td>
</tr>
<tr>
<td>Action</td>
<td>–&gt; Stop Rule Set</td>
</tr>
</tbody>
</table>

We recommend including still another criteria part in a rule like this. As it is the client that provides the information about the user-agent, the client or a malware program might spoof a trusted user-agent to bypass filtering.

A sample rule that has its criteria extended by another part to protect the rule against user-agent spoofing looks as follows.

<table>
<thead>
<tr>
<th>Name</th>
<th>Skip SSL Scanner for user-agents in list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td></td>
</tr>
</tbody>
</table>
In the sample rules, Stop Rule Set is configured as action. To address issues that a user-agent causes with regard to a function of Web Gateway, you insert the rule in the rule set for that function.

For example, if a user-agent causes issues with SSL scanning, insert it at the beginning of the SSL Scanner rule set. If the rule applies, processing of this rule set is stopped, which means that the relevant request skips SSL scanning. The rule can be used in a similar way to skip, for example, user authentication.

If you do not want to let requests skip anything due to issues with user-agents, you can replace the Stop Rule Set action with Block. You can then create a rule set for globally blocking requests (if it does not yet exist in your rule set system) and insert the rule.

Create a rule for working with the user-agent header

Create a rule that performs an action on requests depending on their user-agent headers to address issues caused by the user-agents.

The following procedure assumes that an issue with SSL scanning is caused by a particular user-agent. The rule that is created lets requests with user-agent headers containing this user-agent skip SSL scanning to avoid the issues.

Task

1. Select the rule set for the function that is skipped for requests with the user-agent that causes issues.
   b. On the rules tree, select the SSL Scanner rule set.
   c. Click Unlock View on the configuration pane and confirm with Yes.

2. The nesting SSL Scanner rule set is accessible for inserting rules.

2. Configure the name of the rule that lets requests skip the rules in the rule set.
   a. Click Add Rule.
      The Add Rule window opens with the Name step selected.
   b. In the Name field, type a name for the rule, for example, Skip SSL Scanner for user-agents on list.

3. Configure the property that is used to retrieve the user-agent.
   a. Click Rule Criteria and then Add.
   b. From the drop-down menu, select Advanced Criteria.
      The Add Criteria window opens.
   c. Click Filter, then select Engine | Header and from the filtered list of properties select Header.Request.Get.
   d. Click Parameters at the property.
   e. In the window that opens, make sure that Parameter value is selected and type User-Agent, then click OK to close the window.
4 Configure the operator and the list to compare the property value with.
   a Leave the **Matches in list** operator that is suggested.
   b From the lists under **Compare with**, select **User Agent Whitelist**.

   > The list is initially empty and you must insert an entry for the user-agent that causes issues.

   c Click **OK**.

   The **Add Criteria** window closes and the complete criteria appears in the **Add Rule** window.

5 Configure the rule action.
   a Click **Action**.
   b From the **Action** list select **Stop Rule Set**

6 Complete the configuration.
   a Click **Finish**.

   The **Add Rule** window closes and the rule appears in the **SSL Scanner** rule set.

   > The **SSL Scanner** rule set is empty by default, as the rules for the scanning functions are contained in nesting rule sets. If you find that the nesting rule set contains rules that were inserted after the initial setup, move the new rule into first position.

   b Click **Save Changes**.

---

**Bypassing for Office 365 and other Microsoft services**

Requests sent to Office 365 and other Microsoft services, and responses received from these services, can be configured to bypass filtering to avoid a load increase on Web Gateway.

Bypassing is handled for these requests and responses by rules. A rule set with suitable rules is provided in the default rule set system and in the rule set library.

To configure the bypassing of requests and responses in traffic to and from Office 365 and other Microsoft services, you can work with:

- **Key elements of rules** — After opening the rule set with the bypassing rules, you can view and configure key elements of these rules.

- **Complete rules** — After clicking **Unlock View** in the key elements view, you can view the bypassing rules completely, configure all their elements, including the key elements, and also create rules or delete rules.

   You cannot return from this view to the key elements view unless you discard all changes or reimport the rule set.

**Office 365 and other Microsoft services**

Microsoft offers several cloud-based applications that belong to the Office 365 application suite. These applications rely heavily on HTML5 features to provide an enriched user experience.
Consequently, some of these applications can set up a high number of connections and also several "endless" connections, which might considerably increase the load on a Web Gateway appliance. The increased load can have an impact on the proxy functions of Web Gateway, leading to slow or delayed web access, timeouts, and other issues.

To avoid such issues, you might want to let requests and responses in traffic to and from Office 365 and other Microsoft services bypass filtering on Web Gateway. Many of these requests and responses also use undocumented formats or protocols that are proprietary to Microsoft and cannot be scanned and filtered on Web Gateway.

**Rule set for Microsoft services bypassing**

The Bypass Microsoft (Office 365) Services rule set contains rules that enable bypassing for requests and responses in traffic to and from Office 365 and other Microsoft services.

IP address and URL lists published by Microsoft are used to recognize the requests that are submitted for accessing these services.

The rule set is placed at the top of the default rule set system.

**Using a Domain Name System**

The bypassing rule set requires Web Gateway to access a Domain Name System (DNS). In some configurations, for example when next-hop proxies are used, Web Gateway does not normally require DNS access, so this access might not be configured or even be blocked by a rule.

Most of the rules in the rule set, however, rely on evaluating the URL.Destination.IP property to recognize relevant requests. The DNS is then used to resolve the destination IP address of the request that is currently processed.

So, if a DNS is not correctly configured or not configured at all, you might encounter timeouts or slow performance when working with the rule set.

**Key elements for Microsoft services bypassing**

The key elements of the rules that handle bypassing for Office 365 and other Microsoft services are related to the individual services that requests and responses are sent to and received from.

**Bypassing for Microsoft services**

Options for handling Microsoft services bypassing

**Table 4-41  Bypassing for Microsoft services**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bypass Exchange Online, Bypass Microsoft Federation Gateway, and other options for handling Microsoft services bypassing</td>
<td>When selected, a request from a client of Web Gateway to access Exchange Online or another Microsoft service is forwarded to the service unfiltered. When a response is received from the service, it is also passed on to the client unfiltered. None of these options is enabled by default.</td>
</tr>
</tbody>
</table>
Bypass Microsoft (Office 365) Services rule set

The Bypass Microsoft (Office 365) Services rule set is the default rule set for letting requests and responses in traffic to and from Office 365 and other Microsoft services bypass filtering on Web Gateway.

<table>
<thead>
<tr>
<th>Default rule set – Bypass Microsoft (Office 365) Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.

**Shortcut Microsoft service in response**

Cycle.Name equals "Response" AND User-Defined.Shortcut_Microsoft_Service equals true – Stop Cycle

The rule uses the Cycle.Name property to find out whether processing on Web Gateway is currently going on in the response cycle.

It also uses a user-defined property to check whether the response that is processed in this cycle was triggered by a client requesting access to Office 365 or any of several other Microsoft services.

If such a request is received on Web Gateway, a particular rule that is processed in the request cycle sets the user-defined property to true. The current rule checks whether the property is actually set this way in the response cycle, using the second part of its criteria.

If both criteria parts match, the rule applies and the response cycle is stopped. The response is then forwarded to the requesting client without filtering.

This rule is enabled by default.

All rules that follow the first rule in the rule set work in a similar way. They ensure that a request sent by a client of Web Gateway to a particular Microsoft service is forwarded to this service unfiltered.

Each of them also sets the property that is evaluated by the first rule to true after receiving such a request.

The first of these subsequent rules is explained here as an example in full detail. A summary is then given for all other rules.

**Bypass Exchange Online**

URL.Destination.IP is in range list Exchange Online IP Addresses OR URL.Destination.IP is in range list Exchange Online Protection P Addresses OR URL.Host matches in list Exchange Online URLs – Stop Cycle – Set User-Defined.Shortcut_Microsoft_Service = true

The rule uses the URL.Destination.IP and URL.Host properties to find out whether the IP address and URL that are sent with a request are on particular lists.

If they are, the request cycle is stopped and the request is forwarded to the requested destination, which is the Microsoft Exchange Online service.

The User-Defined.Shortcut_Microsoft_Service property is then set to true by an event. The property is evaluated in the response cycle by the first rule in the rule set.

This rule is not enabled by default.

**Bypass Microsoft Federation Gateway, Bypass Microsoft Lync/Skype for Business Online, and other rules for Microsoft services bypassing**

Similar to the Bypass Exchange Online rule, these rules use the URL.Destination.IP property or the URL.Host property or both (in one case also the URL property) to find out whether the IP addresses or URLs that are sent with requests are on particular lists. The lists vary with each rule depending on the respective service.
If the IP addresses or URLs are found on the lists, the request cycle is stopped and the request is forwarded to the requested destination, which is one of the Microsoft services. The User-Defined.Shortcut.Microsoft.Service property is then set to true by an event. The property is evaluated in the response cycle by the first rule in the rule set.

None of these rules is enabled by default.

---

**Reverse HTTPS proxy**

A reverse HTTPS proxy configuration can prevent clients from uploading unwanted data, such as malware or particular media types, to web servers under the HTTPS protocol.

In this configuration, HTTPS traffic is redirected to an appliance that a proxy is run on. It is inspected and eventually forwarded or blocked, according to the rules implemented on the appliance.

You can configure this in the following ways:

- Set up a transparent bridge or router.
- Set up a DNS configuration that points directly to the appliance when access to a particular web server is requested.

Redirection to an appliance can also be achieved by configuring proxy-aware connections that rely on the use of CONNECT headers.

However, this method would require an additional network device to assemble these headers for incoming requests. It is therefore not recommended.

In addition to configuring your network, you need to configure the handling of SSL certificates.

Optionally, you can configure additional settings that are not SSL-related to ensure a smooth operation of the reverse HTTPS proxy.

**Redirect HTTPS traffic in transparent bridge or router mode**

In transparent bridge or router mode, you can use a port redirect rule (also known as port forwarding rule) to direct HTTPS traffic to the proxy port on an appliance.

You also need to ensure that the redirected requests are treated as SSL-secured communication.

**Task**

1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to redirect traffic to and click Proxies (HTTP(S), FTP, ICAP, and IM).
3. In the Network Setup section, select Transparent bridge (or Transparent router).
   The section with the specific transparent bridge (or router) settings appears.
4. Under Port redirects, click Add.
   The Add Port Redirects window opens.
5. Configure the following settings for a new port redirect rule:
   - **Protocol name** — HTTP
     
     * This setting covers connections under both the HTTP and HTTPS protocols.*
• Original destination ports — 443
  If the web servers that are the destinations for requests can be reached under the HTTP protocol as well, you can add port 80 here (separated by a comma). This type of traffic is then also directed to the appliance.

• Destination proxy port — 9090
  This is the default proxy port on an appliance.

6 Click OK.

The window closes and the new rule appears on the list.

7 Under HTTP proxy port, make sure Enable HTTP proxy is selected and click Add.

The Add HTTP Proxy Port window opens.

8 Make sure the following is configured:
  • Serve transparent SSL connections — Selected
  • Ports treated as SSL — 443

9 Leave the other settings at their default values and click OK.

The window closes and the new HTTP proxy port appears on the list.

10 Click Save Changes.

Let the appliance listen to requests redirected by DNS entries
When requests under the HTTPS protocol are redirected to an appliance according to DNS entries, you can configure the proxy on the appliance to listen directly on the appropriate port. You also need to ensure that only SSL-secured connections are served.

Before you begin
If you want to configure the proxy in this way, make sure of the following:

• The host names of the requested web servers are not resolved to the appliance when the appliance does a DNS lookup.

  You can achieve this by entering the IP addresses of the web servers into the /etc/hosts file on the appliance or by using an appropriately configured internal DNS server.

• A rule set that handles content inspection is implemented on the appliance and enabled.

  A suitable rule set is provided in the default rule set system as nested rule set of the SSL Scanner rule set.

When using DNS entries, a port redirect rule cannot be applied because the purpose of such a rule is forwarding requests for other destinations to the appliance. However, due to the DNS entries, the appliance is already the destination.

You also need to ensure that only SSL-secured connections are served.

Task
1 Select Configuration | Appliances.

2 On the appliances tree, select an appliance for listening to requests and click Proxies (HTTP(S), FTP, ICAP, and IM).
3 Under **HTTP proxy port**, make sure **Enable HTTP proxy** is selected and click **Add**.

The **Add HTTP Proxy Port** window opens.

4 Configure the following settings for a new HTTP proxy port:
  - **Listener address** — 0.0.0.0:443
    
    This setting lets the appliance listen to requests for any web servers, regardless of their IP addresses. You can also specify a particular IP address here and restrict the appliance to listening for requests to the server in question.
    
    If you are running several network interface cards on your appliance, you can specify IP addresses (separated by commas) for as many web servers as there are network interface cards.
  
  - **Serve transparent SSL connections** — Selected
  
  - **Ports treated as SSL** — *

5 Leave the other settings at their default values and click **OK**.

The window closes and the new proxy port appears on the list.

If a web server should also be accessible under the **HTTPS** protocol, you need to add another HTTP proxy port with listener address 0.0.0.0:80 or the address of a particular web server.

6 Click **Save Changes**.

**SSL certificates in a reverse HTTPS proxy configuration**

A reverse HTTPS proxy configuration is usually set up to protect a limited number of web servers against the upload of unwanted data by clients. You need to import SSL certificates for these servers and add them to the appliance configuration.

In a reverse HTTPS proxy configuration, the appliance communicates in SSL-secured mode with its clients. The SSL certificates that the appliance sends to the clients during the SSL handshake cannot be issued, however, by its SSL Scanner module. Therefore, the appliance uses the original certificates of the web servers that the clients request access to.

You can import these certificates when configuring the settings for the SSL Client Context without CA module.

The appliance uses several methods to find the appropriate certificates for sending to its clients.

**Choosing certificates for sending to the clients**

To find out which certificate should be sent to a client in a given situation, the appliance scans the list of imported certificates. On this list, certificates are mapped to the host names of the web servers they belong to. The appliance then sends the certificate that is mapped to the name of the host that a client requested access to.

In an explicit proxy setup, the host name would be transmitted and made known to the appliance in the header of the CONNECT request.
In a transparent setup, the appliance uses the following methods to detect the host names:

- If a client sends an SNI extension, the host name can be found in a way that is similar to detecting it in an explicit proxy configuration.
- If client requests are redirected to the appliance according to DNS entries, the host name is known by the IP address that you specified when configuring redirection. In this case, you also need to create a rule set with rules that set the URL.Host property to the appropriate value for every IP address the appliance has been configured to listen to. This is to let the appliance know where to forward a request to when it has been filtered and allowed.
- If the transparent setup does not use redirection by DNS entries, the appliance will send a handshake message to the web server that a client requested, extract the common name from the certificate it receives from the web server, and use this common name to detect the appropriate host name.
  
  This method requires that the appliance and the web server communicate in SSL-secured mode, too. You can configure a setting on the appliance to ensure this mode is used.

Create settings for SSL certificates in a reverse HTTPS proxy configuration

You can create settings for the SSL certificates that are used for web servers in a reverse HTTPS proxy configuration and import the certificates when configuring these settings.

**Task**

1. Select **Policies | Settings**.
2. On the settings tree, select **Enable SSL Client Context without CA**.
3. Click **Add** above the settings tree.
   
   The **Add Settings** window opens.
4. In the **Name** field, enter a name for the settings you want to add, for example, **Imported web server certificates**.
5. [Optional] In the **Comments** field, type a plain-text comment on the settings.
6. [Optional] Select the **Permissions** tab and configure who is allowed to access the settings.
7. In the **Define SSL Client Context (Without Certificate Authority)** section, configure the settings parameters.
   a. On the toolbar of the inline list **Select server certificate by host or IP**, click **Add**.
      
      The **Add Host to Certificate Mapping** window opens.
   b. Click **Import** and use the options of the **Import Server Certificate** window that opens to import an SSL certificate for a web server.
   c. Configure the other parameters in the **Add Host to Certificate Mapping** window as needed.
   d. Click **OK**.
      
      The window closes and a new entry for mapping an SSL certificate to the host name of a web server appears in the inline list.
   e. Repeat substeps a to d if you want to add more mapping entries to the inline list.
   f. **Select or deselect SSL-Scanner functionality applies only to client connection**, according to whether the connection to the web server should be SSL-secured or not.
      
      If you choose to let this connection be unsecured, you need to create a rule that changes the network protocol from HTTPS to HTTP.
Configure the other settings parameters for the SSL client context as needed.

Click OK.

The Add Settings window closes and the new settings appear on the settings tree.

8 Click OK.

The window closes and the new settings appear on the settings tree.

9 Click Save Changes.

You can use these settings in the rule for setting the client context that is provided in the SSL Scanner rule set of the default rule set system.

**Set the URL.Host property in a reverse HTTPS proxy configuration**

When client requests are redirected to the appliance by DNS entries in a reverse HTTPS proxy configuration, you need to set the IP address of a web server as values of the URL.Host property to let the appliance know where to forward requests to.

After filtering a request has led to the result that it is allowed, the appliance uses the URL.Host property that was submitted with the request to forward it to the requested web server.

When requests are redirected according to DNS entries, web servers are known to the appliance by their IP addresses. If the URL.Host property has the IP address of a web server as its value, the appliance forwards the request to the appropriate destination.

Setting the value of a URL.Host property to an IP address can be done by a rule. You need to create such a rule for each web server that the appliance should forward requests to.

These rules can be contained in a rule set of their own.

**Tasks**

- Create a rule set for setting the URL.Host property on page 139
  You can create a rule set with rules that set the IP address of a web server as the value of the URL.Host property.

- Create rules for setting the URL.Host property on page 140
  You can create rules that set the IP address of a web server as the value of the URL.Host property.

**Create a rule set for setting the URL.Host property**

You can create a rule set with rules that set the IP address of a web server as the value of the URL.Host property.

**Task**

1 Select Policy | Rule Sets.

2 On the rule sets tree, navigate to the position where you want to insert the rule set.

3 Above the tree, click Add and select Rule Set.

   The Add New Rule Set window opens.

4 Under Name, enter a suitable name for the new rule set, for example, Set value of URL.Host to IP address.

5 Make sure Enable is selected.

6 Under Applies to select Requests and IM.

7 Under Apply this rule set, select Always.
[Optional] Under Comment, type a plain-text comment on the rule set.

[Optional] Click the Permissions tab and configure who is allowed to access the rule set.

Click OK.

The window closes and the new rule set appears on the rule sets tree.

**Create rules for setting the URL.Host property**

You can create rules that set the IP address of a web server as the value of the URL.Host property.

**Task**


2. On the rule sets tree, select the rule set you have created for the new rules, for example, Set value of URL.Host to IP address.

3. Click Add Rule.

   The Add Rule window opens with the Name step selected.

4. In the Name field, type a name for a new rule, for example, Set value of URL.Host to 10.141.101.51.

5. Select Rule Criteria, then If the following criteria is matched, and click Add.

   The Add Criteria window opens.

6. Configure the rule criteria as follows:
   a. From the list of properties in the left column, select URL.Destination.IP.
   b. From the list of operators in the middle column, select equals.
   c. In the operand field under Compare with in the right column, type an IP address.

7. Click OK.

   The window closes and the new criteria appears under Rule Criteria.

8. Click Action, select Continue, and leave the default settings for this action.

9. Click Events, then Add, and from the drop-down menu that appears, select Set Property Value.

   The Add Set Property window opens.

10. Set a property as follows:
    a. Under Set this property, select URL.Host.
    b. Under To concatenation of these strings, click Add.
       
       The Please Enter a String window opens.
    c. In the Parameter value field, type the host name of the web server that has the IP address you are using in this rule.
    d. Click OK.

       The window closes and the host name appears in the Add Set Property window.

11. Click OK.

   The window closes and the event for setting the URL.Host property appears under Events.
Click Finish.

The Add Rule window closes and the new rule appears within the rule set that you have created for the value-setting rules.

Click Save Changes.

**Complete optional activities for a reverse HTTPS proxy configuration**

In addition to configuring the network setup and the SSL certificate handling, you can complete several other activities, which are optional, to ensure a smooth operation of the reverse HTTPS proxy.

- Deactivate proxy loop detection
- Restrict access to appliance ports
- Restrict access to web servers
- Address multiple web servers

**Tasks**

- **Deactivate proxy loop detection on page 141**
  An appliance can detect proxy loops by evaluating the Via header of a client request. We recommend that you deactivate this detection process in a reverse HTTPS proxy configuration.

- **Restrict access to appliance ports on page 142**
  In a reverse HTTPS proxy configuration, access should be restricted to the proxy ports of an appliance. You need to configure the user interface and file server settings accordingly.

- **Restrict access to web servers on page 142**
  A reverse HTTPS proxy configuration is usually implemented to protect a limited number of web servers against unwanted data uploads from clients. In this configuration, you should allow access to these servers only and block it for others.

- **Address multiple web servers on page 145**
  You can let an appliance forward consecutive requests to different web servers to achieve load balancing and ensure redundancy.

**Deactivate proxy loop detection**

An appliance can detect proxy loops by evaluating the Via header of a client request. We recommend that you deactivate this detection process in a reverse HTTPS proxy configuration.

**Task**

1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to deactivate proxy loop detection for and click Proxies (HTTP(S), FTP, ICAP, and IM).
3. In the Advanced Settings section, deselect HTTP(S): Inspect Via header to detect proxy loops.
4. Click Save Changes.
Restrict access to appliance ports
In a reverse HTTPS proxy configuration, access should be restricted to the proxy ports of an appliance. You need to configure the user interface and file server settings accordingly.

Task
1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to restrict port access for and click User Interface.
3. Under HTTP Connector Port, enter the appliance proxy port (default: 9090).
5. Under HTTP Connector Port, enter the appliance proxy port (default: 9090).
6. Click Save Changes.

Restrict access to web servers
A reverse HTTPS proxy configuration is usually implemented to protect a limited number of web servers against unwanted data uploads from clients. In this configuration, you should allow access to these servers only and block it for others.

After access to others servers has been requested and blocked, we also recommend that you let the appliance close these connections.

To restrict access:
- Create a list of the web servers you want to protect.
- Create a rule set for a blocking rule.
- Create a rule that blocks access to other web servers and closes connections to clients after blocking their requests.

Tasks
- Create a list of protected web servers on page 142
  You can create a list the web servers that you want to protect in a reverse HTTPS proxy configuration.
- Create a rule set for a blocking rule on page 143
  You can create a rule set for the rule that blocks access to web servers in a reverse HTTPS proxy configuration.
- Create a rule to block access to web servers on page 144
  You can create a rule for blocking access to web servers when these are not on the list of protected servers in a reverse HTTPS proxy configuration.

Create a list of protected web servers
You can create a list the web servers that you want to protect in a reverse HTTPS proxy configuration.

Task
1. Select Policy | Lists.
2. Above the lists tree, click Add.
   - The Add List window opens.
Configure the following settings for the list:

- **Name** — List name, for example, Protected web servers
- **[Optional] Comment** — A plain-text comment on the new list
- **Type** — Wildcard Expression

[Optional] Click the **Permissions** tab and configure who is allowed to access the list.

Click **OK**.

The window closes and the new list appears on the lists tree under Custom Lists | WildcardExpression.

To fill the list with entries, click **Add** above the settings pane.

The Add Wildcard Expression window opens.

To add multiple entries at once, click **Add Multiple**.

Enter one or more wildcard expressions matching the URLs for the web servers you want to protect. Separate multiple entries by commas.

Click **OK**.

The window closes and the new entries appear on the list.

Click **Save Changes**.

**Create a rule set for a blocking rule**

You can create a rule set for the rule that blocks access to web servers in a reverse HTTPS proxy configuration.

**Task**


2. On the rule sets tree, navigate to the position where you want to insert the rule set.

3. Above the tree, click **Add** and select **Rule Set**.

   The Add New Rule Set window opens.

4. Under **Name**, enter a name for the new rule set, for example, Block web servers in a reverse HTTPS proxy configuration.

5. Make sure **Enable** is selected.

6. Under **Applies to**, select Requests and IM.

7. Under **Apply this rule set**, select If the following criteria is matched. Then click **Add**.

   The Add Criteria window opens.

8. Configure the rule set criteria as follows:
   
   a. From the **Property** list, select URL.Protocol.
   
   b. From the **Operator** list, select equals.
   
   c. Under **Operand**, type https.
   
   d. [Optional] Under **Comment**, type a plain-text comment on the new rule set.
[Optional] Click the Permissions tab and configure who is allowed to access the rule set.

10 Click OK.

The window closes and the new rule set appears on the rule sets tree.

**Create a rule to block access to web servers**

You can create a rule for blocking access to web servers when these are not on the list of protected servers in a reverse HTTPS proxy configuration.

**Task**

1 Select Policy | Rule Sets.

2 On the rule sets tree, select the rule set you have created for the blocking rule, for example, Block web servers in a reverse HTTPS proxy configuration.

3 Click Add Rule.

   The Add Rule window opens with the Name step selected.

4 In the Name field, type a name for the rule, for example, Allow access only to protected web servers.

5 Select Rule Criteria, then If the following criteria is matched and click Add.

   The Add Criteria window opens.

6 Configure the rule criteria as follows:
   a From the list of properties in the left column, select URL.Host.
   b From the list of operators in the middle column, select matches in list.
   c From the list of operands in the right column, select the web server list you configured, for example, Protected web servers.

7 Click OK.

   The window closes and the new criteria appears under Rule Criteria.

8 Click Action, select Block and leave the default settings for this action.

9 Click Events, then Add and from the drop-down list that appears, select Event.

   The Add Event window opens.

10 Configure an event as follows:
   a From the Event list, select Enable Proxy Control.
   b From the Settings list, select Do not keep connection to client persistent.

11 Click OK.

   The window closes and the new event appears under Events.

12 Click Finish.

   The Add Rule window closes and the rule appears within the new rule set that you have created.

13 Click Save Changes.
**Address multiple web servers**

You can let an appliance forward consecutive requests to different web servers to achieve load balancing and ensure redundancy.

To implement this, you need to:

- Import the Next Hop Proxy rule set from the rule set library
- Create a list of next-hop proxies
- Create next-hop proxy settings
- Create a rule that uses the list and the settings to trigger the Enable Next Hop proxy event when a web server from the list of protected servers is requested.

The list also uses a list of protected servers. For this list, you can use the one that you created to restrict access to these servers.

**Tasks**

- *Create a list of next-hop proxies on page 145*
  
  You can create a list of the web servers that are addressed as next-hop proxies when a suitable rule triggers the Enable Next Hop Proxy event.

- *Create next-hop proxy settings on page 146*
  
  You can create next-hop proxy settings for the rule that triggers the Enable Next Hop Proxy event when a server from the list of protected web servers is requested.

- *Create a rule for the Enable Next Hop proxy event on page 146*
  
  You can create a rule that triggers the Enable Next Hop Proxy event when a server from the list of protected web servers is requested.

**Create a list of next-hop proxies**

You can create a list of the web servers that are addressed as next-hop proxies when a suitable rule triggers the Enable Next Hop Proxy event.

**Task**

1. Select Policy | Lists.

2. Above the lists tree, click Add.

   The Add List window opens.

3. Configure the following settings for the list:
   - **Name** — List name, for example, Protected web servers as next-hop proxies
   - [Optional] **Comment** — Plain-text comment on the new list
   - **Type** — NextHopProxy

4. [Optional] Click the Permissions tab and configure who is allowed to access the list.

5. Click OK.

   The window closes and the new list appears on the lists tree under Custom Lists | NextHopProxy.

6. To fill the list with entries, click Add above the settings pane.

   The Add Wildcard Expression window opens.

   To add multiple entries at once, click Add Multiple.
7 Enter one or more wildcard expressions matching URLs for the web servers you want to address. Separate multiple entries by commas.

8 Click OK.

The window closes and the new entries appear on the list.

9 Click Save Changes.

**Create next-hop proxy settings**
You can create next-hop proxy settings for the rule that triggers the Enable Next Hop Proxy event when a server from the list of protected web servers is requested.

**Task**
1 Select Policy | Settings.
2 On the settings tree, select Enable Next Hop Proxy and click Add.

The Add Settings window opens.

3 Configure the following settings parameters:
   • Name — Settings name, for example, Protected web servers
   • [Optional] Comment — A plain-text comment on the new settings

4 Under Next Hop Proxy Servers configure the following:
   a From the List of next hop proxy servers, select the next hop proxy list you created, for example, Protected web servers as next hop proxies.
   
   b Make sure Round Robin is selected.
   
   c Deselect Proxy style requests.

5 Click OK.

The window closes and the new settings appear on the settings tree.

6 Click Save Changes.

**Create a rule for the Enable Next Hop proxy event**
You can create a rule that triggers the Enable Next Hop Proxy event when a server from the list of protected web servers is requested.

**Task**
1 Select Policy | Rule Sets.
2 On the rule sets tree, select the Next Hop Proxy rule set.

The rules of this rule set appear on the settings pane.

3 Click Add Rule.

The Add Rule window opens with the Name step selected.

4 In the Name field, type a name for the rule, for example, Address protected web servers as next-hop proxies.

5 Select Rule Criteria, then If the following criteria is matched, and click Add.

The Add Criteria window opens.
Configure the rule criteria as follows:

a. From the list of properties in the left column, select **URL.Host**.

b. From the list of operators in the middle column, select **does not match in list**.

c. From the list of operands in the right column, select the web server list you configured to restrict access to these servers, for example, **Protected web servers**.

7. Click **OK**.

   The window closes and the new criteria appears under **Rule Criteria**.

8. Click **Action**, and leave the default **Continue**.

9. Click **Events**, then **Add** and from the drop-down list that appears, select **Event**.

   The **Add Event** window opens.

10. Configure an event as follows:

    a. From the **Event** list, select **Enable Next Hop Proxy**.

    b. From the **Settings** list, select the settings you configured for this rule, for example, **Protected web servers**.

11. Click **OK**.

    The window closes and the new event appears under **Events**.

12. Click **Finish**.

    The **Add Rule** window closes and the new rule appears within the **Next Hop Proxy** rule set.

13. Click **Save Changes**.

---

**Proxy auto-configuration**

One or more proxy auto-configuration (PAC) files can be made available on an appliance for web browsers on clients. The browsers can use them to find proxies for accessing particular web pages.

A proxy auto-configuration file usually has **.pac** as its file name extension. There can be several of them on an appliance, for example, a **proxy.pac** and a **webgateway.pac**.

Under the WPAD (Web Proxy Auto-Discovery) protocol, a proxy auto-configuration file must have **wpad.dat** as its file name. Therefore, it can exist on an appliance only once.

**Make a .pac file available**

You can make a .pac file available for proxy auto-configuration to a web browser on a client.

**Task**

1. Store the .pac file in the /opt/mwg/files folder on the appliance.

2. Start the browser and navigate to the network configuration settings.

3. In the **Connection** section, click **Settings**.
4 Select **Automatic proxy configuration URL**, then enter the path and file name for the .pac file.
   For example, enter:
   
   http://mwgappl.webwasher.com:4711/files/proxy.pac

   If you want the clients to use a dedicated port for downloading the file, you must first configure
   this port.

   If no dedicated port is used, clients are directed to the HTTP port for the user interface (the default
   port number is 4711).

5 Click **OK**.

**Create a rule for downloading a wpad.dat file**

To enable the download of a wpad.dat file by a web browser on a client, you need to configure a rule
that forwards the download request to the appropriate port on an appliance.

**Task**

1 On the user interface of the appliance, select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance you want to make the wpad.dat file available on and
   click **Port Forwarding**.

3 Under **Port Forwarding Rules**, click **Add**.
   
   The **Add AppliancePortForwarding** window opens.

4 Configure settings for a port forwarding rule as follows:
   
   • **Source Host** — 0.0.0.0
   
   • **Target Port** — 80
   
   • **Destination Host** — 127.0.0.1
   
   • **Destination Port** — <File download port>

   As <File download port>, enter the HTTP port for the user interface of the appliance (default: 4711) or a dedicated port that you have configured.

5 Click **OK**.
   
   The window closes and the rule appears in the list.

**Configure auto-detection of a wpad host**

You can let a web browser use auto-detection to find the appliance as the host where a wpad.dat file is stored.

**Task**

1 Start the web browser and go to the network configuration settings.

2 In the **Connection** section, click **Settings**.

3 Select **Auto-detect proxy settings for this network**.

4 Click **OK**.
Using the Helix proxy

The Helix proxy is a third-party proxy for handling real-time streaming data. It is initially not accessed from the user interface of the appliance, but from a command line interface, which is, for example, provided on your administration system.

After accessing the Helix proxy, you can administer it on its own user interface.

Configure use of the Helix proxy

You can configure the use of the Helix proxy from a command line interface.

**Task**

1. On the command line interface, enter an activation command for the Helix proxy.
   
   This command could, for example, look as follows:

   ```
   service helix-proxy activate
   ```

   You are asked to enter a user name and password for the initial administrator account.

2. Enter both.

   The Helix proxy is started.

   After the start, you can find configuration files for the proxy in the `/opt/helix-proxy` folder on the appliance and modify them manually as needed.

3. Connect to the user interface of the Helix proxy with the following command:
   
   ```
   http://<IP address of the Helix proxy>:21774/admin/index.html
   ```

   The user interface appears and displays a logon window.

4. Enter the user name and password from Step 2.

   After a successful logon, the user interface of the Helix proxy becomes accessible.

5. Use this interface for further configuration of the Helix proxy as needed.

6. Configure your real-player application to use the appliance as a proxy.
   
   This can be done, for example, in the following way:

   a. Start the real player.

   b. On its user interface, go to the proxy settings.

   c. In the appropriate input field, for example, the RTSP (Real-Time Streaming Protocol) field, enter the IP address of the appliance with 554 as the port number.
Proxies
Using the Helix proxy
Central Management

Central Management allows you to administer multiple appliances that you have set up within your network as nodes in a common configuration.

When administering a Central Management configuration, you are dealing mainly with:

- **Nodes** — An appliance can be set up as a node that is connected to other nodes and can send and receive data to and from them to perform updates, backups, downloads and other activities.

- **Node groups** — Nodes are assigned to different types of node groups that allow data transfer in different ways.

- **Scheduled jobs** — Data can be transferred according to different kinds of schedules that you can configure.

Update schedules can also be configured for the nodes in a Central Management configuration specifying the time when updates should be performed and when not.

**Contents**

- Central Management configuration
- Configure Central Management
- Add an appliance to a Central Management configuration
- Configure the Central Management settings
- Assign a node to node groups
- Best practices - Configuring node groups in a Central Management configuration
- Verify the synchronization of nodes
- Add a scheduled job
- Update the appliance software in a Central Management configuration
- Central Management settings
Central Management configuration

In a Central Management configuration, multiple appliances run as nodes and can be administered from any node according to what you have configured.

The nodes in a Central Management configuration are connected within your network as follows:

- Each node is connected to client systems of your network that direct their web traffic to it.
- Nodes are assigned to node groups.
  - Node groups allow common administration activities for the group members, for example, transferring data for updates from one node to another node or several other nodes.

When configuring appliances as nodes, you must make sure that they can connect to ("see") each other. The default port on an appliance that listens to messages from other appliances is 12346.

Using the *ping* command is a method to verify that appliances can connect. This method is, however, not applicable to all networks.

- There are different types of node groups that allow different kinds of data transfer between the group members.

A Central Management configuration of multiple Web Gateway appliances is sometimes referred to as a *cluster*.

However, it is a cluster in the sense of a High Availability cluster with fail-over functions only if you configure the Proxy HA (High Availability) mode for the proxy functions of the appliances that are involved.

The following diagram shows several appliances that run as nodes in a Central Management configuration.

![Central Management configuration diagram]

*Figure 5-1  Central Management configuration*
Types of node groups

The nodes of a Central Management configuration can be assigned to node groups.

Node groups have names and differ with regard to their types. There are the following types of node groups:

- **Runtime group** — A node that is a member of a runtime group can share runtime data with all other nodes in the group.
  
  Runtime data is data that is created at runtime on an appliance. For example, the amount of time that is left for a user at a given point in time when a quota restriction has been imposed on web usage is runtime data.
  
  A node can only be a member of one particular runtime group.

- **Update group** — A node that is a member of an update group can share updates with all other nodes in the group.
  
  A node can only be a member of one particular update group.

- **Network group** — A node that is a member of a network group can immediately connect to all other node in the group.
  
  A node can be a member of different network groups at the same time.
  
  When a node is a member of different node groups, for example, of groups A and B, it is possible to transfer data through that node from other nodes in group A that are not members of group B to nodes in group B that are not members of group A.

Scheduled jobs

You can schedule jobs on an appliance, such as creating a configuration backup or downloading files, for execution on a particular time and date or in regular intervals.

You can also configure the schedule on the user interface of the appliance you are currently working on and have the job executed on another node of the same Central Management configuration.

Configure Central Management

You can configure Central Management for multiple appliances within your network to administer them as nodes in a common configuration.

Complete the following high-level steps.

**Task**

1. Begin with configuring Central Management on the user interface of an appliance within your network and add at least one other appliance as a node in a common configuration.

   Appliances are not by default included as nodes in any Central Management configuration, so all relevant activities must be performed by the administrator.

   For all these activities, you work with the options on the **Appliances** tab of the **Configuration** top-level menu.

   To add a node to a configuration, you need to configure at least the following:

   - Host name or IP address of the appliance you want to add as a node
   - Membership of the node in a network node group
You can also configure the following settings for a node:

- IP addresses and ports that should be used for communication with other nodes
- Membership in runtime and update node groups
- Scheduled jobs
- Updates

Repeat these activities for any other appliance you want to add as a node to the configuration.

After initially setting up a Central Management configuration, perform more configuration activities as needed.

You can, for example, do the following:

- Review the settings for Central Management on any node of the configuration and modify them
  You can review and modify settings for any node on the user interface of any other node of the configuration.
- Add one or more new nodes to the configuration

Save your changes.

---

### Add an appliance to a Central Management configuration

You can add an appliance as a node to a Central Management configuration and assign it to a network group.

**Task**

1. On the user interface of an appliance, select **Configuration** | **Appliances**.
2. On the appliances toolbar, click **Add**.
   The **Add Appliance** window opens.
3. In the **Host name or IP** field, type the host name or the IP address of another appliance within your network.
4. From the **Network group** list, select a network group for the appliance.
5. Click **OK**.
   The window closes and the appliance appears on the appliances tree.
   It is now a node in a Central Management configuration with the appliance you have been working on to complete the addition.
Configure the Central Management settings
You can configure the Central Management settings to enable the administration of multiple appliances as nodes in a common configuration.

Task
1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to configure settings for and click Central Management.
   The Central Management settings appear on the settings pane.
3. Configure these settings as needed.
4. Click Save Changes.

Assign a node to node groups
You can assign an appliance that is a node in a Central Management configuration to node groups of a different types to allow different kinds of data transfer between nodes.

The procedure for assigning a node to a runtime or an update group is nearly the same.

The procedure for a network group is different because a node can be a member in more than one network group.

Tasks
- **Assign a node to a runtime group on page 155**
  You can assign a node to a runtime group by typing the group name in the appropriate input field.
- **Assign a node to an update group on page 156**
  You can assign a node to an update group by typing the group name in the appropriate input field.
- **Assign a node to network groups on page 156**
  You can assign a node to one or more network groups by entering the group name or names into the appropriate list.

Assign a node to a runtime group
You can assign a node to a runtime group by typing the group name in the appropriate input field.

Task
1. On the user interface of an appliance, select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to assign as a node to a runtime group and click Central Management.
Assign a node to node groups

You can assign a node to one or more network groups by entering the group name or names into the appropriate list.

Task
1. On the user interface of an appliance, select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to assign as a node to one or more network groups and click Central Management.
3. To assign the node to a network group other than the default all group, click the Add icon on the toolbar of the Group network inline list.
   - The default group is provided to give you the option of not using different network groups, but having only one network group for all nodes.
   - If you want to have more than one network group, you should delete the all group or rename it.
   - The Add String window opens.
4 Configure a new network group.
   a In the **Name** field, type a name for the network group.
   b [Optional] In the **Comment** field, type a plain-text comment on the network group.
   c Click **OK**.

   The window closes and the new network group appears in the **Group network** inline list.

   The node is now a member of this network group.

You can also add multiple network groups at once by clicking the **Add multiple** icon and working with the **Add Strings** window that opens.

5 To include another node in the same network group or groups, select this node on the appliances tree, click **Central Management** again, and enter the same group name or names in the **Group network** inline list.

   Repeat this procedure for every node you want to include in the same network group or groups.

6 Click **Save Changes**.

---

**Best practices - Configuring node groups in a Central Management configuration**

In a Central Management configuration, nodes are assigned to node groups, which enables different ways of communication between the nodes. Node groups can also include nodes that are installed in different physical locations.

Before you begin to configure these groups, make sure the following applies:

- Appropriate routes are configured in your network to allow communication between nodes.

   If nodes in different locations are protected by firewalls, they must allow use of the port that is configured on each node for communication with other nodes (default port: 12346).

- Time is synchronized. Node communication depends on this when it is determined which node has the most up-to-date configuration.

   We highly recommend that you configure the use of an NTP server on each node for automatic synchronization. This is done as part of configuring the **Date and Time** settings of the **Configuration** top-level menu.

   If you are not using an NTP server for your network, you can configure the default server that is provided by McAfee at [ntp.webwasher.com](http://ntp.webwasher.com).

- The same version and build of Web Gateway is running on all appliances that are configured as nodes.

**Small sample configuration**

In this sample configuration, there are two different locations (Tokyo and New York) with two nodes each. In both locations, the nodes are assigned to their own runtime, update, and network groups. The group names are **tokyo** and **newyork**, respectively, for all types of groups.
One node in each location is also assigned to the transit network group, which is the same for both locations.

The following diagram shows this configuration.

![Diagram showing node groups](image)

This way, the following is achieved:

- Policy changes that an administrator configures on any node are distributed to all other nodes, due to the existence of a transit group node in each location. This ensures the web security policy remains the same on all nodes.

  The changes are transferred, for example, from the non-transit node in New York to the transit node because both are in one network group. They are then transferred from this transit node to the node in Tokyo, again, because both are in one network group, the transit group.

  Finally, the changes are transferred from the Tokyo transit node to the other node in this location.

- Updates of anti-malware and URL filtering information for the respective modules (engines) of Web Gateway are only distributed between nodes in Tokyo and between nodes in New York.

  This allows you to account for differences in the network structure of locations, which is advisable regarding the download of potentially large update files.

  Nodes in one location with, for example, fast connections and LAN links can share these updates, while they are not distributed between these nodes and those in other locations with, for example, slower connections and WAN links.

  We generally recommend that you include only nodes of one location in the same update group.

- Runtime data, for example, the quota time consumed by users, is only distributed between nodes in Tokyo and between nodes in New York.

  This makes sense, as probably users in one location will only be directed to the local nodes when requesting web access. So it would not be required for a node in New York to be informed about, for example, the remaining quota time of a user in Tokyo.

  If the nodes in one location are assigned to different user groups with regard to their web access, you can also configure these nodes in different runtime groups to avoid an information overhead on any node.

### Larger sample configuration

Not more than 10 nodes should be configured for a network group together with a transit node. This means that in larger locations, you need to configure more than one node for the transit network group.
In the following sample configuration, there are 22 nodes in one location (Tokyo), which are split into two network groups (toknet1 and toknet2), both of which include one node that is also a member of the transit group.

The 18 nodes in the second location (New York) are configured in the same way, whereas the 9 nodes in the third location (Paderborn) are all in one network group with one node that is also in the transit group.

The following diagram shows this configuration.

Regarding runtime and update node groups, there is one of each type for every location.

Policy changes, updates of anti-malware and URL filtering information, as well as sharing of runtime data are handled in the same way as for the smaller sample configuration.

Verify the synchronization of nodes

The user interface displays, among other general information, a timestamp for each node in a Central Management Configuration, which allows you to verify whether all nodes are synchronized.

Task

1. Select Configuration | Appliances.

2. On the appliances tree, select Appliances (Cluster).

   Status and general information about the configuration and its nodes appears on the settings pane.

   Under Appliances Information, a list is shown that contains a line with information for every node. The timestamp is the last item in each line.

3. Compare the timestamps for all nodes.

   If they are the same for all nodes, the Central Management configuration is synchronized.
Add a scheduled job

You can add a scheduled job to a list of jobs to let them be executed according to a time schedule that you configure.

**Task**

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to add a scheduled job on and click Central Management.

3. On the settings pane, expand the Advanced Scheduled Jobs section.

   The list of scheduled jobs list appears.

4. On the toolbar above the list, click Add.

   The Add Scheduled Job window opens.

5. Configure settings for the scheduled job.

6. Click OK.

   The window closes and the new scheduled job appears on the job list.

7. Click Save Changes.

Update the appliance software in a Central Management configuration

To update the appliance software on the nodes of a Central Management configuration, you can perform the update procedure from the user interface of one of the nodes, which is itself the last to be updated.

**Before you begin**

Make sure you have created a backup of the current configuration.

**Task**

1. Install a repository with the product version you want to update to on each appliance that is a node in the configuration.
   
   a. Log on to an appliance from a system console using SSH.

   b. Run the following command:

   ```
   yum install yumconf-<version number>-mwg
   ```

   *yumconf-<version number>-mwg* is the repository name. The digits of the version number must be separated by dots.

2. Log on to the user interface of one appliance in the configuration.

3. Select Configuration | Appliances.

   On the appliances tree, select an appliance other than the one you have logged on to.
4 Update each appliance on the appliances tree, except the appliance you are working from.
   a On the appliances tree, select an appliance.
   b On the toolbar above the settings pane, click Update appliance software.

5 When all other appliances that are nodes in the configuration are running their updates, perform
   the update for the appliance you are working from.
   a Select the appliance on the appliances tree.
   b Click Update appliance software.

   If the nodes in a configuration are assigned to different network groups, with some nodes
   being members of more than one group, we recommend that you:
   • Perform the update procedure from one of the nodes with multiple membership.
   • Update any other node with multiple membership at the end of the procedure.
   • Update the node you are working from last.

   For example, you have network group A with nodes 1, 2, 3, 4 and network group B with
   nodes 3, 4, 5, 6. Then choose node 3 or 4 to perform the update procedure from. Update
   nodes 1, 2, 5, 6 first, then 4 (if you have chosen 3 to perform the procedure from), and
   finally 3.

   The appliance software is now updated.

Central Management settings
The Central Management settings are used for configuring appliances that you administer as nodes in
a common configuration.

Central Management Settings
Settings for basic communication parameters of a node in a Central Management configuration

Table 5-1 Central Management Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP addresses and ports of this node for</td>
<td>Provides a list for entering the IP addresses and port numbers that a node uses to communicate with other nodes in a Central Management configuration.</td>
</tr>
<tr>
<td>Central Management communication</td>
<td></td>
</tr>
<tr>
<td>Timeout for distributing messages to other</td>
<td>Limits the time (in seconds) that is allowed for another node to respond to a message from the current node to the specified value.</td>
</tr>
<tr>
<td>nodes</td>
<td>The time can range from 10 to 600 seconds.</td>
</tr>
<tr>
<td></td>
<td>It is set on a slider scale.</td>
</tr>
</tbody>
</table>

The following table describes the elements of an entry in the IP addresses and ports list.

Table 5-2 IP addresses and ports – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Specifies the IP address and port number for a node.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on an IP address and a port number.</td>
</tr>
</tbody>
</table>
### Advanced Management Settings

Settings for advanced administration of a Central Management configuration

#### Table 5-3  Advanced Management Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Multiplier for timeout when distributing over multiple nodes** | Sets a factor for increasing the time interval that has been configured under Timeout for distributing messages to other nodes in the Central Management Settings section.  
Increasing the time interval gives messages more time to proceed from one node to another, from there to the next node, and so on.  
The interval can be increased by a value between 1 and 2.  
The value is set on a slider scale. |
| **Node priority**                         | Sets the priority that a node takes within a node group  
The highest priority is 1.  
If the configuration data on a node is no longer synchronized with that of other nodes, for example, because the node has been down for some time, the node receives the most recent configuration data from the node with the highest priority.  
If this is not your intention, make sure that all nodes have the same priority, which is also the recommended setting.  
The priority of a node can range from 1 to 100.  
It is set on a slider scale. |
| **Allow a GUI server to attach to this node** | When selected, a server providing an additional user interface for the appliance is allowed to connect to the node. |
| **Allow to attach a GUI server from non-local host** | When selected, a server with an additional user interface that is not running on the current node is allowed to connect to the node. |
| **GUI control address**                   | Specifies the IP address and port number the additional user interface uses for connecting to the current node. |
| **GUI request address**                   | Specifies the IP address and port number of this server used when sending requests to it. |
| **Contact other nodes unencrypted**       | When selected, messages sent from this node to other nodes in the configuration are not encrypted.  
However, authentication using certificates is still performed. |
| **Enable IP checking for other nodes**    | When selected, the IP address can be verified when messages are sent from this node to other nodes in the configuration.  
This function is intended to increase web security, but can lead to problems for some network setups, for example, NAT setups. |
Table 5-3  Advanced Management Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed time difference</td>
<td>Limits the time difference (in seconds) allowed for accepting configuration changes to the specified value. The number of seconds can range from 10 to 600. It is set on a slider scale.</td>
</tr>
<tr>
<td>Enable version checking for other nodes</td>
<td>When selected, the version of the appliance software is checked before configuration changes are distributed between nodes. Configuration changes are not distributed to a node if the version of the appliance software on this node does not match the version on the node that distributes the changes.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Level of version check</strong> – Sets a level of thoroughness when verifying the version of the appliance software. The level is set on a slider scale. It can take the following values:</td>
</tr>
<tr>
<td></td>
<td>- 1 – Only major version number (7 in 7.3.0) must match.</td>
</tr>
<tr>
<td></td>
<td>- 2 – Minor version number (3 in 7.3.0) must also match.</td>
</tr>
<tr>
<td></td>
<td>- 3 – Feature version number (0 in 7.3.0) must also match.</td>
</tr>
<tr>
<td></td>
<td>- 4 – Maintenance version number (if any, for example, 1 in 7.3.0.1.2) must also match.</td>
</tr>
<tr>
<td></td>
<td>- 5 – Hotfix version number (if any, for example, 2 in 7.3.0.1.2) must also match.</td>
</tr>
<tr>
<td></td>
<td>- 6 – Build number (for example, 14379) must also match.</td>
</tr>
</tbody>
</table>

This Node is a Member of the Following Groups

Settings for including a node in a group of nodes

Table 5-4  This Node is a Member of the Following Groups

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group runtime</td>
<td>Determines the group of a node, in which runtime data can be shared with all nodes in the group, for example, time quotas.</td>
</tr>
<tr>
<td>Group update</td>
<td>Determines the group of a node, in which updates can be shared with all nodes in the group</td>
</tr>
</tbody>
</table>
| Group network| Determines the group of a node, in which the node can immediately connect to all other nodes in the group

A node can be a member of more than one network group.

In this case, the nodes of a group that a node is a member of can connect through this node to nodes of another group that this node is also a member of.

All groups that a node is a member of are listed in the Group network list.

The following table describes the elements of a list entry in the group network list.

Table 5-5  Group network – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Specifies the name of a network node group.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a network node group.</td>
</tr>
</tbody>
</table>
Automatic Engine Updates

Settings for scheduling automatic updates of database information for modules used in the filtering process.

Table 5-6  Automatic Engine Updates

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable automatic updates</td>
<td>When selected, database information is automatically updated.</td>
</tr>
<tr>
<td>Allow to download updates from the internet</td>
<td>When selected, database updates are downloaded from the internet.</td>
</tr>
<tr>
<td>Allow to download updates from other nodes</td>
<td>When selected, database updates are downloaded from other nodes in a Central Management configuration.</td>
</tr>
</tbody>
</table>
| Update interval                 | Limits the time (in minutes) that elapses before database information is again updated to the specified value.  
                                    The time is set on a slider scale. 
                                    Allowed values range from 15 to 360. |
| CRL update interval             | Limits the time (in hours) that elapses before certificate revocation lists used in filtering SSL-secured web traffic are updated to the specified value.  
                                    This update uses a method that differs from those of other updates and must therefore be configured separately. 
                                    The time is set on a slider scale 
                                    Allowed values range from 3 to 168. |
| Enable update proxies           | When selected, proxy servers are used for routing updated database information. |
| Update proxies (fail over)      | Provides a list for entering the proxy servers that are used for routing updated database information.  
                                    The proxy servers are used in failover mode. The first server on the list is tried first and only if the configured timeout has elapsed is the next server tried. |

The following table describes the elements of an entry in the Update proxies list.

Table 5-7  Update proxies – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Specifies the host name or IP address of a server that is used as a proxy for routing updates.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port on a proxy that listens for update requests.</td>
</tr>
<tr>
<td>User</td>
<td>Specifies the user name of a user who is authorized to access a proxy for routing updates.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets a password for this user.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a proxy.</td>
</tr>
</tbody>
</table>

Advanced Update Settings

Settings for advanced update functions.
**Table 5-8  Advanced Update Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow to upload updates to other nodes</td>
<td>When selected, updated database information can be uploaded from the appliance (as a a node in a Central Management configuration) to other nodes.</td>
</tr>
<tr>
<td>The first time an update starts, it should wait an appropriate time before starting</td>
<td>Limits the time (in seconds) that elapses before an update is started to the specified value. Allowed values range from 5 to 1200.</td>
</tr>
<tr>
<td>The first time an automatic update starts, it uses the startup interval to update</td>
<td>Limits the time (in seconds) that elapses between attempts to start an automatic update for the first time to the specified value. During an update, the coordinator subsystem, which stores updated information on the appliance, tries to connect to the appliance core, where the modules reside that use this information. A low value for this interval can therefore speed up updates because it reduces the time the coordinator might have to wait until the core is ready to receive data. Allowed values range from 5 to 600.</td>
</tr>
<tr>
<td>Try to update with start interval</td>
<td>Limits the number of attempts (1 to 9) the appliance makes when trying to start an update to the specified value.</td>
</tr>
<tr>
<td>Use alternative URL</td>
<td>Specified the URL of an update server that is used instead of the default server.</td>
</tr>
<tr>
<td>Verify SSL tunnel</td>
<td>When selected, a certificate sent to a node by an update server in SSL-secured communication is verified.</td>
</tr>
<tr>
<td>Enter a special custom parameter sequence for an update server</td>
<td>Updates of URL filtering information are taken from the URL filter database server that is specified by the URL entered here.</td>
</tr>
<tr>
<td>No updates should be made in defined time window</td>
<td>Provides a list for entering daily time slots during which no updates of database information should be made.</td>
</tr>
</tbody>
</table>

The following table describes the elements of an entry in the time slot list.

**Table 5-9  Time slot – List entry**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start of time slot (hour)</td>
<td>Sets the hour when a daily time slot begins.</td>
</tr>
<tr>
<td>Start of time slot (minute)</td>
<td>Sets the minute in an hour when a daily time slot begins.</td>
</tr>
<tr>
<td>Start of time slot (second)</td>
<td>Sets the second in a minute when a daily time slot begins.</td>
</tr>
<tr>
<td>End of time slot (hour)</td>
<td>Sets the hour when a daily time slot ends.</td>
</tr>
<tr>
<td>End of time slot (minute)</td>
<td>Sets the minute in an hour when a daily time slot ends.</td>
</tr>
<tr>
<td>End of time slot (second)</td>
<td>Sets the second in a minute when a daily time slot ends.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a time slot.</td>
</tr>
</tbody>
</table>

**Advanced Subscribed Lists Settings**

Settings for advanced subscribed lists functions
Table 5-10  Advanced Subscribed Lists Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Allow to download customer subscribed lists | When selected, customer subscribed lists can be downloaded from the current appliance.  
  If the appliance is a node in a Central Management configuration and this option is also selected on other nodes, one of the nodes will download the lists.  
  If you want a particular node to download the lists, you need to make sure the option is deselected on every other node.  
  When a node is restarted and one or more subscribed lists are configured on this node, list content is downloaded to ensure a valid configuration.  
  The download is performed regardless of whether this download option is selected or not.  
  When a node is added to a configuration with other nodes that have subscribed lists configured, list content is downloaded for these lists onto the new node.  
  To reduce internal traffic, the download is performed without prior communication with other nodes.  
  The download is performed regardless of whether this download option is selected or not. |

Manual Engine Updates

Setting for performing manual updates of database information for modules used in the filtering process

Table 5-11  Manual Engine Updates

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Manual Engine Update | Updates database information for modules used in the filtering process immediately.  
  Database information is only updated for the modules on the appliance you are currently working on. |

Handle Stored Configuration Files

Settings for storing configuration file folders on disk
Table 5-12 Handle Stored Configuration Files

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep saved configuration folders for a minimal time</td>
<td>Limits the time (in days) that configuration file folders are at least stored on disk to the specified value. The number of days can range from 1 to 100.</td>
</tr>
<tr>
<td>Keep minimal number of configuration folders</td>
<td>Limits the number of configuration file folders that are at least stored on disk at any time to the specified value. The number can range from 1 to 100.</td>
</tr>
<tr>
<td>Keep minimal number of packed folders</td>
<td>Limits the number of packed configuration file folders that are at least stored on disk at any time to the specified value. Configuration folders are packed when the minimal time configured for storing them on disk has elapsed and the minimal number of folders stored on disk at any time would be exceeded if they were stored unpacked any longer. The number of folders can range from 1 to 100.</td>
</tr>
</tbody>
</table>

Advanced Scheduled Jobs
Settings for scheduled jobs

Table 5-13 Advanced Scheduled Jobs

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job list</td>
<td>Provides a list of scheduled jobs.</td>
</tr>
</tbody>
</table>

The following table describes the elements of a list entry.

Table 5-14 Job list entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start job</td>
<td>Specifies the time setting for starting a scheduled job, for example, hourly, daily, once.</td>
</tr>
<tr>
<td>Start job immediately if it was not started at its original schedule</td>
<td>Lets a scheduled job start immediately if this has not happened according to the originally configured schedule.</td>
</tr>
<tr>
<td>Job</td>
<td>Specifies the type of job, for example, Backup Configuration.</td>
</tr>
<tr>
<td>Unique job ID</td>
<td>Identifies a scheduled job.</td>
</tr>
<tr>
<td>When this job has finished run job with ID</td>
<td>Provides the ID of a job that is run immediately after this job.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a scheduled job.</td>
</tr>
</tbody>
</table>

Add Scheduled Job window
Settings in the window for adding a scheduled job

- **Time Settings** — Settings for the time when a scheduled job is started
- **Job Settings** — Settings for the type and ID of a scheduled job
- **Parameter Settings** — Settings for additional parameters of a scheduled job
These settings differ for each job type as follows:

- (Backup configuration settings) — Settings for a scheduled job that creates a backup of an appliance configuration
- (Restore backup settings) — Settings for a scheduled job that restores a backup of an appliance configuration
- (Upload file settings) — Settings for a scheduled job that uploads a file to an external server using the HTTP or HTTPS protocol
- (Download file settings) — Settings for a scheduled job that downloads a file to the appliance using the HTTP or HTTPS protocol

For a scheduled job that performs a yum update, there are no additional parameter settings.

### Table 5-15 Time Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start job</strong></td>
<td>Lets you select a time setting.</td>
</tr>
<tr>
<td>• Hourly — Starts a scheduled job every hour</td>
<td></td>
</tr>
<tr>
<td>• Daily — Starts a scheduled job once on a day</td>
<td></td>
</tr>
<tr>
<td>• Weekly — Starts a scheduled job once in a week</td>
<td></td>
</tr>
<tr>
<td>• Monthly — Starts a scheduled job once in a month</td>
<td></td>
</tr>
<tr>
<td>• Once — Starts a scheduled job only once</td>
<td></td>
</tr>
<tr>
<td>• Activated by other job — Starts a scheduled job after another job has been completed</td>
<td></td>
</tr>
<tr>
<td><strong>(Time parameter settings)</strong></td>
<td>Settings specifying the parameters for a time setting, for example, the minute in an hour when a job scheduled for hourly execution should be started</td>
</tr>
<tr>
<td></td>
<td>Which time parameter settings are shown depends on the selected time setting.</td>
</tr>
<tr>
<td></td>
<td>For example, if you have selected Hourly, you can configure the minute in an hour, but not the day in a month.</td>
</tr>
<tr>
<td></td>
<td>• Minute — Sets a minute in an hour</td>
</tr>
<tr>
<td></td>
<td>• Hour — Sets an hour on a day</td>
</tr>
<tr>
<td></td>
<td>• Day of month — Sets a day in a month</td>
</tr>
<tr>
<td></td>
<td>• Enter day of week — Provides a list for setting a day in a week</td>
</tr>
<tr>
<td></td>
<td>• Month — Sets a month in a year (specified by a number from 1 to 12)</td>
</tr>
<tr>
<td></td>
<td>• Year — Sets a year (four digits)</td>
</tr>
<tr>
<td><strong>Start job immediately if it was not started at its original schedule</strong></td>
<td>When selected, a scheduled job is started immediately if this has not happened according to the originally configured schedule.</td>
</tr>
<tr>
<td></td>
<td>This can be the case, for example, when an appliance is temporarily shut down due to overload and a job was scheduled to run during this downtime.</td>
</tr>
<tr>
<td></td>
<td>The job is then executed as soon as the appliance is up again.</td>
</tr>
</tbody>
</table>
Table 5-16 Job Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job</td>
<td>Lets you select the type of a scheduled job.</td>
</tr>
<tr>
<td></td>
<td>• Backup configuration — Creates a backup of an appliance configuration</td>
</tr>
<tr>
<td></td>
<td>• Restore backup — Restores a backup of an appliance configuration</td>
</tr>
<tr>
<td></td>
<td>• Upload file — Uploads a file to an external server using the HTTP or HTTPS protocol</td>
</tr>
<tr>
<td></td>
<td>• Download file — Downloads a file onto the appliance using the HTTP or HTTPS protocol</td>
</tr>
<tr>
<td></td>
<td>• Yum update — Performs a yum update on an appliance configuration</td>
</tr>
<tr>
<td></td>
<td>This scheduled job type is not available when an appliance runs in a FIPS-compliant mode</td>
</tr>
<tr>
<td>Unique job ID</td>
<td>Identifies a scheduled job.</td>
</tr>
<tr>
<td></td>
<td>The characters specified in this string are case-sensitive</td>
</tr>
<tr>
<td>Job description</td>
<td>Provides an optional description of a scheduled job in plain-text format.</td>
</tr>
<tr>
<td>When this job has</td>
<td>Provides the ID of a scheduled job that is to run immediately after the job configured here has</td>
</tr>
<tr>
<td>finished run job with ID</td>
<td>finished.</td>
</tr>
<tr>
<td></td>
<td>For this job, you must have configured the Activated by other job time setting.</td>
</tr>
<tr>
<td>Execute job on</td>
<td>Provides a list for selecting other nodes of the configuration to execute a scheduled job.</td>
</tr>
<tr>
<td>remote node</td>
<td>The list displays the host names for the other nodes.</td>
</tr>
<tr>
<td></td>
<td>The scheduled job that you configure on this appliance is executed with its time and parameter</td>
</tr>
<tr>
<td></td>
<td>settings on the selected node or nodes.</td>
</tr>
<tr>
<td></td>
<td>A message is sent to the other node or nodes to inform them about the scheduled job.</td>
</tr>
</tbody>
</table>

Table 5-17 Parameter Settings – Backup configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use most recent configuration</td>
<td>When selected, the scheduled job creates a backup from the most recent appliance configuration</td>
</tr>
<tr>
<td></td>
<td>Format:</td>
</tr>
<tr>
<td>Backup configuration path</td>
<td>Specifies the name of the path to the folder where the configuration is stored that should be used for the backup.</td>
</tr>
<tr>
<td></td>
<td>Format: /opt/mwg/storage/default/configfolder</td>
</tr>
<tr>
<td></td>
<td>This setting is only available when Use most recent configuration is deselected.</td>
</tr>
<tr>
<td>Save configuration to path</td>
<td>Specifies the path and file name for a backup configuration.</td>
</tr>
<tr>
<td></td>
<td>Format: /&lt;path name&gt;/&lt;file name with file name extension&gt;</td>
</tr>
<tr>
<td></td>
<td>You must set user rights for the folder you want to store the backup configuration in, making the appliance the owner who is allowed to write data into the folder.</td>
</tr>
<tr>
<td></td>
<td>On the command line provided, for example, by a serial console, run the appropriate commands to create a folder or change the rights for an existing folder.</td>
</tr>
</tbody>
</table>
### Table 5-18 Parameter Settings – Restore backup

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore backup from file</td>
<td>Specifies the path and file name for the file that should be used to restore a backup.</td>
</tr>
<tr>
<td></td>
<td>Format:</td>
</tr>
<tr>
<td>Only restore policy</td>
<td>When selected, a scheduled job backs up only settings related to the web security policy that was implemented on an appliance. Other settings, for example, settings needed for connecting an appliance to a network are not restored.</td>
</tr>
<tr>
<td>Lock storage during restore</td>
<td>When selected, no other files can be stored on the appliance until the scheduled job has completely restored the backup configuration.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets a password that is submitted for basic authentication.</td>
</tr>
<tr>
<td>Set</td>
<td>Opens the New Password window for setting a password. When a password has been set, the Set button is replaced by a Change button, which opens the New Password window for changing a password. This setting is only available when Enable basic authentication is selected.</td>
</tr>
</tbody>
</table>

### Table 5-19 Parameter Settings – Upload file

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>File to upload</td>
<td>Specifies the path and file name for a file that should be uploaded.</td>
</tr>
<tr>
<td></td>
<td>Format:</td>
</tr>
<tr>
<td>Destination to upload file to</td>
<td>Specifies the name of the path to the server that a file should be uploaded to under the HTTP or HTTPS protocol and the file name for storing the file on the server.</td>
</tr>
<tr>
<td></td>
<td>Format: http</td>
</tr>
<tr>
<td>Enable basic authentication</td>
<td>When selected, basic authentication is required for uploading a file.</td>
</tr>
<tr>
<td>User name</td>
<td>Specifies a user name that is submitted for basic authentication. This setting is only available when Enable basic authentication is selected.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets a password that is submitted for basic authentication.</td>
</tr>
<tr>
<td>Set</td>
<td>Opens the New Password window for setting a password. When a password has been set, the Set button is replaced by a Change button, which opens the New Password window for changing a password. This setting is only available when Enable basic authentication is selected.</td>
</tr>
</tbody>
</table>

### Table 5-20 Parameter Settings – Download file

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL to download</td>
<td>Specifies a URL for the location of a file that should be downloaded under the HTTP or HTTPS protocol and the name of the file.</td>
</tr>
<tr>
<td></td>
<td>Format: http</td>
</tr>
<tr>
<td>Save downloaded file to</td>
<td>Specifies a path to the location where a downloaded file should be stored and the file name for storing the file.</td>
</tr>
<tr>
<td></td>
<td>Format:</td>
</tr>
<tr>
<td>Enable basic authentication</td>
<td>When selected, basic authentication is required for downloading a file.</td>
</tr>
</tbody>
</table>
Table 5-20  Parameter Settings – Download file  (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specifies a user name submitted for basic authentication. This setting is only available when Enable basic authentication is selected.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets a password that is submitted for basic authentication.</td>
</tr>
<tr>
<td>Set</td>
<td>Opens the New Password window for setting a password. When a password has been set, the Set button is replaced by a Change button, which opens the New Password window for changing a password. This setting is only available when Enable basic authentication is selected.</td>
</tr>
</tbody>
</table>
Web filtering and authentication is controlled by rules, which you can implement and modify to let them suit the needs of your network.

Rules are grouped and made available in rule sets, each of which usually covers a particular field of filtering activities. There can be, for example, a virus and malware filtering rule set, a URL filtering rule set, an authentication rule set, and so on.

At the initial setup of the appliance, a default system of rule sets is implemented. You can review these rule sets and their rules, modify and delete them, and also create your own rules and rule sets or even a complete system of your own.

Additionally, you can import rule sets from libraries and modify them in the same way as the other rule sets.

Contents

- Rule flexibility
- About filtering
- Rule elements
- Rule representation in the documentation text
- Rule sets
- Rule set system
- Rule set library
- Rule Sets tab
- Create a rule
- Create a rule set
- Import a rule set
- Best practices - Rule configuration
- Restrict access to configuration items

**Rule flexibility**

When working with web security rules on Web Gateway, a considerable flexibility allows you to modify these rules in many ways, depending on what is best suited for your network.

The rules that are implemented as part of the default rule set system after the initial setup of Web Gateway can therefore be seen as a sample system. This system is meant to show you what a system of web security rules might look like. You are not required to keep this system or any part of it unmodified or to keep it at all.

Similarly, the rules in the rule sets of the rule set libraries are sample solutions for extending the web security functions of Web Gateway in one way or other. They are open to modification in the same way as the default rules.
The documentation explains the default and many library rules to let you understand how they work and what they can be used for.

But the documentation never says that you must necessarily implement a particular default rule set or import a particular library rule set. Nor does it say that you must handle a particular rule and its elements in the same way as it is explained in the documentation.

The specific needs of your network can always require that what you actually implement differs from a given explanation.

**About filtering**

A filtering process is performed on the appliance that uses the implemented rules to ensure web security for your network.

This process filters web traffic. It blocks some objects and lets others pass through, like a tea sieve or strainer that catches the tea leaves and allows the liquid to flow through its perforations.

How does the process tell the tea leaves from the liquid? The tea strainer obviously uses size as a key concept. If something is too big, it cannot pass through.

Similarly, the filtering process on the appliance uses in its rules all kinds of properties that web objects can have or that are related in some way to web objects to make filtering decisions.

**Properties of filtered objects**

A property of a web object checked in the filtering process is, for example, *being virus-infected*. A web object can have the property of being virus-infected, put more simply, it can be virus-infected.

Other examples could be the property of belonging into a particular URL category or the property of having a particular IP address.

The following can then be asked about these and other properties:

- For a given web object, what value does property \( p \) have?
- And: If this value is \( x \), what action is required?

Giving an answer to the second question leads to a rule:

*If the value of property \( p \) is \( x \), action \( y \) is required.*

A property is a key element in every rule on the appliance. Understanding the property is essential to understanding the rule.

When you are creating a rule, it is a good idea to begin by thinking about the property you want to use. Using a property of an already existing rule as an example, you might consider something like the following:

*I want to filter viruses and other malware. I use the property of being virus-infected and build a rule around it. I let this rule require a blocking action to be taken if a given web object has this property.*

The rule could look as follows:

*If being virus-infected has the value true (for a given web object), block access to this object.*

The web object could, for example, be a file that a web server has sent because a user of your network requested it and that is intercepted and filtered on the appliance.
Properties and rules are explained in this section using normal language. However, the format they have on the user interface of the appliance does not differ from this very much.

For example, the above rule about virus infections could appear on the user interface as follows:

\[\text{Antimalware.Infected equals true} \rightarrow \text{Block (Default)}\]

where \text{Antimalware.infected} is the property and \text{Block} is the action, which is executed in the default way.

The arrow does not appear on the user interface, it is inserted here to show that the blocking action is triggered if a given web object really has the property in question.

**Filtering users**

Properties can be related to web objects, but also to the users that request them.

For example, a rule could use the property \text{user groups that user is member of} to block requests sent by users who are not in an allowed group:

\[\text{If user groups that user is member of (for a given user) are not on the list of allowed groups, block requests sent by this user.}\]

**Filtering cycles**

The filtering process on the appliance has three cycles: the request cycle, the response cycle, and the embedded objects cycle. Only one of them can go on at a given moment.

The request cycle is performed for filtering requests that users of your network send to the web, the response cycle is for the responses received upon these requests from the web.

When embedded objects are sent with requests or responses, the embedded objects cycle is performed as an additional cycle of processing.

An embedded object could, for example, be a file sent with a request to upload a file and embedded in this file. The filtering process begins with the request cycle, filtering the request and checking the file that is requested for uploading. Then the embedded objects cycle is started for the embedded file.

Similarly, the response cycle and the embedded objects cycle are started one after another for a file that is sent in response from a web server and has another file embedded in it.

For every rule on the appliance, it is specified in which cycle it is processed. However, the cycle is not specified individually for a rule, but for the rule set that contains it.

A rule set can be processed in just one cycle or in a combination of cycles.

**Process flow**

In the filtering process, the implemented rules are processed one after another, according to the positions they take in their rule sets.

The rule sets themselves are processed in the order of the rule set system, which is shown on the Rule Sets tab of the user interface.

In each of the three cycles, the implemented rule sets are looked up one after another to see which must be processed in this cycle.

When a rule is processed and found to apply, it triggers an action. The action executes a filtering measure, such as blocking a request to access a web object or removing a requested object.
In addition to this, an action has an impact on the filtering process. It can specify that the filtering process must stop completely, or skip some rules and then continue, or simply continue with the next rule.

Processing also stops after all implemented rules have been processed.

Accordingly, the process flow can be as follows:

- **All rules have been processed for each of the configured cycles and no rule has been found to apply.**
  
  
  Processing stops.  
  
  In the request cycle, the request is allowed to pass through to the appropriate web server.  
  
  In the response cycle, the response sent from the web is forwarded to the appropriate user.  
  
  In the embedded objects cycle, the embedded object is allowed to pass through with the request or response it was sent with.  
  
  Processing begins again when the next request is received.

- **A rule applies and requires that processing must stop completely.**
  
  Processing stops.  
  
  An example of a rule that stops processing completely is a rule with a blocking action.  
  
  If, for example, a request is blocked because the requested URL is on a blocking list, it is no use to process anything else.  
  
  No response is going to be received because the request was blocked and not passed on to the appropriate web server. Filtering an embedded object that might have been sent with the request is also not needed because the request is blocked anyway.  
  
  A message is sent to the user who is affected by the action, for example, to inform this user that the request was blocked and why.  
  
  Processing begins again when the next request is received.

- **A rule applies and requires that processing must stop for the current rule set.**
  
  Processing stops for this rule set.  
  
  The rules that follow the stopping rule in the rule set are skipped.  
  
  An example of a rule that stops the processing of a rule set is a whitelisting rule followed by a blocking rule in the same rule set.  
  
  When a requested web object is found on a whitelist, the request is allowed to pass through without further filtering. Therefore the rule set is not processed any further and the rule that eventually blocks the object is skipped.  
  
  Processing continues with the next rule set.  
  
  The next rule set can contain rules that, for example, block a request, although it was allowed to pass through the preceding rule set.

- **A rule applies and requires that processing must stop for the current cycle.**
  
  Processing stops for this cycle.  
  
  The rules and rule sets that follow the stopping rule in the cycle are skipped.  
  
  An example of a rule that stops the processing of a cycle is a global whitelisting rule.  
  
  When a requested object is found on a global whitelist, the request is allowed to pass through to the appropriate web server. To ensure the request is not blocked eventually by any of the following rules and rule sets, the request cycle is not processed any further.  
  
  Processing continues with the next cycle.
A rule applies and requires that processing continues with the next rule.

Processing continues with the next rule.

This can be the next rule in the current rule set or the first rule in the next rule set or cycle.

An example of a rule that lets the filtering process continue unimpeded is a statistics rule.

This rule just counts requests by increasing a counter and does otherwise nothing.

## Rule elements

A web security rule on the appliance has three main elements: criteria, action, and (optionally) event.

1 **Criteria**

Determines whether a rule applies.

- **Property**
  - Is related to a web object or a user.
  
  *the category of a URL*

- **Operator**
  - Links the property to an operand.
  
  *is on list*

- **Operand**
  - Specifies a value that the property can have.
  
  *x (list name)*

2 **Action**

Is executed if the criteria is matched.

*block the URL*

3 **Event**

Is executed if the criteria is matched.

*and log this action*

An event is optional for a rule. A rule can also have more than one event.
Rule format on the user interface

On the user interface, a rule appears in the following format.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Allows you to enable or disable the rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the rule</td>
</tr>
<tr>
<td></td>
<td>• Block URLs ... — Name text</td>
</tr>
<tr>
<td></td>
<td>• Category BlockList (in rule name) — List used by the rule</td>
</tr>
<tr>
<td></td>
<td>- Clicking on the list name opens the list for editing.</td>
</tr>
<tr>
<td></td>
<td>• Yellow triangle (next to a list name) — Indicates that the list is initially empty and you need to fill the entries.</td>
</tr>
<tr>
<td>Criteria</td>
<td>Criteria of the rule</td>
</tr>
<tr>
<td></td>
<td>• The criteria is only visible after clicking the Show details toggle button.</td>
</tr>
<tr>
<td></td>
<td>• URL.Categories — Property</td>
</tr>
<tr>
<td></td>
<td>• &lt;Default&gt; — Settings of the module that retrieves a value for the property</td>
</tr>
<tr>
<td></td>
<td>- For example, the Default settings that appear here are settings of the URL Filter module.</td>
</tr>
<tr>
<td></td>
<td>- Clicking on the settings name opens the settings for editing.</td>
</tr>
<tr>
<td></td>
<td>The module name is not visible in the rule. It appears, however, in the Edit window for the rule criteria.</td>
</tr>
<tr>
<td></td>
<td>• at least one in list — Operator</td>
</tr>
<tr>
<td></td>
<td>• Category BlockList — Operand (also known as parameter)</td>
</tr>
<tr>
<td></td>
<td>- The list name appears both in the rule name and the criteria to let it be available when the criteria is not visible.</td>
</tr>
</tbody>
</table>

Figure 6-1  Format of a rule on the user interface

The following table explains the meaning of the rule elements.

Table 6-1  Elements of a rule on the user interface
Table 6-1  Elements of a rule on the user interface (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>Action of the rule</td>
</tr>
<tr>
<td>• <strong>Block</strong> — Name of the action</td>
<td></td>
</tr>
<tr>
<td>• <strong>&lt;URLBlocked&gt;</strong> — Settings of the action</td>
<td></td>
</tr>
<tr>
<td><strong>Events</strong></td>
<td>One or more events of the rule</td>
</tr>
<tr>
<td>• <strong>Statistics.Counter.Increment</strong> — Name of the event</td>
<td></td>
</tr>
<tr>
<td>• “BlockedByURLFilter, 1” — Parameters of the event</td>
<td></td>
</tr>
<tr>
<td>• <strong>&lt;Default&gt;</strong> — Settings of the event</td>
<td></td>
</tr>
</tbody>
</table>

Complex criteria

The criteria of a rule can be made complex by configuring it with two or more parts.

In complex criteria each of the parts has a property with operator and operand. The parts are linked by AND or OR.

The criteria is matched if a filtered URL belongs to a category that is on any of the two specified category lists (or on both).

If you configure criteria with three or more parts and use both AND and OR between them, you also need to put brackets to indicate how the parts are logically connected. For example, (a AND b) OR c differs in meaning from a AND (b OR c).

When you add a third criteria part on the user interface, lowercase letters appear before the parts and an additional field is inserted at the bottom of the configuration window.

The field displays your criteria parts in short, for example, a AND b OR c. You can then type brackets in the field as needed.

Rule representation in the documentation text

When rules are explained in the Web Gateway documentation, different ways of representing them within the documentation text are used.

A rule can be represented in a long or short format, providing more or less explicit information about the structure of a rule. The individual elements of a rule can be marked using different fonts to distinguish them from each other or all appear in the same font.

The long and the short formats can both be combined with different element markup to represent rules as follows:

• **Short rule representation** — A rule is represented in a short format with different fonts used for the individual rule elements.

• **Short unified rule representation** — A rule is represented in a short format with the same fonts used for all rule elements.
• **Long rule representation** — A rule is represented in a long format with different fonts used for the individual rule elements.

• **Long unified rule representation** — A rule is represented in a long format with the same fonts used for all rule elements.

All rule representations are followed by explanations of the respective rules in plain text.

**Rule representation on the user interface**

On the user interface of Web Gateway, a rule looks like this. The three main rule elements (criteria, action, and events) are each shown in a separate column. The rule name appears in bold above the rule criteria.

![Figure 6-2 Rule representation on the user interface](image)

In this sample representation, the rule name and elements are as follows:

- **Name** — Block if virus was found
- **Criteria** — Antimalware.Infected<Gateway Anti-Malware> equals true
- **Action** — Block<Virus Found>
- **Event** — Statistics.Counter.Increment("BlockedByAntiMalware",1)<Default>

The different representation methods used in the documentation text all rely in one way or other on how a rule is represented here.

**Short rule representation**

The short rule representation shows the main elements of a rule next to each other with the rule name in bold above the criteria. This representation method comes closest to the way that a rule is shown on the user interface.

To distinguish the main rule elements even further than it is done on the user interface, the criteria is shown in italics and the action is preceded by an arrow. The arrow symbolizes the relation between the criteria and the action (if the criteria matches, then the action is performed).

The rule event is always optional. It is also executed if the criteria matches, so it is just added after the action, separated by a dash.

**Block if virus was found**

Antimalware.Infected<Gateway Anti-Malware> equals true –> Block<Virus Found> – Statistics.Counter.Increment("BlockedByAntiMalware",1)<Default>

**Short unified rule representation**

The short *unified* rule representation differs from the short rule representation in that it does not use different fonts to distinguish the name from the rule elements and the rule elements from each other. It rather shows them all in narrow bold font.

**Block if virus was found**

Antimalware.Infected<Gateway Anti-Malware> equals true – Block<Virus Found> – Statistics.Counter.Increment("BlockedByAntiMalware",1)<Default>
Long rule representation

The long rule representation shows each rule element in a separate row within a table, preceded by the element name. The rule name appears in red above the table like a section title.

Block if virus was found

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Antimalware.Infected&lt;Gateway Anti-Malware&gt; equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;Virus Found&gt;</td>
</tr>
<tr>
<td>Event</td>
<td>Statistics.Counter.Increment (&quot;BlockedByAntiMalware&quot;,1)&lt;Default&gt;</td>
</tr>
</tbody>
</table>

Long unified rule representation

The long unified rule representation differs from the long rule representation in that all individual rule elements are marked in narrow bold font.

Block if virus was found

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Antimalware.Infected&lt;Gateway Anti-Malware&gt; equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;Virus Found&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>Statistics.Counter.Increment (&quot;BlockedByAntiMalware&quot;,1)&lt;Default&gt;</td>
</tr>
</tbody>
</table>

Rule sets

Rules are grouped and included in rule sets on the appliance. A rule can never stand on its own, it must be included in a rule set.

A rule set can include just a single rule or several of them. It can also include one or more nested rule sets. If it includes nested rule sets, it can include individual rules on the same level as the nested rule sets.

Rule sets usually include rules that work together to provide a particular function for ensuring web security.

For example, a virus and malware filtering rule set will include a rule that blocks infected rule sets and one or several others that whitelist objects to let them skip the blocking rule and ensure users can access them.

You can modify the implemented rule sets and create rule sets of your own to build functional units in whatever way is suitable for your network.

Rule set criteria

Like rules, rule sets have criteria and are applied if their criteria matches.

Usually, the criteria of a rule set differs from that of its rules. For a rule to apply, both its own criteria and the criteria of its rule set must match.

Rule set cycles

Rule sets are processed, with their rules, in the three cycles of the filtering process.
A rule set can be processed in any combinations of these cycles, for example, only in the request cycle or in both request and response cycles, and also in all three cycles.

The cycles of a rule set are at the same time those of the individual rules it includes. A rule cannot differ with regard to cycles from its rule set.

**Nested rule sets**

Rule sets can have other rule sets nested within them. A nested rule set has its own criteria.

Regarding cycles, it can only be processed in the cycles of the nesting rule set, but need not be processed in all of them.

This way, a nested rule set can be configured to deal especially with a particular cycle, while another nested rule set deals with a different cycle.

For example, a media type filtering rule set could apply to all cycles, but have nested rule sets that are not processed in all of them.

*Media Type Filtering* rule set (for requests, responses, and embedded objects)
- Nested rule set *Media Type Upload* (for requests)
- Nested rule set *Media Type Download* for responses and embedded objects

---

**Rule set system**

Rule sets are implemented on the appliance within a rule set system.

When a request for web access is received on the appliance, all rule sets in the system are processed for this request from top to bottom.

If a rule in a rule set is found to apply, the action of this rule is executed. If the action is **Block**, processing stops. Other actions let processing continue in one or the other way.

Similarly, the rule sets of the implemented system are processed for responses and embedded objects sent with requests and responses.

**Working with the rule set system**

During the initial setup of the appliance, a default system of rule sets is implemented. You can do the following to fine-tune this system and adapt it to the requirements of your network:

- Modify rules and rule sets
- Delete rules and rule sets
- Create rules and rule sets
- Import rule sets
- Move rules and rule sets to new positions
- Copy rules and paste them into other rule sets

**Default rule set system**

The default rule system looks like this (nested rule sets are not shown).
### Table 6-2 Default rule set system

<table>
<thead>
<tr>
<th>Rule set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bypass Microsoft (Office 365) Services</strong></td>
<td>Lets requests and responses that are sent to and received from Office 365 and other Microsoft services bypass filtering.</td>
</tr>
<tr>
<td><strong>(not enabled by default)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SSL Scanner</strong></td>
<td>Prepares SSL-secured web traffic for processing by other filtering functions.</td>
</tr>
<tr>
<td><strong>(not enabled by default)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Global Whitelist</strong></td>
<td>Lets requests for whitelisted URLs or IP addresses skip further filtering.</td>
</tr>
<tr>
<td><strong>Remove Privacy Violation Header</strong></td>
<td>Removes privacy violation headers from requests to prepare them for processing by other filtering functions.</td>
</tr>
<tr>
<td><strong>Common Rules</strong></td>
<td>Provides functions that support the filtering process, such as web caching, progress indication, and opening of archives.</td>
</tr>
<tr>
<td><strong>URL Filtering</strong></td>
<td>Controls filtering of individual URLs and URL categories.</td>
</tr>
<tr>
<td><strong>Media Type Filtering</strong></td>
<td>Controls filtering of particular types of media.</td>
</tr>
<tr>
<td><strong>Gateway AntiMalware</strong></td>
<td>Controls virus and malware filtering using virus signatures and proactive methods.</td>
</tr>
<tr>
<td><strong>Dynamic Content Classification</strong></td>
<td>Controls dynamic classification of content.</td>
</tr>
</tbody>
</table>

### Rule set library

The rule set library provides rule sets for you to import into your rule set system.

You can import a rule set, for example, to add a function that is missing in your system or when the implemented rule sets do not suit your network.

- The rule set library also contains the rule sets that are part of the default rule set system.
- More rule sets are available from an online rule set library. A link to this library is provided in the window of the standard rule set library.

In the standard rule set library, rule sets are grouped in categories, for example, authentication or URL filtering.

The following table shows the categories of the standard rule set library.

### Table 6-3 Categories of library rule sets

<table>
<thead>
<tr>
<th>Rule set category</th>
<th>Includes rule sets for ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Control</td>
<td>Filtering applications and individual functions of applications</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authenticating users</td>
</tr>
<tr>
<td>Coaching/Quota</td>
<td>Imposing quotas and other restrictions on the web access of users</td>
</tr>
<tr>
<td>Cloud Services</td>
<td>Implementing single sign-on access to cloud applications</td>
</tr>
<tr>
<td>Common Rules</td>
<td>Supporting the filtering process, for example, by web caching, progress indication, or opening of archives</td>
</tr>
<tr>
<td>DLP</td>
<td>Implementing data loss prevention</td>
</tr>
<tr>
<td>ePO</td>
<td>Enabling use of the ePolicy Orchestrator</td>
</tr>
<tr>
<td>Error Handling</td>
<td>Implementing error handling measures</td>
</tr>
<tr>
<td>Gateway Anti-Malware</td>
<td>Filtering web objects for infections by viruses and other malware</td>
</tr>
<tr>
<td>HTML/Script Filter</td>
<td>Filtering HTML pages and scripts</td>
</tr>
</tbody>
</table>
Table 6-3  Categories of library rule sets *(continued)*

<table>
<thead>
<tr>
<th>Rule set category</th>
<th>Includes rule sets for ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICAP Client</td>
<td>Running an ICAP client on an appliance</td>
</tr>
<tr>
<td>Logging</td>
<td>Logging filtering and other activities</td>
</tr>
<tr>
<td>Media Type Filter</td>
<td>Filtering particular types of media</td>
</tr>
<tr>
<td>Mobile Security</td>
<td>Filtering mobile traffic</td>
</tr>
<tr>
<td>Next Hop Proxy</td>
<td>Using next-hop proxies for data transfer</td>
</tr>
<tr>
<td>Privacy</td>
<td>Modifying requests to ensure privacy</td>
</tr>
<tr>
<td>SiteAdvisor Enterprise</td>
<td>Using the SiteAdvisor for filtering request</td>
</tr>
<tr>
<td>SSL Scanner</td>
<td>Handling SSL-secured web traffic</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Performing troubleshooting measures</td>
</tr>
<tr>
<td>URL Filter</td>
<td>Filtering individual URLs and URL categories</td>
</tr>
<tr>
<td>Web Hybrid</td>
<td>Enabling synchronization with the McAfee SaaS Web Protection Service</td>
</tr>
</tbody>
</table>

**Rule Sets tab**

Use the Rule Sets tab to work with rules and rule sets.

![Rule Sets tab](image)

**Figure 6-3  Rule Sets tab**

**Main elements of the Rule Sets tab**

The following table describes the main elements of the Rule Sets tab.

**Table 6-4  Main elements of the Rule Sets tab**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule sets toolbar</td>
<td>Items for working with the rule sets on the rule sets tree</td>
</tr>
<tr>
<td>Rule sets tree</td>
<td>Tree structure displaying the rule sets of the appliance configuration</td>
</tr>
</tbody>
</table>
Table 6-4  Main elements of the Rule Sets tab (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule sets menu</td>
<td>Buttons for displaying tree structures of:</td>
</tr>
<tr>
<td></td>
<td>• (General) rule sets</td>
</tr>
<tr>
<td></td>
<td>• Log handler rule sets</td>
</tr>
<tr>
<td></td>
<td>• Error handler rule sets</td>
</tr>
<tr>
<td></td>
<td>• User-defined properties (for use in rule set criteria, rule criteria, and rule events)</td>
</tr>
<tr>
<td>Rules toolbar</td>
<td>Items for working with rules</td>
</tr>
<tr>
<td>Rules</td>
<td>Rules of the currently selected rule set</td>
</tr>
</tbody>
</table>

Rule sets toolbar
The rule sets toolbar provides the following options.

Table 6-5  Rule sets toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Opens a menu or a window for adding an item, depending on what is currently selected from the Rule sets menu.</td>
</tr>
<tr>
<td></td>
<td>• (Rule Sets is selected) — Opens a menu, from which you can select:</td>
</tr>
<tr>
<td></td>
<td>• Rule Set from Library — Opens the Add from Rule Set Library window for importing a rule set from the rule set library.</td>
</tr>
<tr>
<td></td>
<td>• Rule Set — Opens the Add New Rule Set window to let you add a rule set to the appliance configuration.</td>
</tr>
<tr>
<td></td>
<td>• Top-Level Rule Set — Opens the Add New Top-Level Rule Set window for adding a rule set at the top level of the rule sets tree.</td>
</tr>
<tr>
<td></td>
<td>• (Log Handler is selected) — Lets you select Log Handler from a menu as the only accessible item to open the Add New Log Handler window for adding a new Log Handler rule set.</td>
</tr>
<tr>
<td></td>
<td>• (Error Handler is selected) — Lets you select Error Handler from a menu as the only accessible item to open the Add New Error Handler window for adding a new Error Handler rule set.</td>
</tr>
<tr>
<td></td>
<td>• (User-Defined Property is selected) — Lets you select User-Defined Property to open the Add New User-Defined Property window for adding a property.</td>
</tr>
<tr>
<td>Export</td>
<td>Opens the Export Rule Set window for exporting a rule set to the library or into a file.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the Edit Rule Set window for editing a selected rule set.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a selected rule set.</td>
</tr>
<tr>
<td></td>
<td>A window opens to let you confirm the deletion.</td>
</tr>
<tr>
<td>Move up</td>
<td>Moves a rule set up among other rules sets on the same level.</td>
</tr>
<tr>
<td>Move down</td>
<td>Moves a rule set down among other rule sets on the same level.</td>
</tr>
<tr>
<td>Move out of</td>
<td>Moves a rule out of its nesting rule set and onto the same level as the nesting rule set.</td>
</tr>
<tr>
<td>Move into</td>
<td>Moves a rule set out of its nesting rule set and into the rule set following this rule set.</td>
</tr>
<tr>
<td>Expand all</td>
<td>Expands all collapsed items on the rule sets tree.</td>
</tr>
<tr>
<td>Collapse all</td>
<td>Lets all expanded items on the rule sets tree collapse.</td>
</tr>
</tbody>
</table>

Rules toolbar
The rules toolbar provides the following options.
<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Opens the Add Rule window for adding a rule.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the Edit Rule window for editing a selected rule.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a selected rule. A window opens to let you confirm the deletion.</td>
</tr>
<tr>
<td>Move up</td>
<td>Moves a rule up within its rule set.</td>
</tr>
<tr>
<td>Move down</td>
<td>Moves a rule down within its rule set.</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies a selected rule.</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes a copied rule.</td>
</tr>
<tr>
<td>Show details</td>
<td>Shows (or hides) details of a rule entry including the criteria.</td>
</tr>
</tbody>
</table>

Create a rule

Creating a rule includes several activities that are related to the different elements of a rule. The Add Rule window is provided for creating a rule. It allows you to complete the activities for configuring the rule elements in the order that you prefer.

You can, for example, begin with naming and enabling a rule and then add the criteria, the action, and an event.

**Tasks**

- *Name and enable a rule on page 186*
  Configure name and enabling as general settings for a rule.
- *Add the rule criteria on page 189*
  Add the rule criteria to determine when a rule is applied.
- *Add the rule action on page 190*
  Add the action that is executed if the rule criteria matches.
- *Add a rule event on page 191*
  Optionally add one or more events that are executed if the rule criteria matches.

**Name and enable a rule**

Configure name and enabling as general settings for a rule.

**Task**

2. On the rule sets tree, select a rule set for the new rule.
3. Click Add Rule above the settings pane.
   The Add Rule window opens with the Name step selected.
4. Configure general settings for the rule:
   a. In the Name field, type a name for the rule.
   b. Select Enable rule to let the rule be processed when its rule set is processed.
   c. [Optional] In the Comment field, type a plain-text comment on the rule.
Continue with adding the rule elements.

**Working with the Add Criteria window**

The window for adding the rule criteria provides several functions to help you with selecting suitable criteria elements.

According to the three elements of the rule criteria, the window is divided into the following columns:

- Left column for selecting a property
- Middle column for selecting an operator
- Right column for selecting an operand

Within a column, properties, operators, and operands are displayed in lists.

For example, you can select the following:

- **Left column:** `MediaType.EnsuredTypes`
- **Middle column:** `none in list`
- **Right column:** `Anti-Malware Media Type Whitelist`

This creates the criteria `MediaType.EnsuredTypes none in list Anti-Malware Media Type Whitelist`. If you add *Block* as the action, you get a rule for blocking access to media of all types that have not been entered in the specified whitelist.

To help you make suitable selections, the window does the following:

- Filters lists according to the filter settings that you provide
- Adapts lists in other columns when you select an item in one column to show only items that are suitable for being configured with the selected item
- Groups lists items in the left and right columns into the categories **Recommended**, **Suggested**, and **Other** if this categorization is possible for the currently displayed items
- Preselects two or three items (one per column) if they can be recommended for being combined with each other

**Beginning with the left or right column**

You can begin by selecting an item from the left or right column, depending on what you have already in mind about the criteria you are going to add.

For example, if this criteria is to be part of a rule for filtering infected web objects, you might begin by selecting the property `Antimalware.Infected` from the left column and then see what are suitable items to go with it. The result could be: `Antimalware.Infected` (property) *equals* (operator) `true` (operand).

On the other hand, if you want to include the criteria in a rule that prevents the users of your network from accessing drug-selling web sites, you might begin by selecting the URL category list `Drugs` as an operand and then combine it with a suitable operator and property. The result could be: `URL.Categories` (property) *at least one in list* (operator) `Drugs` (operand).

**Left column**

The list in the left column of the window allows you to select a property. The currently selected property appears at the top of the column in the **Selected property** field.
You can adapt the list in the following ways:

- Filter the list.
  - Using the **Filter** menu to filter according to:
    - Property type
    - Module (or engine) that is called to deliver a value for a property
    - Criteria group, such as Anti-Malware criteria, Media Type criteria, and others

This part of the menu appears also immediately before the window opens. After selecting a criteria group, the lists in all columns show only items that are suitable for configuring criteria of the selected group.

- User-defined properties (to show only those properties)
- Using a filtering term that you type in the input field below the menu
- Add self-configured properties to the list using the **Add User-Defined Property** button and window.

The list is automatically adapted when you select an operand from the list in the right column. Then it shows only properties that are suitable for being configured with this operand.

After selecting a property, you can configure its settings and parameters if it has any. The **Settings** and **Parameter** buttons are then displayed with the property, which open windows for configuring the respective items.

### Middle column

The list in the middle column of the window allows you to select an operator. The currently selected operator appears at the top of the column in the **Selected operator** field.

The list is automatically adapted when you select an item from the list in the left or right column. Then it shows only operators that are suitable for being configured with the selected item.

### Right column

The list in the right column of the window allows you to select an operand. The currently selected operand appears at the top of the column in the **Compare with** field.

An operand can be a single item of different types, a list of items, or another property. Types for single operands include Boolean, String, Number, Category, and others.

You can adapt the list in the following ways:

- Select an operand type (including the list and property types) from the list at the top of the column.
  
  Only items of this type are then displayed in the main list.

- (Only for lists and properties:) Filter the list using the **Filter** drop-down menu or the input field below.

If lists are displayed as operands, the **Add <list type>** and **Edit <list type>** buttons are provided at the bottom of the column. They open windows for adding and editing lists in the usual way.

The list is automatically adapted when you select a property from the list in the left column. Then it shows only operands that are suitable for being configured with this property.
Add the rule criteria

Add the rule criteria to determine when a rule is applied.

Task

1. In the Add Rule window, click Rule Criteria.

2. In the Apply this rule section, select when the rule is applied:
   - **Always** — The rule is always applied.
     Continue with adding another element, for example, the rule action.
   - **If the following criteria is matched** — The rule is applied if the configured criteria is matched.
     Continue with the next step.

3. In the Criteria section, click Add and select a criteria group from the drop-down menu.

   The Add Criteria window opens displaying items that are suitable for configuring criteria from the selected group.

   - **To display items for all criteria, select Advanced criteria.**

   The window has three columns:
   - Left column for selecting a property
   - Middle column for selecting an operator
   - Right column for selecting an operand

   The currently selected elements are displayed at the top of each column under **Selected property**, **Selected operator**, and **Compare with**.

   The window supports you in selecting suitable elements by automatically adapting the lists in the other columns after you have selected an item in one column. Then the other columns show only items that are suitable for being configured with the selected item.

   You can begin by selecting an item from the left or right column. Accordingly, steps 4 to 6 could also be completed in a different order.

   - **If your criteria is to use a list as an operand, we recommend that you begin with selecting this list from the right column.**

4. Select a property.
   a. From the list in the left column, select an item or leave the one that is preselected (if there is any).
      - **You can filter the list and add self-configured properties.**
   
   b. [Conditional] If you have selected a property that requires settings, select settings from the **Settings** drop-down list that is displayed with the property or leave the preconfigured settings.
   
   c. [Conditional] If you have selected a property that requires the setting of parameters, click **Parameters** below the property name and work with the options in the window that opens to set values for all required parameters.
5 Select an operator from the list in the middle column or leave the one that is preselected (if there is any).

6 Select an operand from the list in the right column or leave the one that is preselected (if there is any). If the list is empty, type a suitable value, for example, a number.

To change the type of operands that are displayed, select a type from the list at the top of the column.

After selecting an individual operand or a type of operands, the lists in the middle and left columns are adapted to show suitable operators and properties.

7 Click OK to close the Add Criteria window.

The new criteria appears in the Add Rule window.

If you want to configure complex criteria, repeat steps 3 to 6 to configure more criteria parts.

Connect criteria parts by AND or OR, which are then provided as options. For three or more criteria parts, type parentheses to indicate how they are logically connected in the Criteria combination field, which appears then.

Continue with adding another element, for example, the rule action.

**Add the rule action**

Add the action that is executed if the rule criteria matches.

**Task**

1 In the Add Rule window, click Action.

2 From the Action list, select one of the following actions:
   - Continue — Continues with processing the next rule
   - Block — Blocks access to an object and stops processing rules
   - Redirect — Redirects the client that requested access to an object to another object
   - Authenticate — Stops processing the current cycle and sends an authentication request
   - Stop Rule Set — Stops processing the current rule set and continues with the next rule set
   - Stop Cycle — Stops processing the current cycle, but does not block access to the requested object
   - Remove — Removes the requested object and stops processing the current cycle

3 [Conditional] If you have selected an action that requires settings (Block, Redirect, Authenticate), select settings from the Settings list.

Click Add or Edit before selecting settings to open windows for adding new settings or editing existing settings.

4 If you have created all required rule elements, but do not want to add an event:
   a [Optional] Click Summary to review what you have configured.
   b Click Finish.

The Add Rule window closes and the new rule appears within the rule set you have selected for it.
Add a rule event
Optionally add one or more events that are executed if the rule criteria matches.

Task
1 In the Add Rule window, click Events.
2 In the Events section, click Add and select Events from the drop-down list.
   The Add Event window opens.
3 From the Event list, select an event.
   To filter the list, type a filtering term in the input field above the list.
4 [Conditional] If you have selected an event that requires settings, select settings from the Settings list.
   Click Add or Edit before selecting settings to open windows for adding new settings or for editing existing settings.
5 [Conditional] If you have selected an event that requires the setting of parameters, click Parameters and work with the options in the window that opens to set values for all required parameters.
6 Click OK.
   The Add Event window closes and the new event appears in the Events list.
7 If this is the last of the adding procedures:
   a [Optional] Click Summary to review what you have configured.
   b Click Finish.
      The Add Rule window closes and the new rule appears within the rule set you have selected for it.

Create a rule set
You can create a rule set and add it to your configuration.

Task
1 Select Policy | Rule Sets.
2 On the rule sets tree, navigate to the position where you want to insert the new rule set.
3 Click Add above the rule sets tree.
   A drop-down list opens.
4 Select Rule Set.
   The Add New Rule Set window opens.
5 Configure the following general settings for the rule set:
   • Name — Name of the rule
   • Enable — When selected, the rule set is enabled.
   • [Optional] Comment — Plain-text comment on the rule set
In the **Apply to** section, configure the processing cycles. You can select only one cycle, or any combination of these three:

- **Requests** — The rule set is processed when requests from the users of your network are received on the appliance.
- **Responses** — The rule set is processed when responses from web servers are received.
- **Embedded objects** — The rule set is processed for embedded objects sent with requests and responses.

In the **Apply this rule set** section, configure when the rule set is applied:

- **Always** — The rule set is always applied.
- **If the following criteria is matched** — The rule set is applied if the criteria configured below is matched.

In the **Criteria** section, click **Add**.

The Add Criteria window opens.

In the **Property** area, use the following items to configure a property:

- **Property** — List for selecting a property (property types shown in brackets)
- **Search** — Opens the Property Search window to let you search for a property.
- **Parameter** — Opens the Property Parameters window for adding up to three parameters, see Step 10.

The icon is grayed out if the property has no parameters.

- **Settings** — List for selecting the settings of the module that delivers a value for the property (module names shown in brackets)

The icon is grayed out if no settings are required for the property and *(not needed)* is added.

- **Add** (String, Boolean, or numerical) — Configure it in the Value area. Then click **OK**.
- **Edit** — Opens the Edit Settings window for editing the selected settings.

If no parameters need to be configured for the property, click **OK** and continue with Step 11.

If you need to add property parameters:

a. Click **Parameter**.

The Property Parameters window opens.

b. Add as many parameters as needed.

A parameter can be a:

- **Value** (String, Boolean, or numerical) — Configure it in the Value area. Then click **OK**.
- **Property** — Follow the instructions for editing properties, beginning with Step 4.

From the **Operator** list, select an operator.

In the **Parameter** area, add a parameter (also known as operand).

This can be a:

- **Value** (String, Boolean, or numerical) — Configure it in the Value area.
- **Property** — Follow the instructions for editing properties, beginning with Step 4.

Click **OK** to close the Add Criteria window.

[Optional] Click the **Permissions** tab and configure who is allowed to access the new rule set.
15 Click OK. to close the Add New Rule Set window.

The Add New Rule Set window closes and the rule set is inserted into your rule set system.

16 Click Save Changes.

Import a rule set

You can import a rule set from the library into your rule set system.

Task

1 Select Policy | Rule Sets.

2 On the rule sets tree, navigate to the position where you want to insert the new rule set.

3 From the Add drop-down list, select Rule Set from Library.

   A window with a list of the library rule sets opens.

4 Select the rule set you want to import, for example, the Gateway Antimalware rule set.

   If conflicts arise when importing this rule set, they are displayed in the window.

   Conflicts arise when a rule set uses configuration objects, such as lists or settings, that already exist in your rule set system.

5 Use one of the following methods to solve conflicts:

   • Click Auto-Solve Conflicts and choose one of the following strategies for all conflicts:

     • Solve by referring to the existing objects — If rules of the imported rule set refer to objects existing in the appliance configuration under the same names, references are made to apply to these existing objects.

     • Solve by copying and renaming to suggested — If rules of the imported rule set refer to objects existing in the appliance configuration under the same names, these objects are also used, but are renamed, so as to avoid conflicts.

   • Click the listed conflicts one after another and solve them individually by choosing either of the two above strategies each time.

6 Click OK.

   The rule set is inserted in the rule sets tree. It is enabled by default.

   List and settings that the rule set needs to perform its filtering job are implemented with the rule set and can be viewed on the lists and settings trees.

7 If necessary, use the blue arrows above the rule sets tree, to move the rule set to where you want it to be.

8 Click Save Changes.
Best practices - Rule configuration

Web Gateway offers many ways to configure rules. However, to achieve an efficient filtering process, some guidelines should be observed.

- **Use rules and rule sets in appropriate filtering cycles** — Some filtering activities are better handled in the request cycle, while others can be left to processing in the response cycle. For example, a rule that blocks requests based on the categories of the submitted URLs should be processed in the request cycle.

- **Use "expensive" properties toward the end of the filtering process** — Some properties require more time and bandwidth to retrieve values for them during the filtering process.

  For example, the *Antimalware.Infected* property is expensive in this sense, so a rule that contains this property should be placed after a rule with, for example, the less expensive *URL.Categories* property. If a request is blocked by the first rule, the effort of processing the second rule is avoided.

- **If possible, do not use more than two properties in the rule criteria** — This guideline does not save processing resources, but makes it easier to understand how rules work.

Using rules and rule sets in appropriate cycles

Rule processing on Web Gateway is performed in different cycles. Perform filtering activities in the cycles that are best suited for them.

The following cycles are available:

- **Request cycle** — For processing requests from clients of Web Gateway

  This cycle works with any data that is available in a request, such as client IP address, URL, user name (if authentication is performed), or browser-related header information.

  If a request is blocked in this cycle, no response cycle is performed, as the request is not forwarded to a web server and therefore no response is received.

- **Response cycle** — For processing responses by web servers, responding to the requests that Web Gateway forwarded to them

  This cycle works with any data that is available in a response, such as the requested data or server-related header information.

- **Embedded objects cycle** — For processing web objects that are embedded in requests or responses

  This cycle is performed when an opener is called in the request or response cycle to allow the filtering modules to look into a web object more deeply. The following two openers are available:

  - **Composite Opener** — The "normal" opener for inspecting files with formats such as .zip, .exe, and others

  - **HTML Opener** — Used very rarely in some advanced configurations

  The embedded objects cycle is performed after the request or response cycle if embedded objects need to be inspected. If there are no embedded objects, the cycle is not performed.

After the request, response, and embedded object cycles are completed, rule sets with logging rules are processed on Web Gateway to let data be written into log files. Processing these rule sets is sometimes also referred to as performing the **logging cycle**.
General guideline for using the request cycle

Let any information that is available in a request be filtered in the request cycle to get any blocked matter out of the way as soon as possible. To understand this guideline, consider cases like the following:

- If filtering based on URL categories is performed in the response cycle, rather than in the request cycle, the requested data might be received from the web server, only to find out that it cannot be passed on to the client because their category is not allowed.

- If filtering based on client IP addresses is performed in the request cycle and a request is blocked, no response cycle is performed, so it is useless to have a rule for filtering this data in the response cycle. If a request is allowed, it is not necessary to filter the data a second time in the response cycle.

Processing cycles and recommended filtering activities

The following table shows the filtering activities that should be performed in the different cycles.

### Table 6-7 Processing cycles and recommended filtering activities

<table>
<thead>
<tr>
<th>Request cycle</th>
<th>Response cycle</th>
<th>Embedded objects cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filtering based on whitelists</td>
<td>Filtering based on whitelists</td>
<td>Inspecting the body of a request or response</td>
</tr>
<tr>
<td>Filtering based on blocking lists</td>
<td>Filtering based on server-sent headers, such as Content-Length and others</td>
<td>Media type filtering</td>
</tr>
<tr>
<td>Filtering based on client-sent headers, such as User-Agent and others</td>
<td>Media type filtering</td>
<td>Anti-malware scanning for embedded objects</td>
</tr>
<tr>
<td>User authentication</td>
<td>Anti-malware scanning for downloads</td>
<td></td>
</tr>
<tr>
<td>URL filtering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-malware scanning for uploads</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As this overview also shows, there are some activities that are only recommended for one cycle, while others, for example, whitelisting or anti-malware scanning, are recommended for two or more cycles.

Using expensive properties at the end of the filtering process

"Expensive" properties require a huge processing effort. Rules with these properties should be placed at the end of the rule set system.

When rules are processed, the modules (or engines) on Web Gateway are called to retrieve values for their properties. Some of these modules usually consume more time and bandwidth than others. For example, running the engines for anti-malware scanning usually consumes more resources than letting the URL Filter module retrieve URL category information.

To improve performance, place rule sets containing rules with expensive properties at the end of the rule set system, so that rules with less expensive properties are processed first. If one of these rules already blocks a request or response, the rules with the more expensive properties need not be processed.

Expensiveness of properties

The following table shows the "expensiveness" of some properties that are often used in rules.
Properties marked by an * (asterisk) rely also on external components, for example, on an authentication server, which additionally impacts performance. The table also shows expensiveness for two rule elements that are not properties, but events.

<table>
<thead>
<tr>
<th>Less expensive</th>
<th>Medium</th>
<th>More expensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>URL.Destination.IP*</td>
<td>Antimalware.Infected</td>
</tr>
<tr>
<td>URL.Host</td>
<td>Media.EnsuredTypes</td>
<td>Properties used in DLP (Data Loss Prevention) filtering</td>
</tr>
<tr>
<td>URL.Categories*</td>
<td>Properties* used for authenticating users</td>
<td>Using the HTML Opener (enabled by an event)</td>
</tr>
<tr>
<td>Client.IP</td>
<td>Using the Composite Opener (enabled by an event)</td>
<td></td>
</tr>
<tr>
<td>Proxy.IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy.Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System.Hostname</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Properties used to check HTTP header information</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Expensiveness of properties considered for individual rules**

The guideline for using properties according to their expensiveness applies not only to a suitable placement of rules and rule sets within the rule set system as a whole, but also to the use of properties in individual rules.

The following rule blocks a request for access to a web server with a particular host name if this request was sent by a client with a particular IP address.

**Name**

Block host abcd.com for client with IP address 1.2.3.4

**Criteria**

Client.IP equals 1.2.3.4 AND URL.Host matches *abcd.com

**Action**

Block<Default>Continue

When the rule is processed, the value for Client.IP is retrieved first to see where the request comes from. If it does not equal the configured operand, the rule does not apply and processing continues with the next rule. Only if the value for Client IP is actually 1.2.3.4, will the value for URL.Host be retrieved as well, to see if the criteria matches completely.

Client.IP is placed first in the criteria because comparing two client IP addresses is less expensive than verifying that a host name matches a wildcard expression.

**Using not more than two properties in the criteria of a rule**

Using not more than two properties in the criteria of a rule (where possible) makes the rule easier to understand for others and for you when you get back to it after some time.

The following sample rule allows access to destinations within a particular domain and for administrators, but only if they use a particular port for access. There are four different properties in the criteria of this rule for checking the following parameters:

- **Host name of a URL** — Is access requested to the configured domain?
- **User group** — Did authentication show that the user who sent the request is in the user group for administrators?
• **Client IP address range** — Was the request sent from a client with an IP address within the address range that is reserved for administrators?

• **Proxy port** — Is access to the domain requested over the configured port?

The rule looks as follows:

<table>
<thead>
<tr>
<th>Name/Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow only administrators using port 9090 access to test domain</strong></td>
<td>Block &lt;Default&gt;</td>
<td></td>
</tr>
<tr>
<td>URL.Host matches &quot;testdomain.com&quot; AND (Authentication.UserGroups does not contain &quot;Administrator&quot; OR Client.IP is not in range 192.168.42.0/24 OR Proxy.Port does not equal 9090)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For a match that lets the rule apply, the first part of the rule criteria requires that a request for access to the test domain is actually submitted.

All other criteria parts are phrased negatively. If the user is not an administrator or the client IP address is not within the configured range or the proxy port is not 9090, then the request is blocked.

In other words, only if a request for access to the test domain is sent by an administrator from a client with an IP address that is within the configured range, using proxy port 9090, does this rule allow access.

The last three criteria parts are included in parentheses, so a combined truth value can be found for them and then checked together with the value for the first criteria part.

The same filtering behavior can be achieved by splitting this rule up into the following three rules.

<table>
<thead>
<tr>
<th>Name/Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Check whether request is for accessing test domain</strong></td>
<td>Stop Rule Set</td>
<td></td>
</tr>
<tr>
<td>URL.Host does not match *testdomain.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Block access if not over proxy port 9090</strong></td>
<td>Block &lt;Default&gt;</td>
<td></td>
</tr>
<tr>
<td>Proxy.Port does not equal 9090</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Block users who are not administrators based on user name and client IP address</strong></td>
<td>Block &lt;Default&gt;</td>
<td></td>
</tr>
<tr>
<td>Authentication.UserGroups does not contain &quot;Administrator&quot; OR Client.IP is not in range 192.168.42.0/24</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The first of the three rules checks whether a request for access to the test domain is actually submitted. If this is not the case, processing the rules that follow this rule within the same rule set is stopped.

This means the two blocking rules that follow the first rule would not be processed. It is not necessary to process them, however, as there is no attempt made to access the test domain in the first place.

When the two blocking rules are processed, they check the parameters that are involved in deciding whether a request to access the test domain is allowed. The checking is performed in the same way as in the preceding single rule with four properties in its criteria.

The parameters that concern the administrator status of a user are combined within one rule with two properties.
Restrict access to configuration items

When creating rule sets, lists, or settings, or working with existing ones, you can restrict access to them.

**Task**

1. Select Policy | Rule Sets (or Lists or Settings).
2. On the tree structure, navigate to the position where you want to add the new item.
3. Click Add above the tree structure.
   
   An Add window opens.
4. Complete the steps for adding a new item. Then click the Permissions tab.
   
   Three modes of access can be configured: Read and Write, Read, and No Access.
5. Click Add under the Read and Write pane.
   
   The Add Role or User window opens.
6. Select a role or a user (or more than one of each type at once) from the list in the corresponding pane. Or type a wildcard expression as the name of a role or user in the Wildcard field.
7. Add as many entries to the Read and Write list as needed.
   
   Use the Delete button under the pane to delete entries
8. Fill the Read and No Access panes in the same way.
9. Use the radio buttons under All other roles have to configure access for all roles and users that are not included in one of the lists on the tab.
10. Click OK to close the window.
11. Click Save Changes
Lists

Lists are used by rules for retrieving information on web objects and users. There are several types of lists, which differ, for example, with regard to who created them or which type of elements they contain. Accordingly, you work with these lists in different ways.

Lists appear in different places on the user interface, for example, in the criteria of rules and rule sets, on the Lists tab, and within settings.

At the initial setup of the appliance, lists are implemented together with the rule set system.

You can then review the lists of the implemented system, modify and delete them, and also create your own lists.

Contents

- List types
- Lists tab
- Access a list
- Create a list
- Work with different types of lists
- Subscribed lists
- External lists
- Map Type lists
- Common Catalog
- JavaScript Object Notation data
List types

Web security rules on Web Gateway use several types of lists for retrieving information about web objects and users.

The following are the main list types:

- **Custom lists** — You can modify these lists. They are displayed on the upper branch of the lists tree on the Lists tab, for example, the list of URLs that are exempted from filtering.

  Custom lists can have entries in string, number, category, and other formats. Lists with different formats can require different methods of maintaining them. Some custom lists are initially empty and must have their entries filled by you.

  To the custom lists that Web Gateway provides after the initial setup, you can add lists that you create on your own.

- **System lists** — You cannot modify these lists. They are displayed on the lower branch of the lists tree on the Lists tab.

  System lists include category, media type, and application name lists, as well as lists of connectors used for cloud single sign-on. They are updated when an upgrade to a new version of Web Gateway is performed.

  System lists for Data Loss Prevention (DLP), application filtering, and the Dynamic Content Classifier can be included in automatic updates that you schedule.

- **Inline lists** — You can modify these lists, but they do not appear on the Lists tab. They appear inline as part of the settings for a configuration item, for example, a list of HTTP ports as part of the proxy settings.

- **Subscribed lists** — You set up these lists with a name on Web Gateway. They are initially empty and have their content retrieved from a data source that you subscribe to. Subscribed lists are displayed on the lists tree at the end of the custom lists.

  There are two subtypes of subscribed lists:

  - **McAfee-maintained lists** — Content for these lists is retrieved from a McAfee server.

    A number of lists are available on the McAfee server, for example, lists of IP address ranges or media types.

  - **Customer-maintained lists** — Content for these lists is retrieved from a data source that you specify.

    Sources that you can specify are files on web servers running under HTTP, HTTPS, or FTP.

List content is maintained on the respective servers. To ensure that newer versions of this content are transferred to your lists on Web Gateway, you can perform updates manually or configure automatic updates.
• **External lists** — These lists reside on external sources under their own names. They have their content transferred to Web Gateway, where they provide the value of a property in a rule.

  External list content is transferred during runtime, which means it is retrieved when the rule with the external list property is processed.

  When the content has been retrieved, it is cached and reused until its date of expiration, which you can configure. After expiration, the transfer is repeated when the rule is processed again.

  Sources that content can be retrieved from include files on web servers running under HTTP, HTTPS, FTP, or LDAP, and in particular types of databases. They also include files that are stored within your local file system.

• **Map type lists** — These lists store pairs of keys and values that are mapped to each other. You can create map type lists and fill list entries on Web Gateway, or retrieve them as subscribed or external lists from other sources.

  Keys and values on map type lists are initially stored in string format, but can be converted into different formats using suitable properties in rules.

• **Common Catalog lists** — These lists can be pushed from a McAfee ePO server to Web Gateway.

  Common Catalog lists can have entries in IP address, domain name, string, or wildcard expression format. They are maintained on the McAfee ePO server.
**Lists tab**

Use the **Lists** tab to work with lists.

![Lists tab interface](image)

**Figure 7-1  Lists tab**

### Main elements of the Lists tab

The following table describes the main elements of the **Lists** tab.

<table>
<thead>
<tr>
<th><strong>Table 7-1  Main elements of the Lists tab</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Element</strong></td>
</tr>
<tr>
<td>Lists toolbar</td>
</tr>
<tr>
<td>Lists tree</td>
</tr>
<tr>
<td>List entries toolbar</td>
</tr>
<tr>
<td>List entries</td>
</tr>
</tbody>
</table>

### Lists toolbar

The lists toolbar provides the following options.
Table 7-2  Lists toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Opens the Add List window for adding a list.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the Edit List window for editing a selected list.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a selected list. A window opens to let you confirm the deletion.</td>
</tr>
<tr>
<td>Import</td>
<td>Opens the file manager on your system to let you import a list.</td>
</tr>
<tr>
<td>Export</td>
<td>Opens the file manager on your system to let you export a list that you have selected on the lists tree.</td>
</tr>
<tr>
<td>View</td>
<td>Opens a menu to let you display the lists in different ways (A-Z, Z-A, by list type, with or without list types for which currently no lists exist).</td>
</tr>
<tr>
<td>Expand all</td>
<td>Expands all collapsed items on the lists tree.</td>
</tr>
<tr>
<td>Collapse all</td>
<td>Lets all expanded items on the lists tree collapse.</td>
</tr>
</tbody>
</table>

List entries toolbar

The list entries toolbar provides the following options.

Table 7-3  Lists entries toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Opens the Add List type window for adding a list entry, for example, the Add String window.</td>
</tr>
<tr>
<td>Add multiple</td>
<td>Opens the Add List type window for adding multiple list entries if this is possible for a list type.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the Edit List type window for editing a selected list entry, for example, the Edit String window.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a selected list entry. A window opens to let you confirm the deletion.</td>
</tr>
<tr>
<td>Move up</td>
<td>Moves an entry up the list.</td>
</tr>
<tr>
<td>Move down</td>
<td>Moves an entry down the list.</td>
</tr>
<tr>
<td>Filter</td>
<td>Input field for typing a filtering term to display only matching list entries. The filtering function works as soon as you type a character in the field.</td>
</tr>
</tbody>
</table>

Access a list

You can access a list on the Lists tab or by clicking a list name in a rule.

Tasks

- **Access a list on the Lists tab on page 204**
  To access a list on the Lists tab, you locate it on the lists tree and select the list.
- **Access a list in a rule on page 204**
  To access a list in a rule, you locate the rule on the Rule Sets tab and click the list name.
Access a list on the Lists tab
To access a list on the Lists tab, you locate it on the lists tree and select the list.

**Task**

1. Select Policy | Lists

2. On the lists tree, navigate to the branch that contains the list you want to access and click the list name.
   
   The list entries appear on the settings pane.

You can now work with the list.

Access a list in a rule
To access a list in a rule, you locate the rule on the Rule Sets tab and click the list name.

**Task**

1. Select Policy | Rule Sets

2. On the rule sets tree, select the rule set that contains the rule with the list you want to access.
   
   The rules of the rule set appear on the settings pane.

3. Make sure Show details is selected.

4. In the rule with the list you want to access, do one of the following:
   
   - Click the list name in the rule name if it is contained in this name.
   - Click the list name in the rule criteria.

   An Edit List <Type> window opens, where <Type> is the type of the list you are accessing.

You can now work with the list.

Create a list
You can create lists of your own in addition to those that were implemented on the appliance at the initial setup or when you imported a list from the library.

Creating a list includes the following two steps:

- Adding a new list
- Filling the new list with entries

**Tasks**

- *Add a new list on page 205*
  
  You can add a new list that you fill with entries later.

- *Fill a list with entries on page 205*
  
  When you have added a new list on the appliance, you need to fill it with entries.
Add a new list
You can add a new list that you fill with entries later.

Task
1. Select Policy | Lists.
2. On the lists tree, navigate to the position where you want to add the list.
3. Click Add on the toolbar.
   The Add List window opens, with the Add List tab selected.
4. Use the following items to configure general settings for the list:
   - Name — Name of the list
   - Comment — [Optional] Plain-text comment on the list
   - Type — List for selecting a list type
5. [Optional] Click the Permissions tab and configure who is allowed to access the list.
6. Click OK.
   The Add List window closes and the new list appears on the lists tree.
7. Click Save Changes.

You can now fill the list with entries.

Fill a list with entries
When you have added a new list on the appliance, you need to fill it with entries.

Task
1. Select Policy | Lists.
2. From the lists tree, select the list you want to add entries to.
3. Click Add on the settings pane.
   The Add <List type> window opens, for example, the Add String window.
4. Add an entry in the way it is done for a particular list type.
5. [Optional] In the Comment field, type a plain-text comment on the list entry.
6. Click OK.
   The Add <List type> window closes and the entry appears in the list.
7. Click Save Changes.

Work with different types of lists
Working with lists is done differently depending on the list type.
For example, if the type is String, you can add entries by typing strings in the String field of the Add String window. However, if the type is MediaType, you need to select an entry from a media type folder, which is part of a system of folders.
For string and wildcard expression lists, there is the option to add multiple entries at once by clicking Add multiple and typing text for each entry in a new line.

For media type lists, you can select multiple entries or folders at once if you do not want to add them separately.

**Tasks**
- *Add a wildcard expression to a global whitelist for URLs on page 206*
  You can add a wildcard expression to a whitelist used by a global whitelisting rule.
- *Add a URL category to a blocking list on page 207*
  You can add a URL category to a blocking list to block access to all URLs falling into that category.
- *Add a media type to a media type filter list on page 207*
  You can add a media type to a list for media type filtering.

**Add a wildcard expression to a global whitelist for URLs**
You can add a wildcard expression to a whitelist used by a global whitelisting rule.

**Task**
2. On the rule sets tree, select a rule set that contains rules for global whitelisting, for example Global Whitelist.
   The rules appear on the settings pane.
3. Find the rule that uses a whitelist to exempt requests when they submit URLs for hosts matching the wildcard expressions on the list, for example, URL.Host matches in list Global Whitelist and click on the list name.
   
   A yellow triangle next to the list name means the list is initially empty and you need to fill the entries.

   The Edit List (Wildcard Expression) window opens.
4. Click Add.
   The Add Wildcard Expression window opens.
5. In the Wildcard expression field, type a wildcard expression.
   To add multiple wildcard expressions at once, click Add multiple and type every wildcard expression in a new line.
6. [Optional] In the Comment field, type a comment on the wildcard expression.
7. Click OK.
   The window closes and the wildcard expression appears on the whitelist.
8. Click Save Changes.
Add a URL category to a blocking list
You can add a URL category to a blocking list to block access to all URLs falling into that category.

**Task**

2. On the rule sets tree, select the rule set that contains rules for URL filtering.
   The rules appear on the settings pane.
3. Find the rule that uses a category blocking list, for example, **Block URLs whose category is in Category BlockList**, and click on the list name.
   A yellow triangle next to the list means that the list is initially empty and you need to fill the entries.
   
   The Edit List (Category) window opens.
4. Expand the group folder with the category you want block, for example, **Purchasing**, and select the category, for example, **Online Shopping**.
   To add multiple categories at once, select multiple categories or one or multiple group folders.
5. Click **OK**.
   The window closes and the category appears on the blocking list.
6. Click **Save Changes**.

Add a media type to a media type filter list
You can add a media type to a list for media type filtering.

**Task**

2. On the rule sets tree, navigate to a rule set that contains rules for media filtering, for example, the nested **Download Media Types** rule set of the Media Type Filtering rule set and select it.
   The rules appear on the settings pane.
3. Select the rule **Block types from Media Type Blocklist** and click on the list name.
   The Edit List (MediaType) window opens.
4. Click **Edit**.
   An Edit window opens. It displays a list of group folders with media types.
5. Expand the group folder with the media type you want to add, for example, **Audio**, and select the media type, for example, **audio/mp4**.
   To add multiple media types at once, select multiple media types or one or multiple group folders.
6. Click **OK**.
   The window closes and the media type appears on the filter list.
7. Click **Save Changes**.
Subscribed lists

Lists for use in web security rules can be filled with content that is retrieved from suitable servers. These lists are known as subscribed lists.

When working with subscribed lists, you only have to configure general settings, such as the list name, yourself. For the list content, for example, IP addresses or URLs, you rely on a server, which can be the McAfee server that is provided for maintaining subscribed lists or another server that you specify.

Subscribed lists that retrieve their content from the McAfee server are known as McAfee-maintained lists. Lists that retrieve their content from another server are known as customer-maintained lists.

After you have created a subscribed list, it appears on the Subscribed Lists branch of the lists tree on the user interface. You can work with a subscribed list in the same way as with other lists on the lists tree.

There is a restriction in size for subscribed lists. A subscribed list must not be larger than 4 MB or contain more than 100,000 entries.

By configuring update schedules or performing updates manually, you ensure that the latest content is made available to the web security rules by a subscribed list.

Retrieving list content from the McAfee server

When the content of a subscribed list is retrieved from the McAfee server that is provided for this purpose, you select the type of content for this list from a catalog.

The content is maintained on the McAfee server. To ensure that McAfee-maintained lists hold the latest content, you perform manual updates on the user interface of your appliance.

Retrieving list content from another server

When the content of a subscribed list is retrieved from a server other than the McAfee server, you specify the URL for the file that holds this content on the server.

The content is maintained on this server. Updates for this kind of subscribed lists are performed according to a schedule that you set up when configuring the list settings.

Create a subscribed list

To create a subscribed list, you configure general list settings and settings for the list content.

Task

1. Select Policy | Lists.

2. Above the lists tree, click the Add icon.

   The Add List window opens.

3. Configure general settings for the list.
   a. In the Name field, type the list name.
   b. From the Type lists, select the list type.
   c. Under Contains, select the type of entry that the list will contain.
d  [Optional] In the Comments field, type a plain-text comment on the list.

e  [Optional] Click the Permissions tab and configure who is allowed to access the list.

4  Select List content is managed remotely.

5  Configure settings for the list content.
   • For list content that is retrieved from the McAfee server:
     • Under Source, select McAfee maintained list.
     • Click Choose.
       The Choose List Content window opens.
     • Select a content type
     • Click OK to close the window.
   • For list content that is retrieved from another server:
     • Under Source, select Customer maintained list.
     • Click Setup.
       The Setup window opens.
     • Configure settings for the list content.
     • Click OK to close the window.

6  Click OK again.

   The Add List window closes and the list appears on the Subscribed Lists branch of the lists tree.

7  Click Save Changes.

Settings for subscribed lists content

When a subscribed list is maintained on a server other than the McAfee server, settings must be configured for its content.

Table 7-4  Settings for subscribed list content

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL to download</td>
<td>Specifies the URL of a file with content for a subscribed list. The format for specifying the URL is: HTTP</td>
</tr>
<tr>
<td>Use this</td>
<td>When selected, the certificate contained in the certificate authority chain appearing next to the radio button is used. This is required if the connection to the server that provides the list content is a SSL-secured connection for communication under the HTTPS protocol.</td>
</tr>
<tr>
<td>Ignore certificate errors</td>
<td>When selected, certificate errors will not cause a failure to retrieve a list content from a server.</td>
</tr>
</tbody>
</table>
| URL authentication    | Provides settings for configuring a user name and password if authentication is required for access to a server.  
   • User name — Specifies a user name for authenticating to a server.  
   • Password — Sets a password for authenticating to a server. |
### Table 7-4 Settings for subscribed list content (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy</td>
<td>Provides a list for selecting proxy servers that are used to access a server with list content. By default, no proxy server is used to access a list content server.</td>
</tr>
<tr>
<td>Add Proxy</td>
<td>Opens a window for adding a proxy server to the list.</td>
</tr>
<tr>
<td>List content update</td>
<td>Provides settings for configuring an update schedule for list content. An update can be performed:</td>
</tr>
<tr>
<td></td>
<td>• Hourly at — Sets the minutes after the full hour.</td>
</tr>
<tr>
<td></td>
<td>• Daily at — Sets hours and minutes.</td>
</tr>
<tr>
<td></td>
<td>• Weekly at — Sets a day of the week with hours and minutes.</td>
</tr>
<tr>
<td></td>
<td>• Every — Sets the minutes of the interval that is to elapse before the next update happens.</td>
</tr>
</tbody>
</table>

### Updating subscribed lists

Updates of subscribed lists content are performed manually or according to a schedule, depending on whether the content is retrieved from the McAfee server that is provided for this purpose or from another server.

For list content that is retrieved from the McAfee server, you must perform updates manually. Each time you perform a manual update, all McAfee-maintained lists are updated together.

The content of McAfee-maintained lists is also updated each time you create a new list of this kind.

For list content that is retrieved from a server other than the McAfee server, updates are performed according to a schedule. Each subscribed list has a schedule of its own. You can set up and modify the schedule when configuring the settings for the list content.

When administering subscribed lists on a node in a Central Management configuration, updates are shared by all other nodes within the update group.

The update group is configured in the section This Node is a Member of the Following Groups of the Central Management settings.

### Update subscribed lists maintained on the McAfee server

For subscribed lists that are maintained on the McAfee server, you must perform updates manually. The content of McAfee-maintained lists is also updated each time you create a new list.

#### Task

1. Select Configuration | Appliances.

2. On the toolbar above the appliances tree, click Manual Engine Update.

   The content of all McAfee-maintained lists is updated.
Creating a content file for a customer-maintained list

When a subscribed list has been configured as a customer-maintained list, a content file describing the list structure must be created and stored on the web server that the content for this list is retrieved from.

A content file is created in txt or xml format, depending on whether it describes the structure of a simple or complex customer-maintained list. For simple lists, the content file can be created in both formats, for complex lists in xml format only.

Simple customer-maintained lists can be lists of the following types: Application Name, Category, Dimension, IP, IPRange, MediaType, Number, String, Wildcard Expression.

Complex customer-maintained can be lists of the following types: Certificate Authority, Extended List Element, HostAndCertificate, ICAP Server, NextHopProxy.

Content file for a simple list in txt format

The following is an example of a content file in txt format for a customer-maintained list of the Wildcard Expression type.

```
type=regex
"*.txt" "txt file extension"
"*.xml" "xml file extension"
```

The example illustrates the following conventions for a content file in txt format.

- The first line in the file specifies the type of the customer-maintained list that the content file is provided for. The format is: `type=<list type>`
  
  For the list type, one of the following terms must be used: applcontrol, category, dimension, ip, iprange, mediatype, number, string, regex.

- The lines below the first line are for list entries in the customer-maintained list.
  
  A line contains as many items as a list entry in the customer-maintained list. Each item is included in double quotes.
  
  An entry in a list of the Wildcard Expression type contains two items. One is the wildcard expression, the other is a comment that describes the wildcard expression.

The following example illustrates some more conventions for a content file.

```
type=string
"withoutDescription"
"emptyDescription\"\""
"data with description and more spaces in-between" "description"
"data with spaces*" "description"
"Hello\"Michael\" "Michael!\""
```

- An entry in a list of the String type also contains two items: the string and a comment that describes it. However, the description can be omitted.
  
  If the description is omitted, the item for it in the content file can also be omitted, which is shown in line 2.

- Alternatively, if the description is omitted, this can be represented by two double quotes with nothing in between, as shown in line 3.
The line also illustrates the following:

- Double quotes occurring in a string must be masked by a following backslash.
- A backslash that does not follow on double quotes represents itself (a backslash).
- Non-alphanumerical characters, such as the * (asterisk), are allowed at the beginning of a string.

On the user interface, the list entry specified in line 3 would look as follows: `*emptyDescription ""`

- If multiples spaces are inserted between items in the content file, they are ignored in the list entries of the customer-maintained file.

On the user interface, the entry specified in line 4 would therefore look as follows: "data with description and more spaces in-between" "description"

- Multiple spaces within a string in a content file are also ignored in the list entry of the customer-maintained list.

So, on the use interface, the entry specified in line 5 would look as follows: "data with spaces* " "description"

- Line 6 illustrates several of the already mentioned conventions.

**Content file for a simple list in xml format**

The following is an example of a content file in xml format for a customer-maintained list of the Wildcard Expression type. The list content is the same as in the first example of the preceding subsection.

```xml
<content type="regex">
  <listEntry>
    <entry>*.txt</entry>
    <description>txt file extension</description>
  </listEntry>
  <listEntry>
    <entry>*.xml</entry>
    <description>xml file extension</description>
  </listEntry>
</content>
```

For the content type, the same terms must be used as for a content file in txt format.

**Content files for complex lists**

Manually creating a content file for a complex customer-maintained list is rather difficult. However, you can use the options of the user interface to export an existing complex list and store it in a file.

In this file, the complex list appears in xml format. If you delete all lines in the file that precede the opening `</content>` tag and follow the closing `</content>` tag, you almost get a content file for that complex list.

Then you only need to modify the opening `</content>` tag to read `<content type="<file type>", for example, `<content type="nexthopproxy">`.
The terms you can use to specify the file type are: `ca`, `extendedlist`, `icapserver`, `hostandcertificate`, `nexthopproxy`.

**Best practices - Working with a McAfee-maintained subscribed list**

You can use a subscribed list that is maintained by McAfee in a rule of your web security policy, for example, to let particular traffic bypass SSL scanning.

Web traffic might be sent from the clients of your corporate network to particular destinations, for example, WebEx applications, using SSL-secured connections. When this traffic is received on Web Gateway, you might want to let it skip SSL scanning.

For this purpose, you need a list with the IP address ranges that are used by WebEx. As these addresses change frequently, McAfee maintains an address list, saving you the effort of keeping this list up to date manually.

The list is included in the update schedule that you configure on Web Gateway to make sure that any updates by McAfee are eventually passed on to your Web Gateway appliance or to all the appliances that you are running in a Central Management configuration.

To use this McAfee-maintained list in your web security policy:

- Create an empty list of your own and let this list be filled with WebEx address ranges from the McAfee list
- Set up a rule that uses your list to let requests for accessing WebEx destinations skip SSL scanning

**Create a McAfee-maintained subscribed list with IP address ranges**

To create a subscribed list with IP address ranges for WebEx applications that is maintained by McAfee, create a list of your own and let its content be provided by a McAfee-maintained list.

**Task**

1. Select Policy | Lists.
2. Above the lists tree, click the **Add** icon.
3. In the **Add List** window, configure a list as follows.
   a. Configure general settings for the list:
      - **Name**: "WebEx Subscribed List" or any other suitable name
      - **Type**: `IPRange`
   b. Select **List content is managed remotely**.
   c. Select **McAfee-maintained list** and click **Choose**.
   d. In the **Choose List Content** window, select the list named "WebEx IP Ranges".
4. Click **OK** in both windows.
   The list appears on the **Subscribed Lists** branch of the lists tree
5. Click **Save Changes**.

You can now use the list that you have created in a suitable rule.
Use a McAfee-maintained subscribed list in a rule

To use a McAfee-maintained subscribed list in a rule that performs a suitable action on web traffic to particular destinations, configure the list as part of the rule criteria.

Task


2. On the rule sets tree, select the SSL Scanner default rule set and click Unlock View to view the complete rules view.

3. Make sure the rule set is enabled and select the nested Handle CONNECT Call rule set.

4. Click Add Rule and in the window that opens configure a rule as follows.
   a. Under Name, type the rule name, for example, Bypass SSL scanning for WebEx destinations.
   b. Under Criteria, configure the following:
      • Property: URL.Destination.IP
      • Operator: is in range list
      • Compare with (operand): WebEx IP Ranges Subscribed Lists
   c. Under Action, select Stop Rule Set.
   d. Click Finish.

5. Click Save Changes.

Requests for destinations with the IP addresses on the WebEx list will now bypass SSL scanning on Web Gateway.

External lists

Data can be retrieved from external sources, for example, web servers, and used in rules on the appliance.

This data can be a complete list or a single value. It is generally referred to as external lists or external list data. Different data types can be used in an external list, such as strings, numbers, IP addresses, and others.

An important feature of external lists is that they are processed dynamically on the appliance. All retrieving and conversion of external list data happens at run time when the data is first used in a rule.

When the data has been retrieved, it is stored in an internal cache for a period of time that you can configure, but not on disk, so it will not persist after a restart of the appliance. Also external lists do not appear on the lists tree of the user interface.
External lists properties

Access to data retrieved from external sources is provided through special properties. The name of an external list property is `ExtLists.<type>`, where `<type>` is the type of elements in the list that is the value of the property. For example, the value of `ExtLists.IntegerList` is a list of integers. Possible list element types include String, Number, Wildcard Expression, and others.

Usually the value of an external list property is a list, but there also external list properties for single values. When an external source delivers more than one value as input for the latter type of property, only the last value is retrieved and stored.

External list data can be filtered, depending on the source type, and converted into a different format, depending on the type of the property used in a given rule.

By configuring parameters for an external list property, you can specify placeholders that are substituted with property parameters at run time. Using these placeholders, you can let the content of an external list depend on criteria such as a user name or user group name.

For logging purposes, you can use the `ExtLists.LastUsedListName` property, which has as its value the name of the settings for the External Lists module that were used last.

External Lists module

To specify which data is to be retrieved from an external source, you need to configure the settings of the External Lists module (also known as the External Lists filter or engine), which retrieves the data.

When external data cannot be retrieved successfully, the External Lists module returns an error code, which you can process using Error Handler rules. A separate range of error IDs is available for this purpose.

The External Lists module consumes memory for caching data that it retrieves from external sources. You should take this into account when setting up rules for external list handling.

Sources of external list data

The sources of the content that external lists are filled with can be the following:

- A web service, which is accessed under the HTTP, HTTPS, or FTP protocol
- A file within your local file system
- An LDAP or LDAPS server
- A database:
  - PostgreSQL
  - SQLite3

For performing queries on the databases, the SQL query language is used. However, the particular query format can be different for both database types.

As an SQLite3 database operates file-based, we recommend it for testing, rather than for production environments. However, you might still want to use it if you already have data in a database of this type. Otherwise it is easier to use Web Service or File data sources for retrieving external list content.

Recommended use

Working with the external lists feature is recommended in cases like the following.
You need to handle a large number of lists that are mostly stored in external sources, you are running multiple appliances as nodes in a Central Management configuration, and you need to apply frequent changes to the list data.

Synchronizing all list data on all nodes could then no longer be scalable.

**Use of external list data in rules**

To handle external list data, you need to configure rules that contain suitable external list properties in their criteria.

Suppose you want to block a request for a web object if its URL has a destination IP address that is within one of the IP address ranges on a list that is stored in an external source.

You can achieve this with the following rule:

**Block URLs with IP addresses in forbidden range**

URL.Destination.IP is in range ExtLists.IPRangeList("", "", "")<External Lists> -- Block<URL Blocked>

When the rule is processed, it is checked whether the IP address that is the value of the URL.Destination.IP property is within one of the ranges on the list that is the value of ExtLists.IPRangeList.

Together with the external list property, the <External Lists> settings are specified. These are the settings that the External Lists module uses to retrieve the appropriate data as the value for the external list property.

You need to configure these settings to let the module know where a particular external list can be retrieved from and how the retrieval is performed. For example, if this list is stored in a text file on a web server, you can specify the URL that allows access to the file.

Other information that you can configure as part of these settings includes timeouts and size limits.

The parameters of an external list property are optional. They are empty in this example.

By default, no rules for handling external lists exist on the appliance. If you want to use external list data to restrict web access for the users of your network, you need to set up one or more rules like the above and insert them into a suitable rule set.

**Substitution and placeholders**

To allow more flexibility in retrieving external list data, placeholders can be used when configuring the settings of the External Lists module, for example, in URLs.

A placeholder is substituted at run time with a value that you provide as a parameter of an external list property.

For example, you want to retrieve data from a web service that delivers lists of media types allowed for individual users. A URL for a particular media type list would then be:

http://my-web-service.com/ mediatypes?user= <value>

where <value> is the name of a user.
Configuring separate settings for the External Lists module to cover each user individually would be tiresome, so you can use a placeholder in the following way:

- For the **Web service’s URL** parameter in the settings, you specify:

  \[
  \text{http://my-web-service.com/mediatypes?user=${0}}
  \]

  where $${0}$$ is a placeholder for the first of the three parameters of the external list property you are using in a rule.

- For the first parameter of the external list property, you specify the **Authentication.Username** property.

This retrieves a list with the media types that are allowed for an individual user. The user name is the one that this user submitted when required to authenticate after sending a request to access media of a particular type.

You can use the following two types of placeholders:

- **${<n>}** — Placeholder that is substituted with a converted value

  $$<n>$$ is the position number (0, 1, 2) for a parameter of an external list property. At run time, this placeholder is substituted by the value that you specified when configuring the parameter.

  Before the placeholder is substituted, the value is converted. This process is also known as “escaping”. The conversion is performed according to the internal rules of the data source that is involved.

  For example, if the source is a web service, it replaces all characters that are not allowed by %XX sequences, as is specified in the corresponding HTTP standard (RFC 2616).

- **$<<n>>** — Placeholder that is substituted with a non-converted value

  As above, but without conversion. This means you need to ensure yourself that the substitution does not lead to unwanted results.

  You can use this type of placeholder when complete URLs, rather than parts of them are to be substituted.

**Configure the External Lists module**

You can configure settings for the External Lists module to provide the information the module needs to retrieve external list data.

By default, no settings exist for this module on the appliance. You need to add individual settings and configure them for each external list you want to retrieve data from in a rule.

**Task**

1. Select Policy | Settings.

2. On the settings tree, select External Lists and click Add.

   The Add Settings window opens.

3. In the Name field, type the settings name.

4. [Optional] In the Comment field, type a plain-text comment on the settings.

5. [Optional] Click the Permissions tab and configure who is allowed to access the settings.

6. Configure the other settings parameters as needed.
7 Click OK.

The window closes and the settings appear under External Lists on the settings tree.

8 Click Save Changes.

External Lists module settings

The External Lists module settings are used to configure the module that retrieves data from external sources.

Data Source Type

Settings for the type of source that data is retrieved from

You can configure specific settings for each source type in another section, which appears depending on what you select here.

Table 7-5 Data Source Type

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web service</td>
<td>Data is retrieved using a web service under the HTTP, HTTPS, or FTP protocol.</td>
</tr>
<tr>
<td>File on disk</td>
<td>Data is retrieved from a file within your local file system.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Data is retrieved from an LDAP server.</td>
</tr>
<tr>
<td>Database</td>
<td>Data is retrieved from a PostgreSQL or SQLite3 database.</td>
</tr>
</tbody>
</table>

Common Parameters

Settings for time limits in handling external lists
Table 7-6 Common Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation timeout</td>
<td>Limits the time (in seconds) that elapses before an operation for handling external lists is aborted if it cannot be completed successfully.</td>
</tr>
<tr>
<td></td>
<td>This option applies when the source of an external list is a web server. The timeout is reached, for example, when a web server does not respond to a request from the appliance.</td>
</tr>
<tr>
<td></td>
<td>You can specify the expiration of the timeout as:</td>
</tr>
<tr>
<td></td>
<td>• Simple expiration — When selected, you can specify the time (in minutes) to elapse before retrieved list data is removed from the internal cache in the Expiration time input field</td>
</tr>
<tr>
<td></td>
<td>• Scheduled expiration — When selected, you can specify the time that is to elapse before an external list is removed from the internal cache in several input fields that appear</td>
</tr>
</tbody>
</table>

Expiration time | Limits the time (in minutes) that elapses before retrieved data is removed from the internal cache to the specified value.          |

Minutes/Hours/ Days/Months/ Week days | Limits the time that elapses before retrieved data is removed from the internal cache to the specified value.                      |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>These input fields appear when you select Scheduled expiration.</td>
</tr>
<tr>
<td></td>
<td>Your input must be in a “cron”-compliant format because the removal is calculated and performed by a cron job.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the crontab (5) man page of the documentation for Linux (UNIX) operating systems.</td>
</tr>
<tr>
<td></td>
<td>You can specify values in one of these fields or in any combination of fields.</td>
</tr>
</tbody>
</table>

Data Conversion Settings

Settings for converting data that is retrieved from an external source

These settings are only available when you have selected Web service or File on disk as the source of the data.

Table 7-7 Data Conversion Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data type</td>
<td>Lets you select the input format of the data that is converted.</td>
</tr>
<tr>
<td></td>
<td>You can select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Plain text — The data is in plain-text format</td>
</tr>
<tr>
<td></td>
<td>Each line appears as a separate entry in a converted list.</td>
</tr>
<tr>
<td></td>
<td>Optionally, you can specify a regular expression as a filtering term in the input field below. Only strings matching this term are then entered into the list.</td>
</tr>
<tr>
<td></td>
<td>If there is no grouping operator in the regular expression, the complete string is stored in a list. Otherwise, the data captured by the first group is stored.</td>
</tr>
<tr>
<td></td>
<td>• XML — The data is in XML format</td>
</tr>
<tr>
<td></td>
<td>You need to specify an XPath expression to select the data that is to be retrieved. Data can be retrieved, for example, according to XML tags or attributes.</td>
</tr>
<tr>
<td>Regular expression</td>
<td>Specifies a regular expression used to retrieve the data that is converted.</td>
</tr>
<tr>
<td></td>
<td>This option appears when you have selected Plain text under Data type.</td>
</tr>
</tbody>
</table>
Table 7-7 Data Conversion Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>XPath expression</td>
<td>Specifies an XPath expression used to retrieve the data that is converted. This option appears when you have selected <strong>XML text</strong> under <strong>Data type</strong>. For information on how to use XPath expressions, refer to appropriate documentation, for example, the XPath tutorial that is provided on the w3schools site.</td>
</tr>
<tr>
<td>XPath expression for second attribute (only for MapType)</td>
<td>Specifies an XPath expression for a second attribute used in retrieving Map Type conversion data. The data retrieved using the second attribute provides the value of a Map Type key-value pair. Data for the key is retrieved using a first attribute, which is configured by specifying an XPath expression in the XPath expression field. The number of entries that are retrieved from an external list using this XPath expression must be the same as the number of entries retrieved with the expression for the first attribute. The order in which entries are retrieved using the two expressions must also be the same.</td>
</tr>
</tbody>
</table>

Web Service Specific Parameters

Settings applying when the source of an external list is provided by a web service

These settings appear when Web service is selected in the **DataSource Type** section.

Table 7-8 Web Service Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web service's URL</td>
<td>Specifies the URL of a file on a web server that contains an external list and is provided by a particular web service (HTTP, HTTPS, or FTP). You can specify a placeholder inside the URL.</td>
</tr>
<tr>
<td>Specify authentication data</td>
<td>When selected, you can specify information for an authentication that must be performed successfully before data can be retrieved from a web service.</td>
</tr>
<tr>
<td>Type of HTTP authentication</td>
<td>Provides a list for selecting a type of HTTP authentication. Supported types are: None, Basic, Digest</td>
</tr>
<tr>
<td>User's name</td>
<td>Specifies a user name that is submitted for authentication.</td>
</tr>
<tr>
<td>User's password</td>
<td>Sets a password that is submitted for authentication. Click <strong>Set</strong> to open a window for settings a password.</td>
</tr>
<tr>
<td>Use next-hop proxy for access to server</td>
<td>When selected, access to the web server is achieved using a next-hop proxy server. After selecting this checkbox, the following three items become accessible.</td>
</tr>
<tr>
<td>List of next-hop proxy servers to use</td>
<td>Provides a list for selecting a list of servers that can be used as next-hop proxies to access a web server. Click <strong>Add</strong> or <strong>Edit</strong> to open windows for adding a new list or editing an existing list.</td>
</tr>
</tbody>
</table>
Table 7-8  Web Service Specific Parameters (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of certificate authorities</td>
<td>Provides a list for selecting a list of certificate authorities that can be used in SSL-secured communication with a web service. Click Add or Edit to open windows for adding a new list or editing an existing list.</td>
</tr>
<tr>
<td>List of additional HTTP headers</td>
<td>Provides a list for selecting headers that are added to an HTTP request after it has been received on an appliance.</td>
</tr>
</tbody>
</table>

The following table describes the elements of a entry in the List of additional HTTP headers.

Table 7-9  Additional HTTP headers – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header name</td>
<td>Specifies the name of a header that is added to an HTTP request.</td>
</tr>
<tr>
<td>Header value</td>
<td>Specifies the value of a header that is added to an HTTP request.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a header.</td>
</tr>
</tbody>
</table>

File Specific Parameters

Settings applying when the source of an external list is a file within your local file system

These settings appear when File on disk is selected in the Data Source Type section.

Table 7-10  File Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full path to the file</td>
<td>Specifies the path to the file within your local file system that is the source of an external list.</td>
</tr>
</tbody>
</table>

LDAP Specific Parameters

Settings applying when the source of an external list is an LDAP server

These settings appear when LDAP is selected in the Data Source Type section.

Table 7-11  LDAP Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP server’s URL</td>
<td>Specifies the name of the file from your local file system that is the source of an external list. You can specify a placeholder inside the URL. To restrict the possible location of the file, you can specify a part of your local file system when configuring the External Lists system settings. The file must be within the specified part then, for example, <code>opt/mwg/temp</code>.</td>
</tr>
<tr>
<td>List of certificate authorities</td>
<td>Provides a list for selecting a list of certificate authorities that can be used in SSL-secured communication with a web service. Click Add or Edit to open windows for adding a new list or editing an existing list.</td>
</tr>
<tr>
<td>User name</td>
<td>Specifies the user name the appliance submits when attempting to connect to the LDAP server.</td>
</tr>
</tbody>
</table>
### Table 7-11 LDAP Specific Parameters (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP password</td>
<td>Sets the password that an appliance submits when attempting to connect to an LDAP server. You can set or change the password using the Set/Change toggle button that is provided.</td>
</tr>
<tr>
<td>Search DN</td>
<td>Specifies the name of a domain in the database on an LDAP server that is searched for an external list. You can specify a placeholder inside this name.</td>
</tr>
<tr>
<td>Search scope</td>
<td>Lets you select the scope of the search for an external list on an LDAP server.</td>
</tr>
<tr>
<td></td>
<td>* Subtree — The complete subtree of the domain specified under Search DN is searched.</td>
</tr>
<tr>
<td></td>
<td>* One level — Only one level below the domain specified under Search DN is searched.</td>
</tr>
<tr>
<td></td>
<td>* Base — Only the base of the domain specified under Search DN is searched.</td>
</tr>
<tr>
<td>Search filter</td>
<td>Specifies a term for filtering the results of the search for an external list on an LDAP server.</td>
</tr>
<tr>
<td></td>
<td>Only if the name of an entry in the database matches the filtering term, the item that the entry represents is retrieved. You can specify a placeholder within this term.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Specifies the attribute of an item in the database on an LDAP server that is the intended search result, for example, an email address.</td>
</tr>
<tr>
<td>Second attribute (only for MapType)</td>
<td>Specifies a second attribute of a database item on an LDAP server that is the intended search result when the data for this item is Map Type data.</td>
</tr>
<tr>
<td>Enable LDAP version 3</td>
<td>When selected, version 3 of the LDAP protocol is used. If you disable this option, you need to provide the encoding that is used for communication with the LDAP server.</td>
</tr>
<tr>
<td>Allow LDAP library to follow referrals</td>
<td>When selected, referrals to locations outside the LDAP server that a search for an external list performed on can be followed to retrieve the list.</td>
</tr>
</tbody>
</table>

### Database Specific Parameters

Settings applying when the source of an external list is a database

These settings appear when **Database** is selected in the **Data Source Type** section.
Table 7-12  Database Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL query</td>
<td>Specifies a string to denote the type of query that is performed on a database. The default type of query used for retrieving external lists information is SELECT. You can put a ; (semicolon) at the end of the string, but this is not required. A query can also use placeholders to include variable data. If the $N placeholder is used, the data that is filled in as the value of the variable is &quot;escaped&quot; to prevent an SQL injection. Then a \ (backslash) is replaced with \\ (double backslash), and a ' (apostrophe) is preceded by a \ (backslash). An SQL query usually returns one data column. If you perform a query that returns multiple columns, only the first is used for external list content. To retrieve content from several columns, you need to specify combined columns for output, using appropriate SQL operators.</td>
</tr>
<tr>
<td>Type of database</td>
<td>Specifies the type of database that external list content is retrieved from. The following two types are available: • PostgreSQL • SQLite3 After selecting a database type, database specific parameters appear according to this type.</td>
</tr>
</tbody>
</table>

Table 7-13  PostgreSQL Database Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database host</td>
<td>Specifies the host name of the server that a database resides on.</td>
</tr>
<tr>
<td>Database port</td>
<td>Specifies the port number of the port on a database host that listens to queries for retrieving external list content. The default port number is 5432.</td>
</tr>
<tr>
<td>Name of database on database server</td>
<td>Specifies the name a database is known under on the database server.</td>
</tr>
<tr>
<td>Database user name</td>
<td>Specifies the user name of an appliance when connecting to a database server.</td>
</tr>
<tr>
<td>Database password</td>
<td>Sets a password for the user name of an appliance. The Set button opens a window for setting the password.</td>
</tr>
</tbody>
</table>

Table 7-14  SQLite Database Specific Parameter

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>File path to SQLite database</td>
<td>Specifies the full path to the file on an appliance that contains a database.</td>
</tr>
</tbody>
</table>

Advanced Parameters

Settings for advanced methods of handling external lists
Table 7-15  Advanced Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skip &quot;bad&quot; entries during data conversion</td>
<td>When selected, data that cannot be converted to the required type, such as Integer, Double, or Boolean, is omitted</td>
</tr>
<tr>
<td>Maximal number of entries to fetch</td>
<td>Limits the number of entries that are retrieved from an external list to the specified value.</td>
</tr>
<tr>
<td></td>
<td>The number can range from 0 to unlimited</td>
</tr>
<tr>
<td></td>
<td>We recommend that you specify a limit here to avoid high memory consumption in case of large lists.</td>
</tr>
<tr>
<td>Maximal size of entries to fetch</td>
<td>Limits the amount of data (in KB) that is retrieved from an external list.</td>
</tr>
<tr>
<td></td>
<td>The number can range from 0 to unlimited</td>
</tr>
<tr>
<td></td>
<td>We recommend that you specify a limit here to avoid high memory consumption in case of large lists.</td>
</tr>
<tr>
<td></td>
<td>This option is not available when the source of the external list is an LDAP server.</td>
</tr>
</tbody>
</table>

Configure general settings for external lists

You can configure settings applying to all external lists that are retrieved for use on the appliance.

Task

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance you want to configure settings for and click External Lists.

   The settings for the external lists appear on the settings pane.

3. Configure these settings as needed.

4. Click Save Changes.

External Lists system settings

The External Lists system settings apply to all external lists that are processed on the appliance.

Global Configuration

Setting for the internal cache on the appliance that stores external list data

Table 7-16  Global Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush External Lists Cache</td>
<td>Removes the data that is stored in the internal cache.</td>
</tr>
<tr>
<td>Time before retry after failure</td>
<td>Limits the time (in seconds) that the External Lists module remembers a failure to retrieve data from a particular external source to the specified value.</td>
</tr>
<tr>
<td></td>
<td>The module will not perform retries for a source as long as it remembers the failure.</td>
</tr>
<tr>
<td></td>
<td>We recommend that you keep the default value or modify it according to the requirements of your network.</td>
</tr>
<tr>
<td></td>
<td>This way you avoid adding load by constant retries to a web server that is already overloaded.</td>
</tr>
</tbody>
</table>
File Data Source Configuration
Setting for the local file system that external list data can be retrieved from

Table 7-17  File Data Source Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| File system allowed for file data access | Specifies the path that leads to the folder for storing external lists within your local file system.  
External lists that data is retrieved from must be stored in this folder.  
Otherwise an attempt to retrieve the data will lead to an access-denied error.  
When external list data is retrieved from an SQLite database, the path specified here is the path to the folder within your local file system that contains the database. |

Web Data Source Configuration
Setting for all web services that are the sources of external list data

Table 7-18  Web Data Source Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Check SSL certificate identity      | When selected, a certificate that a web server submits in SSL-secured communication under the HTTPS protocol is verified  
The verification is performed according to the SSL scanning rules that are implemented on the appliance.  
This can, for example, lead to an error if the web server uses a self-signed certificate. |

Map Type lists
Map Type lists, also known as maps, can be used to store pairs of keys and values mapped to each other. Both the keys and their values are of the string type. Lookup operations can be performed on existing maps, for example, to find out whether a particular key exists in a map or what value is mapped to a key. Other operations include setting and deleting values for a particular key or converting a complete map into a single string.

You can create and fill Map Type lists on the user interface of Web Gateway or retrieve them from a remote location using the external lists and subscribed lists functions. If you want to work with other data types for your maps, for example, numbers or IP addresses, you can convert them using properties such as Number.ToString or IP.ToString.

Create a Map Type list
To create a Map Type list, add a list of this type and fill it with pairs of keys and values.

Task
1. Select Policy | Lists.
2. Above the lists tree, click the Add icon.
   The Add List window opens.
3 Add a MapType list.
   a In the Name field, type a list name.
   b From the Type list, select MapType.
   c Click OK.

   The window closes and the new Map Type list appears on the lists tree under Custom Lists | MapType.

   The settings pane is ready for filling the list with entries.

4 Click the Add icon on the settings pane.

   The Add Map Type window opens.

5 For each pair of entries, you need to fill the list as follows.
   a In the key field, type a key name.
   b In the value field, type a value.
   c Click OK.

   The window closes and the pair of entries appears in the first row on the settings pane.

6 Click Save Changes.

Using properties to work with Map Type lists

There are several properties for working with Map Type lists. Using these properties in rule criteria, you can retrieve information about a Map Type list, modify a list, create a new list, and also convert a list into a string.

To retrieve information about a Map Type list (map), you can:

- Retrieve a map that you specify a name for
- Retrieve a list of the keys in a map
- See whether a particular key exists within a map
- Retrieve the value for a given key in a map
- Retrieve the number of key-value pairs in a map

The following properties are used to perform these activities.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map.ByName</td>
<td>Provides a map with the name that you specified.</td>
</tr>
<tr>
<td>MapHasKey</td>
<td>Is true if the specified map includes the specified key.</td>
</tr>
<tr>
<td>Map.Size</td>
<td>Provides the number of key-value pairs in a map.</td>
</tr>
<tr>
<td>Map.GetKeys</td>
<td>Provides a list of the keys in a map.</td>
</tr>
<tr>
<td>Map.GetStringValue</td>
<td>Provides the string that is the value of the specified key in the specified map.</td>
</tr>
</tbody>
</table>

You can, for example, use the Map.GetStringValue property in the criteria of a rule to see whether a key in a list has a particular value. The key could be a user name and the value a string that serves as a token for authentication.

The criteria would then be configured as follows:

Map.GetStringValue (testmap, "sampleuser") equals "sampletoken"
If the *sampleuser* key has *samplertoken* as its value, the criteria matches, and the rule executes a particular action, for example, *Continue*.

When a map is modified, the modification is applied to a copy of the original map, while the original map itself remains unmodified. To modify a map in this way, you can:

- Set a key to a particular value
- Delete a key

The following properties are used to perform these activities.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map.SetStringValue</td>
<td>Provides a map in which the specified value is set for the specified key.</td>
</tr>
<tr>
<td>Map.DeleteKey</td>
<td>Provides a map in which the specified key is deleted.</td>
</tr>
</tbody>
</table>

To create a new map or convert a map into a string, the following properties are used.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map.CreateStringMap</td>
<td>Provides a new map, which is still empty.</td>
</tr>
<tr>
<td>Map.ToString</td>
<td>Provides a map converted into a string.</td>
</tr>
</tbody>
</table>

**Retrieving map data from external and subscribed lists**

Data for Map Type lists (maps) can be retrieved from external and subscribed lists.

**External lists**

For retrieving map data from an external list, the *ExtLists.StringMap* property is provided, which you can use in the criteria of a suitable rule. The value of this property is a list of maps that have an external list as their source.

For example, to find out whether a particular key is contained in a list that is retrieved from an external source, you can configure the following rule criteria:

```
Map.GetKeys(ExtLists.StringMap(" " , " " , " ")<External Lists>) contains "samplekeyname"
```

To specify the external list and where it can be retrieved from, you need to configure the settings of the External Lists module, which is the module that performs the retrieval. In the above criteria, these settings appear under the name of *External Lists*. 
External list data can be retrieved from a web service, a file, a PostgreSQL or SQLite3 database, or using LDAP. For these source types, the following must be observed when configuring the retrieval of data for a map:

- **Web service or file**
  
  The type of data that is retrieved from a web service or a file must be *Plain Text*.
  
  To locate the data, a regular expression is used that includes two parts. The first part is for the keys, the second for the values.

- **Databases**
  
  The database query for retrieving the data must return two columns. The first column delivers the keys, the second column delivers the values.

- **LDAP**
  
  To retrieve the data, a first and a second attribute are configured within the LDAP settings. The first attribute delivers the keys, the second attribute delivers the values.

**Subscribed lists**

Entries in subscribed lists that map data is retrieved from must have the following format.

```xml
<listEntry>
  <complexEntry defaultRights="2">
    <configurationProperties>
      <configurationProperty key="key" type="com.scur.type.string" value="key"/>
      <configurationProperty key="value" type="com.scur.type.string" value="value"/>
    </configurationProperties>
  </complexEntry>
  <description></description>
</listEntry>
```

Within the *listEntry* element, there’s a *complexEntry* embedded. This allows the Subscribed Lists module to process the format.

**Common Catalog**

The Common Catalog provides lists that can be pushed from a McAfee ePO server to a Web Gateway appliance.

The following types of lists can be pushed: IP address, domain name, string, wildcard expression.

- Do not modify the content of the lists on the Web Gateway appliance, because this content is updated in intervals on the McAfee ePO server. These updates will overwrite any changes that you might have applied.

A REST (Representational State Transfer) interface runs internally on both systems to enable the list transfer. A McAfee ePO extension for Web Gateway must also be running on the McAfee ePO server.

This extension includes a help extension, which provides online Help for handling the extension. An extension package is provided on the user interface of Web Gateway under the *ePolicy Orchestrator* system settings.

To let requests from the McAfee ePO server bypass filtering by web security rules on Web Gateway, you need to import a suitable rule set from the library, place it at the topmost position of the rule sets tree, and enable it.
In addition to this, you need to set up a McAfee ePO user account, as there must be an instance on the appliance that is allowed to handle the list transfer. For setting up this account, the ePolicy Orchestrator system settings are used.

The user of the McAfee ePO account must also appear as an administrator with an account among the internal Web Gateway administrator accounts.

After lists from the Common Catalog have been pushed to Web Gateway, they appear on the Lists tab of its user interface. A prefix in the list name indicates that a McAfee ePO server is the source of a list. You can use these lists to configure rules like any other lists on the Lists tab.

**Prepare the use of Common Catalog lists**

To prepare the use of Common Catalog lists that are pushed from a McAfee ePO server to a Web Gateway appliance, complete the following high-level steps.

**Task**

1. Set up an account for a McAfee ePO user on Web Gateway.
2. Set up an administrator account with the same user name and password on Web Gateway.
3. Enable use of the REST interface on Web Gateway.
4. Import the Bypass ePO Requests rule set from the library on the user interface of Web Gateway, move it to the topmost position of the rule sets tree, and enable it.
5. Download a McAfee ePO extension package for Web Gateway and install it on the McAfee ePO server.
6. On the user interface of the McAfee ePO server, register a new server for communication with Web Gateway, specifying an appliance that Web Gateway runs on.

   On the dashboard of the user interface, you should see, after about 15 minutes, data on web traffic that is processed on Web Gateway.

7. Push lists from the McAfee ePO server to Web Gateway.

You should see the lists that you have pushed to Web Gateway on the lists tree of its user interface.

For more information on how to install a McAfee ePO extension package and perform activities on the McAfee ePO server, refer to the McAfee ePO documentation.

**Set up a user account for Common Catalog lists**

To enable the use of Common Catalog lists, you must set up a McAfee ePO user account on Web Gateway to create an instance that is allowed to handle the list transfer.

**Task**

1. Select Configuration | ePolicy Orchestrator.
2. Under ePolicy Orchestrator Settings, configure a user account.
   a. In the ePO user account field, leave the preconfigured value, which is epo.
   b. Next to the Password field, click Change.
      
      The New Password window opens.
   c. Use the window options to set a new password.
3 Make sure Enable data collection for ePO is selected.

4 Click Save Changes.

The user of the McAfee ePO account that you have configured must also appear as an administrator in an administrator account on Web Gateway.

**Set up an administrator account for Common Catalog lists**

To enable the use of Common Catalog lists, you must set up an administrator account on Web Gateway with the same user name and password as for the McAfee ePO user account.

**Task**

1 Select Accounts | Administrator Accounts.

2 Under Internal Administrator Accounts, click Add.

The Add Administrator window opens.

3 Set up an administrator account for using Common Catalog lists.

a In the User name field, type epo.

b In the Password and Password repeated fields, type the password you configured when setting up the user account for the ePO user.

c From the Role list, select the ePO Common Catalog Administrator role.

d Click Edit to review the current role settings.

The Edit Role window opens. Enable the following settings if necessary:

- Policy — Lists accessible
- Policy — Lists creation
- REST Interface accessible

e Click OK.

The window closes and the new administrator account appears under Internal Administrator Accounts.

Together with the user account for the McAfee ePO user, this administrator account serves as the instance on Web Gateway that must exist for handling the transfer of lists from a McAfee ePO server.

**Enable use of the REST interface for Common Catalog lists**

For communication with the McAfee ePO server that Common Catalog lists can be transferred from, you need to enable the internal REST (Representational State Transfer) interface on Web Gateway.

**Task**

1 Select Configuration | Appliances.

2 On the appliances tree, select the appliance that you want to transfer Common Catalog lists to and click User Interface.

3 Under UI Access, select both Enable Rest Interface over HTTP and Enable Rest Interface over HTTPS.

4 Under Login Page Options, select Allow multiple logins per login name.

5 Click Save Changes.
Sample settings for registering Web Gateway on a McAfee ePO server

To transfer Common Catalog lists to a Web Gateway appliance, you must register the appliance as a new server on the McAfee ePO server.

The following are sample settings for this registration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Sample value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server type</td>
<td>McAfee Web Gateway 7</td>
</tr>
<tr>
<td>Name</td>
<td>mwg7-3.sample-lab.local</td>
</tr>
<tr>
<td>Notes</td>
<td>(optional)</td>
</tr>
<tr>
<td>Host name</td>
<td>mwg7-3.sample-lab.local</td>
</tr>
<tr>
<td>Host address</td>
<td>171.18.19.226</td>
</tr>
<tr>
<td>Administration port</td>
<td>4712</td>
</tr>
<tr>
<td>Statistics retrieval port</td>
<td>9090</td>
</tr>
<tr>
<td>User name (for access to the host GUI)</td>
<td>&lt;Initial or current user name for access to the Web Gateway user interface&gt;</td>
</tr>
<tr>
<td>Password</td>
<td>&lt;Initial or current password for access to the Web Gateway user interface&gt;</td>
</tr>
<tr>
<td>User name (for statistics retrieval and list management)</td>
<td>epo</td>
</tr>
<tr>
<td>Password</td>
<td>&lt;Same password as the one that was configured for the ePO user and administrator accounts on Web Gateway&gt;</td>
</tr>
<tr>
<td>Options</td>
<td>Allow ePO to manage lists on this system (enabled)</td>
</tr>
</tbody>
</table>

The initial user name and password for access to the user interface of Web Gateway are admin and webgateway.

JavaScript Object Notation data

Data that is encoded in JavaScript Object Notation (JSON) format can be read, modified, and created on Web Gateway.

JavaScript Object Notation is a text-based data-interchange format. It can be read easily by JavaScript, but is not tied to using this language. The notation is used for communication with interactive websites, as well as with NoSQL and document-oriented databases, for example, MongoDB or Couch DB.

JSON-based programming interfaces exist for use in well-known social networks, such as Facebook or Twitter.

On Web Gateway, JSON data is used, for example, in scanning reports that are provided by McAfee® Advanced Threat Defense (Advanced Threat Defense). Lists that are retrieved form external sources and processed on Web Gateway can also be in JSON data format.

**JSON data**

JSON data is made available in what is called *objects*. A JSON object is a container that includes data of the same or of different ordinary types, such as strings, numbers, and others.
The basic structure of a JSON object can be represented as follows:

```
object: {"key": value, "key": value, ...}
```

For example:

```
Employee: {"First name": "Joe", "Last name": "Miller", "Age": 32}
```

The value of a JSON element can be data of the following types: string, number, Boolean, null.

A JSON object can also include an array:

```
object: {"key": value, "key": value, array: [value, value, ...]}
```

For example:

```
Employee: {"First name": "Joe", "Last name": "Miller", "Children": [Ian, Lisa]}
```

In original JavaScript Object Notation, only objects and arrays can occur at the top level of a hierarchical data structure. However, when it is supported on Web Gateway, a simple element can also occur in top-level position.

A JSON object can also be embedded in another JSON object.

**Using properties to handle JSON data**

Several properties are available on Web Gateway for reading, modifying, and creating JSON data.

For example, the `JSON.FromString` property is used to create a JSON element from a string. The string is specified as a parameter of the property. So `JSON.FromString("Miller")` delivers the string "Miller" as the value of a JSON element.

A JSON object is created using the `JSON.CreateObject` property. This object is initially empty. To store a JSON element inside an object, you need to identify both items by giving them names.

An object is given a name by making it a user-defined property, which is always configured with a name.

For example, you can create a user-defined property under the name `User-Defined.myjsonemployee` and then use an event in a rule to give it the value of the `JSON.CreateObject` property.

**Name**

**Create JSON object as user-defined property**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>-&gt; Continue</td>
<td>Set User-Defined.myjsonemployee = JSON.CreateObject</td>
</tr>
</tbody>
</table>

The empty JSON object `User-Defined.myjsonemployee` can be filled using the `JSON.StoreByName` property, which has parameters for object name, element key, and element value.

For example, the following stores an element with the key "Last name" and the value "Miller" in the object:

```
JSON.StoreByName(User-Defined.myjsonemployee, "Last name", JSON.FromString("Miller"))
```
Storing an element inside an object can also be performed in a simpler way:

- You need not create the object before using the JSON.StoreByName property. Specifying the object name as a parameter of the property creates the object if it did not exist before.
- You need not use the JSON.FromString property to obtain the element value. Specifying a string directly also creates this value. The same applies to the other ordinary data types that the value of a JSON element can have.

So, the following also stores an element inside an object:

```
JSON.StoreByName(User-Defined.myjsonemployee, "Last name", "Miller")
```

### Groups of JSON properties

Many JSON properties are similar to other properties in that they are used to perform the same kind of data handling activity.

The JSON.From<x> properties, for example, JSON.FromString, deliver a JSON element that has the value of a simple data type. The value of the simple data type is specified as the parameter of the JSON property.

The following are some important groups of JSON properties:

- **JSON.From<x>** = Delivers a JSON element that has the value of a simple data format
  
  Properties: `JSON.FromString`, `JSON.FromNumber`, `JSON.FromBool`, `JSON.FromStringList`, `JSON.FromNumberList`

- **JSON.As<x>** = Delivers the value of a JSON element in a simple data format
  
  The properties of this group are used to perform an operation that is the reverse of what the JSON.From<x> properties do.

  For these properties to work correctly, the format of the JSON element must match the simple data format.

  For example, the JSON.AsString property will only deliver a (simple) string if the value of the JSON element is a (JSON) string.

  Properties: `JSON.AsString`, `JSON.AsNumber`, `JSON.AsBool`

- **JSON.Create<x>** = Creates a JSON object, array, or the element value 0.
  
  Properties: `JSON.CreateObject`, `JSON.CreateArray`, `JSON.CreateNull`

- **JSON.Get<x>** = Delivers a JSON element from within an object or the data type of an element
  
  `JSON.GetByName` delivers an element that is identified by its key from within a JSON object.

  `JSON.GetAt` delivers an element that is identified by its position within a JSON array.

  `JSON.GetType` delivers the type of an element.

### Using JSON properties in filtering rules

The `JSON.ToString` property delivers the value of a JSON element in string format.

You can use this property, for example, in a simple rule to whitelist a particular client IP address.
In this rule, a given client IP address is compared to the client IP address you want to whitelist to see whether both addresses match.

**Name**

**Allow client IP address provided as JSON element value**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client.IP equals String.ToIP(JSON.ToString(User-Defined.myjsonipaddress))</td>
<td>-&gt; StopCycle</td>
</tr>
</tbody>
</table>

The client IP address that is to be whitelisted is provided as the value of the user-defined property User-Defined.myjsonipaddress.

The JSON.ToString property delivers this value in string format. The String.ToIP property converts the string back into an IP address, so it can be compared to the address that is the value of the Client.IP property at the beginning of the rule.

Before the UserDefined.myjsonipaddress property can be used in the sample rule, you must create it in JSON data format and set its value to the address that is to be whitelisted.

To set the value, you can use an event in another sample rule, as shown in the following.

**Name**

**Set value of JSON type user defined property to client IP address**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>-&gt;</td>
<td>Continue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set User-Defined.myjsonipaddress = JSON.FromString (&quot;10.149.8.34&quot;)</td>
</tr>
</tbody>
</table>

The JSON.FromString property in the rule event converts the client IP address, which is specified as a property parameter in string format, into the value of a JSON element.

**Retrieving JSON data from an Advanced Threat Defense report**

When Advanced Threat Defense is called by a rule on Web Gateway to scan a web object, the scanning result is stored as the value of the AntiMalware.MATD.Report property.

The result is provided as a string that has the elements of the result arranged in JSON style. It can be converted into a JSON element, using the JSON.ReadFromString property. This property takes the AntiMalware.MATD.Report property as a parameter.

The JSON element can then be set as the value of a user-defined property.

The rule that uses these properties could look as follows:

**Name**

**Set value of JSON type user defined property to Advanced Threat Defense report**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>-&gt;</td>
<td>Continue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set User-Defined.myjsonmatdreport = JSON.ReadFromString (AntiMalware.MATD.Report)</td>
</tr>
</tbody>
</table>

You can retrieve the data of the result using the JSON.GetByName property and, for example, write it into a log file.

**Name**

**Write JSON data from Advanced Threat Defense report into log file**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
</table>
In the event of this rule, "Summary" is the key of a JSON element that has the data of a scanning result as its value. This key and its value are contained in a JSON object, which is the value of the Antimalware.MATD.Report property.

The structure of the JSON object is shown in the following.

It contains several embedded objects. The element keys are the ones that are actually used in a report, while the values are examples.

```json
Report: {
    "Summary": {
        "Selectors": [{
            "Engine": "GAM engine",
            "MalwareName": "EICAR test file",
            "Severity": "5"
        }],
        "Verdict": {
            "Severity": "5",
            "Description": "Subject is malicious"
        },
        "Stats": [{
            "ID": "0",
            "Category": "Persistence, Installation Boot Survival",
            "Severity": "5"
        }]
    }
}
```

**Retrieving external lists in JSON data format**

For handling JSON data in a list that has been retrieved from an external source, the `Ext.Lists.JSON` property is available. After retrieving the external list, the list content is a JSON element that is the value of this property.

Like all external list properties, `Ext.Lists.JSON` has three parameters in string format, which can be used to identify the external source.
Lists
JavaScript Object Notation data
Settings

Settings are used within Web Gateway for configuring modules (engines), rule actions, and system functions.

Settings names appear in different places on the user interface, for example, in the criteria, action, and events of rules or on the Settings and Appliances tabs.

After clicking a settings name, you can access and configure the parameters and values of the settings.

At the initial setup of the appliance, module and action settings are implemented together with the rule set system, as well as settings for the appliance system. Additional module and action settings are implemented when you import a rule set from the rule set library.

You can review and modify the initially implemented or imported settings. You can also completely delete module and action settings and create module and action settings of your own.

Contents

- Types of settings
- Settings tab
- Access settings
- Create action and module settings

Types of settings

Different types of settings are used in rule processing and with other functions on the appliance.

- **Module settings** — Settings for the modules (also known as engines) that are called by rules to deliver values for properties and perform other jobs
- **Action settings** — Settings for the actions that rules execute
- **System settings** — Settings of the appliance system

Module settings

Module settings are settings for the modules (also known as engines) that are called by rules to deliver values for properties and perform other jobs.

For example, the URL Filter module retrieves information on URL categories to deliver values for the URL.Categories property in a filtering rule.

In a rule, the settings name for a module that is called by the rule appears next to a rule property. For example, in a rule for virus and malware filtering, *Gateway Antimalware* can appear as the settings name next to the *Antimalware.Infected* property.
This means that when the Anti-Malware module is called to deliver the value true or false for the property, the module runs with the Gateway Antimalware settings. These settings specify, for example, which methods are used in scanning web objects for infections.

You can access module settings in rules and on the lower main branch of the settings tree on the Settings tab.

You can modify these settings and also create new settings.

**Action settings**

Action settings are settings for the actions that are executed by rules.

They are mainly configured to specify the messages that are sent to users who are affected by rule actions, such as Block or Authenticate. Actions that do not affect users have no settings, for example, Continue or Stop Rule Set.

You can access these settings in rules and on the upper main branch of the settings tree on the Settings tab.

You can modify these settings and also create new settings.

**System settings**

System settings are settings of the appliance system, for example, network interface settings or domain name system settings.

You can access these settings on the Appliances tab of the Configuration top-level menu.

You can modify these settings, but not create new system settings.
**Settings tab**

Use the **Settings** tab to work with settings for actions and modules (engines).

---

**Main elements of the Settings tab**

The following table describes the main elements of the **Settings** tab.

### Table 8-1 Main elements of the Settings tab

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings toolbar</td>
<td>Controls for working with settings for actions and modules (engines)</td>
</tr>
<tr>
<td>Settings tree</td>
<td>Tree structure displaying actions and modules (engines)</td>
</tr>
<tr>
<td>Settings</td>
<td>Parameters and values of the currently selected action or module (engine)</td>
</tr>
</tbody>
</table>

**Settings toolbar**

The settings toolbar provides the following options.

### Table 8-2 Settings toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Opens the <strong>Add Settings</strong> window for creating new settings.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the <strong>Edit Settings</strong> window for editing existing settings.</td>
</tr>
</tbody>
</table>
### Table 8-2 Settings toolbar (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Deletes the selected settings. A window opens to let you confirm the deletion.</td>
</tr>
<tr>
<td>Expand all</td>
<td>Expands all collapsed items on the settings tree.</td>
</tr>
<tr>
<td>Collapse all</td>
<td>Lets all expanded items on the settings tree collapse.</td>
</tr>
</tbody>
</table>

### Access settings

You can access settings on the **Settings** tab or by clicking a settings name in a rule. For accessing system settings, you must work with the **Appliance** tab of the **Configuration** top-level menu.

### Tasks

- **Access action and module settings on the Settings tab** on page 240
  You can use the **Settings** tab to access settings for actions and modules.

- **Access action and module settings in a rule** on page 240
  You can click names of settings for actions and modules that appear in rules to access these settings.

- **Access system settings** on page 241
  You can access system settings using the **Configuration** top-level menu.

### Access action and module settings on the Settings tab

You can use the **Settings** tab to access settings for actions and modules.

#### Task

1. Select Policy | **Settings**.

2. On the settings tree, navigate to the **Actions** or **Engines** branch to access the settings you want to work with.

3. To select settings, do one of the following:
   - On the **Actions** branch, click an action to expand it, and select the action settings you want to access.
   - On the **Engine** branch, click a module (also known as engine) to expand it, and select the module settings you want to access.

   The parameters and values of the settings appear on the settings pane.

   You can now work with the settings.

### Access action and module settings in a rule

You can click names of settings for actions and modules that appear in rules to access these settings.

#### Task

1. Select Policy | **Rule Sets**

2. On the rule sets tree, select the rule set that contains the rule with the settings you want to access.

   The rules of the rule set appear on the settings pane.
3 Make sure Show details is selected.

4 In the rule with the settings you want to access, click the settings name:
   • In the rule criteria to access module settings
   • In the rule action to access action settings

   The Edit Settings window opens with the settings that you selected.

You can now work with the settings.

**Access system settings**
You can access system settings using the Configuration top-level menu.

**Task**
1 Select Configuration | Appliances

2 On the appliances tree, select the appliance you want to configure system settings for and click the settings name.

   The parameters and values of the settings appear on the settings pane.

You can now work with the settings.

**Create action and module settings**
You can create settings for modules and actions.

When creating these settings, you do not create them completely new, but use existing settings that you give a new name and modify as needed.

**Task**
1 Select Policy | Settings.

2 To select the settings that serve you as the starting point for creating new settings, use one of the following two methods:
   • On the settings tree, select these settings and click Add.
     
     The Add Settings window opens with the parameters and values of the selected settings.
   • Click Add right away.
     
     The Add Settings window opens.
     
     Select settings from the Settings for pane of the window.
     
     The parameters and values of these settings appear in the window.

3 In the Name field of the window, type a name for the new settings.

4 [Optional] In the Comment field, type a plain-text comment on the settings.

5 Modify the existing values of the settings as needed.

6 [Optional] Click the Permissions tab and configure who is allowed to access the settings.
7 Click OK.

The window closes and the new settings appear on the settings tree.

8 Click Save Changes.
Authentication

Users can be “filtered” on an appliance, which means you can allow web access only for those who are able to authenticate.

Authentication is not implemented by default, but there are preconfigured authentication rule sets, which you can use.

The types of authentication that you can implement include:

• **Standard authentication** — You can configure authentication for users who send requests for web access under a standard protocol, such as HTTP, HTTPS, or FTP.

  When the authentication rule set of the default rule set system is enabled, user information is by default retrieved from an internal user database.

  You can change this setting and configure a different method, such as NTLM, LDAP, Kerberos, and others.

• **Instant messaging authentication** — You can configure authentication for users who send requests for web access under an instant messaging protocol, such as Yahoo, Windows Live Messenger, ICQ, and others.

You can also control administrator access to an appliance by setting up and maintaining administrator accounts and roles.

**Contents**

- Authenticating users
- LDAP digest authentication
- Configure authentication
- Configure the Authentication module
- Authentication settings
- Implement a different authentication method
- Using system settings to configure authentication
- Best practices - Configuring authentication for deployment types
- Best practices - Configuring LDAP authentication
- Instant messaging authentication
- One-time passwords
- Client Certificate authentication
- Administrator accounts
Authenticating users

Authenticating the users of your network ensures that they cannot access the web if they are not successfully authenticated. The authentication process looks up user information, for example, in an internal database or on a web server and blocks or allows access accordingly.

The process includes several elements, which contribute to it in different ways.

- Authentication rules control the process.
- The Authentication module, which is called by the rules, retrieves information about users from a database.

An authentication process is not implemented by default on Web Gateway after the initial setup. You can implement a process by importing suitable rule sets from the rule set library and modify this process to adapt it to the requirements of your web security policy.

To configure authentication, you can work with:

- **Key elements of rules** — After importing the library rule sets for authentication and clicking them on the rule sets tree, you can view and configure key elements of the rules for the authentication process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the rules for the authentication process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

**Authentication rules**

Authentication rules usually include a rule that asks an unauthenticated user to authenticate and blocks requests from users who cannot be successfully authenticated.

There can also be whitelisting rules that allow users who send a request to skip authentication, for example, depending on the IP address that a request was sent from or the URL that is requested.

Rule sets with rules for several types of authentication, for example, IM and cookie authentication, are available in the rule sets library.

**Authentication module**

The Authentication module is also known as Authentication engine. It retrieves information about users from a database. The module is called by the rules that need to know whether a user who requests access to a web object is authenticated.

Different methods of retrieving this information can be used:

- **NTLM** — Uses a database on a Windows domain server

- **NTLM Agent** — Uses an external agent on a Windows-based system for applying the NTLM authentication method

- **User Database** — Uses an internal database on the appliance

  - This method is used by default when the rule set of the default rule set system is enabled.

- **LDAP** — Uses a database on an LDAP server
- **Novell eDirectory** — Uses data from a directory on a server that takes the role of an LDAP server
- **RADIUS** — Uses a database on a RADIUS server
- **Kerberos** — Uses a database on a Kerberos server
- **Authentication Server** — Uses a database on another external server

You can configure settings for the Authentication module to specify the authentication method and other parameters of the authentication process.

### LDAP digest authentication

The LDAP digest authentication method, which is based on the LDAP authentication method, uses a shared secret known by both sides of the authentication process: a user requesting web access, using a browser on a client of Web Gateway, and Web Gateway.

Web Gateway uses its proxy functions to intercept the request to enable authentication and further filtering under the configured web security policy.

Unlike simpler authentication methods, such as basic authentication, no password is sent directly from the browser to Web Gateway. Instead the password is a part of the shared secret that is known on both sides of the authentication process.

A hash value is calculated for the shared secret and several additional parameters on the client and transmitted to Web Gateway, which calculates the hash again, using its instance of the shared secret, to see if the result is identical. If it is, the user is authenticated.

The hash value that is transmitted from the client to Web Gateway is also referred to as *digest*. Web Gateway retrieves the shared secret that it requires for recalculating the hash from an LDAP server.

#### Calculating a hash for LDAP digest authentication

The MD5 method for calculating a hash is used when LDAP digest authentication is performed in an authentication process with Web Gateway.

Before the client sends the hash, Web Gateway sends a request for authentication to the client, including a so-called *nonce* (number only once), which is a number that is randomly created on Web Gateway and is one of the parameters that must be used in addition to the shared secret for calculating the hash.

The complete list of parameters that is used for calculating the hash includes the following:

- User name (part of the shared secret)
- Realm name (part of the shared secret)
- Password (part of the shared secret)
- Nonce
- HTTP request that was sent from the client
- URL of the requested destination in the web

#### Configuring LDAP digest authentication on Web Gateway

LDAP digest authentication on Web Gateway requires the following:

- LDAP authentication must have been configured as the general authentication method on Web Gateway.
- The realm name must be configured as part of the common authentication settings on Web Gateway. This name must also be used for the shared secret.
You must configure the following parameters for LDAP digest authentication:

- Enabling of LDAP digest authentication
- Name of the attribute on the LDAP server that stores the authentication hash
- Maximum number of times that a nonce can be used
- Maximum time that a nonce can be used

Optionally, you can do the following.

- Allow only LDAP digest authentication as an authentication method under the current settings
  When configuring other authentication settings, you could, however, still allow other authentication methods, for example, the User database method with basic authentication.

- Let a check be performed for the URL that a client sends as a parameter for calculating the hash
  This URL should be the same as the URL that this client sends in its request for accessing a particular destination in the web. Otherwise successfully passing digest authentication, based on identical hash values, might allow a user to access a destination that was not requested. So if the result of the check is that both URLs are not the same, the request is blocked.

  As the browsers that are used on clients for sending this information use different URL formats, this check might fail, however, due to the formatting problem, even if two URLs are really the same. For this reason, the URL check is optional.

The realm name that is used for the shared secret is configured under Common Authentication Parameters, which is a section that is available under every authentication method at the beginning of the Authentication settings.

The parameters for LDAP digest authentication are configured on Web Gateway as part of the settings for the Authentication module (or engine).

When LDAP is selected as the general authentication method at the beginning of these settings, a section named Digest Authentication becomes available after the section for other LDAP specific parameters.

See also
Authentication settings on page 247

Configure authentication
You can implement authentication and adapt it to the needs of your network.
Complete the following high-level steps.

Task
1 Enable the Authenticate and Authorize rule set of the default rule set system.
2 Review the nested Authenticate with User Database rule set.
   This rule set contains a single rule, which asks unauthenticated users to authenticate.

   The rule criteria includes settings for the Authentication module, which specify use of the User Database authentication method. This means information for authenticating users is retrieved from an internal database on the appliance.

3 Modify the default rule set as needed.
You can, for example, do the following:

- Modify the common parameters of the Authentication module
- Modify the specific parameters for the User Database method
- Implement a different authentication method, for example, NTLM or LDAP
- Modify the specific parameters for the new authentication method

4 Consider importing a rule set from the library to implement authentication for a different type of communication, for example, instant messaging authentication.

5 Save your changes.

**Configure the Authentication module**

You can configure the Authentication module to modify the way user information is retrieved to authenticate users.

**Task**

1 Select **Policy ▶ Rule Sets**.

2 On the rule sets tree, select the rule set for authentication.
   In the default rule set system, this is the **Authenticate and Authorize** rule set.

3 Select a rule that controls user authentication and click the settings that are specified in the rule criteria.
   In the rule set of the rule set system, this is, for example, the rule **Authenticate with User Database** in the nested **Authenticate with User Database** rule set and the settings name is **User Database**.
   The **Edit Settings** window opens. It provides the settings for the Authentication module.

4 Configure these settings as needed.

5 Click **OK** to close the window.

6 Click **Save Changes**.

**See also**

*Authentication settings on page 247*

**Authentication settings**

The Authentication settings are used for configuring the method the Authentication module applies when it is looking up information about users in the authentication process.

**Authentication Method**

Settings for selecting an authentication method
Table 9-1 Authentication Method

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication method</td>
<td>Provides a list for selecting an authentication method.</td>
</tr>
<tr>
<td></td>
<td>You can select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• NTLM</td>
</tr>
<tr>
<td></td>
<td>• NTLM-Agent</td>
</tr>
<tr>
<td></td>
<td>• User Database</td>
</tr>
<tr>
<td></td>
<td>• LDAP</td>
</tr>
</tbody>
</table>

If you want to configure Secure LDAP, also known as LDAPS, you must work with LDAP version 3.

This version can be selected under LDAP Specific Parameters. It is by default selected.

• RADIUS
• Kerberos
• SSL Client Certificate
• Authentication Server
• One-Time Password
• SWPS (McAfee® Client Proxy)

After selecting a method, settings that are specific to it appear below the common settings.

Authentication Test

Settings for testing whether a user with given credentials would be authenticated

Table 9-2 Authentication Test

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Specifies the user name that is tested.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the tested password.</td>
</tr>
<tr>
<td>Authenticate User</td>
<td>Executes the test.</td>
</tr>
<tr>
<td>Test result</td>
<td>Displays the outcome of the test.</td>
</tr>
</tbody>
</table>

Common Authentication Parameters

Settings common to all authentication methods

There is also an advanced setting that is common to all authentication methods. It is described at the end of this main section after the last of the subsections for the specific authentication parameters.

Table 9-3 Common Authentication Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Realm</td>
<td>Specifies the location of the proxy that receives requests from users who are asked to authenticate.</td>
</tr>
<tr>
<td>Authentication attempt timeout</td>
<td>Limits the time (in seconds) that elapses before the authentication process terminates if not completed successfully to the specified value.</td>
</tr>
</tbody>
</table>
Table 9-3 Common Authentication Parameters (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use authentication cache</td>
<td>When selected, authentication information is stored in a cache. Authentication is then based on this stored information, rather than on information retrieved from an authentication server or the internal user database.</td>
</tr>
<tr>
<td>Authentication cache TTL</td>
<td>Limits the time (in minutes) that authentication information is stored in the cache to the specified value.</td>
</tr>
</tbody>
</table>

**NTLM Specific Parameters**

Settings for the NTLM authentication method

Table 9-4 NTLM Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default NTLM domain</td>
<td>Specifies the name of the default Windows domain used for looking up authentication information. This is one of the domains you have configured on the Appliances tab of the Configuration top-level menu.</td>
</tr>
<tr>
<td>Get global groups</td>
<td>When selected, information on global user groups is searched for on the Windows domain server.</td>
</tr>
<tr>
<td>Get local groups</td>
<td>When selected, information on local user groups is searched for on the Windows domain server.</td>
</tr>
<tr>
<td>Prefix group name with domain name (domain\group)</td>
<td>When selected, the name of the Windows domain appears before the name of the user group when authentication information on this group is sent from the domain server.</td>
</tr>
<tr>
<td>Enable basic authentication</td>
<td>When selected, the basic NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then sent in plain-text format (less secure) to the Windows domain server.</td>
</tr>
<tr>
<td>Enable integrated authentication</td>
<td>When selected, the integrated NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then encrypted before it is sent to the Windows domain server.</td>
</tr>
<tr>
<td>Enable NTLM cache</td>
<td>When selected, NTLM authentication information is stored in this cache. Authentication is then based on this stored information, rather on information retrieved from the Windows domain server.</td>
</tr>
<tr>
<td>NTLM cache TTL</td>
<td>Limits the time (in seconds) that authentication information is stored in this cache to the specified value.</td>
</tr>
<tr>
<td>International text support</td>
<td>Specifies a set of characters used by default for a request sent from a client, for example, ISO-8859-1.</td>
</tr>
</tbody>
</table>

**NTLM Agent Specific Parameters**

Settings for the NTLM Agent authentication method
### Table 9-5  NTLM Agent Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use secure agent connection</td>
<td>When selected, the connection used for communicating with the NTML Agent is SSL-secured.</td>
</tr>
<tr>
<td>Authentication connection timeout in seconds</td>
<td>Limits the time (in seconds) that elapses before the connection to the NTLM Agent is closed if no activities occur on it to the specified value.</td>
</tr>
<tr>
<td>Agent Definition</td>
<td>Provides a list for entering the agents that are involved in performing NTLM authentication.</td>
</tr>
<tr>
<td>Default NTLM domain</td>
<td>Specifies the name of the default Windows domain used for looking up authentication information.</td>
</tr>
<tr>
<td></td>
<td>This is one of the domains you have configured on the Appliances tab of the Configuration top-level menu.</td>
</tr>
<tr>
<td>Get global groups</td>
<td>When selected, information on global user groups is searched for on the Windows domain server.</td>
</tr>
<tr>
<td>Get local groups</td>
<td>When selected, information on local user groups is searched for on the Windows domain server.</td>
</tr>
<tr>
<td>Prefix group name with domain name (domain/group)</td>
<td>When selected, the name of the Windows domain appears before the name of the user group when authentication information on this group is sent from the domain server.</td>
</tr>
<tr>
<td>Enable basic authentication</td>
<td>When selected, the basic NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then sent in plain-text format (less secure) to the Windows domain server.</td>
</tr>
<tr>
<td>Enable integrated authentication</td>
<td>When selected, the integrated NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then encrypted before it is sent to the Windows domain server.</td>
</tr>
<tr>
<td>Enable NTLM cache</td>
<td>When selected, NTLM authentication information is stored in this cache. Authentication is then based on this stored information, rather on information retrieved from the Windows domain server.</td>
</tr>
<tr>
<td>NTLM cache TTL</td>
<td>Limits the time (in seconds) that authentication information is stored in this cache to the specified value.</td>
</tr>
<tr>
<td>International text support</td>
<td>Specifies a set of characters used by default for a request sent from a client, for example, ISO-8859-1.</td>
</tr>
</tbody>
</table>

### User Database Specific Parameters

Settings for the User Database authentication method

### Table 9-6  User Database Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send domain and machine name to the client</td>
<td>When selected, the names of the appliance and the domain it has been assigned to are sent to the client that a user who is to be authenticated sent a request from.</td>
</tr>
<tr>
<td>Enable basic authentication</td>
<td>When selected, the basic NTLM authentication method is applied to authenticate users. Information that a user submits for authentication is then sent in plain-text format (less secure) to the Windows domain server.</td>
</tr>
</tbody>
</table>
### Table 9-6  User Database Specific Parameters (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable integrated authentication</td>
<td>When selected, the integrated NTLM authentication method is applied to authenticate users.</td>
</tr>
<tr>
<td></td>
<td>Information that a user submits for authentication is then encrypted before it is sent to the Windows domain server.</td>
</tr>
<tr>
<td>Enable NTLM cache</td>
<td>When selected, NTLM authentication information is stored in this cache. Authentication is then based on this stored information, rather on information retrieved from the Windows domain server.</td>
</tr>
<tr>
<td>NTLM cache TTL</td>
<td>Limits the time (in seconds) that authentication information is stored in this cache to the specified value.</td>
</tr>
<tr>
<td>International text support</td>
<td>Specifies a set of characters used by default for a request sent from a client, for example, ISO-8859-1.</td>
</tr>
</tbody>
</table>

### LDAP Specific Parameters

Settings for the LDAP authentication method

### Table 9-7  LDAP Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP server(s) to connect to</td>
<td>Provides a list for entering the LDAP servers that authentication information is retrieved from.</td>
</tr>
<tr>
<td>List of certificate authorities</td>
<td>Provides a list for entering the certificate authorities that issue certificates when a Secure LDAP (S-LDAP) connection is used for communication with an LDAP server.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Specifies the user name of an appliance for logging on to an LDAP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets the password for a user name.</td>
</tr>
<tr>
<td></td>
<td>The Set button opens a window for configuring a new password.</td>
</tr>
<tr>
<td>International text support</td>
<td>Specifies a set of characters used by default for a request sent from a client, for example, ISO-8859-1.</td>
</tr>
<tr>
<td>Enable LDAP version 3</td>
<td>When selected, version 3 of the LDAP protocol is used.</td>
</tr>
<tr>
<td></td>
<td>If you want to configure Secure LDAP authentication, also known as LDAPS, it is this LDAP version that you must use.</td>
</tr>
<tr>
<td></td>
<td>This version is by default selected.</td>
</tr>
<tr>
<td>Allow LDAP library to follow referrals</td>
<td>When selected, the lookup of user information can be redirected from the LDAP server to other servers.</td>
</tr>
<tr>
<td>Connection live check</td>
<td>Limits the time (in minutes) that elapses between checks to see whether the connection to the LDAP server is still active to the specified value.</td>
</tr>
<tr>
<td>LDAP operation timeout</td>
<td>Limits the time (in seconds) that elapses before the connection to the LDAP server is closed if no communication occurs to the specified value.</td>
</tr>
<tr>
<td>Base distinguished name to user objects</td>
<td>Specifies the Distinguished name (DN) in the directory on an LDAP server where the lookup of user attributes should begin.</td>
</tr>
<tr>
<td>Map user name to DN</td>
<td>When selected, the name of the user who asks for authentication must map to a DN (Distinguished Name). This name identifies the user in the directory on the LDAP server.</td>
</tr>
</tbody>
</table>
Table 9-7  LDAP Specific Parameters (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter expression to locate a user object</td>
<td>Specifies a filtering term for restricting the lookup of user attributes.</td>
</tr>
<tr>
<td></td>
<td>To substitute the user name in the filtering term, u% is used as a variable.</td>
</tr>
<tr>
<td>Get user attributes</td>
<td>When selected, user attributes are looked up on the LDAP server to</td>
</tr>
<tr>
<td></td>
<td>authenticate a user.</td>
</tr>
<tr>
<td>User attributes to retrieve</td>
<td>Provides a list for entering the user attributes that should be retrieved from an LDAP server.</td>
</tr>
<tr>
<td>Attributes concatenation string</td>
<td>Specifies a string for separating user attributes found by a lookup, for example, / (slash).</td>
</tr>
<tr>
<td>Get groups attributes</td>
<td>When selected, user group attributes are also looked up on the LDAP server to authenticate a user.</td>
</tr>
<tr>
<td>Base distinguished name to group objects</td>
<td>Specifies the Distinguished name (DN) in the directory on the LDAP server where the lookup of group attributes should begin</td>
</tr>
<tr>
<td>Filter expression to locate a group object</td>
<td>Specifies a filtering term for restricting the lookup of group attributes.</td>
</tr>
<tr>
<td></td>
<td>To substitute the user name in the filtering term, u% is used as a variable.</td>
</tr>
<tr>
<td>Group attributes to retrieve</td>
<td>Provides a list for entering the group attributes that should be retrieved from an LDAP server.</td>
</tr>
</tbody>
</table>

Digest Authentication

Settings for LDAP digest authentication

Table 9-8  Digest Authentication

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable digest</td>
<td>When selected, digest authentication is performed as method for authenticating authentication</td>
</tr>
<tr>
<td>User attribute with</td>
<td>specifies the attribute of a user entry on the LDAP server that stores the value password hash for the authentication hash.</td>
</tr>
<tr>
<td>Nonce maximal use count</td>
<td>Sets a limit to repeated uses of the nonce (number only once) that is transmitted in the authentication process and required as a parameter for calculating the authentication hash. The maximum number of times that a nonce can be used by default is 100.</td>
</tr>
<tr>
<td>Nonce maximal TTL</td>
<td>Sets a limit to the time period (in minutes) that a nonce remains valid. The maximum time that a nonce can remain valid by default is 30 minutes.</td>
</tr>
<tr>
<td>Enable digest URI check</td>
<td>When selected, a check is performed to ensure that the URL that a client sends as a parameter for calculating the authentication hash is the same as the URL that this client sends in its request for accessing a particular destination in the web. If this check fails, the request is blocked. As this check might also fail due to problems with the different formats that the browsers on the clients use for sending URLs, it is optional. The check is enabled by default.</td>
</tr>
<tr>
<td>Allow digest</td>
<td>When selected, digest authentication must always be performed if a user is to authentication only be authenticated under the LDAP authentication method.</td>
</tr>
</tbody>
</table>
## Novell eDirectory Specific Parameters

Settings for the Novell eDirectory authentication method

### Table 9-9  Novell eDirectory Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP server(s) to connect to</td>
<td>Provides a list for entering the eDirectory servers that take the role of LDAP servers in providing authentication information.</td>
</tr>
<tr>
<td>List of certificate authorities</td>
<td>Provides a list for entering the certificate authorities that issue certificates when a Secure LDAP (S-LDAP) connection is used for communication with an LDAP server.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Specifies the user name of an appliance for logging on to an LDAP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets a password for a user name. The <em>Set</em> button opens a window for configuring a new password.</td>
</tr>
<tr>
<td>International text support</td>
<td>Specifies a set of characters used by default for a request sent from a client, for example, ISO-8859-1.</td>
</tr>
<tr>
<td>Enable LDAP version 3</td>
<td>When selected, version 3 of the LDAP protocol is used.</td>
</tr>
<tr>
<td>Allow LDAP library to follow referrals</td>
<td>When selected, the lookup of user information can be redirected from an LDAP server to other servers.</td>
</tr>
<tr>
<td>Connection live check</td>
<td>Limits the time (in minutes) that elapses between checks to see whether the connection to an LDAP server is still active to the specified value.</td>
</tr>
<tr>
<td>LDAP operation timeout</td>
<td>Limits the time (in seconds) that elapses before the connection to an LDAP server is closed if no communication occurs to the specified value.</td>
</tr>
<tr>
<td>eDirectory network address attribute</td>
<td>Specifies the name of the attribute that provides the network addresses used for an eDirectory server</td>
</tr>
<tr>
<td>eDirectory network login time attribute</td>
<td>Specifies the name of the attribute that provides the logon time used on an eDirectory server</td>
</tr>
<tr>
<td>eDirectory network minimal update interval</td>
<td>Specifies the time that elapses (in seconds) before information from an eDirectory server is updated.</td>
</tr>
<tr>
<td>Base distinguished name to user objects</td>
<td>Specifies the Distinguished name (DN) in the directory on an LDAP server where the lookup of user attributes should begin.</td>
</tr>
<tr>
<td>Map user name to DN</td>
<td>When selected, the name of the user who asks for authentication must map to a DN (Distinguished Name). This name identifies the user in the directory on the LDAP server.</td>
</tr>
<tr>
<td>Filter expression to locate a user object</td>
<td>Specifies a filtering term for restricting the lookup of user attributes. To substitute the user name in the filtering term, u% is used as a variable.</td>
</tr>
<tr>
<td>Get user attributes</td>
<td>When selected, user attributes are looked up on the LDAP server to authenticate a user.</td>
</tr>
<tr>
<td>User attributes to retrieve</td>
<td>Provides a list for entering the user attributes that should be retrieved from an LDAP server.</td>
</tr>
<tr>
<td>Attributes concatenation string</td>
<td>Specifies a string for separating user attributes found by a lookup, for example, / (slash).</td>
</tr>
<tr>
<td>Get groups attributes</td>
<td>When selected, user group attributes are also looked up on the LDAP server to authenticate a user.</td>
</tr>
<tr>
<td>Base distinguished name to group objects</td>
<td>Specifies the Distinguished name (DN) in the directory on an LDAP server where the lookup of group attributes should begin.</td>
</tr>
</tbody>
</table>
Table 9-9  Novell eDirectory Specific Parameters (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter expression to locate a group object</td>
<td>Specifies a filtering term for restricting the lookup of group attributes.</td>
</tr>
<tr>
<td></td>
<td>To substitute the user name in the filtering term, <em>u%</em> is used as a variable.</td>
</tr>
<tr>
<td>Group attributes to retrieve</td>
<td>Provides a list of group attributes that should be retrieved from an LDAP server.</td>
</tr>
</tbody>
</table>

RADIUS Specific Parameters
Settings for the RADIUS authentication method

Table 9-10  RADIUS Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS server definition</td>
<td>Provides a list for entering the RADIUS servers that authentication information is retrieved from.</td>
</tr>
<tr>
<td>Default domain name</td>
<td>Specifies the name of the domain that information is retrieved from if no other domain is specified.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Sets the password used by an appliance to get access to a RADIUS server.</td>
</tr>
<tr>
<td>Radius connection timeout in seconds</td>
<td>Limits the time (in seconds) that elapses before the connection to the RADIUS server is closed if no traffic occurs to the specified value.</td>
</tr>
<tr>
<td>International text support</td>
<td>Specifies the set of characters used by default for a request sent from a client, for example, ISO-8859-1.</td>
</tr>
<tr>
<td>Value of attribute with code</td>
<td>Sets the code value for the attribute retrieved with the user group information, according to RFC 2865. For example, 25 is the code for the “class” attribute.</td>
</tr>
<tr>
<td>Vendor specific attribute with vendor ID</td>
<td>Sets the Vendor ID that is required for retrieving vendor-related data in the search for user group information. According to RFC 2865, the vendor ID is a part of the vendor attribute, followed by a number of subattributes. Its code value is 26.</td>
</tr>
<tr>
<td>Vendor subattribute type</td>
<td>Sets a code value for the type of subattributes included in a vendor attribute. according to RFC 2865. Since not all vendors adhere to this structure, we recommend to specify 0 as value here. This allows the authentication module to retrieve all available vendor information.</td>
</tr>
</tbody>
</table>

Kerberos Specific Parameters
Settings for the Kerberos authentication method

More settings for this authentication method can be configured using the Kerberos Administration system settings, which can be accessed under the Configuration top-level menu.
Table 9-11 Kerberos Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extract group membership IDs from the ticket</td>
<td>When selected, information to identify the groups that a user is a member of is retrieved from the ticket that is used in the process of authenticating users under the Kerberos authentication method. When this option is selected, the following option becomes accessible.</td>
</tr>
<tr>
<td>Look up group names via NTLM</td>
<td>When selected, the names of the groups that a user is a member of are retrieved using the NTLM authentication method.</td>
</tr>
</tbody>
</table>

Authentication Server Specific Parameters

Settings for the Authentication Server method

Table 9-12 Authentication Server Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication server URL</td>
<td>Specifies the URL of a server that is used under this method to look up authentication information.</td>
</tr>
<tr>
<td>Require client ID</td>
<td>When selected, the authentication server requires the ID of the client that a user sent a request from.</td>
</tr>
<tr>
<td>Store authentication result in a cookie</td>
<td>When selected, the information retrieved from the authentication server is stored in a cookie If cookie authentication is implemented, the cookie is added to the next request sent by the respective user, so that this user need not authenticate again.</td>
</tr>
<tr>
<td>Allow persistent cookie for the server</td>
<td>When selected, a cookie can be used persistently for sending multiple requests to the authentication server</td>
</tr>
<tr>
<td>Cookie TTL for the authentication server in seconds</td>
<td>Limits the time (in seconds) that a cookie sent with a request to the server is stored to the specified value.</td>
</tr>
<tr>
<td>Cookie prefix</td>
<td>Specifies a prefix that is added on the appliance to a cookie, for example, MWG_Auth.</td>
</tr>
</tbody>
</table>

One-Time Password Specific Parameters

Settings for the One-Time Password authentication method
### Table 9-13 One-Time Password Specific Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OTP server</strong></td>
<td>Specifies the IP address and port number of the OTP server that Web Gateway connects to when authenticating a user under the One-Time Password authentication method.</td>
</tr>
</tbody>
</table>
| **Communicate with SSL and trust certificate below** | When selected, communication with the OTP server is performed using an SSL-secured connection.  
When this option is selected, the information in the following four fields is no longer grayed out and the **Import** button below these fields becomes accessible.  
The fields provided detailed information about the certificate that is currently used in SSL-secured communication with the OTP server.  
• **Subject** — Provides general information about the certificate.  
  • **Common Name (CN)** — Specifies the common name of the certificate.  
    By default, this name is **localhost**.  
  • **Organization (O)** — Specifies the organization of the certificate.  
    By default, the organization is **OTP Server**.  
  • **Organizational Unit (OU)** — Specifies the organizational unit of the certificate.  
    By default, the organizational unit is not set.  
• **Issuer** — Provides information about the issuer of the certificate.  
  • **Common Name (CN)** — Specifies the common name of the issuer.  
    By default, this name is **localhost**.  
  • **Organization (O)** — Specifies the organization of the issuer.  
    By default, the organization is **OTP Server**.  
  • **Organizational Unit (OU)** — Specifies the organizational unit of the server certificate.  
    By default, the organizational unit is not set.  
• **Validity** — Limits the time the certificate is valid.  
  • **Not before** — Shows the date and time when the validity of the certificate begins.  
  • **Not after** — Shows the date and time when the validity of the server certificate ends.  
• **Extensions** — Provides additional information on the certificate.  
  • **Comment** — Provides a plain-text comment on the certificate.  
    By default no comment is provided.  
• **Import** — Opens a window for importing a certificate. |
| **WS client name**                          | Specifies the user name for Web Gateway in communication with the OTP server.                                                             |
| **WS client password**                      | Specifies the password for Web Gateway in communication with the OTP server.                                                              |
| **OTP message**                             | Specifies the prefix to messages that are sent from the OTP server to Web Gateway and the delimiters that include a message.  
By default a message looks like this:  
OTP for MWG: $$<OTP message>$$ |
Table 9-14 McAfee Client Proxy

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer ID</td>
<td>Specifies an identifier for a customer.</td>
</tr>
<tr>
<td>Shared password</td>
<td>Sets a password for a customer. Clicking Set opens a window that allows you to perform the setting.</td>
</tr>
<tr>
<td>Keep domain in group name</td>
<td>When selected, domain information contained in the name of a user group is kept. This option is selected by default.</td>
</tr>
<tr>
<td>Remove custom headers used for authentication</td>
<td>When selected, headers contained in the information that is submitted for authentication are removed. This option is selected by default.</td>
</tr>
<tr>
<td>Export MCP credentials to XML file</td>
<td>Lets you export the credentials that are submitted when performing the SWPS (McAfee Client Proxy) authentication method. By default a message looks like this: OTP for MWG: $$&lt;OTP message&gt;$$</td>
</tr>
</tbody>
</table>

Advanced Parameters

Setting for configuring advanced authentication

This is setting is the same for all authentication methods. Its description is therefore also provided at the beginning of this description of the authentication settings, after the description of the common settings.

Table 9-15 Advanced Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always evaluate property value</td>
<td>When selected, a new evaluation to assign a value to a property is performed each time a rule containing this property is processed. If a value has been stored for a property in the cache, it is not used. While it is normally recommended to let cache values be used to improve performance, there can be situations where the new evaluation of a property is required. In these situations, the same property is used more than once within the authentication rules and with the same settings of the Authentication module. A new evaluation ensures the most current value is assigned to the property each time.</td>
</tr>
</tbody>
</table>
Implement a different authentication method

If you do not want to use the User Database authentication method of the default rule set, you can implement a different method, such as NTLM, LDAP, and others.

**Task**


2. On the rule sets tree, navigate to the rule set that contains rules for authenticating users, for example, the default Authentication and Authorize rule set and select the nested Authenticate with User Database rule set.

   The rules of the nested rule set appear on the settings pane.

3. Select the rule Authenticate with User Database and in the rule criteria click User Database.

   The Edit Settings window opens.

4. From the list provided under Authentication Method, select an authentication method, for example, NTLM.

5. Configure common and specific parameters for the selected method as needed.

6. Click OK to close the window.

7. Click Save Changes.

   We recommend that after changing the authentication method, you rename the settings of the Authentication module, the authentication rule, and the nested rule set, accordingly.

   For example, after selecting NTLM, rename the settings to NTLM and both the rule and the nested rule set to Authenticate with NTLM.

   Instead of renaming the default settings, you can also keep several settings with different names and parameter values for the Authentication module.

Using system settings to configure authentication

For some authentication methods, you need to configure settings that are not settings of the Authentication module, but of the appliance system.

This applies when you are implementing NTLM as the authentication method. In this case, you need to join the appliance to a Windows domain and configure the Windows Domain Membership settings, which are system settings.

It applies also for the Kerberos authentication method, which is implemented using the Kerberos Administration system settings.

**Kerberos Administration settings**

The Kerberos Administration settings are specific settings for the Kerberos authentication method.

**Kerberos Administration**

Settings for the Kerberos authentication method
Table 9-16 Kerberos Administration

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key tab file</strong></td>
<td>Specifies the file that contains the master key required to access the Kerberos server. You can type a file name or use the <strong>Browse</strong> button to browse to the file and enter its name in the field. When a ticket is issued for authentication according to the Kerberos method, the master key is read on the appliance and used to verify the ticket. If you are running a load balancer that directs web requests to the appliance, tickets are issued for the load balancer and verified on the appliance. It is then not checked whether a request is directed to the appliance.</td>
</tr>
<tr>
<td><strong>Kerberos realm</strong></td>
<td>Specifies an administrative domain configured for authentication purposes. Within the boundaries of this domain the Kerberos server has the authority to authenticate a user who submits a request from a host or using a service. The realm name is case sensitive, however, normally only uppercase letters are used, and it is good practice to make the realm name the same as that of the relevant DNS domain.</td>
</tr>
</tbody>
</table>
| **Maximal time difference between appliance and client** | Limits the time (in seconds) that the system clocks on the appliance and its clients are allowed to differ to the specified value. Configuring Kerberos as the authentication method can lead to problems when particular browsers are used for sending requests:  
  • When the Microsoft Internet Explorer is used in a version lower than 7.0, Kerberos authentication might not be possible at all.  
  • When this explorer runs on Windows XP, Kerberos authentication might not work as expected.  
  • When Mozilla Firefox is used, Kerberos authentication must be configured in the browser settings to enable this authentication method. |
| **Enable replay cache**              | When selected, a ticket that is issued for authentication cannot be used more than once.                                                                                                                                                                                                                                                                                                                                                   |

Join the appliance to a Windows domain
When using the NTLM authentication method, you need to join an appliance to a Windows domain to let the authentication module retrieve user information stored on the domain server. An appliance can be joined to more than one domain.

**Task**

1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance you want to join and click **Windows Domain Membership**. A list of domains appears on the settings pane. It is initially empty.
3. Click **Join** to enter a domain into the list. The **Join Domain** window opens.
4 Configure a domain name, a domain controller, and other settings in the window.

5 Click **OK**.

The window closes and the new domain appears in the list. The appliance is now a member of this domain.

Repeat Steps 3 to 5 to add multiple domains.

Use the other icons on the toolbar to work with the list, for example, to modify a list entry or to let an appliance leave a domain.

**See also**

*Windows Domain Membership settings on page 260*

**Windows Domain Membership settings**

The Windows Domain Membership settings are used for joining an appliance to a Windows domain.

**Join Domain**

Settings for joining an appliance to a Windows domain

**Table 9-17 Join Domain**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows domain name</td>
<td>Specifies the name of the domain.</td>
</tr>
<tr>
<td>McAfee Web Gateway account name</td>
<td>Specifies the name of an account for an appliance.</td>
</tr>
<tr>
<td>Overwrite existing account</td>
<td>When selected, an existing account is overwritten.</td>
</tr>
<tr>
<td>Use NTLM version 2</td>
<td>When selected, NTLM version 2 is used.</td>
</tr>
<tr>
<td>Timeout for requests to this NTLM domain</td>
<td>Limits the time (in seconds) that elapses before processing stops for a request sent from an appliance to a domain controller if no response is received to the specified value.</td>
</tr>
<tr>
<td>Wait time for reconnect to domain controller</td>
<td>Specifies the time (in seconds) that elapses before another attempt is made to connect to a domain controller after a previous attempt failed. The allowed range is from 5 to 300 seconds.</td>
</tr>
<tr>
<td>Configured domain controllers</td>
<td>Provides a list for entering the domain controllers that an appliance can connect to in order to retrieve authentication information. Entries must be separated by commas.</td>
</tr>
<tr>
<td>Number of active domain controllers</td>
<td>Maximum number of configured domain controllers that can be active at the same time The allowed range is from 1 to 10.</td>
</tr>
<tr>
<td>Administrator name</td>
<td>Specifies the user name for the account that is created when an appliance is joined to a domain. User name and password are only used for this purpose and not stored.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets a password for the administrator name.</td>
</tr>
</tbody>
</table>
Best practices - Configuring authentication for deployment types

When configuring authentication, you need to consider the type of deployment that is configured for handling the traffic between Web Gateway and its clients, such as the explicit proxy mode or a transparent mode. For each type, there is a rule set in the rule set library that is best suited to handle authentication.

The following two questions are important with regard to the authentication process:

• How are the user credentials that are evaluated during this process obtained by Web Gateway?

  This part of the authentication process is sometimes referred to as the authentication front-end.

  The method for obtaining user credentials depends on whether the explicit proxy mode (also known as direct proxy mode) or a transparent mode (transparent router or bridge mode) is configured for handling the traffic between Web Gateway and its clients.

  For the explicit proxy mode, you can configure that clients use a service under the WCCP protocol to send requests as an additional option.

  The rule set library provides suitable rule sets for each of these modes.

• How should credentials be evaluated once they have been obtained?

  This is sometimes referred to as the authentication back-end.

  The evaluation of credentials depends on the authentication method that is configured, for example, LDAP or NTLM.

Library rule sets for authentication

The rule sets for configuring authentication are located in the Authentication rule set group of the rule set library.

The following table shows which of these rule sets are recommended for particular types of deployment.

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Recommended library rule set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explicit proxy mode</td>
<td>Direct Proxy Authentication and Authorization</td>
</tr>
<tr>
<td>Transparent router or bridge mode</td>
<td>Authentication Server (Time/IP Based Session)</td>
</tr>
<tr>
<td>Explicit proxy mode with WCCP</td>
<td>If traffic is processed in:</td>
</tr>
<tr>
<td></td>
<td>• Explicit proxy mode — Direct Proxy Authentication and Authorization</td>
</tr>
<tr>
<td></td>
<td>• WCCP mode — Authentication Server (Time/IP Based Session)</td>
</tr>
</tbody>
</table>

After importing a rule set from the library, you can modify its rules to adapt them further to the needs of your network.

Position in the rule sets tree

An authentication rule set should be placed after the Global Whitelist rule set, but before the Common Rules rule set (if you keep these items from the default rule sets tree).

Placing an authentication rule set in this way ensures that a user needs not be authenticated when sending a request for accessing a web object that is on the global whitelist.
Authentication for the explicit proxy mode

When configuring authentication for the explicit proxy mode, a suitable rule set must be implemented on Web Gateway.

Library rule set for the explicit proxy mode

The recommended library rule set for the explicit proxy mode is Direct Proxy Authentication and Authorization.

This rule set has two nested rule sets:

- Authenticate with User Database
- Authorize User Groups

When this rule set is implemented, the authentication process is performed for each request that is received from a client of Web Gateway unless an exception rule applies.

Using this rule set is also the preferred way of handling authentication when Citrix is installed or workstations are shared in a configuration.

Direct Proxy Authentication and Authorization rule set

This rule set contains rules for making exceptions that allow a request to be processed on Web Gateway without authenticating the user who sent the request.

Exceptions can be based on:

- The IP address of the client that a request was sent from
- The URL of the web object that is the destination of the request

Using these rules you can ensure that requests coming in from trusted clients or going out to trusted destinations are spared the effort of performing an authentication process for their users, which increases performance.

You can also create rules of your own and add them to this rule set to allow for more exceptions.

Authenticate with User Database nested rule set

This rule set contains a rule that lets authentication be performed for a user who sends a request for web access from a client of Web Gateway. The user is asked to submit credentials, which are evaluated based on information that is stored in the internal user database.

The rule set applies if the user in question has not yet been authenticated and not tried unsuccessfully to authenticate before. The \texttt{Authentication.Is.Authenticated} and \texttt{Authentication.Failed} properties are used to check this.

Instead of using information from the internal user database to evaluate the credentials, you can configure a different authentication method, for example, LDAP or NTLM.

Authorize User Groups nested rule set

This rule set contains a rule that allows only requests of authorized users, which means a request is blocked if the user who sent it is not a member of one of the user groups on a particular list. The request is blocked, even if the user has successfully passed the evaluation that was performed before.

This rule allows you to implement an additional security check. If you want to use it, you need to fill the list that is used in this rule set with user groups. If you do not want to use it, you can disable or delete the rule set.
Modifying the rule set for the explicit proxy mode
When configuring authentication for the explicit proxy mode, you can modify the library rule set to adapt it to the needs of your network.

This includes:

- Changing the authentication method
- Modifying, disabling, or deleting user authorization
- Configuring more exception rules

Changing the authentication method
By default, the method used for evaluating credentials is comparing them to the information stored in the internal user database.

To change this authentication method (authentication back-end), you need to configure the settings that appear next to the Authentication.Authenticate property in the only rule of the Authenticate with User Database rule set.

Under Authentication method, a list of authentication methods is provided to let you select a method that is better suited to the needs of your network, for example, LDAP or NTLM.

Modifying, disabling, or deleting user authorization
The nested Authorized User Groups rule set allows only requests from authorized users. You can fill the list that is provided in the only rule of this rule set with user groups as needed.

If you do not want to use this rule as an additional security check, you can disable or delete the rule set.

Configuring more exception rules
You can add rules to the Direct Proxy Authentication and Authorization rule set to cover more exceptions from the authentication process.

If any of these rules applies, processing of the rule set is stopped, which means it is not executed for the nested rule sets that handle authentication.

For example, you can add a rule to allow requests when the browser on the client they were sent from runs with a particular user agent. Information about the user agent is taken from the request header.

The rule might look as follows:

<table>
<thead>
<tr>
<th>Skip authorization for user agents that are in list Allowed User Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Header.Request.Get(&quot;User-Agent&quot;) matches in list Allowed User Agents</code> -&gt; Stop Rule Set</td>
</tr>
</tbody>
</table>

Another rule could allow requests for access to objects on web servers with IP addresses that are on a particular list. The IP address is taken from the URL that was submitted with a request.

This rule might look as follows:

<table>
<thead>
<tr>
<th>Skip authorization for destination IPs that are in list Allowed Destination IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>URL.Destination.IP is in range list Allowed Destination IPs</code> -&gt; Stop Rule Set</td>
</tr>
</tbody>
</table>
Authentication for transparent modes

When configuring authentication for the transparent modes, the settings on the browsers that are used for sending requests to Web Gateway need to be modified. A suitable rule must also be implemented on Web Gateway.

Modifying the browser settings

To enable authentication for the transparent router or bridge mode, the settings of each web browser that is used for sending requests must be configured to let it trust Web Gateway.

If NTLM or Kerberos is also configured as the authentication method on Web Gateway, the authentication process is handled internally, without asking the user to authenticate.

- When using Microsoft Internet Explorer, you need to modify the security settings by:
  - Configuring your local intranet as a security zone
  - Adding Web Gateway as a website to this zone
    This is done by specifying a URL with an IP address or a fully qualified domain name, for example, http://10.10.69.73 or http://*.mcafee.local.
  - Configuring automatic logon for all websites in the zone as the security setting for user authentication

You can configure this under Internet Options, using the Local Intranet and Security Settings - Local Intranet Zone windows.

If group policies can be configured for a browser, you can also use the Group Policy Management Editor together with the Site to Zone Assignment List and the Logon Options window.

- When using Mozilla Firefox, you need to configure an IP address or a fully qualified domain name for Web Gateway under about:config as the value of the network.automatic-ntlm-auth.trusted-uris parameter, for example, 10.10.69.73 or mwgappl.yourdomain.local.

For more information, refer to the documentation of the respective web browser.

Library rule set for transparent modes

The recommended library rule set for the transparent router or bridge mode is Authentication Server (Time/IP Based Session).

It has two nested rule sets:

- Check for Valid Authentication Session
- Authentication Server

Differing from the authentication process that is performed for the explicit proxy mode, this rule set handles authentication by creating an authentication session when a user who sent a request for web access is successfully authenticated.

Subsequent requests that this user sends are processed without requiring authentication again as long as this session is still valid. The default session length is 600 seconds.

Using this rule set in a configuration where Citrix is installed or workstations are shared can lead to the following situation: User A sends a request, is authenticated, and an authentication session is created. Later on, user B sends a request from the same workstation and is still allowed to continue with user A's session.

Authentication Server (Time/IP Based Session) rule set

This rule set serves as a container for the two nested rule sets and has no rules of its own.
Check for Valid Authentication Session nested rule set

This rule set contains a rule that checks whether a valid session exists for a user who sends a request from a client. Session information is stored in an internal session database. It includes the user name, the IP address of the client, and the session length.

If a valid session exists, processing of the request is continued for the remaining rules and rule sets that are configured. If no valid session exists, the request is redirected to the authentication server.

Authentication Server nested rule set

This rule set contains a rule that lets authentication be performed for a user whose request has been redirected to the authentication server. If the authentication was successful, a session is created for this user in the session database.

The method used by default for evaluating the user’s credential is comparing them to the information that is stored in the internal user database. You can replace this method with a different method, for example, LDAP or NTLM.

Modifying the rule set for transparent modes

When configuring authentication for transparent modes, you can modify the library rule set to adapt it to the needs of your network.

This includes:

- Modifying the authentication server URL
- Changing the authentication method
- Enabling the ideal conditions rule
- Increasing the session TTL

Modifying the authentication server URL

If you have modified the security settings of the browsers that are used for sending requests to Web Gateway by configuring your local domain as a security zone, you can include Web Gateway as a website in this zone by specifying a URL with an IP address or fully qualified domain name for it.

In this case, you also need to modify the URL of the authentication server, which by default contains an IP address for Web Gateway, by inserting the name of your local domain.

The authentication server URL is dynamically generated for an appliance that Web Gateway runs on. As there can be several Web Gateway appliances in a configuration, the IP address cannot be static, but must be configured dynamically, which is done using internal configuration properties.

You can modify this URL under the IP Authentication Server settings, which appear next to the Authentication.Authenticate property in the Redirect clients that do not have a valid session to the authentication server rule of the Check for Valid Authentication Session rule set.

By default, the URL looks like this:

```
http://$<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.proxy.ip"/>$: <$<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.proxy.port"/>
```

Shown in human readable format, a particular authentication server URL could be:

```
http://10.10.69.71:9090
```
After adapting the URL to the browser settings that have your local domain configured within a security zone, it looks like this:

http://$<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system"/>$.yourdomain.local:$<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.proxy.port"/>$ with "com.scur.engine.system.proxy.ip"/$ having been replaced by "com.scur.engine.system"/>$.yourdomain.local.

In human readable format, this could be, for example

http://mwgappl.yourdomain.local:9090

where mwgappl is the host name of an appliance that Web Gateway runs on.

**Changing the authentication method**

By default, the method used for transparent modes to evaluate credentials is comparing them to the information stored in the internal user database.

To change this authentication method (authentication back-end), you need to configure the settings that appear next to the Authentication.Authenticate property in the Authenticate user against user database rule of the Authentication Server rule set.

Under Authentication method, a list of authentication methods is provided to let you select a method that is better suited to the needs of your network, for example, LDAP or NTLM.

**Enabling the ideal conditions rule**

The Revalidate session under ideal conditions rule in the Check for Valid Authentication Session rule set lets a user authenticate again under "ideal" conditions, which means authentication will not be asked for at a time when the session has already expired.

In more detail, these conditions are by default:

- The remaining session time is less than 400 seconds.
- The network protocol is HTTP.
- The request that the user sends is a GET request.

Enabling this rule avoids a situation like the following:

1. A user sends a request from a client of Web Gateway and authenticates (600 seconds are allowed for the session time).
2. The user wants to send a ticket to the help desk and begins filling out a data form (300 seconds are used up).
3. The user needs more information to fill out the form and browses the web for this information, which lets some GET requests be received on Web Gateway (200 more seconds are used up).
4. The user completes the data form and submits it, which lets a POST request be received on Web Gateway (200 more seconds elapse, session time expires after the first 100 seconds).
5. As the session time has expired, the user is asked to authenticate again before the POST request is processed. However, due to the session expiration, all filled-out data is lost.

If the ideal conditions rule is enabled, the user is already asked when browsing for information at step 3 to authenticate again, which leaves enough time to complete the form and submit it.
Increasing the session TTL
You can increase the allowed time for an authentication session, for example, from the default 600 seconds (10 minutes) to an hour.

You can also modify the time condition in the criteria of the Revalidate session under ideal conditions rule, for example, by increasing it from 400 to 600 seconds.

This way, the rule will ask a user, upon receiving a GET request, to authenticate when session expiration is still 10 minutes away.

Authentication for the explicit proxy mode with WCCP
Configuring authentication for the explicit proxy mode with WCCP includes import and modification of two rule sets, as well as specifying ports for incoming traffic to trigger the use of the appropriate rule set.

When the explicit proxy mode with WCCP is configured, clients send requests to Web Gateway in explicit proxy mode or using a service under the WCCP protocol.

To handle authentication for the explicit proxy mode, the Direct Proxy Authentication and Authorization rule set is recommended, for the WCCP mode, which is a transparent mode, it is the Authentication Server (Time/IP Based Session) rule set.

This means you should import both rule sets and complete additional activities as needed for both modes, including the modification of the browser settings for the WCCP mode.

To let traffic for each mode be handled by the appropriate authentication rule set, you can configure different ports for both types of traffic and specify the respective port in the criteria of each rule set.

Configuring different ports for the explicit proxy and WCCP modes
The ports for the explicit proxy and WCCP modes could, for example, be 9090 and 9091. You need to specify the port for the WCCP mode when configuring a WCCP service and both ports in the list of HTTP ports.

A WCCP service is configured by entering it in the WCCP Services list. This list appears after selecting WCCP in the Transparent Proxy section of the Proxies (HTTP(S), FTP, ICAP, and IM) system settings.

The section appears within these settings when you begin to configure the explicit proxy mode with WCCP by selecting Proxy (optional WCCP) under Network Setup.

The entry for a WCCP service that is used for traffic coming in on port 9091 could, for example, look as follows:

<table>
<thead>
<tr>
<th>No</th>
<th>Service ID</th>
<th>WCCP router ...</th>
<th>Ports ...</th>
<th>Proxy listener ...</th>
<th>Proxy listener port</th>
<th>MD5 ...</th>
<th>Assignment</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>91</td>
<td>10.10.69.7 80, 443 false</td>
<td>10.10.69.73 9091</td>
<td>000000</td>
<td>1000</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The HTTP Port Definition List can be configured in the HTTP Proxy section, which is located below the Transparent Proxy section.

The entries for the explicit proxy and WCCP modes could look as follows:

<table>
<thead>
<tr>
<th>No</th>
<th>Listener address</th>
<th>Serve ...</th>
<th>Ports ...</th>
<th>Transparent ...</th>
<th>McAfee ...</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0.0.0:9090</td>
<td>true</td>
<td>443</td>
<td>false</td>
<td>true</td>
<td>Explicit proxy traffic</td>
</tr>
<tr>
<td>2</td>
<td>0.0.0.0:9091</td>
<td>true</td>
<td>443</td>
<td>false</td>
<td>true</td>
<td>WCCP traffic</td>
</tr>
</tbody>
</table>
Adapting the criteria of the authentication rule sets

After configuring different ports for traffic coming in under the explicit proxy mode or using a WCCP service, for example, 9090 and 9091, you need to adapt the criteria of the rule sets for handling the two kinds of traffic.

The adapted rule criteria of the Direct Proxy Authentication and Authorization rule set would then look as follows:

Proxy.Port equals 9090 AND (Connection.Protocol equals "HTTP" OR Connection.Protocol equals "HTTPS")

For the Authentication Server (Time/IP Based Session) rule set, the adapted criteria would be:

Proxy.Port equals 9091

Best practices - Configuring LDAP authentication

LDAP authentication is one of the methods that can be configured on Web Gateway for authenticating users.

LDAP stands for Lightweight Directory Access Protocol. Under this protocol, the authentication process on Web Gateway can be integrated with an existing directory service in a network. The directory holds user information, which can be queried and used for authentication.

In addition to authenticating a user, a directory can be queried to find other pieces of information about a user and the groups that a user belongs to. These pieces of information are called attributes.

An entry for a user in, for example, the Microsoft Windows Server Active Directory (Active Directory) usually includes a memberOf attribute holding information about the groups that the user belongs to. An entry for a group usually has a member attribute to hold the group members' user names.

The results returned by lookups for both user and group attributes are stored on Web Gateway as the value of the Authentication.UserGroups property.

LDAP authentication process

The process that integrates user authentication on Web Gateway and a directory on an LDAP server includes the following main steps.

- Web Gateway sends an initial bind request with administrator credentials to the LDAP server.
- If the request is successful, Web Gateway sends a query with the user name that the user submits. The purpose of this query is to find a distinguished name that the user name is mapped to in the directory on the LDAP server.
- If a distinguished name is found, the LDAP server sends it back. The distinguished name (DN) is a combination of information about a user, a user group, and a network domain provided in an LDAP-style syntax.

For example, for the user name jsmith, the LDAP server sends back the distinguished name cn=John Smith,cn=users,dc=ldap,dc=local.
• Web Gateway sends a second bind request to the LDAP server with the purpose of authenticating the user.

  This request includes the distinguished name and the password that the user submitted.

• If the request is successful, the user is authenticated.

  You can record the steps of the authentication process in a tcpdump to review them.

**Rule for authenticating a user under LDAP**

To configure LDAP authentication on Web Gateway, you must implement a rule that authenticates a user in an integrated process with Web Gateway and a directory on an LDAP server.

The rule set library provides a rule set with a default rule that you can modify and use for this purpose. The modified rule looks as follows:

**Name**

Authenticate with LDAP

**Criteria**

\[ \text{Authentication.Authenticate}<\text{LDAP}> \text{ equals false} \]

**Action**

\[ \rightarrow \text{Authenticate}<\text{Default}> \]

The rule applies if a user has not yet been authenticated using the LDAP authentication method.

The settings of the Authentication.Authenticate property in this rule are configured to provide the information that is necessary to run the authentication process successfully, including the IP address of the LDAP server and the administrator credentials for Web Gateway.

**Configure the LDAP method for authenticating a user**

To configure the LDAP method for authenticating a user, you can adapt an already existing authentication rule. Modify the names and settings within this rule in a way that makes them suitable for LDAP authentication.

**Task**

1. Import the Explicit Proxy Authentication and Authorization rule set from the rule set library.

   This rule set is for authentication in explicit proxy mode. For a transparent mode, import the Authentication Server rule set.

2. Adapt the authentication rule in the nested Authenticate with User Database rule set to make it suitable for LDAP authentication.

   For a transparent mode, adapt the authentication rule in the nested Authentication Server rule set.

   a. Rename the current rule name to Authenticate with LDAP.
   
   b. Rename the settings of the Authentication.Authenticate property to a name that is appropriate for LDAP-related settings, for example, LDAP.
   
   c. Modify the settings to make them suitable for LDAP authentication.
3 Rename the nested rule set to Authenticate with LDAP.

Instead of adapting the nested library rule set, you can also disable or delete it and create a new nested rule set for LDAP authentication.

The second nested rule set of the Explicit Proxy Authentication and Authorization library rule set, Authorize User Groups, is not needed for LDAP authentication.

If you delete this nested rule set, you should rename the nesting rule set or have only one rule set named, for example, Explicit Proxy Authentication with LDAP.

4 Click Save Changes.

See also
Configure the settings for the LDAP authentication method on page 270

Configure the settings for the LDAP authentication method
Configure the settings for the LDAP authentication method by modifying the settings in the rule for authenticating a user that you have imported from the rule set library.

Task

1 In the imported rule, click the settings of the Authentication.Authenticate property that you have renamed to LDAP or a similar name.

The Edit Settings window opens.

2 Under Authentication Method, select LDAP.

The LDAP Specific Parameters section appears next to Common Authentication Parameters.

You can leave the common parameters as they are, as well as the LDAP-specific parameters that are not mentioned in the following.

3 In the LDAP server(s) to connect to list, add an entry for the LDAP server that the directory with the user information resides on.

The syntax for an entry is as follows:

{LDAP | LDAPS}://<IP address>[:<port number>]

For example: LDAP://10.205.67.8:389

LDAP is an insecure protocol, as it transmits information in clear text. We recommend using LDAPS (secure LDAP) if possible.

The default LDAP port is 389 while LDAPS uses 636.

4 Provide the administrator credentials that Web Gateway submits when trying to connect to the LDAP server.

a Under Credentials, type a common name and a domain controller name in LDAP style, for example:

cn:administrator,cn:users,dc:ldap,dc:local
b Under **Password**, type an administrator password.

5 If the directory on the LDAP server is an Active Directory, deselect **Allow LDAP directory to follow referrals**.

6 Provide information for the query to find the distinguished name of the user who is to be authenticated.
   a Under **Base distinguished name to user objects**, specify a starting point for the query.
      The starting point is specified in LDAP style, for example:
      
      `cn:users,dc:ldap,dc:local`
   
   b Select **Map user name to DN**.
      Selecting this option lets the query search for a distinguished name that the submitted user name is mapped to in the directory.
   
   c Under **Filter expression to locate a user object**, specify a user attribute that allows the distinguished name to be found.
      Specifying this filter expression enables the search to find the entry for a user in the directory. The filter expression is the user name that the user submitted. The user name is stored in the directory as the value of an attribute that is part of the entry for a user.
      
      In an Active Directory, the name of the attribute that stores the user name is **sAMAccountName**. On Web Gateway, the user name is stored in a variable named `%u`.
      
      The filter expression must therefore be specified as follows if an Active Directory is used:
      
      `samaccountname=%u`
      
      Using this filter expression, the query will find the user entry and, consequently, try to map the user name to a distinguished name that might have been entered into the directory for a user with that user name.

7 Click **OK** to close the window.

8 Click **Save Changes**.

These settings enable Web Gateway to authenticate a user under the LDAP authentication method. To retrieve information stored in other attributes within a directory, additional settings are required.

See also

*Configure queries for user and group attributes on page 271*

**Configure queries for user and group attributes**

Configure additional settings to perform queries that retrieve ("pull") more information about users and user groups from a directory on an LDAP server.

The settings for these queries are part of the settings that you configure for the Authentication module (engine) on Web Gateway to handle the integrated process for authenticating a user.

**Task**

1 Configure a query for user attributes.
   a Select **Get user attributes**.
      You need not configure any special values for the **Base distinguished name to user objects** option, as these values are the same as those that you already configured for the purpose of authenticating a user.
b In the User attributes to retrieve list, add the name of the attribute that the query should find a value for. You can also add multiple names here.

For example, to retrieve information about the group or groups that a user belongs to, add memberof.

c Under Attributes concatenation string, type a character for separating multiple resulting values, for example, a comma.

2 Configure a query for group attributes.

a Select Get group attributes.

b Under Base distinguished name to group objects, provide a starting point for the query using LDAP syntax, for example, ou=groups,dc=ldap,dc=local.

c Under Filter expression to locate a group object, specify an attribute of a group that allows the group to be found.

For example, specify member=%u, which has member as the attribute name and the $u variable that holds the user's user name on Web Gateway as the attribute value.

d In the Group attributes to retrieve list, add the name of the attribute that the query should find a value for. You can also add multiple names here

For example, to find the so-called common name of a group, add cn.

e Under Attributes concatenation string, type a character for separating multiple resulting values, for example, a comma.

Storing an attribute in a separate property

You can store a user or group attribute in a separate User-Defined property for logging and other purposes.

When a query for an attribute of a user or user group is performed in a directory on an LDAP server, the resulting information is stored on Web Gateway as the value of the Authentication.UserGroups property.

If you are interested in a particular piece of information, for example, the email address of a user, you can also retrieve it separately and store it in a User-Defined property.

For this purpose, you must create an additional rule, as well as additional settings named, for example, LDAP Email Lookup, for the Authentication module (engine). In this rule, the Authentication module runs with the additional settings to retrieve the information that is stored within the entry for a user as the value of the email attribute.

Options must be especially configured in the additional settings as follows:

• Get user attributes must be enabled.

• The User attributes to retrieve list must contain a single entry for the email attribute. When an Active Directory is running on the LDAP server, the attribute name is mail.

• Map user to DN must be disabled.

Not disabling the option produces an error, as the user name has already been mapped when the Authentication module was running with the LDAP settings to authenticate the user.

All other options can be configured in the same way as the settings within the rule that authenticates the user.
The complete rule should look as follows:

**Name**

Get email information and store separately

**Criteria**

- `Authentication.IsAuthenticated equals true` AND
- `Authentication.GetUserGroups <LDAP_Email_:Lookup> does not contain "no-group"`

**Action**

- Continue

The rule must be added to the rule set for LDAP authentication and placed after the rule that authenticates the user.

**Storing the original user name for logging**

The original user name can be stored for logging purposes.

When a user has been authenticated using the LDAP method, the value of the `Authentication.Username` property is set to the user’s distinguished name. If the property is used for creating a log entry, the part of the log entry that identifies the user will look, for example, as follows:

`CN=John Smith,CN=Users,DC=LDAP,DC=local`

To let the log entry show the original user name, which might be `jsmith`, rather than the distinguished name, you can modify the rule set for LDAP authentication in a suitable manner.

Instead of having only a rule that authenticates a user under LDAP, the rule set should contain the following:

- A rule that handles LDAP authentication for a user and stores the original user name in a User-Defined property
- One or more rules that perform other LDAP-related activities, for example, retrieving information about the group that a user belongs to
- A rule that restores the original user name as the value of the `Authentication.Username` property after all LDAP-related activities have been completed

**Rule for authenticating a user and storing the user name**

The following rule stores the original user name after authenticating the user. An event in this rule sets the value of a User-Defined property accordingly.

**Name**

Authenticate user and store user name

**Criteria**

- `Authentication.IsAuthenticated equals false` AND
- `Authentication.Authenticate<LDAP> equals true`

**Action**

- Continue

The user name is retrieved by querying the directory on the LDAP server for this name. The settings of the `Authentication.Authenticate` property, which is responsible for authenticating the user, are configured accordingly.
When the query has been performed, the user name is stored as the value of the Authentication.Groups property. It is converted into a string, using the ListOfString.ToString property.

The original value of the converted property is a list of strings, as it might include not only the user name, but also other pieces of information, after all LDAP-related activities have been completed.

**Rule for retrieving user group information**

The following rule is an example for an additional LDAP-related activity. It retrieves information about the groups that a user belongs to.

Name

**Get user group information**

Criteria

Authentication.IsAuthenticated equals true AND Authentication.GetUserGroups<LDAP_Group_:Lookup> does not contain "no-group"

Action

Continue

To identify the user, the rule still needs to know the user's distinguished name, so the original user name can not yet be restored as the value of the Authentication.Username property.

You must create different settings and configure them for the Authentication module (engine) to run and retrieve a value for the Authentication.GetUserGroups property.

The name of these settings might, for example, be LDAP Group Lookup, as in this sample rule.

Within these settings, the Map user to DN option must be disabled.

**Rule for restoring the original user name**

The following rule restores the original user name as the value of the Authentication.UserName property.

Name

**Restore user name**

Criteria

Authentication.Authenticate<LDAP> equals false

Action

Stop Rule
Set

Event

Set Authentication.UserName=
User-Defined.Authentication.Username

An event in this rule sets this property to the value of the User-Defined property that you created to store the original user name in a preceding rule. The distinguished name that has temporarily been the value of this property is overwritten.

When the original user name has been restored, the property can be used for logging purposes.

**Testing and troubleshooting LDAP authentication**

Several activities can be completed for testing and troubleshooting the LDAP authentication process.

A tool for testing the configured authentication process with a given user name and password is available on the user interface of Web Gateway.
If running the tool shows that the process failed, carefully review what you have configured. If no errors can be found, you can create a debug log using another tool. If this does not explain the failure either, create a tcpcdump using a third tool.

**Test authentication for a given user name and password**
The settings for the Authentication module include a section for testing purposes. You can enter a username and password and let Web Gateway attempt to authenticate the user.

**Task**
1. Select Policy | Settings.
2. On the Engines branch of the settings tree, click the settings for the Authentication module (engine) that you have modified or newly created, for example, the LDAP settings.
3. Under Common Authentication Parameters, deselect Use authentication cache. Otherwise no changes in the directory on the LDAP server are detected until the cache expiration time has elapsed.
4. Expand Authentication Test and type a user name and password in the fields that are provided.
5. Click Authenticate User.
   The result of the authentication process is shown under Test result.
   • If the process is successfully performed, an OK message appears.
   The testing tool also displays any attribute values that you have configured queries for.
   • If the process fails, the following message appears: Error: Authentication failed.

**Create a debug log file for troubleshooting authentication**
You can create a debug log file to record the authentication process and review it for troubleshooting purposes.

**Task**
1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance that you want to create a debug log file on, then click Troubleshooting.
3. In the Authentication Troubleshooting section, select Log authentication events.

   **Tips**
   We recommend that you also select Restrict tracing to one IP and specify a client IP address to prevent the log file from becoming too large.

4. Reproduce the authentication process.
   A debug log file is created for the process.
5. Locate the debug log file.
   a. Select Troubleshooting
   b. On the troubleshooting tree, select the appliance that you created the debug log file on, then click Log files.
   c. Open the debug folder and look for the mwg-core.Auth.debug.log file with the appropriate time stamp.
The log file contains log lines showing failure IDs for the authentication process. The meaning of these IDs is as follows:

0 – NoFailure: Authentication was successful
2 – UnknownUser: Cannot map user name to user DN
3 – WrongPassword: Bind with user password failed
4 – NoCredentials: Credentials are missing or have invalid format
5 – NoServerAvailable: Could not get a server connection
6 – ProxyTimeout: Request is being processed longer than the configured timeout
8 – CommunicationError: Communication with server failed, for example, due to a timeout

Create a tcpdump for troubleshooting authentication

If the reason for a failed authentication process cannot be found by reviewing a debug log file, create a tcpdump to retrieve more information.

Task
1 Select Troubleshooting.
2 On the troubleshooting tree, select the appliance that you want to create a tcpdump on, then click Packet tracing.
3 In the Command line parameters field, type the following:
   "-s 0 -i any port 389"
   The port parameter lets Web Gateway connect to the LDAP server over an unencrypted port, which is required for troubleshooting purposes.
4 Click tcpdump start.
5 Reproduce the problem, then click tcpdump stop.
6 Open the trace using the wireshark tool. Then work with the ldap.bindResponse display filter to find a response from the LDAP server.

The server response usually includes LDAP, Active Directory, and other error codes. For example, in the following line from a server response:

"invalidCredentials (80090308: LdapErr: DSID-0c09030f, comment: AcceptSecurityContext error, data 773, vec)"

the 773 error code is an Active Directory error code meaning that the user password must be changed.

Instant messaging authentication

Instant messaging authentication ensures that users of your network cannot access the web through an instant messaging service if they are not authenticated. The authentication process looks up user information and asks unauthenticated users to authenticate.

The following elements are involved in this process:

• Authentication rules that control the process
• The Authentication module, which retrieves information about users from different databases
An authentication rule can use an event to log information on the authentication of users who requested access to the web.

In this case, a logging module is also involved in the process.

**Authentication rules**

Instant messaging authentication is not implemented by default on the appliance, but you can import the *IM Authentication* rule set from the library.

This rule set contains a rule that looks up user information to see whether users who request web access are already authenticated. The method used for looking up the information is the User Database method.

Unauthenticated users that no information can be found for in the user database are asked to submit their credentials for authentication.

Another rule looks up information using the Authentication Server method to see whether users are authenticated and asks unauthenticated users for their credentials.

The Authentication module is called by these rules to retrieve the user information from the appropriate databases.

You can review the rules in the library rule set, modify or delete them, and also create your own rules.

**Authentication module**

The Authentication module (also known as *engine*) retrieves information that is needed to authenticate users from internal and external databases. The module is called by the authentication rules.

The different methods of retrieving user information are specified in the module settings. Accordingly, two different settings appear in the rules of the library rule set for instant messaging communication:

- User Database at IM Authentication Server
- Authentication Server IM

These settings are implemented with the rule set when it is imported from the library.

You can configure these settings, for example, to specify the server that user information is retrieved from under the Authentication Server method.

**Logging module**

The library rule set for instant messaging authentication includes a rule that logs authentication-related data, such as the user name of a user who requested web access, or the URL of the requested web object.

The logging is handled by the FileSystemLogging module, which you can also configure settings for.

**Configure instant messaging authentication**

You can implement instant messaging authentication and adapt it to the needs of your network. Complete the following high-level steps.

**Task**

1. Import the IM Authentication rule set from the library.
2. Review the rules in the rule set and modify them as needed.
You can, for example, do the following:

- Modify the settings of the Authentication module for the User Database or the Authentication Server method.
- Modify the settings of the logging module that handles the logging of information about instant messaging authentication.

3 Save your changes.

**Configure the Authentication module for instant messaging authentication**

You can configure the Authentication module to specify how it retrieves the information that is needed to authenticate users of an instant messaging service.

**Task**

1 Select **Policy | Rule Sets**.

2 On the rule sets tree, select the rule set for instant message authentication.
   
   If you have imported this rule set from the library, it is the *IM Authentication* rule set.

   The rules of the rule set appear on the settings pane.

3 Make sure **Show details** is selected.

4 Find the rules that call the Authentication module.
   
   In the library rule set, these are the rules *Authenticate Clients against the User Database* and *Redirect Not Authenticated Clients to the Authentication Server*.

5 In the rule criteria, click the settings name of the settings you want to configure.
   
   This name appears next to the **Authentication. Authenticate** property.

   In the library rule set, it is the *User Database at IM Authentication Server IM* settings.

   The **Edit Settings** window opens. It provides the settings for the Authentication module.

6 Configure these settings as needed.

7 Click **OK** to close the window.

8 Click **Save Changes**.

**See also**

*Authentication settings on page 247*
Configure the File System Logging module for instant messaging authentication

You can configure the File System Logging module to specify how it logs information that is related to instant messaging authentication.

**Task**
1. Select **Policy | Rule Sets**.
2. On the rule sets tree, select the rule set for instant message authentication.
   - If you have imported this rule set from the library, it is the *IM Authentication* rule set.
   - The rules of the rule set appear on the settings pane.
3. Make sure **Show details** is selected.
4. Find the rule that calls the File System Logging module.
   - In the library rule set, this is the rule *Show Authenticated page*.
5. In the rule event, click the name of the settings for the module.
   - In the library rule set, this name is *IM Logging*.
   - The *Edit Settings* window opens. It provides the settings for the File System Logging module.
6. Configure these settings as needed.
7. Click **OK** to close the window.
8. Click **Save Changes**.

**See also**
*File System Logging settings on page 584*

**IM Authentication rule set**

The IM Authentication rule set is a library rule set for instant messaging authentication.

<table>
<thead>
<tr>
<th>Library rule set – IM Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Always</em></td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

The following rule sets are nested in this rule set:
- IM Authentication Server
- IM Proxy

**IM Authentication Server**

This nested rule set handles authentication for instant messaging users. It applies the User Database method for retrieving user information.

<table>
<thead>
<tr>
<th>Nested library rule set – IM Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Authentication.IsServerRequest equals true</em></td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when authentication has been requested for a user of an instant messaging service.
The rule set contains the following rules.

**Authenticate clients against user database**

Authenticate.Authenticate<User Database at IM Authentication server> equals false

The rule uses the `Authenticate.Authenticate` property to check whether a user who sends a chat message or file under an instant messaging protocol is authenticated. The settings that follow the property in the rule criteria specify the User Database method for this authentication.

If a user is not authenticated under this method, processing stops and a message is displayed asking the user to authenticate.

The action settings specify that the IM Authentication template is used for displaying the authentication message to the user.

Processing continues when the next user request is received.

**Show Authenticated page**

Always

Redirect<Show IM Authenticated> —

Set User-Defined.logEntry = "["

+ DateTime.ToISOString

+ "]"

+ URL.GetParameter ("prot")

+ "auth"

+ Authentication.Username

+ ""

+ URL.GetParameter ("scrn")

+ ""

FileSystemLogging.WriteLogEntry (User-Defined.logEntry)<IM Logging>

The rule redirects a request sent from a client by an instant messaging user to an authentication server and displays a message to inform the user about the redirect.

The action settings specify that the Show IM Authenticated template is used for the message.

The rule also uses an event to set values for a log entry on the authentication request. It uses a second event to write this entry into a log file. A parameter of this event specifies the log entry.

The event settings specify the log file and the way it is maintained.

**IM Proxy**

This nested rule set handles authentication of instant messaging users. It applies the Authentication Server method to retrieve user information.

<table>
<thead>
<tr>
<th>Nested library rule set – IM Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <code>Connection.Protocol.IsIM equals true AND IM.MessageCanSendBack is true</code></td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user sends a chat message or a file on a connection under an instant messaging protocol and a message can already be sent back from the appliance to the user.

The rule set contains the following rule.
Redirect not authenticated users to the authentication server

Authentication.Authenticate<Authentication Server IM> equals false --> Authenticate<IM Authentication>

The rule uses the Authentication.Authenticate property to check whether a user who sends a chat message or file under an instant messaging protocol is authenticated. The settings that follow the property in the rule criteria specify the Authentication Server method for this authentication.

If a user is not authenticated under this method, processing stops and a message is displayed, asking the user to authenticate.

The action settings specify that the IM Authentication template is used for displaying the authentication message to the user.

Processing continues when the next user request is received.

One-time passwords

One-time passwords (OTPs) can be processed on Web Gateway to authenticate users. This includes the use of passwords for authorized overriding when a web session has terminated due to quota expiration.

When a user sends a request for web access, authentication is first performed using one of the other authentication methods that are available on Web Gateway, for example, authentication based on information stored in the internal user database.

If the use of one-time passwords is configured, this authentication method is performed as a second step. Web Gateway informs the user that a one-time password is also needed for web access and upon the user's request for such a password, it forwards the user name to a McAfee® One Time Password (McAfee OTP) server and asks the server to provide a password.

If the request is granted, the McAfee OTP server returns a one-time password, which is, however, not exposed to Web Gateway. In its response, the McAfee OTP server also includes what is called "context" information in a header field.

The context information lets the password field and submit button in the page that was presented to the user be activated, so the user can click the button, which submits the one-time password and lets the user access the requested web object.

To implement the use of one-time passwords on Web Gateway, you can import a rule set from the rule set library. After importing the rule set, default settings are provided, which you can configure to adapt them to the needs of your network.

The settings that need to be configured include the IP address or host name of the McAfee OTP server and the port on this server that listens to requests from Web Gateway.

A user name and password for Web Gateway to authenticate to the McAfee OTP server are also required.

If the communication between Web Gateway and the McAfee OTP server should be SSL-secured, you need to import a certificate for use in this communication.

The McAfee OTP server must be configured for working with Web Gateway to handle the authentication process.

One-time passwords for authorized overriding

When quota restrictions are imposed on web usage from within your network, a one-time password can be used as the password that is required to override the termination of a web session due to quota expiration.
To implement the use of one-time passwords for authorized overriding, you can import a different rule set from the library, which also allows you to configure the settings for the authentication process.

**Using one-time passwords from a McAfee Pledge device**

One-time passwords for authenticating users or performing an authorized override can be provided by a McAfee® Pledge device.

To enable this method of using one-time passwords for the authentication process, you need to implement suitable rule sets, which you can import from the rule set library. Settings for the authentication process are implemented with the import.

For more information on working with a McAfee Pledge device, refer to the documentation for this product.

**Configure one-time passwords for authenticating users**

To configure the use of one-time passwords for authenticating users, complete the following high-level steps.

**Task**
1. Import the *Authentication Server (Time/IP Based Session with OTP)* rule set from the rule set library.
   
   When using one-time passwords from a McAfee Pledge device, import the *Authentication Server (Time/IP Based Session with OTP and Pledge)*
   
   The rule sets are located in the *Authentication* rule set group.

2. Configure the settings for one-time passwords.

3. Save your changes.

For information on how to configure the McAfee OTP server for working with Web Gateway, refer to the McAfee OTP server documentation.

**Configure one-time passwords for authorized overriding**

To configure the use of one-time passwords for authorized overriding, complete the following high-level steps.

**Task**
1. Import the *Authorized Override with OTP* rule set from the rule set library.
   
   When using one-time passwords from a McAfee Pledge device, import *Authorized Override with OTP and Pledge*.
   
   The rules sets are located in the *Coaching/Quota* rule set group.

2. Configure the settings for one-time passwords.

3. Save your changes.

For information on how to configure the McAfee OTP server for working with Web Gateway, refer to the McAfee OTP server documentation.
Configure the settings for one-time passwords

Settings for one-time passwords are implemented with default values after importing the rule sets that handle the use these passwords. Configure these settings to adapt them to the requirements of your network.

You need to configure different settings for authentication and authorized overriding with one-time passwords.

**Task**

1. Select Policy | Settings.

2. On the Engines branch of the settings tree, expand Authentication.

3. To configure settings for using one-time passwords to authenticate users, complete the following substeps. Otherwise continue with step 4.
   
   a. Click OTP.  
   
   The OTP settings appear on the settings pane.

   b. Configure the settings in the One-Time Password Specific Parameters section and the settings in the other sections, which are common authentication settings, as needed.

   c. Click IP Authentication Server.  
   
   The IP Authentication Server settings appear on the settings pane.

   d. Configure the settings in the IP Authentication Server Specific Parameters section and the settings in the other sections, which are common authentication settings, as needed.

   e. Click User Database at Authentication Server.  
   
   The User Database at Authentication Server settings appear on the settings pane.

   f. Configure the settings in the User Database Specific Parameters section and the settings in the other sections, which are common authentication settings, as needed.

   Then continue with step 5.

4. To configure settings for using one-time passwords in authorized overriding, complete the following substeps.

   a. Click OTP.  
   
   The OTP settings appear on the settings pane.

   b. Configure the settings in the One-Time Password Specific Parameters section and the settings in the other sections, which are common authentication settings, as needed.

5. Click Save Changes.

**Authentication Server (Time/IP Based Session with OTP) rule set**

The Authentication Server (Time/IP Based Session with OTP) rule set is a library rule set that enables the use of one-time passwords for authenticating users.

<table>
<thead>
<tr>
<th>Library rule set – Authentication Server (Time/IP Based Session with OTP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The following rule sets are nested in this rule set:
• Check for Valid Authentication Session

• Authentication Server

**Check for Valid Authentication Session**

This nested rule redirects a user's request sent from a client to the authentication server if the user has not yet been successfully authenticated on that server.

### Nested library rule set – Check for Valid Authentication Session

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies if the request that is currently processed is not requesting a connection to the authentication server and the protocol used in this communication is one of the four that are specified.

The rule set contains the following rules:

**Fix hostname**


The rule uses an event to set the host name that is submitted with the URL of a request to a particular value, which is required when communication is going on under the SSL protocol. This value is the common name of the certificate that is provided in this communication.

The rule applies if the request that is processed contains the CERTVERIFY command and no wildcards are allowed for the common name.

**Redirect clients that do not have a valid session to the authentication server**

*Authentication.Authenticate<IP Authentication Server> equals false AND Command.Name does not equal "CONNECT"* –> Authenticate<Default>

The rule uses the Authentication.Authenticate property to check whether the user who sends a request is successfully authenticated at the user database of the authentication server. For this purpose, the IP address of the client that the request was sent from is evaluated.

The Command.Name property is used to check whether the request is a connection request in SSL-secured communication.

If neither is the case, the user is asked to submit credentials for authentication. This action is executed with the specified settings.

**Revalidate session under ideal conditions**

*Authentication.CacheRemainingTime less than 400 AND Connection.Protocol equals "HTTP" AND Command.Name equals "GET"* –> Authenticate<Default>

Under particular conditions (which could be termed "ideal"), a user is asked to authenticate again after sending a request to ensure the current web session is prolonged before the time quota has elapsed completely.
This is done if communication is going on under the HTTP protocol and the request contains the GET command.

The rule is not enabled by default.

**Authentication Server**

This nested rule set forwards a request for web access when a user submitted a valid one-time password. A user who could not submit a valid one-time password is asked to authenticate.

Authentication is first performed using information from the user database on an authentication server. A successfully authenticated user is then informed that web access also requires a one-time password, which is sent by Web Gateway upon the user's request.

<table>
<thead>
<tr>
<th>Nested library rule set – Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authentication.IsServerRequest equals true</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user who sent a request must be authenticated using information from an authentication server.

The rule set contains the following rules:

**Redirect if we have a valid OTP**

*Authentication.Authenticate<OTP> equals true* -> Redirect <Redirect Back from Authentication Server>

The rule uses the *Authentication.Authenticate* property to check whether a user who submitted a one-time password with a request for web access could be successfully authenticated.

If this is the case, web access is allowed and the user is redirected from the authentication server to the requested web object.

**Stop after providing an invalid OTP**

*Authentication.Failed equals true* -> Block<Authorized Only>

The rule uses the *Authentication.Failed* property to check whether a user who submitted a one-time password with a request for web access could not be successfully authenticated.

If this is the case, the request is blocked and a message informs the user about the blocking and the block reason.

**Authenticate user against user database**

*Authentication.Authenticate<User Database at Authentication Server> equals false* -> Authenticate<Default>

The rule uses the *Authentication.Authenticate* property to check whether a user who sent a request and submitted an invalid one-time password could be successfully authenticated at the user database on the authentication server.

If this is not the case, the user is asked to authenticate.

**Send OTP if requested**

*Header.Exists(Request.OTP) equals true* -> Continue – Authentication.SendOTP<OTP>

If none of the preceding rules in this rule set has applied, it means no valid one-time password was submitted by a user who sent a request for web access, but authentication at the user database on the authentication server was successful.

Then this rule is processed, which uses the *Header.Exists* property to check whether the request has a header providing the information that sending a one-time password is requested.

If this is the case, the rule uses an event to send a one-time password to the user.
**Return authentication data to client**

`Header.Exists("Request.OTP") equals true -> Block<Authentication Server OTP> – `  

The rule uses the `Header.Exists` property to check whether there is a header in a request with information that sending a one-time password is requested.

If this is the case, the request is blocked and a message sent to inform the user who sent the request that a one time password is required for access.

An event is also triggered that adds a header with context information about the one-time password authentication process to the block message.

The first of the two event parameters specifies the header information that is added. The second parameter is a property that has information about the one-time password authentication process as its value, which is the source of the added information.

**Block request and offer sending OTP**

`Always -> Block<Authentication Server OTP>`

If none of the preceding rules in this rule set have applied, the Block action of this rule is always executed.

The action stops rule processing and the request is not forwarded.

The action settings specify that a message is sent to inform the user that a one-time password is required for web access, which can be obtained from Web Gateway.

**Authorized Override with OTP rule set**

The Authorized Override with OTP rule set is a library rule set for enabling the use of one-time passwords in authorized overriding.

<table>
<thead>
<tr>
<th>Library rule set – Authorized Override with OTP and Pledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – SSL.ClientContext.IsApplied equals true OR Command.Name does not equal &quot;CONNECT&quot;</td>
</tr>
</tbody>
</table>
| Cycles – Requests (and IM) |}

The rule criteria specified that the rule set applies when SSL-secured communication is configured or the request that is currently processed is not a CONNECT request, which is usually sent at the beginning of this communication.

The following rule sets are nested in this rule set:

- Verify OTP
- OTP Needed?

**Verify OTP**

This nested rule checks whether a user who sends a one-time password with a request for authorized overriding is successfully authenticated and performs a redirect to the requested web object if this is true.

<table>
<thead>
<tr>
<th>Nested library rule set – Verify OTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Quota.AuthorizedOverride.IsActivationRequest.Strict&lt;Default&gt; equals true</td>
</tr>
</tbody>
</table>
| Cycles – Requests (and IM) |}

The rule set criteria specifies that the rule set applies when a user sends a request to override the termination of a web session due to quota expiration and to continue with the session.
The rule set contains the following rules:

**Verify OTP**

*Authentication.Authenticate<OTP> equals false* → *Block<Authorized Only>*

The rule uses the *Authentication.Authenticated* property to check whether the user who submitted a one-time password when sending an authorized overriding request has been successfully authenticated.

If this is not the case, the request is blocked and the user is informed about the blocking and the reason for it.

The Block action is executed with the specified settings.

**The session is validated. Redirect to the original page**

*Always* → *Redirect<Default>*

If authentication of a user who submitted a one-time password with a request for authorized overriding did not fail, the preceding rule in this rule set does not apply and processing continues with this rule.

The rule always allows the user to continue with the current session and performs a redirect to the requested web object.

The Redirect action is executed with the specified settings.

**OTP Needed?**

This nested rule set provides a one-time password for a user who sends a request for authorized overriding if the requested web object is located on a host within the corporate domain of McAfee.

<table>
<thead>
<tr>
<th>Nested library rule set – OTP Needed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – *URL.Host matches <em>mcafee.com</em></td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when the host of the URL sent in a request is located within the corporate domain of McAfee.

The rule set contains the following rules:

**Send OTP if requested**

*Header.Exists(Request.OTP) equals true* → *Continue – Authentication.SendOTP<OTP>*

If none of the proceeding rules in this rule set have applied when processing a request, it means no valid one-time password was submitted by the user who sent the request, but authentication at the user database of the authentication server was successful.

Then this rule is processed, it uses the *Header.Exists* property to check whether the request has a header providing the information that sending a one-time password is requested.

If this is the case, an event is triggered that send a one-time password to the user.

**Return authentication data to client**

*Header.Exists(Request.OTP) equals true* → *Block<Authentication Server OTP>* → *Header.Block.Add("OTP Context", Authentication.OTP.Context<OTP>)*

The uses the *Header.Exists* property to check whether the request has a header providing the information that sending a one-time password is requested.

If none of the proceeding rules in this rule set have applied when processing a request, it means no valid one-time password was submitted by the user who sent the request, but authentication at the user database of the authentication server was successful.

If this is the case, the request is not forwarded and an event is triggered that sets a particular property to a value that provides information about the authentication of the user.
The Block action is executed with the specified settings, which require that a message is sent to inform the user about the reason of the blocking.

The information that the event provides is specified by the OTP.Context event parameter. The property that has its value set to this information is specified in a second parameter.

**Block request and offer sending OTP**

*Always* –> Block<Authentication Server OTP>

If none of the preceding rules in this rule set have applied when processing a request, the action of this rule is always executed.

It stops rule processing and the request is not forwarded. The action settings specify that a message is sent to inform the user that a one-time password can be obtained from Web Gateway.

**Authentication Server (Time/IP Based Session with OTP and Pledge) rule set**

The Authentication Server (Time/IP Based Session with OTP and Pledge) rule set is a library rule set for authenticating users through one-time passwords that are provided by a McAfee Pledge device.

<table>
<thead>
<tr>
<th>Criteria – Authentication Server (Time/IP Based Session with OTP and Pledge)</th>
<th>Cycle – Requests (and IM)</th>
</tr>
</thead>
</table>

The following rule sets are nested in this rule set:

- Check for Valid Authentication Session
- Authentication Server

**Check for Valid Authentication Session**

This nested rule redirects a user's request sent from a client to the authentication server if the user has not yet been successfully authenticated on that server.

<table>
<thead>
<tr>
<th>Nested library rule set – Check for Valid Authentication Session</th>
<th></th>
</tr>
</thead>
</table>

The rule set criteria specifies that the rule set applies if the request that is currently processed is not requesting a connection to the authentication server and the protocol used in this communication is one of the four that are specified.

The rule set contains the following rules:

**Fix hostname**

The rule uses an event to set the host name that is submitted with the URL of a request to a particular value, which is required when communication is going on under the SSL protocol. This value is the common name of the certificate that is provided in this communication.

The rule applies if the request that is processed contains the CERTVERIFY command and no wildcards are allowed for the common name.

**Redirect clients that do not have a valid session to the authentication server**

Authentication.Authenticate<IP Authentication Server> equals false AND Command.Name does not equal "CONNECT" –> Authenticate<Default>

The rule uses the Authentication.Authenticate property to check whether the user who sends a request is successfully authenticated at the user database of the authentication server. For this purpose, the IP address of the client that the request was sent from is evaluated.

The Command.Name property is used to check whether the request is a connection request in SSL-secured communication.

If neither is the case, the user is asked to submit credentials for authentication. This action is executed with the specified settings.

**Revalidate session under ideal conditions**

Authentication.CacheRemainingTime less than 400 AND Connection.Protocol equals "HTTP" AND Command.Name equals "GET"

→ Authenticate<Default>

Under particular conditions (which could be termed "ideal"), a user is asked to authenticate again after sending a request to ensure the current web session is prolonged before the time quota has elapsed completely.

This is done if communication is going on under the HTTP protocol and the request contains the GET command.

The rule is not enabled by default.

**Authentication Server**

This nested rule set forwards a request for web access by a user who submitted a valid one-time password that was retrieved from a McAfee Pledge device.

A user who did not submit a valid one-time password is asked to authenticate. Authentication is first performed using information from the user database of the authentication server.

A successfully authenticated user is then informed that web access also requires a one-time password from a McAfee Pledge device.

### Nested library rule set – Authentication Server

**Criteria** – Authentication.IsServerRequest equals true

**Cycle** – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user who sent a request must be authenticated using information from an authentication server.

The rule set contains the following rules:

**Authenticate user against user database**

Authentication.Authenticate<User Database at Authentication Server> equals false –> Authenticate<Default>
The rule uses the `Authentication.Authenticate` property to check whether a user who sent a request and submitted an invalid one-time password could be successfully authenticated at the user database on the authentication server.

If this is not the case, the user is asked to authenticate.

**Show block template**

`URL.GetParameter(pledgeOTP) equals " "` → `Block<Authentication.Server OTP with PledgeOTP>`

The rule uses the `URL.GetParameter` property to check whether a one-time password from a McAfee Pledge device was sent as a parameter of the URL in a request.

If the parameter is empty, the request is blocked and the user is informed that authentication using a one-time password from a McAfee Pledge device is also required for web access.

**Retrieve OTP context**

`Always` → `Continue` → `Authentication.SendOTP<OTP>`

The rule uses an event to send context information on the one-time password authentication process to an authenticated user.

This way the information is retrieved that is required to validate a one-time password on a McAfee OTP server.

**Redirect back if we have a valid OTP**

`Authentication.Authenticate<OTP> equals true` → `Redirect<Redirect Back from Authentication Server>`

The rule uses the `Authentication.Authenticate` property to check whether a user who submitted a one-time password with a request for web access could be successfully authenticated.

If this is the case, web access is allowed and the user is redirected from the authentication server to the requested web object.

**Stop after providing an invalid OTP**

`Authentication.Failed equals true` → `Block<Authorized Only>`

The rule uses the `Authentication.Failed` property to check whether a user who submitted a one-time password with a request for web access could not be successfully authenticated.

If this is the case, the request is blocked and a message informs the user about the blocking and the block reason.

**Authorized Override with OTP and Pledge rule set**

The Authorized Override with OTP and Pledge rule set is a library rule set for authorized overriding using one-time passwords that are provided by a McAfee Pledge device.

<table>
<thead>
<tr>
<th>Library rule set – Authorized Override with OTP and Pledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <code>SSL.ClientContext.IsApplied equals true OR Command.Name does not equal &quot;CONNECT&quot;</code></td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule criteria specified that the rule set applies when SSL-secured communication is configured or the request that is currently processed is not a CONNECT request, which is usually sent at the beginning of this communication.

The following rule sets are nested in this rule set:
- Verify OTP
- OTP Needed?

**Verify OTP**
This nested rule checks whether a user who sends a one-time password with a request for authorized overriding is successfully authenticated and performs a redirect to the requested web object if this is true.

<table>
<thead>
<tr>
<th>Nested library rule set – Verify OTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Quota.AuthorizedOverride.IsActivationRequest.Strict&lt;Default&gt; equals true</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user sends a request to override the termination of a web session due to quota expiration and to continue with the session.

The rule set contains the following rules:

**Verify OTP**

Authentication.Authenticate<OTP> equals false –> Block<Authorized Only>

The rule uses the Authentication.Authenticated property to check whether the user who submitted a one-time password when sending an authorized overriding request has been successfully authenticated.

If this is not the case, the request is blocked and the user is informed about the blocking and the reason for it.

The Block action is executed with the specified settings.

**The session is validated. Redirect to the original page**

Always –> Redirect<Default>

If authentication of a user who submitted a one-time password with a request for authorized overriding did not fail, the preceding rule in this rule set does not apply and processing continues with this rule.

The rule always allows the user to continue with the current session and performs a redirect to the requested web object.

The Redirect action is executed with the specified settings.

**OTP Needed?**
This nested rule set provides a one-time password for a user who sends a request for authorized overriding if the requested web object is located on a host within the corporate domain of McAfee.

<table>
<thead>
<tr>
<th>Nested library rule set – OTP Needed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – URL.Host matches <em>mcafee.com</em> AND Quota.AuthorizedOverride.SessionExceeded&lt;Default&gt; equals true</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when the host of the URL sent in a request is located within the corporate domain of McAfee and the time quota for a session that can be continued after an authorized override has been exceeded.

The rule set contains the following rules:

**Retrieve OTP context**

Always –> Continue – Authentication.SendOTP<OTP>
The rule uses an event to send a one-time password to an authenticated user. This way the context information is obtained that is required for authenticating a user through a one-time password that is validated on a McAfee OTP server.

**Block request and offer sending OTP**

*Always –> Block<OTP Required with Pledge>*

The rule blocks a request for web access. The action settings specify that a message is sent to inform the user web access can be allowed after submitting a one-time password that can be obtained from a McAfee Pledge device.

---

**Client Certificate authentication**

Submitting a client certificate can be configured as a method of accessing the user interface of the appliance. This method is known as *Client Certificate authentication or X.509 authentication*.

Client Certificate authentication is one of the methods you can choose for the authentication procedure when configuring the proxy functions of the appliance.

The following applies to the method when using it in proxy configuration.

- No user name and password is required to authenticate a user who sends a request, as is the case with other methods such as NTLM or LDAP.

- The method can be implemented for requests that are sent in SSL-secured communication from a web browser on a client to an appliance that is configured in explicit proxy mode.

- The protocol used for this communication is HTTPS.

A client certificate is submitted when the SSL handshake is performed as one of the initial steps in the communication between the appliance and a client. The request is then redirected to an authentication server to validate the certificate.

If it is valid, authentication is successfully completed for the client and the request is eventually forwarded to the appropriate web server.

When running multiple appliances as nodes in a configuration, it is important that the authentication server resides on the node that a request was originally directed to.

Also forwarding to the web after successful authentication must be done from the same node.

Use of an authentication server for Client Certificate authentication is controlled by rules. You can import an authentication server rule set and modify the rules in its nested rule sets to enable the use of appropriate certificates.

You must also implement a way to let Client Certificate authentication be applied. A recommended way of doing this is using cookie authentication.

If this method is implemented, authentication is required for a client that a request was sent from, but a cookie is set for this client after a certificate has been submitted and recognized as valid once. Submitting a certificate is then not required for subsequent requests from that client.

You can import and modify a rule set for having Client Certificate authentication handled in this way.
Use of certificates for Client Certificate authentication

Different types of certificates are required for performing authentication under the Client Certificate authentication method, which can be implemented for SSL-secured communication.

Client certificate

A client certificate is needed to certify the identity of a client that sends a request to the appliance.

Only if the client is trusted will a request that it sends be accepted. A client is trusted if the certificate that is submitted with the request has been signed by a Root CA (certificate authority) that is trusted.

Under the Client Certificate authentication method, the client certificate is also used for authentication. Authentication is successfully completed if the client certificate that is submitted with a request has been signed by a trusted certificate authority.

Server certificate

A server certificate is needed to certify the identity of a server that is involved in SSL-secured communication.

A server is trusted by a client if the certificate that it sends during the initial steps of the communication has been signed by a Root CA (certificate authority) that is also trusted by the client.

Under the Client Certificate authentication method, a server certificate is needed for the authentication server.

Root CA

A Root CA (certificate authority) is an instance that signs other certificates.

In SSL-secured communication, a Root CA appears itself as a certificate that can be viewed in the communication process.

If a Root CA is trusted by a client or server, certificates that have been signed by it are trusted as well, which means that if a client or server submits such a signed certificate, it is trusted.

Rule sets for Client Certificate authentication

Rule sets for implementing the Client Certificate authentication method are available in the rule set library.

Authentication Server (for X509 Authentication) rule set

The Authentication Server (for X509 Authentication) rule set uses several nested rule sets to handle use of the authentication server under the Client Certificate authentication method.

- **SSL Endpoint Termination** — Prepares the handling of requests in SSL-secured communication
  - **Accept Incoming HTTPS Connections** — Provides the certificates that can be submitted for the authentication server
  - **Content Inspection** — Enables inspection of the content that is transmitted with a request
• **Authentication Server Requests** — Redirects requests back to the proxy on the appliance for further processing after authentication on the authentication server was completed successfully.

Requests are also redirected if a cookie has been set for a client that a request was sent from.

If authentication could not be completed successfully on the authentication server, the user is asked to submit credentials for authentication on the user database.

• **Block All Others** — Blocks requests for which authentication was not completed successfully.

**Cookie Authentication (for X509 Authentication) rule set**

The Cookie Authentication (for X509 Authentication) rule set uses several nested rule sets to initiate use of the Client Certificate authentication method and handle the setting of cookies.

• **Cookie Authentication at HTTP(S) Proxy** — Contains nested rule sets that handle Client Certificate authentication with cookies.

  • **Set Cookie for Authenticated Clients** — Sets a cookie after authentication has been successfully completed once for a client and redirects the request that the client sent back to the proxy on the appliance for further processing.

  • **Authenticate Clients with Authentication Server** — Redirects requests sent from clients for which no cookie has been set to the authentication server.

**Redirecting requests to an authentication server**

Under the Client Certificate authentication method, a request is redirected to an authentication server for validating the client certificate that was submitted with it. The redirecting can be done using a special listener port on the appliance or a unique host name.

**Using a special listener port**

Requests can be redirected to an authentication server using a special listener port, for example, port 444. Suppose the IP address of an appliance is 192.168.122.119, then a request will be redirected to the authentication server by:

https://192.168.122.119:444/
However, it is important to consider whether exceptions from using a proxy have been configured for the web browser on a client that sends the request.

- **No proxy exceptions configured** — If no proxy exceptions have been configured, all requests are sent to the proxy port that is listening for them on the appliance, which is port 9090 by default.

   Even a request to `https://192.168.122.119:444/` will arrive on port 9090 if this is the configured proxy port.

   If a firewall is part of your network configuration, no exceptions from the firewall rules are needed because there is no connection from the client to port 444.

   To ensure requests are redirected to the authentication server, 444, or another value that you want to use for this purpose, must be configured for the `URL.Port` property in the criteria of the Authentication Server (for X509 Authentication) rule set.

   The value of the `URL.Port` property is the port contained in the URL that is specified by a request. It can be, for example, 444, even if the request actually arrives at port 9090.

- **Proxy exceptions configured** — Proxy exceptions can be configured for various reasons. For example, a web browser could be configured not to use proxies for accessing local hosts.

   A request to `https://192.168.122.119:444/` will then not arrive at port 9090.

   Because the browser is configured to access its destination directly, it will try to connect to the appliance on port 444. This means that you need to set up a listener port with port number 444.

   If firewall rules are in place, an exception is also needed to allow requests to arrive at port 444.

   To ensure requests are processed by the appropriate rules, 444, or another value that you want to use for this purpose, must be configured for the `Proxy.Port` property in the criteria of the Authentication Server (for X509 Authentication) rule set.

   The value of the `Proxy.Port` property is the port that a request actually arrives at. It is, for example, 444 if you have set up a port with this number for receiving requests that are to be redirected to an authentication server.

**Using a unique host name**

Requests can be redirected to an authentication server using a unique host name, for example, authserver.local.mcafee. Using this name, requests are redirected to the authentication server by:

`https://authserver.mcafee.local`

The client that the request was sent from must not try to look up the host name using DNS, as the URL will most likely not resolve and the client will be unable to connect.

To ensure that requests are processed by the appropriate rules, this host name must be configured as the value for the `URL.Host` property in the criteria of the Authentication Server (for X509 Authentication) rule set.

**Implement Client Certificate authentication**

The Client Certificate authentication method uses client certificates that are sent with requests for authentication. To implement this method on the appliance, complete the following high-level steps.

**Task**

1. Import the Authentication Server (for X509 Authentication) rule set.
2. Modify the nested rule sets to configure the use of appropriate certificates.
3 Configure a listener port for requests sent by web browsers that are not using the proxy port on the appliance.

4 Configure a way to let Client Certificate authentication be applied.
   You can import and modify the Cookie Authentication (for X509 Authentication) rule set to use a cookie for authentication after Client Certificate authentication has been applied once and successfully been completed.

5 Make sure a suitable client certificate is available on a web browser that is used for sending requests to the appliance.

**Import the Authentication Server (for X509 Authentication) rule set**

To implement the Client Certificate authentication method on the appliance, there must be a rule set that handles authentication in this way. You can import the Authentication Server (for X509 Authentication) rule set for this purpose.

We recommend that you insert the rule set at the top of the rule sets tree.

**Task**

1 Select Policy | Rule Sets.

2 On the rule sets tree, navigate to the position where you want to insert the rule set and click Add.

3 Click Top Level Rule Set, then click Import Rule Set from Library.

   The Add from Rule Set Library window opens.

4 Select the Authentication Server (for X509 Authentication) rule set and click OK.
   If conflicts arise from the import, they are displayed next to the list of rule sets. Follow one of the suggested procedures for solving them before clicking OK.

   The rule set is inserted with its nested rule sets in the rule sets tree.

5 Review the rule set criteria and modify them if necessary.
   After the import, the criteria is:

   URL.Port equals 444 or Proxy.Port equals 444.

   This ensures that the rule set is applied to all requests coming in on that port. If you want to use a different port, specify its port number here.

**Modify a rule set to configure the use of server certificates**

The Authentication Server (for X509 Authentication) rule set needs to be modified to ensure appropriate server certificates are submitted for the authentication server. The modification is done in a nested rule set.

Because it is possible to reach the authentication server under different host names and IP addresses, you can let the appliance submit a different server certificate each time, so that the host name or IP address is matched by the common name in the certificate.

To achieve this, you need to import a server certificate for each host name or IP address and add it to the list of server certificates.
**Task**

2. Expand the nested SSL Endpoint Termination rule set and, within this rule set, select the nested Accept Incoming HTTPS Connections rule set.
3. In the Set client context rule, click the Proxy Certificate event settings. The Edit Settings window opens.
4. In the Define SSL Context section, review the list of server certificates.
5. To add a server certificate to the list:
   - a. Click the Add icon above the list. The Add Host to Certificate Mapping window opens.
   - b. In the Host field, enter the host name or IP address that the certificate should be submitted for.
   - c. Click Import. The Import Server Certificate window opens.
   - d. Click Browse and browse to the certificate you want to import.
   - e. Repeat this activity to import a key and certificate chain with the certificate.
   - f. Click OK. The window closes and the import is performed. The certificate information appears in the Add Host to Certificate Mapping window.
6. [Optional] In the Comment field, type a plain-text comment on the server certificate.
7. Click OK. The window closes and the server certificate appears in the list.
8. Make sure the SSL-Scanner functionality applies only to client connection checkbox is selected.
   This lets the appliance accept requests from its clients without contacting other servers of the network, which is not required in this communication.
9. Click OK to close the Edit Settings window.
10. Click Save Changes.

**Modify a rule set to configure the use of certificate authorities**

The Authentication Server (for X509 Authentication) rule set needs to be modified to ensure appropriate Root CAs (certificate authorities) are configured. The modification is done in a nested rule set.

A client certificate is trusted if signed by a certificate authority from the list that is maintained on the appliance. You need to import all certificate authorities into the list that you want to be signing instances for trusted client certificates.

**Task**

2. Expand the nested SSL Authentication Server Request rule set.
3. In the Ask user for client certificate rule, click the **X509 Auth** module settings. The *Edit Settings* window opens.

4. In the **Client Certificate Specific Parameters** section, review the list of certificate authorities.

5. To add a certificate authority to the list:
   a. Click the **Add** icon above the list.
      The *Add Certificate Authority* window opens.
   b. In the **Host** field, enter the host name or IP address that the certificate should be submitted for.
   c. Click **Import**.
      A window providing access to your local file system opens.
   d. Browse to the certificate authority file you want to import.
   e. Click **OK**.
      The window closes and the import is performed. The certificate appears in the *Add Certificate Authority* window.

6. Make sure the **Trusted** checkbox is selected.

7. [Optional] In the **Comment** field, type a plain-text comment on the certificate authority.

8. Click **OK**.
   The window closes and the certificate authority appears in the list.

9. Click **OK** to close the *Edit Settings* window.

10. Click **Save Changes**.

### Configure a listener port for incoming requests on the appliance

Requests that are sent to the appliance can be received on the proxy port or a special listener port. The proxy port is port 9090 by default. You need to configure a listener port if proxy exceptions have been created that prevent requests from arriving at the proxy port.

**Task**

1. Select **Configuration** | **Appliances**.

2. On the appliances tree, select the appliance you want to configure a listener port on and click **Proxies (HTTP(S), FTP, ICAP, and IM)**.
   The proxy settings appear on the settings pane.

3. Scroll down to the **HTTP Proxy** section.

4. Make sure **Enable HTTP proxy** is selected.

5. On the toolbar of the **HTTP port definition list**, click the **Add** icon.
   The *Add HTTP Proxy Port* window opens.
Configure a listener port as follows:

a. In the **Listener address** field, type `0.0.0.0:444`.
   
   If you want to use a different port for listening to incoming requests, type it here.

b. In the **Ports treated as SSL** field, type `*`.

c. Make sure all other checkboxes are selected.

7. Click **OK** to close the **Edit Settings** window.

8. Click **Save Changes**.

9. Restart the appliance to make the configuration of the listener port effective.

**Import the Cookie Authentication (for X509 Authentication) rule set**

When the Client Certificate authentication method is used on the appliance, use of this method can be initiated by the Cookie Authentication (for X509 Authentication) rule set.

We recommend that you insert this rule set after the rules sets for functions that do not require authentication, but before the rule sets that handle the filtering functions.

This ensures the filtering functions are not executed when a request is blocked because authentication failed, which saves resources and improves performance.

If your rule set system is similar to the default system, you can insert the rule set after the SSL Scanner and Global Whitelist rule sets, but before the Content Filtering and Gateway Antimalware rule sets.

**Task**

1. Select **Policy | Rule Sets**.

2. On the rule sets tree, navigate to the position where you want to insert the rule set and click **Add**.

3. Click **Top Level Rule Set**, then click **Import Rule Set from Library**.

   The **Add from Rule Set Library** window opens.

4. Select the **Cookie Authentication (for X509 Authentication)** rule set and click **OK**.

   If conflicts arise from the import, they are displayed next to the list of rule sets. Follow one of the suggested procedures for solving them before clicking OK.

   The rule set is inserted with its nested rule sets in the rule sets tree.

**Modify a rule set to change the listener port for incoming requests**

You can modify the Cookie Authentication (for X509 Authentication) rule set to configure a listener port for incoming requests that you want to use instead of port 444, which is the default port. The modification is done in a nested rule set.

A special listener port must be used for receiving incoming requests if proxy exceptions are in place that prevent requests from arriving at the proxy port of the appliance. Requests that arrive at port 444 or a different port you have configured for this purpose are redirected to the authentication server.
**Task**

1. Select **Policy | Rule Sets** and expand the **Cookie Authentication (for X509 Authentication)** rule set.

2. Expand the nested **Cookie Authentication at HTTP(S) Proxy** rule set and, within this rule set, select the nested **Authenticate Clients with Authentication Server** rule set.

3. In the **Set client context** rule, click the **Proxy Certificate** event settings.

   The **Edit Settings** window opens.

4. In the **Authentication Server Specific Parameters** section, review the URL in the **Authentication server URL** field.

   The URL is by default as follows:

   https://$<propertyInstance useMostRecentConfiguration="false" propertyId="com.scur.engine.system.proxy.ip"/>$:444

   When the rule is processed, the $...$ term is replaced by the IP address of the appliance.

5. To configure a different listener port, type the number of this port here.

6. Click **OK** to close the **Edit Settings** window.

7. Click **Save Changes**.

**Import a client certificate into a browser**

A suitable client certificate must be available on a web browser to be sent with a request to an appliance in SSL-secured communication.

Procedures for importing certificates vary for different browsers and are subject to change. Browser menus can also vary depending on the operating system you are using.

The following are two possible procedures for importing a client certificate into Microsoft Internet Explorer and Mozilla Firefox.

**Tasks**

- **Import a client certificate into Microsoft Internet Explorer** on page 300
  
  You can import a client certificate and make it available on Microsoft Internet Explorer for presenting it in SSL-secured communication.

- **Import a client certificate into Mozilla Firefox** on page 301
  
  You can import a client certificate and make it available on Mozilla Firefox for presenting it in SSL-secured communication.

**Import a client certificate into Microsoft Internet Explorer**

You can import a client certificate and make it available on Microsoft Internet Explorer for presenting it in SSL-secured communication.

**Before you begin**

To import the certificate file, you must have stored it within your local file system.

**Task**

1. Open the browser and on the top-level menu bar, click **Tools**, then click **Internet Options**.

   The **Internet Options** window opens.

2. Click the **Content** tab.
In the Certificates section, click Certificates.

The Certificates window opens.

Click Import.

The Certificate Import Wizard appears.

On the wizard pages, proceed as follows:

a. On the Welcome page, click Next.

b. On the File to Import page, click Browse and navigate to the location where you stored the certificate file.

c. In the File Name field, type *.pfx, then press Enter.

d. Select the certificate file and click Open, then click Next.

e. On the Password page, type a password in the Password field. Then click Next.

f. On the Certificate Store page, click Place all certificates in the following store.

g. In the Certificate Store section on the same page, select Personal, then click Next.

h. On the Completing the Certificate Import Wizard page, click Finish.

Confirm the message that appears by clicking OK.

Click Close, then click OK to close the Certificates and Internet Options windows.

Import a client certificate into Mozilla Firefox

You can import a client certificate and make it available on Mozilla Firefox for presenting it in SSL-secured communication.

**Before you begin**

To import the certificate file, you must have stored it within your local file system.

**Task**

1. Open the browser and on the top-level menu bar, click Tools, then click Options.

   The Options window opens.

2. Click Advanced, then click Encryption.

3. In the Certificates section of the Encryption tab, click View Certificates.

   The Certificate Manager window opens.

4. Click Import.

   Your local file manager opens.

5. Navigate to the certificate file that you have stored and click Open.

6. When prompted, submit a password, then click OK.
Administrator accounts

Administrator accounts can be set up and managed on the appliance or on an external server. Roles can be created with different access privileges for administrators.

Add an administrator account

You can add administrator accounts to the account that is created by the appliance system at the initial setup.

Task
1. Select Accounts | Administrator Accounts.
2. Under Internal Administrator Accounts, click Add.
   The Add Administrator window opens.
3. Add a user name, a password, and other settings for the account. Then click OK.
   The window closes and the new account appears in the accounts list.
4. Click Save Changes.

See also
Administrator account settings on page 303

Edit an administrator account

You can edit administrator accounts including the one that is created by the appliance system at the initial setup.

Task
1. Select Accounts | Administrator Accounts.
2. Under Internal Administrator Accounts, select an account and click Edit.
   Before selecting an account, you can type a filtering term in the Filter field to display only accounts with matching names.
   The Edit Administrator window opens
3. Edit the settings of the account as needed. Then click OK.
   The window closes and the account appears with your changes in the accounts list.
4. Click Save Changes.

See also
Administrator account settings on page 303
Delete an administrator account
You can delete any administrator account, as long as there is at least one that remains.

Task
1. Select Accounts | Administrator Accounts.
2. Under Internal Administrator Accounts, select an account and click Delete.
   Before selecting an account, you can type a filtering term in the Filter field to display only accounts with matching names.
   A window opens to let you confirm the deletion.
3. Click Save Changes.

Administrator account settings
The administrator account settings are used for configuring credentials and roles for administrators.

Administrator account settings
Settings for administrator accounts

Table 9-19 Administrator account settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specifies the user name of an administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets an administrator password.</td>
</tr>
<tr>
<td>Password repeated</td>
<td>Lets you repeat the password and confirm it.</td>
</tr>
<tr>
<td>Role</td>
<td>Provides a list for selecting an administrator role.</td>
</tr>
<tr>
<td></td>
<td>You can use the Add and Edit options to add and edit roles.</td>
</tr>
<tr>
<td></td>
<td>The added and edited roles appear in the list of administrator roles.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the real name of the person that an account is set up for.</td>
</tr>
<tr>
<td></td>
<td>Configuration of this name is optional.</td>
</tr>
</tbody>
</table>

Test with current settings
Settings for testing whether an administrator with given credentials would be admitted on the appliance

Table 9-20 Test with current settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Specifies a user name that is tested.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the tested password.</td>
</tr>
<tr>
<td>Test</td>
<td>Executes the test.</td>
</tr>
<tr>
<td></td>
<td>The Authentication Test Results window opens to display the outcome of the test.</td>
</tr>
</tbody>
</table>
Manage administrator roles

You can create roles and use them for configuring administrator accounts.

One administrator role is already created by the appliance system at the initial setup.

**Task**

1. Select **Accounts | Administrator Accounts**.

2. To add an administrator role:
   a. Under **Roles**, click **Add**.
      
      The **Add Role** window opens.
   b. In the **Name** field, type a role name.
   c. Configure access rights for the dashboard, rules, lists, and other items.
   d. Click **OK**.
      
      The window closes and the new role appears in the list of administrator roles.

3. Use the **Edit** and **Delete** options in similar ways to edit and delete roles.

4. Click **Save Changes**.

The newly added or edited role is now available for being assigned to an administrator account.

**See also**

*Administrator role settings on page 304*

Administrator role settings

The administrator role settings are used for configuring roles that can be assigned to administrators.

**Administrator role settings**

Settings for administrator roles

**Table 9-21  Administrator role settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specifies the user name of an administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets an administrator password.</td>
</tr>
<tr>
<td>Password repeated</td>
<td>Lets you repeat the password and confirm it.</td>
</tr>
<tr>
<td></td>
<td>In the <strong>Edit Administrator</strong> window, you need to select <strong>Set a new password</strong> before the two password fields become available.</td>
</tr>
<tr>
<td>Role</td>
<td>Provides a list for selecting an administrator role,</td>
</tr>
<tr>
<td></td>
<td>You can use the <strong>Add</strong> and <strong>Edit</strong> options to add and edit roles.</td>
</tr>
<tr>
<td></td>
<td>The added and edited roles appear in the list of administrator roles.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the real name of the person that an account is set up for.</td>
</tr>
<tr>
<td></td>
<td>Configuring this name is optional.</td>
</tr>
</tbody>
</table>
Configure external account management

You can let administrator accounts be managed on external authentication servers and map externally stored user groups and individual users to roles on an appliance.

**Task**

1. Select **Accounts | Administrator Accounts**.

2. Click **Administrator accounts are managed in an external directory server**.
   
   Additional settings appear.

   
   These settings determine the way the Authentication module on the appliance retrieves information from that server.

4. Use the settings under **Authentication group = role mapping**, to map user groups and individual users stored on the external server to roles on the appliance:
   
   a. Click **Add**.
      
      The **Add Group/User Role Name Mapping** window opens.
   
   b. Select the checkboxes next to the field for group or user matching as needed and type the name of a group or user in this field.
   
   c. Click **OK**.
   
   d. Under **Role to map to**, select a role.
   
   e. Click **OK**.
      
      The window closes and the new mapping appears on the mappings list.
   
   f. Click **Save Changes**.

You can use the **Edit** and **Delete** options in similar ways to edit and delete mappings.
Quota management is a means of guiding the users of your network in their web usage. This way you can ensure that resources and performance of your network are not impacted in excess.

Quotas and other restrictions can be imposed in several ways:

- **Time quotas** — Limit the time that users are allowed to spend on their web usage
- **Volume quotas** — Limit the volume that users are allowed to consume during their web usage
- **Coaching** — Limits the time that users can spend on their web usage, but allows them to exceed the configured time limit if they choose to do so
- **Authorized override** — Limits the time that users can spend on web usage in the same way as coaching
  
  However, the time limit can only be exceeded by an action of an authorized user, for example, a teacher in a classroom.

- **Blocking sessions** — Blocks access to the web for a configured period of time after a user attempted to access a web object, for which access was not allowed

Quotas and other restrictions can be imposed separately or in a combination of measures.

**Contents**

- Imposing quotas and other restrictions on web usage
- Time quota
- Volume quota
- Coaching
- Authorized override
- Blocking sessions
- Quota system settings

**Imposing quotas and other restrictions on web usage**

Imposing quotas and other restrictions in a quota management process for the users of your network allows you to guide their web usage and limit their consumption of network resources.

The quota management process includes several elements, which contribute to it in different ways.

- Quota management rules control the process.
- Quota management lists are used by the rules to impose restrictions with regard to users and particular web objects, such as URLs, IP addresses, and others.
- Quota management modules, which are called by the rules, handle time and volume quotas, session times, and other restrictions within the process.
A quota management process is not implemented by default on Web Gateway after the initial setup. You can implement a process by importing suitable rule sets from the rule set library and modify this process to adapt it to the requirements of your web security policy.

To configure quota management, you can work with:

- **Key elements of rules** — After importing the library rule sets for quota management and clicking them on the rule sets tree, you can view and configure key elements of the rules for the quota management process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the rules for the quota management process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

  You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

### Quota management rules

The rules that control the management of quotas and other restrictions are contained in different rule sets, according to the type of restriction, for example, in a time quota or a coaching rule set.

The rules in these rule sets check whether the configured limits for time or volume have been exceeded and eventually block requests for further web access. They also redirect requests when a user chooses to continue with a new session.

Quota management rule sets are not implemented in the default rule set system, but can be imported from the rule set library. The library rule set names are *Time Quota*, *Volume Quota*, *Coaching*, *Authorized Override*, and *Blocking Sessions*.

You can review the rules that are implemented with the library rule sets, modify or delete them, and also create your own rules.

### Quota management lists

The rule sets for managing quotas and other restrictions use lists of web objects and users to impose restrictions accordingly. The lists are contained in the criteria of a rule set.

For example, a list contains a number of URLs and the time quota rule set has this list in its criteria. Then this rule set and the rules within it apply only if a user accesses one of the URLs on the list. Lists of IP addresses or media types can be used in the same way.

You can add entries to these lists or remove entries. You can also create your own lists and let them be used by the quota management rule sets.

### Quota management modules

The quota management modules (also known as engines) handle the time and volume parameters of the quota management process and are checked by the rule sets of the process to find out about consumed and remaining times or volumes, session times, and other values.

There is a module for each type of restriction, for example, the *Time Quota* or the *Coaching* module.

By configuring settings for these modules, you specify the times and volumes that apply in the quota management process. For example, when configuring the time quota module, you specify how much hours and minutes per day users can access web objects with particular URLs or IP addresses.
Session time

Among the settings that you can configure for the quota management module is also session time. This is the time allowed for a single session that a user spends on web usage.

Session time is configured separately and handled differently for time quotas, volume quotas, and other parameters of the quota management process.

- **Session time for time quotas** — When configuring time quotas, you also need to configure a session time. Whenever session time has elapsed for a user, the amount of time that is configured as session time is deducted from the user’s time quota.

  As long as the time quota has not been used up, the user can start a new session. When the time quota has elapsed, a request that the user sends is blocked and a block message is displayed.

- **Session time for volume quotas** — When configuring volume quotas, the session time has no impact on the volume quota for a user.

  You can still configure a session time to inform the user about the amount of time that has been used up for web access. When time has elapsed for a session, the user can start a new session, as long as the configured volume has not been consumed.

  If you set the session time to zero, no session time is configured and communicated to the user.

- **Session time for other quota management functions** — Session time can also be configured for other Coaching, Authorized Override, and Blocking Sessions. Accordingly, there can be a coaching, an authorized override, or a blocking session.

  When session time has elapsed for coaching and authorized overriding, a request that a user sends is blocked.

  A message is displayed to the user, stating why the request was blocked. The user can start a new session unless time quota has also been configured and is used up.

  The session time that is configured for a blocking session is the time during which requests sent by a particular user are blocked. When this time has elapsed, requests from the user are again accepted unless time quota has also been configured and is used up.

Combining quota management functions

Using a particular quota management function to restrict web usage has no impact on the use of other quota management functions. For example, time quotas and volume quotas are configured and implemented separately on the appliance.

You can, however, combine these functions in meaningful ways.

For example, you can impose coaching on users’ access to some URL categories, while requesting authorized override credentials for others.

For still another group of categories you could block users who attempt to access them over a configured period of time.
Time quota

By configuring time quotas, you can limit the time that users of your network are allowed to spend for web usage.

Time quotas can be related to different parameters:

- **URL categories** — When time quotas are related to URL categories, users are allowed only a limited time for accessing URLs that fall into particular categories, for example, Online Shopping.

- **IP addresses** — When time quotas are related to IP addresses, users who send requests from particular IP addresses are allowed only a limited time for web usage.

- **User names** — When time quotas are related to user names, users are allowed only a limited time for web usage. Users are identified by the user names they submitted for authentication on the appliance.

These parameters are used by the rules in the library rule set for time quotas. You can create rules of your own that use other parameters in relation to time quotas.

The time that users spend on web usage is stored on the appliance. When the configured time quota has been exceeded for a user, a request that this user sends is blocked. A message is displayed to the user stating why the request was blocked.

Users are identified by the user names they submitted for authentication. If no user name is sent with a request, web usage is recorded and blocked or allowed for the IP address of the client system that the request was sent from.

Web usage can be limited to time spent per day, per week, or per month.

Configure time quotas

You can configure time quotas to limit the time users of your network spend on web usage.

**Task**

1. Select **Policy | Rule Sets**.

2. On the rule sets tree, expand the rule set that contains rules for time quotas, for example, the **Time Quota** library rule set.

   The nested rule sets appear.

3. Select the appropriate nested rule set.

   For example, to configure time quotas with regard to URL categories, select **Time Quota With URL Configuration**.

   The general settings and rules of the rule set appear on the settings pane.

4. In the rule set criteria, click the **URL Category Block List for Time Quota** list name.

   A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.

   The **Edit List (Category)** window opens.

5. Add URL categories to the blocking list. Then click **OK** to close the window.

6. In the criteria for one of the rules, click the **URL Category Configuration** settings name.

   The **Edit Settings** window opens.
7  Configure session time and the time quota per day, week, and month. Then click OK to close the window.

8  Click Save Changes.

**Time Quota settings**
The Time Quota settings are used for configuring the module that handles time quota management.

**Time Quota per Day, Week, Month, and Session Time**
Settings for time quotas

When a time unit or the session time is selected, the heading of the next section reads accordingly.

**Table 10-1  Time Quota per Day, Week, Month, and Session Time**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time quota per day (week, month)</td>
<td>When selected, the quota that is configured in the next section applies to the selected time unit.</td>
</tr>
<tr>
<td>Session time</td>
<td>When selected, the quota that is configured in the next section applies to the session time.</td>
</tr>
</tbody>
</table>

**Hours and Minutes for . . .**
Settings for time quotas that apply to the selected time unit or the session time

The heading of this section varies according to what you selected in the preceding section.

For example, if you selected Time quota per week, the heading reads **Hours and Minutes for Time Quota per Week**.

**Table 10-2  Hours and Minutes for . . .**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours</td>
<td>Sets the allowed hours per day, week, month, or for the session time.</td>
</tr>
<tr>
<td>Minutes</td>
<td>Sets the allowed minutes per day, week, month, or for the session time.</td>
</tr>
</tbody>
</table>

**Actual Configured Time Quota**
Displays the configured time quotas.

**Table 10-3  Actual Configured Time Quota**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time quota per day (week, month)</td>
<td>Shows the allowed time per day, week, or month.</td>
</tr>
<tr>
<td>Session time</td>
<td>Shows the allowed session time.</td>
</tr>
</tbody>
</table>

**Time Quota rule set**
The Time Quota rule set is a library rule set for imposing time quotas on web usage.

**Library rule set – Time Quota**

Criteria – SSL.Client.Context.IsApplied equals true OR Command.Name does not equal "CONNECT"
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication, which does not use the CONNECT command at the beginning.
The following rule sets are nested in this rule set:

- **Time Quota With URL Configuration**
- **Time Quota With IP Configuration**
  This rule set is not enabled initially.
- **Time Quota With Authenticated User Configuration**
  This rule set is not enabled initially.

**Time Quota With URL Configuration**

This nested rule set handles time quotas related to URL categories.

<table>
<thead>
<tr>
<th>Nested library rule set – Time Quota With URL Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – URL.Categories&lt;Default&gt; at least one in list URL Categories Blocklist for Time Quota</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for time quotas related to URL categories.

The rule set contains the following rules:

**Redirecting after starting new time session**

*Quota.Time.IsActivationRequest equals true* → Redirect<Redirection After Time Session Activation>

The rule redirects a request to let a user again access a web object after session time has been exceeded and the user has chosen to continue with a new session.

The action settings specify a message to the requesting user.

**Check if time session has been exceeded**

*Quota.Time.Session.Exceeded<URL Category Configuration> equals true* → Block<ActionTimeSessionBlocked>

The rule uses the *Quota.Time.SessionExceeded* property to check whether the configured session time has been exceeded for a user. If it has, the user’s request for web access is blocked.

The *URL Category Configuration* settings, which are specified with the property, are the settings of the module that handles time quotas.

The action settings specify a message to the requesting user.

**Check if time quota has been exceeded**

*Quota.Time.Exceeded<URL Category Configuration> equals true* → Block<ActionTimeQuotaBlocked>

The rule uses the *Quota.Time.Exceeded* property to check whether the configured time quota has been exceeded for a user. If it has, the user’s request for web access is blocked.

The *URL Category Configuration* settings, which are specified with the property, are the settings of the module that handles time quotas.

The action settings specify a message to the requesting user.

**Time Quota With IP Configuration**

This nested rule set handles time quotas related to IP addresses.
Nested library rule set – Time Quota With IP Configuration

Criteria – Client.IP is in list IP Blocklist for Time Quota
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a user sends a request from a client with an IP address that is on the blocking list for time quotas related to IP addresses.

The rules in this rule set are the same as in the Time Quota with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are IP Configuration.

Time Quota With Authenticated User Configuration

This nested rule set handles time quotas related to user names.

Nested library rule set – Time Quota With Authenticated User Configuration

Criteria – Authenticated.RawUserName is in list User Blocklist for Time Quota
Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies when a request is sent by a user whose username is on the blocking list for time quotas related to user names.

The rules in this rule set are the same as in the Time Quota with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are Authenticated User Configuration.

Volume quota

By configuring volume quotas, you can limit the volume of web objects, measured in GB and MB, that the users of your network are allowed to download from the web.

Volume quotas can be related to several parameters:

- **URL categories** — Users are allowed to download only a limited volume of web objects through URLs that fall into particular categories, for example, Streaming Media.
- **IP addresses** — Users who send download requests from particular IP addresses are allowed only a limited volume.
- **User names** — Users are allowed to download web objects only up to a limited volume. Users are identified by the user names they submitted for authentication on the appliance.
- **Media types** — Users are allowed to download web objects belonging to particular media types only up to a limited volume.

These parameters are used by the rules in the library rule set for volume quotas. You can create rules of your own that use other parameters in relation to volume quotas.

Information on the volume that users download from the web is stored on the appliance. When the configured volume quota has been exceeded for a user, a request that this user sends is blocked. A message is displayed to the user stating why the request was blocked.

Users are identified by the user names they submitted for authentication. If no user name is sent with a request, web usage is recorded and blocked or allowed for the IP address of the client system that the request was sent from.

Web downloads can be limited to volume downloaded per day, per week, or per month.
Configure volume quotas
You can configure volume quotas to limit the volume that user of your network consume during their web usage.

Task
2. On the rule sets tree, expand the rule set that contains rules for the volume quota, for example, the Volume Quota library rule set.
   The nested rule sets appear.
3. Select the appropriate nested rule set, for example, Volume Quota With IP Configuration.
   The general settings and rules of the rule set appear on the settings pane.
4. In the rule set criteria, click the appropriate blocking list name, for example, IP Block List for Volume Quota.
   A yellow triangle next to the list name means the list is initially empty and you need to fill the entries.
   The Edit List (Category) window opens.
5. Add the appropriate entries to the blocking list, for example, IP addresses. Then click OK to close the window.
6. In the criteria for one of the rules, click the appropriate settings name, for example, IP Configuration.
   The Edit Settings window opens.
7. Configure the appropriate parameters, for example, session time and the volume quota per day, week, and month. Then click OK to close the window.
8. Click Save Changes.

Volume Quota settings
The Volume Quota settings are used for configuring the module that handles volume quota management.

Volume Quota per Day, Week, and Month
Settings for volume quotas
When a time unit or the session time is selected, the heading of the next section reads accordingly.

Table 10-4 Volume Quota per Day, Week, and Month

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume quota per day (week, month)</td>
<td>When selected, the quota that is configured in the next section applies to the selected time unit</td>
</tr>
<tr>
<td>Session time</td>
<td>When selected, the quota that is configured in the next section applies to the session time</td>
</tr>
</tbody>
</table>

Volume for . . .
Settings for volume quotas that apply to the selected time unit or the session time
The heading of this section varies according to what you selected in the preceding section.
For example, if you selected *Volume quota per week*, the heading reads *Volume for Volume Quota per Week*.

However, if you selected *Session Time*, the heading reads *Hours and Minutes*.

**Table 10-5  Volume for . . .**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>GiB</td>
<td>Specifies the number of GiB that are allowed as volume.</td>
</tr>
<tr>
<td>MiB</td>
<td>Specifies the number of MiB that are allowed as volume.</td>
</tr>
</tbody>
</table>

**Actual Configured Volume Quota**

Displays the configured volume quotas.

**Table 10-6  Actual Configured Volume Quota**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume quota per day (week, month)</td>
<td>Shows the allowed volume per day, week, or month.</td>
</tr>
<tr>
<td>Session time</td>
<td>Shows the allowed session time.</td>
</tr>
</tbody>
</table>

**Volume Quota rule set**

The Volume Quota rule set is a library rule set for imposing volume quotas on web usage.

**Library rule set – Volume Quota**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Cycle</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL.Client.Context.IsApplied equals true OR Command.Name does not equal &quot;CONNECT&quot;</td>
<td>Requests (and IM)</td>
<td>The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication that does not use the CONNECT command at the beginning. The following rule sets are nested in this rule set: • Time Quota With URL Configuration • Time Quota With IP Configuration This nested rule set is not enabled initially. • Time Quota With Authenticated User Configuration This nested rule set is not enabled initially.</td>
</tr>
<tr>
<td>SSL.Client.Context.IsApplied equals true OR Command.Name does not equal &quot;CONNECT&quot;</td>
<td>Requests (and IM)</td>
<td>The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication, which does not use the CONNECT command at the beginning. The following rule sets are nested in this rule set: • Volume Quota With URL Configuration • Volume Quota With IP Configuration This rule set is not enabled initially.</td>
</tr>
</tbody>
</table>
Volume Quota With Authenticated User Configuration
This rule set is not enabled initially.

Volume Quota With Media Type Configuration
This rule set is not enabled initially.

Volume Quota With URL Configuration
This nested rule set handles volume quotas related to URL categories.

<table>
<thead>
<tr>
<th>Nested library rule set – Volume Quota With URL Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – URL.Categories&lt;Default&gt; at least one in list URL Categories Blocklist for Volume Quota</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for volume quotas related to URL categories.

The rule set contains the following rules:

**Redirecting after starting new time session**
Quota.Volume.IsActivationRequest<URL Category Configuration> equals true -> Redirect<Redirection After Volume Session Activation>

The rule redirects a request to let a user again access a web object after session time has been exceeded and the user has chosen to continue with a new session.

The **URL Category Configuration** settings, which are specified with the property, are the settings of the module that handles volume quotas.

The action settings specify a message to the requesting user.

**Check if volume session has been exceeded**
Quota.Volume.Session.Exceeded<URL Category Configuration> equals true -> Block<ActionVolumeSessionBlocked>

The rule uses the Quota.Volume.SessionExceeded property to check whether the configured session time has been exceeded for a user. If it has, the user’s request for web access is blocked.

The **URL Category Configuration** settings, which are specified with the property, are the settings of the module that handles volume quotas.

The action settings specify a message to the requesting user.

**Check if volume quota has been exceeded**
Quota.Time.Exceeded<URL Category Configuration> equals true -> Block<ActionVolumeSessionBlocked>

The rule uses the Quota.Volume.Exceeded property to check whether the configured volume quota has been exceeded for a user. If it has, the user’s request for web access is blocked.

The **URL Category Configuration** settings, which are specified with the property, are the settings of the module that handles volume quotas.

The action settings specify a message to the requesting user.

Volume Quota With IP Configuration
This nested rule set handles volume quotas related to IP addresses.

<table>
<thead>
<tr>
<th>Nested library rule set – Volume Quota With IP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Client.IP is in list IP Blocklist for Volume Quota</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for volume quotas related to URL categories.
The rule set criteria specifies that the rule set applies when a user sends a request from a client with an IP address that is on the blocking list for volume quotas related to IP addresses.

The rules in this rule set are the same as in the Volume Quota with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are IP Configuration.

**Volume Quota With Authenticated User Configuration**

This nested rule set handles volume quotas related to user names.

| Nested library rule set – Volume Quota With Authenticated User Configuration |
| Criteria – Authenticated.RawUserName is in list User Blocklist for Volume Quota |
| Cycle – Requests (and IM) |

The rule set criteria specifies that the rule set applies when a request is sent by a user whose user name is on the blocking list for volume quotas related to user names.

The rules in this rule set are the same as in the Volume Quota with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are Authenticated User Configuration.

**Volume Quota With Media Type Configuration**

This nested rule set handles volume quotas related to media types.

| Nested library rule set – Volume Quota With Media Type Configuration |
| Criteria – MediaType.FromFileExtension at least one in list Media Type Blocklist for Volume Quota |
| Cycle – Requests (and IM) |

The rule set criteria specifies that the rule set applies when a request is sent to access a web object belonging to a media type that is on the blocking list for volume quotas related to media types.

The rules in this rule set are the same as in the Volume Quota with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are Media Type Configuration.

---

**Coaching**

By configuring coaching quotas, you can limit the time that users of your network are allowed to spend for web usage, but allow them to continue if they choose to do so.

To coach the web usage of your users, you configure a coaching session with a particular length of time. When this session time has elapsed for a user, a block message is displayed. The user can then choose to start a new session.

You can configure coaching in relation to the parameters used in the Coaching library rule set, such as URL categories, IP addresses, and user names. You can also create rules of your own using other parameters.
Configure coaching
You can configure coaching to restrict web usage for the users of your network, but allow them to continue when they choose to do so after the configured time limit has been exceeded.

Task
2. On the rule sets tree, expand the rule set that contains rules for coaching, for example, the Coaching library rule set.
   The nested rule sets appear.
3. Select the appropriate nested rule set, for example, Coaching With IP Configuration.
   The general settings and rules of the rule set appear on the settings pane.
4. In the rule set criteria, click the appropriate blocking list name, for example, IP Block List for Coaching.
   A yellow triangle next to the list name means the list is initially empty and you need to fill the entries.
   The Edit List (Category) window opens.
5. Add the appropriate entries to the blocking list, for example, IP addresses. Then click OK to close the window.
6. In the criteria for one of the rules, click the appropriate settings name, for example, IP Configuration.
   The Edit Settings window opens.
7. Configure the appropriate parameters, for example, the session time. Then click OK to close the window.
8. Click Save Changes.

Coaching settings
The Coaching settings are used for configuring the module that handles coaching.

Hours and Minutes of Session Time
Settings for configuring the length of a coaching session

Table 10-7  Hours and Minutes of Session Time

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days</td>
<td>Sets the days of a coaching session.</td>
</tr>
<tr>
<td>Hours</td>
<td>Sets the hours of a coaching session.</td>
</tr>
<tr>
<td>Minutes</td>
<td>Sets the minutes of a coaching session.</td>
</tr>
</tbody>
</table>

Coaching rule set
The Coaching rule set is a library rule set for imposing restrictions on web usage that can users can pass by if they choose to do so.

Library rule set – Coaching
Criteria – SSL.Client.Context.IsApplied equals true OR Command.Name does not equal "CONNECT"
Cycle – Requests (and IM)
The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication, which does not use the CONNECT command at the beginning.

The following rule sets are nested in this rule set:

- Coaching With URL Configuration
- Coaching With IP Configuration
  This rule set is not enabled initially.
- Coaching With Authenticated User Configuration
  This rule set is not enabled initially.

**Coaching With URL Configuration**

This nested rule set handles coaching related to URL categories.

<table>
<thead>
<tr>
<th>Nested library rule set – Coaching With URL Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <strong>URL.Categories&lt;Default&gt;</strong> at least one in list <strong>URL Categories Blocklist for Coaching</strong></td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for coaching related to URL categories.

The rule set contains the following rules:

**Redirecting after starting new coaching session**

*Quota.Coaching.IsActivationRequest equals true* → *Redirect<Redirection After Coaching Session Activation>*

The rule redirects a request to let a user again access a web object after session time has been exceeded and the user has chosen to continue with a new session.

The action settings specify a message to the requesting user.

**Check if coaching session has been exceeded**

*Quota.Coaching.Session.Exceeded<URL Category Configuration> equals true* → *Block<ActionCoachingSessionBlocked>*

The rule uses the *Quota.Coaching.SessionExceeded* property to check whether the configured session time has been exceeded for a user. If it has, the user's request for web access is blocked.

The **URL Category Configuration** settings, which are specified with the property, are the settings of the module that handles coaching.

The action settings specify a message to the requesting user.

**Coaching Quota With IP Configuration**

This nested rule set handles coaching related to IP addresses.

<table>
<thead>
<tr>
<th>Nested library rule set – Coaching With IP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <strong>Client.IP is in list IP Blocklist for Coaching</strong></td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user sends a request from a client with an IP address that is on the blocking list for coaching related to IP addresses.

The rules in this rule set are the same as in the Coaching with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are **IP Configuration**.
Coaching With Authenticated User Configuration

This nested rule set handles coaching related to user names.

<table>
<thead>
<tr>
<th>Nested library rule set – Coaching With Authenticated User Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authenticated.RawUserName is in list User Blocklist for Coaching</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a request is sent by a user whose user name is on the blocking list for coaching related to user names.

The rules in this rule set are the same as in the Coaching with URL Configuration rule set, except for the module settings that appear in the rule criteria, which are Authenticated User Configuration.

Authorized override

You can configure session time for a session that allows authorized overriding.

When this session time has elapsed, a user request is blocked and a block message is displayed. The message also asks for submission of a user name and password to start a new session.

These credentials must be those of an authorized user. For example, in a classroom situation, a user who gets blocked after termination of an authorized override session could be a student, while the teacher is the authorized user.

Authentication of this user is performed according to the configured authentication method. However, when configuring this method, you cannot let it include an integrated authentication mode.

The block message also provides an option to specify the time length of the authorized override session for the user who was blocked.

The time length that is configured for this user should not exceed the time length configured for all other users as part of the module settings for authorized overriding.

You can configure authorized overriding in relation to the parameters used in the library rule set, such as URL categories, IP addresses, and user names. You can also create rules of your own using other parameters.

Configure authorized overriding

You can configure authorized overriding to restrict the web usage of your users, but allow the configured time limit to be passed by through the action of an authorized user.

Task


2. On the rule sets tree, expand the rule set that contains rules for authorized overriding, for example, Authorized Override library rule set.

   The nested rule sets appear.

3. Select the appropriate nested rule set, for example, Authorized Override With IP Configuration.

   The general settings and rules of the rule set appear on the settings pane.
4 In the rule set criteria, click the appropriate blocking list name, for example, IP Block List for Authorized Override.

A yellow triangle next to the list name means the list is initially empty and you need to fill the entries.

The Edit List (Category) window opens.

5 Add the appropriate entries to the blocking list, for example, IP addresses. Then click OK to close the window.

6 In the criteria for one of the rules, click the appropriate settings name, for example, IP Configuration.

The Edit Settings window opens.

7 Configure the appropriate parameters, for example, the session time. Then click OK to close the window.

8 Click Save Changes.

**Authorized Override settings**

The Authorized Override settings are used for configuring the module that handles authorized overriding.

**Hours and Minutes of Maximum Session Time**

Settings for configuring the maximum time length of a session with authorized overriding.

**Table 10-8 Hours and Minutes of Maximum Session Time**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days</td>
<td>Sets the days of an Authorized Override session.</td>
</tr>
<tr>
<td>Hours</td>
<td>Sets the hours of an Authorized Override session.</td>
</tr>
<tr>
<td>Minutes</td>
<td>Sets the minutes of an Authorized Override session.</td>
</tr>
</tbody>
</table>

**Authorized Override rule set**

The Authorized Override rule set is a library rule set for imposing a time limit on web usage that can be passed by through the action of authorized user.

**Library rule set – Authorized Override**

Criteria – SSL.Client.Context.IsApplied equals true OR Command.Name does not equal "CONNECT"

Cycle – Requests (and IM)

The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication, which does not use the CONNECT command at the beginning.

The following rule sets are nested in this rule set:

- Authorized Override With URL Configuration
- Authorized Override With IP Configuration
  This rule set is not enabled initially.
- Authorized Override With Authenticated User Configuration
  This rule set is not enabled initially.
Authorized Override With URL Configuration
This nested rule set handles authorized overriding related to URL categories.

<table>
<thead>
<tr>
<th>Nested library rule set – Authorized Override With URL Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – URL.Categories&lt;Default&gt; at least one in list URL Categories Blocklist for Authorized Override</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for authorized overriding related to URL categories.

The rule set contains the following rules:

Redirect after authenticating for authorized override
Quota.AuthorizedOverride.IsActivationRequest<URL Category Configuration> equals true AND Authentication.Authenticate<User Database> equals true –> Redirect<Redirection After Authorized Session Activation>
The rule redirects a request to let a user again access a web object after session time has been exceeded and the credentials the user submitted to continue with a new session have been validated.

The action settings specify a message to the requesting user.

Check if authorized override session has been exceeded
Quota.AuthorizedOverride.SessionExceeded<URL Category Configuration> equals true –> Block<Action Authorized Override Blocked>
The rule uses the Quota.AuthorizedOverride.SessionExceeded property to check whether the configured session time has been exceeded for a user. If it has, the user’s request for web access is blocked.

The URL Category Configuration settings, which are specified with the property, are the settings of the module that handles authorized overriding.

The action settings specify a message to the requesting user.

Authorized Override With IP Configuration
This nested rule set handles authorized overriding related to IP addresses.

<table>
<thead>
<tr>
<th>Nested library rule set – Authorized Override With IP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Client.IP is in list IP Blocklist for Authorized Override</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a user sends a request from a client with an IP address that is on the blocking list for authorized overriding related to IP addresses.

The rules in this rule set are the same as in the Authorized Override with URL Configuration rule set, except for the module settings in the rule criteria, which are IP Configuration.

Authorized Override With Authenticated User Configuration
This nested rule set handles authorized overriding related to user names.

<table>
<thead>
<tr>
<th>Nested library rule set – Authorized Override With Authenticated User Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authenticated.RawUserName is in list User Blocklist for Authorized Override</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a request is sent by a user whose user name is on the blocking list for authorized overriding related to user names.
The rules in this rule set are the same as in the Authorized Override with URL Configuration rule set, except for the module settings in the rule criteria, which are Authenticated User Configuration.

### Blocking sessions

By configuring blocking sessions you can block requests sent by a user for a configured period of time. A blocking session is imposed after a user has sent a request that is blocked according to a configured rule, for example, a request for a URL that falls into a category that is not allowed.

This is a means of enforcing a web security policy that handles unwanted access to web objects with more strictness.

You can configure blocking sessions in relation to the parameters that are used in the library rule set. You can also create rules of your own using other parameters.

### Configure blocking sessions

You can configure blocking sessions to block session for a user over a configured period of time after an attempt to access a web object that is not allowed.

#### Task


2. On the rule sets tree, expand the rule set that contains rules for the blocking session, for example, the Blocking Sessions library rule set.

   The nested rule sets appear.

3. Select the appropriate nested rule set, for example, Blocking Sessions With IP Configuration.

   The general settings and rules of the rule set appear on the settings pane.

4. In the rule set criteria, click the appropriate blocking list name, for example, IP Block List for Blocking Sessions.

   A yellow triangle next to the list name means the list is initially empty and you need to fill the entries.

   The Edit List (Category) window opens.

5. Add the appropriate entries to the blocking list, for example, IP addresses. Then click OK to close the window.

6. In the criteria for one of the rules, click the appropriate settings name, for example, IP Configuration.

   The Edit Settings window opens.

7. Configure the appropriate parameters, for example, the period of time over which sessions are blocked. Then click OK to close the window.

8. Click Save Changes.
**Block Session settings**

The Block Session settings are used for configuring the module that handles blocking sessions.

**Hours and Minutes for Session Time**

Settings for configuring the time length of a blocking session

<table>
<thead>
<tr>
<th>Table 10-9 Hours and Minutes for Session Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
</tr>
<tr>
<td>Days</td>
</tr>
<tr>
<td>Hours</td>
</tr>
<tr>
<td>Minutes</td>
</tr>
</tbody>
</table>

**Blocking Sessions rule set**

The Blocking Sessions rule set is a library rule set for blocking web sessions after an attempt to access a web object that is not allowed.

**Library rule set – Blocking Sessions**

| Cycle – Requests (and IM)                                        |

The rule set criteria specifies that the rule set applies to SSL-secured communication and to any other communication, which does not use the CONNECT command at the beginning.

The following rule set is nested in this rule set: *Blocking Sessions With URL Configuration*

**Blocking Sessions With URL Configuration**

This nested rule set handles blocking sessions related to URL categories.

| Nested library rule set – Blocking Sessions With URL Configuration |
| Criteria – URL.Categories<Default> at least one in list URL Categories Blocklist for Blocking Sessions |
| Cycle – Requests (and IM)                                      |

The rule set criteria specifies that the rule set applies when a user sends a request for a URL that falls into a category on the blocking list for blocking sessions related to URL categories.

The rule set contains the following rules:

**Block user if blocking session is active**

`BlockingSession.IsBlocked<Blocking Session Configuration> equals true` → Block<Blocking Session Template>

The rule uses the `BlockingSession.IsBlocked` property to check whether a blocking session has been activated for a user who sends a request. If it has, the request is blocked.

The action settings specify a message to the requesting user.

**Activate blocking session if category is in list Category List for Blocking Sessions**

`URL.Categories<Default> at least one in list Category List for Blocking Session` → Continue —

`BlockingSession.Activate<Blocking Session Configuration>`
The rule uses the \textit{URL.Categories} property to check whether a URL that a user requests access to falls into a category on the blocking list maintained especially for blocking sessions. If it falls into a category on the list, a blocking session is activated for the user.

The \textit{BlockingSession.Activate} event is used to activate the blocking session. The event settings are specified with the event.

\section*{Quota system settings}

Quota system settings are general settings for time intervals related to quota management.

If an appliance is a node in a Central Management configuration, you can configure time intervals for data synchronization with other nodes.

These settings are configured on the \textit{Appliances} tab of the \textit{Configuration} top-level menu.

They can also appear under the name of \textit{Coaching} (instead of Quota), but apply in both cases to all options that are provided for quota management: Authorized override, blocking sessions, coaching, time quota, and volume quota.

\subsection*{Quota Intervals for Synchronisation and Saving in Minutes}

Settings for time intervals related to quota management

\begin{table}[H]
\centering
\begin{tabular}{|l|l|}
\hline
\textbf{Option} & \textbf{Definition} \\
\hline
\textbf{Save interval} & Limits the time (in minutes) that elapses before current quota values are saved on an appliance to the specified value.  \\
& Quota value to be saved are, for example, the byte volumes that have been consumed by users. \\
\hline
\textbf{Interval for sending updated quota data} & Limits the time (in minutes) that elapses before current quota values are distributed from an appliance to all nodes in a Central Management configuration to the specified value.  \\
& The distributed data includes the changes in quota values that have occurred since the last time that data were distributed from the appliance. \\
\hline
\end{tabular}
\end{table}
# Table 10-10 Quota Intervals for Synchronisation and Saving in Minutes (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Interval for base**         | **synchronisation** limits the time (in minutes) that elapses before quota values are synchronized on all nodes in a Central Management configuration to the specified value.  
                                  | The synchronization takes a snapshot of the current quota values on all appliances. The values that are most recent with regard to individual users are distributed to all appliances.  
                                  | The values are also distributed to nodes that were temporarily inactive and did not receive updates sent during that time. They are, furthermore, distributed to nodes that have been newly added to the configuration, so they did not receive any previous updates. |
| **Cleanup database after**    | limits the time (in days) that elapses before data is deleted in the quota database to the specified value.  
                                  | Before data is deleted, a check is performed to see whether the data is obsolete. Data is obsolete if the time interval that has been configured for a quota management function has elapsed.  
                                  | For example, if a particular amount of bytes has been configured as volume quota for a user to be consumed during a month, the amount that the user actually consumed during a month becomes obsolete when a new month begins. The cleanup then deletes this data if the time configured under the **Cleanup database after** option has also elapsed.  
                                  | Stored data becomes obsolete after a month for time quotas. For other quota management functions, other time intervals are relevant. For example, for coaching and authorized overriding, the cleanup cannot be performed before the allowed session time has elapsed. |
Web filtering

When the users of your network send requests for web access, Web Gateway filters these requests, as well as the responses that are sent back from the web. Embedded objects sent with requests and responses are also filtered.

Web filtering is performed in various ways. It is controlled by rules, which you can review and modify to adapt them to the requirements of your web security policy.

Default filtering on Web Gateway includes:

- **Virus and malware filtering** — Blocks access to web objects that are infected by viruses and other malware
- **URL filtering** — Blocks or allows access to web objects with particular URLs
- **Media type filtering** — Blocks or allows access to web objects that belong to particular media types

Global whitelisting allows access to web objects before any of the rules for the above filtering methods are applied. SSL scanning enables the filtering of requests that are sent on SSL-secured connections.

**Contents**

- Virus and malware filtering
- URL filtering
- Media type filtering
- Application filtering
- Streaming media filtering
- Global whitelisting
- SSL scanning
- Hardware Security Module
- Advanced Threat Defense
- Data loss prevention

**Virus and malware filtering**

Virus and malware filtering ensures that the users of your network cannot access web objects that are infected by viruses and other malware. The filtering process detects infections and blocks access accordingly.

The process includes several elements, which contribute to it in different ways.

- Filtering rules control the process.
- Whitelists are used by rules to let some web objects skip virus and malware filtering.
- The Anti-Malware module, which is called by a particular rule, scans web objects for infections by viruses and other malware.
A default process for virus and malware filtering is implemented on Web Gateway after the initial setup. You can modify this process to adapt it to the requirements of your web security policy.

To configure virus and malware filtering, you can work with:

- **Key elements of rules** — After clicking the default Gateway Anti-Malware rule set on the rule sets tree, you can view and configure key elements of the default rules for the filtering process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the default rules for the filtering process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

  You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

### Filtering rules

The rules that control virus and malware filtering are usually contained in one rule set. The key rule in this rule set is the one that blocks access to web objects if they are infected by viruses and other malware.

To find out whether an object is infected, the rule calls the Anti-Malware module, which scans the object and lets the rule know about the result.

Whitelisting rules can be placed and processed in this rule set before the blocking rule. If any of them applies, the blocking rule is skipped and the whitelisted objects are not scanned.

When the default rule set system is implemented, a rule set for virus and malware filtering is included. Its name is *Gateway Anti-Malware*.

### Whitelists

Whitelists are used by whitelisting rules to let the blocking rule be skipped for particular web objects, which means no scanning is applied to these objects. There can be whitelists for URLs, media types, and other types of objects.

You can add entries to these lists or remove entries. You can also create your own lists and let them be used by the whitelisting rules.

Blocking lists are typically not used in virus and malware filtering because here the blocking depends not on entries in lists, but on the findings of the Anti-Malware module.

### Anti-Malware module

The Anti-Malware module is also known as the Anti-Malware *engine*. This module scans objects to detect infections by viruses and other malware. According to the findings of this module, the blocking rule blocks access to web objects or lets them pass through.

When the Anti-Malware module is called to run and scan web objects, it is by default a combination of two modules (engines) that are running. These modules can be seen as submodules of the Anti-Malware module. Each of these submodules uses different scanning methods.

The two default submodules are the *McAfee Gateway Anti-Malware engine*, and the *McAfee Anti-Malware engine*. The latter uses virus signatures to detect infections in web objects.

However, this method can only detect viruses and other malware that are already known and have been given signatures. To ensure a higher level of web security, the McAfee Gateway Anti-Malware engine uses also proactive methods to detect new viruses and malware.
When configuring settings for the Anti-Malware module, you can change the default mode to have a third-party submodule running in addition or alone.

To avoid temporary overloading of the submodules, you can configure an anti-malware queue that requests are moved to before being scanned.

**Configure key elements for virus and malware filtering**

Configure key elements of the rules for virus and malware filtering to adapt important parts of the filtering process to the requirements of your web security policy.

**Task**


2. On the rule sets tree, select the **Gateway Anti-Malware** rule set.

   Key elements of the rules for the filtering process appear in the configuration pane.

3. Configure the key elements as needed.

4. Click **Save Changes**.

**See also**

*Key elements for virus and malware filtering on page 329*

**Key elements for virus and malware filtering**

The key elements of the rules for virus and malware filtering deal with important parts of this filtering process.

**Bypass Scanning for These Agents and Hosts**

Key elements for bypassing scanning by the Anti-Malware module

**Table 11-1 Bypass scanning for these agents and hosts**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User agent whitelist</td>
<td>Clicking <strong>Edit</strong> opens a window to let you edit the User Agent Whitelist that is used by a rule. You can add, modify, and remove entries on the list.</td>
</tr>
<tr>
<td>URL host whitelist</td>
<td>Clicking <strong>Edit</strong> opens a window to let you edit the URL Host Whitelist that is used by a rule. You can add, modify, and remove entries on the list.</td>
</tr>
</tbody>
</table>

**Scanning Options**

Key elements for the scanning activities of the Anti-Malware module
Table 11-2  Scanning Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Remove partial content for HTTP requests    | When selected, a rule is enabled that removes the specification in an HTTP or HTTPS request for accessing only a part of the content of a web object and lets the request ask for the complete content.  
If a web object, for example, a file, is delivered completely by the web server in question, it can also be scanned completely on Web Gateway. A complete scan can detect infections that might not be noticed if only a part of the web object was scanned. |
| Block partial content for FTP requests       | When selected, a rule is enabled that blocks FTP requests for access to only a part of the content of a web object.                                                                                              |
| Use the Media Stream Scanner                | When selected, the Media Stream Scanner scans and delivers web objects that are streaming media chunk-by-chunk, to speed up the process. The proactive functions of the McAfee Gateway Anti-Malware engine are used for the scanning, but the other engines that are available for this purpose on Web Gateway are not involved. |

Gateway Anti-Malware Settings

Key elements for configuring settings for the Anti-Malware module

Table 11-3  Gateway Anti-Malware Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Anti-Malware scanning</td>
<td>When selected, a rule is enabled that calls the Anti-Malware Module, which scans web objects for infections by viruses and other malware.</td>
</tr>
<tr>
<td>Settings</td>
<td>Clicking Edit opens a window to let you edit the settings for the Anti-Malware module.</td>
</tr>
</tbody>
</table>

Configure virus and malware filtering using the complete rules view

You can configure virus and malware filtering to adapt this process to the requirements of your network.

Complete the following high-level steps.

Task

1 Review the rules in the rule set for virus and malware filtering.
   By default, this is the Gateway Anti-Malware rule set.

2 Modify these rules as needed.
   You can, for example, do the following:
   • Enable or disable whitelisting rules
   • Edit the lists used by the whitelisting rules

   A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.
• Create whitelists of your own and let them be used by the whitelisting rules
• Modify the combination of submodules that run when the Anti-Malware module is called to scan web objects
  By default, the combination includes the following submodules:
  • McAfee Gateway Anti-Malware
  • McAfee Anti-Malware
• Modify other settings of the Anti-Malware module

Configure the anti-malware queues as needed to avoid overloading of the modules that scan web objects.

4 Save your changes.

**Configure settings for the Anti-Malware module**
You can configure the Anti-Malware module to modify the way web objects are scanned for infections by viruses and other malware.

**Task**
1 Select *Policy | Rule Sets*.

2 On the rule sets tree, select the rule set for virus and malware filtering.
  By default, this is the *Gateway Anti-Malware* rule set.
  The rules of the rule set appear on the settings pane.

3 Make sure *Show details* is selected.

4 Find the rule that calls the Anti-Malware module.
  By default, this is the rule *Block if virus was found*.

5 In the rule criteria, click the settings name.
  This name appears next to the *Antimalware.Infected* property. By default, it is *Gateway Anti-Malware*.
  The *Edit Settings* window opens. It provides the settings for the Anti-Malware module.

6 Configure these settings as needed. Then click **OK** to close the window.

7 Click **Save Changes**.

**See also**
*Anti-Malware settings on page 333*

**Change the module combination for scanning web objects**
When configuring the settings of the Anti-Malware module, you can change the combination of submodules that run to scan web objects.
Different submodules can run under the name of *Anti-Malware* module (or engine) to perform the scanning. Which of them are available on your appliance depends on the licenses you have purchased.
**Task**


2. Access the Anti-Malware settings.
   a. On the rule sets tree, select the rule set for virus and malware filtering.
      By default, this is the *Gateway Anti-Malware* rule set.
      The rules of the rule set appear on the settings pane.
   b. Make sure *Show details* is selected.
   c. Find the rule that calls the Anti-Malware module.
      By default, this is the rule *Block if virus was found*.
   d. In the rule criteria, click the settings name.
      This name appears next to the Antimalware.Infected property. By default, it is *Gateway Anti-Malware*.
      The *Edit Settings* window opens. It provides the settings for the Anti-Malware module.

3. In the *Select scanning engines and behavior* section, select one of the following combinations of submodules:
   - **Full McAfee coverage**: The recommended high-performance configuration — When selected, the McAfee Gateway Anti-Malware engine and the McAfee Anti-Malware engine are active.
     The scanning mode is then: *Proactive methods + virus signatures*
     This module combination is enabled by default.
   - **Layered coverage**: Full McAfee coverage plus specific Avira engine features – minor performance impact — When selected, the McAfee Gateway Anti-Malware engine, the McAfee Anti-Malware engine, and, for some web objects, also the third-party Avira engine are active.
     The scanning mode is then: *Proactive methods + virus signatures + third-party module functions for some web objects*
   - **Duplicate coverage**: Full McAfee coverage and Avira engine – less performance and more false positives — When selected, the McAfee Gateway Anti-Malware engine, the McAfee Anti-Malware engine, and the third-party Avira engine are active.
     The scanning mode is then: *Proactive methods + virus signatures + third-party module functions*
   - **Avira only**: Only uses Avira engine — not recommended — When selected, only the Avira engine is active.
     The scanning mode is then: *Third-party module functions*

4. Click **OK** to close the window.

5. Click **Save Changes**.

If you select the Avira only option when working with the Gateway Anti-Malware rule set, you should rename the settings and the rule set to indicate that a key setting has changed.

The renaming could, for example, be from *Gateway Anti-Malware* (settings and rule set) to *Avira Anti-Malware* (settings and rule set).
Instead of renaming the rule set and the settings, you can also create an additional rule set and additional settings to have them available when needed for configuring rules.

**Anti-Malware settings**

The Anti-Malware settings are used for configuring the way the Anti-Malware module scans web objects for infections by viruses and other malware.

**Select Scanning Engines and Behavior**

Settings for selecting a combination of scanning engines and their behavior in case one of them detects an infection

The scanning engines are the submodules that run together as the Anti-Malware module to scan web objects.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full McAfee coverage: The recommended high-performance configuration</td>
<td>When selected, the McAfee Gateway Anti-Malware engine and the McAfee Anti-Malware engine are active. Web objects are then scanned using: <em>Proactive methods + Virus signatures</em> This option is selected by default.</td>
</tr>
<tr>
<td>Layered coverage: Full McAfee coverage plus specific Avira engine features — minor performance impact</td>
<td>When selected, the McAfee Gateway Anti-Malware engine, the McAfee Anti-Malware engine, and, for some web objects, also the third-party Avira engine are active. Web objects are then scanned using: <em>Proactive methods + Virus signatures + Third-party module functions for some web objects</em></td>
</tr>
<tr>
<td>Duplicate coverage: Full McAfee coverage and Avira engine — less performance and more false positives</td>
<td>When selected, the McAfee Gateway Anti-Malware engine, the McAfee Anti-Malware engine, and the third-party Avira engine are active. Web objects are then scanned using: <em>Proactive methods + Virus signatures + Third-party module functions</em></td>
</tr>
<tr>
<td>Avira only: Only uses Avira engine — not recommended</td>
<td>When selected, only the Avira engine is active. Web objects are then scanned using: <em>Third-party module functions</em></td>
</tr>
<tr>
<td>Stop virus scanning right after an engine detected a virus</td>
<td>When selected, engines stop scanning a web object as soon as one of them has detected an infection by a virus or other malware.</td>
</tr>
</tbody>
</table>

**Mobile Code Behavior**

Settings for configuring a risk level in classifying mobile code

The risk level can take values from 60 to 100.

A low value means the risk in proactively scanning the behavior of mobile code and not detecting that it is malware is low because the scanning methods are applied very strictly. Mobile code will then be classified as malware even if only a few criteria of being potentially malicious have been detected.

This can lead to classifying mobile code as malware that is actually not malicious ("false positives").
While more proactive security is achieved with a stricter setting, accuracy in determining which mobile code is really malicious will suffer. Consequently, the appliance might block web objects that you want to get through to your users.

A high value means the risk in not detecting malicious mobile code is high (more "false negatives"), but more accuracy is achieved in classifying mobile code correctly as malicious or not (fewer “false positives”).

**Table 11-5 Mobile Code Behavior**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification threshold</td>
<td>Sets a risk level as described above on a slider scale.</td>
</tr>
<tr>
<td></td>
<td>• Minimum value (maximum proactivity): 60</td>
</tr>
<tr>
<td></td>
<td>• Maximum value (maximum accuracy): 100</td>
</tr>
</tbody>
</table>

**Advanced Settings**

Advanced settings for all scanning submodules

**Table 11-6 Advanced Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Antivirus prescan</td>
<td>When selected, performance of the submodules is improved by reducing the load sent to them for scanning.</td>
</tr>
<tr>
<td>Increase Web Gateway performance by making a light-weight pass on:</td>
<td>This option is by default selected. We recommend that you keep this setting.</td>
</tr>
<tr>
<td>• Common web files</td>
<td>When this option is selected, the three options below it are also accessible.</td>
</tr>
<tr>
<td>• Common web files and other low-risk files</td>
<td>You can select one of them to configure the range of file types that light-weight malware scanning should be applied to.</td>
</tr>
<tr>
<td>• Common web files, other low-risk files, and web content on trustworthy sites</td>
<td>The third option is selected by default.</td>
</tr>
<tr>
<td>Files matching the selected option do not continue to the standard anti-malware scanning.</td>
<td>The three options are related to each other: If the first option is configured, the other two options are not effective. The second option includes the first option, the third option includes the first and the second option.</td>
</tr>
<tr>
<td></td>
<td>The URL Filter module is involved to verify whether the web site that a file is downloaded from is trustworthy.</td>
</tr>
<tr>
<td></td>
<td>Updates of virus and malware filtering information can modify the categorization of file types as safe or rarely exploited or hosted on trustworthy web sites.</td>
</tr>
<tr>
<td>Enable GTI file reputation queries</td>
<td>When selected, information on the reputation of files retrieved from the Global Threat Intelligence system is included in the scanning result.</td>
</tr>
<tr>
<td>Enable heuristic scanning</td>
<td>When selected, heuristic scanning methods are applied to web objects.</td>
</tr>
</tbody>
</table>
### Advanced Settings for McAfee Gateway Anti-Malware

Advanced settings for the McAfee Gateway Anti-Malware submodule

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable detection for potentially unwanted programs</td>
<td>When selected, web objects are also scanned for potentially unwanted programs.</td>
</tr>
<tr>
<td>Enable mobile code scanning</td>
<td>When selected, mobile code is scanned in general. Individual settings can be configured under <em>Scan the following mobile code types</em>.</td>
</tr>
<tr>
<td>Enable removal of disinfectable content detected in HTML documents by mobile code filter</td>
<td>When selected, the content described here can be removed.</td>
</tr>
<tr>
<td>Scan the following mobile code types</td>
<td>When the following mobile code types are selected, they are scanned.</td>
</tr>
</tbody>
</table>

**Windows executables**
- Once downloaded from the web or received by email, these executables can become a threat when launched because they run with all the privileges of the current user.

**JavaScript**
- JavaScript code can be embedded virtually anywhere, from web pages and PDF documents to video and HTML files.

**Flash ActionScript**
- ActionScript code can be embedded in flash videos and animations and has access to the flash player and the browser with all their functions.

**Java applets**
- Java applets can be embedded in web pages. Once activated, they can run at different permission levels, based on a digital certificate and the user’s choice.

**Java applications**
- Java applications run stand-alone with all privileges of the current user.

**ActiveX controls**
- ActiveX controls can be embedded in web pages and office documents. Once activated, they run with all privileges of the current user.

**Windows libraries**
- These libraries usually come along with an executable in a setup package or are downloaded from the web by a running executable or by malicious code.

**Visual Basic script**
- Visual Basic script code can be embedded in web pages or in emails.

**Visual Basic for applications**
- Visual Basic macros can be embedded in office documents created with Word, Excel, or PowerPoint.

**Block the following behavior**
- When the following types of behavior are selected, web objects showing this behavior are blocked.

**Data theft: Backdoor**
- Malicious applications grant an attacker full remote access and control to a victim’s system through existing or newly created network channels.

**Data theft: Keylogger**
- Malicious applications hook into the operating system to record and save keyboard strokes.
- The captured information, such as passwords, is sent back to the attacking party.

**Data theft: Password stealer**
- Malicious applications gather, store, and leak sensitive information, such as the system configuration, confidential data, credentials, and other data for user authentication.
<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>System compromise: Code execution exploit</td>
<td>Exploits for vulnerabilities in client applications, such as browsers, office programs, or multi-media players, allow an attacker to run arbitrary code on the compromised system.</td>
</tr>
<tr>
<td>System compromise: Browser exploit</td>
<td>Exploits for vulnerabilities in browser applications and plug-ins allow an attacker to run arbitrary code, steal sensitive data, or escalate privileges.</td>
</tr>
<tr>
<td>System compromise: Trojan</td>
<td>Malicious applications pretend to be harmless or useful, but actually perform damaging activities.</td>
</tr>
<tr>
<td>Stealth activity: Rootkit</td>
<td>Malicious applications or device drivers manipulate the operating system and hide presence of malware on infected systems. After the compromise, files, registry keys, and network connections belonging to the malware processes turn invisible and can be hard to recover.</td>
</tr>
<tr>
<td>Viral Replication: Network worm</td>
<td>Malicious applications or device drivers self-replicate using email, the internet, peer-to-peer networking, or by copying themselves onto removable media such as USB devices.</td>
</tr>
<tr>
<td>Viral Replication: File infector virus</td>
<td>Self-replicating applications infect existing files on the hard-disk, embedding viral code in order to spread through the newly infected host file.</td>
</tr>
<tr>
<td>System compromise: Trojan downloader</td>
<td>Malicious applications or script code download and execute additional payload from the web.</td>
</tr>
<tr>
<td>System compromise: Trojan dropper</td>
<td>Malicious applications carry hidden payload, extract, and launch it upon execution.</td>
</tr>
<tr>
<td>System compromise: Trojan proxy</td>
<td>Malicious applications allow to relay potentially malicious hidden network activities through the compromised system.</td>
</tr>
<tr>
<td>Web threats: Infected website</td>
<td>Websites contain injected malicious script code or request additional malicious code as soon as it is opened in a browser. The initial infection could have taken place through an SQL injection attack against the web server.</td>
</tr>
<tr>
<td>Stealth activity: Code injection</td>
<td>Applications copy their code into other, often legitimate processes, which results in a hijacking of the respective privileges and trust. This technique is typically employed by malware that tries to hide its presence on compromised systems and to evade detection.</td>
</tr>
<tr>
<td>Detection evasion: Obfuscated code</td>
<td>Applications consist of highly scrambled or encrypted code, so malicious code portions are hard to detect.</td>
</tr>
<tr>
<td>Detection evasion: Packed code</td>
<td>Applications have their content compressed by a run-time packer or protector. This changes the way the content looks, so it is harder to classify.</td>
</tr>
<tr>
<td>Potentially unwanted: Ad-/Spyware</td>
<td>Applications show potentially annoying or unwanted advertisements, but also track and analyze user behavior and activities.</td>
</tr>
<tr>
<td>Potentially unwanted: Adware</td>
<td>Applications show potentially annoying or unwanted advertisements, but also track and analyze user behavior and activities.</td>
</tr>
<tr>
<td>Data theft: Spyware</td>
<td>Applications track and analyze user behavior and activities, steal sensitive data, and leak this data to the attacker’s servers.</td>
</tr>
<tr>
<td>Potentially unwanted: Dailer</td>
<td>Applications provide access to content, for example, pornography, through a more expensive network connection.</td>
</tr>
</tbody>
</table>
Table 11-7 Advanced Settings for McAfee Gateway Anti-Malware (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web threats: Vulnerable ActiveX controls</td>
<td>ActiveX controls appearing on web pages that are restricted to other on-browser usage present potential vulnerabilities.</td>
</tr>
<tr>
<td>Potentially unwanted: Suspicious activity</td>
<td>Potentially malicious code shows either non-standard or not fully trusted behavior.</td>
</tr>
<tr>
<td>Web threats: Cross-site scripting</td>
<td>Malicious scripts exploit access-control vulnerabilities in browsers or web applications to steal user data, for example, cookies.</td>
</tr>
<tr>
<td>Potentially unwanted: Deceptive behavior</td>
<td>Messages mislead the user, play missing code tricks, and fake alerts. These threats could tell users that their systems are infected with spyware and promote fake AV applications for cleaning.</td>
</tr>
<tr>
<td>Potentially unwanted: Redirector</td>
<td>Redirecting code forwards users visiting a website to other, potentially malicious locations. This behavior is often caused by an infection of a previously legitimate website.</td>
</tr>
<tr>
<td>Potentially unwanted: Direct kernel communication</td>
<td>Applications directly communicate with a Windows kernel or in kernel mode, trying, for example, to install a root kit or to destabilize the system.</td>
</tr>
<tr>
<td>Potentially unwanted: Privacy violation</td>
<td>Potentially malicious code accesses sensitive or private data, which can result in eavesdropping clipboard content or in reading registry keys.</td>
</tr>
</tbody>
</table>

Advanced Settings for Avira
Advanced settings for the Avira submodule

Table 11-8 Advanced Settings for Avira

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size of archive member</td>
<td>Limits the size (in MB) of a member in an archive that the Avira engine scans for infections. If an archive member exceeds this size, it is not scanned and the archive is blocked. The default size limit is 1024 MB.</td>
</tr>
</tbody>
</table>

Gateway Anti-Malware rule set
The Gateway Anti-Malware rule set is the default rule set for virus and malware filtering.

Default rule set – Gateway Anti-Malware

Criteria – Always
Cycles – Requests (and IM), Responses, Embedded Objects

The rule set contains the following rules.

Allow if user agent matches User Agent Whitelist

Header.Request.Get ("User-Agent") matches in list User Agent WhiteList -> Stop Rule Set

The rule uses the Header.Request.Get property to check the user agent information that is sent with the header of a request.

If the user agent in question is on the specified whitelist, processing of the rule set stops, so the blocking rule at the end of the rule set is not processed.
A parameter of the property specifies that it is the user agent information that must be checked when the rule is processed.

This rule is not enabled by default.

Using this rule alone for whitelisting will cause a security problem because usually a client can set whatever user agent it prefers.

Allow URL host that matches in list Anti-Malware URL Whitelist

URL Host matches in list Anti-Malware URL Whitelist -> Stop Rule Set

The rule uses the URL.Host property to check whether a given URL matches one of the entries on the specified whitelist.

If it does, processing of the rule set stops and the blocking rule at the end of the rule set is not processed.

You can use this rule to exempt web traffic from filtering when the hosts of the URLs involved are well-known web servers for which it is safe to assume that they spread no viruses and other malware.

Whitelisting increases performance because it avoids the effort of scanning the respective web objects.

Remove partial content for HTTP requests

Cycle TopName equals "Request" AND (Connection.Protocol equals "http" OR Connection.Protocol equals "https") -> Continue – Header.RemoveAll ("Range")

The rule uses the Cycle.TopName and Connection.Protocol properties to check whether the current processing cycle is the request cycle and whether a request is sent in HTTP or HTTPS mode.

If this is the case, the Header.RemoveAll event modifies the request by removing the specification that only partial content is requested. A request for complete content is then forwarded to the relevant web server and eventually received from there, so that the complete content of a web object can be processed on the appliance.

For example, a complete archive can be opened and scanned for viruses and other malware. Malicious content that is distributed over several parts of a file can be detected by scanning the complete file, while it could go unnoticed if only parts of the file were scanned.

The Continue action lets processing continue with the next rule.

Block partial content for FTP requests

Cycle TopName equals "Request" AND Connection.Protocol equals "ftp" AND Command.Categories contains "Partial" -> Block <Partial Content Not Allowed>

The rule uses the Cycle.TopName, Connection.Protocol, and Command.Categories properties to check whether the current processing cycle is the request cycle, the request is sent in FTP mode, and the command category used for the FTP transfer contains Partial as a string.

This allows Web Gateway to detect an FTP request for partial content and block it.

Unlike with HTTP or HTTPS requests, an FTP request for partial content cannot be modified to make it a request for complete content. However, security problems would arise if partial content was accepted on the appliance, which are the same as the ones that were explained in the comment on the rule for blocking HTTP and HTTPS requests.

The action settings specify a message to the requesting user.

Start Media Stream Scanner on streaming media and skip anti-malware scanning

Cycle Name equals "Response" AND StreamDetector.IsMediaStream <Default Streaming Detection> equals true -> Stop Rule Set – Enable Media Stream Scanner
The rule uses the *Cycle.Name* property to check whether processing is in the response cycle and the *StreamDetector.IsMediaStream* property to check whether the web object that is sent in response to Web Gateway is streaming media.

If both are the case, processing of the rule set stops, so the remaining rule is not processed, and an event is used to start the Media Stream Scanner.

**Block if virus was found**

```
Antimalware.Infected<Gateway Anti-Malware> equals true -> Block<Virus Found> –
Statistics.Counter.Increment ("BlockedByAntiMalware",1)<Default>
```

The rule uses the *Antimalware.Infected* property to check whether a given web object is infected by a virus or other malware.

When the Anti-Malware module is called to scan the object, it runs with the Gateway Anti-Malware settings, as specified with the property. These settings let the module use all its three submodules and their methods to scan web objects.

If the module finds that a web object is infected, processing of all rules stops and the object is not passed on further. Access to it is blocked this way.

In a request cycle, the infected web object is not passed on to the web. In the response and embedded object cycles, it is not passed on to the user who requested it.

The action settings specify a message to this user.

The rule also uses an event to count blocking due to virus and malware infections.

The event parameters specify the counter that is incremented and the size of the increment. The event settings specify the settings of the Statistics module, which executes the counting.

**Media stream scanning**

Media streams can be scanned on Web Gateway chunk-by-chunk, which allows users to see or hear downloaded streaming media faster, as they do not have to wait until a stream has been scanned completely.

This scanning method is performed by the Media Stream Scanner, which is provided by the McAfee Gateway Anti-Malware engine. Streaming media is scanned and delivered chunk-by-chunk to the client that requested the download. If an infection is detected in a chunk, the download stops, and this chunk and the rest of the streaming media are not delivered.

The scanning that is performed by the Media Stream Scanner uses the proactive functions of the Gateway Anti-Malware engine. The McAfee Anti-Malware and Avira engines, which can also be configured to scan web objects for infections by viruses and other malware, are not involved when the Media Stream Scanner is active.

The scanner is started by an event of a rule in the Gateway Anti-Malware rule set of the default rule set system. The rule applies if the Stream Detector module finds that a web object that was received on Web Gateway in response to a download request is streaming media.

Processing of the rule set stops and the remaining rule in the rule set, which also lets web objects be scanned for infections by viruses and other malware, is not processed.

If a web object is not recognized by the Stream Detector as streaming media, the rule does not apply, processing continues with the remaining rule, and the web object is scanned according to the settings that are configured for this rule.
Anti-malware queue

To avoid overloading of the modules that scan web objects for infections by viruses and other malware, requests for access to web objects are moved to a queue before being processed.

This queue is known as the anti-malware queue. When a request has been received on the appliance, it is moved to this queue by a working thread of the proxy module. It remains there until it is fetched by another thread and forwarded to a thread of one of the scanning modules.

The same applies to responses received from web servers that requests have been forwarded to.

The working threads that deliver requests and responses to the scanning modules, as well as those that are used by the modules to execute scanning activities, are referred to as anti-malware working threads or simply as AV threads.

When configuring the anti-malware queue, you can specify the following:

- Number of available anti-malware working threads
- Size of the anti-malware queue
- Maximum time for requests and responses to stay in the queue

Moving requests and responses to the anti-malware queue is a solution to avoid load peaks occurring over a short period of time. Permanent overloading should be addressed by other measures.

Configure the anti-malware queue

You can configure settings for the anti-malware queue to avoid overloading of the scanning modules.

Task

1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to configure the anti-malware queue on and click Anti-Malware.

The settings for the anti-malware queue appear on the settings pane.
3. Configure these settings as needed.
4. Click Save Changes.

Anti-Malware system settings

The Anti-Malware system settings are used for configuring the anti-malware queue.

Global Anti-Malware Settings

Settings for the anti-malware queue
Table 11-9 Global Anti-Malware Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of threads for AV scanning</td>
<td>Sets the number of anti-malware working threads that are available on an appliance.</td>
</tr>
<tr>
<td></td>
<td>The number you specify here applies to both the threads that forward requests and responses to threads of the scanning modules and the scanning module threads themselves.</td>
</tr>
<tr>
<td></td>
<td>For example, if you specify 25, there will be 25 threads for forwarding and 25 for scanning.</td>
</tr>
<tr>
<td>Use at least as many AV threads as the number of</td>
<td>When selected, the number of AV threads use for scanning activities is at least the same as the number of available CPU cores.</td>
</tr>
<tr>
<td>CPU cores available</td>
<td></td>
</tr>
<tr>
<td>Maximum number of jobs in the queue</td>
<td>Limits the number of requests or responses that can be moved to the anti-malware queue as jobs for the scanning modules.</td>
</tr>
<tr>
<td>Number of seconds a scanning job stays in the</td>
<td>Limits the time (in seconds) that elapses before a request or response is removed from the anti-malware queue if it has not been forwarded for scanning.</td>
</tr>
<tr>
<td>queue before being removed</td>
<td></td>
</tr>
</tbody>
</table>

URL filtering

URL filtering ensures that the users of your network cannot access web objects that are considered a risk for web security or are not allowed for other reasons. The filtering process uses blocking lists, category information, and reputation scores for the URLs of web objects and blocks or allows access accordingly.

The process includes several elements, which contribute to it in different ways.

- Filtering rules control the process.
- A whitelist and various blocking lists are used by rules to let some web objects skip URL filtering and block others.
- The URL Filter module, which is called by particular rules, retrieves information on URL categories and web reputation scores from the Global Threat Intelligence service.

A default process for URL filtering is implemented on Web Gateway after the initial setup. You can modify this process to adapt it to the requirements of your web security policy.

To configure URL filtering, you can work with:

- **Key elements of rules** — After clicking the default URL filtering rule set on the rule sets tree, you can view and configure key elements of the default rules for the filtering process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the default rules for the filtering process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.
Filtering rules

The rules that control the URL filtering process are usually contained in one URL filtering rule set. One of these rules says, for example, that access to a URL is blocked if it matches an entry on a blocking list.

Another rule blocks URLs if they belong to a category that is on a blocking list. This rule calls the URL Filter module to retrieve category information for URLs from the Global Threat Intelligence system. Another rule works in a similar way to block URLs that have a bad reputation.

A whitelisting rule exempts URLs from filtering if they match entries on the list used by the rule. This rule is placed and processed before the blocking rules. If it applies, the blocking rules are skipped and no URL filtering is performed for the whitelisted objects.

When the default rule set system is implemented, a rule set for URL filtering is included. Its name is URL Filtering.

Whitelist and blocking lists

A whitelist is used by a whitelisting rule to let some URLs skip the blocking rule, which means there is no filtering for these URLs.

Since a URL filtering rule set controls only URL filtering, multiple whitelists for several types of objects are not needed in the filtering process, in contrast to virus and malware filtering.

Another rule blocks URLs if they belong to a category that is on a blocking list. This rule calls the URL filter module to retrieve category information for URLs from the Global Threat Intelligence system. Another rule works in a similar way to block URLs that have a bad reputation.

Since a URL filtering rule set handles only URL filtering, whitelists are not needed for several types of objects as they are in virus and malware filtering.

Blocking lists are used by rules for blocking URLs according to the categories they belong to or because they match an entry on a list. Each of the blocking rules uses its own list.

Filter module

The URL Filter module is also known as the URL Filter engine. It retrieves information on URL categories and reputation scores from the Global Threat Intelligence™ service that is provided by McAfee. Based on this information, blocking rules block access to URLs.

Various technologies, such as link crawlers, security forensics, honeypot networks, sophisticated auto-rating tools, and customer logs are used to gather this information. An international, multi-lingual team of McAfee web analysts evaluates the information and enters URLs under particular categories into a database.

To gather information on the reputation of a URL, its behavior on a worldwide real-time basis is analyzed, for example, where a URL shows up in the web, its domain behavior, and other details.

You can configure settings for this module, for example, to let it include category information retrieved from an extended list that you provide or to perform a DNS lookup for URLs and include the corresponding IP address in the search for category information.
Configure key elements for URL filtering

Configure key elements of the rules for URL filtering to adapt important parts of the filtering process to the requirements of your web security policy.

**Task**
2. On the rule sets tree, select the URL Filtering rule set.
   - Key elements of the rules for the filtering process appear in the configuration pane.
3. Configure the key elements as needed.
4. Click Save Changes.

**See also**
*Key elements for URL filtering on page 343*

### Key elements for URL filtering

The key elements for URL filtering deal with important parts of this filtering process.

#### Basic Filtering

Key elements for performing basic URL filtering

**Table 11-10 Basic Filtering**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL whitelist</td>
<td>Clicking Edit opens a window to let you edit the URL whitelist that is used by a rule. You can add, modify, and remove entries on the list.</td>
</tr>
<tr>
<td>URL blocklist</td>
<td>Clicking Edit opens a window to let you edit the URL blocklist that is used by a rule. You can add, modify, and remove entries on the list.</td>
</tr>
<tr>
<td>URL category blocklist</td>
<td>Clicking Edit opens a window to let you edit the URL category blocklist that is used by a rule. You can add, modify, and remove entries on the list.</td>
</tr>
</tbody>
</table>

#### SafeSearch

Key elements for integrating SafeSearch in the URL filtering process

**Table 11-11 SafeSearch**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SafeSearch</td>
<td>When selected, a rule is enabled that controls the SafeSearch part of the URL filtering process.</td>
</tr>
<tr>
<td>SafeSearch settings</td>
<td>Clicking Edit opens a window to let you edit the settings for the SafeSearch Enforcer module (or engine). This module handles the integration of the SafeSearch Enforcer, which is an additional web security product, in the URL filtering process on Web Gateway.</td>
</tr>
</tbody>
</table>
**GTI reputation**

Key element for evaluating reputation scores retrieved from the Global Threat Intelligence service within the URL filtering process

Table 11-12 GTI reputation

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block URLs with a High Risk reputation</td>
<td>When selected, a rule is enabled that blocks URLs with a reputation score that lets them appear to be a high or medium risk to web security.</td>
</tr>
<tr>
<td></td>
<td>The reputation score of a URL is established by the Global Threat Intelligence service, which is provided by McAfee. It is retrieved from this service by the URL Filter module.</td>
</tr>
</tbody>
</table>

**Uncategorized URLs**

Key element for handling URLs that could not be categorized during the URL filtering process

Table 11-13 Uncategorized URLs

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncategorized URLs</td>
<td>Selecting <strong>Block</strong> enables a rule that blocks requests for access to web objects with URLs that could not be categorized during the URL filtering process.</td>
</tr>
<tr>
<td></td>
<td>Selecting <strong>Allow</strong> means that no action is executed by this rule. URL filtering continues with processing the next rule.</td>
</tr>
</tbody>
</table>

**Configure URL filtering using the complete rules view**

You can configure URL filtering to adapt this process to the needs of your network.

To configure URL filtering, you can work with the key elements view or the rules view.

**Task**

1. Review the rules in the rule set for URL filtering.  
   By default, this is the **URL Filtering** rule set.

2. Modify these rules as needed.  
   You can, for example, do the following:  
   - Enable or disable blocking rules and the whitelist rule  
   - Edit the lists used by these rules  

   **A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.**

   - Modify the settings of the URL Filter module

3. Save your changes.
Configure settings for the URL Filter module

You can configure the URL Filter module to modify the way information on URL categories and reputation scores is retrieved from the Global Threat Intelligence system.

**Task**


2. On the rule sets tree, select a rule set for URL filtering.
   In the default rule set system, rule sets for URL filtering are nested in the rule sets for content filtering.
   The rules appear on the settings pane.

3. Make sure Show details is selected.

4. Find the rule that uses a category blocking list.
   By default, this is the rule Block URLs whose category is in Category BlockList.

5. In the rule criteria, click the settings name.
   This name appears next to the URL.Categories property. By default, it is Default.
   The Edit Settings window opens. It provides the settings for the URL Filter module.

6. Configure these settings as needed.

7. Click OK to close the window.

8. Click Save Changes.

**See also**

URL Filter settings on page 345

**URL Filter settings**

The URL Filter settings are used for configuring the way the URL Filter module retrieves information from the Global Threat Intelligence system.

**Extended List**

Settings for extended lists

<table>
<thead>
<tr>
<th>Table 11-14  Extended List</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td>Use the extended list</td>
</tr>
<tr>
<td>Add</td>
</tr>
<tr>
<td>Edit</td>
</tr>
</tbody>
</table>

**Rating Settings**

Settings for retrieving rating information on URLs based on categories and reputation scores
Table 11-15 Rating Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search the CGI parameters for rating</strong></td>
<td>When selected, CGI parameters are included in the search for information. CGI (Common Gateway Interface) parameters in a URL trigger scripts or programs when the URL is accessed. Information on CGIs is considered when categorizing a URL.</td>
</tr>
<tr>
<td><strong>Search for and rate embedded URLs</strong></td>
<td>When selected, embedded URLs are included in the search for information and rated. Information on an embedded URL is considered when categorizing the embedding URL.</td>
</tr>
<tr>
<td><strong>Do a forward DNS lookup to rate URLs</strong></td>
<td>When selected, a DNS lookup is performed for a URL that no relevant information has been found for. The IP address that was looked up is used for another search.</td>
</tr>
<tr>
<td><strong>Do a backward DNS lookup for unrated IP-based URLs</strong></td>
<td>When selected, a backward DNS lookup, based on its IP address, is performed for a URL that no relevant information has been found for. The host name that was looked up is used for another search.</td>
</tr>
<tr>
<td><strong>Use the built-in keyword list</strong></td>
<td>When selected, the built-in keyword list is included in the search.</td>
</tr>
<tr>
<td><strong>Only use online GTI web reputation and categorization services</strong></td>
<td>When selected, information on URL categories and reputation scores is only retrieved from the Global Threat Intelligence system.</td>
</tr>
<tr>
<td><strong>Use online GTI web reputation and categorization services if local rating yields no results</strong></td>
<td>When selected, information on URL categories and reputation scores is only retrieved from the Global Threat Intelligence system if the search in the internal database yielded no results.</td>
</tr>
<tr>
<td><strong>Use default GTI server for web reputation and categorization services</strong></td>
<td>When selected, the appliance connects to the default server for retrieving information on URL categories and reputation scores from the Global Threat Intelligence system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP of the server</strong> — Specifies the IP address of the server used to connect to the Global Threat Intelligence system when the default server is not used.</td>
</tr>
<tr>
<td></td>
<td>Format: &lt;domain name&gt; or &lt;IPv4 address&gt; or &lt;IPv4 address mapped to IPv6 address&gt;</td>
</tr>
<tr>
<td></td>
<td>Regular IPv6 addresses cannot be specified here.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Port of the server</strong> — Specifies the port number of the port on this server that listens to requests from the appliance.</td>
</tr>
<tr>
<td></td>
<td>Allowed range: 1–65535</td>
</tr>
</tbody>
</table>

**Advanced Settings**

Advanced settings for the URL Filter module
### Table 11-16 Advanced Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treat connection problems to the cloud as errors</td>
<td>When selected, problems arising on the connection from the appliance to the Global Threat Intelligence server are logged as errors. Properties for error handling are set and eventually rules from an Error Handler rule set are executed.</td>
</tr>
<tr>
<td>Do a backward DNS lookup also for private addresses</td>
<td>When selected, private IP addresses are included in the backward DNS lookup. Excluding these addresses from the lookup leads to an increase in performance for URL filtering. This option is disabled by default. The lookup includes the following types of addresses: • IPv4 • Private addresses • Zeroconf addresses • IPv6 • Link local addresses • Site local addresses • Unique local addresses</td>
</tr>
</tbody>
</table>

Settings for configuring a proxy the appliance can use to connect to the Global Threat Intelligence™ system

### Table 11-17 Proxy Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use upstream proxy</td>
<td>When selected, the appliance uses a proxy for connecting to the Global Threat Intelligence server on which lookups for URL category information, also known as “in-the-cloud” lookups, can be performed.</td>
</tr>
<tr>
<td>IP or name of the proxy</td>
<td>Specifies the IP address or host name of the proxy.</td>
</tr>
<tr>
<td>Port of the proxy</td>
<td>Specifies the number of the port on the proxy that listens for lookup requests from the appliance.</td>
</tr>
<tr>
<td>User name</td>
<td>Specifies a user name for the appliance when logging on to the proxy.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets a password for an appliance.</td>
</tr>
<tr>
<td>Set</td>
<td>Opens a window for setting a password.</td>
</tr>
</tbody>
</table>

Settings for logging URL filtering activities on the appliance
### Table 11-18 Logging

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable logging</td>
<td>When selected, URL filtering activities are logged on the appliance.</td>
</tr>
<tr>
<td></td>
<td>If this option is not selected, the following logging options are grayed out.</td>
</tr>
<tr>
<td>Log level</td>
<td>Provides a list for selecting the log level.</td>
</tr>
<tr>
<td></td>
<td>Log levels are as follows:</td>
</tr>
<tr>
<td></td>
<td>• 00 FATAL — Logs only fatal errors.</td>
</tr>
<tr>
<td></td>
<td>• 01 ERRORS — Logs all errors.</td>
</tr>
<tr>
<td></td>
<td>• 02 WARNING — Logs errors and warnings.</td>
</tr>
<tr>
<td></td>
<td>• 03 INFO — Logs errors, warnings, and additional information.</td>
</tr>
<tr>
<td></td>
<td>• 04 DEBUG1 ... 013 DEBUG9 — Log information required for debugging URL filtering activities. The amount of logged information increases from level DEBUG1 to DEBUG9.</td>
</tr>
<tr>
<td></td>
<td>• 14 TRACE — Logs information required for tracing URL filtering activities.</td>
</tr>
<tr>
<td></td>
<td>• 15 ALL — Logs all URL filtering activities</td>
</tr>
<tr>
<td>(Log area)</td>
<td>Provides a set of options for including different areas of URL filtering activities into the logging.</td>
</tr>
<tr>
<td></td>
<td>• LOG_AREA_ALL — When selected, all URL filtering activities are logged.</td>
</tr>
<tr>
<td></td>
<td>• LOG_AREA_NETWORK — When selected, activities regarding the network connections used for URL filtering are logged.</td>
</tr>
<tr>
<td></td>
<td>• LOG_AREA_DATABASE_SEARCH — When selected, activities regarding the retrieval of data for URL filtering from the internal database are logged.</td>
</tr>
<tr>
<td></td>
<td>• LOG_AREA_DNS — When selected, activities regarding a DNS lookup that is performed for URL filtering are logged.</td>
</tr>
<tr>
<td></td>
<td>• LOG_AREA_URL — When selected, activities for handling URLs, such as parsing them, are logged.</td>
</tr>
<tr>
<td></td>
<td>• LOG_AREA_CLOUD — When selected, activities regarding the retrieval of information from the Global Threat Intelligence system are logged.</td>
</tr>
</tbody>
</table>

### Best practices - Using URL properties to whitelist web objects

URL properties, such as `URL`, `URL.Host`, `URL.Host.BelongsToDomains`, and others, can be used in the criteria of rules to whitelist web objects.

When a web object is whitelisted, users are allowed to access it, for example, to view a web page or download a file. Whitelisting rules are inserted into appropriate rule sets within the rule set system of Web Gateway. They usually stop further rule processing with regard to the current request for accessing a web object to prevent other rules from blocking this access.

Different URL properties can be used for different kinds of whitelisting. To allow access to an individual web object, for example, to ensure users can download a particular file, the `URL` property is best used together with a list that contains the full URL for this file.

The following examples explain which URL properties are best used for different kinds of whitelisting and how to do it.
In addition to this, some tips and examples are given regarding the:

- Values that different URLs are set to when a sample URL is processed that has been sent to Web Gateway in a request for web access
- Use of the two operators *is in list* and *matches in list* in the criteria of a rule
- Good and bad entries in the lists that are used with different URL properties

**Whitelisting individual web objects – URL**

**Goal**
Allow users to access individual web objects.

For example, download the file *Stinger.exe*, which can be accessed using the URL


**How to do it**
Use the *URL* string property with a list of full URLs in the criteria of a rule.

The rule could, for example, be configured as follows:

*URL is in list URLWhiteList* –> Stop Rule Set

If you add the URL *http://download.mcafee.com/products/mcafee-avert/Stinger/Stinger.exe* to the list *URLWhiteList*, the file *Stinger.exe* is whitelisted when the rule is processed.

In a similar way, you can block access to the file using the following rule from the default URL Filtering rule set:

*URL matches in list URLBlockList* –> Block

If you add the URL in question to the list *URLBlockList*, the file is blocked when the rule is processed.

If the *matches in list* operator is used instead of *is in list*, expressions containing wildcards can be entered into the list that is used by the property. The property can then also be used to whitelist multiple web objects.

However, if all web objects provided by a particular host should be whitelisted, this can be achieved more easily using the *URL.Host* property.

**Whitelisting hosts – URL.Host**

**Goal**
Allow users to access the web objects that are provided on particular hosts.

For example, download the file *Stinger.exe* or any other file that is provided on the host *download.mcafee.com*.

**How to do it**
Use the *URL.Host* string property with a list for host names in the criteria of a rule.

A rule that the *URL.Host* property is used in could, for example, be configured as follows:

*URL.Host is in list HostWhiteList* –> Stop Rule Set

If you add the host *download.mcafee.com* to the list *HostWhiteList*, all web objects that are provided by this host are whitelisted when the rule is processed.

If the *matches in list* operator is used instead of *is in list*, expressions containing wildcards can be entered into the list that is used by the property. The property can then also be used to whitelist multiple hosts.
However, if all hosts within a particular domain should be whitelisted, this can be achieved more easily using the \texttt{URL.Host.BelongsToDomains} property.

**Whitelisting domains – \texttt{URL.Host.BelongsToDomains}**

**Goal**
Allow users to access the web objects that are provided within particular domains.

For example, download the file \texttt{Stinger.exe} and any other file that is provided by the host \texttt{download.mcafee.com}, as well as any other downloadable file provided by any other host within the domain \texttt{mcafee.com}.

**How to do it**
Use the \texttt{URL.Host:BelongsToDomains} Boolean property with a list of domain names in the criteria of a rule.

The rule could, for example, be configured as follows:

\texttt{URL.Host.BelongsToDomains("Domain List") equals true \rightarrow Stop Rule Set}

If you add the domain \texttt{mcafee.com} to the list \texttt{Domain List}, all web objects within this domain are whitelisted when the rule is processed.

The list \texttt{Domain List} is configured as a parameter of the \texttt{URL.Host:BelongsToDomains} property, which is of the Boolean type.

When, for example, the URL \texttt{http://download.mcafee.com/products/mcafee-avert/Stinger/Stinger.exe} is processed, the value of the property (true or false) depends on whether the \texttt{mcafee.com} domain has been entered into the list \texttt{Domain List} or not.

The following example shows which entries in the list \texttt{Domain List} lead to a match when the property is used for whitelisting:

\texttt{mcafee.com}
\texttt{dell.com}
\texttt{k12.ga.us}
\texttt{twitter.com}
\texttt{xxx}

Then the criteria:

\texttt{URL.Host.BelongsToDomains("Domain List") equals true}

matches for the following URLs:

\texttt{https://contentsecurity.mcafee.com}
\texttt{https://my.mcafee.com}
\texttt{http://my.support.dell.com}
\texttt{http://www.dekalb.k12.ga.us}
\texttt{http://twitter.com}
\texttt{http://www.twitter.com}
\texttt{any.site.xxx}

but not for:

\texttt{https://www.mymcafee.com}
Using the `URL.Host.BelongsToDomains` property also avoids the effort of creating more complicated solutions to achieve the same, for example:

- Using two entries in a list of wildcard expressions, such as:
  
  `twitter.com`
  `*twitter.com`

  - Using a single, complex entry in a list of wildcard expressions, such as:
    
    `regex((.*)\.|(.?)twitter\.com)`

### Property values for a sample URL

When the sample URL `http://www.mcafee.com/us/products/web-gateway.aspx` is processed, the URL properties below are set to different values as follows.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value for sample URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL.Host</td>
<td><code>www.mcafee.com</code></td>
</tr>
<tr>
<td>URL.Host.BelongsToDomain</td>
<td><code>true</code> or <code>false</code></td>
</tr>
<tr>
<td>URL.FileName</td>
<td><code>web-gateway.aspx</code></td>
</tr>
<tr>
<td>URL.Path</td>
<td><code>/us/products/web-gateway.aspx</code></td>
</tr>
<tr>
<td>URL.Protocol</td>
<td><code>http</code></td>
</tr>
</tbody>
</table>

### Use of operators for different types of matches

It makes an important difference whether the `is in list` or `matches in list` operator is used in the criteria of a rule.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is in list</td>
<td>Requires an exact string match. If there are wildcard characters in a list entry, they are interpreted as literal strings.</td>
</tr>
<tr>
<td>matches in list</td>
<td>Allows and evaluates wildcards in list entries.</td>
</tr>
</tbody>
</table>

### Good and bad entries in lists for URL properties

Entries in the lists that are used by the different URL properties can be good or bad, according to how they fit in with the intended use of a property. The following are examples of good and bad list entries.
### URL property

<table>
<thead>
<tr>
<th>URL with <em>is in list</em> operator</th>
<th>Good</th>
<th>Bad</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>Good</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The full URL is entered, as it is required for this property. No wildcards are specified, as these are not evaluated when the <em>is in list</em> operator is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Bad</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The entry does not specify the full URL, as the protocol information, <em>http://</em>, is not included.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>URL with <em>matches in list</em> operator</th>
<th>Good</th>
<th>Bad</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>Good</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://www.mcafee.com/">http://www.mcafee.com/</a>*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This entry contains a wildcard for allowing access to any web object provided by the host <a href="http://www.mcafee.com">www.mcafee.com</a>, which is appropriate when the <em>matches in list</em> operator is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>The entry will not match for <a href="http://mcafee.com/">http://mcafee.com/</a></strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>**regex(http(p</td>
<td>ps):/(.*)</td>
</tr>
<tr>
<td></td>
<td>This entry is more complex, as it uses regular expressions. When matched, it allows access, under the HTTP or HTTPS protocol, to any web object within the domain mcafee.com and its subdomains.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>**regex(http(p</td>
<td>ps):/(.*)</td>
</tr>
<tr>
<td></td>
<td>This entry is the same as the previous, but shows how other top-level domains, such as .com or .co.us, can be whitelisted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Bad</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>.mcafee.com</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The entry does not exclude unwanted matches, for example, a match for the URL <em><a href="http://malicious-download-site.cc/malicious-file.exe?url=www.mcafee.com">http://malicious-download-site.cc/malicious-file.exe?url=www.mcafee.com</a></em></td>
<td></td>
</tr>
<tr>
<td>URL property</td>
<td>Good and bad list entries</td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>URL.Host with <em>is in list</em> operator</td>
<td><strong>Good</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://www.mcafee.com">www.mcafee.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A host name is entered, which fits in with the intended use for this property. No wildcards are specified, which is appropriate when the <em>is in list</em> operator is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Bad</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mcafee.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The entry specifies a domain name (<em>mcafee.com</em>), whereas the value of the property is a host name (<em><a href="http://www.mcafee.com">www.mcafee.com</a></em> if, for example, the URL <em><a href="http://www.mcafee.com/us/products/web-gateway.aspx">http://www.mcafee.com/us/products/web-gateway.aspx</a></em> is processed). No match will be produced this way.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>*.*mcafee.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The entry contains a wildcard, which is not evaluated when the <em>is in list</em> operator is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>*.<em>mcafee.com/us</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The entry includes path information (<em>/us</em>), which does not fit in with the intended use of the property. In addition to this, a wildcard is specified, which is not evaluated when the <em>is in list</em> operator is used.</td>
<td></td>
</tr>
</tbody>
</table>
### URL property

**URL.Host with matches in list operator**

<table>
<thead>
<tr>
<th>Good</th>
<th>Bad</th>
</tr>
</thead>
</table>
| *.mcafee.com  
The entry matches for on any host within the domain mcafee.com, but not for mcafee.com itself.  
regex((.*\.|\.|\?mcafee\.com))  
The entry uses regular expressions to whitelist the domain mcafee.com and any of the hosts within it. | *.mcafee.com*  
The entry does not exclude unwanted matches, for example, http://www.mcafee.com.malicious-download-site.cc/.  
*.mcafee.com/us*  
The entry includes path information (/us), which does not fit in with the intended use of the property. |

**URL.HostBelongsToDomains**

<table>
<thead>
<tr>
<th>Good</th>
<th>Bad</th>
</tr>
</thead>
</table>
| mcafee.com entered in the list Domain List, which is configured as a parameter of the property.  
The entry matches for the mcafee.com domain and all hosts within it, for example, www.mcafee.com or secure.mcafee.com.  
www.mcafee.com  
The entry does not specify a domain, but is valid. It only whitelists the host www.mcafee.com.  
This can also be achieved by adding the entry to a list for the URL.Host property used together with the is in list operator. | *.mcafee.com*  
The entry contains a wildcard, which does not fit in with the intended use of the property.  
The property was rather developed to avoid the effort of using wildcards in list entries. Instead it requires an exact domain match, for example, a match for mcafee.com. |

### URL Filtering rule set

The URL Filtering rule set is the default rule set for URL filtering.

**Default rule set – URL Filtering**

| Criteria – Always  
Cycles – Requests (and IM), responses, embedded objects |

The rule set contains the following rules.

**Allow URLs that match in URL WhiteList**

URL matches in list URLWhiteList –> Stop Rule Set
The rule uses the URL property to check whether a given URL is on the specified whitelist. If it is, processing of the rule set stops and the blocking rules that follow the whitelisting rule are not processed.

You can use this rule to exempt URLs from filtering to make sure they are available to the users of your network and do not get blocked by any of the following blocking rules. Whitelisting also increases performance because it avoids the effort of retrieving information about the respective URLs.

**Block URLs that match in URL BlockList**

URL matches in list URL BlockList -> Block<URLBlocked> — Statistics.Counter.Increment ("BlockedByURLFilter",1)<Default>

The rules uses the URL property to check whether a given URL is on the specified blocking list. If it is, processing of all rules stops and the request for access to the URL is not passed on to the appropriate web server. Access to it is blocked this way.

The action settings specify a message to the requesting user.

The rule also uses an event to count blocking due to virus and malware infections. The event parameters specify the counter that is incremented and the size of the increment. The event settings specify the settings of the Statistics module, which executes the counting.

**Enable SafeSearchEnforcer**

Always -> Continue — Enable SafeSearchEnforcer<Default>

The rule enables the SafeSearchEnforcer, which is an additional module for filtering access to web sites with adult content.

The enabling is done by executing an event. The settings of the module are specified with the event. Processing continues with the next rule.

**Allow uncategorized URLs**

List.OfCategory.IsEmpty(URL.Categories<Default>) equals true -> Stop Rule Set

The rule uses the List.OfCategoryIsEmpty property, which has the URL.Categories property as a parameter, to check whether the list of categories for categorizing a URL is empty. This would mean that the URL is uncategorized, as it could not be assigned to any of the existing categories. Specifying the URL.Categories property as a parameter ensures that it is a particular list of categories that is checked. It is the list that is the value of this property.

To provide a list of categories as the value for the URL.Categories property, the URL Filter module is called, which retrieves this list from the Global Threat Intelligence system. The module runs with the specified Default settings.

If a URL is uncategorized, processing of the rule set stops and the blocking rules that follow this rule are not processed. The request for the URL is forwarded to the appropriate web server and, unless access to the URL is blocked in the response or embedded object cycle, the user is allowed to access the web object that was requested by submitting the URL.

**Block URLs whose category is in URL Category BlockList**

URL.Categories<Default> at least one in list Category BlockList -> Block<URLBlocked> — Statistics.Counter.Increment ("BlockedByURLFilter",1)<Default>

The rule uses the URL.Categories property to check whether one of the categories a given URL belongs to is on the specified blocking list. The URL Filter module, which is called to retrieve information on these categories, runs with the Default settings, as specified with the property.

If one of the URL’s categories is on the list, processing of all rules stops and the request for access to the URL is not passed on to the appropriate web server. Access to it is blocked this way.

The URLBlocked action settings specify that the user who requested this access is notified of the blocking.

The rule also uses an event to count blocking due to URL filtering in the same way as the blocking rule for individual URLs in this rule set.
Block URLs with bad reputation

\[ URL.IsHighRisk<Default> \text{ equals } \text{true} \rightarrow \text{Block<URLBlocked>} \rightarrow \text{Statistics.Counter.Increment} \text{("BlockedByURLFilter",1)<default>} \]

The rules use the \text{URL.IsHighRisk} property to find out whether a URL has a reputation that lets access to it appear as a high risk. If the value for this property is true, processing of all rules stops and the request for access to the URL is not passed on to the appropriate web server. Access to it is blocked this way.

The reputation score is retrieved by the URL Filter module, which runs with the settings specified after the property.

The \text{URLBlocked} action settings specify that the user who requested this access is notified of the blocking.

The rule also uses an event to count blocking due to URL filtering in the same way as the blocking rule for individual URLs in this rule set.

URL filtering using the Dynamic Content Classifier

URLs can be categorized for filtering by the Dynamic Content Classifier.

The Dynamic Content Classifier (DCC) is another source of category information with regard to URLs, in addition to the local database and the Global Threat Intelligence service.

You can configure use of the Dynamic Content Classifier when lookups for URL category information involving the other two sources yield no results.

Configure use of the Dynamic Content Classifier

You can configure use of the Dynamic Content Classifier for detecting URL categories when other methods of detection yield no results.

\textbf{Task}


2. On the rule sets tree, select a rule set with rules for URL filtering.

   In the default rule set system, this is, for example, the URL Filtering rule set.

   The rules appear in the settings pane.

3. Make sure \text{Show details} is selected.

4. Select the rule for handling URL categories that you want to configure use of the Dynamic Content Classifier for.

   In the URL Filtering rule set, this is, for example, the rule \text{Block URLs whose category is in Category BlockList}.

5. Click the settings of the URL Filter module in the rule criteria.

   In the sample rule, these are the \text{Default} settings in the criteria \text{URL.Categories <Default> at least one in list Category BlockList}.

   The Edit Settings window opens. It provides the settings of the URL Filter module.

6. Under Rating Settings, make sure \text{Enable the Dynamic Content Classifier if GTI web categorization yields no results} is selected.

7. [Optional] Edit the list of URL categories the Dynamic Content Classifier should detect.

   a. Above the list Categories that will be dynamically detected, click the Edit icon.

   The Edit window opens.
b Under DCC category, expand the Supported Categories folder.

c Select or deselect URL categories as needed.

d Click OK.

The Edit window closes and the selected categories appear on the list.

8 Click OK to close the Edit Settings window.

9 Click Save Changes.

The Dynamic Content Classifier is now involved in detecting whether a URL that is submitted in a request for web access falls into one of the configured URL categories.

**Using your own URL filter database**

URL filtering can be performed using information that is retrieved from a database of your own.

URL filtering on a Web Gateway appliance uses information about the categories that URLs fall into and the web reputation scores that are assigned to them. This information is retrieved from the local URL filter database, the Global Threat Intelligence system, or the Dynamic Content Classifier, depending on how the settings of the module for URL filtering are configured.

The information in the local database is the result of storing categories and web reputation scores there after they have been determined for particular URLs by the Global Threat Intelligence system. When a lookup in the local database yields no results, the other two information sources can additionally be used.

Instead of the local database, you can use a database of your own, containing information on URL categories and web reputation scores. To replace the local database, you need to specify the URL of the server that your database resides on when configuring the Central Management settings.

You can use your own database as the source that is searched first to retrieve URL filtering information, but also disable the other two sources and restrict the filtering process to using the information stored in your database.

**Configure use of your own URL filter database**

To retrieve URL filtering information from a database of your own, configure the use of this database as part of the Central Management settings.

**Task**

1 Select Configuration | Appliances.

2 On the appliances tree, select the appliance that should use your database information and click Central Management.

3 Scroll down to Advanced Update Settings.

4 In the Enter a special custom parameter for an update server field, enter the URL of the server that your database resides on.

5 Click Save Changes.

When database information is used to filter URLs on the appliance, it is not retrieved from the local database, but from your own database.
You can additionally disable other sources of URL filtering information to restrict the filtering process to the information stored in your own database.

**Restrict URL filtering to using database information**

To use only database information for URL filtering, disable use of the Global Threat Intelligence system and the Dynamic Content Classifier.

If you configured the use of your own URL filter database, filtering information is retrieved only from this database.

**Task**

1. Select **Policy | Settings**.
2. Under **Engines | URL Filter**, select the URL Filter settings you want to disable information sources for.
3. Under **Rating Settings**, deselect the following two checkboxes one after another:
   - Enable the Dynamic Content Classifier if GTI web categorization yields no result
   - Use online GTI web reputation and categorization services if local rating yields no result
4. Click **Save Changes**.

**URL filtering using an IFP proxy**

URL filtering can be performed on requests to web access submitted under the IFP protocol.

To perform URL filtering on such requests, you need to:

- Set up an IFP proxy.
- Implement suitable filtering rules.

Filtering activities for IFP requests are displayed on the dashboard of the user interface. Connection tracing can also be performed for these activities.

**Setting up an IFP proxy**

To process and filter requests for web access that users submit from their client systems under the IFP protocol, the proxy functions of the appliance must be appropriately configured. An IFP proxy must be set up that intercepts these requests and makes them available for URL filtering.

To set up the proxy, you need to specify a number of settings on the user interface under **Configuration | Proxies**. These settings include:

- Enabling or disabling the proxy
- List of proxy ports, specifying for each proxy:
  - IP address and port number
  - Message mode (Indicates whether a block message is sent as a redirect or as normal message under the IFP protocol)
- Maximum number of concurrent IFP requests
  
  Using this setting, you can prevent an overloading of the IFP proxy.

**Rules for filtering IFP requests**

There is no default or library rule set for controlling the process of filtering IFP requests. However, you can create a rule set of your own and also make use of the IFP proxy functions in existing rule sets.
When creating a rule set for filtering IFP requests, you need to specify use of the IFP protocol as the rule set criteria to ensure the rule set is applied to requests that are submitted under this protocol. This is achieved by including the `Connection.Protocol` property in the criteria and configuring the IFP protocol as its operand.

As the IFP protocol covers only requests, you can exclude filtering responses and embedded objects as activities that the rule set should apply to.

The rules in the rule set can be the same as in the default URL Filtering rule set.

If you want to perform URL filtering only for requests sent under the IFP protocol, we recommend that you delete the default URL Filtering rule set and use only the IFP filtering rule set you have created in the way described here.

Using the IFP proxy functions in existing rule sets can be an option, for example, if you have authentication implemented for requests submitted under various other protocols and want to add authentication for IFP requests.

The Authentication Server (Time/IP-based Session) library rule set contains an embedded rule set with rules that check whether there is already an authenticated session for a client that a request is received from. Otherwise a rule redirects a request to the authentication server.

The embedded rule set covers protocols such as HTTP or HTTPS. Using the `Connection.Protocol` property, you can extend the criteria to include the IFP protocol.

**Restrictions for IFP filtering**

When using an IFP proxy for filtering URLs, you should be aware of the following restrictions:

- **Limited use of SafeSearch Enforcer**
  
  When performing IFP filtering, you the SafeSearch Enforcer will only work for filtering search requests that are carried out using Google.
  
  The reason for this is that only Google uses URLs for submitting the search criteria while all other search providers use cookies. However, cookies cannot be processed by the IFP proxy on an appliance.

- **HTTP proxy required for some functions**
  
  An HTTP proxy must be set up in addition to the IFP proxy if you want to do the following:
  
  - Redirect IFP requests that are blocked due to a filtering rule to a blocking page to let a block message appear on the client of the user who sent the request.
  
  - Authenticate users on the appliance by having their credentials verified on the internal authentication server.
  
  - Restrict web usage of users by implementing the Time Quota library rule set.
IFP filtering activities on the dashboard

The dashboard on the user interface provides information on several IFP filtering activities.

- Number of IFP requests processed
  This information is shown under Web Traffic Summary | Requests per protocol.

- Domains that access to was requested most often (counting the number of requests)
  Among these requests can be such that were submitted under the IFP protocol.
  This information is shown under Web Traffic | Top Level Domains by Number of Requests.

- Websites that were most often the destinations of requests (counting the number of requests)
  Among these requests can be such that were submitted under the IFP protocol.
  This information is shown under Web Traffic | Destinations by Number of Requests.

Connection tracing for IFP filtering activities

Connection tracing can be performed for filtering IFP requests.

When connection tracing is enabled, connection tracing files are created and stored. They can be accessed on the user interface under the Troubleshooting top-level menu.

Configure the IFP Proxy settings

You can configure the IFP proxy settings to set up a proxy that enables the processing of requests for web access submitted under this protocol.

Task

1. Select Configuration | Appliances.

2. On the appliances tree, expand the appliance you want to configure the IFP proxy settings for and click Proxies (HTTP(S), FTP, ICAP, and IM).

3. On the settings pane, scroll down to the IFP Proxy section.

4. Configure the settings in this section as needed.

5. Click Save Changes.

IFP Proxy settings

The IFP Proxy settings are used for configuring a proxy that intercepts requests for web access submitted under the IFP protocol and makes them available for URL filtering.

IFP Proxy

Settings for configuring an IFP proxy
Table 11-19  IFP Proxy

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IFP proxy</td>
<td>When selected, an IFP proxy is enabled on an appliance.</td>
</tr>
<tr>
<td>IFP port definition list</td>
<td>Allows you to create a list of ports that listen for IFP requests.</td>
</tr>
<tr>
<td>Maximum number of concurrent IFP</td>
<td>Limits the number of IFP requests that are processed at the same time to</td>
</tr>
<tr>
<td>requests allowed.</td>
<td>the specified value.</td>
</tr>
<tr>
<td></td>
<td>You can use this setting to prevent an overloading of the IFP proxy.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the IFP port definition list.

Table 11-20  IFP Port Definition

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listener address</td>
<td>Specifies the IP address and port number of a port that listens to IFP</td>
</tr>
<tr>
<td></td>
<td>requests.</td>
</tr>
<tr>
<td>Send error message as redirect</td>
<td>When set to true, a user who sent a request is informed, for example, about a blocking of the request, by directing the request to an error message page. Otherwise the relevant information is sent as a normal message under the IFP protocol.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a port that listens to IFP requests.</td>
</tr>
</tbody>
</table>

Create a rule set for filtering IFP requests

You can create a rule set with rules that filter requests for web access submitted under the IFP protocol.

Task


2. In the Name field, enter a suitable name for the rule set, for example Filter IFP Requests.

3. Under Applies to, deselect Responses and Embedded Objects.

4. Under Apply this rule set, select If the following criteria is matched.

5. Configure the rule set criteria.
   a. Under Criteria, click Add and select Advanced criteria. The Add Criteria window opens
   b. From the properties list, select Connection.Protocol.
   c. From the operators list, select equals.
   d. In the input field for operands, type IFP.
   e. Click OK. The Add Criteria window closes and the criteria appears in the Criteria field.

6. Click OK. The Add New Rule Set window closes and the new rule set appears on the rule set tree.
When the rule set has been created, you need to insert rules for URL filtering into it. You can, for example, copy rules from the default URL Filtering rule set and adapt them as needed.

**Modify an authentication rule set to include the IFP protocol**
You can include the IFP protocol in the criteria of an authentication rule set to enable authentication for requests that are submitted under that protocol.

**Task**

1. Import an authentication rule set from the library.
   a. Select Policy | Rule Sets, then click Add and select Top Level Rule Set.
      The Add Top Level Rule Set window opens.
   b. Click Import rule set from Rule Set Library.
      The Add from Rule Set Library window opens.
   c. From the Rule Set Library list, select the Authentication (Time/IP-based Session) rule set.
   d. In the Import conflicts area, select the conflict that is listed and under Conflict Solution choose a conflict-solving strategy.
   e. Click OK.
      The Add from Rule Set Library window closes and the rule set appears on the rule set tree.

2. Expand the rule set and select the embedded Check for Valid Authentication Session rule set.
   The criteria and rules of the embedded rule set appear on the settings pane.

3. Click Edit. The Edit Rule Set window opens.

4. Modify the rule set criteria.
   a. Under Criteria, click Add and select Advanced criteria.
   b. From the properties list, select Connection.Protocol.
   c. From the operators list, select equals.
   d. In the input field for operands, type IFP.
   e. Click OK.
      The Add Criteria window closes and the criteria appears in the Criteria field.
   f. Under Criteria combination remove the closing parenthesis after the letter e and insert one after d.

5. Click OK.
   The Edit Rule Set window closes.

6. Click Save Changes.
Media type filtering

Media type filtering ensures that the users of your network cannot access media that belong to particular types, such as images, audio, or streaming media, when these types are not allowed under your web security policy.

This way you can, for example, prevent your users from consuming too many resources.

The media type filtering process includes several elements, which contribute to it in different ways.

- Filtering rules control the process.
- A blocking list is used by a rule to block access to media that belong to particular types.

A default process for media type filtering is implemented on Web Gateway after the initial setup. You can modify this process to adapt it to the requirements of your web security policy.

To configure media type filtering, you can work with:

- **Key elements of rules** — After clicking the default `Media Type Filtering` rule set on the rule sets tree, you can view and configure key elements of the default rules for the filtering process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can expand the `Media Type Filtering` rule set on the rule sets tree, which lets the nested `Upload Media Types` and `Download Media Types` rule sets appear.

  Clicking either of them lets you view their default rules for the filtering process completely. You can configure all their elements, including the key elements, and also create new rules or delete rules.

  You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

**Filtering rules**

The rules that control the media type filtering process are usually contained in one media type filtering rule set. It can have two nested rule sets with rules for filtering media types that are uploaded to and downloaded from the web.

When the default process is implemented, a rule set for media type filtering with two nested rule sets is included. The name of the nesting rule set is `Media Type Filtering`, those of the nested rule sets are `Upload Media Types` and `Download Media Types`.

A media type filtering rule can use a list of media types. It can also rely on the use of a suitable property in its criteria, such as the `MediaType.IsAudio` or `MediaType.IsVideo` properties.

**Blocking list**

A blocking list is used by a rule for blocking media that belong to particular types. There can be a blocking list for media that should not be uploaded from within your network to the web, as well as one for media that should not be downloaded from the web to your network.
Configure key elements for media type filtering

Configure key elements of the rules for media type filtering to adapt important parts of the filtering process to the requirements of your web security policy.

**Task**
2. On the rule set tree, select the Media Type Filtering rule set.
   - Key elements of the rules for the filtering process appear in the configuration pane.
3. Configure the key elements as needed.
4. Click Save Changes.

**Key elements for media type filtering**
The key elements for media type filtering deal with important parts of this filtering process.

**Block Media Types in Uploads**
Key elements for filtering media that are uploaded to the web

**Table 11-21  Block Media Types in Uploads**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media types to block</td>
<td>Clicking Edit opens a window to let you edit the Upload Media Type Block List that is used by a rule. You can add, modify, and remove entries on the list.</td>
</tr>
</tbody>
</table>

**Block Media Types in Downloads**
Key elements for filtering media that are downloaded from the web

**Table 11-22  Block Media Types in Downloads**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media types to block</td>
<td>Clicking Edit opens a window to let you edit the Download Media Type Block List that is used by a rule. You can add, modify, and remove entries on the list.</td>
</tr>
<tr>
<td>Block undetectable media types</td>
<td>When selected, a rule is enabled that blocks media if no type could be detected for them.</td>
</tr>
<tr>
<td>Block unsupported media types</td>
<td>When selected, a rule is enabled that blocks media if it belongs to a type that cannot be handled on Web Gateway.</td>
</tr>
<tr>
<td>Block multimedia</td>
<td>When selected, a rule is enabled that blocks media if it belongs to the multimedia type.</td>
</tr>
<tr>
<td>Block streaming media</td>
<td>When selected, a rule is enabled that blocks media if it is streaming media.</td>
</tr>
</tbody>
</table>

**Configure media type filtering using the complete rules view**
You can configure media type filtering to adapt this process to the needs of your network.

To configure URL filtering, you can work with the key elements view or the rules view.
Task
1 Review the rules in the rule set for URL filtering.
   By default, this is the URL Filtering rule set.

2 Modify these rules as needed.
   You can, for example, do the following.
   • Enable or disable blocking rules and the whitelist rule
   • Edit the lists used by these rules

   A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.

   • Modify the settings of the URL Filter module

3 Save your changes.

Properties for media type filtering
Most media type filtering rules in the default rule set use the MediaType.EnsuredTypes property in their criteria. Using other properties lets media type filtering be executed in a different way. There is, for example, the MediaType.NotEnsuredTypes property. If you use this property in the criteria of a blocking rule, the rule blocks media whose types are on a block list even if the probability that they actually are of this type is less than 50%.

You could use this property to make sure a media type gets blocked under all circumstances.

The following table lists the properties that are available for rules in media type filtering.

Table 11-23 Media type filtering properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| MediaType.EnsuredTypes    | Property of media that have their types ensured with a probability of more than 50%  
                           | This level of probability is assumed if a media type signature from an internal list on the appliance can be found in the object code of the media. |
| MediaType.NotEnsuredTypes | Property of media for which the probability that they actually are of their respective types is less than 50%                                |
| MediaType.FromFileExtension | Property of media for which types are assumed based on the extensions of the media type file names                                    |
|                           | Extensions and the media types associated with them are looked up in an internal catalog on the appliance. There are, however, extensions that are used by more than one media type. |
| MediaType.FromHeader      | Property of media for which types are assumed according to the content type field of the headers sent with the media                        |
|                           | Headers are read and evaluated in a standardized format. To filter headers in their original formats, you can use the Header.Get property.   |
| MediaType.IsSupported     | Property of embedded or archived media that can be extracted by the opener module of the appliance.                                           |
| List.OfMediaType.IsEmpty  | Property of media with types that are not on an internal list.                                                                               |
Modify a media type filtering rule
You can modify a media type filtering rule to filter a different kind of media types by changing the property in the rule criteria. Then you also need to create a new filter list for use by the modified rule.

Tasks
- Create a filter list for a modified rule on page 366
  You can create a new filter list for use in a modified media type filtering rule.
- Replace a property in a media type filtering rule on page 366
  You can replace the property in the criteria of a media type filtering rule with a different property to let the rule filter a different kind of media types.

Create a filter list for a modified rule
You can create a new filter list for use in a modified media type filtering rule.

Task
1  Select Policy | Lists.
2  On the Custom Lists branch of the lists tree, select Media Type and click Add.
   The Add List window opens.
3  In the Name field, type a name for the new list, for example, Not Ensured Download Media Type Blocklist.
4  [Optional] In the Comment field, type a plain-text comment on the new list.
5  [Optional] Click the Permissions tab and configure who is allowed to access the list.
6  Click OK.
   The Add List window closes and the new list appears on the lists tree under MediaType.
You can now fill the entries for the new list to let the media type filtering rule know what to block or allow.

Replace a property in a media type filtering rule
You can replace the property in the criteria of a media type filtering rule with a different property to let the rule filter a different kind of media types.

Task
1  Select Policy | Rule Sets.
2  On the rule sets tree, select a rule set for media type filtering, for example, the nested Download Media Type rule set in the Media Type Filtering rule set.
3  Select a rule, for example, Block types from Download Media Type Blocklist, and click Edit.
   The Edit Rule window opens with the Name step selected.
4  Click Rule Criteria and under Criteria select the rule. Then click Edit.
   The Edit Criteria window opens.
5 Edit the rule criteria as follows:
   a From the list of properties in the left column, select a new property, for example, MediaType.NotEnsuredTypes (instead of MediaType.EnsuredTypes).
   b From the list of operands in the right column, select Not Ensured Download Media Type Blocklist.
6 Click OK.
   The window closes and the modified criteria appears under Rule Criteria.
7 Click Finish.
   The Edit Rule window closes and the modified rule appears within the nested rule set that you selected.
8 Click Save Changes.

Media Type Filtering rule set
The Media Type Filtering rule set is the default rule set for media type filtering.

<table>
<thead>
<tr>
<th>Library rule set – Media Type Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

The following rule sets are nested in this rule set:

- Upload Media Type
  This rule set is not enabled by default.
- Download Media Type

Upload Media Type
This nested rule set blocks the upload of media belonging to particular media types. It is processed in request cycles when users request to upload media to the web, as well as in embedded object cycles when objects are embedded in media.

<table>
<thead>
<tr>
<th>Nested library rule set – Upload Media Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM) and embedded objects</td>
</tr>
</tbody>
</table>

The rule set contains the following rule:

Block types from list Upload Media Type Blocklist

Media.TypeEnsuredTypes at least one in list Upload Media Type Blocklist -> Block<Media Type (Block List)> — Statistics.Counter.Increment ("BlockedByMediaFilter", 1)<Default>

The rule uses the Media.TypeEnsuredTypes property to check for media that have their type ensured if they are on the specified list. If they are, access to the media type is blocked and processing rules stop.

The rule uses an event to count blocking due to media type filtering. The event parameters specify the counter that is incremented and the size of the increment. The event settings specify the settings of the Statistics module, which executes the counting.

Processing continues with the next request that is received on the appliance.
Download Media Type

This nested rule set blocks the download of media belonging to particular media types. It is processed in response cycles when web servers send media in response to user requests for downloading them, as well as in embedded object cycles when objects are embedded in media.

<table>
<thead>
<tr>
<th>Nested library rule set – Download Media Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Responses and embedded objects</td>
</tr>
</tbody>
</table>

The rule set contains the following rule.

**Block types from list Download Media Type Blocklist**

(`Media.TypeEnsuredTypes at least one in list Download Media Type Blocklist `) `-> Block<Media Type (Block List)>` `— Statistics.Counter.Increment ("BlockedByMediaFilter", 1)`<Default>

The rule uses the `Media.TypeEnsuredTypes` property to check for media that have their type ensured if they are on the specified list. If they are, access to the media type is blocked and processing rules stop.

The rule uses an event to count blocking due to media type filtering. The event parameters specify the counter that is incremented and the size of the increment. The event settings specify the settings of the Statistics module, which executes the counting.

Processing continues with the next request that is received on the appliance.

---

Application filtering

Application filtering ensures that the users of your network cannot access unwanted applications, which could be, for example, Facebook, Xing, and others. The filtering process application names and reputation scores and blocks access accordingly. Filtering can also be applied to individual functions of applications.

The following elements are involved in this process:

- Filtering rules that control the process
- Application lists that are used by rules to block applications
- Application system lists that are updated in intervals

Update status and statistics of the application filtering process are shown on the dashboard.

**Rules for application filtering**

The rules that control application filtering are usually contained in one rule set. They block access to applications and individual functions of applications using the following two methods:

- Block applications and individual functions that are on a list
- Block applications that are assigned a particular risk level

To block applications and individual functions according to a list, the `Application.Name` property is used.

The value of this property is the name of an application or an individual function of an application that appears in a request sent by a user who wants to access the application or application function. If this name is on a blocking list, access is blocked, as, for example, the following rule does it.
Name

**Block applications according to list**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application.Name is in list Unwanted Applications</td>
<td>Block&lt;Application Blocked&gt;</td>
</tr>
</tbody>
</table>

To block applications according to their risk levels, properties, such as Application.IsMediumRisk or Application.IsHighRisk are used, which have true or false as their values.

Risk evaluation is based on the reputation score for an application that is assigned to it by the Global Threat Intelligence system. If the risk for allowing access to an application is considered to be high, it means it has a bad reputation.

If an application reaches or exceeds this level, access to it is blocked, as, for example, the following rule does it.

Name

**Block high-risk applications**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application.IsMediumRisk equals true OR Application.IsHighRisk equals true</td>
<td>Block&lt;Application Blocked&gt;</td>
</tr>
</tbody>
</table>

Both methods rely on the application system lists. Only applications and application functions that are on these lists can appear on a list that is used by an application filtering rule.

The risk levels for applications and application functions are also those that are shown on the application system lists.

For logging purposes, there are the Application.To String and Application.Reputation properties, which are the name of a requested application converted into a string and a numerical value for its reputation score, respectively.

You can use these properties in rules that record information in log file entries.

Application filtering is not performed by default on an appliance. However, you can import the Application Control rule set from the library.

You can then review the rules in this rule set, modify or delete them, and also create your own rules.

**Blocking lists**

Blocking lists are used by rules to block access to applications that are requested by users. The rules in the library rule set include lists that are already filled with several application names.

You can add application names to a list from the library rule set or remove them and also create your own lists. If you add application names, you must take them from the application system list.

In the same way, you can create and edit lists with names of application functions.

**Application system lists**

The applications and application functions that can be blocked by application filtering rules appear on lists, which are provided by the appliance system and updated in intervals.

You can view these lists by expanding the Application Name folder under System Lists on the lists tree of the Lists tab. This folder contains a number of subfolders for different types of applications, for example, File Sharing or Instant Messaging.
A subfolder contains a list of applications, providing the following information for each of them:

- Application name (or application name with application function)
- Comment
  - Risk level
  - Description of the application (or application function)

A function of an application appears in parentheses after the application name, for example, Orkut(Orkut Chat). If you include an application function in the list of a blocking rule, only this function is blocked, not the complete application.

The following is an example of an entry for an application in a system list:

MessengerFX | Risk: Minimal: A web-based instant messaging service

The next example shows an entry for an application function:

Orkut(Orkut Chat) | Risk: High: Allows users to send instant messages.

**Application filtering information on the dashboard**

The dashboard provides the following information on application filtering:

- Update status of the application list
- Statistics on applications and application functions that have actually been blocked

**Configure application filtering**

You can configure application filtering to adapt this process to the needs of your network.

Complete the following high-level steps.

**Task**

1. Import the *Application Control* rule set.

2. Review the rules in this rule set and modify them as needed.
   
   You can, for example, do the following.
   
   - Enable or disable blocking rules
   - Edit the lists used in rules by adding or removing applications
   - Create lists of your own and use them instead of or in addition to the existing lists
   - Change the reputation levels used in rules by replacing the relevant properties, for example, by replacing `Application.IsHighRisk` with `Application.IsMediumRisk`

   You can also create blocking rules of your own.

3. Save your changes.
Create a list for application filtering

You can create a list for use in an application filtering rule and fill it with entries for applications or individual functions of applications that should be blocked.

**Task**

1. Select Policy | Lists and click the Add icon. The Add List window opens.

2. Configure general list settings.
   a. In the Name field, type a name for the list, for example, Unwanted Applications.
   b. From the Type list, select Application Name.
   c. [Optional] Click the Permissions tab and configure who is allowed to access the list.
   d. [Optional] In the Comments field, type a plain-text comment on the list.

3. Click OK. The Add List window closes and the list appears on the list tree under Custom Lists | Application Name.

4. Select the list and, above the settings pane, click the Edit icon. The Edit window opens with a collection of folders that contain application names.

5. Fill the list with entries for applications or individual functions of applications.
   a. Expand a folder that contains an application or application function that name you want to add to the list, for example, Instant Messaging Web Applications.
   b. Select an application or application function, for example, MessengerFX or Orkut(Orkut Chat).

   ![You can select multiple applications or application functions at once, you can select items from multiple folders at once, and you can select complete folders.]

   c. Click OK. The Edit window closes and the selected applications and application functions appear on the list.

   ![You can also add a complete folder and afterwards delete the entries for applications or application functions that you do not want to include.]

6. Click Save Changes.

You can use the list you created in the criteria of an application filtering rule, for example, to let the criteria match if the name of an application or application function that access is requested to appears on the list.

Modify the risk level in an application filtering rule

You can modify the risk level in a rule that filters applications according to the risk they present to web security, for example, from high to medium. This increases web security because a blocking action can then be triggered even if an application is only a medium risk.

**Before you begin**

The following procedure assumes that you have imported the Application Control rule set from the library.
Task
   The Add New Rule Set window opens.
2. Expand the Application Control rule set, then expand the nested Block Applications in Request Cycle rule set.
   The general settings and rules of the nested rule set appear on the settings pane.
3. Make sure Show details is selected.
4. Select the rule Block web applications with high risk and click Edit.
   The Edit Rule window opens.
5. Under Steps, select Rule Criteria and in the Criteria section, select the upper part of the complex criteria (the one that uses the Application.IsHighRisk property), then click Edit.
   The Edit Criteria window opens with the Application.IsHighRisk property selected in the properties list.
6. From the properties list, select Application.IsMediumRisk.
7. Click OK.
   The Edit Criteria window closes and the modified criteria appears in the Criteria section.
8. Click Finish.
   The Edit Rule window closes and the rule with the modified criteria appears on the settings pane.
9. Click Save Changes.

Application Control rule set
The Application Control rule set is a library rule set for application filtering.

<table>
<thead>
<tr>
<th>Library rule set – Application Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses</td>
</tr>
</tbody>
</table>

The following rule sets are nested in this rule set:

- Block Applications in Request Cycle
- Block Applications in Response Cycle

Block Applications in Request Cycle
This nested rule set handles application filtering in the request cycle.

<table>
<thead>
<tr>
<th>Nested library rule set – Block Applications in Request Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycle – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set contains the following rules:

**Block instant messaging applications**

Application.Name is in list Instant Messaging → Block<Default>
The rule uses the `Application.Name` property to check whether the name of an application is contained in a specified list. If it is, it blocks a request for this application.

The action settings specify a message to the requesting user.

The rule is not enabled by default.

**Block web applications with high risk**

```
Application.HighRisk equals true AND Application.Name is in list Web Browsing and Web Conferencing -> Block<Default>
```

The rule uses the `Application.HighRisk` property to check the reputation score of an application and the `Application.Name` property to check whether the name of this application is contained in a specified list. If the reputation score reaches or exceeds the high-risk level and the application name is also on the list, it blocks a request for this application.

The action settings specify a message to the requesting user.

The rule is not enabled by default.

**Block Facebook chat**

```
Application.ToString(Application.Name) equals "Facebook.Chat" -> Block<Default>
```

The rule uses the `Application.ToString` property to check whether the name of an application is equal to a specified string. For this purpose, the name of the application is converted into a string. If the converted application name equals the specified string, a request for the application is blocked.

The action settings specify a message to the requesting user.

The rule is not enabled by default.

**Block Applications in Response Cycle**

This nested rule set handles application filtering in the response cycle.

<table>
<thead>
<tr>
<th>Nested library rule set – Block Applications in Response Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycle – Responses</td>
</tr>
</tbody>
</table>

The rule set contains the following rule:

**Applications to be looked for in response cycle**

```
Application.Name is in list of Applications to Search for in Response Cycle -> Block<Default>
```

The rule uses the `Application.Name` property to check whether the name of an application is contained in a specified list. If it is, it blocks a request for this application.

The action settings specify a message to the requesting user.

The rule is not enabled by default.

**Block web applications with high risk**

```
Application.HighRisk equals true AND Application.Name is in list Web Browsing and Web Conferencing -> Block<Default>
```

The rule uses the `Application.HighRisk` property to check the reputation score of an application and the `Application.Name` property to check whether the name of this application is contained in a specified list. If the reputation score reaches or exceeds the high-risk level and the application name is also on the list, it blocks a request for this application.

The action settings specify a message to the requesting user.

**Block Facebook chat**

```
Application.ToString(Application.Name) equals "Facebook.Chat" -> Block<Default>
```

The rule uses the `Application.ToString` property to check whether the name of a application is equal to a specified string. For this purpose, the name of the application is converted into a string. If the converted application name equals the specified string, a request for the application is blocked.

The action settings specify a message to the requesting user.

The rule is not enabled by default.
The rule uses the *Application.To String* property to check whether the name of an application is equal to a specified string. For this purpose, the name of the application is converted into a string. If the converted application name equals the specified string, a request for the application is blocked.

The action settings specify a message to the requesting user.

The rule is not enabled by default.

---

**Streaming media filtering**

Streaming media filtering ensures that web objects of this media type are detected when they are received on Web Gateway and handled according the configured rules.

When virus and malware filtering is implemented on Web Gateway, web objects that are sent to it are scanned for infections. To achieve a comprehensive scanning result, the web object needs to be scanned completely.

However, streaming media is never "complete", so if the usual scanning method is applied to it, it will not deliver a result, as it would for other, non-streaming media.

Processing streaming media would also be delayed endlessly, as the scanning process would never finish.

This means that once a web object has been detected to be streaming media, you can block it to prevent the users of your network from accessing web objects that have not been scanned for infections.

Or you let streaming media skip virus and malware scanning and allow your users to access media of this type unscanned.

The following elements on Web Gateway are involved in the filtering process:

- Filtering rules that control the process
- A module that calculates the probability for web objects that they are streaming media

  The module sets the value of a suitable property to *true* if the probability for a web object to be streaming media reaches or exceeds a configured value.

Streaming media filtering is usually applied in the response cycle of the filtering process to deal with streaming media sent by web servers in response to user requests.

**Rules for streaming media detection**

To block or allow web objects that are streaming media with a given probability you can set up a rule that uses the *StreamDetector.IsMediaStream* property.

If the value of this property is true, access to a web object would be blocked by the following rule.

**Name**

**Block access to streaming media**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>StreamDetector.IsMediaStream</em>&lt;Streaming Detection&gt; equals true</td>
<td>Block&lt;Streaming Media Blocked&gt;</td>
</tr>
</tbody>
</table>
It would be allowed by the following rule:

Name

**Allow access to streaming media**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>StreamDetector.IsMediaStream&lt;Streaming Detection&gt;</code> equals true</td>
<td>–&gt; Continue</td>
</tr>
</tbody>
</table>

The value of the `StreamDetector.IsMediaStream` property is provided by the Stream Detector module.

Streaming media filtering is not performed by default on Web Gateway. If you want to have it done, you need to create a rule like the ones described above.

We recommend to use this rule not in a rule set of its own, but to insert it into another, suitable rule set, for example, in a media type filtering rule set.

The default Gateway Anti-Malware rule set contains a rule that lets streaming media skip virus and malware filtering. In this rule set, the skipping rule is placed before the rule that lets web object be scanned by the Anti-Malware scanning module.

**Additional properties for streaming media filtering**

When the `StreamDetector.IsMediaStream` property is set to true, two additional properties are given related values. The value of the `StreamDetector.Probability` property is the percentage that was actually calculated for a web object, for example, 60 or 70.

The value of the `StreamDetector.MatchedRule` property is the name of the rule that matched.

You can use these additional properties in rules that record information in log file entries.

**Module for streaming media detection**

The probability that web objects are streaming media is calculated by the *Stream Detector* module (also known as *filter* or *engine*), which uses information about URL categories, content-type headers, source IP addresses, and other items for its calculation. The result of a probability calculation is a percentage.

The types of streaming media that can be detected in this way include the following:

- Flash-based video
- IC9 streams
- MS WMSP
- RealMedia
- MP3 streams

You can configure settings for this module and name them, for example, *Streaming Media Detection*. The settings include the minimum probability that must be reached for a web object to be considered as streaming media.

**Configure streaming media filtering**

You can configure streaming media filtering to adapt this process to the needs of your network. Complete the following high-level steps.
**Task**

1. Create a streaming media filtering rule that blocks web objects if the probability that they are streaming media reaches or exceeds a configured level.

2. Insert this rule in a suitable rule set, for example, in a media type filtering rule set.
   - You can modify the rule later on by increasing or reducing the probability level. This is done by configuring the settings of the Stream Detector module.

3. Save your changes.

**Configure the streaming media detection module**

You can configure the module that calculates the streaming media probability for a given web object to adapt it to the requirements of your network.

**Task**

1. Select Policy | Settings.

2. Select Stream Detector and click Add.
   - The Add Settings window opens.

3. In the Name input field, type a name for the settings.

4. [Optional] In the Comment input field, type a comment on the settings.

5. [Optional] Click the Permissions tab and configure who is allowed to access the settings.

6. Under Streaming Detector, configure settings for the module as needed.

7. Click Save Changes.

**Best practices - Configuring the Stream Detector**

Configuring the Stream Detector, you can set up a way to handle streaming media. The recommended way is to perform a special kind of scanning when the Stream Detector has found that a web object belongs to this media type.

Virus and malware filtering on Web Gateway usually requires that web objects are completely downloaded and scanned by the Anti-Malware module (also known as engine or filter). However, as completeness can never be achieved for streaming media, the usual scanning method will not deliver results, but delay processing of this media type endlessly.

Streaming media must therefore be handled in a special way. Two components on Web Gateway are available for this:

- The Stream Detector detects that a web object is streaming media.
- The Media Stream Scanner scans streaming media chunk-by-chunk.

Compared to the usual method, the Media Stream Scanner performs a less intensive way of scanning.

Following the progress made by the Media Stream Scanner, streaming media is also delivered chunk-by-chunk to the client that a download request was received from. If an infection is detected in a chunk, the process is stopped, and this chunk and the rest of the streaming media are not delivered.

The Stream Detector is a separate module on Web Gateway, not a part of the Anti-Malware module like the Media Stream Scanner.
A suitable rule calls both components to perform their jobs. It is contained in the default Gateway Anti-Malware rule set.

However, the rule is not available in older versions of McAfee Web Gateway. So we recommend that you do the following:

- Inspect your rule set system.
- If the rule is not included in the default Gateway Anti-Malware rule set or any other rule set you are using for virus and malware filtering, configure the rule in one of these rule sets.

Make sure you place it immediately before the rule that triggers the usual anti-malware scanning.

**Rule for streaming media filtering**

The default rule for streaming media filtering looks as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Start Media Stream Scanner on streaming media and skip anti-malware scanning</th>
</tr>
</thead>
</table>

**Criteria**

<table>
<thead>
<tr>
<th>Cycle.Name equals &quot;Response&quot; AND</th>
</tr>
</thead>
<tbody>
<tr>
<td>StreamDetector.IsMediaStream&lt;Default Streaming Detection&gt; equals true</td>
</tr>
</tbody>
</table>

**Action**

- Stop Ruleset – Enable Media Stream Scanner

In the default Gateway Anti-Malware rule set, this rule is placed immediately before the rule that triggers the usual anti-malware scanning.

When the Stream Detector finds that a web object is streaming media, the rule stops processing for this rule set and starts the Media Stream Scanner, so the special way of scanning streaming media is performed and the rule for the usual scanning is skipped.

The criteria part that uses the Cycle.Name property ensures that the rule only applies in the response cycle of processing when web objects are received on Web Gateway from the web, in response to a request that was forwarded.

**Settings for the Stream Detector**

The settings for the Stream Detector module can be accessed on the settings tree under Stream Detector. The name of the default settings is Default Streaming Detection.

The default settings include only the following option:

**Minimal probability** — Sets the probability of being streaming media that is sufficient for treating a web object as streaming media.

- The probability is measured in percent and configured as a number from 1 to 100.
- The probability is found by the Stream Detector. If the minimal probability is reached, the StreamDetector.IsMediaStream property, which is used in the default rule for streaming media filtering, is set to true.
- The default minimal probability is 60. We recommend that you leave this value unchanged.
Stream Detector settings
The Stream Detector settings are used to configure the module that calculates the probability for web objects that they are streaming media.

Streaming Detector
Setting for the module that calculates streaming media probabilities

Table 11-24  Streaming Detector

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal probability</td>
<td>Sets the probability (in percent, specified by a number from 0 to 100) that is sufficient for a web object to be considered as streaming media.</td>
</tr>
</tbody>
</table>

Global whitelisting
Global whitelisting ensures that all further filtering is skipped for the web objects that are whitelisted, so access to them cannot be blocked.

The global whitelisting process includes several elements, which contribute to it in different ways.

- Filtering rules control the process.
- Whitelists are used by rules to let some web objects skip further filtering.

A default process for global whitelisting is implemented on Web Gateway after the initial setup. You can modify this process to adapt it to the requirements of your web security policy.

To configure global whitelisting, you can work with:

- **Key elements of rules** — After clicking the default Global Whitelist rule set on the rule sets tree, you can view and configure key elements of the default rules for the filtering process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the default rules for the filtering process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

  You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

Filtering rules
The rules that control global whitelisting are usually contained in one rule set.

Whitelisting rules are placed and processed in this rule set. If any of them applies, the following rule sets are skipped and no further filtering is performed for the whitelisted objects.

You can review these rules, modify or delete them, and also create your own rules.

When the default rule set system is implemented, a rule set for global whitelisting is included. Its name is Global Whitelist.

Whitelists
Whitelists are used by whitelisting rules to let particular web objects skip further filtering. There can be whitelists for URLs, media types, and other types of objects.
You can add entries to these lists or remove entries. You can also create your own lists and let them be used by the whitelisting rules.

**Configure global whitelisting**

You can configure global whitelisting to adapt this process to the needs of your network.

Complete the following high-level steps.

**Task**

1. Review the rules in the rule set for global whitelisting. By default, this is the *Global Whitelisting* rule set.

2. Modify these rules as needed. You can, for example, do the following:
   - Enable or disable whitelisting rules
   - Edit the lists used by the whitelisting rules

   A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.
   
   • Create whitelists of your own and let them be used by the whitelisting rules

3. Save your changes.

**Global Whitelist rule set**

The Global Whitelist rule set is the default rule set for global whitelisting.

<table>
<thead>
<tr>
<th>Default rule set – Global Whitelist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>Always</em></td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.

**Client IP is in list Allowed Clients**

*Client.IP is in list Allowed Clients* --> Stop Cycle

The rule uses the *Client.IP* property to check whether the IP address of a client that a request was sent from is on the specified whitelist.

If it is, the rule applies and stops the current processing cycle. The request is then forwarded to the appropriate web server.

**URL.Host matches in list Global Whitelist**

*URL.Host matches in list Global Whitelist* --> Stop Cycle

The rule uses the *URL.Host* property to check whether the host that a URL sent in a request provides access to is on the specified whitelist.

If it is, the rule applies and stops the current processing cycle. The request is then forwarded to the web server that is the requested host.
SSL scanning

SSL scanning ensures that SSL-secured web traffic can be processed and made available to other filtering functions. The SSL scanning process includes several elements, which contribute to this in different ways.

- SSL scanning rules control the process.
- Whitelists and other lists that are used by the rules to let web objects skip SSL scanning and to perform other functions within the process.
- SSL scanning modules, which are called by the rules, perform certificate verification and other functions within the process.

To configure SSL scanning, you can work with:

- **Key elements of rules** — After clicking the default SSL Scanner rule set on the rule sets tree, you can view and configure key elements of the default rules for the filtering process.

  To configure SSL scanning, you can work with:

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the default rules for the filtering process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

  You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

SSL scanning rules

The rules that control SSL scanning are usually contained in one rule set that has several nested rule sets. Each of the nested rule sets controls a particular function of the SSL scanning process:

- **Handle the CONNECT call** — There is a rule set with rules for handling the CONNECT call, which is sent at the beginning of SSL-secured communication under the HTTPS protocol.

- **Verify certificates** — There are rule sets for verifying certificates that are submitted by clients and servers in SSL-secured communication, for example, by verifying the common names in these certificates.

  This part of the process allows verification for both explicit proxy and transparent setups.

- **Enable content inspection** — Another rule set contains rules for enabling the inspection of content that is transferred in SSL-secured communication.

To find out whether an object is infected, the rule calls the Anti-Malware module, which scans the object and lets the rule know about the result.

Whitelisting rules can be placed and processed in this rule set before the blocking rule. If any of them applies, the blocking rule is skipped and the whitelisted objects are not scanned.

You can review the rules that are implemented on the appliance for SSL scanning, modify or delete them, and also create your own rules.

When the default rule set system is implemented, a rule set for SSL scanning is included. Its name is SSL Scanner. However, the rule set is not enabled initially.

Whitelists and other lists for SSL scanning

Whitelists are used by the SSL scanning rules to let web objects skip parts of the process. For example, a certificate whitelist exempts certificates from undergoing verification.
Other lists used in SSL scanning contain the port numbers that are allowed in CONNECT calls if these are to be accepted or the servers that require a special kind of certificate verification because a particular method of exchanging keys cannot be applied on them.

You can add entries to these lists or remove entries. You can also create your own lists and let them be used by the SSL scanning rules.

**Modules for SSL scanning**

The following modules (also known as engines) are called by the SSL scanning rules to perform different parts of the SSL scanning process:

- **SSL Scanner** — Handles certificate verification or the enabling of content inspection, depending on the settings it runs with.

  Accordingly, the module is called by the rules for certificate verification and content inspection with different settings.

- **Modules for setting the client context** — Handle the submitting of a certificate for the appliance to the clients that send requests to it in SSL-secured communication.

  When this certificate is submitted, the certificate authority (CA) that issued the certificate can be sent with it or not. Accordingly, there is a module for submitting a certificate with and another module for submitting a certificate without its certificate authority.

  The SSL Scanner rule set of the default system, uses the method of submitting a certificate with its certificate authority.

  A default certificate authority is available for use after the initial setup. However, we recommend that you provide a certificate authority of your own for further use.

- **Certificate Chain** — Handles the building of a certificate chain

  When building the chain, the module uses a list of certificate authorities for the certificates that are included in the chain. You can add certificate authorities to existing lists and also add new lists.

**Configure SSL scanning**

You can configure SSL scanning to adapt this process to the needs of your network. Complete the following high-level steps.

**Task**

1. Enable the rule set for SSL scanning and review the rules in this rule set.

   By default, this is the **SSL Scanner** rule set.

2. Modify these rules as needed.

   You can, for example, do the following:

   - Replace the default root certificate authority (CA) for signing certificates that the appliance sends to its clients by a certificate of your own.

     This can be a certificate authority that you create yourself on the user interface or one that you import from your file system.

   - Enable or disable whitelisting rules, for example:

     - The default rule for skipping certificate verification when a certificate that was submitted by a client is on a whitelist
     - The default for skipping content inspection when the host of a requested URL is on a whitelist
• Edit the lists used by the whitelisting rules
  
  A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.

• Create whitelists of your own and let them be used by the whitelisting rules

• Modify the settings of the modules involved in SSL scanning.
  • SSL Scanner module
  • SSL Client Context module
  • Certificate Chain module

3 Save your changes.

**Configure the modules for SSL scanning**

You can configure the modules for SSL scanning to modify the way SSL-secured web traffic is processed.

The following modules are involved in SSL scanning and can be configured:

• SSL Scanner module
• SSL Client Context module
• Certificate Chain module

**Task**

1 Select **Policy | Rule Sets**.

2 On the rule sets tree, find the rule set for SSL scanning.
   
   By default, this is the **SSL Scanner** rule set.

3 Expand the rule set and select the nested rule set that contains the rule with the settings for the module you want to configure.

   For example, to configure the SSL Scanner module, expand the nested **Handle CONNECT Call** rule set. It contains by default the rule **Enable certificate verification** with the **Default certificate verification** settings for the SSL Scanner module.

   The rules of the nested rule set appear on the settings pane.

4 Make sure **Show details** is selected.

5 Find the rule with the settings for the module you want to configure.

   This could be, for example, the **Enable certificate verification** rule that was mentioned above.

6 Within the rule, click a settings name.

   For example, in the rule event of **Enable certificate verification**, click **Default certificate verification**.

   The **Edit Settings** window opens. It provides the settings for a module, for example, the SSL Scanner module.

7 Configure these settings as needed.

8 Click **OK** to close the window.

9 Click **Save Changes**.
Replace the default root certificate authority
You can replace the default root certificate authority that is provided after the initial setup for signing the certificates that the appliance sends to its clients by a certificate authority of your own. You can create a new root certificate authority on the user interface or import one from your file system.

Tasks
- Create a root certificate authority on page 383
  You can create a root certificate authority (CA) for signing the certificates the appliance sends to its clients and use it instead of the default certificate authority.
- Import a root certificate authority on page 383
  You can import a root certificate authority (CA) for signing the certificates the appliance sends to its clients and use it instead of the default certificate authority.

Create a root certificate authority
You can create a root certificate authority (CA) for signing the certificates the appliance sends to its clients and use it instead of the default certificate authority.

Task
1. Select Policy | Settings.

2. On the Engines branch of the settings tree, go to SSL Client Context with CA and select the settings you want to use the new certificate authority for.

3. Click Generate New.
   The Generate New Certificate Authority window opens.

4. In the Organization and Locality fields, type suitable information for your own certificate authority.

5. [Optional] In the Organizational unit and State fields, type suitable information. From the Country list, select a country.

6. In the Common name field, type a common name for your own certificate authority.

7. [Optional] In the Email address field, type an email address of your organization.

8. From the Valid for list, select the time that your certificate authority should be valid.

9. [Optional] In the Comment field, type a plain-text comment on the certificate authority.

10. Click OK.
    The new certificate authority is generated.

11. Click Save Changes.

Import a root certificate authority
You can import a root certificate authority (CA) for signing the certificates the appliance sends to its clients and use it instead of the default certificate authority.

Task
1. Select Policy | Settings.

2. On the settings tree, select SSL Client Context with CA and click the settings you want to use the imported certificate authority for.
3 Click Import.

The Import Certificate Authority window opens.

4 Enter the name of the certificate authority file in the Certificate field by clicking Browse and browsing to a suitable file.

The file must be encoded in PEM (Privacy-enhanced mail) format.

5 Enter the name of the certificate key file in the Private key field by clicking Browse and browsing to a suitable file.

The file must be encoded in PEM format. The key must have a length of at least 2048 bit.

6 [Conditional] If the private key is protected by a password, type it in the Password field.

Only unencrypted keys and key that are AES-128-bit encrypted can be used here.

7 [Conditional] If the certificate authority is part of a certificate chain and you want to provide information on this chain with the certificate, enter the name of the file containing the information in the Certificate chain field by clicking Browse and browsing to a suitable file.

The file must be encoded in PEM format.

8 Click OK.

The certificate authority is imported.

9 Click Save Changes.

**Client certificate list**

The client certificate list is a list of certificates that can be sent to a web server when a client request is received on an appliance in SSL-secured communication and passed on to the appropriate web server.

The certificate is sent when the web server asks for it at the initial and subsequent handshakes, as SSL renegotiation is performed.

A rule event tells the appliance to use a client certificate for communication with the web server. The certificate can then be selected from the client certificate list.

In this case, the private key for the certificate must be provided by the client that sent the request.

Alternatively, a preconfigured certificate can be used that is always sent to the web server.

The rule event that triggers the use of a certificate from the client certificate list can belong to rules that apply to CONNECT requests (even in transparent setups) or to rules in rule sets for certificate verification that have CERTVERIFY as value for the Command.Name property in their criteria.

You can configure settings for the rule event that include a client certificate list and the instruction to use it. The settings can also specify that the private key for the certificates that the clients of the appliance provide is stored unencrypted.
Create a client certificate list
You can create a list of client certificates that can be sent to web servers in SSL-secured communication.

Task
1. Select Policy | Settings.
2. On the settings tree, select SSL Client Certificate Handling and click Add.
   The Add Settings window opens with the Add Settings tab selected.
3. Configure general settings parameters.
   a. In the Name field, type a name for the settings.
   b. [Optional] In the Comments field, type a plain-text comment on the settings.
   c. [Optional] Click the Permissions tab and configure who is allowed to access the settings.
4. Under Client Certificate Handling, make sure the option Use client certificate from Known client certificates list if client has proven ownership is selected.
5. On the toolbar of the Known client certificates list, click Add.
   The Add Client Certificate window opens.
6. Click Import to import a client certificate.
   The Import Client Certificate window opens.
7. Import a client certificate.
   a. Next to the Certificate field, click Browse, and within the local file manager that opens, browse to a suitable certificate file and select it.
      The file manager closes and the certificate file name appears in the field.
   b. Next to the Private key field, click Browse, and within the local file manager that opens, browse to a suitable key file and select it.
      The file manager closes and the key file name and password appear in the Private key and Password fields.
   c. Click OK.
      The window closes and the certificate file information appears in the Import Client Certificate window.
   d. [Optional] In the Comments field, type a plain-text comment on the certificate.
8. Click OK.
   The Add Client Certificate window closes and the certificate file name and comment (if provided) appear in the Known client certificates list.
   Repeat Steps 5 to 8 for any other certificate you want to add to the list.
9. Click OK to close the Add Settings window.
10. Click Save Changes.
**SSL Client Certificate Handling settings**
The SSL Client Certificate Handling settings are used for configuring client certificates that are sent to web servers in SSL-secured communication.

**SSL Client Certificate Handling**
Settings for configuring SSL client certificates

**Table 11-25  SSL Client Certificate Handling**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use client certificate from Known client certificates list if client has proven ownership</td>
<td>When selected, the client certificate that is sent to a web server in SSL-secured communication is taken from the list of known client certificates. However, the certificate is only taken from this list if it is proven that the client whose request the appliance forwards to a server is the owner of this certificate. After selecting this radio button, the Known Client Certificates section appears, which provides settings for configuring a list of certificates.</td>
</tr>
<tr>
<td>Always use predefined client certificate</td>
<td>When selected, the same client certificate is always sent to a web server in SSL-secured communication. After selecting this radio button, the Predefined Client Certificate section appears, which provides settings for configuring a single certificate.</td>
</tr>
</tbody>
</table>

**Known client certificates**
Settings for configuring a list of known client certificates that can be sent to a web server

**Table 11-26  Known client certificates**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of known client certificates</td>
<td>Provides a list of client certificates that can be sent to a web server in SSL-secured communication.</td>
</tr>
</tbody>
</table>

The following table describes the elements of an entry in the list of known client certificates.

**Table 11-27  Known client certificates – List entry**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>Specifies the name of a client certificate.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a certificate.</td>
</tr>
</tbody>
</table>

**Predefined client certificate**
Settings for configuring a client certificate that is always sent to a web server

**Table 11-28  Predefined client certificate**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject, Issuer, Validity, Extensions</td>
<td>Provides information on the client certificate that is currently used for sending to a web server.</td>
</tr>
<tr>
<td>Import</td>
<td>Opens the Import Client Certificate window for importing a client certificate. After the import, information on the client certificate appears under Subject, Issuer, and in the other information fields.</td>
</tr>
<tr>
<td>Export</td>
<td>Opens your local file manager to let you store a client certificate in a suitable location.</td>
</tr>
</tbody>
</table>
Table 11-28  Predefined client certificate (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Key</td>
<td>Opens your local file manager to let you store the private key for a client certificate in a suitable location.</td>
</tr>
<tr>
<td>Certificate Chain</td>
<td>Displays a certificate chain if one has been imported with a client certificate.</td>
</tr>
</tbody>
</table>

SSL Scanner settings

The SSL Scanner settings are used for configuring the way certificates are verified and content inspection is enabled for SSL-secured web traffic.

Enable SSL Scanner

Settings for configuring certificate verification or the enabling of content inspection

Table 11-29  Enable SSL Scanner

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL scanner function</td>
<td>Selects the function that is performed by the SSL Scanner module.</td>
</tr>
<tr>
<td>• Certificate verification</td>
<td>— When selected, the module verifies certificates submitted in SSL-secured communication.</td>
</tr>
<tr>
<td>• SSL inspection</td>
<td>— When selected, the module inspects the content of web objects transmitted in SSL-secured communication.</td>
</tr>
<tr>
<td>SSL protocol version</td>
<td>When selected, the module inspects the content of web objects transmitted in SSL-secured communication.</td>
</tr>
<tr>
<td>• TLS 1.0</td>
<td>— When selected, TLS (Transport Layer Security) version 1.0 is used.</td>
</tr>
<tr>
<td>• SSL 3.0</td>
<td>— When selected, SSL version 3.0 is used .</td>
</tr>
<tr>
<td>Server cipher list</td>
<td>Specifies a string of Open SSL symbols used for decrypting server data.</td>
</tr>
<tr>
<td></td>
<td>The SSL Scanner module uses different strings for default certificate verification and for verifying certificates from servers that do not support the EDH (Ephemeral Diffie-Hellman) method.</td>
</tr>
<tr>
<td>SSL session cache TTL</td>
<td>Limits the time (in seconds) for keeping the parameter values of a session in SSL-secured communication stored in the cache to the specified value.</td>
</tr>
<tr>
<td>Allow handshake and renegotiation with servers that do not implement RFC 5746</td>
<td>When selected, the SSL Scanner module performs these activities also in communication with web servers that fail to comply with the specified standard.</td>
</tr>
</tbody>
</table>

Allow Alternative Handshakes

Settings for handshakes in SSL-secured communication that use alternative parameter values
Table 11-30  Allow Alternative Handshakes

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use alternative handshake settings after handshake failure</td>
<td>When selected, the SSL Scanner module uses alternative parameter values after the first attempt to perform a handshake in SSL-secured communication has failed.</td>
</tr>
<tr>
<td>SSL protocol version</td>
<td>Selects the version of the protocol the SSL Scanner module follows when it performs an alternative handshake.</td>
</tr>
<tr>
<td>• TLS 1.0</td>
<td>When selected, TLS (Transport Layer Security) version 1.0 is used</td>
</tr>
<tr>
<td>• SSL 3.0</td>
<td>When selected, SSL version 3.0 is used</td>
</tr>
<tr>
<td>Server cipher list</td>
<td>Specifies a string of Open SSL symbols used for decrypting server data.</td>
</tr>
<tr>
<td></td>
<td>The SSL Scanner module uses different strings for default certificate verification and for verifying certificates from servers that do not support the EDH (Ephemeral Diffie-Hellman) method.</td>
</tr>
</tbody>
</table>

SSL Client Context with CA settings

The SSL Client Context with CA settings are used to configure the sending of certificates with information about the certificate authority to the clients of a Web Gateway appliance.

Define SSL Client Context (Certificate Authority)

Settings for sending a certificate to the clients with information about the certificate authority
### Table 11-31 Define SSL Client Context (Certificate Authority)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| (Current certificate and default root certificate authority) | Under **Subject**, **Issuer**, and other field names, information about the certificate is provided that is currently sent to the clients of an appliance in SSL-secured communication.  
Information is also provided about the root certificate authority (root CA) that signed this certificate.  
After the initial setup, the certificate is signed by the default root certificate authority. This certificate authority is McAfee.  
The certificate is therefore called a self-signed certificate, as McAfee signed a certificate for one of their own products. Self-signed certificates are not trusted by all partners in SSL-secured communication.  
For further administration of the SSL functions on Web Gateway, we recommend that you create your own root certificate authority.  
Use the **Generate New** option to create this certificate authority. |
| Certificate Authority | Provides several options for performing activities that are related to a certificate authority.  
- **Generate New** — Opens a window for generating a new certificate authority.  
- **Import** — Opens a window for importing a certificate authority.  
The window provides an option for importing a file with information about a certificate authority and the certificate that was signed by it.  
Additionally, you can include a file with information about the chain of certificate authorities that were involved in the validation process.  
The file with information about the certificate chain can be a file that you created and stored in the file system before.  
In this case, the file will contain information about the following:  
  - The certificate that an appliance sends as server to its clients  
  - The intermediate certificate authorities, one of which signed the certificate, while the others each validated another certificate authority  
  - The root certificate authority, which is the first instance that validated another certificate authority  
When importing a certificate chain file, you must make sure that it only contains information about the intermediate certificate authorities.  
All other information must be removed from the file. Otherwise the import will fail.  
- **Export** — Lets you browse to a location within your file system that you can export a certificate authority file to.  
- **Export key** — Lets you browse to a location within your file system that you can export the key file for a certificate authority to. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Send certificate chain      | When selected, the appliance sends information on the chain of certificates and certificate authorities that were involved in the process of validating a certificate with this certificate to its clients.  
To retrieve this information, you must include the certificate chain when using the option for importing a certificate authority.  
The appliance sends the certificate that is configured here as a server to its clients. The certificate is therefore also referred to as the server certificate.  
The server certificate is considered to exist on level 0. When a certificate authority signs this certificate to validate it, it is done on level 1.  
When an additional certificate authority validates the first certificate authority, it is done on level 2. With each additional certificate authority that is involved, the level increases by one. |
| Certificate chain           | Provides information on a certificate chain.  
After importing a certificate authority file with information about the certificate chain, the information appears in this field. |
SSL Client Context without CA settings

The SSL Client Context without CA settings are used to configure the sending of certificates with no information about the certificate authority to the clients of a Web Gateway appliance.

Define SSL Client Context (Without Certificate Authority)

Settings for sending a certificate to the clients with no information about the certificate authority

| Table 11-32 Define SSL Client Context (Without Certificate Authority) |
|--------------------|-------------------|
| **Option**         | **Definition**    |
| Select server certificate by host or IP | Provides a list of certificates that are sent to the clients and the host systems that they have been retrieved from. A host system is identified by a host name or an IP address. The certificates are sent from an appliance in its role as a server to the clients. The certificates are therefore referred to as server certificates. |

| Table 11-33 Select server certificate by host or IP — List entry |
|--------------------|-------------------|
| **Option**         | **Definition**    |
| Host               | Specifies the host name or IP address of the host system that a certificate is retrieved from. |
| Server Certificate | Provides information on the certificate that is currently sent from an appliance in its role as a server to its clients. When adding an entry for a new certificate to the list, you can generate or import the certificate. Options for performing these activities are provided in the window for adding a list entry under Server Certificate. |
| • Generate         | Opens a window for generating a new certificate. |
| • Import           | Opens a window for importing a certificate. The window provides an option for importing a file with information about a certificate. Additionally, you can include a file with information about the chain of certificate authorities that were involved in the validation process. |
| The file with information about the certificate chain can be a file that you created and stored in the file system before. In this case, the file will contain information about the following: |
| • The certificate that an appliance sends as server to its clients |
| • The intermediate certificate authorities, one of which signed the certificate, while the others each validated another certificate authority |
| • The root certificate authority, which is the first instance that validated another certificate authority |
| When importing a certificate chain file, you must make sure that it only contains information about the intermediate certificate authorities. All other information must be removed from the file. Otherwise the import will fail. |
| • Export | Lets you browse to a location within your file system that you can export a certificate authority file to. |
| • Export key | Lets you browse to a location within your file system that you can export the key file for a certificate authority to. |
**Table 11-33  Select server certificate by host or IP — List entry (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSM</td>
<td>Provides information on a Hardware Security Module that is used to protect the certificate information.</td>
</tr>
<tr>
<td>Certificate chain</td>
<td>Provides information on the chain of certificates and certificate authorities that were involved in the validation of the certificate that is sent to the clients.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a certificate.</td>
</tr>
</tbody>
</table>

**Table 11-34  Define SSL Client Context (Without Certificate Authority) — Continued**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Scanner functionality applies only to client connection</td>
<td>When selected, traffic is only processed using the SSL scanning functions on the connection from an appliance to its clients.</td>
</tr>
<tr>
<td>Client cipher list</td>
<td>Specifies a string of Open SSL symbols used for decrypting client data.</td>
</tr>
<tr>
<td>SSL session cache TTL</td>
<td>Limits the time (in seconds) that SSL session parameters are stored in the cache.</td>
</tr>
<tr>
<td>Perform insecure renegotations</td>
<td>When selected, Web Gateway renegotiates the parameters for the SSL-secured communication even if this is insecure to do.</td>
</tr>
<tr>
<td>Send empty plain-text fragment</td>
<td>When selected, an empty plain-text fragment is sent with the certificate to the clients.</td>
</tr>
<tr>
<td>SSL protocol version</td>
<td>Selects the version of the protocol that the SSL Scanner module follows when dealing with handshakes.</td>
</tr>
<tr>
<td>• TLS 1.2</td>
<td>When selected, TLS (Transport Layer Security) version 1.2 is used.</td>
</tr>
<tr>
<td>• TLS 1.1</td>
<td>When selected, TLS (Transport Layer Security) version 1.1 is used.</td>
</tr>
<tr>
<td>• TLS 1.0</td>
<td>When selected, TLS (Transport Layer Security) version 1.0 is used.</td>
</tr>
<tr>
<td>• SSL 3.0</td>
<td>When selected, SSL version 3.0 is used.</td>
</tr>
</tbody>
</table>

**Certificate Chain settings**

The Certificate Chain settings are used for configuring the module that handles the building of certificate chains.

**Certificate Verification**

Settings for building a chain of certificates

**Table 11-35  Certificate Verification**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of certificate authorities</td>
<td>Provides a list for selecting a list of certificate authorities (CAs) that sign the certificates in a certificate chain.</td>
</tr>
</tbody>
</table>

The following table describes the elements of a list entry

**Table 11-36  List of certificate authorities**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate authority</td>
<td>Specifies the name of a certificate authority.</td>
</tr>
<tr>
<td>Certificate revocation list</td>
<td>Specifies the list providing information on when a certificate signed by this certificate authority becomes invalid and the URI used to access the list.</td>
</tr>
</tbody>
</table>
Table 11-36  List of certificate authorities (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>When selected, a certificate authority is trusted on the appliance.</td>
</tr>
<tr>
<td>Comment</td>
<td>Plain-text comment on a certificate authority</td>
</tr>
</tbody>
</table>

**SSL Scanner rule set**

The SSL Scanner rule set is the default rule set for SSL scanning.

<table>
<thead>
<tr>
<th>Default rule set – SSL Scanner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The following rule sets are nested in this rule set:

- Handle CONNECT Call
- Certificate Verification
  - Verify Common Name (proxy setup)
- Content Inspection
- Verify Common Name (transparent setup)

**Handle CONNECT Call**

This nested rule set handles the CONNECT call in SSL-secured communication and enables certificate verification.

<table>
<thead>
<tr>
<th>Nested library rule set – Handle CONNECT Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Command.Name equals “CONNECT”</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a request is received on the appliance that contains the CONNECT command, which is sent in the opening phase of SSL-secured communication.

The rule set contains the following rules:

**Set client context**

*Always –> Continue – Enable SSL Client Context with CA <Default CA>*

The rule enables the use of a server certificate that is sent to a client.

The event settings specify the McAfee Web Gateway root certificate authority (CA), which is implemented on the appliance after the initial setup, as the default issuer of this certificate.

The Continue action lets processing continue with the next rule.

**Tunneled hosts**

*URL.Host is in list SSL Host Tunnel List –> Stop Cycle*

The rule lets requests for access to hosts with a URL that is on the specified whitelist skip SSL scanning.

**Restrict destination ports to Allowed CONNECT Ports**

*URL.Port is not in list Allowed Connect Ports –> Block<Connect not allowed>*
The rule blocks requests with destination ports that are not on the list of allowed CONNECT ports.

The action settings specify a message to the requesting user.

**Enable certificate verification without EDH for hosts in no-EDH server list**

URL.Host is in list No-EDH server –> Block<Connect not allowed> Stop Rule Set – Enable SSL Scanner<Certificate Verification without edh>

The rule enables the certificate verification for requests sent from a host on the no-EDH (Ephemeral Diffie-Hellman) server list.

The action settings specify a message to the requesting user.

The event settings specify running in verification mode for the SSL Scanner module and a special cipher string for data encryption on non-EDH hosts.

**Enable certificate verification**

Always –> Stop Rule Set – Enable SSL Scanner<Default certificate verification>

The rule enables certificate verification.

The event settings specify that the SSL Scanner module runs in verification mode.

**Certificate Verification**

This nested rule set handles the CERTVERIFY call in SSL-secured communication. It lets whitelisted certificates skip verification and blocks others according to particular criteria.

<table>
<thead>
<tr>
<th>Nested library rule set – Certificate Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Command.Name equals &quot;CERTVERIFY*&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule criteria specifies that the rule set applies if a request is received on the appliance that contains the CERTVERIFY command, which is sent to request the verification of a certificate.

The following rule set is nested in this rule set:

- Verify Common Name (proxy setup)

The rule set contains the following rules:

**Skip verification for certificates found in Certificate Whitelist**

SSL.Server.Certificate.HostAndCertificate is in list Certificate Whitelist –> Stop Rule Set

The rule lets whitelisted certificates skip verification.

**Block self-signed certificates**

SSL.Server.Certificate.SelfSigned equals true –> Block <Certificate incident>

The rule blocks requests with self-signed certificates.

The action settings specify a message to the requesting user.

**Block expired server (7 day tolerance) and expired CA certificates**

SSL.Server.Certificate.DaysExpired greater than 7 OR
SSL.Server.CertificateChain.ContainsExpiredCA<Default> equals true –> Block <Certificate incident>

The rule blocks requests with expired server and CA certificates.

The action settings specify a message to the requesting user.
Block too long certificate chains

SSLServer.CertificateChain.PathLengthExceeded<Default> equals true -> Block <Certificate incident>
The rule blocks a certificate chain if it exceeds the path length.
The settings in the property specify a list for the module that checks the certificate authorities.
The action settings specify a message to the requesting user.

Block revoked certificates

SSLServer.CertificateChain.ContainsRevoked<Default> equals true -> Block <Certificate incident>
The rule blocks a certificate chain if one of the included certificates has been revoked.
The settings in the property specify a list for the module that checks the certificate authorities.
The action settings specify a message to the requesting user.

Block unknown certificate authorities

SSLServer.CertificateChain.FoundKnownCA<Default> equals false -> Block <Certificate incident>
The rule blocks a certificate chain if none of the certificate authorities (CAs) issuing the included certificates is a known CA.
The settings in the property specify a list for the module that checks the certificate authorities.
The action settings specify a message to the requesting user.

Block untrusted certificate authorities

SSLServer.FirstKnownCAIsTrusted<Default> equals false -> Block <Certificate incident>
The rule blocks a certificate chain if the first known CA that was found is not trusted.
The settings in the property specify a list for the module that checks the certificate authorities.
The action settings specify a message to the requesting user.

Verify Common Name (proxy setup)

This nested rule set verifies the common name in a certificate. It applies to requests sent in explicit proxy mode.

<table>
<thead>
<tr>
<th>Nested library rule set – Verify Common Name (proxy setup)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Connection.SSL.TransparentCNHandling equals false</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule criteria specifies that the rule set applies if a request is received on a connection used in SSL-secured communication and verification of the common name is not performed in transparent mode.

The rule set contains the following rules:

Allow matching hostname

URL.Host equals Certificate.SSL.CN -> Stop Rule Set
The rule allows a request if the URL of the requested host is the same as the common name in the certificate.

Allow wildcard certificates

Certificate.SSL.CN.HasWildcards equals true AND URL.Host matches.Certificate.SSL.CN.ToRegex(Certificate.SSL.CN) -> Stop Rule Set
The rule allows requests to hosts sending certificates that have wildcards in their common names matching the URLs of the hosts.

To verify that a common name containing wildcards matches a host, this name is converted into a regular expression.

**Allow alternative common names**

URL.Host is in list Certificate.SSL.AlternativeCNs → Stop Rule Set

The rule allows requests to hosts with alternative common names in their certificates if the host matches at least one of them.

**Block incident**

Always → Block <Common name mismatch>

If any of the rules for allowing matching common names applies, processing of the rule set stops and this rule is not processed. Otherwise, requests are blocked by this rule because it is then a common name mismatch.

The action settings specify a message to the requesting user.

**Content Inspection**

This nested rule set completes the handling of a CERTVERIFY call. It lets some requests skip content inspection according to particular criteria and enables inspection for all others.

<table>
<thead>
<tr>
<th>Nested library rule set – Content Inspection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Command.Name equals &quot;CERTVERIFY*&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule criteria specifies that the rule set applies if a request is received on the appliance that contains the CERTVERIFY command, which is sent to request the verification of a certificate.

The rule set contains the following rules:

**Skip content inspection for hosts found in SSL Inspection Whitelist**

Connection.SSL.Transparent equals false AND URL.Host matches in list SSL Inspection Whitelist → Stop Rule Set

The rule lets requests sent to whitelisted hosts skip content inspection. It applies only in non-transparent mode.

**Skip content inspection for CN found in SSL Inspection Whitelist**

Connection.SSL.Transparent equals true AND Certificate.SSL.CN matches in list SSL Inspection Whitelist → Stop Rule Set

The rule lets requests with whitelisted common names in their certificates skip content inspection. It applies only in transparent mode.

The rule is not enabled initially.

**Do not inspect connections with client certificates**

Connection.Client.CertificateIsRequested equals true → Stop Rule Set

The rule lets requests skip inspection if they require the use of client certificates.

The rule is not enabled initially.

**Enable content inspection**

Always → Continue – Enable SSL Scanner<Enable content inspection>

The rule enables content inspection.
The event settings specify that the SSL Scanner module runs in inspection mode. If any of the rules for skipping content inspection applies, processing of the rule set stops and this last rule, which enables the inspection, is not processed. Otherwise, content inspection is enabled by this rule.

**Verify Common Name (transparent setup)**

This nested rule set verifies the common name in a certificate. It applies to requests sent in explicit proxy mode. It applies only to requests sent in transparent mode.

With requests sent in explicit proxy mode, the host name that is compared to the common name is taken from the CONNECT request that a client sends.

As in transparent mode no CONNECT request is sent, the host name is taken from the request for web access that a client sends.

<table>
<thead>
<tr>
<th>Nested library rule set – Verify Common Name (transparent setup)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong> –</td>
</tr>
<tr>
<td><strong>Cycles</strong> –</td>
</tr>
</tbody>
</table>

The rule criteria specifies that the rule set applies if a request is received on a connection used in SSL-secured communication and verification of the common name is performed in transparent mode.

The rule set contains the following rules:

**Allow matching hostname**

\[URL.Host equals Certificate.SSL.CN \rightarrow Stop Rule Set\]

The rule allows a request if the URL of the requested host is the same as the common name in the certificate.

**Allow wildcard certificates**

\[Certificate.SSL.CN.HasWildcards equals true AND URL.Host matches.Certificate.SSL.CN.ToRegex(Certificate.SSL.CN) \rightarrow Stop Rule Set\]

The rule allows requests to hosts sending certificates that have wildcards in their common names matching the URLs of the hosts.

To verify that a common name containing wildcards matches a host, this name is converted into a regular expression.

**Allow alternative common names**

\[URL.Host is in list Certificate.SSL.AlternativeCNs \rightarrow Stop Rule Set\]

The rule allows requests to hosts with alternative common names in their certificates if the host matches at least one of them.

**Block incident**

\[Always \rightarrow Block <Common name mismatch>\]

If any of the rules for allowing matching common names applies, processing of the rule set stops and this rule is not processed. Otherwise, requests are blocked by this rule because it is then a common name mismatch.

The action settings specify a message to the requesting user.
Use of a Hardware Security Module (HSM) enhances security when dealing with private keys for the certificates that are sent to servers and clients in SSL-secured communication.

Keys for SSL-certificates can be public or private. If you are using private keys and do not want to expose them, you can store them on a Hardware Security Module, which is a separate hardware component that is installed on a Web Gateway appliance.

When a certificate is imported and a private key is needed for enabling its use, the key is referenced by its ID (also known as *key name*) while remaining protected on the hardware component.

This method of key handling provides greater security than storing private keys in a file within your file system, as this file might easily be opened and read.

### Installing and accessing a Hardware Security Module

A Hardware Security Module is made available on a PCI card, which is installed together with the appropriate drivers on an appliance that Web Gateway runs on.

When the module card is installed, you can access the module by logging on to the appliance from a system console. To perform activities on the module, such as generating keys or unlocking them, you enter suitable commands in the command line.

For more information on how to install a Hardware Security Module card and perform activities on the module, see the documentation of the McAfee partner who provides the module (Thales).

### Key handling on a Hardware Security Module

All cryptographic operations related to using a private key for a certificate are performed on the Hardware Security Module.

Keys can be generated on the module, but can also be imported to it. To be available on Web Gateway they are loaded by the HSM Agent, which is a component of the Web Gateway appliance system.

To enable the loading of keys, you must make the key ID known to the agent by adding it in string format to a list on the user interface of Web Gateway.

Communication with the agent is handled by the *HSM server*, which is set up on a Web Gateway appliance that has a Hardware Security Module installed. The setup is configured on the user interface of Web Gateway.

Generating private keys usually includes the use of passwords or an Operator Card System (OCS) to create additional security. Keys can also be generated, however, without any of these additional options. If a key is protected by a password or OCS, you must unlock it before you can use it, which is done on the Hardware Security Module.

### Using a private key on a Hardware Security Module for a certificate

The user interface of Web Gateway provides options for importing a certificate as part of several settings. When an HSM server is configured, selecting a private key for the certificate from a Hardware Security Module is included within these options.

To make the key available for the certificate, it is referenced by its ID, which can be selected from a list.
Extended use of a Hardware Security Module

Use of a Hardware Security Module on a Web Gateway appliance can be extended as follows.

- **Using a Hardware Security Module remotely** — A Hardware Security Module can be used by other Web Gateway appliances within your network that have no module installed.

  An HSM server is configured on the appliance that has the module installed. Appliances that have no modules installed are configured as the clients of this server, which enables them to connect to the server and load private keys. This configuration is performed on the user interface of Web Gateway.

- **Generating a private key for a root certificate** — Your company can set up a security infrastructure, which includes a root certificate authority for use throughout the company. The root certificate authority on Web Gateway can be configured as an intermediate certificate authority that is subordinate to the company-wide root certificate authority.

  A certificate issued by the company-wide root certificate authority is then created for the intermediate certificate authority on Web Gateway. The private key for this certificate is generated on the Hardware Security Module.

  For more information, see *Working with a security infrastructure* in this document.

Administrator responsibilities in key handling

To enhance security in key handling, responsibilities can be assigned to different administrators.

For example, one administrator might be responsible for generating private keys on a Hardware Security Module, while the Web Gateway administrator uses the keys when configuring certificates on the user interface of Web Gateway.

The Web Gateway administrator must be sure to know the key IDs that were generated, as well as the key passwords that might additionally have been set.

Logging key operations

Key operations involving the Hardware Security Module are logged on Web Gateway and displayed on the dashboard of its user interface under SSL Scanner Statistics as **Remote Private Key Operations**.

Use a Hardware Security Module for key handling

To enhance security for the private keys of the certificates used in SSL-secured communication, you can work with a Hardware Security Module. You can generate keys on the module, store them, and perform other activities.

The following steps can be in the responsibility of different administrators.

**Task**

1. Prepare a Web Gateway appliance for running a Hardware Security Module, which is made available on a PCI card.
   
   a. Install the PCI card with the Hardware Security Module on the appliance.
   
   b. From a system console, install the drivers for the Hardware Security Module.

   For more information about how to install the PCI card, see the *McAfee Web Gateway Installation Guide*. 

   McAfee Web Gateway 7.6.0  Product Guide  399
For more information about installing the module drivers, see the documentation of the McAfee partner who provides the module (Thales).

2 From a system console, create a Security World and (optionally) an Operator Card Set for the keys on the Hardware Security Module. Then generate keys or import them and remember the key IDs. For more information about creating these items, see the documentation of the McAfee partner who provides the module (Thales).

3 On the user interface of Web Gateway, configure one of the following use options:
   - Local use of the module
     Set up an HSM server for local use on an appliance that has a Hardware Security Module installed.
   - Remote use of the module
     - Set up an HSM server for local use on an appliance that has a Hardware Security Module installed. Then allow remote use of the module for the clients of this server.
     - Configure the appliances that have no module installed, but are to use it remotely, as HSM clients.

4 From a system console, unlock the keys on the Hardware Security Module that are protected by a password or an Operator Card Set.
   For more information about unlocking keys, see the documentation of the McAfee partner who provides the module (Thales).

You can now select keys when importing certificates on the user interface of Web Gateway.

See also
Configure local use of a Hardware Security Module on page 400
Configure remote use of a Hardware Security Module on page 401
Select a private key on a Hardware Security Module on page 401

Configure local use of a Hardware Security Module
You can configure local use of a Hardware Security Module to let it only be used on the appliance that has the module installed.

Task
1 Select Configuration | Appliances.
2 On the appliances tree, select the appliance you want to configure local use of the module for, then click Hardware Security Module.
3 Under HSM Server, select Start local HSM server.
4 In the Keys to be loaded list, add entries for the keys that you want to be available for loading.
   For each key, enter its key ID in string format.
5 Click Save Changes.

See also
Hardware Security Module settings on page 403
Configure remote use of a Hardware Security Module

Configure remote use of a Hardware Security Module to make it available to appliances within your network that have no module installed.

**Task**

1. Select Configuration | Appliances.

2. On the appliances tree, select the appliance with the module that you want to configure remote use for, then click Hardware Security Module.

3. Configure an HSM server on this appliance.
   a. Under HSM Server, select Start local HSM server.
   b. In the Keys to be loaded list, add entries for the keys that you want to be available for loading.
      For each key, enter its key ID in string format.
   c. Click Allow remote connections.
   d. In the HSM server port definition list, add one or more ports that listen to client requests.
   e. Under Server identification, generate or import a certificate for the server. Then export it to a location where you can import it from when configuring the clients.

4. For each appliance that you want to configure as an HSM client:
   a. On the appliances tree, select an appliance that has no module installed, then click Hardware Security Module.
   b. Under HSM Client, select Use remote HSM server.
   c. In the Remote server list, add an entry for the HSM server.
      Enter host name and listener port and import the server certificate.
   d. Under Client identification, generate or import a certificate for the client. Then export it to a location where you can import it from when configuring the list of permitted clients.

5. Under HSM Server, add an entry for each HSM client to the Permitted clients list.
   Enter the host name and import the client certificate.

6. Click Save Changes.

Select a private key on a Hardware Security Module

To select a private key on a Hardware Security Module for a certificate, reference the key by selecting its ID from a list.

Private keys on a Hardware Security Module can be used when importing certificates as part of the configuration activities for settings that are related to filtering SSL-secured communication. These settings include:

- SSL Client Certificate Handling
- SSL Client Context with CA
- SSL Client Context without CA

The following sample procedure uses a private key for importing a certificate within the SSL Client Context with CA settings.
Task
1 Select Policy | Settings.

2 On the Engines branch of the settings tree, expand SSL Client Context with CA, and select the Default CA settings.

3 Under Define SSL Client Context, click Import next to Certificate Authority.
   The Import Certificate Authority window opens.

4 Click Browse next to Certificate, then locate and import a certificate file.

5 Select HSM next to Private key source.
   A list with the IDs for the available keys opens.

6 Select a key ID, then click Import to import the certificate with its key information.

7 Click Save Changes.

Working with a security infrastructure
You can work with a security infrastructure that exists within your company to generate a certificate for the root certificate authority on Web Gateway. The private key for this certificate is retrieved from a Hardware Security Module.
Many companies have a security infrastructure that provides elements, such as certificate and keys, for use in SSL-secured communication. This infrastructure usually includes a root certificate authority for company-wide use.

With regard to the public keys that are usually included in a security infrastructure, this structure or a part of it is sometimes referred to as PKI (Public Key Infrastructure).

The root certificate authority on Web Gateway can be configured as an intermediate authority under the company-wide root certificate authority. A certificate issued by the company-wide root certificate authority is required for this configuration.

To create this certificate, a certificate signing request is submitted to Web Gateway from a system console. The request also specifies a private key on the Hardware Security Module that is installed on Web Gateway.

Create a certificate using a security infrastructure
You can have a certificate issued by a company-wide root certificate authority within a security infrastructure and use it as the certificate for the root certificate authority on Web Gateway.

Task
1 Generate a private key for the certificate on the Hardware Security Module and remember the key ID.
   For more information about how to generate a key, see the documentation of the McAfee partner who provides the module (Thales).
2 Use a certificate signing request to generate a certificate for the root certificate authority on Web Gateway.
   
a On a system console that is connected to a Web Gateway appliance, log on as root administrator.
   
b Run the following openssl command. For `<key ID>`, specify the ID of the key that you generated in step 1.

   ```bash
   openssl req -engine chil -keyform engine -new -sha256 -key <key ID> -out mwg.csr
   ```

   The command delivers a file with the certificate as its output. The file name and extension are mwg.csr, as specified in the command.

2 Store the certificate file within your file system.

You can now import the stored certificate when configuring a root certificate authority for Web Gateway within the settings for filtering SSL-secured communication.

**Hardware Security Module settings**

The Hardware Security Module settings are used to configure the handling of certificate keys on a local or remote Hardware Security Module.

**HSM Server**

Settings for a Hardware Security Module on the Web Gateway appliance that you are currently configuring

**Table 11-37  HSM Server**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start local HSM server</td>
<td>When selected, a Hardware Security Module is run on this appliance for storing and loading keys.</td>
</tr>
<tr>
<td></td>
<td>The module is provided on a server that other Web Gateway appliances in your network can connect to as clients to load the keys that are stored on the module.</td>
</tr>
<tr>
<td>Keys to be loaded</td>
<td>Provides a list of the key IDs for the keys that are stored on the Hardware Security Module and can be loaded for use with a certificate.</td>
</tr>
<tr>
<td></td>
<td>For each key that you want to use on Web Gateway, you need to add the key ID in string format to this list.</td>
</tr>
</tbody>
</table>

The key IDs become known when keys are generated or imported on the Hardware Security Module.

The following table describes an entry in the key list.

**Table 11-38  Keys to be loaded – List entry**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Specifies the key ID for a key that is stored on the Hardware Security Module.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a key.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow local connections</td>
<td>When selected, the keys that are stored on this Hardware Security Module can be used for connections that are set up on this appliance.</td>
</tr>
<tr>
<td>Allow remote connections</td>
<td>When selected, the keys that are stored on this Hardware Security Module can be used remotely for connections that are set up by other Web Gateway appliances within your network. If you select this option, you need to specify the ports of the HSM server on this appliance that are available for remote connections.</td>
</tr>
<tr>
<td>HSM server port definition list</td>
<td>Provides a list of the ports on the HSM server.</td>
</tr>
<tr>
<td>Permitted clients</td>
<td>Provides a list of other appliances in your network that can run as clients of the HSM server and use the Hardware Security Module for loading keys.</td>
</tr>
</tbody>
</table>

The following tables describe the entries in the list of HSM server ports and the permitted clients list.

**Table 11-39 HSM server port definition list – List entry**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listener address</td>
<td>IP address and port number of a port on the HSM server that listens to requests for setting up a remote connection.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a port.</td>
</tr>
</tbody>
</table>

**Table 11-40 Permitted clients – List entry**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Specifies the host name or IP address of a Web Gateway appliance in your network that is permitted to load the keys that are stored on the Hardware Security Module on this appliance.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Provides a certificate that a client submits when connecting to the HSM server.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a permitted client.</td>
</tr>
</tbody>
</table>

**Server Identification**

Settings for the certificate that the HSM server submits when connecting to its clients

A certificate issued by the McAfee root CA is provided by default for the HSM server after the initial setup of a Web Gateway appliance. We recommend that you replace this certificate by a certificate of your own.

**Table 11-41 Server Identification**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject, Issuer, Validity, Extensions, Private key</td>
<td>Provide information on the certificate that is currently in use.</td>
</tr>
</tbody>
</table>
| Server certificate             | Provides buttons for performing various activities with regard to a server certificate:  
  • Generating a certificate  
  • Importing a certificate  
  • Exporting a certificate  
  • Exporting a certificate key                                                                                                                                                                                                                                                                                                                                                                                 |
HSM Client

Settings for configuring the use of a Hardware Security Module that resides on another Web Gateway appliance in your network

Table 11-42  HSM Server

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use remote HSM server</td>
<td>When selected, this appliance uses the keys that are stored on a Hardware Security Module that resides on another Web Gateway appliance in your network. The module is provided on a server that this appliance can connect to as a client. If you select this option, you need to specify a server or multiple servers in a list.</td>
</tr>
<tr>
<td>Remote server</td>
<td>Provides a list of other Web Gateway appliances in your network running a Hardware Security Module on a server that this appliance can connect to as a client.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the list of remote servers.

Table 11-43  Remote server – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Specifies the host name or IP address of a Web Gateway appliance in your network that runs a Hardware Security Module on a server.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Certificate that the server submits when connecting to a client.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a remote server.</td>
</tr>
</tbody>
</table>

Client Identification

Settings for the certificate that this appliance submits when connecting as a client to an HSM server

A certificate issued by the McAfee root CA is provided by default for this client after the initial setup of a Web Gateway appliance.

We recommend that you replace this certificate by a certificate of your own.

Table 11-44  Server Identification

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject, Issuer, Validity, Extensions, Private key</td>
<td>Provide information on the certificate that is currently in use.</td>
</tr>
<tr>
<td>Client certificate</td>
<td>Provides buttons for performing various activities with regard to a client certificate:</td>
</tr>
<tr>
<td></td>
<td>• Generating a certificate</td>
</tr>
<tr>
<td></td>
<td>• Importing a certificate</td>
</tr>
<tr>
<td></td>
<td>• Exporting a certificate</td>
</tr>
<tr>
<td></td>
<td>• Exporting a certificate key</td>
</tr>
</tbody>
</table>
Advanced Threat Defense

After a web object has been scanned by Web Gateway for infections by viruses or other malware, it can additionally be scanned by the McAfee® Advanced Threat Defense (Advanced Threat Defense) web security product.

Advanced Threat Defense uses a sandboxing approach for scanning, which means that the behavior of a particular web object in a "sandbox" environment is analyzed. The scanning result is recorded in a report and delivered to Web Gateway.

The additional scanning performed by Advanced Threat Defense is also referred to as offline scanning or background scanning.

To enable the use of Advanced Threat Defense, suitable rules must be implemented on Web Gateway. You can import rule sets that contain such rules from the rule set library.

To configure the use of Advanced Threat Defense on Web Gateway, you can work with:

- **Key elements of rules** — After importing the library rule sets for the use of Advanced Threat Defense and clicking them on the rule sets tree, you can view and configure key elements of the rules for the additional scanning process.

- **Complete rules** — After clicking Unlock View in the key elements view, you can view the rules for the additional scanning process completely, configure all their elements, including the key elements, and also create new rules or delete rules.

You cannot return from this view to the key elements view unless you discard all changes or re-import the rule set.

Options for configuring the use of Advanced Threat Defense

You can configure different options to implement an additional scanning by Advanced Threat Defense.

- **Forwarding a web object depending on the additional scanning** — When this option is configured, the result of the additional scanning by Advanced Threat Defense determines whether a web object is forwarded to the user who requested it.

  If a web object is found to be safe, it is forwarded, otherwise not.

- **Forwarding a web object before the additional scanning** — When this option is configured, a web object is forwarded to the user who requested it before the additional scanning by Advanced Threat Defense.

  If a web object is found to be infected, a warning message is sent to the administrator of the network that the user sent his request from.

You can also configure that a web object is not scanned a second time by Advanced Threat Defense if it has been scanned before. In this case, the existing report that was produced after the first scanning is evaluated once again.

Availability of Advanced Threat Defense

For use with Web Gateway, the Advanced Threat Defense web security software is delivered pre-installed on the same hardware platform, where it runs as an appliance on a separate server.

Several instances of the product can also run on different servers and be used to support Web Gateway. Each instance of the product must be installed on its own hardware platform.
Workflows for using Advanced Threat Defense

Different workflows can be configured when Advanced Threat Defense is used to perform an additional scanning of web objects.

Forwarding a web object depending on the additional scanning

The following diagram shows the workflow that forwards a web object to a user depending on the scanning result of Advanced Threat Defense.

![Diagram of workflow](image)

**Figure 11-1  Web object is forwarded depending on additional scanning result**

1. A user sends a request to access a web object, for example, a file, from a system within your network that is a client of Web Gateway.

2. If the request passes filtering according to the configured rules, Web Gateway forwards it to the appropriate web server.
   
   A progress page is sent to the client, telling the user to wait while the request is processed.

3. The web server sends the object to Web Gateway.

4. If the criteria for using Advanced Threat Defense are met, Web Gateway passes the object on for scanning.
   
   To retrieve information on the scanning progress, Web Gateway queries Advanced Threat Defense in regular intervals.

5. When Advanced Threat Defense has completed the scanning, it lets Web Gateway know whether the object is malicious or not.

6. Depending on this information, Web Gateway allows the user to access the requested object or sends a block page, which states that access is blocked and gives a reason for the blocking.
Criteria for additional scanning by Advanced Threat Defense

Web Gateway uses the functions of Advanced Threat Defense for scanning a web object after the object has been scanned by the anti-malware engines on Web Gateway.

The Advanced Threat Defense library rule set uses this probability in its criteria. The default value that must be reached for the criteria to match is 60. This means that only if scanning a web object on Web Gateway results in a malware probability of 60 percent or more, is it passed on to Advanced Threat Defense.

When configuring the use of Advanced Threat Defense, you can increase or lower this value and, consequently, let this product support Web Gateway more or less frequently.

It is therefore important that, on the rule sets tree, the rule set for Advanced Threat Defense is placed behind the rule set for the normal anti-malware functions on Web Gateway, which is usually the Gateway Anti-Malware default rule set.

The Anti-Malware module (or engine) runs with two different settings, when Web Gateway and Advanced Threat Defense work together: one for the Web Gateway part and one for the part of the supporting product.

The default names of the two settings are Gateway Anti-Malware and Gateway ATD.

One important point in which the settings differ from each other is that the Gateway ATD settings have the option for using Advanced Threat Defense selected, whereas this option is deselected in the other settings.

Configuration elements for using Advanced Threat Defense

To enable the additional scanning of web objects by Advanced Threat Defense, suitable rules must be implemented on Web Gateway. You can import rule sets that contain such rules from the rule set library. After importing this rule set, a list and settings are also implemented.

Rule sets for the additional scanning

There is a rule set for forwarding a web object depending on the additional scanning, as well as a rule set for forwarding a web object before the additional scanning and delivering any warning information afterwards.

- **Advanced Threat Defense library rule set** — This rule set implements the workflow that lets a web object additionally be scanned by Advanced Threat Defense and forwarded to the user depending on the scanning result.

  After importing this rule set, a list and settings are also implemented.
• **ATD - Init Offline Scan nested library rule set** — This nested rule set has the same criteria as the rule set that forwards a web object to the user depending on the result of the additional scanning.

The rule set applies if previous scanning by Web Gateway has resulted in a configured degree of probability that a web object is infected, the web object is on the list of web objects that can be scanned, and a particular object size is not exceeded.

The rule set contains only one rule that uses the `Antimalware.MATD.InitBackgroundScan` property in its criteria. The value of this property is `true` by default.

In this case, data for the current transaction is recorded. This includes all data that is related to a request for web access and the response to it from a web server, such as the IP address of the client, authentication information, the URL of the web server, and the requested web object that was sent as the body of the response message.

An internal request is sent to initiate scanning by Advanced Threat Defense. After this has been completed, the requested web object is forwarded to the user while the scanning is performed later on, using the data that was recorded.

If the value of the `Antimalware.MATD.InitBackgroundScan` property is `false`, scanning by Advanced Threat Defense could not be initiated and a rule event is used to display an error message.

• **ATD - Handle Offline Scan nested library rule set** — This nested rule set has the `Antimalware.MATD.IsBackgroundScan` property for its criteria. The value of this criteria is `true` by default.

In this case, the data that was recorded by the rule in the `ATD - Init Offline Scan` rule set, is used by Advanced Threat Defense to scan the web object specified by the data.

The rule set has a rule that uses an event to increase a counter if a scanned web object has been found to be infected, a rule that uses another event to create and send a message about the infected web object to the administrator, and finally a rule that stops the processing cycle.

**List and settings for the additional scanning**

The *Advanced Threat Defense* library rule set provides rules for enabling the use of Advanced Threat Defense on Web Gateway and forwarding a requested web object to the user depending on the scanning result.

After importing this rule set, a list and settings are also implemented.

• **Advanced Threat Defense Supported Types list** — This list is used within the criteria of the library rule set. Only web objects belonging to the media types on this list are passed on to Advanced Threat Defense for scanning.

The list contains several media types by default. You can add media types to the list or remove them.

• **Gateway ATD settings** — These are settings for the Anti-Malware module (or *engine*) on Web Gateway, which handles virus and malware filtering, including the additional use of Advanced Threat Defense.
The settings include mainly options for configuring the following:

• Communication between Web Gateway and the server that Advanced Threat Defense runs on

• Severity grade that lets a web object, for example, a file, be classified as malicious

  When an object is scanned by Advanced Threat Defense, the result is a severity grade on a scale from 0 to 5 (very high severity).

  You can set a value on this scale, for example, 3, which means all objects with a scanning result of 3 or higher are considered to be malicious.

  For these objects, the Antimalware.Infected property is set to true, so a rule that uses this property in its criteria will block a web object and prevent it from being passed on to the user who requested access to it.

**Using an existing Advanced Threat Defense scanning report**

A report that is generated by Advanced Threat Defense after scanning a web object can be used by Web Gateway to evaluate this object and handle access to it.

When using an existing report, Web Gateway will not trigger a new scanning run on Advanced Threat Defense. If more than one report exists, the latest report is used for evaluation. Hash values are calculated internally on Web Gateway to determine whether a web object is the same as another object, so the same report can be used.

To use an existing scanning report on Web Gateway, you need to implement a rule with the Antimalware.ATD.GetReport property. If the value of this Boolean property is true, it means that a particular web object has been found to have already been scanned by Advanced Threat Defense and a report for this scan has been retrieved.

This report can be made available to other rules, for example, to a rule with the Antimalware.Infected property, which evaluates the report to find out whether an object is infected.

**Options for using an existing scanning report**

There are several options for using an existing scanning report to handle access to web objects.

• **Allow a file when a scanning report shows that it is not infected** — There are files that are uploaded manually to Advanced Threat Defense where they are scanned and a report is generated. Web Gateway then allows users to download such a file if a report exists for it and this report shows that the file is not infected.

  If a scanning report does not exist for a web object, the Antimalware.ATD.GetReport property can still be used in suitable rules. In these rules, the value of this property is false, as no scanning report was retrieved.

• **Allow a file if no scanning report is available and scan this file offline** — If no scanning report exists for a file that was requested for downloading, a rule can allow a user to download the file and let an offline scan be performed. After the scanning, a report is generated and forwarded to the administrator of the user's network.

• **Block a file if no scanning report is available and scan this file offline** — If no scanning report exists for a file that was requested for downloading, a rule can block access to the file and let an offline scan be performed. After the scanning, a report is generated and forwarded to the administrator of the user's network.
**Sample rules for using an existing scanning report**

There is no preconfigured rule set for using an existing Advanced Threat Defense scanning report in the default rule set system or the rule set library. You can, however, create suitable rules and a rule set for them on your own.

The following sample rules implement the solution that lets files be uploaded manually to Advanced Threat Defense. Downloading a file is allowed if the report that was generated by Advanced Threat Defense shows that the file is not infected.

The name of the rule set might be *Use Existing Advanced Threat Defense Scanning Report*. It must have the same criteria regarding media types as the *Advanced Threat Defense* library rule set and apply for all processing cycles.

The rule set should contain the following rules:

- A rule that uses the `Antimalware.ATD.GetReport` property to retrieve an existing scanning report
- A rule that evaluates files using this report and blocks access if the report shows that they are infected

The rule that retrieves the report might look as follows:

Name

**Allow files that have been scanned before**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Antimalware.ATD.GetReport</code></td>
<td><code>Block</code></td>
<td><code>Statistics.Counter.Increment&quot;(BlockedByMATD&quot;,1)&quot;&lt;Default&gt;</code></td>
</tr>
<tr>
<td><code>equals false</code></td>
<td><code>&lt;BlockedByMATD&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

The rule blocks access to a file if no report exists for it. In this case, the next rule is not processed. This rule evaluates a report. It might look as follows:

Name

**Block infected files**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Antimalware.Infected</code></td>
<td><code>Block</code></td>
<td><code>Statistics.Counter.Increment&quot;(BlockedByMATD&quot;,1)&quot;&lt;Default&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Gateway ATD&gt;</code> <code>equals true</code></td>
<td><code>&lt;BlockedByMATD&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

In both rules, a counter records how often files were blocked when Advanced Threat Defense functions were used.

**Using an ongoing Advanced Threat Defense scanning run**

While a scanning run is being performed by Advanced Threat Defense, the results of this run can be used not only for processing the request that it was started for, but also for other requests to access the same web object.

To let the results of one scanning run be used for processing multiple requests, the requests must be received on Web Gateway while the scanning is still going on. Hash values are calculated internally on Web Gateway to determine whether a web object is the same as another object, so it can be decided whether requests for the same object are received.

To use the results of one scanning run for multiple requests to access the same object, you need to enable an option within the *Gateway ATD* settings for the Anti-Malware module (or engine) must be enabled. The name of this option is *Re-use running task if same sample is being analyzed*. 
There is no preconfigured rule set in the default rule set system or the rule set library for using the results of one scanning run when multiple requests for the same object are received. You can, however, create suitable rules and a rule set for them on your own.

**Limiting object sizes for scanning by Advanced Threat Defense**

The size of objects that are additionally scanned by Advanced Threat Defense must be checked to comply the size limits that exist for this product.

There are some restrictions for Advanced Threat Defense with regard to the size of web objects that can be scanned. The general size limit is 125 MB, which means that web objects of any type must not exceed this limit.

Other size limits exist for particular types of web objects. For example, the size limit for archives is 10 MB.

For more information about existing size limits and ways to change these limits for particular types of web objects, see the *McAfee Advanced Threat Defense Product Guide*.

**Configuring size limits on Web Gateway**

On Web Gateway, you can configure rules that block web objects of different types if they exceed a particular size limit. By inserting these rules in a rule set for handling Advanced Threat Defense scanning activities, you can make sure that only web objects with suitable sizes are passed on to Advanced Threat Defense.

If you have imported the library rule sets for Advanced Threat Defense, you can insert the size limit rules there. Some of these rule sets contain a rule for uploading web objects to Advanced Threat Defense.

By inserting the size limit rules before this rule, web objects that exceed the size limits are blocked and the rule for uploading to Advanced Threat Defense is not executed.

**Rule for setting a size limit**

The following sample rule assumes that archives must not exceed a size limit of 10 MB if they are to be scanned by Advanced Threat Defense and that no special size limit exists for executable files, so only the general size limit for Advanced Threat Defense applies to this type of web objects.

So, the rule blocks archives and executable files that exceed the respective size limits.

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit object size for scanning by Advanced Threat Defense</td>
</tr>
</tbody>
</table>

Criteria:  
(\text{MediaType.IsArchive} \text{ equals true AND Body.Size greater than 10000000})  
\text{OR} (\text{MediaType.IsExecutable} \text{ equals true AND Body.Size greater than 125000000})

To extend the size check to other types of web objects, suitable parts must be added to the rule criteria. For example, if you want to cover audio files as well, a criteria part must be added that uses the \text{MediaType.IsAudio} property instead of the media type properties that are so far used in the sample rule.

To let the user who sent a request involving an over-sized object to the web know that and why this request was blocked, you can configure appropriate settings for the block action. In the sample rule, these settings are named \text{ATD limit}. 
Configure the use of Advanced Threat Defense

You can configure the use of Advanced Threat Defense for additionally scanning web objects after they have been scanned by Web Gateway. Another option is to let a scanning report that has been generated for a web object by Advanced Threat Defense be evaluated on Web Gateway to handle access to this object.

If an existing scanning report for a web object is evaluated, Web Gateway will not trigger a new additional scanning run by Advanced Threat Defense for this object.

Tasks

- **Configure scanning by Advanced Threat Defense on page 413**
  Configure additional scanning by Advanced Threat Defense after a scanning run by Web Gateway has been completed.

- **Configure use of an existing Advanced Threat Defense scanning report on page 414**
  If you do not want a new scanning run to be performed on a web object, you can let an existing Advanced Threat Defense scanning report be used to evaluate the web object.

Configure scanning by Advanced Threat Defense

Configure additional scanning by Advanced Threat Defense after a scanning run by Web Gateway has been completed.

Task

1. Configure Advanced Threat Defense to integrate it into your network.
   For more information, see the McAfee Advanced Threat Defense Product Guide.

2. On the user interface of Web Gateway, complete the following activities:
   a. Import the rule set for one of the two additional scanning workflows from the rule set library.
      These rule sets are located in the Gateway Anti-Malware rule set group.

      - **Advanced Threat Defense** — For forwarding web objects depending on the additional scanning
        On the rule sets tree, place this rule set after the rule set for scanning by Web Gateway. By default, this is the Gateway Anti-Malware rule set.

      - **ATD - Offline Scanning with Immediate File Availability** — For forwarding web objects before the additional scanning
        After importing this rule set, the following two rule sets appear on the rule sets tree.

        - **ATD - Init Offline Scan** — This rule set that initiates the additional scanning.
          On the rule sets tree, place this rule set after the rule set for scanning by Web Gateway. By default, this is the Gateway Anti-Malware rule set.

        - **ATD - Handle Offline Scan** This rule set handles the additional scanning once it has been initiated.
          On the rule sets tree, place this rule set after the rule sets that perform global or common activities and before the rule sets that perform particular filtering activities.

          For example, on the default rule sets tree, place this rule set after the Common Rules rule set and before the Media Type Filtering rule set.
b To enable monitoring of Advanced Threat Defense scanning activities on Web Gateway, import the ATD Scanning Log and Block on ATD Errors rule sets from the rule set library and add them to the existing Log Handler and Error Handler rule sets, respectively.

c Add media types to the list for supported media types or remove them as needed. After importing either of the library rule sets, the name of this list is Advanced Threat Defense Supported Types.

   After importing a rule set, you can work with this list on the key elements view of the rule set.

d Configure the settings for scanning by Web Gateway. By default, the name of these settings is Gateway Anti-Malware.

   After importing a rule set, you can work with these settings on the key elements view of the rule set.

e Configure the settings for scanning by Advanced Threat Defense. After importing either of the library rule sets, the name of these settings is Gateway ATD.

   After importing a rule set, you can work with these settings on the key elements view of the rule set.

f Save your changes.

Configure use of an existing Advanced Threat Defense scanning report

If you do not want a new scanning run to be performed on a web object, you can let an existing Advanced Threat Defense scanning report be used to evaluate the web object.

There are several options for using an existing scanning report. The following task assumes that:

- Scanning reports were generated for web objects that were uploaded manually to Advanced Threat Defense and scanned.
- Web Gateway allows access if a report shows that a web object is not infected and blocks it if no report exists.

Complete the following high-level steps:

Task

1 Create a rule set for the rules that handle the use of an existing Advanced Threat Defense scanning report.

2 In this rule set, create the following.
   - A rule that retrieves a scanning report for a file and blocks access to a file if no report exists for it
   - A rule that evaluates a scanning report and blocks a file that is infected according to the report

3 Configure the Gateway ATD settings of the Anti-Malware module.
   a Make sure Re-use previous detection ... is selected.
   b [Optional] Under Maximum detection age, modify the time limit for excluding older reports as needed. This limit is 30 minutes by default.

4 Save your changes.
Configure key elements for using Advanced Threat Defense

Configure key elements for additional scanning by Advanced Threat Defense to adapt important parts of the scanning process to the requirements of your web security policy.

Task

1. Import the Advanced Threat Defense or the ATD - Offline Scanning with Immediate File Availability rule set from the rule set library.

2. On the rule sets tree, select the rule set that you have imported.
   Key elements of the rules for the scanning process appear in the configuration pane.

3. Configure the key elements as needed.

4. Click Save Changes.

See also
Key elements for using Advanced Threat Defense on page 415

Key elements for using Advanced Threat Defense

The key elements of the rules for using Advanced Threat Defense in the process of additionally scanning web objects deal with important parts of this process. Different key elements can be configured for the rules in the rule sets that are implemented for the additional scanning.

- **Advanced Threat Defense** — When this rule set is implemented, the following groups of key elements can be configured:
  - Enable Advanced Threat Defense for These Supported Media Types
  - Gateway Anti-Malware Settings
  - Gateway Advanced Threat Defense Settings

- **ATD - Init Offline Scan Advanced** — When this rule set is implemented, the following groups of key elements can be configured:
  - Enable Advanced Threat Defense for These Supported Media Types
  - Gateway Anti-Malware Settings

- **ATD - Handle Offline Scan** — When this rule set is implemented, the following group of key elements can be configured:
  - Gateway Advanced Threat Defense Settings

The key elements of these rule sets are described in the following.

Enable Advanced Threat Defense for These Supported Media Types

Key element for selecting web objects that are eligible for additional scanning by Advanced Threat Defense
Table 11-45  Enable Advanced Threat Defense for These Supported Media Types

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media types to insert</td>
<td>Clicking Edit opens a window to let you edit the Advanced Threat Defense Supported Media Types list that is used by a rule.</td>
</tr>
<tr>
<td></td>
<td>Only web objects that belong to media types on this list will additionally be scanned by Advanced Threat Defense if also the other criteria are met.</td>
</tr>
<tr>
<td></td>
<td>You can add, modify, and remove entries on the list.</td>
</tr>
</tbody>
</table>

**Gateway Anti-Malware Settings**

Key element for configuring the scanning by the Anti-Malware module before the additional scanning by Advanced Threat Defense

Table 11-46  Gateway Anti-Malware Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Clicking Edit opens a window to let you edit the settings for the Anti-Malware module when it runs with the module components that are usually available on Web Gateway.</td>
</tr>
<tr>
<td></td>
<td>This scanning is performed before any scanning by Advanced Threat Defense. Depending on the result of this scanning, additional scanning by Advanced Threat Defense is performed or not.</td>
</tr>
</tbody>
</table>

**Gateway Advanced Threat Defense Settings**

Key element for configuring additional scanning by Advanced Threat Defense

Table 11-47  Bypass scanning for these agents and hosts

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Clicking Edit opens a window to let you edit the settings for the Anti-Malware module on Web Gateway when the scanning is actually performed by Advanced Threat Defense.</td>
</tr>
</tbody>
</table>

**Configure settings for using Advanced Threat Defense**

You can configure settings for the Anti-Malware module (or engine) on Web Gateway to enable the use of Advanced Threat Defense for scanning web objects.

**Task**

1. Select Policy | Settings.
2. On the Engines branch of the settings tree, expand Anti-Malware and select the settings for configuring the use of Advanced Threat Defense.
   - After importing the Advanced Threat Defense library rule set, the name of these settings is Gateway ATD.
3. Configure these settings as needed.
4. Click Save Changes.

**See also**

Gateway ATD settings on page 418
Monitoring the use of Advanced Threat Defense

Several methods are available for monitoring the scanning activities that are performed by Advanced Threat Defense when it is used to support Web Gateway.

The monitoring can be done on Web Gateway and on McAfee Content Security Reporter.

Monitoring the use of Advanced Threat Defense on Web Gateway

On Web Gateway, you can implement rule sets with rules for logging information about the scanning jobs that Advanced Threat Defense performs and for handling errors that occur during these jobs.

You can also review Advanced Threat Defense activities on the dashboard of the user interface.

- **Log Handler** — The *ATD Scanning Log* rule set can be imported from the *Logging* group of rule sets in the rule set library.

  The rule set contains a logging rule that records information about each scanning job Advanced Threat Defense performs on a web object that was passed on to it by Web Gateway.

  This information includes:
  - Severity grade that is the result of scanning
  - Server that Advanced Threat Defense runs on
  - Task ID for a scanning job
  - Hash value for a scanning job

  To create the log entries that provide this information, the rule uses suitable properties.

- **Error Handler** — The *Block on ATD Errors* rule set can be imported from the *Error Handling* group of rule sets in the rule set library.

  It contains blocking rules for handling errors that occur when Advanced Threat Defense performs a scanning job.

  The rules use the appropriate error IDs in their criteria. The error IDs range from 14010 to 14012.

  A rule in the Block on Anti-Malware Engine Errors rule set covers the range from 14002 to 14050.

  The Block on ATD Errors rule set should, therefore, be placed before this anti-malware rule set.

  Otherwise, the blocking rules in the Block on ATD Errors rule set would never be processed and only block messages with text that is related to anti-malware errors in general would be sent to users.

- **Anti-Malware properties** — Several properties are available for monitoring the activities of Advanced Threat Defense. Their names begin with *Antimalware.MATD*, for example, *Antimalware.MATD.Server* or *Antimalware.MATD.Report*.

  These properties are used in the logging rules of the ATD Scanning Log rule set.

  When a scanning job has been performed by Advanced Threat Defense, the value of the *Antimalware.MATD.Report* property is a report on this job. The report is provided as a string that represents the data structure of a JavaScript Object Notation (JSON) object.

  Using JSON properties together with the *Antimalware.MATD.Report* property, you can extract report information.
• **Dashboard** — The dashboard charts and tables show how the following data evolved during a particular time interval.

• Under **Executive Summary**: Number of requests for web objects that were blocked due to the scanning results found by Advanced Threat Defense.

• Under **Malware Statistics**: Number of requests for web objects that were passed on to Advanced Threat Defense for scanning, number of requests that were blocked due to the scanning results, and the time consumed for the scanning.

**Monitoring the use of Advanced Threat Defense on Content Security Reporter**

With McAfee® Content Security Reporter, you can collect data about the scanning activities that Advanced Threat Defense performs when it is used to support Web Gateway.

• To collect the data, configure both Web Gateway and Advanced Threat Defense as log sources.

• To view the data, register the server that Advanced Threat Defense runs on. You can then view the data on the dashboard monitor.

For more information, see the *McAfee Content Security Reporter Product Guide*.

**Gateway ATD settings**

The Gateway ATD settings are used for configuring the use of Advanced Threat Defense for scanning web objects that have been passed on to it from Web Gateway.

**Select Scanning Engines and Behavior**

Settings for selecting a combination of scanning engines and their behavior in case one of them detects an infection

**Table 11-48 Select Scanning Engines**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full McAfee coverage: The recommended high-performance configuration</strong></td>
<td>When selected, the McAfee Gateway Anti-Malware engine and the McAfee Anti-Malware engine are active. Web objects are then scanned using: <em>Proactive methods + Virus signatures</em> This option is selected by default.</td>
</tr>
<tr>
<td><strong>Layered coverage: Full McAfee coverage plus specific Avira engine features — minor performance impact</strong></td>
<td>When selected, the McAfee Gateway Anti-Malware engine, the McAfee Anti-Malware engine, and, for some web objects, also the third-party Avira engine are active. Web objects are then scanned using: <em>Proactive methods + Virus signatures + Third-party module functions for some web objects</em></td>
</tr>
<tr>
<td><strong>Duplicate coverage: Full McAfee coverage and Avira engine — less performance and more false positives</strong></td>
<td>When selected, the McAfee Gateway Anti-Malware engine, the McAfee Anti-Malware engine, and the third-party Avira engine are active. Web objects are then scanned using: <em>Proactive methods + Virus signatures + Third-party module functions</em></td>
</tr>
</tbody>
</table>
Table 11-48 Select Scanning Engines (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avira only: Only uses Avira engine — not recommended</td>
<td>When selected, only the Avira engine is active. Web objects are then scanned using: Third-party module functions</td>
</tr>
<tr>
<td>McAfee Advanced Threat Defense only: Send files to an MATD appliance for deep analysis through sandboxing</td>
<td>When selected, only scanning by Advanced Threat Defense is active. Web objects are then scanned using: Advanced Threat Defense functions</td>
</tr>
<tr>
<td>Stop virus scanning right after an engine detected a virus</td>
<td>When selected, engines stop scanning a web object as soon as one of them has detected an infection by a virus or other malware.</td>
</tr>
</tbody>
</table>

**MATD Setup**

Common part of the settings for configuring the use of Advanced Threat Defense

**Table 11-49 MATD Setup**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specifies the user name Web Gateway submits when trying to connect to Advanced Threat Defense.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password Web Gateway submits when trying to connect to Advanced Threat Defense.</td>
</tr>
<tr>
<td>Clicking Set</td>
<td>Clicking Set opens a window for setting the password.</td>
</tr>
<tr>
<td>Server list</td>
<td>Provides a list of servers that Advanced Threat Defense runs on.</td>
</tr>
<tr>
<td>List of certificate authorities</td>
<td>Provides a drop-down list for selecting a list of known certificate authorities. These certificate authorities will be used to refer to when communication between Web Gateway and Advanced Threat Defense is going on in SSL-secured mode under the HTTPS protocol.</td>
</tr>
</tbody>
</table>
| Severity threshold to indicate a malicious file | Sets a threshold for the severity grade of the malicious features that is detected in a web object, for example, a file, when scanned by Advanced Threat Defense.  
If this threshold is reached, the object is classified as malicious and the value of the Antimalware.Infected property is set to true.  
The threshold is set on slider scale with values ranging from 0 to 5 (very high severity). |
| Reuse previous detection, McAfee Web Gateway will retrieve latest report from MATD based on the hash of the file | When selected, the severity grade that was found for a web object at its last scanning by Advanced Threat Defense is used for classifying it as malicious or not.  
When this option is selected, the following option becomes accessible. |
| Maximum detection age                | Sets the maximum time (in minutes) that might elapse after a severity grade has been found for a web object before this value can no longer be used to classify the object as malicious or not.  
The default maximum time is 30 minutes. |
Table 11-49  MATD Setup (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reuse running task if same sample is analyzed</td>
<td>When selected, a running task is used for evaluation if it is the same web object that is analyzed.</td>
</tr>
<tr>
<td>Send client IP to MATD server</td>
<td>When selected, the IP address of a client that has sent a request for downloading a web object is sent to the server on which Advanced Threat Defense is running.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the server list.

Table 11-50  Server list – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Specifies the name of a server that Advanced Threat Defense runs on.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a server.</td>
</tr>
</tbody>
</table>

Network Setup

Settings for configuring the connection to the server that Advanced Threat Defense runs on

Table 11-51  Network Setup

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection timeout</td>
<td>Sets the time (in seconds) that elapses before the connection to a server is closed when no response is received from it.</td>
</tr>
<tr>
<td></td>
<td>The default time is 5 seconds.</td>
</tr>
<tr>
<td>Scan timeout</td>
<td>Sets the time (in minutes and seconds) that Advanced Threat Defense is allowed for scanning a web object.</td>
</tr>
<tr>
<td></td>
<td>If this time is exceeded, Web Gateway records it as an error.</td>
</tr>
<tr>
<td></td>
<td>Minutes — Time allowed in minutes</td>
</tr>
<tr>
<td></td>
<td>Seconds — Time allowed in seconds</td>
</tr>
<tr>
<td></td>
<td>The default time is 10 minutes.</td>
</tr>
<tr>
<td>Poll interval</td>
<td>Sets the time interval (in seconds) that elapses before the next attempt is made to retrieve information from Advanced Threat Defense about the progress made in scanning a web object.</td>
</tr>
<tr>
<td></td>
<td>The default time is 20 seconds.</td>
</tr>
</tbody>
</table>

Advanced Threat Defense rule set

The Advanced Threat Defense rule set is a library rule set for enabling Web Gateway to work with Advanced Threat Defense when filtering web objects.

Library rule set – Advanced Threat Defense

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Antimalware.Proactive.Probability&lt;Gateway Anti-Malware&gt; greater than or equals 60 AND MediaType.EnsuredTypes at least one in list Advanced Threat Defense Supported Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Responses, Embedded Objects</td>
</tr>
</tbody>
</table>
The rule set criteria specifies that the rule set applies if the following is true:

- As a result of previous scanning by the anti-malware engines on Web Gateway, the probability that a web object is malicious equals or exceeds 60 percent
- The media type of the object is on the list of supported types for scanning by Advanced Threat Defense.

The rule set contains the following rules.

**Enable progress page**

*Always* –> *Continue* – Enable Progress Page<Default>

The rule enables an event that lets a page be shown to indicate the progress made when a web object is downloaded to a client.

**Upload file to ATD and wait for scanning result**

*Antimalware.Infected<Gateway ATD>* –> *Block<Virus Found>* –
Statistics.Counter.Increment("BlockedByMATD",1)<Default>

The rule uses the *Antimalware.Infected* property to check whether a web object, for example, a file, is infected by a virus or other malware.

The scanning that is required for this check is performed under the Gateway ATD settings, which means it is carried out by Advanced Threat Defense.

If the object is found to be infected, the process of forwarding the object to the requesting client is blocked and a block message is shown to the user who requested access to the object.

The block action is recorded by the statistics counter.

### ATD - Offline Scanning with Immediate File Availability rule set

The ATD - Offline Scanning with Immediate File Availability rule set is a library rule set for enabling Web Gateway to work with Advanced Threat Defense when filtering web objects.

When this rule set is implemented, a web object is forwarded to the user who requested it before it has been additionally scanned by Advanced Threat Defense, so the object is immediately available to the user.

If the scanning result is that the web object is infected, a message is sent to the administrator of the network that the user sent the request from.

This use of the scanning functions of Advanced Threat Defense is also known as **offline scanning** or **background scanning**.

After importing this rule set, the following two rule sets are implemented and appear on the rule sets tree:

- ATD - Init Offline Scan
- ATD - Handle Offline Scan

A rule set with the name **ATD - Offline Scanning with Immediate File Availability** is not implemented.

**ATD - Init Offline Scan**

This rule set initiates the additional scanning by Advanced Threat Defense.
The rule set criteria specifies that the rule set applies if the following is true:

- As a result of previous scanning by Web Gateway, the probability that a web object is malicious equals or exceeds 60 percent.
- The media type of the object is on the list of supported types for scanning by Advanced Threat Defense.
- The web object does not exceed a particular size.

The rule set contains the following rule.

**Offline scanning with immediate file availability**

Antimalware.MATD.InitBackgroundScan(5) equals false –> Block<ATD Communication Failed>

When this rule is processed, all data related to the request for web access that has been sent to Web Gateway is recorded, including the response that was received from the requested web server. The response usually includes in its body the requested web object, for example, a file. The body with the web object is stored on Web Gateway.

An internal request is also created within Web Gateway to initiate the scanning by Advanced Threat Defense. Web Gateway then waits for an answer to this internal request to see whether the request is accepted and the scanning will be performed.

The time that Web Gateway waits for this answer is measured in seconds and a parameter of the Antimalware.MATD.InitBackgroundScan property. By default, this time is 5 seconds. You can configure this time by editing the property parameter.

If no answer to the internal request is received within the configured time, the property is set to false, so this criteria matches and the rule applies. A message is then sent to inform the administrator that the additional scanning by Advanced Threat Defense could not be executed.

If the answer is received within the configured time, the web object is forwarded to the user.

Further handling of the additional scanning is performed by the next rule set..
The rule uses the `Antimalware.Infected` property to check whether a web object, for example, a file, is infected by a virus or other malware. The scanning that is required for this check is performed under the Gateway ATD settings, which means it is carried out by Advanced Threat Defense.

For this purpose, the previously stored web object is forwarded from Web Gateway to Advanced Threat Defense.

If the scanning result is that the web object is infected, this is recorded by a statistics counter.

**Offline scanning with immediate file availability**

```plaintext
Antimalware.Infected<Gateway ATD> equals true -> Block<Virus Found> - Set
User-Defined.MessageText =
"Client.IP: "
+ IP.ToString(Client.IP)
+ "Requested URL: "
+ URL
+ "Virus name: "
```

When the rule is processed, it is checked whether the value of the `Antimalware.Infected` property is `true`.

If it is, it means the scanning that was performed by Advanced Threat Defense has found a web object to be infected by a virus or other malware.

A warning message is then created and sent to the administrator for the network of the user who sent the request to access the web object. The message contains information on the request that was recorded by the rule of the preceding rule set.

**Stop cycle**

`Always` -> Stop Cycle

This rule stops the processing cycle. It is always executed after the preceding rules have been processed.

---

**Data loss prevention**

Data loss prevention (DLP) ensures that sensitive content is not allowed to leave your network. The prevention process detects this content and blocks traffic going out to the web accordingly.

The following elements are involved in this process:

- Data loss prevention rules that control the process
- Default classifications and a dictionary that you fill with entries for data loss prevention
- Data loss prevention modules, which are called by the rules that are processed to find out about sensitive content

You can also use data loss prevention rules to keep inappropriate content from entering your network. However, this can have an impact on performance.

The data loss prevention process can be applied to text contained in the body that is sent with a request or response or to any other text that is contained in requests or responses, for example, URL parameters or headers.
When you are running the appliance together with a DLP solution that uses an ICAP server for the filtering process, you can implement a rule set to ensure the smooth flow of data between the appliance and the ICAP server.

**Data loss prevention rules**

Data loss prevention is not implemented by default on the appliance, but you can import the *Data Loss Prevention* rule set from the library.

You can then review the rules of this rule set, modify or delete them, and also create your own rules.

A data loss prevention rule blocks, for example, a request if the text that is sent as its body includes sensitive content. To find out whether this is true for a given request body, the rule calls a module that inspects the body. To know what is considered sensitive, the module refers to the default classifications on the system lists or to dictionary entries, according to what is configured.

When a request or response is processed, its body text is stored as the value of the *Body.Text* property. Before body text can be stored and inspected, it must be extracted. The Composite Opener module performs the opening jobs. A rule in a rule set of the *Common Rules* rule set enables the opener by default.

A request body could, for example, be a text file that uploading to the web is requested for. The value of a suitable body-related property in the rule criteria would then have to be true for the rule to apply and execute the blocking.

The following rule uses the *DLP.Classification.BodyText.Matched* property in this way. If a request includes sensitive content in its body, this is detected by the data loss prevention module. The value of the property is set to *true*, and the request is blocked.

**Name**

**Block files with SOX information**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>DLP.Classification.BodyText.Matched&lt;SOX&gt;</em> equals true</td>
<td>Block&lt;<strong>DLP.Classification.Block</strong>&gt;</td>
</tr>
</tbody>
</table>

When this rule is processed, the data loss protection module knows, due to its settings, that it has to look for content that is sensitive with regard to the SOX (Sarbanes-Oxley) regulations, which deal with responsibilities of public companies.

Events can be added to the rule to log information on data loss prevention or to increment a counter that counts how often it has occurred that a request is blocked due to this rule.

**Default classifications and dictionary entries**

Default classifications and dictionary entries are used in data loss prevention to specify sensitive content that should be prevented from leaving your network.

However, you can also use system lists and dictionary entries to specify inappropriate content, such as discriminatory or offensive language, that should not be allowed to enter your network. Inappropriate content could, for example, be specified this way to let a rule block content sent from web servers in response to requests.

The library rule set for data loss prevention contains a nested rule set for processing body text in the response cycle.
Default classifications and dictionary entries differ in the following ways:

- **Default classifications** — Provide information for detecting different kinds of sensitive or inappropriate content, for example, credit card numbers, social security numbers, or medical diagnosis data.

  Default classifications are contained in folders and subfolders on system lists and updated by the appliance system. You can view the system lists under **DLP Classification** in the **System Lists** branch of the lists tree, but you cannot edit or delete them.

  When you edit the settings of the module that handles classifications, you can select suitable subfolders from the folders on these lists and create a list with classifications for data loss prevention in your network.

- **Dictionary entries** — Specify sensitive or inappropriate content, for example, names of persons or keywords indicating content that should not leave your network.

  The dictionary is created as part of the settings for the module that handles this list.

  Creating a dictionary and filling it with entries for sensitive or inappropriate content is a means to configure the data loss prevention process beyond what is possible by using the default classifications on the system lists. This way you can adapt the process to the requirements of your network.

**Data loss prevention modules**

The job of the data loss prevention modules (also known as *engines*) is to detect sensitive or inappropriate content in the body text of requests and responses and also in any other text that is sent with requests and responses.

When composite objects, such as archive documents, bodies of POST requests, and others, are sent with requests or responses, they are also included in the data loss prevention process. To account for such objects, the data loss prevention rules are also processed in the embedded objects cycle.

Depending on what the data loss prevention modules find out, body-related properties in rule criteria are set to *true* or *false*, so web traffic is eventually blocked or allowed.

There are two modules that differ in their use of lists for detecting relevant content:

- **Data Loss Prevention (Classifications)** — Uses default classifications on system lists for data loss prevention

- **Data Loss Prevention (Dictionaries)** — Uses dictionaries with entries for sensitive and inappropriate content that you provide yourself for data loss prevention

When configuring settings for the modules, you let them know which content to look for. The default classifications and dictionary entries that specify the content are among the settings parameters.

**Search methods for data loss prevention**

There are different methods of searching content that should be prevented from leaving or entering your network.

- A search can aim at finding out whether a given request or response body includes portions of content that are specified as sensitive or inappropriate.

- A search can begin with a portion of content, for example, an URL parameter or header, and find out whether it is sensitive or inappropriate according to what you have configured.

For the first method, you can use the **DLP.Classification.BodyText.Matched** property that was already shown in a sample rule.
For the second, you can use the `DLP.Classification.AnyText.Matched` property. This property takes a string parameter for the content portion that is checked for being on a system list or in a dictionary.

Depending on what you are working with, you would use the two already mentioned parameters with system lists and `DLP.Dictionaries.BodyText.Matched` and, `DLP.Dictionaries.AnyText.Matched` with the dictionary.

**Logging data loss prevention**

Additional properties are provided for logging the results of the data loss prevention process. They allow you to log this data, for example, using an event in a rule.

When the value of `DLP.Classification.BodyText.Matched` is `true` for the body text of a request or response that was processed, the following applies for the relevant logging properties:

- `DLP.Classification.BodyText.MatchedTerms` contains a list of the matching terms from the body text
- `DLP.Classification.BodyText.MatchedClassifications` contains a list of the matching classifications


Similarly, matching terms and classifications can be logged for the search method that looks for matches of a given text string.

When the value of `DLP.Classification.AnyText.Matched` is `true`:

- `DLP.Classification.AnyText.MatchedTerms` contains a list of matching terms found in text other than body text.
- `DLP.Classification.AnyText.MatchedClassifications` contains a list of matching classifications found in text other than body text.

When the match is in a dictionary, `DLP.Dictionary.AnyText.Matched` is `true` and `DLP.Dictionary.AnyText.MatchedTerms` contains a list of matching terms.

Information on data loss prevention results is also shown on the dashboard.

**Preventing loss of medical data**

The following is an example of data loss prevention that assumes medical data must be prevented from leaving the network of an American hospital.

Default classifications for preventing the loss of medical data are contained in the HIPAA (Health Insurance Portability and Accountability Act) folder. In addition to this default information, the names of the doctors who are working in the hospital are entered in a dictionary to ensure they also do not leave the network.

The following activities need to be completed for configuring data loss prevention in this example:

- Configure settings for the Data Loss Prevention (Classifications) module that include the default HIPAA classifications
- Configure settings for the Data Loss Prevention (Dictionaries) module that include the doctors' names as dictionary entries
• Make sure the rule that activates the Composite Opener is enabled

In the default rule set system, this rule is contained in the Enable Opener rule set, which is nested in the Common Rules rule set.

• Create a rule that checks content according to the configured settings

The rule must be included in a rule set that applies in the request cycle for request to upload data from the hospital network to the web.

This rule set can be a nested rule set of the default rule set for data loss prevention or a rule set that you create yourself.

In this example, the rule checks only text contained in the body of a request. It could look as follows:

Name

Prevent loss of HIPAA data and doctors' names

Criteria

Action


→ Block<DLP.Classification.Block>

Configure data loss prevention

You can configure data loss prevention to keep sensitive content from leaving your network. You can also use it to keep inappropriate content from entering.

Complete the following high-level steps.

Task

1 Import the Data Loss Prevention rule set from the library.

2 Review its rules and modify them as needed.

You can, for example:

• Configure settings for data loss prevention using default classifications.

• Configure settings for data loss prevention using dictionary entries.

• Modify other settings parameters.

• Create rules of your own.

You can also create your own rule set for data loss prevention instead of using the library rule set.

3 Make sure the Composite Opener is enabled, so the body text sent with requests and responses can be inspected.

In the default rule set system, this rule is contained in the Enable Opener rule set, which is nested in the Common Rules rule set.

4 If you want to run data loss prevention with ICAP, you can import another rule set from the library and modify its rules as needed.

5 Save your changes.
Configure data loss prevention using default classifications
You can configure data loss prevention by selecting default classifications from system lists and entering them in a list that is included in the settings of the data loss prevention module for processing classifications.

Task
1  Select Policy | Settings.
2  On the settings tree, select Data Loss Prevention (Classifications) and click Add.
   The Add Settings window opens.
3  Configure general settings parameters:
   a  In the Name field, type a name for the settings.
   b  [Optional] In the Comment field, type a plain-text comment on the settings.
   c  [Optional] Click the Permissions tab and configure who is allowed to access the settings.
4  On the toolbar of the DLP Classifications inline list, click the Edit icon.
   An Edit window opens with a tree structure of folders containing subfolders with default classifications.
5  Expand a folder, for example, SOX Compliance, and select a subfolder, for example, Compliance Reports. Then click OK.
   You can also select several subfolders of a folder at once, select folders from different subfolders, or select complete folders with all their respective subfolders.
   The Edit window closes and the subfolder or subfolders appear in the DLP Classifications inline list.
6  Click Save Changes.

Configure data loss prevention using dictionary entries
You can enter text and wildcard expressions that specify sensitive or inappropriate content into as entries in a dictionary for data loss prevention.
After importing the library Data Loss Prevention rule set, use of a dictionary with entries specifying sensitive or inappropriate content is not yet implemented. You need to create appropriate settings to implement it and fill the dictionary with entries.

Tasks
- Create settings with a dictionary on page 429
  For data loss prevention that uses dictionary entries, you must create settings that include a dictionary.
- Fill the dictionary with entries on page 429
  After creating settings with a dictionary, you can fill the dictionary with entries.
Create settings with a dictionary

For data loss prevention that uses dictionary entries, you must create settings that include a dictionary.

**Task**

1. Select Policy | Settings.
2. On the settings tree, select Data Loss Prevention (Dictionaries) and click Add.
   
   The Add Settings window opens.
3. Configure general settings parameters:
   
   a. In the Name field, type a name for the settings.
   b. [Optional] In the Comment field, type a plain-text comment on the settings.
   c. [Optional] Click the Permissions tab and configure who is allowed to access the settings.

You can now fill the dictionary with entries.

Fill the dictionary with entries

After creating settings with a dictionary, you can fill the dictionary with entries.

**Task**

1. Within the settings you have created for data loss prevention using dictionary entries, click the Add icon on the toolbar of the Dictionary inline list.
   
   The Add DLP Dictionary Entry window opens.
2. Under Type of data to search, select Text or Wildcard expression.
3. In the Text or wildcard expression field, enter a text string or a wildcard expression.
4. [Optional] Specify additional information for an entry:
   
   - If you have entered a text string, select one of the following options or any combination of them:
     - Case-sensitive
     - At start of word
     - At end of word
   - If you have entered a wildcard expression, select Case-sensitive or leave it deselected as needed.
5. [Optional] In the Comment field, type a plain-text comment on an entry.
6. Click OK.

   The Add DLP Dictionary Entry window closes and the new entry appears in the dictionary.
   
   Repeat Steps 1 to 6 to add more entries.
7. Click OK in the Add Settings window.

   The window closes and the new settings appear on the settings tree under Data Loss Prevention (Dictionaries).
**Data Loss Prevention (Classifications) settings**

The Data Loss Prevention (Classifications) settings are used for configuring entries in classification lists that specify sensitive or inappropriate content.

**DLP Classifications Parameters**

Settings for configuring the use of classification lists when searching for sensitive or inappropriate content

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking policy</td>
<td>Sets the scope of the search for sensitive or inappropriate content in the body text of requests and responses. The search is carried out for all classifications that have been selected. You can, however, configure it in the following ways:</td>
</tr>
<tr>
<td></td>
<td>• Minimum — The search stops when an instance of sensitive or inappropriate content has been found for a particular classification or if no instance could be found. It is then continued for the next classification. This goes on until all classifications have been processed.</td>
</tr>
<tr>
<td></td>
<td>• Maximum — The search tries to find all instances of sensitive or inappropriate content for a particular classification. When the search is completed for a classification, it continues with the next. This goes on until all classifications have been processed.</td>
</tr>
<tr>
<td>DLP Classifications</td>
<td>Provides a list for selecting entries in classification lists from the system lists provided under <strong>DLP Classification</strong> on the lists tree.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the DLP Classifications list

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Classification</td>
<td>Provides information about detecting sensitive or inappropriate content.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on an entry.</td>
</tr>
</tbody>
</table>

**Advanced Parameters**

Settings for configuring advanced functions for data loss prevention

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported context width</td>
<td>Limits the number of characters shown around a matching term in a list to the specified value. The matching term is the value of the <strong>DLP.Classification.Matched.Terms</strong> property.</td>
</tr>
<tr>
<td>Context list size</td>
<td>Limits the number of matching terms shown in a list to the specified value. The matching terms are the values of the <strong>DLP.Classification.Matched.Terms</strong> property.</td>
</tr>
</tbody>
</table>
Data Loss Prevention (Dictionaries) settings
The Data Loss Prevention (Dictionaries) settings are used for configuring text and wildcard expressions that specify sensitive or inappropriate content.

DLP Dictionary Parameters
Settings for configuring text and wildcard expressions specifying sensitive or inappropriate content

Table 11-55  DLP Dictionaries Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking policy</td>
<td>Sets the scope of the search for sensitive or inappropriate content in the body text of requests and responses. The search is carried out for all dictionary entries that have been created. It can, however, be configured in the following ways:</td>
</tr>
<tr>
<td></td>
<td>• Minimum — The search stops when an instance of sensitive or inappropriate content has been found for a particular dictionary entry or if no instance could be found. It is then continued for the next entry.</td>
</tr>
<tr>
<td></td>
<td>• Maximum — The search tries to find all instances of sensitive or inappropriate content for a particular dictionary entry. When the search is completed for an entry, it continues with the next.</td>
</tr>
<tr>
<td>Dictionary</td>
<td>Provides a list for entering text strings and wildcard expressions that are sensitive or inappropriate content or match with it.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the Dictionary list.

Table 11-56  Dictionary – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text or wildcard expression</td>
<td>Specifies a text string or wildcard expression that is sensitive or inappropriate content or matches with it.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a text string or wildcard expression.</td>
</tr>
</tbody>
</table>

Advanced Parameters
Settings for configuring advanced functions for data loss prevention

Table 11-57  Advanced Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported context width</td>
<td>Limits the number of characters shown around a matching term in a list to the specified value. The matching term is the value of the DLP.Dictionary.Matched.Terms property.</td>
</tr>
<tr>
<td>Context list size</td>
<td>Limits the number of matching terms shown in a list to the specified value. The matching terms are the values of the DLP.Classification.Matched.Terms property.</td>
</tr>
</tbody>
</table>
Data Loss Prevention rule set

The Data Loss Prevention (DLP) rule set is a library rule set for preventing sensitive content from leaving your network or inappropriate content from entering it.

<table>
<thead>
<tr>
<th>Default rule set – Data Loss Prevention (DLP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

The following rule sets are nested in this rule set:

- DLP in Request Cycle
- DLP in Response Cycle
  
  This rule set is not enabled by default.

**DLP in Request Cycle**

This nested rule set blocks requests that are sent from clients of our network to web servers if it is detected that sensitive content is involved. For example, a request to upload a file to the web that has sensitive content is blocked.

<table>
<thead>
<tr>
<th>Nested library rule set – DLP in Request Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Cycle.TopName equals &quot;Request&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM) and embedded objects</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a request is processed on the appliance.

The rule set contains the following rules:

**Block files with HIPAA information**

\[
\text{DLP.Classification.BodyText.Matched <HIPAA> equals true} \rightarrow \text{Block\{DLP.Classification.Block\}} \rightarrow \text{Statistics.Counter.Increment ("BlockedByDLPMatch",1)}<\text{Default}>
\]

The rule uses the \text{DLP.Classification.BodyText.Matched} property to check whether the body of the request that is currently processed contains text that is considered to be sensitive content. This text could, for example, be in a file that uploading to the web is requested for.

Text is considered to be sensitive content according to the HIPAA health care regulations. Use of the relevant information is configured as part of the module settings, which are specified after the property name.

If there is sensitive content in the text of a request body, the request is blocked. The settings of the Block action specify a message to the requesting user.

The rule also uses an event to count blocking due to a data loss prevention match.

**Block files with Payment Card Industry information**

\[
\text{DLP.Classification.BodyText.Matched <Payment Card Industry> equals true} \rightarrow \text{Block\{DLP.Classification.Block\}} \rightarrow \text{Statistics.Counter.Increment ("BlockedByDLPMatch",1)}<\text{Default}>
\]

The rule uses the \text{DLP.Classification.BodyText.Matched} property to check whether the body of the request that is currently processed contains text that is considered to be sensitive content. This text could, for example, be in a file that uploading to the web is requested for.

Text is considered to be sensitive content according to the regulations that apply for payment cards. A credit card number would, for example, be content under these regulations. Whether there is sensitive content in a text, is detected using appropriate information in the same way as for the HIPAA-related rule.
If there is sensitive content in the text of a request body, the request is blocked. The settings of the Block action specify a message to the requesting user.

The rule also uses an event to count blocking due to a data loss prevention match.

**Block files with SOX information**

\[DLP\textunderscore Classification\textunderscore BodyText\textunderscore Matched <SOX> \text{ equals true} \rightarrow \text{Block}<\text{DLP\textunderscore Classification\textunderscore Block}> - \text{Statistics\textunderscore Counter\textunderscore Increment} \left(\text{"BlockedByDLPMatch"},1\right)<\text{Default}\]

The rule uses the `DLP\textunderscore Classification\textunderscore BodyText\textunderscore Matched` property to check whether the body of the request that is currently processed contains text that is considered to be sensitive content. This text could, for example, be in a file that uploading to the web is requested for.

Text is considered to be sensitive content according to the regulations of the Sarbanes-Oxley (SOX) act on public company accountability. Board meeting minutes would, for example, be sensitive content under this act. Whether there is sensitive content in a text, is detected using appropriate information in the same way as for the HIPAA-related rule.

If there is sensitive content in the text of a request body, the request is blocked. The settings of the Block action specify a message to the requesting user.

The rule also uses an event to count blocking due to a data loss prevention match.

**DLP Response Cycle**

This nested rule set blocks responses that are received on the appliance from web servers if it is detected that they contain inappropriate content, for example, discriminatory or offensive language.

<table>
<thead>
<tr>
<th>Nested library rule set – DLP Response Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong> – Cycle\textunderscore TopName equals &quot;Response&quot;</td>
</tr>
<tr>
<td><strong>Cycles</strong> – Responses and embedded objects</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when a response is processed on the appliance.

The rule set contains the following rule:

**Acceptable use**

\[DLP\textunderscore Classification\textunderscore BodyText\textunderscore Matched <Acceptable Use> \text{ equals true} \rightarrow \text{Block}<\text{DLP\textunderscore Classification\textunderscore Block}> - \text{Statistics\textunderscore Counter\textunderscore Increment} \left(\text{"BlockedByDLPMatch"},1\right)<\text{Default}\]

The rule uses the `DLP\textunderscore Classification\textunderscore BodyText\textunderscore Matched` property to check whether the body of the response that is currently processed contains text that is considered to be sensitive content. This text could, for example, be in a file that is sent in response to a download request.

The module that is called by the rule to find out whether there is inappropriate content in the response body uses appropriate information from classification lists. Use of these lists is configured as part of the module settings, which are specified after the property name.

If there is inappropriate content in the text of a response body, the response is blocked. The settings of the Block action specify a message to the user who the response should have forwarded to.

The rule also uses an event to count blocking due to a data loss prevention match.
Preventing data loss using an ICAP server

When you have implemented data loss prevention with an ICAP server that handles the filtering process, you can configure settings and implement a rule set to ensure the smooth flow of data between the appliance and the ICAP server.

You can use a solution called nDLP for data loss prevention. Within this solution, data that users want to upload from your network to the web is filtered to prevent data loss. The filtering is done on an ICAP server. The data flow is as follows:

- Data sent from the client systems of your users is forwarded to the appliance.
- The appliance provides an ICAP client that sends REQMOD requests with the user data to the ICAP server.
- The requests are filtered on the server by modifying them according to the ICAP protocol and passed on to the web servers that are the destinations of the requests.

After importing the Data Loss Prevention with ICAP rule set from the library, rules that are implemented on the appliance control the sending of requests to the ICAP server.

According to these rules, a request is not forwarded if:

- The body of the request contains no data and the request does not include URL parameters.
- The body of the request exceeds a given size (default: 50 MB).

Together with the rule set, settings are imported that you need to configure. These include a list of the ICAP servers that the appliance can forward requests to.

You can also configure the ICAP client on the appliance not to open more connections for sending requests than a particular ICAP server can handle at the same time.

Create an ICAP server list for data loss prevention

When running the nDLP solution for data loss prevention, which uses an ICAP server for filtering data, you need to configure a list of these servers.

**Task**

1. Select Policy | Settings.
2. On the settings tree, select ICAP Client and click the ReqMod settings.
3. Configure the ICAP server list that is provided under these settings as needed.
4. Click Save Changes.

**ICAP Client settings**

The ICAP Client settings are used for configuring communication in REQMOD mode between an ICAP client on the appliance and ICAP servers.

**ICAP Service**

Settings for ICAP servers that the ICAP client on the appliance sends requests to
Table 11-58  Select Scanning Engines

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of ICAP Servers</td>
<td>Provides a list for selecting a list of servers that are used in ICAP communication. Requests coming in from ICAP clients are distributed to the servers in the selected list in round-robin mode. For this purpose, the list is checked in intervals of 60 seconds.</td>
</tr>
</tbody>
</table>

The following table describes an entry for an ICAP server in a server list.

Table 11-59  Entry in a list of ICAP servers

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>URI</td>
<td>Specifies the URI of an ICAP server. Format: ICAP://&lt;IP address&gt;:&lt;port number&gt;</td>
</tr>
<tr>
<td>Respect max concurrent connections limit</td>
<td>When selected, the ICAP client on the appliance does not open more connections at the same time for sending requests than the ICAP server can handle.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on an ICAP server.</td>
</tr>
</tbody>
</table>

**Data Loss Prevention With ICAP rule set**

The Data Loss Prevention with ICAP rule set is a library rule set for configuring the data flow between the appliance and an ICAP server in a solution for data loss prevention.

**Library rule set – Data Loss Prevention With ICAP**

Criteria — URL.Host does not equal ""
Cycles — Requests (and IM) and embedded objects

The rule set criteria specifies that the rule set applies when a host name can be found for a URL that is sent in a request to the appliance.

The rule set contains the following rules.

**Skip requests that do not carry information**

Body.Size equals 0 AND ListOfString.IsEmpty(URL.Parameters) equals true —> Stop Rule Set

The rule uses the Body.Size property to check whether a request has a body that is empty. It also uses the ListOfString.IsEmpty property to check whether a request has URL parameters.

If one of the two parts of this criteria is matched, processing of the rule set stops and the request is not forwarded to the ICAP server.

**Skip body that is greater than 50 MB**

Body.Size greater than 52428800 —> Stop Rule Set

The rule uses the Body.Size property to check whether the body of a request does not exceed 50 MB. If it does, processing of the rule set stops and the request is not forwarded to the ICAP server.

In the rule set criteria, the size of a request body that must not be exceeded is specified in bytes.

**Call ReqMod server**

ICAP.ReqMod.Satisfaction<ReqMod> equals true —> Stop Cycle

When a request has passed filtering according to the first two rules of the rule set, it is forwarded to the ICAP server. If this has been done, the value of the ICAP.ReqMod.Satisfaction property is true.

The rule checks whether this is the case for a request and eventually stops processing the current cycle.
Web filtering
Data loss prevention
Supporting functions

Some functions on the appliance do not filter web objects or users, but support the filtering process in different ways.

You can use the supporting functions to do the following:

- **Show download progress** — You can configure methods to show users the progress made in downloading web objects.

- **Throttle bandwidth for uploads and downloads** — You can limit the speed for uploading data from clients to the appliance or downloading them from web servers to the appliance.

- **Use the web cache to store and provide web objects** — You can speed up responses to client requests by delivering objects from the web cache on the appliance.

- **Route requests through next-hop proxies** — You can use these proxies to route requests to their destination.

**Contents**

- Progress indication
- Bandwidth throttling
- Web caching
- Next-hop proxies

**Progress indication**

Progress indication is a process that shows a user who has started the download of a web object the progress made in downloading the object.

The following elements are involved in this process:

- Progress indication rules that control the process

- Progress indication modules that are called by the rules to handle the different methods for progress indication

**Progress indication rules**

The rules that control progress indication are usually contained in one rule set. Different rules control the use of different methods for progress indication. Accordingly, they call different modules to handle these methods.
Two methods for progress indication are available on the appliance. Which method is appropriate for a download depends on the browser that a user sends the download request with.

- **Progress page** — For Mozilla browsers
  Under this method, a page with a progress bar is shown to the user who started a download and then another page for download completion.

- **Data trickling** — For all other browsers
  Under this method, a web object is forwarded to the user in chunks and at a particular forwarding rate.

Progress indication is not implemented with the default rule set system. A library rule set provides these functions. It's name is *Progress Indication*.

You can implement this rule set, review its rules, modify or delete them, and also create your own rules.

**Progress indication modules**

Two progress indication modules (also known as *engines*) are available for handling different methods of progress indication:

- **Progress Page module** — For the progress page method
- **Data Trickling module** — For the data trickling method

You can configure settings for these modules to modify the way they handle these methods.

Templates are provided for configuring the two pages used for the progress page method. The configuration is done in the same way as for user message templates.

**Configure progress indication**

You can implement progress indication and configure it to adapt it to the needs of your network. Complete the following high-level steps.

**Task**

1. **Import** the Progress Indication rule set from the library.

2. **Review** the rules in this rule set and modify them as needed.
   You can, for example, do the following:
   - Configure settings for the Progress Page module:
     - Choose a particular language for the progress page
     - Modify the text of the progress page
     - Specify timeouts for the downloaded page, for example, a timeout for the time that a page is available after the download
   - Configure settings for the Data Trickling module:
     - Size of the first chunk in the trickling process
     - Forwarding rate

3. **Save** your changes.
Configure the progress indication modules

You can configure the progress indication modules to modify the way progress made in downloading a web objects is shown to users.

There are two different modules for progress indication: the Progress Page and the Data Trickling modules.

**Task**


2. On the rule sets tree, select the rule set for progress indication.
   - If you have implemented the library rule set for this function, this is the Progress Indication rule set.
   - The rules of the rule set appear on the settings pane.

3. Make sure Show details is selected.

4. Find the rule that calls the Progress Page module or the rule that calls the Data Trickling module, according to what you want to configure.
   - In the library rule set, these are the rules Enable progress page and Enable data trickling.

5. In the rule event of the appropriate rule, click the settings name.
   - The Edit Settings window opens. It provides the settings for the Progress Page or the Data Trickling module.

6. Configure these settings as needed.

7. Click OK to close the window.

8. Click Save Changes.

**See also**

*Data Trickling settings on page 440*
*Progress Indication rule set on page 441*

**Progress Page settings**

The Progress Page settings are used for configuring the progress page that is shown to users when they are downloading web objects.

**Progress Page Parameters**

Settings for the progress page

**Table 12-1  Progress Page Parameters**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Templates</td>
<td>Provides settings for the templates that are used by the progress page.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>Provides settings timeouts that are related to the progress page.</td>
</tr>
</tbody>
</table>

**Templates**

Settings for the templates used by the progress page
Table 12-2 Templates

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Provides settings for selecting the language of the progress page.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto (Browser)</strong> — When selected, the message is in the language of the browser that the blocked request was sent from.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Force to</strong> — When selected, the message is in the language chosen from the list that is provided here.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Value of ‘Message.Language’ property</strong> — When selected, the message is in the language that is the value of the Message.Language property. This property can be used for creating a rule.</td>
</tr>
<tr>
<td>Collection</td>
<td>Provides a list for selecting a template collection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> — Opens the Add Template Collection window for adding a template collection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> — Opens the Template Editor for editing a template collection.</td>
</tr>
<tr>
<td>Template name for progress bar page</td>
<td>Provides a list for selecting a template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> — Opens the Add Template window for adding a template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> — Opens the Template Editor for editing a template.</td>
</tr>
<tr>
<td>Template name for download finished page</td>
<td>Provides a list for selecting a template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> — Opens the Add Template window for adding a template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> — Opens the Template Editor for editing a template.</td>
</tr>
<tr>
<td>Template name for download canceled page</td>
<td>Provides a list for selecting a template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> — Opens the Add Template window for adding a template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> — Opens the Template Editor for editing a template.</td>
</tr>
</tbody>
</table>

Timeouts

Settings for the timeouts that are related to the progress page

Table 12-3 Templates

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay for redirects to progress page</td>
<td>Limits the time (in seconds) that elapses before the progress page appears to the specified value.</td>
</tr>
<tr>
<td>File availability time before download</td>
<td>Limits the time (in minutes) that elapses before a file is no longer available to a user before the download to the specified value.</td>
</tr>
<tr>
<td>File availability time after download</td>
<td>Limits the time (in minutes) that elapses before a file is no longer available to a user after the download to the specified value.</td>
</tr>
</tbody>
</table>

Data Trickling settings

The Data Trickling settings are used for configuring the data trickling process that is applied when a user has started the download of a web object.

Data Trickling Parameters

Settings for the portions of a web object that are forwarded in data trickling mode.
Table 12-4  Data Trickling Parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of first chunk</td>
<td>Specifies the size (in bytes) of the first chunk of a web object that is forwarded using the data trickling method.</td>
</tr>
<tr>
<td>Forwarding rate</td>
<td>Specifies the portion of a web object that is forwarded every five seconds.</td>
</tr>
<tr>
<td></td>
<td>The forwarding rate is the thousandth part of the entire volume that is to be forwarded multiplied by the value you configure here.</td>
</tr>
</tbody>
</table>

**Progress Indication rule set**

The Progress Indication rule set is a library rule set for showing users the progress made in downloading a web object.

**Library rule set – Progress Indication**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Cycles</th>
</tr>
</thead>
<tbody>
<tr>
<td>MediaType.FromHeader does not equal text/html</td>
<td>Requests (and IM), responses, embedded objects</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when media that is sent from the web in response to the request submitted by a user not of the text or html type.

The rule set contains the following rules.

**Enable progress page**

`Header.Request.Get ("User-Agent") matches regex (*.mozilla.*)` → Stop Rule Set – Enable Progress Page <Default>

The rule enables a progress page for Mozilla browsers. The event settings specify what the progress page looks like, for example, the language it uses.

**FTP upload timeout prevention**


The rule enables the FTP Upload Progress Indication function if a file has been sent from a client for uploading to the web under the FTP protocol.

Messages indicating upload progress are then sent to the client during the upload to prevent a timeout that could occur on the client if the upload takes more time.

This could be due, for example, to scanning the file that is to be uploaded for infections by viruses and other malware.

**Enable data trickling**

`Always` → Stop Rule Set – Enable Data Trickling<Default>

The rule enables data trickling for all browsers that are not Mozilla. The event settings specify the chunk and block sizes used for the trickling.

**Bandwidth throttling**

You can limit the speed for uploading and downloading data to the appliance in a process also known as bandwidth throttling.

You can use bandwidth throttling, for example, to avoid a situation where the network performance you need for completing a particular task is impacted by other users who are individually uploading objects to the web or are requesting large downloads from the web.
Bandwidth throttling rules
Bandwidth throttling rules limit the transferring speed when user upload objects to the web or download them.

Events in bandwidth throttling rules
Two events are available for use in rules that control bandwidth throttling:

• **Throttle.Client** — Limits the speed of data transfer from a client to the appliance
  This is the case when a client sends a request for uploading an object to a web server and the request is intercepted on the appliance together with the object.

• **Throttle.Server** — Limits the speed of data transfer from a web server to the appliance
  In this case, there has been a client request to download an object from a web server, and after this request has been filtered on the appliance and forwarded, the web server sends the object in response.

Bandwidth throttling rule for uploads
The following is an example of a rule that can execute bandwidth throttling rule for uploads.

**Limit upload speed for hosts on throttling list**

*URL.Host is in list Upload Throttling List* → Continue – Throttle.Client (10)

The rule uses the **Throttle.Client** event to limit the speed with which uploads are performed to 10 Kbps if the web server that the data should be uploaded to is on a particular list.

In the criteria of the rule, the URL.Host property is used to retrieve the host name of the web server that is specified in the uploading request.

If the Upload Throttling List contains this name, the criteria is matched and the rule applies. The throttling event is then executed.

The Continue action lets rule processing continue with the next rule.

Bandwidth throttling rule for downloads
The following is an example of a rule that can execute bandwidth throttling rule for downloads.

**Limit download speed for media types on throttling list**

*MediaType.EnsuredTypes at least one in list MediaType Throttling List* → Continue – Throttle.Server (1000)

The rule uses the **Throttle.Server** event to limit the speed with which downloads are performed to 1000 Kbps if the web object that should be downloaded belongs to a media type on a particular list.

In the criteria of the rule, the MediaType.EnsuredTypes property is used to detect the media type of the web object that the web server sends. An object can also be found to belong to more than one type.

If any of these types is on the Media Type Throttling List, the criteria is matched and the rule applies. The throttling event is then executed.

The Continue action lets rule processing continue with the next rule.
**Bandwidth throttling rules and rule sets**

We recommend that you create an overall rule set for bandwidth throttling rules and embed two rule sets in it, one for throttling uploads and another for throttling downloads. You can then let the embedded upload rule set apply for the request cycle and the embedded download rule set for the response cycle.

Within each embedded rule set, you can have multiple throttling rules that apply to different kinds of web objects.

The overall rule set for bandwidth throttling should be placed at the beginning of your rule set system. If this is not done, rules in other rule sets can start unthrottled downloads of web objects before your throttling rules are executed.

For example, a rule for virus and malware filtering could trigger the download of a web object that has been sent by a web server in response to a user request. The web object then needs to be completely downloaded to the appliance to see whether it is infected.

If your bandwidth throttling rule set is placed and processed after the rule set with the virus and malware filtering rule, bandwidth throttling is not applied to that download.

**Configure bandwidth throttling**

You can implement bandwidth throttling and configure it to adapt it to the needs of your network.

Complete the following high-level steps.

**Task**

1. Create lists of web objects for use by the bandwidth throttling rules.
   You can, for example, create the following:
   - A list of hosts that transferring speed is limited for when objects are uploaded to them
   - A list of media types that transferring speed is limited for when an object that belongs to one of these types is downloaded

2. Create a rule set for bandwidth throttling.

3. Within this rule set, create rules for bandwidth throttling.
   You can, for example, create the following:
   - A rule for limiting transferring speed when objects are uploaded to particular hosts.
   - A rule for limiting transferring speed when an object that belongs to a particular media type is downloaded.

4. Design these rules as needed.
   You can, for example, do the following:
   - Configure a particular transferring speed for the *Throttle.Client* event that enables bandwidth throttling for uploading objects to the web.
   - Configure a particular transferring speed for the *Throttle.Server* event that enables bandwidth throttling for downloading objects from the web.

5. Save your changes.
Web caching

A web cache is provided on the appliance for storing web objects to speed up responses to client requests.

Use of the appliance web cache is controlled by rules in a rule set.

To find out whether a web cache rule set is implemented on your appliance, review the system of rule sets on the Rule Sets tab of the Policy top-level menu.

If none is implemented, you can import the Web Cache library rule set. After importing this rule set, you can review and modify it on the Rule Sets tab to make it suit your network. Alternatively, you can create a rule set with rules of your own.

A web cache rule set typically contains rules for reading objects from the cache and writing them to it. Additionally, there can be bypass rules that exclude objects from being read or written.

Verify the enabling of the web cache

You can verify whether the web cache is enabled.

Task

1. Select Configuration Appliances.

2. On the appliances tree, select the appliance that you want to verify enabling of the web cache for and click Proxies (HTTP(S), FTP, ICAP, and IM).

3. Scroll down to the Web Cache section and see whether Enable Cache is selected. If necessary, enable this option.

4. If necessary, click Save Changes.

Web Cache rule set

The Web Cache rule set is a library rule set for web caching.

<table>
<thead>
<tr>
<th>Library rule set – Web Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
<tr>
<td>and responses</td>
</tr>
</tbody>
</table>

The following rule sets are nested in this rule set:

- Read from Cache
- Write to Cache

Read from Cache

This nested rule set enables the reading of web objects from the cache and forbids it for URLs that are on a bypassing list.

<table>
<thead>
<tr>
<th>Nested library rule set – Read from Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.
Skip caching URLs that are in Web Cache URL Bypass List

URL matches in list Web Cache URL Bypass List -> Stop Rule Set

The rule uses the URL property to check for requested URLs whether they are on the specified bypass list.

If they are, processing of the rule set stops. The rule that enables reading from the cache is then not processed.

Processing continues with the next rule set.

The rule is not enabled by default.

Enable Web Cache

Always -> Continue — Enable Web Cache

The rule is always processed unless it is skipped because the bypassing rule placed before it in the rule set applies. It enables the web cache, so objects stored in it can be read.

Processing continues with the next rule set.

Write to Cache

This nested rule set enables the writing of web objects to the cache and forbids it for large objects, as well as for URLs and media types on particular bypassing lists.

<table>
<thead>
<tr>
<th>Nested library rule set – Write to Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Responses</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.

Skip caching URLs that are in Web Cache URL Bypass List

URL matches in list Web Cache URL Bypass List -> Stop Rule Set

The rule uses the URL property to check for requested URLs whether they are on the specified bypass list.

If they are, processing of the rule set stops. The rule that enables reading from the cache is then not processed.

Processing continues with the next rule set.

The rule is not enabled by default.
Processing continues with the next rule set.
The rule is not enabled by default.

**Enable Web Cache**

*Always -> Continue — Enable Web Cache*

The rule is always processed unless it is skipped because the bypassing rule placed before it in the rule set applies. It enables the web cache, so objects stored in it can be read.

Processing continues with the next rule set.

---

### Next-hop proxies

Next-hop proxies can be used as an additional means of forwarding requests received from the clients of an appliance to their destinations.

When next-hop proxies are implemented, a rule in a corresponding rule set uses a module (also known as *engine*) to call next-hop proxies that have been entered into a list for forwarding requests.

For example, you can forward requests that have internal destinations using internal next-hop proxies. IP addresses of destinations that are internal are then entered into a list, which the forwarding rule relies on. In addition to this, there is a list of internal next-hop proxies for use by the rule.

A rule set with a rule for using next-hop proxies is not implemented on the appliance after the initial setup. You can import a rule set from the library and modify it according to your needs or create a rule set of your own.

When you import the next-hop proxy rule set, a list of servers that can be used as next-hop proxies is also imported. The list is initially empty and must be filled by you. You can also create more than one list and use these lists for routing in different situations.

Settings for the next-hop proxy module are imported with the library rule set. You can configure these settings to let the module use a particular next-hop proxy list and to determine the mode of calling the next-hop proxies (round-robin or failover).

### Next-hop proxy modes

When multiple servers are available as next-hop proxies for routing requests, the next-hop proxy module can use several modes to call them: Round-robin, failover, and stickiness.

**Round-robin mode for next-hop proxies**

When routing a request in round-robin mode, the next-hop proxy module calls the next-hop proxy that is next on the list to the one that was called last time.

For the next request, this is handled in the same way, so all servers on the list will eventually have been used as next-hop proxies.
The following diagram shows a next-hop proxy configuration in round-robin mode.

![Diagram of next-hop proxies in round-robin mode]

**Figure 12-1  Next-hop proxies in round-robin mode**

The round-robin mode is configured as part of the settings for next-hop proxies.

**See also**

*Next Hop Proxy settings* on page 457

**Failover mode for next-hop proxies**

When routing a request in failover mode, the next-hop proxy module calls the first next-hop proxy on the list.

If this next-hop proxy fails to respond, the call is repeated until the configured number of retries is reached. Only then is the second next-hop proxy in the list tried. It is called in the same way as the first, and eventually the third next-hop proxy in the list is tried.

This is continued until a next-hop proxy responds or all next-hop proxies in the list were found to be unavailable.

The following diagram shows a next-hop proxy configuration in failover mode.

![Diagram of next-hop proxies in failover mode]

**Figure 12-2  Next-hop proxies in failover mode**

The failover mode is configured as part of the settings for next-hop proxies.
Next-hop proxy stickiness
A next-hop proxy can also be selected according to what is known as the "sticky" mode. In this mode, requests of a particular kind, for example, requests coming in from the same client of Web Gateway are directed to the same next-hop proxy.

The part of a request that qualifies it for being handled in sticky mode is configured as the value of a property on Web Gateway. An event in a rule sets the property to this value.

The name of the property that is configured to enable next-hop proxy stickiness is NextHopProxy.StickinessAttribute. If you want, for example, to let requests from the same client be directed to the same next-hop proxy, you can use the IP address of a client as the value for this property.

In addition to creating a rule, you must also select stickiness as an option within the settings for handling next-hop proxies. The settings also include an option for limiting the time that the next-hop proxy stickiness mode is applied.

Rule for configuring next-hop proxy stickiness
The following sample rule sets the NextHopProxy.StickinessAttribute property to the value of the Client.IP property to let requests with the same client IP address be directed to the same next-hop proxy.

Name
Set next-hop proxy stickiness attribute

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>-&gt;</td>
<td>Continue Set NextHopProxy.StickinessAttribute = IP.ToString(Client.IP)</td>
</tr>
</tbody>
</table>

The rule uses an event to set the NextHopProxy.StickinessAttribute property. As this property is of the string type, the value for the Client.IP property must be converted into a string before it can be used for setting the NextHopProxy.StickinessAttribute property.

See also
Next Hop Proxy settings on page 457
Configure next-hop proxy stickiness on page 450

Configure next-hop proxies
You can implement the use of next-hop proxies and configure it to adapt it to the needs of your network.

Complete the following high-level steps.

Task
1. Import the Next Hop Proxy rule set from the library.

2. Review the rules in this rule set and modify them as needed.
   You can, for example, do the following:
   - Edit the lists used by the next-hop proxy rule.
     A yellow triangle next to a list name means the list is initially empty and you need to fill the entries.
   - Configure the settings of the Next Hop Proxy module
3  Save your changes.

**Add a next-hop proxy to a list**
To add a next-hop proxy to a list, complete the following steps.

**Task**
1  Open the Edit Settings window for settings of the Next Hop Proxy module.
2  Under Next Hop Proxy Server, select a next-hop proxy list from List of next-hop proxy servers and click Edit.
   The Edit List (Next Hop Proxy Server) window opens.
3  Under List Content, click the Add icon.
   The Add Next Hop Proxy window opens.
4  Configure settings for a next-hop proxy as needed.
5  Click OK for all open windows.
6  Click Save Changes.

The next-hop proxy is added to the list that you selected.

*See also*
*Add Next Hop Proxy settings on page 457*

**Configure the Next Hop Proxy module**
You can configure the Next Hop Proxy module to modify the way next-hop proxies are used for forwarding requests to the web.

**Task**
1  Select Policy | Rule Sets.
2  On the rule sets tree, select the rule set for next-hop proxies.
   If you have implemented the library rule set for this function, this is the Next Hop Proxy rule set.
   The rules of the rule set appear on the settings pane.
3  Make sure Show details is selected.
4  Find the rule that calls the Next Hop Proxy module.
   In the library rule set, this is the rule *Use internal proxy for internal host*.
5  In the rule event, click the settings name.
   In the library rule set, this name is *Internal Proxy*.
   The Edit Settings window opens. It provides the settings for the Next Hop Proxy module.
6  Configure these settings as needed.
7  Click OK to close the window.
8  Click Save Changes.

*See also*
*Next Hop Proxy rule set on page 459*
Configure next-hop proxy stickiness

To configure next-hop proxy stickiness, select this mode in the Next Hop Proxy settings and add a stickiness rule to a rule set for handling next-hop proxies.

Task

1. Select the stickiness mode for next-hop proxies.
   a. Select Policy | Settings.
   b. On the Engines branch of the settings tree, expand Next Hop Proxy and select the settings that you want to configure next-hop proxy stickiness for.
   c. Under Next Hop Proxy Server select Sticky.
   d. Under Minimum time for stickiness, modify the time period during which the stickiness mode is applied as needed.

2. Add a rule for next-hop proxy stickiness.
   b. Open a rule set for next-hop proxy handling, for example, the Next Hop Proxy library rule set.
   c. Add a rule that sets the NextHopProxy.Stickiness.Attribute property to the value for identifying the requests that are directed to the same proxy.

3. Click Save Changes.

Requests that contain the part specified in the additional rule are now directed to the same next-hop proxy during the configured time period.

See also

Next Hop Proxy settings on page 457
Next-hop proxy stickiness on page 448

Next-hop proxies for SOCKS traffic

A next-hop proxy can be configured to forward web traffic under the SOCKS (Sockets) protocol. Under this protocol, web traffic also follows an embedded protocol, which can be detected on Web Gateway. If the embedded protocol is HTTP or HTTPS, web traffic can be filtered according to the configured rules.

Versions 4 and 5 of the SOCKS protocol can be used for forwarding web traffic. When setting up a next-hop proxy, you can configure the SOCKS version to use. By default, the version of the incoming traffic is also used when it is forwarded.
Configure a next-hop proxy for SOCKS traffic
To configure a next-hop proxy for SOCKS traffic, let Web Gateway run as a SOCKS proxy and implement suitable rule sets for enabling a next-hop proxy and filtering the traffic.

Tasks

- **Enable a SOCKS proxy on page 451**
  Enable Web Gateway to run as a SOCKS proxy by configuring the proxies settings accordingly.

- **Configure a next-hop proxy rule set for SOCKS traffic on page 451**
  To configure a rule set for SOCKS traffic, modify the criteria of the Next Hop Proxy library rule set and add a rule that enables a next-hop proxy under the SOCKS protocol.

- **Configure the SOCKS Proxy rule set on page 452**
  Configure a setting in the SOCKS Proxy rule set that is required for filtering traffic that is forwarded to next-hop proxies under the SOCKS protocol.

Enable a SOCKS proxy
Enable Web Gateway to run as a SOCKS proxy by configuring the proxies settings accordingly.

**Task**

1. Select Configuration | Appliances.
2. On the appliances tree, select the Web Gateway appliance that you want to configure for running as a SOCKS proxy and click Proxies.
3. Scroll down to the SOCKS Proxy section and select Enable SOCKS proxy.
4. Click Save Changes.

Configure a next-hop proxy rule set for SOCKS traffic
To configure a rule set for SOCKS traffic, modify the criteria of the Next Hop Proxy library rule set and add a rule that enables a next-hop proxy under the SOCKS protocol.

**Task**

1. Import the Next Hop Proxy library rule set from the library.
2. On the rule sets tree, move the rule set up and let it follow immediately after the rule set that you are using for authenticating users, for example, the Explicit Proxy Authentication and Authorization rule set.
3. Replace Always as the rule set criteria by Connection.Protocol equals "SOCKS".
4. Add a rule that enables a next-hop proxy.
   a. Configure the rule criteria to let the rule apply for particular requests.
      For example, use Client.IP matches in list Client IP as the rule criteria to let the rule apply only for requests sent from clients with an IP address that is on a particular list.
   b. Configure Continue as the rule action.
   c. Configure Enable Next Hop Proxy as the rule event.
d) Configure the settings of the rule event.
   • Add a next-hop proxy to the list of next-hop proxies.
     When adding the next-hop proxy, make sure that you specify the SOCKS parameters as needed.
   • Configure the remaining options as needed.

5) Click Save Changes.

You can add more rules to the Next Hop Proxy rule set, using different criteria each time for setting up a next-hop proxy.

See also
- Next Hop Proxy rule set on page 459
- Add a next-hop proxy to a list on page 449
- Add Next Hop Proxy settings on page 457
- Rules for enabling next-hop proxies for SOCKS traffic on page 452

Configure the SOCKS Proxy rule set
Configure a setting in the SOCKS Proxy rule set that is required for filtering traffic that is forwarded to next-hop proxies under the SOCKS protocol.

Task
1) Import the SOCKS Proxy rule set from the library.
   The rule set can be found under Common Rules.

2) On the rule sets tree, let the rule set follow immediately after the Next Hop Proxy rule set.

3) In the nested Protocol Detection rule set of the SOCKS Proxy rule set, click the settings for the Protocol Detector module.
   The default name of these settings is Default.
   The Edit Settings window opens.

4) Under Protocol Detector Options, select Determine next-hop proxy after receiving embedded data.

5) Click OK to close the window.

6) Click Save Changes.

For more information about the SOCKS Proxy rule set, see the Proxies chapter.

See also
- Protocol Detector settings on page 458

Rules for enabling next-hop proxies for SOCKS traffic
You can add various rules to the Next Hop Proxy rule set, using different criteria for setting up a next-hop proxy.

The following rule enables a next-hop proxy for a request that was received from a client of Web Gateway with an IP address that is on a particular list.

Name
Enable next-hop proxy for SOCKS traffic if received from listed client
Criteria Action
The rule uses the \texttt{Client.IP} property to check whether the IP address of the client that a request was received from is on the list.

In this case, an event enables a next-hop proxy for this traffic. The event is executed with particular settings that you can configure to specify, for example, the version of the SOCKS protocol that should be used.

The next rule enables a next-hop proxy if the embedded protocol under the SOCKS protocol is HTTP.

Name \textbf{Enable next-hop proxy for SOCKS traffic with embedded HTTP protocol}

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{ProtocolDetector.DetectedProtocol&lt;Default&gt; equals &quot;HTTP&quot;}</td>
<td>\texttt{Continue} \texttt{Enable Next Hop Proxy&lt;Embedded Protocol HTTP Next Hop Proxy&gt;}</td>
</tr>
</tbody>
</table>

The rule uses the \texttt{ProtocolDetector.DetectedProtocol<} property to check whether the embedded protocol is HTTP.

In this case, an event enables a next-hop proxy for this traffic. The event is executed with particular settings that you can configure to specify, for example, the version of the SOCKS protocol that should be used.

When using this rule, you also need to enable the option \textbf{Determine next-hop proxy after receiving embedded data} in the settings for the Protocol Detector module (or engine).

The next rule enables a next-hop proxy if the embedded protocol under the SOCKS protocol is HTTPS.

Name \textbf{Enable next-hop proxy for SOCKS traffic with embedded HTTPS protocol}

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{ProtocolDetector.DetectedProtocol&lt;Default&gt; equals &quot;HTTPS&quot;}</td>
<td>\texttt{Continue} \texttt{Enable Next Hop Proxy&lt;Embedded Protocol HTTPS Next Hop Proxy&gt;}</td>
</tr>
</tbody>
</table>

The rule uses the \texttt{ProtocolDetector.DetectedProtocol<} property to check whether the embedded protocol is HTTP.

In this case, an event enables a next-hop proxy for this traffic. The event is executed with particular settings that you can configure to specify, for example, the version of the SOCKS protocol that should be used.

When using this rule, you also need to enable the option \textbf{Determine next-hop proxy after receiving embedded data} in the settings for the Protocol Detector module (or engine).

The next rule enables a next-hop proxy for any embedded protocol under the SOCKS protocol.

Name \textbf{Enable next-hop proxy for SOCKS traffic with any embedded protocol}

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{Connection.Protocol.Parent equals &quot;SOCKS&quot;}</td>
<td>\texttt{Continue} \texttt{Enable Next Hop Proxy&lt;Embedded Protocol Next Hop Proxy&gt;}</td>
</tr>
</tbody>
</table>
The rule uses the `Connection.Protocol.Parent` property to check whether the SOCKS protocol appears as the parent protocol in a request for forwarding SOCKS traffic to the web. If SOCKS appears as the parent protocol, it means that there must be an embedded protocol.

In this case, an event enables a next-hop proxy for this traffic. The event is executed with particular settings that you can configure to specify, for example, the version of the SOCKS protocol that should be used.

The next rule is very similar to the preceding rule. It enables a next-hop proxy for traffic under the SOCKS protocol or traffic that goes on under the HTTP protocol directly, without being embedded in the SOCKS protocol.

Name

**Enable next-hop proxy for SOCKS traffic with any embedded protocol**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Connection.Protocol.Parent equals &quot;SOCKS&quot; OR</code></td>
<td>Continue</td>
</tr>
<tr>
<td><code>Connection.Protocol equals &quot;HTTP&quot;</code></td>
<td>Enable Next Hop Proxy&lt;Embedded Protocol Next Hop Proxy&gt;</td>
</tr>
</tbody>
</table>

See also

*Protocol Detector settings* on page 458

**Best practices - Troubleshooting next-hop proxy issues**

Reviewing the settings for next-hop proxies can help solve issues with connection delays or unavailability.

Next-hop proxy issues are indicated by alerts on the dashboard. Settings for next-hop proxies can be reviewed to troubleshoot these issues and also to ensure that next-hop proxies have appropriately been configured to enable cloud lookups for URL filtering and regular updates of other filtering information.

**Next-hop proxy alerts**

Alerts on the dashboard indicating next-hop proxy issues look like this.

- **Next hop proxy 10.44.44.44 has been marked as down for 10 seconds**
  
  This alert appears if, after trying to connect to a next-hop proxy, Web Gateway detects that the next-hop proxy is down and 10 seconds are configured as the waiting time until the next retry.
  
  The waiting time begins after the configured number of retries, which are performed immediately, have been completed unsuccessfully.

- **Connection to next hop proxy 10.44.44.44 failed**
  
  This alert appears, if after trying to connect to a next-hop proxy, Web Gateway detects that the next-hop proxy is down and no waiting time (0 seconds) is configured. After unsuccessfully completing the configured number of retries, Web Gateway immediately performs the next retry.

**Connection retry settings for next-hop proxies**

If you notice slowness on next-hop proxy connections, we recommend reviewing the connection retry settings, which are part of the *Next Hop Proxy* settings.

The settings include the number of retries Web Gateway performs after a failed connection attempt, and the waiting time before performing the next retry after the configured number of retries has been completed unsuccessfully.

We recommend configuring a low number of retries, for example, 3, and no waiting time at all.
Configuring the settings in this way does not prevent the alerts from appearing, but avoids unnecessary delay with connection retries.

Avoiding delay is also important, as sometimes a next-hop proxy can erroneously be marked as down on Web Gateway, which would make waiting until the next retry even less appropriate.

**Next-hop proxies for URL filtering**

Slowness or failure in URL filtering can also be related to the next-hop proxy configuration.

The settings for URL filtering are by default configured to let categorizations of URLs be looked up on a cloud server of the McAfee Global Threat Intelligence McAfee Global Threat Intelligence system if no category for a given URL can be found in the local database on a Web Gateway appliance.

Next-hop proxies can be configured for connecting to these servers as part of the **URL Filter** settings. If no next-hop proxies are configured or if the configuration settings are faulty, attempts to perform cloud lookups can fail or be slow.

**Next-hop proxies for updates**

You can also use next-hop proxies for connecting to the update servers, which provide regular updates for anti-malware filtering, URL filtering, and other activities. Next-hop proxies for updates are configured as part of the **Central Management** settings.

**See also**

- Review the connection retry settings for next-hop proxies on page 455
- Review the settings of next-hop proxies for URL filtering on page 456
- Review the settings of next-hop proxies for updates on page 456

**Review the connection retry settings for next-hop proxies**

Review the connection retry settings for next-hop proxies to troubleshoot connection issues.

The connection retry settings can cause additional delay on connections if not appropriately configured.

**Task**

1. Navigate to the connection retry settings for next-hop proxies.
   a. Select **Policy | Settings**.
   b. On the settings tree, expand **Next Hop Proxy** and click the settings that you want to review.
      The settings appear in the configuration pane.
   c. Under **Next Hop Proxy Server**, select a list of next-hop proxy servers and click **Edit**.
      The **Edit List (NextHopProxy)** window opens.
   d. From the **List Content** list, select a next-hop proxy and click **Edit**.
      The **Edit NextHopProxy** window opens.

2. Under **Next Hop Proxy Definition**, configure the following.
   a. Set **Number of retries** to 3.
   b. Set **After final failure wait** to 10 (seconds).

   Close all open windows when you are done.

3. Click **Save Changes**.
See also
Best practices - Troubleshooting next-hop proxy issues on page 454

Review the settings of next-hop proxies for URL filtering
Review the settings of next-hop proxies that are used in URL filtering to troubleshoot connection issues.
Next-hop proxies are used in URL filtering to connect to the cloud servers of the McAfee Global Threat Intelligence system.

Task
1. Select Policy | Settings.
2. On the settings tree, expand URL Filter and click the particular settings that you want to review.
   The settings appear in the configuration pane.
3. Scroll down to Advanced Settings and check whether one or more next-hop proxies are correctly configured under Proxy Settings.
4. Correct the settings as needed. If no next-hop proxy is configured, add settings for one or more of them.
5. Click Save Changes if you have modified or made additions to the settings.

See also
Best practices - Troubleshooting next-hop proxy issues on page 454

Review the settings of next-hop proxies for updates
Review the settings of next-hop proxies used for updates to troubleshoot connection issues.
Next-hop proxies are used for updates to connect to the various update servers.

Task
1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance that you want to review settings on and click Central Management.
3. Scroll down to Automatic Engine Updates and verify that the following applies:
   • Enable Update Proxies is selected.
   • One or more next-hop proxies are correctly configured under Update proxies.
4. Correct the settings as needed. If no next-hop proxy is configured, add settings for one or more of them.
5. Click Save Changes if you have modified or made additions to the settings.

See also
Best practices - Troubleshooting next-hop proxy issues on page 454
Next Hop Proxy settings
The Next Hop Proxy settings are used for configuring next-hop proxies to forward requests that have been received on the appliance to the web.

Next Hop Proxy Server
Settings for next-hop proxies

Table 12-5 Next Hop Proxy Server

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of next-hop proxy servers</td>
<td>Provides a list for selecting a next-hop proxy server list.</td>
</tr>
<tr>
<td>Round robin</td>
<td>When selected, the Next Hop Proxy module uses the next-hop proxy following the one in the list that has been used last. When the end of the list has been reached, the first next-hop proxy in the list is again selected.</td>
</tr>
<tr>
<td>Fail over</td>
<td>When selected, the Next Hop Proxy module tries the first next-hop proxy in the list first. If the first next-hop proxy fails to respond, it is retried until the configured retry maximum has been reached. Then the second next-hop proxy in the list is tried, and so on, until a server responds or all are found to be unavailable.</td>
</tr>
<tr>
<td>Sticky</td>
<td>When selected, the Next Hop Proxy module uses the same next-hop proxy over a time period that you can also configure.</td>
</tr>
<tr>
<td>Minimum time for stickiness</td>
<td>Sets the period of time (in seconds) that the same next-hop proxy is used for forwarding a request. The default time period is 300 seconds.</td>
</tr>
<tr>
<td>Proxy style requests</td>
<td>When selected, requests in proxy style are forwarded to the requested web servers using next-hop proxies. This options is selected by default.</td>
</tr>
</tbody>
</table>

Add Next Hop Proxy settings
The Add Next Hop Proxy settings are used for configuring a next-hop proxy that is added to a list of next-hop proxies.

Next Hop Proxy Definition
Settings for configuring a next-hop proxy

Table 12-6 Next Hop Proxy Definition

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Provides a plain-text description of the next-hop proxy.</td>
</tr>
<tr>
<td>Proxy address</td>
<td>Provides information on the host that the next-hop proxy resides on by specifying a host name or IP address and a port number.</td>
</tr>
<tr>
<td>Host</td>
<td>Specifies the name of the host or its IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the number of the port on the host that listens to requests for forwarding web traffic.</td>
</tr>
<tr>
<td>Proxy authentication</td>
<td>Provides information for the process of authenticating to the next-hop proxy by specifying a user name and setting a password.</td>
</tr>
<tr>
<td>User</td>
<td>Specifies a user name for authenticating to the next-hop proxy.</td>
</tr>
</tbody>
</table>
Table 12-6  Next Hop Proxy Definition (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Sets a password for authenticating to the next-hop proxy.</td>
</tr>
<tr>
<td>Connection behavior</td>
<td>Provides information on the behavior of the next-hop proxy by specifying several relevant parameters.</td>
</tr>
<tr>
<td>Number of retries</td>
<td>Limits the number of attempts to call the next-hop proxy after the first attempt failed. The default number of retries is 1.</td>
</tr>
<tr>
<td>After final failure wait</td>
<td>Limits the time (in seconds) that elapses before another next-hop proxy is tried when all attempts to call this next-hop proxy have failed. The default time is ten seconds.</td>
</tr>
<tr>
<td>Use persistent connections</td>
<td>When selected, the next-hop proxy uses persistent connections for forwarding web traffic.</td>
</tr>
</tbody>
</table>

SOCKS Specific Parameters

Settings for configuring a next-hop proxy under the SOCKS protocol

Table 12-7  Next Hop Proxy Definition

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOCKS version to use with next-hop proxy</td>
<td>Provides information on the protocol version that is used when a next-hop proxy forwards web traffic under the SOCKS protocol.</td>
</tr>
<tr>
<td>Same as incoming SOCKS connection</td>
<td>When selected, the next-hop proxy uses the version of the SOCKS protocol that is used by incoming traffic. The setting is selected by default.</td>
</tr>
<tr>
<td>SOCKS v4</td>
<td>When selected, the next-hop proxy uses version 4 of the SOCKS protocol.</td>
</tr>
<tr>
<td>SOCKS v5</td>
<td>When selected, the next-hop proxy uses version 5 of the SOCKS protocol.</td>
</tr>
</tbody>
</table>

Protocol Detector settings

The Protocol Detector settings are used for configuring the module (or engine) for handling activities that are related to processing traffic under the SOCKS protocol.

Protocol Detector Options

Setting for the Protocol Detector module

Table 12-8  Protocol Detector Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine next-hop proxy after receiving embedded data</td>
<td>When selected, the Protocol Detector module enables a next-hop proxy for forwarding SOCKS traffic under the HTTP or HTTPS protocol when this traffic is received on Web Gateway and it is detected that this traffic also follows one of these two protocols. The option is not selected by default.</td>
</tr>
</tbody>
</table>
Next Hop Proxy rule set

The Next Hop Proxy rule set is a library rule set for using next-hop proxies to forward requests to the appropriate destinations.

<table>
<thead>
<tr>
<th>Library rule set – Next Hop Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <strong>Always</strong></td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set contains the following rule.

**Use proxy depending on the destination**

- **URL.Destination.IP is in range list Next Hop Proxy IP Range List OR**
- **URL.Destination.IP is in list Next Hop Proxy IP List -> Continue — Enable Next Hop Proxy<Internal Proxy>**

The rule uses the **URL.Destination.IP** property to check whether an IP address that corresponds to a URL is in one of the ranges specified on a list or has been entered into a list directly. If it is, the rule uses an event to forward requests for these URLs through internal next-hop proxies.

The event settings specify settings that include the next-hop proxy list and the mode for calling proxies.
Supporting functions
Next-hop proxies
13 User messages

Messages can be sent to users when a filtering rule blocks their requests for web access or affects them in other ways.

When you are administering this process, you are mainly dealing with the following:

- **Messages** — Messages are sent to users to inform them that their requests for web access are blocked, or redirected, or that they need to authenticate.

- **Action settings** — Messages to users are part of the settings for the action that is explained in a message.

- **Templates** — Messages to users are based on templates, which can be edited using the Template Editor.

Default settings apply for user messages and their templates after the initial setup of the appliance, which you can review and modify as needed.

**Contents**

- Sending messages to users
- Edit the text of a user message
- Authenticate settings
- Block settings
- Redirect settings
- Templates tab
- Template Editor

**Sending messages to users**

Messages are sent to users to inform them about actions of the filtering rules that affect them. User messages belong to different types and are based on templates.

**Message types**

There are different types of user messages, according to the action that a message informs a user about.

- **Authenticate message** — Informs a user that authentication is required to access a URL

- **Block message** — Informs a user that a request was blocked for various reasons, for example, because a virus was detected in the requested object

- **Redirect message** — Informs a user that redirecting to another URL is needed for accessing the requested object
**Message templates**

Messages that are sent to users are based on templates. To modify what a message looks like, you need to adapt these templates. You can do this under the settings for an action.

Message templates contain standard text with variables. The variables are filled with values as needed in a given situation.

All variables used in message templates are also properties used by rules. For example, `URL` is a variable in a message text and a property when used in a rule to exempt URLs from filtering.

Different versions can exist of a particular template regarding:

- **Language** — English and other languages
- **File format** — html or txt

Activities that you can complete when editing a message template include the following:

- Select a language for the message
- Edit the message text
- Replace the variables in the template
- Specify a block reason for logging purposes (only for Block action templates)
- Specify a URL for redirecting (only for Redirect action templates)

**Message text and variables**

The following text and variables could be contained in a Block message that is sent to a user when access to a requested object has been blocked due to a virus infection of the object.

- **Standard text** — The transferred file contained a virus and was therefore blocked.
- **Variables** — as follows:
  - **URL** — URL that the user requested to access the file
    The variable used to display a URL is `$URL$`.
  - **Virus name** — Name of the found virus that caused the blocking of the file
    The variable used to display a virus name is `$List.Of.String.ByName(String)$`.

When editing a message template, you can select and insert variables from a list of properties. To serve as variables in message templates, these are converted into strings (if they are not strings already).

For this reason, it makes no sense to select “string converter” properties here, which are properties whose job it is to convert other data types into strings, for example, the `NumberToString(String)` property.
Template Editor

The Template Editor is a component of the user interface that allows you to work with templates for messages to users. You can access it in several ways.

- Select it under the Policy top-level menu.
- Select the settings for an action:
  - Under Policy | Settings
    - OR
  - In a rule of a rule set, after enabling the complete rules view and Show details.
Then click Edit within these settings for a template collection or an individual template.

Edit the text of a user message

You can edit the text of a user message to adapt it to the requirements of your network.

Task
2. Select the rule set of a rule that includes the action with the user message you want to edit.
   For example, select the Gateway Antimalware rule set.
   The rules of the rule set appear on the settings pane.
3. Make sure that Show Details is enabled.
4. In the appropriate rule, click the settings of the action with the user message.
   For example, in the rule Block if virus was found, click the Virus Found settings of the Block action.
   The Edit Settings window opens.
5. Next to the Template Name field, click Edit.
   The Template Editor opens.
6. On the templates tree, expand the appropriate action template folder, for example, Virus Found.
   The available language versions of the template appear.
7. Expand a language version, for example, en for English.
   The available message formats of the language version appear.
8. Select a format, for example, html.
   The content of the template appears on the configuration pane in the selected format. It contains the text of the user message.
   For example, in the HTML format of the English Virus Found template, this text reads initially:
   The transferred file contained a virus and was therefore blocked.
9. Edit the text as needed.
Authenticate settings

The **Authenticate** settings are used for configuring the way the Authenticate action is executed when a filtering rule with that action applies.

**Failed Login Message Template**

Settings for configuring user messages and a block reason for logging purposes

**Table 13-1  Failed Login Message Template**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Language</strong></td>
<td>Provides settings for selecting the language of a user message.</td>
</tr>
<tr>
<td>• Auto (Browser)</td>
<td>When selected, the message is in the language of the browser that the blocked request was sent from.</td>
</tr>
<tr>
<td>• Force to</td>
<td>When selected, the message is in the language chosen from the list that is provided here.</td>
</tr>
<tr>
<td>• Value of Message.Language property</td>
<td>When selected, the message is in the language that is the value of the Message.Language property. This property can be used for creating a rule.</td>
</tr>
<tr>
<td><strong>Template collection</strong></td>
<td>Provides a list for selecting a template collection.</td>
</tr>
<tr>
<td>• Add</td>
<td>Opens the Add Template Collection window for adding a template collection.</td>
</tr>
<tr>
<td>• Edit</td>
<td>Opens the Template Editor for editing a template collection.</td>
</tr>
<tr>
<td><strong>Template name</strong></td>
<td>Provides a list for selecting a template.</td>
</tr>
<tr>
<td>• Add</td>
<td>Opens the Add Template window for adding a template.</td>
</tr>
<tr>
<td>• Edit</td>
<td>Opens the Template Editor for editing a template.</td>
</tr>
<tr>
<td><strong>McAfee Web Reporter block reason ID</strong></td>
<td>Provides a numerical value that identifies a block reason.</td>
</tr>
<tr>
<td><strong>Block reason</strong></td>
<td>States the block reason in plain text.</td>
</tr>
</tbody>
</table>

See also

*List of block reason IDs on page 646*

Block settings

The **Block settings** are used for configuring the way the Block action is executed when a filtering rule with that action applies.

**Language and Template Settings**

Settings for configuring user messages and a block reason for logging purposes

10 Click **OK** to close the **Edit Settings** window.

11 Click **Save Changes**.

See also

_Template Editor on page 467_
Table 13-2 Language and Template Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Provides settings for selecting the language of a user message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto (Browser)</strong> — When selected, the message is in the language of the browser that the blocked request was sent from.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Force to</strong> — When selected, the message is in the language chosen from the list that is provided here.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Value of Message.Language property</strong> — When selected, the message is in the language that is the value of the <code>Message.Language</code> property.</td>
</tr>
<tr>
<td></td>
<td>This property can be used for creating a rule.</td>
</tr>
<tr>
<td>Template collection</td>
<td>Provides a list for selecting a template collection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> — Opens the <strong>Add Template Collection</strong> window for adding a template collection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> — Opens the Template Editor for editing a template collection.</td>
</tr>
<tr>
<td>Template name</td>
<td>Provides a list for selecting a template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> — Opens the <strong>Add Template</strong> window for adding a template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> — Opens the Template Editor for editing a template.</td>
</tr>
<tr>
<td>McAfee Web Reporter block reason ID</td>
<td>Provides a numerical value that identifies a block reason.</td>
</tr>
<tr>
<td>Block reason</td>
<td>States the block reason in plain text.</td>
</tr>
</tbody>
</table>

See also

[List of block reason IDs on page 646]

Redirect settings

The Redirect settings are used for configuring the way the Redirect action is executed when a filtering rule with that action applies.

Redirect Settings

Settings for configuring user messages and a block reason for logging purposes

Table 13-3 Redirect Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect.URL</td>
<td>When selected, the value of the <code>Redirect.URL</code> property is the URL that is used for redirecting.</td>
</tr>
<tr>
<td></td>
<td>This property can be used in a suitable rule.</td>
</tr>
<tr>
<td>User-defined URL</td>
<td>When selected, the redirecting URL must be specified by you</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>Specifies the URL for a redirecting URL.</td>
</tr>
</tbody>
</table>
### Table 13-3 Redirect Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Language</strong></td>
<td>Provides settings for selecting the language of a user message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto (Browser)</strong> — When selected, the message is in the language of the browser that the blocked request was sent from.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Force to</strong> — When selected, the message is in the language chosen from the list that is provided here.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Value of Message.Language property</strong> — When selected, the message is in the language that is the value of the <code>Message.Language</code> property.</td>
</tr>
<tr>
<td></td>
<td>This property can be used for creating a rule.</td>
</tr>
<tr>
<td><strong>Template collection</strong></td>
<td>Provides a list for selecting a template collection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> — Opens the <strong>Add Template Collection</strong> window for adding a template collection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> — Opens the Template Editor for editing a template collection.</td>
</tr>
<tr>
<td><strong>Template name</strong></td>
<td>Provides a list for selecting a template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> — Opens the <strong>Add Template</strong> window for adding a template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> — Opens the Template Editor for editing a template.</td>
</tr>
<tr>
<td><strong>McAfee Web Reporter</strong></td>
<td>Provides a numerical value that identifies a block reason.</td>
</tr>
<tr>
<td><strong>block reason ID</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Block reason</strong></td>
<td>States the block reason in plain text.</td>
</tr>
</tbody>
</table>
**Templates tab**

Use the Templates tab to work with templates for messages to Web Gateway users.

![Templates tab in McAfee Web Gateway](image)

**Figure 13-1  Templates tab**

You can access this tab from the Policy top-level menu.

The content of the tab also appears within the Template Editor. This editor opens when you select an action setting from the settings tree and click Edit for a template or template collection under Language and Template Settings.

**See also**

*Template Editor on page 467*

---

**Template Editor**

The Template Editor is a component of the user interface that allows you to work with templates for messages to the users of your network. The editor also provides templates for customizing the SSO application launchpad and logon pages and for SAML communication with an external Identity Provider.

**Templates**

Shows the existing templates in a tree structure.

The following table describes the Templates options.
Table 13-4  Templates

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>The templates are arranged in groups, which are also known as template collections. Each collection is stored in a top-level folder of the tree structure.</td>
</tr>
<tr>
<td>Template</td>
<td>The following template collections are available by default:</td>
</tr>
<tr>
<td>groups</td>
<td>• Default Schema — Provides user message templates that you can customize.</td>
</tr>
<tr>
<td></td>
<td>• Single Sign On Schema — Provides templates for SAML authentication requests (SAMLRequest.html) and responses (SAMLRedirectToAuth.html) sent to and received from an external Identity Provider, respectively.</td>
</tr>
<tr>
<td></td>
<td>• SAML Request Schema — Provides templates for customizing the application launchpad and logon pages.</td>
</tr>
<tr>
<td>Templates</td>
<td>Templates can exist in different language versions and formats.</td>
</tr>
<tr>
<td></td>
<td>All language versions and formats for a particular template are stored in a subfolder under the template name, for example, Anti-Malware Engine Overload.</td>
</tr>
<tr>
<td></td>
<td>Within each template folder, a subfolder for each language version is available for the template. A language version folder stores individual templates in different formats.</td>
</tr>
<tr>
<td></td>
<td>The available formats are HTML and .txt.</td>
</tr>
<tr>
<td></td>
<td>For example, the Anti-Malware Engine Overload folder contains:</td>
</tr>
<tr>
<td></td>
<td>• en — Subfolder with English versions of the template</td>
</tr>
<tr>
<td></td>
<td>• html — Template in HTML format</td>
</tr>
<tr>
<td></td>
<td>• txt — Template in .txt format</td>
</tr>
<tr>
<td></td>
<td>By default, there is an English version for each template in HTML format, while most templates are also available in .txt format.</td>
</tr>
<tr>
<td></td>
<td>When you click a template format, the template content appears on the HTML Editor pane.</td>
</tr>
<tr>
<td>Expand icon</td>
<td>Expands all collapsed items on the templates tree.</td>
</tr>
</tbody>
</table>
Table 13-4 Templates (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collapse icon</td>
<td>Collapses all expanded items.</td>
</tr>
<tr>
<td>Right-click a collection, template, language version, or format</td>
<td>Opens a menu with the following options. The selection of the options varies with the item that is right-clicked.</td>
</tr>
<tr>
<td>• Add Template Collection</td>
<td>Opens a window for adding a collection folder.</td>
</tr>
<tr>
<td>• Add Template</td>
<td>Opens a window for adding a template folder.</td>
</tr>
<tr>
<td>The new template folder contains a language version folder for the language that you selected when adding the folder and empty templates in the selected formats.</td>
<td></td>
</tr>
<tr>
<td>• Add Index File</td>
<td>Opens a window for adding a language version folder that does not belong to a particular template folder.</td>
</tr>
<tr>
<td>This folder is placed immediately under a collection folder. It contains empty templates in the formats that you selected.</td>
<td></td>
</tr>
<tr>
<td>• Add Content File</td>
<td>Opens a window for adding a language version folder within a particular template folder.</td>
</tr>
<tr>
<td>The new folder contains empty templates in the formats that you selected.</td>
<td></td>
</tr>
<tr>
<td>• Import Template Files</td>
<td>Opens a window for importing templates.</td>
</tr>
<tr>
<td>• Export Template Files</td>
<td>Opens a window for exporting templates.</td>
</tr>
<tr>
<td>• Clone</td>
<td>Opens a window for inserting a copy of a collection or template folder with content under a new name.</td>
</tr>
<tr>
<td>• Change</td>
<td>Opens a window for changing a language version.</td>
</tr>
<tr>
<td>• Rename</td>
<td>Opens a window for renaming a template folder.</td>
</tr>
<tr>
<td>• Delete</td>
<td>Deletes an item.</td>
</tr>
<tr>
<td>A window opens to let you confirm the deletion.</td>
<td></td>
</tr>
</tbody>
</table>

**File System**

Shows the existing templates, as well as image and other files that are related to templates, in a tree structure.

The following table describes the **File System** options.
### Table 13-5 File System

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template groups</td>
<td>The templates are arranged in groups. Each group is stored in a top-level folder of the tree structure.</td>
</tr>
<tr>
<td></td>
<td>The following template groups are available by default:</td>
</tr>
<tr>
<td></td>
<td>• SAML</td>
</tr>
<tr>
<td></td>
<td>• default</td>
</tr>
<tr>
<td></td>
<td>• singleSignOn</td>
</tr>
<tr>
<td>Templates, images, and other related files</td>
<td>Within each group folder, templates are stored in alphabetical order within language version folders, while image files are stored in a separate folder.</td>
</tr>
<tr>
<td></td>
<td>Other related files can be stored in a group folder outside the language version and image folders.</td>
</tr>
<tr>
<td></td>
<td>For example, the default group folder contains:</td>
</tr>
<tr>
<td></td>
<td>• en — Subfolder with English versions of all existing templates</td>
</tr>
<tr>
<td></td>
<td>• img — Subfolder with all existing image files</td>
</tr>
<tr>
<td></td>
<td>• Related files, such as index and style sheet files</td>
</tr>
<tr>
<td></td>
<td>When you click a template format, the template content appears on the HTML Editor pane.</td>
</tr>
<tr>
<td>Add</td>
<td>Opens the following menu:</td>
</tr>
<tr>
<td></td>
<td>• New File — Opens a window for adding a file.</td>
</tr>
<tr>
<td></td>
<td>• New Directory — Opens a window for adding a directory.</td>
</tr>
<tr>
<td></td>
<td>• Existing File or Directory — Opens the local file manager for selecting and adding a file or folder.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the following menu:</td>
</tr>
<tr>
<td></td>
<td>• Rename — Opens a window for renaming an item.</td>
</tr>
<tr>
<td></td>
<td>• Delete — Deletes an item.</td>
</tr>
<tr>
<td></td>
<td>A window opens to let you confirm the deletion.</td>
</tr>
<tr>
<td>Cut</td>
<td>Copies and deletes a selected item.</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies a selected item.</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes a cut out or copied item.</td>
</tr>
<tr>
<td>Expand icon</td>
<td>Expands all collapsed items on the file system tree.</td>
</tr>
<tr>
<td>Collapse icon</td>
<td>Lets all expanded items collapse.</td>
</tr>
</tbody>
</table>

Right-clicking an item opens a menu with the preceding options, except for the expand and collapse options. Options that do not apply for an item are grayed out.

**HTML Editor**

Displays the content of the template that is selected on the Templates or File System pane for editing.

The following table describes the HTML Editor options.
### Table 13-6 HTML Editor

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Add      | Opens the following menu:  
  - **Resource Reference** — Opens a window for entering the path to a resource, such as an image or other graphical element, that is inserted into a template.  
  - **Property** — Opens a window for adding a property that appears as a variable in a template, for example, $URL$. |
| Edit     | Opens the following menu:  
  - **Cut** — Copies and deletes a selected portion of template content.  
  - **Copy** — Copies a selected portion.  
  - **Paste** — Pastes a copied portion.  
  - **Delete** — Deletes a selected portion.  
  - **Select All** — Selects the complete template content. |
| Show Source | Shows or hides the HTML source code of a template (toggle button). |
| Languages drop-down list | Lets you select the language of the preview. |
| Preview  | Shows a preview of a template. |

### Viewer

Displays the image contained in a selected image file.

The **Viewer** is made available (instead of the **HTML Editor**) when an image file is selected on the file system tree.

The following table describes the **Viewer** options.

### Table 13-7 Viewer

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zoom In</td>
<td>Enlarges an image.</td>
</tr>
<tr>
<td>Zoom Out</td>
<td>Shrinks an image.</td>
</tr>
<tr>
<td>Fit to Window</td>
<td>Lets an image fill out the <strong>Viewer</strong> pane completely.</td>
</tr>
<tr>
<td>Original Size</td>
<td>Displays an image in its original size again.</td>
</tr>
</tbody>
</table>
Cloud single sign-on (SSO) is the Web Gateway service that allows end users in your organization to access cloud services and applications after providing credentials one time. The SSO service is implemented by the Single Sign On module.

In the context of cloud single sign-on, unless otherwise noted, the following terms are used as described here:

- The terms *cloud service* and *cloud application* are used interchangeably.
- The term *user* refers to the end user in your organization who seeks access to cloud services and applications. Using the launchpad provided by Web Gateway, users submit credentials, open applications, and manage their accounts in the applications.
- The term *user interface* refers to the Web Gateway user interface where administrators configure the SSO service.
- The term *custom connector* refers to any cloud connector configured from a template. Web Gateway provides a range of connector templates. Some templates come with most, but not all, configuration built in. Other templates allow you to build cloud connectors from scratch.

Contents

- How cloud single sign-on is configured
- SSO process in proxy and non-proxy modes
- Supported authentication methods
- SSO Catalog of supported cloud services
- SSO Connector lists
- Providing SSO services for HTTP cloud applications
- Providing SSO services for SAML 2.0 cloud applications
- SAML authentication using an external Identity Provider
- Providing SSO services for .NET and Java web applications
- How the end user works with the application launchpad
- Customizing the application launchpad
- Creating bookmarks to cloud services for your organization
- Monitoring logons to cloud services on the dashboard
- Single Sign On rule set summary
- Key elements for configuring cloud single sign-on
- Single Sign On rule set reference
- Single Sign On lists and settings
- SSO logging overview
- Resolving SSO issues
How cloud single sign-on is configured

To configure SSO access to cloud services and applications, complete the following high-level tasks.

SSO tasks require the Single Sign On rule set, which you import from the Rule Set Library. All SSO tasks can be performed using the default rules, settings, and lists visible in the key elements view of this rule set. To view the rules making up the rule set and create rules, settings, and lists of your own, unlock the key elements view.

**Task**

1. Configure a method for authenticating users.

2. Import the Single Sign On rule set from the rule sets library and configure the rules.

   The Single Sign On rule set is located in the Cloud Services rule set group. You can configure the rules in the key elements view or click Unlock View to view configuration details as well as configure rules of your own.

3. Configure the Single Sign On settings for the Single Sign On module, which retrieves values and parameters for SSO properties and events in the Single Sign On rule set. This module comes with default settings named Default. In the SSO rules, properties and events that require these settings reference them using the notation <Default>. You can modify the default settings or create new settings.

   To locate these settings, select Policy | Settings | Engines | Single Sign On | Default.

4. For single sign-on to SAML and IceToken cloud services, configure an X.509 certificate and private key pair.

   To locate these settings, select Policy | Settings | Engines, then select SSO Certificates or SSO Private Keys, respectively.

5. Using SSO lists, you can configure custom cloud connectors from templates and lists of connectors to cloud services that users are allowed to access.

   - **SSO Host to Service ID mapping** — (Optional) Lets you map a name that is easy to remember (host name) to the Service ID of a configured custom connector.

     To locate this list, select Policy | Lists | Custom Lists | MapType.

   - **SSO Connector** — Lets you configure lists of connectors to services that users are allowed to access. You can add connectors to the default lists that come with the SSO service or create and configure lists of your own.

     To locate the SSO Services lists, select Policy | Lists | Custom Lists | SSO Connector.

   - **SSO Catalog** — Lets you view the predefined connectors and the custom connectors configured from templates. You can configure new connectors from templates, then view them in the Custom connectors list.

     To locate the catalog, select Policy | Lists | System Lists.

6. We recommend that you secure all launchpad communication with the HTTPS protocol. To do so, configure the Launchpad certificate settings used by the SSL Client Context without CA module, which handles certificates for SSL-secured communication.

   To locate the Launchpad certificate settings: In the key elements view, locate SSL Scanner settings, then click Edit.
7 To secure communication between Web Gateway and all cloud services with the HTTPS protocol, configure the SSL Scanner module settings. This step is required for proxy mode.

8 To require OTP authentication for SSO access to cloud services, enable OTP authentication, configure the OTP server settings, select an OTP delivery method, and configure the list of connectors to services that require OTP authentication.

To locate these settings: In the key elements view, see the OTP Usage (One Time Passwords) section.

9 To log SSO requests to the SSO access log instead of the general access log, enable SSO logging. To enable detailed logging for debugging purposes, enable SSO trace logging.

To access these settings, select Policy | Rule Sets | Log Handler, then import the SSO Log rule set from the Logging rule set group in the Rule Set Library.

10 Save the changes.

**SSO process in proxy and non-proxy modes**

The steps in the SSO process depend on whether the user's credentials are submitted to the cloud application directly (non-proxy mode) or through Web Gateway (proxy or inline mode).

In proxy and non-proxy modes, Web Gateway authenticates the user, then presents the launchpad. The launchpad displays icons corresponding to the cloud applications the user is allowed to access. The SSO process appears the same to the user in both modes:

1 From a web browser on a client of Web Gateway, the user requests a launchpad.

2 After authenticating the user, Web Gateway sends a launchpad.

3 To open an application, the user clicks the icon corresponding to the application on the launchpad.

4 Web Gateway sends a logon form to the user.

5 If requesting access for the first time, the user is prompted for credentials, which the user provides and submits to Web Gateway. If requesting access for a second or later time, the logon form is automatically filled with the user's credentials and submitted to Web Gateway.

6 If the credentials are valid, the user is allowed SSO access to the cloud application.
Proxy mode

In proxy mode, Web Gateway forwards the user's credentials to the cloud application.

![Diagram of Proxy mode](image)

**Figure 14-1 Single sign-on in proxy mode**

When single sign-on takes place in proxy mode, Web Gateway can provide additional functionality that is not available in non-proxy mode:

- **Dynamic cloud applications** — Web Gateway can support HTTP cloud applications that provide logon page information dynamically, such as DropBox, by adding Javascript to the logon page. The Javascript completes the fields on the page with information.

- **Encrypted password** — The password is encrypted and hidden from the client computer.

Non-proxy mode

In non-proxy mode, the user's browser forwards the credentials to the cloud application.

![Diagram of Non-proxy mode](image)

**Figure 14-2 Single sign-on in non-proxy mode**

When single sign-on takes place in non-proxy mode, Web Gateway functions as a web server. When configuring your Domain Name Service and all SSO settings, you must use the IP address of the Web Gateway appliance in place of a host name.
Supported authentication methods

Generally, each cloud service or application uses one authentication method to log on end users.

Web Gateway provides SSO services for cloud applications that use HTTP or SAML 2.0 authentication. Web Gateway also provides SSO services for cloud applications using a proprietary authentication method implemented through a custom token named IceToken.

Cloud connectors

Web Gateway supports many HTTP and SAML 2.0 cloud applications with individual cloud connectors. A cloud connector is the configuration that allows Web Gateway to connect to and provide identity and SSO services for an application in the cloud. Predefined cloud connectors come fully configured with Web Gateway. Cloud connector templates come partly configured and require some configuration before they can be used.

SSO data sources

The data source from which Web Gateway obtains the end user's credentials or information depends on whether single sign-on is to an HTTP or SAML service.

- **HTTP services** — Web Gateway uses an integrated credential store: a secure database that stores credentials like the user names and passwords required by HTTP services. Users who seek access to an HTTP service must first authenticate against the database.

- **SAML services** — Web Gateway retrieves identity information from an external data source and produces a SAML assertion attesting to the user's identity.

See also

*Configuring external data sources for SAML single sign-on on page 496*

SSO Catalog of supported cloud services

The SSO Catalog consists of all cloud applications and services supported by Web Gateway with cloud connectors.

Connectors can be fully configured (predefined connectors) or templates that you can select and fully configure (custom connectors). The catalog also includes all connectors configured from templates by administrators. Connectors allow end users in your organization to access hundreds of cloud applications and services after authenticating one time.

A cloud connector is the configuration that allows Web Gateway to connect to and provide identity and SSO services for a cloud service or application. Each configured connector is saved in a file and includes information like the following:

- Information about the cloud service, such as name and category
- URLs needed for the SSO process
- Pages containing logon forms
- Data for generating the launchpad
Viewing the SSO Catalog
You can view the SSO Catalog in the user interface or in a technical note that can be downloaded in PDF format.

User interface
The user interface provides the most comprehensive and up-to-date view of the SSO Catalog. It includes all components making up the catalog: predefined connectors, connector templates, and custom connectors configured from connector templates by administrators.

The catalog is implemented as a system list. Like other system lists, it is updated between Web Gateway releases. Changes are delivered by update servers and can be viewed in the user interface. New connectors are added, and whenever possible, broken connectors are fixed. Connectors that are no longer supported are highlighted and the change is noted.

The system list consists of the following sublists. To view the sublists in the user interface, select Policy | Lists. In the Lists tree, expand System Lists | SSO Catalog.

- **Predefined connectors** — These connectors come fully configured with Web Gateway and only need selecting from the catalog.

- **Custom connectors** — These connectors are configured from templates that come with some, but not all, configuration built in. Custom connectors require configuration before they can be added to the catalog and selected.

In the user interface, predefined connectors and connector templates are organized by the names of the cloud applications and services they support. Custom connectors configured from connector templates are organized by the names that you specify.

To view the connector templates from which you configure custom connectors, select Policy | Lists. In the Lists tree, expand System Lists | SSO Catalog. Select Custom connectors, then click the Add icon. In the Add Connector dialog box, open the Template drop-down list. Notice that the generic connector templates are at the top of the list.

Custom connectors include any connector that you configure from a template for your situation. Connectors configured from generic templates (like generic HTTP and generic SAML 2.0) are custom connectors.

Technical note
The technical note is a snapshot of the SSO Catalog taken each time there is a major release of Web Gateway. It is not updated each time there is a release of the SSO Catalog.

The technical note lists all predefined connectors and connector templates in a single location. It includes the authentication method used by each service and optionally, a note describing the status of the service. For example, if a connector is no longer supported or has been renamed, this status is noted.

The technical note does not include custom connectors, which do not exist until they are configured from a connector template by an administrator.

SSO Catalog in the user interface
Predefined and custom connectors are listed in table format. While the tables include the same information, the details differ for each type of list.

Predefined connector values are provided by the Single Sign On module and cannot be changed. Custom connector values, which administrators configure, can be changed.
### Column heading | Description
---|---
Icon | Displays the logo that represents the cloud application or service. When configuring a custom connector, you can specify a custom image.
Name | Uniquely identifies the predefined connector or custom connector instance.  
- **Predefined connectors** — Displays the name of the cloud application or service and can include spaces.  
  Example: Air Canada  
- **Custom connectors** — Displays the name that you configure for each connector instance.  
  From one connector template, you can configure multiple connector instances. For example, you can configure one connector instance for each user group and assign the instances different names, as follows:  
  - Google Calendar - IT  
  - Google Calendar - Sales
Description | (Custom connectors) Allows you to provide a description for each connector instance.
Categories | Specifies the type of service provided by the cloud application or service. When configuring a custom connector, you can change the default category or create a new one.  
Examples: Collaboration, Marketing, Social
Service ID | Predefined connectors — Specifies a name that uniquely identifies the predefined connector in the SSO Catalog. Typically, the service ID is the same as the name with the spaces removed.  
Example: AirCanada  
- Custom connectors — Specifies a number that uniquely identifies the custom connector in the SSO Catalog. This number is set by the Single Sign On module and cannot be changed.
Types | Specifies the method that each cloud application or service uses to authenticate end users. Sometimes, applications and services are referred to by type, such as an HTTP application or a SAML service. This value is set by the Single Sign On module.

### SSO Catalog as a service
The SSO Catalog is a cloud service. As a cloud service, it is updated between Web Gateway releases.

The SSO Catalog is also known as the Connector Catalog as a Service (CCaaS).

Occasionally, a Service Provider changes the configuration details required for connecting to a cloud service or stops providing a cloud service altogether. These changes, which can break the connector to a service temporarily or permanently, require modifications to the SSO Catalog. Modifications, including new and fixed connectors, are delivered by update servers.

When the catalog is updated, an update message is displayed in the Web Gateway user interface. Broken connectors for which no resolution is planned are no longer supported and are flagged in the user interface as follows:
- **SSO Catalog**
  
  - **Connectors** — Predefined and custom connectors that are no longer supported are available for selection in the catalog. However, they are flagged with a yellow triangle and *No longer supported* message.
  
  - **Templates** — Templates for custom connectors that are no longer supported are available for selection in the catalog and can be configured. However, they are flagged with a yellow triangle and *No longer supported* message.
  
  - **SSO Connector lists** — SSO Connector lists are custom lists of connectors to cloud services that end users are allowed to access. Connector lists containing connectors that are no longer supported are highlighted in yellow. Connectors in connector lists that are no longer supported are highlighted in yellow and flagged with a *No longer supported* message.

**Generic vs. individual connector templates**

Generic cloud connector templates support any cloud application that uses the specified authentication method. Because generic templates are more flexible than individual connector templates, they require more configuration.

**Individual connector templates**

Individual cloud connector templates provide the basis for configuring a connection to a specific cloud application. For example, the Salesforce connector template allows you to configure a custom connection to the Salesforce application in the cloud.

Because templates are configurable, you can create multiple custom connectors to a single cloud application such as Salesforce. To identify custom connectors, you assign them unique names.

**Generic connector templates**

Generic cloud connector templates allow you to configure a connection to any cloud application that uses the specified authentication method. For example, using the Generic HTTP Connector template, you can configure a connection to any cloud application that uses HTTP authentication to log on users. Generic templates allow you to configure connectors to cloud applications not found in the SSO Catalog.

Web Gateway provides generic cloud connector templates for the following authentication methods.

- **Generic HTTP connector** — Select this template when you want to configure a connector to an HTTP service that Web Gateway does not support with an individual connector.

- **Generic SAML2 connector** — Select this template when you want to configure a connector to a SAML 2.0 service that Web Gateway does not support with an individual connector.

- **Generic IceToken connector** — Select this template when you want to configure a connector to a service that uses an authentication method which Web Gateway does not support.

**See also**

- Configure an HTTP cloud connector on page 484
- Configure a generic HTTP cloud connector on page 484
- Configure a SAML2 cloud connector on page 491
- Configure a generic SAML2 cloud connector on page 492
- Configure a generic IceToken cloud connector on page 512
Configure a custom cloud connector using a template

After you configure a connector to a cloud service from a template, end users in your organization can access the service without authenticating more than one time.

**Task**

1. Select Policy | Lists.

2. In the Lists tree, expand System Lists | SSO Catalog, then click Custom connectors.

3. Click the Add icon.

   The Add Connector dialog box opens.

4. Provide values for the following fields and settings:
   - **Name** — Specifies a name that uniquely identifies the cloud connector instance.
   - **Description** — (Optional) Describes the cloud connector instance.
   - **Template** — From the drop-down list, select the template corresponding to the cloud service for which you want to configure SSO access.
     Template-specific settings open.
   - **Categories** — Specifies the type of service provided by the cloud service or application. When you select the template, a default value is loaded automatically. You can modify this value by clicking Choose.
   - **Browse** — Allows you to add or modify the logo that represents the cloud connector you are creating.

5. Configure the template-specific settings.

6. Click OK.

   The newly configured cloud connector is added to the SSO Catalog. To view the connector in the catalog, select Custom connectors.

Delete a custom cloud connector

You can remove a custom cloud connector from the SSO Catalog if it is not included in any SSO Connector list. Custom cloud connectors are connectors configured from templates.

Removing a custom cloud connector from the SSO Catalog removes all end user credentials entered for that connector. Recreating the connector with the same settings does not restore the user credentials that were lost when the connector was removed.

**Task**

1. Select Policy | Lists.

2. In the Lists tree, expand System Lists | SSO Catalog, then click Custom connectors.

3. Select the custom cloud connector you want to delete, then click the Delete icon.

   The Confirm deletion dialog box opens.

4. To confirm the deletion, click Yes.

   The custom cloud connector is removed from the SSO Catalog.
Locate information about the latest SSO updates

When working with the cloud single sign-on feature, you might want to know which version of the software and the catalog you are using. In the user interface, you can view the version number and date and time of the latest updates to the SSO feature or engine.

- **McAfee Single Sign On** — Updates include changes to the SSO software, for example, a change to an SSO rule.
- **McAfee SSO Connector Catalog** — Updates include changes to the list of cloud applications and services that Web Gateway supports with connectors.

If you are not receiving SSO updates, confirm that you have a valid license.

**Task**

1. Select **Dashboard | Charts and Tables | System Summary**.
2. To view the version numbers of the latest SSO updates: In the **Update Status** table, in the **Feature** column, locate the following rows:
   - **McAfee Single Sign On**
   - **McAfee SSO Connector Catalog**
3. To view the date and time of the latest SSO updates: In the **Last Update** table, in the **Engine** column, locate the following rows:
   - **McAfee Single Sign On**
   - **McAfee SSO Connector Catalog**
4. To refresh the view with the latest data, click the refresh icon in the upper right corner of the **Update Status** and **Last Update** tables.

**SSO Connector lists**

Web Gateway uses SSO Connector lists to control access to cloud services and applications.

**Configuring cloud access through SSO Connector lists**

Access to cloud services and applications is configured through lists of cloud connectors, each connector corresponding to a supported service in the SSO Catalog.

Some SSO Connector lists enable access. Other lists might require OTP authentication before access is permitted. Users are associated with lists through Web Gateway policies.

You can view the connectors in the catalog and select them when adding connectors to a connector list. The SSO Catalog organizes cloud connectors in two groups:

- **Predefined connectors** — These connectors come fully configured with Web Gateway and only need selecting from the catalog.
- **Custom connectors** — These connectors are configured from templates that come with some, but not all, configuration built in. Custom connectors require configuration before they can be added to the catalog and selected.

  *Generic* connectors are a special type of custom connector.

Configuring access to a cloud service involves the following overall steps:
1. (Custom connectors) Configure a cloud connector to the cloud service you want users to access. The connector is added to the SSO Catalog.

2. Select the predefined or custom cloud connector from the SSO Catalog and add it to an SSO Connector list.

Add a cloud connector to an SSO Connector list
To control access to a cloud service, locate the corresponding cloud connector in the SSO Catalog and add it to an SSO Connector list.

Task
1. Select Policy | Lists.
2. In the Lists tree, expand Custom Lists | SSO Connector, then click the list you want to modify.
3. Click the Edit symbol.
   A dialog box opens showing folders, each folder holding connectors in the specified category.
   Example: Travel & Transportation
4. To add connectors to the list, select them individually or by category, then click OK.
   If the connector you want does not exist, you can create it by clicking Create new.
5. Click Save Changes.

Providing SSO services for HTTP cloud applications
Web Gateway supports many cloud services and applications that use HTTP authentication to log on end users with predefined cloud connectors or individual cloud connector templates.

A cloud connector is the configuration that allows Web Gateway to connect to and provide identity and SSO services for an application in the cloud. Web Gateway also provides a generic HTTP connector template, which can be configured for any cloud application that uses HTTP, but is not included in the SSO Catalog.

Before configuring a connector to an HTTP application, look up the application in the SSO Catalog. Predefined HTTP connectors come fully configured and only need selecting from the catalog. If the connector you want does not exist in the Predefined connectors or Custom connectors lists, you can create it from a template.

Most templates are partially configured connectors to specific cloud applications. If no template exists for your HTTP application, select the Generic HTTP Connector template. The generic HTTP template lets you configure connectors to HTTP applications that Web Gateway does not support with predefined connectors or connector templates.

Web Gateway supports single sign-on to dynamic HTTP applications that provide logon page information dynamically, such as Dropbox, by adding JavaScript to the logon page. Before the logon page can be modified, the SSO process must be running in proxy mode. In proxy mode, Web Gateway hides the real password from the client computer by replacing it with a token.

Single sign-on to HTTP applications that are not dynamic can be implemented in proxy or non-proxy mode.
The SSO credential model for HTTP cloud applications

The SSO credential model for HTTP cloud services and applications supports individual end users who have more than one account in a cloud service or application. It also supports shared accounts, where multiple end users can access one or more cloud services or applications using the same credentials.

The following credential information is passed to most SSO properties and events:

- **Realm** — Specifies the name of the domain in which the current user is authenticated. The authentication domain can be an identity store, such as LDAP or Active Directory, or an authentication service.
- **User ID** — Identifies the current user. By default, the User ID has the same value as the Authentication.UserName property. You can modify the default value by mapping a different authentication attribute to the User ID.
- **Service ID** — Identifies a cloud service or application.
- **Account ID** — Identifies an individual or shared account in the cloud service or application.

Individual users are organized under realms or authentication domains. Users in an authentication domain are associated with one or more lists of cloud services or applications that they are allowed to access. For each cloud service or application, each user can have one or more accounts. The accounts can be individual accounts or shared.

Configure an HTTP cloud connector

Configure a connector to an HTTP service or application using a template.

**Task**

1. Select Policy | Lists.
2. In the Lists tree, expand System Lists | SSO Catalog, then click Custom connectors.
3. Click the Add icon.
   
   The Add Connector dialog box opens.
4. Provide values for the fields and settings common to all cloud connectors.
5. From the Template drop-down list, select the template corresponding to the HTTP service.
6. In the Application Domain Name field, specify the domain name of your instance of the HTTP service or application.
   
   Example: If your service URL is https://myorg.cloudapp.com, myorg is the name of your application domain.
7. Click OK.

The newly configured HTTP connector is added to the SSO Catalog | Custom connectors list.

Configure a generic HTTP cloud connector

Configure a generic HTTP cloud connector when you want to connect to an HTTP service that Web Gateway does not support with an individual connector.

**Task**

1. Select Policy | Lists.
2. In the Lists tree, expand System Lists | SSO Catalog, then click Custom connectors.
3 Click the Add icon.
   The Add Connector dialog box opens.
4 Provide values for the fields and settings common to all connectors.
5 From the Template drop-down list, select Generic HTTP Connector.
6 To configure a connector to a dynamic HTTP cloud service, select Dynamic service.
7 From the drop-down list, select the HTTP method that specifies how the form is sent.
8 In the https:// field, specify where to send the form in URL format.
9 For each attribute sent in the form, configure one form field.
10 For each form field whose source is the credential store, configure one launchpad field.
11 (Optional) Configure one or more logon pages.
   Dynamic HTTP cloud services require one logon page. Some cloud services require more than one logon page.
12 (Optional) Configure the fields on the logon page.
   You only need configure the logon fields when they are different from the form fields.
13 To configure another generic HTTP connector, click New Sign On Request.
14 To save the HTTP connector configuration, click OK.

The newly configured generic HTTP connector is added to the SSO Catalog | Custom connectors list.

**Generic HTTP connector settings**

To configure a connector to an HTTP service or application using the generic HTTP connector template, provide values for the settings in the following table. Not all settings are required for every HTTP service. Some services and situations require more advanced settings, such as dynamic HTTP services.

**Table 14-1  Generic HTTP connector settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign-on Requests</td>
<td></td>
</tr>
<tr>
<td>Dynamic service</td>
<td>When selected, specifies a connector to a dynamic HTTP cloud service or application.</td>
</tr>
</tbody>
</table>
| POST         | Select an HTTP method:  
  • POST — (Default) Specifies that the form is generated using the selected content type and sent in the body of the HTTP request.  
  • GET — Specifies that all information is sent in the URL string. |
| Content type | (POST) Specifies how the form data is encoded. Select an option:  
  • application/x-www-form-urlencoded — (Default) Use this option most of the time.  
  • multipart/form-data — Use this option when sending large amounts of form data. |
| https://     | Specifies the Service Provider URL where the form data is sent.  
  We strongly recommend securing the logon form data by using the HTTPS protocol. |
Table 14-1  Generic HTTP connector settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| regex (optional)| Specifies a regular expression that can detect variations on the Service Provider URL. For example, the regular expression `https://www.mycompany.com/login.*` can detect the following URLs:  
• `https://www.mycompany.com/login`  
• `https://www.mycompany.com/login?session=abc`  
You can use this option to detect POST transactions to dynamic HTTP cloud services. |
| Form Fields     | Maps attribute names from the Identity Provider source (the SSO service) to the Service Provider target (the cloud service or application). Configure one form field for each attribute sent in the form.  
At least one form field is required.  
• Set (parameter) — Specifies the name of the attribute that is sent in the form. This value must be the name of an attribute that the cloud service or application is expecting.  
• to (source) — Specifies the source of the attribute value. Select one:  
  • Constant — Specifies that the attribute has a constant value. Provide the constant value in the value field.  
  • Credential Store — Specifies that the attribute is stored in the credential store that comes integrated with Web Gateway. Provide the name of the attribute in the attribute field. This name can differ from the name of the attribute in the cloud service or application.  
  Attributes commonly mapped from Identity Provider to Service Provider include user name and password. Always map the attribute that uniquely identifies the user in the IdP source to the SP target.  
• Mask — (Proxy mode) When selected, the attribute’s real value is replaced with a token value, then sent to the client computer used by the user. When the form is sent from the client computer to the server, the token value is replaced with the real value.  
This option is selected by default when the source attribute is the password. |
| Login Pages     | (Optional) Specifies the page where users log on to the cloud service or application.  
• https:// — Specifies the URL of the logon page.  
• regex (optional) — Specifies a regular expression that can detect variations on the logon page URL.  
You can use this option to detect modified URLs formed by dynamic HTTP cloud services when redirecting users to the logon page.  
• form locator Javascript (optional) — Specifies the location of the form on the logon page when there are multiple forms on the page using JavaScript.  
• submit action Javascript (optional) — Specifies an alternative form submit action using JavaScript.  
Dynamic HTTP cloud services require one logon page. Some cloud services require more than one logon page. For example, you might need to configure separate logon pages for mobile and desktop browsers. |
Table 14-1  Generic HTTP connector settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Fields</td>
<td>(Optional) Specifies the names of the fields on the logon page. You only need configure</td>
</tr>
<tr>
<td></td>
<td>the names of the logon fields when they are different from the names of the form fields. In</td>
</tr>
<tr>
<td></td>
<td>this case, the source configuration is the same. Only the name in the parameter field changes</td>
</tr>
<tr>
<td></td>
<td>to match the name on the logon page.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Set</strong> (parameter) — Specifies the name of the field on the logon page.</td>
</tr>
<tr>
<td></td>
<td>• <strong>to</strong> (source) — Specifies the source of the attribute value. The source configuration for</td>
</tr>
<tr>
<td></td>
<td>the form field and the logon field is the same. Select one:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Constant</strong> — Specifies that the attribute has a constant value. Provide the constant</td>
</tr>
<tr>
<td></td>
<td>value in the <strong>value</strong> field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Credential Store</strong> — Specifies that the attribute is stored in the credential store that</td>
</tr>
<tr>
<td></td>
<td>comes integrated with Web Gateway. Provide the name of the attribute in the **credential store</td>
</tr>
<tr>
<td></td>
<td>field name** field. This name can differ from the name of the attribute in the cloud service</td>
</tr>
<tr>
<td></td>
<td>or application.</td>
</tr>
<tr>
<td></td>
<td>• <strong>element locator Javascript (optional)</strong> — Specifies the location of the corresponding form</td>
</tr>
<tr>
<td></td>
<td>field using Javascript when the form fields are not unique.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mask</strong> — (Proxy mode) When selected, the attribute's real value is replaced with a token</td>
</tr>
<tr>
<td></td>
<td>value, then sent to the client computer used by the user. When the form is sent from the</td>
</tr>
<tr>
<td></td>
<td>client computer to the server, the token value is replaced with the real value.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="This option is selected by default when the source attribute is the password." /></td>
</tr>
<tr>
<td>Add Sign on Request</td>
<td>When clicked, allows you to configure different values for a SSO request to the same HTTP</td>
</tr>
<tr>
<td></td>
<td>service or application.</td>
</tr>
<tr>
<td>Launchpad Fields</td>
<td>Specifies the launchpad fields that allow users to manage their credentials for the HTTP</td>
</tr>
<tr>
<td></td>
<td>service. For each form field whose source is the credential store, you configure one</td>
</tr>
<tr>
<td></td>
<td>launchpad field.</td>
</tr>
<tr>
<td></td>
<td>• From the drop-down list, select the type of input field to render on the launchpad:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Email</strong> — The text must be in the form of a valid email and is displayed in the field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Number</strong> — The text must consist of numbers and is displayed in the field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password</strong> — The text is masked as it is entered in the field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Text</strong> — The text is displayed in the field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>prompt</strong> — Specifies the prompt to display for the field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>validation regex (optional)</strong> — Specifies a custom regular expression that validates the</td>
</tr>
<tr>
<td></td>
<td>text entered by the user.</td>
</tr>
</tbody>
</table>
Providing SSO services for SAML 2.0 cloud applications

Web Gateway supports cloud services and applications that use SAML 2.0 authentication to log on end users by providing cloud connector templates.

A cloud connector is the configuration that allows Web Gateway to connect to and provide identity and SSO services for an application or service in the cloud. Web Gateway provides connector templates for many individual cloud services and applications. Web Gateway also provides a generic SAML2 connector template. The generic template can be configured for any cloud service or application that uses SAML 2.0, but is not included in the SSO Catalog.

Configuring single sign-on for a SAML 2.0 cloud application requires configuration in your SAML 2.0 application administrator account as well as in the Web Gateway user interface.

How SAML single sign-on is initiated

The SAML SSO process can be initiated by the Identity Provider (IdP) or the Service Provider (SP). The Identity Provider is the service that authenticates the end user. The Service Provider is the SAML cloud service or application that the end user wants to access. In the following examples of SAML single sign-on, Web Gateway performs the Identity Provider role.

The SSO process begins when the user requests access to a SAML application in the cloud. Web Gateway authenticates the user, then redirects the authentication result to the SAML application through the user’s browser. The redirected messages are automatic and take place quickly, so that the user is not aware of the authentication process running in the background.

IdP-initiated SAML single sign-on

Web Gateway initiates the SSO process, which consists of the following overall steps:

1. Web Gateway authenticates the user.
2. Web Gateway presents the user with a launchpad that includes icons for all SAML applications the user is allowed to access. The user requests access to a SAML application (the Service Provider) through Web Gateway (the Identity Provider) by selecting an icon on the launchpad.
3. Web Gateway redirects the authentication result to the SAML application through the user’s browser.
4. The SAML application grants access to the user.

Figure 14-3  IdP-initiated SAML single sign-on
**SP-initiated SAML single sign-on**

The SAML application in the cloud initiates the SSO process, which consists of the following overall steps:

1. The user requests access to a SAML application (the Service Provider) directly.
2. The SAML application redirects the user’s request to Web Gateway (the Identity Provider) through the user’s browser.
3. Web Gateway authenticates the user.
4. Web Gateway redirects the authentication result to the SAML application through the user’s browser.
5. The SAML application grants access to the user.

![Diagram of SP-initiated SAML single sign-on]

**Figure 14-4  SP-initiated SAML single sign-on**

**Pure SP-initiated SAML single sign-on**

Not all SAML applications support IdP-initiated and SP-initiated single sign-on. Some SAML applications support only one. SAML applications that support only SP-initiated single sign-on present a special use case called *pure* SP-initiated single sign-on.

1. Web Gateway authenticates the user.
2. Web Gateway presents the user with a launchpad that includes icons for all SAML applications the user is allowed to access. The user requests access to a SAML application (the Service Provider) through Web Gateway (the Identity Provider) by selecting an icon on the launchpad.
3. Because the SAML application only supports SP-initiated single sign-on, Web Gateway redirects the user’s request to the application through the user’s browser. Because the user is not authenticated, the SAML application redirects the user to Web Gateway with an authentication request.
4 Web Gateway redirects the authentication result to the SAML application through the user’s browser.

5 The SAML application grants access to the user.

![Diagram of SAML single sign-on](image)

**Figure 14-5 Pure SP-initiated SAML single sign-on**

**Certificate management for SAML single sign-on**

SAML single sign-on requires an X.509 certificate and private key. Together, the X.509 certificate and private key are known as the X.509 certificate key pair. The X.509 certificate contains the public key that makes up the key pair and a signature. The certificate can be self-signed or signed by a certificate authority.

X.509 Certificate

- subject
- issuer
- ..... public key
- signature

X.509 Certificate key pair

The private key is used for signing outgoing SAML assertions and requests, and the X.509 certificate is used for verifying incoming signatures. The SSO party signing SAML assertions or requests with the private key provides the X.509 certificate to the SSO party verifying the signatures.

SAML services and applications have different certificate requirements. The following scenarios are common.
Table 14-2 Certificate management

<table>
<thead>
<tr>
<th>SSO process</th>
<th>Certificate management steps</th>
<th>SSO steps</th>
</tr>
</thead>
</table>
| IdP-initiated and SP-initiated SSO | 1 In the Web Gateway interface, the administrator generates or imports a private key and certificate pair and exports the certificate for use by the Service Provider.  
2 In the Service Provider interface, the administrator uploads the certificate corresponding to the private key. | 1 Web Gateway creates signed SAML assertions attesting to the end user's identity using the private key.  
2 The Service Provider uses the certificate to verify the signatures. |
| SP-initiated SSO | 1 In the Service Provider interface, the administrator downloads the certificate corresponding to the private key.  
2 In the Web Gateway interface, the administrator imports the Service Provider certificate. | 1 The Service Provider creates signed SAML SSO requests using the private key.  
2 Web Gateway uses the certificate to verify the signatures. |

Configure a SAML2 cloud connector

Configure a connector to a SAML 2.0 service or application using a template.

**Task**

1. Select Policy | Lists.
2. In the Lists tree, expand System Lists | SSO Catalog, then click Custom connectors.
3. Click the Add icon.
   The Add Connector dialog box opens.
4. Provide values for the fields and settings common to all connectors.
5. From the Template drop-down list, select the template corresponding to the SAML 2.0 service.
6. Provide values for the SAML settings.
7. Click OK.

The newly configured SAML2 connector is added to the SSO Catalog | Custom connectors list.

**SAML2 connector settings**

To configure a connector to a SAML 2.0 service or application, provide values for the settings in the following table. Not all settings are required for every SAML application.

- **Web Gateway is the Identity Provider.**

Table 14-3 SAML2 connector settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Domain Name</td>
<td>Specifies the domain name of your instance of the cloud service or application. Example: If your service URL is <a href="https://myorg.cloudapp.com">https://myorg.cloudapp.com</a>, myorg is the name of your application domain.</td>
</tr>
<tr>
<td>SAML Assertion Issuer (IdP)</td>
<td>Specifies the URL of the SSO service (IdP) that issues SAML assertions attesting to the user's identity.</td>
</tr>
</tbody>
</table>
### Table 14-3  SAML2 connector settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assertion Consumer Service URL (SP)</td>
<td>Specifies the URL of the Assertion Consumer Service (ACS) used by the cloud service or application (SP). The ACS consumes the SAML assertions produced by the SSO service (IdP). You can obtain this value from the Service Provider.</td>
</tr>
<tr>
<td>SAML SSO Request Creation URL (SP)</td>
<td>Specifies the URL of the cloud service or application (SP) required when single sign-on is SP-initiated.</td>
</tr>
<tr>
<td>SAML Subject Attribute Name</td>
<td>Specifies the name of the attribute to use as the subject of the SAML assertion. The SAML subject uniquely identifies the user. This value must be the name of an attribute that the cloud service or application is expecting.</td>
</tr>
<tr>
<td>Other Attribute Names</td>
<td>(Optional) In addition to the SAML subject, you can pass other attribute name-value pairs from the Identity Provider to the Service Provider. These settings include Email, First Name, and Last Name.</td>
</tr>
<tr>
<td>Private Key (IdP)</td>
<td>From the drop-down list, select the X.509 certificate that corresponds to the private key used by the SSO service (IdP) to sign SAML assertions, requests, and responses. The Service Provider uses the certificate to verify the signatures.</td>
</tr>
<tr>
<td>Private Key (SP)</td>
<td>From the drop-down list, select the X.509 certificate that corresponds to the private key used by the cloud service or application (SP) to sign SAML assertions, requests, and responses. The Identity Provider uses the certificate to verify the signatures.</td>
</tr>
<tr>
<td>Name Identifier Format</td>
<td>Specifies the format of the subject attribute that the cloud service or application (SP) is expecting. This attribute uniquely identifies the user.</td>
</tr>
<tr>
<td>Name Qualifier (SP)</td>
<td>Specifies a string that uniquely identifies the cloud service or application (SP) across namespaces.</td>
</tr>
<tr>
<td>Authentication Context Class Ref</td>
<td>Specifies the URI corresponding to the authentication context class used by the cloud service or application (SP). This URI is part of the OASIS SAML standard. Example: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</td>
</tr>
<tr>
<td>Lifetime (seconds)</td>
<td>Specifies a lifetime value to use when calculating the SAML assertion’s expiration time. When the expiration time is exceeded, the SAML assertion is invalid.</td>
</tr>
<tr>
<td>Clock Skew (seconds)</td>
<td>Specifies a value that offsets small differences in time between clocks. This value is used when calculating the SAML assertion’s expiration time.</td>
</tr>
</tbody>
</table>

### Configure a generic SAML2 cloud connector

Configure a generic SAML2 cloud connector when you want to connect to a SAML 2.0 service that Web Gateway does not support with an individual connector template.

**Task**

1. Select Policy | Lists.
2. In the Lists tree, expand System Lists | SSO Catalog, then click Custom connectors.
3. Click the Add icon.
   The Add Connector dialog box opens.
4. Provide values for the fields and settings common to all connectors.
5. From the Template drop-down list, select Generic SAML2 Connector.
6 Provide values for the generic SAML2 settings.

7 Click OK.

The newly configured SAML2 connector is added to the SSO Catalog | Custom connectors list.

**Generic SAML2 connector settings**

To configure a connector to a SAML 2.0 service or application using the generic SAML2 connector template, provide values for the settings in the following table.

Metadata consists of the SAML settings provided by the Service Provider. When configuring a generic SAML2 connector, you can enter the metadata manually or provide the URL from where the metadata can be downloaded automatically.

| Table 14-4  SAML credential mapping |
|-----------------|------------------|
| **Option**      | **Definition**   |
| Subject         | The SAML subject uniquely identifies the user who is seeking access to a cloud service or application. The SAML subject is specified as a source-value pair. From the drop-down list, select a source: |
|                 |  • Constant — Specifies that the subject has a constant value. Type the constant value in the value field. |
|                 |  • Authentication result — Specifies that the subject has the value of an attribute. Type the name of the attribute in the Authentication result field. |
| Attributes      | (Optional) Specifies one or more user attributes that are passed as name-value pairs with the SAML subject in the SAML assertion to the Service Provider. |
|                 |  Set — (parameter) Specifies the attribute name sent in the SAML assertion. This value is the attribute name that the Service Provider is expecting. |
|                 |  to — (source) Specifies the attribute value sent with the attribute name in the SAML assertion. The attribute value is specified as a source-value pair. From the drop-down list, select a source: |
|                 |  • Constant — Specifies that the value sent in the SAML assertion is set to the constant typed in the value field. |
|                 |  • Authentication result — Specifies that the value sent in the SAML assertion is set to the value of the attribute named in the Authentication result field. |
|                 | To view a list of standard LDAP attribute names, click the icon next to this field. |

| Table 14-5  Metadata — Automatically download metadata |
|-----------------|------------------|
| **Option**      | **Definition**   |
| Metadata URL    | Specifies the URL where you can download the SAML metadata in XML format. |
|                 | The format must conform to the SAML metadata specification. |
| Entity ID       | Uniquely identifies the Service Provider. This value is specified by the entityID attribute inside the tags at the top of the SAML metadata file. |
### Table 14-6 Metadata - Specify metadata manually

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assertion Consumer Service (ACS)</td>
<td><strong>ACS URL</strong> — Specifies the URL of the service where SAML assertions are sent and consumed.</td>
</tr>
<tr>
<td>(Optional)</td>
<td></td>
</tr>
<tr>
<td>IdP-initiated SSO (Optional)</td>
<td><strong>Enabled</strong> — When selected, enables Identity Provider-initiated single sign-on. The Service Provider must support IdP-initiated single sign-on.</td>
</tr>
<tr>
<td></td>
<td><strong>Relay state</strong> — Specifies the page in the cloud service or application that opens when single sign-on is successful.</td>
</tr>
<tr>
<td>SP-initiated SSO (Optional)</td>
<td><strong>Enabled</strong> — When selected, enables Service Provider-initiated single sign-on. The Service Provider must support SP-initiated single sign-on.</td>
</tr>
<tr>
<td></td>
<td><strong>SP issuer</strong> — Specifies the name of the Service Provider that receives the SAML authentication request and initiates single sign-on.</td>
</tr>
<tr>
<td></td>
<td><strong>SSO URL</strong> — (Pure SP-initiated SSO) Specifies the URL of the Service Provider to which Web Gateway redirects the SAML authentication request when only SP-initiated single sign-on is supported.</td>
</tr>
<tr>
<td></td>
<td><strong>Signature</strong> — (Optional) Specifies the X.509 certificate corresponding to the private key that the Service Provider uses to sign SAML authentication requests. Web Gateway uses the certificate to verify the signatures.</td>
</tr>
<tr>
<td></td>
<td><img src="image.png" alt="" /> <strong>Before you can select the certificate from the Signature drop-down list, you must:</strong></td>
</tr>
<tr>
<td></td>
<td>1 In the Service Provider interface, download the certificate.</td>
</tr>
<tr>
<td></td>
<td>2 In the Web Gateway interface, import the certificate.</td>
</tr>
</tbody>
</table>

### Table 14-7 Metadata — SAML Assertion

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature key</td>
<td>From the drop-down list, select the X.509 certificate key pair whose private key Web Gateway uses to sign SAML assertions.</td>
</tr>
<tr>
<td></td>
<td><img src="image.png" alt="" /> <strong>Before you can select the key pair from the drop-down list, you must import it in the Web Gateway interface.</strong></td>
</tr>
<tr>
<td>Issuer</td>
<td>Specifies a name that identifies Web Gateway as the SAML assertion issuer.</td>
</tr>
</tbody>
</table>
### Table 14-8 Advanced

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject</strong></td>
<td>Name ID format — From the drop-down list, select the option that identifies the format of the subject sent in the SAML assertion. Example: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</td>
</tr>
</tbody>
</table>
|                          | For more information, see the OASIS SAML 2.0 specification: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.  
|                          | 2 In the open document, look for the section Name Identifier Format Identifiers.                      |
| **Authentication Statement** | Authentication method — From the drop-down list, select the authentication context class that identifies the method used to authenticate the subject sent in the SAML assertion. Example: urn:oasis:names:tc:SAML:2.0:ac:classes:Password |
|                          | For more information, see the OASIS SAML 2.0 specification: Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0.  
|                          | 2 In the open document, look for the section Schemas.                                                     |
| **Time stamp**          | Format — To select a format for the date-time stamp, click the configure button. The options are:      |
|                          | • yyyy-MM-dd'T'HH:mm:ss'Z' (default)                                                                     |
|                          | • yyyy-MM-dd'T'HH:mm.SSS'Z' (includes milliseconds)                                                     |
Table 14-8 Advanced (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Conditions     | **Audiences** — (Optional) Allows you to limit the audience to one or more SAML assertion consumers. To specify an audience:  
1. Click the Add icon.  
2. In the Audience URI field, type the Service Provider issuer string. You can obtain this value from the Service Provider.  
**Clock skew (seconds)** — Specifies a value that offsets small differences in time between clocks on different servers, such as the Identity Provider and Server Provider servers. This value is used when calculating the SAML assertion’s expiration time.  
Default value: 20  
**Lifetime (seconds)** — Specifies a lifetime value to use when calculating the SAML assertion’s expiration time. When the expiration time is exceeded, the SAML assertion is invalid. Using this setting can prevent replay attacks.  
Default value: 60 |
| Signature      | **Method** — From the drop-down list, select a signature method:  
• **Sign Entire Response** — Specifies that Web Gateway signs the entire SAML response.  
• **Sign Assertions** — Specifies that Web Gateway signs only the SAML assertion in the SAML response.  
**Signature generation method** — From the drop-down list, select an algorithm to use when generating the signature:  
• rsaWithSha1  
• rsaWithSha256 |

Configuring external data sources for SAML single sign-on

While credentials for single sign-on to HTTP services are stored in the credential store that comes integrated with Web Gateway, SAML credentials come from external data sources, such as one or more LDAP servers, a database, or a web service. Several external data sources are configured using the external lists feature.

Identity information is fetched from external data sources as user attribute name-value pairs. The names must match the attribute names configured when the cloud connector was created.

LDAP authentication settings for SAML single sign-on

You can configure the Authentication module settings for one or more LDAP servers as the data source for SAML single sign-on. When one server is not available, the authentication module supports fallback to another server.

To locate these settings, select **Policy** | **Settings** | **Engines** | **Authentication**. Then click the Add icon located above the Settings tree.

Table 14-9 LDAP authentication settings for SAML single sign-on

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Name                 | Specifies the name of the authentication module settings.  
Example: LDAP for SAML SSO |
| Authentication method | From the drop-down list, select **LDAP**.                                   |
| LDAP server(s) to connect to | Add at least one LDAP server and specify the server's URI.  
Format: [ldap[s]://]server[:port] |
Table 14-9 LDAP authentication settings for SAML single sign-on (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of certificate authorities</td>
<td>(Secure LDAP connection protocol) From the drop-down list, select a certificate authority.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Specifies the user name required for connecting to the LDAP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password required for connecting to the LDAP server.</td>
</tr>
<tr>
<td>Base distinguished name to user objects</td>
<td>Specifies the distinguished name of the entry in the LDAP tree where the search for users is started.</td>
</tr>
<tr>
<td></td>
<td>Format: attribute=value{, attribute=value}</td>
</tr>
<tr>
<td>Map user name to DN</td>
<td>When selected, allows you to configure a filter expression.</td>
</tr>
<tr>
<td>Filter expression to locate a user object</td>
<td>Specifies an LDAP expression used to filter entries and find a user, where %u is a placeholder for the user name.</td>
</tr>
<tr>
<td></td>
<td>Active Directory example: (samaccountname=%u)</td>
</tr>
<tr>
<td></td>
<td>OpenLDAP example: (cn=%u)</td>
</tr>
<tr>
<td></td>
<td>Format: (attribute operator value)</td>
</tr>
<tr>
<td>Get user attributes</td>
<td>When selected, allows you to configure user attributes.</td>
</tr>
<tr>
<td>User attributes to retrieve</td>
<td>The following attributes are required by all SAML connectors. Add them to the list of user attributes to retrieve.</td>
</tr>
<tr>
<td></td>
<td>• mail — Specifies an email address.</td>
</tr>
<tr>
<td></td>
<td>• cn — (commonName) Specifies the first name followed by the last name.</td>
</tr>
<tr>
<td></td>
<td>• gn — (givenName) Specifies the first name.</td>
</tr>
<tr>
<td></td>
<td>• sn — (surname) Specifies the last name.</td>
</tr>
</tbody>
</table>

Using a web service as the data source for SAML single sign-on

You can configure the External Lists settings to fetch data for SAML single sign-on from any web service that supports the JSON format.

To locate these settings, select Policy | Settings | Engines | External Lists. Then click the Add icon located above the Settings tree.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the external lists settings.</td>
</tr>
<tr>
<td></td>
<td>Example: Web service for SAML SSO</td>
</tr>
<tr>
<td>Data source type</td>
<td>From the drop-down list, select Web Service.</td>
</tr>
<tr>
<td>Data type</td>
<td>From the drop-down list, select JSON.</td>
</tr>
<tr>
<td>Web service's URL</td>
<td>Specifies the URL of the web service.</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="https://webservice.com:5984/users/$%7B0%7D">https://webservice.com:5984/users/${0}</a></td>
</tr>
<tr>
<td></td>
<td>where users specifies a table containing user information and ${0} is a placeholder for the user ID that is passed to the web service.</td>
</tr>
</tbody>
</table>
Using a database as the data source for SAML single sign-on

You can configure the External Lists settings to fetch data for SAML single sign-on from a database.

To locate these settings, select Policy | Settings | Engines | External Lists. Then click the Add icon located above the Settings tree.

The following settings are for a SQLite3 database.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the external lists settings. Example: Database for SAML SSO</td>
</tr>
<tr>
<td>Data source type</td>
<td>From the drop-down list, select Database.</td>
</tr>
<tr>
<td>SQL Query</td>
<td>Specifies the SQL query that fetches the data from the database: select firstname as gn, lastname as sn, email as mail from users where uid = '${0}'; where ${0} is a placeholder for the user ID that is passed to the database.</td>
</tr>
<tr>
<td>Type of Database</td>
<td>From the drop-down list, select SQLite3.</td>
</tr>
<tr>
<td>File path to SQLite3 database</td>
<td>Specifies the path to the SQLite3 database.</td>
</tr>
</tbody>
</table>

Using an LDAP server as the data source for SAML single sign-on

You can configure the External Lists settings to fetch data for SAML single sign-on from an LDAP server. Using these settings, you can configure only one LDAP server as the data source.

To locate these settings, select Policy | Settings | Engines | External Lists. Then click the Add icon located above the Settings tree.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the external lists settings. Example: LDAP server for SAML SSO</td>
</tr>
<tr>
<td>Data source type</td>
<td>From the drop-down list, select LDAP.</td>
</tr>
<tr>
<td>LDAP server’s URL</td>
<td>Specifies the URL of the LDAP server. Format: ldap[s]://server[:port]</td>
</tr>
<tr>
<td>User name</td>
<td>Specifies the user name required for connecting to the LDAP server.</td>
</tr>
<tr>
<td>LDAP password</td>
<td>Specifies the password required for connecting to the LDAP server.</td>
</tr>
<tr>
<td>Search DN</td>
<td>Specifies the distinguished name of the entry in the LDAP tree where the search for users is started.</td>
</tr>
<tr>
<td>Search scope</td>
<td>From the drop-down list, select Sub tree.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search filter</td>
<td>Specifies an LDAP expression used to filter entries and find a user. Example: (uid=${0}) where ${0} is a placeholder for the user ID that is passed to the database.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Specify all attributes required by SAML connectors:</td>
</tr>
<tr>
<td>Additional LDAP attributes</td>
<td>• mail — Specifies an email address.</td>
</tr>
<tr>
<td>to retrieve (only for JSON</td>
<td>• cn — (commonName) Specifies the first name followed by the last name.</td>
</tr>
<tr>
<td>type)</td>
<td>• gn — (givenName) Specifies the first name.</td>
</tr>
<tr>
<td></td>
<td>• sn — (surname) Specifies the last name.</td>
</tr>
</tbody>
</table>

**SAML authentication using an external Identity Provider**

To support organizations that want users to authenticate using a trusted, external Identity Provider, Web Gateway performs the SAML Service Provider role.

SAML authentication refers to how identity information is shared between the Identity Provider and the Service Provider.

In this SAML scenario, the external Identity Provider is a database or authentication service that the organization trusts, but is outside the Web Gateway system. Web Gateway sends a SAML authentication request to the external Identity Provider. The Identity Provider authenticates the user using any authentication method and returns the identity information in a SAML assertion in the SAML authentication response. Web Gateway extracts the identity information from the SAML assertion and sets a cookie, which the user can use to authenticate to a cloud application.

Internally, Web Gateway implements SAML authentication using an external Identity Provider through the authentication server and the proxy, which provides the SAML functionality that the authentication server is missing.

The application in the cloud provides a service and is also known as a Service Provider. However, in this scenario, the Identity Provider and Service Provider roles are assigned to the players in the SAML authentication process itself, not to the service provided in the cloud.

**SAML authentication process using an external Identity Provider**

The authentication server consumes the SAML assertion in the response sent by the external Identity Provider and sets a cookie for the authenticated user.

The SAML authentication process begins when the user requests access to an application in the cloud through Web Gateway. The process consists of HTTP Redirect (GET) and POST messages that are sent through the user's browser (dashed lines). It also consists of messages that are sent and received by...
the user (solid lines). The messages that are sent through the user's browser to another SAML party take place automatically and quickly. The user is not aware of the authentication process running in the background.

Web Gateway sends the SAML authentication request to and receives the SAML authentication response from the Identity Provider using the HTTP POST method.

Figure 14-6 SAML authentication process using an external Identity Provider

1. The user requests access to an application in the cloud through Web Gateway.
2. If Web Gateway does not recognize the user, the proxy redirects the request to the authentication server through the user's browser.
3. The authentication server sends a SAML authentication request to the Identity Provider through the user's browser. The Identity Provider authenticates the user and sends a SAML authentication response back to the authentication server, also through the user's browser.

If the authentication server URL is static, the proxy intercepts the authentication response, constructs a dynamic URL, and redirects the response to the authentication server.

4. The authentication server consumes the SAML assertion in the response, sets a cookie, and redirects the authenticated user with the cookie to the application in the cloud through the proxy.
5. The proxy redirects the user with the cookie to the application in the cloud through the user's browser.
6. The application grants access to the user.

How Web Gateway supports static ACS URLs
Web Gateway supports Identity Providers that do not support dynamic URLs by saving the dynamic ACS URL in the RelayState parameter.

RelayState parameter
The URL of the authentication server, which provides the Assertion Consumer Service, is dynamic. Not all Identity Providers support dynamic URLs, which contain parameters. Web Gateway supports these Identity Providers by saving the value of the dynamic ACS URL at the time the authentication request is created in the RelayState parameter.

The RelayState parameter is configured automatically. No configuration is required on your part.
The authentication server sends the RelayState parameter and the authentication request to the Identity Provider in a POST form. When the Identity Provider returns the RelayState parameter and the authentication response, also in a POST form, the value of the RelayState parameter is unchanged.

If the ACS URL in the response is static, the proxy intercepts the response and restores the dynamic ACS URL from the static ACS URL and the RelayState value. Using the restored ACS URL, the proxy can redirect the SAML authentication response to the authentication server.

**Configuring a static ACS URL**

If the external Identity Provider supports dynamic URLs, the authentication server automatically sends the dynamic value to the Identity Provider and validates the ACS URL that it receives in return. No configuration is required in the Web Gateway interface.

If the external Identity Provider does not support dynamic URLs, the static ACS URL must be configured in two locations in the Web Gateway interface. The configured values must match.

- Static ACS URL value sent to the Identity Provider in the **SAML request** — This value is configured in the Prepare fixed ACS URL rule.

- Static ACS URL value expected in the **SAML response** from the Identity Provider — This value is configured in the SAML Response settings.

> The ACS URL value that you are expecting from the Identity Provider must also be configured at the Identity Provider.

**High-level configuration tasks**

Configuring SAML authentication with Web Gateway in the Service Provider role involves the following high-level tasks.

1. Import the Cookie authentication with SAML back end and fixed ACS URL rule set from the Rule Sets Library.

   > This rule set is located in the Authentication rule set group.

2. Configure a static ACS URL.

   > This task is required when the external Identity Provider does not support dynamic URLs.

3. Configure the SAML authentication request.

   > Web Gateway does not sign the SAML authentication request nor provide an X.509 certificate.

4. Configure the SAML authentication response. This task includes importing the X.509 certificate that the Identity Provider uses to sign the SAML authentication response and assertion.

5. To ensure that the authentication server recognizes the authentication response sent by the external Identity Provider, add the Identity Provider’s service URL to the SAML IdP Whitelist.

6. Configure the SAML attributes that you want mapped to the Authentication.UserName and Authentication.UserGroups properties.

7. Manually configure the external Identity Provider to produce a SAML authentication response that meets the requirements you configure in the Web Gateway interface.
Configure a static ACS URL
Configure a static ACS URL when the external Identity Provider does not support dynamic URLs.

Before you begin
Make sure that the Cookie Authentication with SAML backend and fixed ACS URL rule set is imported from the Rule Set Library.

Task
1  Select Policy | Rule Sets.
2  Expand Cookie Authentication with SAML backend and fixed ACS URL | Cookie Authentication at Authentication Server, then select Authentication Server Request.
3  Select the rule Prepare Fixed ACS URL, then click Edit.
   The Edit Rule dialog box opens.
4  Select the step Events, select the event, then click Edit.
   The Edit Set Property dialog box opens with the User-Defined.SAMLUrlRewrite property selected.
5  Select "- enter your URL here -", then click Edit.
6  In the Enter a String dialog box, type the static URL, then click OK.
7  To close the Edit Rule dialog box, click Finish.
The static ACS URL is updated in the Authentication Server Request rule set view.

Configure a SAML authentication request
Configure the SAML authentication request that the authentication server sends to the external Identity Provider.

Before you begin
Make sure that the Cookie Authentication with SAML backend and fixed ACS URL rule set is imported from the Rule Set Library.

Task
1  Select Policy | Settings.
2  Expand Engines | SAML Request, then select SAML Request.
   The Authn Request window opens for configuration.
3  Provide values for the Authn Request settings.
4  Click Save Changes.
SAML authentication request settings

Specify a unique name for the Service Provider (Web Gateway) and the URL of the external Identity Provider.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EntityID</td>
<td>Specifies a unique name for the Service Provider that sends the SAML authentication request (Web Gateway).</td>
</tr>
<tr>
<td>IdP URL</td>
<td>Specifies the URL of the external Identity Provider where the authentication request is sent.</td>
</tr>
</tbody>
</table>

Configure a SAML authentication response

Configure the SAML authentication response that the authentication server expects to receive from the external Identity Provider. To determine whether the SAML authentication response is valid, the authentication server compares the actual values in the response to the configured values.

Before you begin

Make sure that the Cookie Authentication with SAML backend and fixed ACS URL rule set is imported from the Rule Set Library.

Task

1. Select Policy | Settings.
2. Expand Engines | SAML Response, then select SAML Response.
   The Authn Response window opens for configuration.
3. Provide values for the Authn Response settings.
4. Click Save Changes.

SAML authentication response settings

The SAML authentication response configuration specifies the values that you configure at the Identity Provider.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response must be signed</td>
<td>When selected, specifies that the SAML response must be signed.</td>
</tr>
<tr>
<td>Assertion must be signed</td>
<td>When selected, specifies that the SAML assertion must be signed.</td>
</tr>
<tr>
<td>Import</td>
<td>When clicked, allows you to browse for and import the X.509 certificate file provided by the external Identity Provider. When the certificate file is imported, the certificate values are displayed in the Authn Response window.</td>
</tr>
<tr>
<td>EntityID</td>
<td>Specifies a unique name for the external Identity Provider that issues the SAML authentication response. This value and the value of the <a href="">saml2:Issuer</a> element in the response must match.</td>
</tr>
<tr>
<td>Response must be already valid</td>
<td>When selected, specifies that the current local time must be greater than or equal to the value of the notBefore attribute in the <a href="">saml2:Conditions</a> element in the response.</td>
</tr>
</tbody>
</table>
Table 14-11  SAML authentication response (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative clock skew</td>
<td>(Response must be already valid) Extends the notBefore attribute setting in the response by the specified value.</td>
</tr>
<tr>
<td>Positive clock skew</td>
<td>Extends the notAfter attribute setting in the response by the specified value.</td>
</tr>
<tr>
<td>Audience must be set in the response</td>
<td>Specifies that the <code>&lt;saml2:Audience&gt;</code> element must be included in the response.</td>
</tr>
<tr>
<td>Audience must match predefined value</td>
<td>Specifies that the value of the <code>&lt;saml2:Audience&gt;</code> element in the response must match the value specified in the Audience URI or ACS URL fields in the configuration.</td>
</tr>
<tr>
<td>Audience URI</td>
<td>(Audience must match predefined value) Specifies the URI of the intended audience, which is the authentication server.</td>
</tr>
<tr>
<td>Destination</td>
<td>Specifies the URI of the address to which the external Identity Provider sends the response.</td>
</tr>
<tr>
<td>ACS URL</td>
<td>Specifies the URL of the Assertion Consumer Service provided by the authentication server which consumes the SAML assertion in the response.</td>
</tr>
</tbody>
</table>

If the external Identity Provider does not support dynamic URLs, configure a static ACS URL. Otherwise, leave this setting blank. If set, this value must match the ACS URL value configured in the Prepare Fixed ACS URL rule.

Configure the static ACS URL using one of the following formats.
- Any Web Gateway URL
- A URL having the following format which the proxy recognizes as the authentication server:
  ```
  http[s]://<proxy>:<port>/mwg-internal/<internal-path-id>/plugin?
target=Auth&reason=Auth&setCookie=true
  ```
  Where `<proxy>` and `<port>` specify the IP address and port number of the proxy, respectively, and `<internal-path-id>` specifies the internal path id.

To look up the internal path id, select Configuration | Proxies | Advanced Settings.

Add external IdP URL to SAML IdP Whitelist
To ensure that the authentication server recognizes the authentication response sent by the external Identity Provider, add the Identity Provider URL to the SAML IdP Whitelist.

**Before you begin**
Make sure that the Cookie Authentication with SAML backend and fixed ACS URL rule set is imported from the Rule Set Library.

**Task**
1. Select Policy | Lists.
2. Expand Custom Lists | Wildcard Expression, then select SAML IdP Whitelist.
3. Click Add.
   - The Add Wildcard Expression dialog box opens.
4 In the **Wildcard Expression** field, specify an expression that matches the URL of the external Identity Provider.

5 Click **OK**.

The matching expression is added to the **SAML IdP Whitelist**.

### Configure SAML attribute mapping

You configure the names of the SAML attributes that you want mapped to the `Authentication.UserName` and `Authentication.UserGroups` properties.

**Before you begin**

Make sure that the Cookie Authentication with SAML backend and fixed ACS URL rule set is imported from the Rule Set Library.

**Task**

1 Select **Policy | Rule Sets**.

2 Expand **Cookie Authentication with SAML backend and fixed ACS URL** | **Cookie Authentication at Authentication Server**, then select **Authentication Server Request**.

3 Select the rule **Set user name and groups**, then click **Edit**.

   The **Edit Rule** dialog box opens.

4 Select the step **Events**, select an event, then click **Edit**.

   The **Edit Set Property** dialog box opens with the `Authentication.UserName` or `Authentication.UserGroups` property selected.

5 Navigate to the **Parameters for Property "Map.GetStringValue"** dialog box.

6 Select an option:
   - **Authentication.UserName** — Select 2. **Key (String) Value**: "userId". Replace **userID** with the name of the SAML attribute that you want mapped to the user name property.
   - **Authentication.UserGroups** — Select 2. **Key (String) Value**: "userGroup". Replace **userGroup** with the name of the SAML attribute you want mapped to the user groups property.

7 To save your changes, click **OK**.

8 To close the **Edit Rule** dialog box, click **Finish**.

The names of the SAML attributes that you want mapped are updated in the Authentication Server Request rule set view.

### Validating the SAML authentication response

To validate the SAML authentication response sent by the external Identity Provider, the authentication server compares the values in the response to the values configured in the Web Gateway interface.

You must manually configure the external Identity Provider to produce a SAML authentication response that meets the requirements configured in the Web Gateway interface.

To be valid, the SAML authentication response must meet the following requirements:

- The response must be a valid XML string.
- The response must include at least one SAML assertion.
• The `<saml2p:StatusCode>` element in the response must have the value Success.

• If configured, the response signature and assertion signature must be valid.
  • Response must be signed — If this setting is selected in the SAML authentication response configuration, the authentication server checks that the response is signed and that the signature is valid.
  • Assertion must be signed — If this setting is selected in the SAML authentication response configuration, the authentication server checks that the assertion is signed and that the signature is valid.

• The value of the `<saml2:Issuer>` element in the response must match the EntityID setting in the SAML authentication response configuration.

• The `<saml2:Conditions>` element in the response must include the attributes `notBefore` and `notAfter`.

• The current local time must fall within the specified time range, as follows.
  • Response must be already valid — When selected, this setting specifies that the current local time must be greater than or equal to the `notBefore` value.
  • Negative clock skew — The current local time must be greater than or equal to the `notBefore` time minus the negative clock skew value specified in the SAML authentication response configuration.
  • Positive clock skew — The current local time must be less than or equal to the `notAfter` time plus the positive clock skew value specified in the SAML authentication response configuration.

• If configured, the `audience` element must be included in the response and set to a predefined value, as follows.
  • Audience must be set in the response — If selected in the SAML authentication response configuration, the response must include the element `<saml2:Audience>`.
  • Audience must match the predefined value — If selected in the SAML authentication response configuration, the value of the `<saml2:Audience>` element must match the value specified in the Audience URI or ACS URL field in the configuration.

• The value of the `Destination` attribute in the `<saml2p:Response>` element in the response must match the ACS URL setting specified in the SAML authentication response configuration.

### Cookie authentication with SAML back end and fixed ACS URL — rule set

To support SAML authentication using an external Identity Provider, Web Gateway performs the Service Provider role. The rules in this rule set support this SAML scenario.

<table>
<thead>
<tr>
<th>Library rule set – Cookie authentication with SAML back end and fixed ACS URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following nested rule sets:
Cookie authentication with SAML back end and fixed ACS URL
  - Intercept SAML assertion if IdP uses a fixed ACS URL
  - Cookie authentication at HTTP(S) proxy
    - Set cookie for authenticated clients
    - Authenticate clients with authentication server
  - Cookie authentication at authentication server
    - Authentication server request

This rule set contains the following rule.

**Set client context**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Enable SSL Client Context without CA &lt;Default Without CA&gt;</td>
</tr>
</tbody>
</table>

This rule secures all HTTP communication with the SSL protocol using the default certificate that comes with Web Gateway or one that you import. To configure the SSL certificate, click <Default Without CA>.

**Intercept SAML assertion if IdP uses a fixed ACS URL**

The proxy intercepts SAML authentication responses containing a static ACS URL. It processes the SAML response and redirects the SAML assertion to the authentication server, which provides the Assertion Consumer Service.

**Nested library rule set – Intercept SAML assertion if IdP uses a fixed ACS URL**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Command.Name equals &quot;POST&quot; AND URL.Path is in list SAMLAuthResponseList</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Requests (and IM)</td>
</tr>
</tbody>
</table>

To configure the list of fixed ACS URLs, click SAMLAuthResponseList.

This rule set contains the following rules.

**Handle incoming SAML response**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set Authentication.Token = Request.POSTForm.Get (&quot;SAMLResponse&quot;)</td>
</tr>
<tr>
<td></td>
<td>Set Authentication.SAML.RelayState = Request.POSTForm.Get (&quot;RelayState&quot;)</td>
</tr>
</tbody>
</table>

The proxy retrieves the SAML response and RelayState parameter from the POST form sent by the external Identity Provider. It stores the response in the Authentication.Token property and the RelayState in the property Authentication.SAML.RelayState. When the Identity Provider does not support dynamic URLs, the proxy uses the URL returned in the RelayState to restore the dynamic authentication server URL.
Redirect SAML assertion to authentication server

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Block <code>&lt;SAMLRedirectToAuth&gt;</code></td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.SetStatus (200)</td>
</tr>
</tbody>
</table>

After restoring the dynamic authentication server URL, the proxy redirects the SAML assertion (stored in the Authentication.Token property) to the authentication server and sets the HTTP status code to 200 (OK). To provide custom settings for logging purposes, click `<SAMLRedirectToAuth>`.

Cookie authentication at HTTP(S) proxy

In the context of SAML authentication using an external Identity Provider, the proxy redirects requests that do not contain a valid cookie to the authentication server. The authentication server consumes SAML assertions and stores the user’s identity in a cookie.

<table>
<thead>
<tr>
<th>Nested library rule set – Cookie authentication at HTTP(S) Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria –</td>
</tr>
<tr>
<td>Authentication.IsServerRequest equals false AND (</td>
</tr>
<tr>
<td>Connection.Protocol equals &quot;HTTP&quot; OR</td>
</tr>
<tr>
<td>Connection.Protocol equals &quot;HTTPS&quot;) AND</td>
</tr>
<tr>
<td>Command.Name does not equal &quot;CONNECT&quot; AND</td>
</tr>
<tr>
<td>Command.Name does not equal &quot;CERTVERIFY&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following nested rule sets:

- Set Cookie for Authenticated Clients
- Authenticate Clients with Authentication Server

Set cookie for authenticated clients

After the authentication server consumes the SAML assertion and stores the user’s identity in a cookie, it redirects the user with the cookie through the proxy to the requested application.

<table>
<thead>
<tr>
<th>Nested library rule set – Set cookie for authenticated clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authentication.IsLandingOnServer equals true</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

P3P header to permit third party cookies in Internet Explorer

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Header.Block.Add (&quot;P3P&quot;, &quot;CP=&quot;NOI CUR OUR STP STA&quot;&quot;)</td>
</tr>
</tbody>
</table>

The P3P string is required for the Platform for Privacy Preferences Project (P3P). The string must match the privacy settings in the end user’s browser. If the P3P string is not updated as shown in the table and the browser is Internet Explorer, processing fails.
Set cookie and redirect client to the requested URL

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Redirect &lt;Redirect Back From Authentication Server&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

The authentication server redirects the authenticated user with a cookie through the proxy to the requested application. To provide custom settings for logging purposes, click <Redirect Back From Authentication Server>.

Authenticate clients with authentication server

The proxy allows requests from external Identity Providers whose URLs are on the SAML IdP Whitelist and checks for a valid cookie in the requests. If none exists, the proxy redirects the requests to the authentication server.

<table>
<thead>
<tr>
<th>Nested library rule set – Authenticate clients with authentication server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

Allow IDP requests

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.Domain matches in list SAML IdP Whitelist</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Rule Set</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

The proxy checks that the URL of the external Identity Provider making a request matches one of the URLs in the SAML IdP Whitelist.

To add URLs to the whitelist, click SAML IdP Whitelist.

Redirect clients that do not have a valid cookie to the authentication server

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.Authenticate &lt;Local Cookie Authentication Server&gt; equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Authenticate &lt;Default&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

If the request from the external Identity Provider does not include a valid cookie, the proxy redirects the request to the authentication server. To configure a different authentication method, click <Local Cookie Authentication Server>. To provide custom settings for logging purposes, click <Default>.

Cookie authentication at authentication server

This rule set is a container for the Authentication server request rule set.

<table>
<thead>
<tr>
<th>Nested library rule set – Cookie authentication at authentication server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>
This rule set contains the following nested rule set: Authentication server request.

**Authentication server request**

The rules in this rule set apply to the authentication server when it manages SAML authentication using an external Identity Provider. The authentication server processes the SAML authentication response, but does not set the cookie in this rule set. Cookie authentication is handled instead by the rules in the Cookie authentication at HTTP(S) rule set.

<table>
<thead>
<tr>
<th>Nested library rule set – Authentication server request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Authentication.IsServerRequest equals true</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

**Redirect clients that have a valid cookie**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.Authenticate &lt;Authentication Server - Cookie Check&gt; equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Redirect &lt;Redirect Back From Authentication Server&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

The authentication server redirects users having a valid cookie to the proxy. To change the cookie checking settings used by the authentication server, click `<Authentication Server - Cookie Check>`. To provide custom settings for logging purposes, click `<Redirect Back From Authentication Server>`.

**Prepare fixed ACS URL**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.SAMLUrlRewrite = URL.Protocol + &quot;:/&quot; + URL.Host + &quot;:- enter your URL here -&quot;</td>
</tr>
</tbody>
</table>

You can configure a static ACS URL for external Identity Providers who do not support dynamic URLs in this rule. If set, this value must match the ACS URL value configured in the SAML Response settings.

**POST SAML authentication request**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Command.Name does not match POST</td>
</tr>
<tr>
<td>Action</td>
<td>Block &lt;SAML request&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>Set Authentication.SAML.RelayState = URL&lt;br&gt;Set Authentication.Token = Authentication.SAML.CreateAuthnRequest&lt;br&gt;(User-Defined.SAMLUrlRewrite)&lt;SAML Request&gt;&lt;br&gt;HTTP.SetStatus (200)</td>
</tr>
</tbody>
</table>

The authentication server sends the RelayState parameter and SAML authentication request in a POST form to the external Identity Provider. The RelayState parameter saves the value of the authentication server URL at the time the request is created. The request is created using values configured in the Web Gateway interface. The authentication server then sets the HTTP status code to 200 (OK). To change the SAML authentication request configuration, click `<SAML Request>` in this event.
**Handle SAML authentication response**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Command.Name equals &quot;POST&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set Authentication.Token = Request.POSTForm.Get (&quot;SAMLResponse&quot;)</td>
</tr>
</tbody>
</table>

This rule retrieves the SAML response in the POST form sent by the external Identity Provider and stores it in the Authentication.Token property. It parses the response and returns a TRUE value if the response is valid and a FALSE value if it is not. To change the SAML authentication response configuration, click `<SAML Response>`.

**Block invalid SAML response**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Command.Name equals &quot;POST&quot; AND Authentication.IsAuthenticated equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Block <code>&lt;Authorized Only&gt;</code></td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

After the SAML response is parsed, this rule checks the value of the property Authentication.IsAuthenticated. If the property is false, the SAML response is invalid and processing of the response is blocked. To provide custom settings for logging purposes, click `<Authorized Only>`.

**Set user name and groups**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set Authentication.UserName = Map.GetStringValue (Authentication.SAML.Attributes, &quot;userId&quot;)</td>
</tr>
</tbody>
</table>

This rule maps the SAML attributes "userId" and "userGroup" to the Authentication.UserName and Authentication.UserGroups properties, respectively. You can use the rule editor to change the names of the SAML attributes that are mapped to the authentication properties.

**Block empty user name**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.UserName equals &quot;&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Block <code>&lt;Authorized Only&gt;</code></td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

If the user name property is empty, this rule blocks processing of the response. To provide custom settings for logging purposes, click `<Authorized Only>`. 
P3P header to permit third party cookies in Internet Explorer

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Header.Block.Add (&quot;P3P&quot;, &quot;CP=&quot;NOI CUR OUR STP STA&quot;&quot;&quot;)</td>
</tr>
</tbody>
</table>

The P3P string is required for the Platform for Privacy Preferences Project (P3P). The string must match the privacy settings in the end user's browser. If the P3P string is not updated as shown in the table and the browser is Internet Explorer, processing fails.

Redirect authenticated client back to proxy

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Redirect &lt;Redirect Back From Authentication Server&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

According to the final rule in the rule set, the authentication server redirects the authenticated user back to the proxy. To provide custom settings for logging purposes, click <Redirect Back From Authentication Server>.

Providing SSO services for .NET and Java web applications

Using the Single Sign On rule set and the generic IceToken cloud connector template, you can configure single sign-on to any .NET or Java web application. Use this option when Web Gateway does not support the web application with a predefined connector or connector template.

Web Gateway implements single sign-on using the IceToken authentication method in the same way that it implements single sign-on using SAML authentication. Single sign-on using the two authentication methods has the following differences:

- In both cases, the Identity Provider sends the user information to the Service Provider in an assertion. The format of the user information in the assertion differs depending on the authentication method used.
- Single sign-on using the IceToken authentication method is simpler and easier to configure than single sign-on using SAML authentication.

Configure a generic IceToken cloud connector

To configure single sign-on to a .NET or Java web application, use the generic IceToken cloud connector template.

**Task**

1. Select Policy | Lists.
2. In the Lists tree, expand System Lists | SSO Catalog, then click Custom connectors.
3. Click the Add icon.
   The Add Connector dialog box opens.
4. Provide values for the fields and settings common to all connectors.
From the Template drop-down list, select **Generic IceToken Connector**.

Provide values for the generic IceToken settings.

Click **OK**.

The newly configured IceToken connector is added to the SSO Catalog | Custom connectors list.

**Generic IceToken connector settings**

To configure a connector to a .NET or Java web application using the generic IceToken connector template, provide values for the settings in the following table.

**Table 14-12 Credentials**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject</strong></td>
<td>The IceToken subject uniquely identifies the user who is seeking access to a .NET or Java web application. The IceToken subject is specified as a source-value pair. From the drop-down list, select a source:</td>
</tr>
<tr>
<td>• <strong>Constant</strong> — Specifies that the subject has a constant value. Type the constant value in the value field.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Authentication result</strong> — Specifies that the subject has the value of an attribute. Type the name of the attribute in the Authentication result field.</td>
<td></td>
</tr>
<tr>
<td><em>(Optional)</em> Specifies one or more user attributes that are passed as name-value pairs with the IceToken subject in the IceToken assertion to the Service Provider.</td>
<td></td>
</tr>
<tr>
<td><strong>Set</strong> — (parameter) Specifies the attribute name sent in the IceToken assertion. This value is the attribute name that the Service Provider is expecting.</td>
<td></td>
</tr>
<tr>
<td><strong>to</strong> — (source) Specifies the attribute value sent with the attribute name in the IceToken assertion. The attribute value is specified as a source-value pair. From the drop-down list, select a source:</td>
<td></td>
</tr>
<tr>
<td>• <strong>Constant</strong> — Specifies that the value sent in the IceToken assertion is set to the constant typed in the value field.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Authentication result</strong> — Specifies that the value sent in the IceToken assertion is set to the value of the attribute named in the Authentication result field.</td>
<td></td>
</tr>
</tbody>
</table>

To view a list of standard LDAP attribute names, click the icon next to this field.

**Table 14-13 Assertion Consumer Service (ACS)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACS URL</strong></td>
<td>Specifies the URL of the service where IceToken assertions are sent and consumed.</td>
</tr>
<tr>
<td><strong>ACS bindings</strong></td>
<td>Specifies the HTTP method used to send IceToken assertions:</td>
</tr>
<tr>
<td>• <strong>POST</strong> — Specifies the HTTP POST method.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Redirect</strong> — Specifies the HTTP GET method.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 14-14 IceToken Assertion

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature key</td>
<td>From the drop-down list, select the X.509 certificate key pair whose private key Web Gateway uses to sign IceToken assertions.</td>
</tr>
<tr>
<td></td>
<td>Before you can select the key pair from the drop-down list, you must import it in the Web Gateway interface.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Specifies a name that identifies Web Gateway as the IceToken assertion issuer.</td>
</tr>
</tbody>
</table>

### Table 14-15 Conditions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audiences</td>
<td>(Optional) Allows you to limit the audience to one or more IceToken assertion consumers. To specify an audience:</td>
</tr>
<tr>
<td></td>
<td>1 Click the Add icon.</td>
</tr>
<tr>
<td></td>
<td>2 In the Audience URI field, type the Service Provider issuer string. You can obtain this value from the Service Provider.</td>
</tr>
<tr>
<td>Clock skew (seconds)</td>
<td>Specifies a value that offsets small differences in time between clocks on different servers. This value is used when calculating the IceToken assertion’s expiration time.</td>
</tr>
<tr>
<td></td>
<td>Default value: 20</td>
</tr>
<tr>
<td>Lifetime (seconds)</td>
<td>Specifies a lifetime value to use when calculating the IceToken assertion's expiration time. When the expiration time is exceeded, the IceToken assertion is invalid. Using this setting can prevent replay attacks.</td>
</tr>
<tr>
<td></td>
<td>Default value: 60</td>
</tr>
</tbody>
</table>

### How the end user works with the application launchpad

Using the application launchpad, the end user can open applications and select and manage application accounts.

#### Overall workflow

From the user's point of view, the launchpad workflow appears as follows:

1. Using the launchpad URL provided by an administrator, the user opens the launchpad.

2. The launchpad opens displaying the logon form, where the user enters credentials.

3. If authentication is successful, the launchpad presents icons representing the applications the user is allowed to access. To request an application, the user clicks the corresponding icon.

   The launchpad filters the applications it displays. For example, it does not display dynamic HTTP applications in non-proxy mode, applications that are not supported, or applications that the user is not allowed to access.

#### Opening the launchpad

Using the launchpad URL provided by an administrator, the user opens the launchpad from a web browser on a client of Web Gateway.

JavaScript must be enabled in the web browser.
The launchpad URL must contain the name of the management host configured in the Single Sign On settings. For example, if the host name is sso.mwginternal.com, the launchpad URL has one of the following values:

- https://sso.mwginternal.com
- https://sso.mwginternal.com/launchpad

**Selecting a cloud application**

Icons representing cloud applications are displayed in the left pane. When the user clicks an icon, the account information for that application is displayed in the right pane. If no account information is displayed, a couple of explanations are possible:

- **HTTP applications** — The first time an HTTP application is accessed, the user must provide credentials by clicking **Add Account**. The user also has the option of editing or deleting added accounts.

- **SAML applications** — Account information is not displayed or required, because SAML user information is retrieved from external sources.

You can initiate single sign-on to SAML applications and HTTP applications already configured with an account by clicking the application link in the left or right pane.

If the user has more than one account in an application, the icon representing that application is displayed multiple times in the left pane. Each icon is labeled with the user name corresponding to one account. To open a particular application account, the user can double-click the icon corresponding to the application-account pair.

**Launchpad options**

The launchpad provides options for displaying and selecting cloud applications and for working with application accounts. The following table describes these options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application logos</td>
<td>Allow the user to select cloud applications.</td>
</tr>
<tr>
<td>Find application</td>
<td>Allows the user to type a string that filters the cloud applications displayed by name.</td>
</tr>
<tr>
<td>Display mode</td>
<td>From the drop-down list, the user selects a display mode:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Icons</strong> — Displays the application icons in rows.</td>
</tr>
<tr>
<td></td>
<td>- <strong>List</strong> — Displays the application icons in list format and includes the categories to which the applications belong.</td>
</tr>
<tr>
<td>Sort applications</td>
<td>From the drop-down list, the user selects a method for sorting the cloud applications:</td>
</tr>
<tr>
<td></td>
<td>- <strong>By name</strong> — Displays cloud applications sorted by name.</td>
</tr>
<tr>
<td></td>
<td>- <strong>By category</strong> — Displays cloud applications sorted by category and name.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the icon and name of the cloud application selected by the user.</td>
</tr>
</tbody>
</table>

The following account information is only available for HTTP applications. SAML user information is fetched from external sources.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>Displays the email address of the cloud application account selected by the user.</td>
</tr>
<tr>
<td>Edit Account</td>
<td>Allows the user to edit the selected cloud application account.</td>
</tr>
<tr>
<td>Add Account</td>
<td>Allows the user to add a cloud application account.</td>
</tr>
</tbody>
</table>
### Customizing the application launchpad

In the Web Gateway interface, you can specify a name and description for your organization, customize the look of the text, and import images of your organization and product logos. You can also customize the header, footer, and sidebar that frame the launchpad.

#### Opening the template editor

To customize the launchpad, you edit a collection of files and templates named Single Sign On Schema. To open the collection in a template editor, navigate to the Single Sign On default settings and select Single Sign On Schema from the Collection drop-down list.

Alternatively, you can access the templates directly by selecting the Templates tab.

#### Files in the /dat folder vs. /files folder

When generating the launchpad, the Single Sign On module uses files located in the following folders on the server where the appliance is installed and the SSO process is running:

- **/dat** — Files in this folder are system files maintained by the appliance. They are overwritten each time there is an update from the update server.

- **/files** — Files in this folder and subfolders, including /img, can be customized, because they are not overwritten by the update server.

#### Edit the Launchpad.html file

In the Launchpad.html file, you can specify a name and description for your organization and the names of the style sheet and the image files containing logos. You can also customize the header, footer, and sidebar that frame the launchpad.

For example, you can add a message of the day or links to your IT organization to the sidebar.

#### Task

1. Select Policy | Settings.
2. Expand Engines | Single Sign On, then select Default.
   
   The Single Sign On settings open.
3. From the Collection drop-down list, select Single Sign On Schema, then click Edit.
   
   The Template Editor opens with the Single Sign On Schema folder selected.
4. Expand Single Sign On Schema | Launchpad | en, then select html.
   
   The HTML Editor opens.
5 In the editor:
   a Replace Your Company Name with the name of your organization.
   b Replace Your Company Description with a description of your organization.
   c (Optional) Replace customLaunchpad.css with the name of your custom .css file.
   d Replace sample_logo.png with the name of the image file containing the logo that represents your organization.
   e Replace productCompLogo.png with the name of the image file containing the logo that represents your product.

6 To customize the header, add content to the <div id="header"></div> element.
   Do not remove the "header" element even if it is empty.

7 To customize the footer, add content to the <div id="footer"></div> element.
   Do not remove the "footer" element even if it is empty.

8 To customize the sidebar:
   a Add the <div id="aside"></div> element to the launchpad.html file, as follows.

   ```html
   <div id="main">
     <div id="aside">
       $SSO.GetDatFile("launchpadMain.html")$
     </div>
   </div>
   ```

   b Add content to the <div id="aside"></div> element.
   Example:

   ```html
   <div id="aside">
     <img src="/files/img/your_logo.png">
     $first line of SSO.GetDatFile("version.txt")$
     MWG: $MWG.Version$<br>$MWG.BuildNumber
   </div>
   ```

   This example displays the logo you provide, the version number of the latest update from the update server, and the version and build numbers of the appliance in the sidebar.

9 To close the Template Editor, click OK.

10 Click Save Changes.

**Edit the default launchpad style sheet**

In the default launchpad style sheet that comes with the appliance, you can customize the look of your organization's name and description. You can also customize the header, footer, and sidebar that frame the launchpad.

For example, you can specify the background image that frames the launchpad. The image file can be located in the /files/img or /dat folder.

Alternatively, you can import a custom style sheet.
Task
1 Select Policy | Settings.

2 Expand Engines | Single Sign On, then select Default.
   The Single Sign On settings open.

3 From the Collection drop-down list, select Single Sign On Schema, then click Edit.
   The Template Editor opens with the Single Sign On Schema folder selected.

4 In the File System area, expand singleSignOn, then select customLaunchpad.css.
   The Editor opens.

5 In the editor, specify the font color, font-size, and font-family properties of your organization's name and description as you want them to look on the launchpad.
   Example:
   ```
   /* Organization Name */
   #mainDesc
   { 
    color:RGB(51,51,51);
    font-size: 12pt;
    font-family:verdana;
   }
   
   /* Organization Description */
   #subDesc
   { 
    color:RGB(102,102,102);
    font-size: 9pt;
    font-family:verdana;
   }
   ```

6 In the editor, specify the background image that frames the launchpad.
   In the following example, the background image can be a logo that is repeated until it fills the frame around the launchpad.
   ```
   body {
    width: 100%;
   }
   
   #main {
   // In one of the following lines, replace <image_file> with the filename
   // of the background image and remove the comment tag from that line:
   // background: url("/files/img/<image_file>") repeat;
   // background: url("/dat/<image_file>") repeat;
    padding: 0px;
   }
   
   #aside {
    display: inline-block;
    width: 100px;
    align-self: flex-start;
   }
   ```

7 To close the Template Editor, click OK.

8 Click Save Changes.
Import a custom launchpad style sheet

In the user interface, you can import a launchpad style sheet. It can be one that you exported and edited or one of your own.

When using your own style sheet, remember to place the .css file in the /files directory and to update the name of the .css file in Launchpad.html.

Task
1. Select Policy | Settings.
2. Expand Engines | Single Sign On, then select Default.
   The Single Sign On settings open.
3. From the Collection drop-down list, select Single Sign On Schema, then click Edit.
   The Template Editor opens with the Single Sign On Schema folder selected.
4. In the File System area, select singleSignOn.
5. From the Add drop-down list, select Existing File or Directory, browse for your style sheet file, then click Open.
   Your style sheet file is added to the File System under singleSignOn.
6. To close the Template Editor, click OK.
7. Click Save Changes.

Provide a custom logo for the launchpad

To provide a logo that represents your organization or product on the application launchpad, import a custom image file.

Remember to place the image file in the /files/img or /dat folder and to update the name (and optionally the location) of the image file in Launchpad.html.

Task
1. Select Policy | Settings.
2. Expand Engines | Single Sign On, then select Default.
   The Single Sign On settings open.
3. From the Collection drop-down list, select Single Sign On Schema, then click Edit.
   The Template Editor opens with the Single Sign On Schema folder selected.
4. In the File System area, expand singleSignOn, then select img.
5. From the Add drop-down list, select Existing File or Directory, browse for the file containing your logo, then click Open.
   The image file is added to the File System under img.
6. To close the Template Editor, click OK.
7. Click Save Changes.
Creating bookmarks to cloud services for your organization

You can create bookmarks to cloud services or applications for users across your organization.
To create a bookmark, format the link as follows:
https://sso.mwginternal.com/login?service=<S>

Where <S> specifies the Service ID in the SSO Catalog.

When users click the link to the service, the SSO module delivers the HTML template for the logon page. The JavaScript in the HTML template retrieves the user's account information for the specified service. Depending on the number of accounts the user has, one of the following actions takes place:

- The user has no account in the service — The user is redirected to the launchpad, which presents the option of creating an account. After creating an account, the user can log on to the service following the SSO process.
- The user has one account in the service — The user can log on to the service following the SSO process.
- The user has more than one account in the service — The user is redirected to the launchpad, which presents the option of selecting an account. After selecting an account, the user can log on to the service following the SSO process.

Monitoring logons to cloud services on the dashboard

On the dashboard in the user interface, you can view statistics about the number of logons to all cloud applications and services.

Select Dashboard | Charts and Tables | Single Sign On Statistics to view the following information:

- **All Logins** — Shows the number of logons to all cloud applications and services over the specified time period.
- **Logins per service** — Shows the number of logons by cloud application or service over the specified time period.
- **Logins per service** — Lists the specified number of cloud applications and services from most to least often accessed, including how many times each service was accessed.
- **Number of forbidden logins** — Shows the number of logons to all cloud applications and services over the specified time period that were denied because of invalid tokens.

Single Sign On rule set summary

You configure and manage single sign-on through the Single Sign On rule set as well as related lists and settings.

The Single Sign On rule set comes with a default configuration that you can use and modify. When you first import and select the rule set, the default configuration opens in the simpler, locked view. You can configure and manage single sign-on using the locked view alone.

To access the more advanced view of the rule set, you unlock the view. If you unlock the view and find that you prefer the simpler, locked view, you cannot undo this action. To go back to the simpler, locked view, you must delete the rule set and import it again.

In the unlocked view of the default configuration, the nested rule sets are arranged and processed in the following order. Unless noted, all rule sets are enabled by default.
1. **Select Services** — Rules in this rule set add services to an internal map that determines whether the current user has access to the requested cloud service. The services are added from default lists that you configure.

2. **SSO Management** — This rule set contains the nested rule sets that manage single sign-on.

3. **Perform SSO** — This rule set contains the rule that processes the logon form.

The SSO Management rule set contains the following nested rule sets. They are arranged and processed in the order shown.

1. **HTTPS Handling** — Rules in this rule set secure all launchpad communication using the HTTPS protocol.

2. **Launchpad** — Rules in this rule set generate the application launchpad and logon page using the Single Sign On module settings.

3. **OTP Authentication** — Rules in this rule set enforce OTP authentication as a secondary authentication method. This rule set is disabled by default.

4. **Get Login Action** — This rule set retrieves information about the connector to the service that the user is requesting. For HTTP services, rule set processing stops. For other services, the rule set checks whether the user has the right to access the requested service.

5. **Process Common Tasks** — This rule set processes common SSO tasks using the Single Sign On module settings. It also contains the rule that blocks access to SSO resources that do not exist.

The Get Login Action rule set contains the following nested rule sets. They are arranged and processed in the order shown.

1. **Get Attributes on Premise** — Rules in this rule set fetch user information from an external LDAP data source for SAML single sign-on. The rule set only applies when Web Gateway is installed and running on premise.

2. **Get Attributes in the Cloud** — This rule set constructs the data needed for SAML single sign-on from the authenticated user name. It only applies when Web Gateway is installed and running in the cloud.

3. **Perform SAML SSO** — This rule set generates a response that contains the user information needed for completing single sign-on to the requested SAML service.

4. **Perform IceToken SSO** — This rule set generates a response that contains the user information needed for completing single sign-on to the requested service using the custom IceToken Web Gateway provides.

---

### Key elements for configuring cloud single sign-on

The key elements view of the Single Sign On rule set allows you to modify commonly used SSO settings.

#### SSO Settings

The SSO settings allow you to configure the Single Sign On module. The SSL Scanner settings ensure that all SSO communication with the launchpad is secured with the HTTPS protocol. When single sign-on is implemented in proxy mode, the SSL Scanner module must also be enabled.
Table 14-17  SSO settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO settings</td>
<td>Clicking Edit opens the default settings used by the Single Sign On module.</td>
</tr>
<tr>
<td>SSL Scanner settings</td>
<td>Clicking Edit opens the certificate settings that allow you to secure SSO communication with the launchpad.</td>
</tr>
</tbody>
</table>

SSO Services

These settings allow you to configure lists of connectors to services users are allowed to access.

Table 14-18  SSO services

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services for authenticated users</td>
<td>Clicking Edit opens the Default SSO Services list of connectors to services individual users are allowed to access. You can add connectors to and remove connectors from this list.</td>
</tr>
<tr>
<td>Shared SSO services</td>
<td>Clicking Edit opens the Shared SSO Services list of connectors to services, which users who share an account are allowed to access. You can add connectors to and remove connectors from this list.</td>
</tr>
</tbody>
</table>

Host Names for Easy Login

These settings allow you to configure host names for use in place of Service IDs.

Table 14-19  Host name mapping

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Host name mapping | Clicking Edit opens the SSO Host to Service ID mapping list, where you can map host names to Service IDs. When the mappings are configured, users can access cloud services by entering one of the following short URLs in the browser address window:  
  • http://<hostname>  
  • https://<hostname> |

Support SAML & IceToken SSO

These settings allow you to configure an LDAP data fetching method for single sign-on to cloud services and applications that use the SAML or IceToken authentication method.

Table 14-20  Support SAML & IceToken SSO

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Support for SAML &amp; IceToken SSO</td>
<td>When selected, enables single sign-on to services and applications that use the SAML or IceToken authentication method.</td>
</tr>
</tbody>
</table>
| Get Additional Attributes via  | Select an LDAP data fetching method:  
  • LDAP — Specifies using the Authentication module to fetch data from one or more LDAP servers.  
    The Authentication module supports fallback when multiple LDAP servers are configured.  
  • LDAP as External List — Specifies using the External Lists module to fetch data from a single LDAP server. |
Table 14-20  Support SAML & IceToken SSO (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Settings</td>
<td>Clicking Edit opens the Authentication module settings, where you can configure one or more LDAP servers as the data source.</td>
</tr>
<tr>
<td>LDAP as External List</td>
<td>Clicking Edit opens the External Lists module settings, where you can configure one LDAP server as the data source.</td>
</tr>
</tbody>
</table>

**OTP Usage (One Time Passwords)**

These settings allow you to configure and require OTP authentication.

Table 14-21  OTP usage (one-time passwords)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need OTP to access services</td>
<td>When selected, specifies that a one-time password is required for single sign-on in addition to a primary authentication method.</td>
</tr>
<tr>
<td>OTP server settings</td>
<td>Clicking Edit opens the OTP settings.</td>
</tr>
</tbody>
</table>
| OTP delivery method             | Selecting an option specifies how the one-time password is delivered:  
• Generated OTP (Pledge) — Pledge, an OTP client on a desktop computer or mobile device, generates the one-time password.  
• Delivered OTP — The OTP server generates the one-time password and delivers it by email or SMS.                                    |
| Services that require OTP       | Clicking Edit opens the OTP Secured SSO Services list, where you can add services to the list.                                                                                                       |

**Single Sign On rule set reference**

Using the nested rule sets that come with the Single Sign On rule set, you can configure SSO access to cloud services and applications for end users in your organization.

**Library rule set – Single Sign On**

Criteria – Always  
Cycles – Requests (and IM), Responses

The Single Sign On rule set contains the following nested rule sets:

• Select Services  
• SSO Management  
  • HTTPS Handling  
  • Launchpad  
  • OTP Authentication  
• Get Login Action  
  • Get Attributes on Premise  
  • Get Attributes in the Cloud
• Perform SAML SSO
• Perform IceToken SSO
• Process Common Tasks
• Perform SSO

The rule sets nested in the SSO Management rule set are executed when the SSO.IsManagementRequest property returns a true value. This property is set to true in response to internal and external SSO requests, as follows:

• Internal SSO requests — The SSO.Action property returns a string value corresponding to an internal SSO request action.

• External SSO requests — An external SSO request is sent to the Web Gateway SSO service URL.

The rule sets nested in the Get Login Action rule set fetch user information and perform single sign-on to SAML cloud services and applications.

Select Services rule set

The rules in this rule set retrieve the specified list of cloud services, which the authenticated user or users of a shared account are allowed to access. The list and other information that you configure using the rules in this rule set are then available to the module for other SSO operations.

<table>
<thead>
<tr>
<th>Nested library rule set – Select Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

Add default SSO services (individual accounts)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.IsAuthenticated equals true AND String.IsNullOrEmpty(Authentication.UserName) equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>
| Events       | SSO.AddServices ("defaultIDP", Authentication.UserName, Default SSO Services, 
                   {
                   "label":"Individual",
                   "permit-usage":"yes",
                   "permit-management":"yes"
                   })<Default> |

If the user is authenticated, the Single Sign On module retrieves the specified list of cloud services, which the user is then allowed to access.

The Single Sign On module executes the event with the following properties and settings:

• "defaultIDP" — Specifies the domain in the credential store where user account information is stored.

• Authentication.UserName — Specifies the name of the authenticated user.

• Default SSO Services — Specifies a list of services that the authenticated user is allowed to access.
The following options form one parameter in JSON format:

- **"label"** — Specifies the type of account: individual or shared.
- **"permit-usage"** — Allows you to permit, deny, or require OTP authentication for access to the services on the list by the authenticated user. To configure access, specify the following values respectively: "yes", "no", or "otp".
- **"permit-management"** — Allows you to permit, deny, or require OTP authentication for access to account management functions by the authenticated user. To configure access, specify the following values respectively: "yes", "no", or "otp".
- **<Default>** — Specifies settings for connecting to the SSO service provided by Web Gateway.

### Add OTP secured SSO services (individual accounts, use after OTP authentication)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.IsAuthenticated equals true AND String.IsEmpty(Authentication.UserName) equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>SSO.AddServices(&quot;defaultIDP&quot;, Authentication.UserName, OTP Secured SSO Services, { &quot;label&quot;:&quot;Individual&quot;, &quot;permit-usage&quot;:&quot;otp&quot;, &quot;permit-management&quot;:&quot;otp&quot; })&lt;Default&gt;</td>
</tr>
</tbody>
</table>

If the user is authenticated, the Single Sign On module retrieves the specified list of cloud services. The user is allowed to access or manage these OTP-secured services after authenticating again with a one-time password entered on the launchpad.

The module executes the event with the following properties and settings:

- **"defaultIDP"** — Specifies the domain in the credential store where user account information is stored.
- **Authentication.UserName** — Specifies the name of the authenticated user.
- **OTP Secured SSO Services** — Specifies a list of services that the authenticated user is allowed to access after authenticating again with a one-time password.
The following options form one parameter in JSON format:

- "label" — Specifies the type of account: individual or shared.

- "permit-usage" — Allows you to require OTP authentication for access to the services on the list by the authenticated user. Value: "otp"

- "permit-management" — Allows you to require OTP authentication for access to account management functions by the authenticated user. Value: "otp"

- <Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.

Add shared SSO services (shared accounts)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>SSO.AddServices (&quot;defaultIDP&quot;, &quot;sharedAccounts&quot;, Shared SSO Services, { &quot;label&quot;:&quot;Shared&quot;, &quot;permit-usage&quot;:&quot;yes&quot;, &quot;permit-management&quot;:&quot;yes&quot; })&lt;Default&gt;</td>
</tr>
</tbody>
</table>

The Single Sign On module retrieves the specified list of cloud services, which authenticated users of the shared account are then allowed to access.

- "defaultIDP" — Specifies the domain in the credential store where user account information is stored.

- "sharedAccounts" — Specifies a shared account.

- Shared SSO Services — Specifies a list of services, which authenticated users of the shared account are allowed to access.

The following options form one parameter in JSON format:

- "label" — Specifies the type of account: individual or shared.

- "permit-usage" — Allows you to permit, deny, or require OTP authentication for access to the services on the list by users of the shared account. To configure access, specify the following values respectively: "yes", "no", or "otp".

- "permit-management" — Allows you to permit, deny, or require OTP authentication for access to account management functions by users of the shared account. To configure access, specify the following values respectively: "yes", "no", or "otp".

- <Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.

Handle single sign on using memorable hosts

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Map.HasKey (SSO Host to Service ID mapping, URL.Host) equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Redirect</td>
</tr>
<tr>
<td>Events</td>
<td>Set Redirect.URL = &quot;http://&quot; + SSO.ManagementHost&lt;Default&gt; + &quot;/login?service=&quot; + Map.GetStringValue (SSO Host to Service ID mapping, URL.Host)</td>
</tr>
</tbody>
</table>
If the SSO Host to Service ID Mapping includes the host name configured for the requested cloud service, the request is redirected to the URL configured for that service.

The Single Sign On module constructs the redirect URL from the specified string values and the following properties and settings:

- **SSO.ManagementHost** — Specifies the host name of the SSO service provided by Web Gateway.
- **<Default>** — Specifies settings for connecting to the SSO service provided by Web Gateway.
- **Map.GetStringValue (SSO Host to Service ID Mapping, URL.Host)** — Looks up the host name of the requested service in the SSO Host to Service ID map and returns the Service ID of that service.

### HTTPS Handling rule set

This rule set secures SSO communication between the end user and the launchpad with the HTTPS protocol.

<table>
<thead>
<tr>
<th>Nested library rule set – HTTPS Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

#### Enable SSL

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Command.Name equals &quot;CONNECT&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
</tbody>
</table>
| Events       | Enable SSL Client Context without CA <Launchpad certificate>  
|              | Enable SSL Scanner <Enable Content Inspection> |

If an SSO connection is required, this rule stops the request cycle. The Single Sign On module provides an SSL certificate and enables content inspection.

The module executes the events with the following settings:

- **<Launchpad certificate>** — Specifies the SSL certificate and settings. This certificate can be the default or one that you import.
- **<Enable Content Inspection>** — Specifies the settings that enable content inspection by the SSL Scanner module.

#### Enforce SSL

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Connection.Protocol equals &quot;HTTP&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Redirect&lt;Default&gt;</td>
</tr>
</tbody>
</table>
| Events       | Set URL.Protocol = "https"  
|              | Set Redirect.URL = URL |

If the connection protocol is HTTP, the Single Sign On module sets the SSO protocol to "https" and the SSO request is redirected to the requested URL.

The rule executes the redirect action with the following settings:

- **<Default>** — Specifies settings for connecting to the SSO service provided by Web Gateway.
**Launchpad rule set**
This rule set assembles all information needed for generating the launchpad or a logon page.

<table>
<thead>
<tr>
<th>Nested library rule set – Launchpad</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

**Create launchpad**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.Path equals &quot;/&quot; OR URL.Path equals &quot;/launchpad&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;SSO Launchpad&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.SetStatus (200)</td>
</tr>
</tbody>
</table>

If the requested URL specifies the SSO service or the launchpad, this rule generates the launchpad using the following settings:

<SSO Launchpad> — Specifies the language and template settings used to generate the launchpad.

We recommend that you do not modify the launchpad settings.

The Single Sign On module sets the HTTP status code to 200 (OK).

**Create automatic login page**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.Path equals &quot;/login&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;SSO Login Page&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.SetStatus (200)</td>
</tr>
</tbody>
</table>

If the requested URL specifies the SSO logon page, this rule generates the logon page, including the JavaScript, using the following settings:

<SSO Login Page> — Specifies the language and template settings used to generate the logon page.

We recommend that you do not modify the logon page settings.

The Single Sign On module sets the HTTP status code to 200 (OK).
Create automatic login page (compatibility with some services)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.Path matches regex(/login-.+)</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;SSO Login Page&gt;</td>
</tr>
</tbody>
</table>

This rule applies when the requested URL specifies the SSO logon page using the format "/login-<Service ID>" instead of the default format that the SSO service is expecting: "/login?service=<Service ID>". This rule generates the logon page using the following settings:

<SSO Login Page> — Specifies the language and template settings used to generate the logon page.

We recommend that you do not modify the logon page settings.

The Single Sign On module rebuilds the requested URL using the default format and sets the HTTP status code to 200 (OK).

Some SAML services do not allow query parameters in the IdP URL when single sign-on is SP-initiated.

**OTP Authentication rule set**

Enabling this rule set allows you to enforce OTP authentication as a secondary authentication method for end users who want to access cloud services and applications.

**Nested library rule set – OTP Authentication**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>SSO.OtpRequired&lt;Default&gt; equals true</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Requests (and IM)</td>
</tr>
</tbody>
</table>

The rules in this rule set are executed when the SSO action requires OTP authentication.

**Prepare OTP context**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.HasParameter (&quot;requestOTP&quot;) equals true OR URL.HasParameter (&quot;pledgeOTP&quot;) equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Authentication.SendOTP&lt;OTP&gt;</td>
</tr>
</tbody>
</table>

If there is a request for a one-time password from an authenticated user, the Single Sign On module sends the password to the user. The types of OTP requests are:

- "requestOTP" — The user requests the one-time password through the McAfee OTP server.
- "pledgeOTP" — The user requests the one-time password through Pledge, an OTP client running locally on a computer or mobile device.

The module executes the event with the following settings:

<OTP> — Specifies settings for OTP authentication.
Return OTP context

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>URL.HasParameter (&quot;requestOTP&quot;) equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.GenerateResponse (JSON.ToString (JSON.StoreByName (JSON.CreateObject, &quot;otp-context&quot;, JSON.FromString (Authentication.OTP.Context&lt;OTP&gt;)))) HTTP.SetStatus (403)</td>
</tr>
</tbody>
</table>

If there is a request for a one-time password from an authenticated user, this rule stops the request cycle. The Single Sign On module generates a response containing the OTP context in a JSON object. The OTP context is provided in a header field when the McAfee OTP Server responds with a one-time password.

The module executes this event with the following settings:

<OTP> — Specifies settings for OTP authentication.

The module sets the HTTP status code to 403 (Forbidden).

Verify delivered OTP

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.Authenticate&lt;OTP&gt; equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.GenerateResponse (&quot;{&quot;authentication-required&quot;:&quot;delivered-otp&quot;}&quot;) HTTP.SetStatus (403)</td>
</tr>
</tbody>
</table>

If OTP authentication fails, this rule stops the request cycle. The Single Sign On module generates a response specifying the authentication result and method. The method, delivered OTP, specifies delivery of the one-time password by the McAfee OTP Server.

The module executes this event with the following settings:

<OTP> — Specifies settings for OTP authentication.

The module sets the HTTP status code to 403 (Forbidden).

Verify Pledge generated OTP

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.Authenticate&lt;OTP&gt; equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.GenerateResponse (&quot;{&quot;authentication-required&quot;:&quot;generated-otp&quot;}&quot;) HTTP.SetStatus (403)</td>
</tr>
</tbody>
</table>

Enable this rule if one-time passwords are delivered by McAfee OTP Server.
If OTP authentication fails, this rule stops the request cycle. The Single Sign On module generates a response specifying the authentication result and method. The method, generated OTP, specifies generation of the one-time password by the Pledge OTP client.

The module executes this event with the following settings:

<OTP> — Specifies settings for OTP authentication.

The module sets the HTTP status code to 403 (Forbidden).

Enable this rule if one-time passwords are generated by the Pledge OTP client.

### Get Login Action rule set

This rule set retrieves information about the connector to the requested cloud service or application. For HTTP cloud connectors, processing of the rule set then stops. For other cloud connectors, the rule set checks whether the user has the right to access the requested cloud service or application.

<table>
<thead>
<tr>
<th>Nested library rule set – Get Login Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – SSO.Action&lt;Default&gt; equals &quot;GetLoginAction&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

### Get connector info

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.sso-conn-info = SSO.GetConnectorInfo(String.ToSSOConnector (URL.GetParameter (&quot;service&quot;)))</td>
</tr>
</tbody>
</table>

The Single Sign On module retrieves information about the connector to the service the user is requesting and stores it as a JSON object in a local variable named sso-conn-info. This information includes the following:

- **Name** (string) — Specifies a user-defined name for the cloud connector.
- **Service ID** (string) — Uniquely identifies the cloud service or application.
- **Type** (string) — Specifies the authentication method used by the cloud service.
  Values: HTTP, SAML2
- **Inline** (Boolean) — If true, the cloud connector supports a dynamic HTTP cloud service, which requires single sign-on in proxy or inline mode.
- **Deprecated** (Boolean) — If true, the cloud connector is no longer supported.

### Stop rule set for form based logins

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>JSON.AsString (JSON.GetByName (User-Defined.sso-conn-info, &quot;type&quot;)) equals &quot;http&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Rule Set</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

If the cloud connector type is HTTP, this rule stops the Get Login Action rule set.
Validate user’s access permissions

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>SSO.UserHasAccessToService (URL.GetParameter (&quot;realm&quot;), URL.GetParameter (&quot;user&quot;), URL.GetParameter (&quot;service&quot;), &quot;usage&quot;)&lt;Default&gt; equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;SSO: User Has No Access To Service&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

This rule checks the "service" and "usage" parameters to verify that the user has the right to access the requested service or application. If the "service" parameter is empty or the "usage" parameter is set to "no", this rule blocks access to the requested service.

This rule is executed with the following settings:
- <Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.
- <SSO: User Has No Access To Service> — Specifies the language and template settings used to generate the block message for the user.

Get Attributes on Premise rule set

The rules in this rule set fetch user information from an external LDAP data source for SAML single sign-on. This rule set is disabled by default and only applies when Web Gateway is installed and running on premise and the SSO type is SAML2.

<table>
<thead>
<tr>
<th>Nested library rule set – Get Attributes on Premise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – InTheCloud equals false AND JSON.AsString (JSON.GetByName (User-Defined.sso-conn-info, &quot;type&quot;)) does not equal &quot;HTTP&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

Get additional attributes from LDAP

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>

The Single Sign On module fetches information about the user from an external LDAP data source through the Authentication filter. It then stores the information as a JSON object in a local variable named sso-user-data. The user information consists of the attribute name-value pairs expected by the SAML service or application.

This event is executed with the following settings:
- <LDAP Authentication> — Specifies the Authentication module settings configured for the external LDAP data source.
Get additional attributes from LDAP using External Lists

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.sso-user-data = ExtLists.JSON (Authentication.UserName, &quot;,&quot;, &quot;,&quot;)&lt;LDAP Source&gt;</td>
</tr>
</tbody>
</table>

The Single Sign On module fetches information about the user from an external LDAP data source through the External Lists module. It then stores the information as a JSON object in a local variable named `sso-user-data`. The user information consists of the attribute name-value pairs expected by the SAML service or application.

This event is executed with the following settings:

`<LDAP Source>` — Specifies the External Lists module settings configured for the external LDAP data source.

Get Attributes in the Cloud rule set

This rule set constructs the data needed for SAML single sign-on from the authenticated user name. It is disabled by default and only applies when Web Gateway is installed and running in the cloud and the SSO type is SAML2.

<table>
<thead>
<tr>
<th>Nested library rule set – Get Attributes in the Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – InTheCloud equals true AND JSON.AsString (JSON.GetByName (User-Defined.sso-conn-info, &quot;type&quot;)) does not equal &quot;HTTP&quot;</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rule.

Populate user's data from user name

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Authentication.IsAuthenticated equals true AND Authentication.UserName matches <em>@</em> AND JSON.Size (User-Defined.sso-user-data) equals 0</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.sso-user-data = JSON.StoreByName (User-Defined.sso-user-data, &quot;mail&quot;, JSON.FromString (Authentication.UserName))</td>
</tr>
</tbody>
</table>

This rule only applies when the user is authenticated, the user name is an email address, and the `sso-user-data` variable is empty. The rule stores the attribute name-value pair formed by "mail" and the user's email address as a JSON object in the `sso-user-data` variable.
Perform SAML SSO rule set
This rule set generates a response that contains the end user information needed for completing single sign-on to the requested SAML service or application.

<table>
<thead>
<tr>
<th>Nested library rule set – Perform SAML SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

This rule set contains the following rule.

Get login action (SAML)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>JSON.AsString (JSON.GetByName (User-Defined.sso-conn-info, &quot;type&quot;)) matches saml*</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.GenerateResponse (SSO.GetSAMLLoginAction (URL.GetParameter (&quot;service&quot;), User-Defined.sso-user-data)&lt;Default&gt;)</td>
</tr>
</tbody>
</table>

If the cloud connector type is SAML2, this rule stops the request cycle. The Single Sign On module generates a response containing the user information needed for completing single sign-on to the requested SAML service or application.

This event is executed with the following settings:

<Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.

Perform IceToken SSO rule set
This rule set generates a response that contains the end user information needed for completing single sign-on to the requested service or application.

<table>
<thead>
<tr>
<th>Nested library rule set — Perform IceToken SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria — Always</td>
</tr>
<tr>
<td>Cycles — Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rule.

Get login action (IceToken)

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>JSON.AsString (JSON.GetByName (User-Defined.sso-conn-info, &quot;type&quot;)) equals &quot;icetoken&quot;</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.GenerateResponse (SSO.GetIceTokenLoginAction (URL.GetParameter (&quot;service&quot;), User-Defined.sso-user-data)&lt;Default&gt;)</td>
</tr>
</tbody>
</table>

If the cloud connector type is IceToken, this rule stops the request cycle. The Single Sign On module generates a response containing the user information needed for completing single sign-on to the requested service or application.
This event is executed with the following settings:

<Default> — Specifies settings for connecting to the SSO service provided by Web Gateway.

**Process Common Tasks rule set**
This rule set processes common SSO tasks and blocks access to SSO resources that do not exist.

<table>
<thead>
<tr>
<th>Nested library rule set – Block Management Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

**Process common tasks**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>SSO.ProcessTask&lt;Default&gt; equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

This rule processes common SSO tasks, such as credential management.

**Block invalid or unhandled management requests**

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Block&lt;File Not Found&gt;</td>
</tr>
<tr>
<td>Events</td>
<td>HTTP.SetStatus (404)</td>
</tr>
</tbody>
</table>

This rule blocks access to a requested resource, when the resource does not exist, and is executed with the following settings:

<File Not Found> — Specifies the language and template settings used to generate the block message for the end user.

The Single Sign On module sets the HTTP status code to 404 (Not Found).

**Perform SSO rule set**
This rule set allows the end user to log on to an HTTP cloud service or application when single sign-on is implemented in proxy (inline) mode.

<table>
<thead>
<tr>
<th>Nested library rule set – Perform SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses</td>
</tr>
</tbody>
</table>

This rule set contains the following rule.
Process form login

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>SSO.ProcessFormLogin&lt;Default&gt;</td>
</tr>
</tbody>
</table>

The Single Sign On module processes the logon form that users complete to access HTTP cloud services or applications in proxy (inline) mode. The execution of the event depends on the step in the logon process, as follows:

- The user requests the logon form — The event adds JavaScript to the logon page, enabling single sign-on to dynamic HTTP cloud services, and replaces the real password with a password token.
- The user submits the logon form — The event replaces the password token with the real password.

The SSO module executes this event with the following settings:

<Default> - Specifies settings for connecting to the SSO service provided by Web Gateway.

Single Sign On lists and settings

The Single Sign On module retrieves values and parameters for the SSO properties and events used by the rules in the Single Sign On rule set according to the settings you configure. Some of the settings used by the module are configured as lists.

Single Sign On lists

Some of the settings used by the Single Sign On module are configured as lists.

SSO Host to Service ID Mapping

This list lets you map a name that is easy to remember (host name) to the service ID of a configured connector. The user types the host name in the address field of a web browser. Then the Single Sign On module looks up the host name in the map and finds the service ID. Internally, the host name and service ID are stored as a list of key-value pairs.

This feature is especially useful for custom connectors whose service ID, which is assigned by the module, has a numeric value.

To locate this list, select Policy | Lists | Custom Lists | MapType.

Table 14-22   SSO host to service ID mapping

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Allows you to specify a name for a configured connector that is easy to remember. Example: MyConnector</td>
</tr>
<tr>
<td>Value</td>
<td>Specifies the service ID of the configured connector. You can look up the service ID in the SSO Catalog.</td>
</tr>
</tbody>
</table>

SSO Services

The Single Sign On module comes with default lists that you can configure to determine which cloud services users are allowed to access. You can also create and configure your own access control lists.

To locate these lists, select Policy | Lists | Custom Lists | SSO Connector.
Table 14-23  SSO services

<table>
<thead>
<tr>
<th>List name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default SSO Services</td>
<td>Specifies a default list of configured connectors to cloud services that a user is allowed to access.</td>
</tr>
<tr>
<td>OTP Secured SSO Services</td>
<td>Specifies a list of configured connectors to cloud services that require OTP authentication in addition to a primary authentication method.</td>
</tr>
<tr>
<td>Shared SSO Services</td>
<td>Specifies a list of configured connectors to cloud services that users who share an account are allowed to access.</td>
</tr>
</tbody>
</table>

SSO Catalog

In the SSO Catalog, you can view information about the predefined and custom cloud connectors. You can configure new connectors from templates and view them in the list of custom connectors.

To locate these lists, select Policy | Lists | System Lists | SSO Catalog.

Table 14-24  SSO Catalog

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>The default icon is the logo that identifies the cloud service or application for which the connector is configured. For custom connectors, you can replace the default icon with a custom image.</td>
</tr>
</tbody>
</table>
| Name   | Specifies the name of the predefined or custom connector.  
  • Predefined connectors — The name, which is the same as the service ID, is assigned by the module.  
  • Custom connectors — The name is assigned by the administrator who configures the connector instance. |
| Description | (Optional) Describes each connector instance. |
| Categories | Specifies the type of service that the cloud service or application provides the user. You can modify the default value or configure multiple categories.  
  Examples: Business Intelligence, Content Management, Security |
| Service ID | Uniquely identifies each connector.  
  • Predefined connectors — The identifier is the name of the cloud service or application.  
    Example: ABIresearch  
  • Custom connectors — The identifier is a number assigned by the module.  
    Example: 229 |
| Types   | Specifies the authentication method used by the cloud service or application for which the connector is configured.  
  Values: HTTP, SAML2 |

Single Sign On settings

The Single Sign On module retrieves values and parameters for the SSO properties and events used by the rules in the Single Sign On rule set according to the settings you configure.

To locate the default SSO settings, select Policy | Settings | Engine | Single Sign On | Default.

Single Sign On

Specify the settings needed for connecting to the SSO service provided by Web Gateway.
Table 14-25  Single Sign On

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Host</td>
<td>Specifies the URL of the server where Web Gateway is installed and the SSO process is running. SSO requests are addressed to this URL. Web Gateway recognizes requests received at this URL as SSO requests. When SSO requests are received, the SSO.IsManagementRequest property is set to true. Default value: sso.mwginternal.com For non-proxy mode, configure this setting as the IP address of the Web Gateway appliance. To process requests in proxy and non-proxy modes, configure two rule sets, each rule set using a different Management Host setting.</td>
</tr>
<tr>
<td>Language</td>
<td>Select an option:</td>
</tr>
<tr>
<td></td>
<td>• Auto (Browser) — Specifies using the browser's language setting when displaying text on the launchpad and logon pages.</td>
</tr>
<tr>
<td></td>
<td>• Force to: From the drop-down list, select the language to use when displaying text on the launchpad and logon pages.</td>
</tr>
<tr>
<td>Collection</td>
<td>From the drop-down list, select a template collection, then click Edit. The Template Editor opens.</td>
</tr>
<tr>
<td></td>
<td>• Default Schema — Provides user message templates that you can customize.</td>
</tr>
<tr>
<td></td>
<td>• SAML Request Schema — Provides templates for SAML authentication requests (SAMLRequest.html) and responses (SAMLRedirectToAuth.html) sent to and received from an external Identity Provider, respectively.</td>
</tr>
<tr>
<td></td>
<td>• Single Sign On Schema — Provides templates for customizing the application launchpad and logon pages.</td>
</tr>
<tr>
<td></td>
<td>These settings can also be configured on the Templates tab.</td>
</tr>
</tbody>
</table>

Login Form

Enable proxy mode and import or export a private key in PEM format.

Table 14-26  Login form

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MWG operates inline (Requires: SSL scanning enabled)</td>
<td>When selected, Web Gateway runs the SSO process in proxy (or inline) mode.</td>
</tr>
<tr>
<td>Private Key to Sign SSO Token</td>
<td>You can import a private key in PEM file format for signing SAML assertions produced by the SSO process. You can also export a private key in PEM file format.</td>
</tr>
</tbody>
</table>

Advanced Settings

Configure P3P string configuration and debug logging level settings for the SSO process.
Table 14-27  Advanced settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>P3P string used for setting SSO token cookies</td>
<td>Specifies a configuration string required for the Platform for Privacy Preferences Project (P3P). This value must match the privacy settings in the end user's browser. Usually, you can use the default value: <code>CP=&quot;NOI CUR OUR STP STA&quot;</code>. The default value must be modified for Internet Explorer. If the P3P string is not correctly set, SSO processing fails.</td>
</tr>
<tr>
<td>Log level (Requires: SSO log rule set)</td>
<td>From the drop-down list, select a log level:</td>
</tr>
<tr>
<td></td>
<td>• Off — Logging is turned off.</td>
</tr>
<tr>
<td></td>
<td>• Error — Only error messages are logged.</td>
</tr>
<tr>
<td></td>
<td>• Access — Error and informational messages are logged to the SSO access log file.</td>
</tr>
<tr>
<td></td>
<td>• Full — All messages are logged to the SSO trace log file.</td>
</tr>
<tr>
<td></td>
<td>To enable SSO logging, import the SSO Log rule set from the Logging rule set group in the Rule Set Library.</td>
</tr>
<tr>
<td></td>
<td>If you set the log level to Full, verify that the Trace Log rule set is enabled.</td>
</tr>
</tbody>
</table>

SSO certificate and private key settings

SAML single sign-on requires X.509 certificates and private keys to sign SAML assertions and requests and to verify SAML signatures.

SSO Certificates

The SSO process uses the X.509 certificate provided by the SAML Service Provider to verify SP requests. You can import X.509 certificates in the SSO Certificates settings.

To locate the settings, select Policy | Settings | Engines | SSO Certificates.

Table 14-28  SSO certificates

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name that uniquely identifies the imported X.509 certificate in the user interface.</td>
</tr>
<tr>
<td>Import</td>
<td>Clicking this option allows you to browse for and select the X.509 certificate file you want to import.</td>
</tr>
<tr>
<td>SSO Certificate</td>
<td>After you import the certificate, the following certificate data is displayed:</td>
</tr>
<tr>
<td></td>
<td>• Subject — Specifies the distinguished name of the entity holding the X.509 certificate. This value corresponds to the Service Provider.</td>
</tr>
<tr>
<td></td>
<td>• Issuer — Specifies the distinguished name of the certificate authority (CA) that signed the certificate. If the subject and issuer are the same, the certificate is self-signed.</td>
</tr>
<tr>
<td></td>
<td>• Validity — Specifies the time period during which the certificate is valid.</td>
</tr>
<tr>
<td></td>
<td>• Extensions — Shows any custom fields added to the certificate, such as a comment.</td>
</tr>
</tbody>
</table>
SSO Private Keys

The SSO process signs outgoing SAML assertions attesting to the end user's identity with a private key. The SAML Service Provider uses the corresponding X.509 certificate to verify the signatures. You must generate or import at least one X.509 certificate and private key pair to support the SAML SSO process. After generating or importing a key pair, the certificate and private key will be available for selection from the drop-down lists in the Web Gateway user interface.

To locate these settings, select Policy | Settings | Engines | SSO Private Keys.

Table 14-29  SSO private keys

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name that uniquely identifies the generated or imported X.509 certificate and private key pair in the user interface.</td>
</tr>
<tr>
<td>Generate</td>
<td>Clicking this option allows you to generate an X.509 certificate and private key pair. The following fields uniquely identify the certificate subject specified by the private key. The certificate subject is the entity holding the certificate or your organization. When you configure the settings, you provide values for your organization.</td>
</tr>
<tr>
<td></td>
<td>• Common Name (Required)</td>
</tr>
<tr>
<td></td>
<td>• Organization (Required)</td>
</tr>
<tr>
<td></td>
<td>• Organizational Unit</td>
</tr>
<tr>
<td></td>
<td>• Locality (Required)</td>
</tr>
<tr>
<td>Valid for</td>
<td>— Specifies the time in years during which the certificate is valid. Comment — (Optional) Allows you to add a comment to the certificate data.</td>
</tr>
<tr>
<td>Import</td>
<td>Clicking this option allows you to import an X.509 certificate and private key. Use this option if you already have an X.509 certificate file and private key pair and want to import them in the user interface.</td>
</tr>
<tr>
<td>Private Key &amp;</td>
<td>After you generate or import an X.509 certificate and private key pair, the following data is displayed:</td>
</tr>
<tr>
<td>Certificate</td>
<td>• Subject — Specifies the distinguished name of the entity holding the X.509 certificate. This value corresponds to Web Gateway.</td>
</tr>
<tr>
<td></td>
<td>• Issuer — Specifies the distinguished name of the certificate authority (CA) that signed the certificate. If the subject and issuer are the same, the certificate is self-signed.</td>
</tr>
<tr>
<td></td>
<td>• Validity — Specifies the time period during which the certificate is valid.</td>
</tr>
<tr>
<td></td>
<td>• Extensions — Shows any custom fields added to the certificate, such as a comment.</td>
</tr>
<tr>
<td></td>
<td>• Private Key — Shows whether the private key is present.</td>
</tr>
<tr>
<td>Export</td>
<td>Clicking this option allows you to export an X.509 certificate. The SAML Service Provider needs this file to verify signed SAML assertions and requests.</td>
</tr>
<tr>
<td>Export Key</td>
<td>Clicking this option allows you to export a private key.</td>
</tr>
</tbody>
</table>

SSO logging overview

The SSO Log rule set generates the SSO access log, and optionally the SSO trace log, from information about SSO requests that the proxy stores in the SSO.LogAttributes property.

The SSO proxy stores information about internal and external SSO requests in the SSO.LogAttributes property. When SSO logging is enabled:
• Internal requests are logged to the SSO access log instead of the general access log.
• External requests, which come from outside Web Gateway, are logged to the general access log.

To enable SSO logging, import the SSO Log rule set from the Logging rule set group in the Rule Set Library. The SSO Log rule set consists of the following nested rule sets:
  • Access Log — Logs error and info messages to the SSO access log file.
  • Trace Log — Logs all messages to the SSO trace log file.
  • Stop Logging — Stops the SSO Log rule set cycle.

The trace log is more detailed than the access log and is intended for debugging the SSO feature.

Enabling SSO logging involves these overall steps:
1 Add the SSO Log rule set to the Log Handler rule set tree.
2 Move the SSO Log rule set above the Default logging rule sets in the Log Handler tree. This step ensures that SSO requests are logged to the SSO access log before the general access log and that the logging cycle is then stopped.
3 (Optional) Enable SSO trace logging.

Enable SSO logging
When you enable SSO logging, SSO requests are logged to the SSO access log instead of the general access log. You can also enable SSO trace logging.

If you enable trace logging, we recommend that you set the log level to Full. To locate the log level setting, select Policy | Settings | Engines | Single Sign On | Default | Advanced Settings.

Task
1 Select Policy | Rule Sets | Log Handler | Default.
2 From the Add drop-down list, select Rule Set from Library.
   The Add from Rule Set Library dialog box opens.
3 Expand Logging, then select SSO Log.
4 If importing the rule set creates conflicts, click Auto-Solve Conflicts, click one of the following strategies, then click OK.
   • Solve by referring to existing objects
   • Solve by copying and renaming to suggested
   The SSO Log rule set is added to the Log Handler tree.
5 In the Log Handler tree, move the SSO Log rule set above the Default rule sets.
6 (Optional) To enable detailed logging:
   a In the Log Handler tree, expand SSO Log, then select the Trace Log rule set.
   b In the configuration window, select the Enable checkbox.
SSO Log rule set reference
The SSO Log rule set is activated when the request is made by an SSO component, including the SSO.Client and SSO.Proxy components.

SSO Log rule set

<table>
<thead>
<tr>
<th>Library rule set – SSO Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – JSON.AsString (JSON.GetName (SSO.LogAttributes, &quot;origin&quot;)) matches SSO.*</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

The SSO.LogAttributes property is a JSON object containing the SSO request attributes shown in the following table. The SSO Log rule set generates the SSO access log and optionally the SSO trace log from the attributes in the JSON object.

Table 14-30  SSO.LogAttributes property

<table>
<thead>
<tr>
<th>SSO request log attribute</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>Specifies the name of the internal action performed in response to the SSO request. Examples include:</td>
</tr>
<tr>
<td></td>
<td>• LoadLaunchpad</td>
</tr>
<tr>
<td></td>
<td>• GetServices</td>
</tr>
<tr>
<td></td>
<td>• StartHTMLLogin, StartSAMLLogin, and StartIceTokenLogin</td>
</tr>
<tr>
<td></td>
<td>• AddCredentials, UpdateCredentials, and DeleteCredentials</td>
</tr>
<tr>
<td>config</td>
<td>Specifies the name of the settings used by the internal action performed in response to the SSO request.</td>
</tr>
<tr>
<td>message</td>
<td>Describes the SSO request.</td>
</tr>
<tr>
<td>origin</td>
<td>Specifies the source of the values that the proxy copies to the SSO.LogAttributes property. The source can be one of the following SSO components:</td>
</tr>
<tr>
<td></td>
<td>• SSO.Client — The proxy copies the values provided by the client (browser) to this property without checking them first.</td>
</tr>
<tr>
<td></td>
<td>• SSO.Proxy — The proxy checks the values provided by the client (browser) before copying them to this property.</td>
</tr>
<tr>
<td></td>
<td>SSO.Client values are used by developers when testing and debugging SSO features and are included in the SSO trace log. For security reasons, only values checked by the proxy (SSO.Proxy values) are included in the SSO access log.</td>
</tr>
<tr>
<td>level</td>
<td>Specifies the log level. Only SSO requests having a log level of four or less are included in the SSO access log. SSO requests having a log level higher than four are also included in the SSO trace log, which is more detailed.</td>
</tr>
<tr>
<td></td>
<td>The log levels are:</td>
</tr>
<tr>
<td></td>
<td>• Off (0) — Logging is turned off.</td>
</tr>
<tr>
<td></td>
<td>• Error (1, 2) — Only error messages are logged.</td>
</tr>
<tr>
<td></td>
<td>• Info (3, 4) — Error and info messages are logged to the SSO access log file.</td>
</tr>
<tr>
<td></td>
<td>• Full (5, 6) — All messages are logged to the SSO trace log file.</td>
</tr>
</tbody>
</table>
Table 14-30  SSO.LogAttributes property (continued)

<table>
<thead>
<tr>
<th>SSO request log attribute</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>Specifies the name of the cloud service in the SSO request.</td>
</tr>
</tbody>
</table>
| outward                   | Specifies whether Web Gateway performs the web server role or the web server is external to Web Gateway. This attribute has one of the following values:  
  • FALSE — Web Gateway is the destination of the SSO request and creates the SSO response. In this case, Web Gateway performs the role of a web server. For example, Web Gateway performs the web server role when the user accesses the launchpad.  
  • TRUE — The SSO request is directed to an external web server, which creates the SSO response. In this case, Web Gateway does not perform the role of a web server. |

SSO Access Log rule set

If the Access Log rule set’s criteria are met, the rule in this rule set writes a log entry to the SSO access log file. Each SSO log entry corresponds to one SSO request. To meet the criteria, the SSO component making the request must be the proxy and the log level in the request must be less than or equal to four.

<table>
<thead>
<tr>
<th>Nested library rule set – Access Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – JSON.AsString (JSON.GetByName (SSO.LogAttributes, &quot;origin&quot;)) matches SSO.Proxy* AND JSON.AsNumber (JSON.GetByName (SSO.LogAttributes, &quot;level&quot;)) less than or equals 4</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

This rule set contains the following rule.
### Write sso_access.log

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>
| Events       | Set User-Defined.logLine = DateTime.ToWebReporterString  
+ " "  
+ Authentication.UserName  
+ " "  
+ String.ReplaceIfEquals (IP.ToString (Client.IP), "", ",-")  
+ " "  
+ String.ReplaceIfEquals (Number.ToString (Response.StatusCode), "", ",-")  
+ " "  
+ Request.Header.FirstLine  
+ " "  
+ "="  
+ JSON.AsString (JSON.GetByName (SSO.LogAttributes, "action"))  
+ "="  
+ JSON.AsString (JSON.GetByName (SSO.LogAttributes, "service"))  
+ "="  
+ JSON.AsString (JSON.GetByName (SSO.LogAttributes, "message"))  
+ "="  
|             | FileSystemLogging.WriteLogEntry (User-Defined.logLine) |

This rule creates the SSO access log entry, then writes the entry to the SSO access log file. The rule creates the log entry by retrieving the following information in string format and concatenating the strings:

- Date and time stamp in Web Reporter format
- User name
- Client IP address (if it exists)
- Status code in the response (if it exists)
- First line of the SSO request header
- Type of SSO request (action)
- Name of the cloud service in the SSO request (service)
- Description of the SSO request (message)

To open and configure the file system log settings, click `<SSO Access Log>`.
SSO Trace Log rule set

The rules in the Trace Log rule set build an SSO trace log entry and write it to the SSO trace log file. The trace log is more detailed than the access log and is intended for debugging the SSO feature.

The Trace Log rule set is disabled by default. When you enable trace logging, we recommend that you set the log level to Full. To locate the log level setting, select Policy | Settings | Engines | Single Sign On | Default | Advanced Settings.

### Nested library rule set – Trace Log

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Always</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles</td>
<td>Requests (and IM), Responses, Embedded Objects</td>
</tr>
</tbody>
</table>

This rule set contains the following rules.

#### Web reporter timestamp

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.logLine = DateTime.ToWebReporterString</td>
</tr>
</tbody>
</table>

This rule sets the SSO trace log entry equal to the date and time stamp in Web Reporter format.

#### Add all sso attributes

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>Set User-Defined.logLine = User-Defined.logLine + &quot; &quot; + JSON.ToString (SSO.LogAttributes) + &quot;&quot;</td>
</tr>
</tbody>
</table>

This rule adds the SSO log attributes in string format to the existing SSO trace log entry.

#### Add firstline for outward requests

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>JSON.AsBool (JSON.GetByName (SSO.LogAttributes, &quot;outward&quot;)) equals true</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>

If the SSO request is handled by an external web server, this rule adds the first line of the request header to the SSO trace log entry.
Add firstline

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
</tbody>
</table>
| Events       | Set User-Defined.logLine = User-Defined.logLine  
              + " "  
              + Request.Header.FirstLine  
              + ""

This rule is disabled by default. When enabled, it adds the first line of the SSO request header to the SSO trace log entry for external and internal requests.

Write sso_trace.log

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Always</td>
</tr>
<tr>
<td>Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Events</td>
<td>FileSystemLogging.WriteLogEntry (User-Defined.logLine)&lt;SSO Trace Log&gt;</td>
</tr>
</tbody>
</table>

This rule writes the SSO trace log entry to the SSO trace log file. To open and configure the file system log settings, click <SSO Trace Log>.

SSO Stop Logging rule set

The SSO Stop Logging rule set stops the logging cycle after internal SSO requests are logged to the SSO access log and before they can be logged to the general access log.

Nested library rule set – Stop Logging

Criteria – Always  
Cycles – Requests (and IM), Responses, Embedded Objects

This rule set contains one rule.

Avoid additional logging of internal SSO requests

<table>
<thead>
<tr>
<th>Rule element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>JSON.AsBool (JSON.GetByName (SSO.LogAttributes, &quot;outward&quot;)) equals false</td>
</tr>
<tr>
<td>Action</td>
<td>Stop Cycle</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

If the SSO request is handled by Web Gateway internally, this rule stops the current cycle of the SSO Log rule set. This action prevents internal SSO requests from being logged to the general access log.

For this rule to be effective, you must add the SSO Log rule set to the Log Handler tree above the Default logging rule set.
Resolving SSO issues

See the following table for SSO issues and ways to resolve them.

**Table 14-31 Resolving SSO issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The credential store fails to return credentials when requested.</td>
<td>Check the error log for credential store errors (34050–34090).</td>
</tr>
<tr>
<td>The end user cannot log on to the selected cloud service.</td>
<td>The connector to the service might be broken. Contact the SSO Catalog support team.</td>
</tr>
<tr>
<td>The end user cannot update credentials for a cloud service.</td>
<td>Check the order of the rules in the Single Sign On rule set. The Select Services rule set, which adds services to SSO Connector lists, must be located before the Manage Form Credentials rule set.</td>
</tr>
<tr>
<td>SAML single sign-on fails.</td>
<td>Possible reasons for SAML SSO failure are:</td>
</tr>
<tr>
<td></td>
<td>• Not all user information is provided — Some cloud applications require specific user attributes. To view the missing user attributes, check the error log for SSO errors (34000–34999).</td>
</tr>
<tr>
<td></td>
<td>• Single sign-on is not configured correctly — Verify that single sign-on is configured correctly in the Web Gateway user interface and in the SAML application administrator account.</td>
</tr>
<tr>
<td>When automatic downloading of SAML metadata is configured and the download fails, an error is returned stating that the requested service does not exist.</td>
<td>Possible reasons for this error are:</td>
</tr>
<tr>
<td></td>
<td>• The metadata is downloaded from an HTTPS URL without a trusted certificate.</td>
</tr>
<tr>
<td></td>
<td>• The signature in the SAML metadata file is incorrect.</td>
</tr>
<tr>
<td></td>
<td>• The SAML metadata file is missing the signature.</td>
</tr>
</tbody>
</table>

For more information about this error, see the file: /opt/mcfc/log/mcfc.log.
Cloud storage encryption

When the users of your network work with data that is stored in the cloud using a cloud storage service, Web Gateway provides a function for encrypting this data, together with the corresponding function for decryption.

- **Cloud storage encryption** — When a user uploads data to a cloud storage service, the data can be encrypted.

- **Cloud storage decryption** — When a user downloads encrypted data from a cloud storage service, the data is decrypted to enable the user to work with it.

A suitable rule set is available from the rule set library on Web Gateway for configuring cloud storage encryption and decryption.

Contents

- Encrypting and decrypting cloud storage data
- Configure encryption and decryption of cloud storage data
- Configure the settings for encrypting and decrypting data
- Cloud Storage Encryption settings
- Cloud Storage Encryption Support settings
- Decrypt cloud storage data manually
- Cloud Storage Encryption rule set

Encrypting and decrypting cloud storage data

To enhance security when users of your network complete in-the-cloud activities, you can configure the encryption of data that a user uploads to a cloud storage service. When the data is downloaded, it is decrypted to allow the user to work with it.

A module of Web Gateway, known as the Cloud Storage Encryption module (also referred to as Cloud Storage Encryption filter or engine), handles both encryption and decryption of data, including the metadata. Encryption and decryption remain transparent to the user.

Encryption and decryption is performed for “top-level” data that is processed in the request and response cycles. Data that is embedded in a request or a response and, accordingly, processed in the embedded objects cycle, cannot be encrypted or decrypted.

To encrypt and decrypt data, the module uses a standard algorithm, which can be one of the following:

- AES-128
- AES-192
- AES-256

The algorithm is also known as *cipher*. 
A password is also required as a parameter of the encryption or decryption process.

For performing this process, the module relies on service description files, which exist for each of the various cloud storage services.

The files provide information on how to handle different data formats, the methods that can be used in an upload or download request, for example, PUT or POST, and the URLs that are sent with requests to identify the locations where the data should be uploaded to or downloaded from.

![Info icon] Service description files are updated when a new version of Web Gateway is installed. It is not possible to download new versions of these files from an update server.

Encryption and decryption of data can be performed for the following cloud storage services:

- Box
- Dropbox
- Google Drive
- Microsoft SkyDrive

For the Box cloud storage service, encryption and decryption is supported when a web browser or a native Box client is used to upload and download data. For Dropbox, Google Drive, and Sky Drive, it is supported when upload or download is performed from a web browser.

**Configuring encryption and decryption**

To configure the encryption and decryption process, you need to implement suitable rules on Web Gateway. They are provided in the Cloud Storage Encryption rule set, which you can import from the library.

The rules in the library rule set control the Cloud Storage Encryption module and provide a default password for the encryption or decryption process. The rule set also contains an optional rule for logging the process.

The rule that controls the module for encryption applies if it is found that a request that was received on Web Gateway is a request for uploading data to one of the configured cloud storage services. Similarly, the rule that calls the module for decryption applies if a request for downloading data from one of these services has been received.

If one of the two rules applies, it triggers an event that lets the module perform the encryption or decryption process.

But whereas decryption is executed as soon as the rule processing module (rule engine) has actually found the relevant rule to apply, encryption is not executed before all the following rules have also been processed, including rules configured for processing in the embedded objects cycle.

This ensures the data that is sent with a request for uploading or downloading can be processed in unencrypted format by the other rules.

Module settings are implemented with the import of the library rule set, which you need to configure to specify the following:

- Algorithm (cipher) used for encryption and decryption
- Supported cloud storage services
Data trickling and decryption

If data trickling is implemented as a mode of transferring data, decryption of an encrypted file that is downloaded from a cloud storage service might fail. You should therefore configure these functions as follows:

- On the rule set tree, the Cloud Storage Encryption rule set should be placed immediately before or after the rule set that you use to implement data trickling.

  This prevents rules of other rule sets from being processed between the decryption and the data trickling rules, which can cause the decryption to fail.

  A rule for enabling data trickling is contained in the Progress Indication rule set, which is an embedded rule set of the Common Rules rule set of the default rule set system.

To be completely sure that data trickling does not lead to a failed decryption, you can additionally do the following:

- Replace the `Always` in the criteria of the data trickling rule by `CloudEncryption.IsDecryptionSupported equals false`.

  This prevents data trickling from being started when downloaded data is decrypted. However, configuring the criteria like this will have an impact on the performance of the data trickling process.

A conflict between decryption and data trickling can also be the reason why a file that was downloaded from a cloud storage service is corrupted and cannot be opened, although no decryption errors were reported.

Multiple encryption of data

When a request for uploading data to a cloud storage service is received, the data can be encrypted more than once, performing encryption differently each time.

For each encryption, you need to configure a rule. You can, for example, specify a password for a user group in one rule and let encryption be performed under a particular algorithm, which you also specify in that rule, and then specify a password for an individual user in the next rule and let encryption be performed under a different algorithm.

So when it comes to downloading the data, it can only be decrypted if both passwords are known.

To decrypt what has been encrypted in multiple rules, the same number of rules for decryption is needed. Algorithms and passwords must be the same as in their encryption counterparts and the order of these rules must be the reverse of the order in which you placed the encryption rules.

SSL-secured upload and download requests

To cover also requests for uploading data to a cloud storage service or for downloading data when they are sent using an SSL-secured connection, you need to make sure the SSL Scanner rule set is enabled.

This rule set is implemented in disabled state with the default system of rule sets for Web Gateway.

The certificates that are needed for communication over SSL-secure connections must be installed on the web browsers that users work with to send upload and download requests.

Manual decryption of data

When Web Gateway is temporarily unavailable in your network or when a password conflict arises, it could be required that you decrypt cloud storage data manually.
This can be done if you know the algorithm and password that were used when the data was encrypted. You can download the data directly from the cloud storage service to your system and run a command for manual decryption on this system, which includes algorithm and password parameters.

**Monitoring encryption and decryption on the dashboard**

Statistics about activities performed for encrypting and decrypting cloud storage data can be monitored on the dashboard of the user interface.

The following parameters are shown:

- Number of encryption and decryption operations and errors (over time)
- Volume of encrypted and decrypted data (over time)
- Number of encryption and decryption operations and errors per cloud storage service
- Volume of encrypted and decrypted data per cloud storage service

---

**Configure encryption and decryption of cloud storage data**

To configure the encryption and decryption of data that is uploaded to a cloud storage service or downloaded, complete the following high-level steps.

**Task**

1. Import the *Cloud Storage Encryption* rule set from the rule set library. The rule set is located in the *Cloud Services* rule set group.
2. Configure the settings for encrypting and decrypting cloud storage data.
3. Ensure communication for encrypting and decrypting data can go on in SSL-secured mode.
   - Enable the *SSL Scanner* rule set in the default rule set system of Web Gateway.
   - For the browsers on the clients of Web Gateway that upload and download cloud storage data, make sure the certificates needed for SSL-secured communication are installed.
4. Save your settings.

---

**Configure the settings for encrypting and decrypting data**

To configure the settings for encrypting and decrypting cloud storage data, work with two different module (engine) settings.

**Task**

1. Select **Policy | Settings**.
2. On the *Engines* branch of the settings tree, expand *Cloud Storage Encryption* and select the particular settings for the Cloud Storage Encryption module you want to configure, for example, the *Default* settings.
   
   The settings appear in the settings pane.
3. Configure these settings as needed.
4 Expand **Cloud Storage Encryption Support** and select the particular settings for the Cloud Storage Encryption Support module you want to configure, for example, the **Default** settings.

The settings appear in the settings pane.

5 Configure these settings as needed.

6 Click **Save Changes**.

---

**Cloud Storage Encryption settings**

The Cloud Storage Encryption settings are used for configuring the encryption and decryption of cloud storage data.

**Encryption Parameters**

Settings for encrypting and decrypting cloud storage data

**Table 15-1  Encryption Parameters**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher</td>
<td>Provides a list for selecting an algorithm to encrypt and decrypt cloud storage data. The following algorithms can be selected:</td>
</tr>
<tr>
<td></td>
<td>• AES 128</td>
</tr>
<tr>
<td></td>
<td>• AES 192</td>
</tr>
<tr>
<td></td>
<td>• AES 256</td>
</tr>
</tbody>
</table>

---

**Cloud Storage Encryption Support settings**

The Cloud Storage Encryption Support settings are used for configuring the cloud storage services that are supported on Web Gateway when data for these services is encrypted or decrypted.

**Supported Cloud Storage Services**

Settings for cloud storage services

**Table 15-2  Supported Cloud Storage Services**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud storage services list</td>
<td>Allows you to select the cloud storage services that are supported on Web Gateway when data for these services is encrypted or decrypted. The following services can be selected:</td>
</tr>
<tr>
<td></td>
<td>• Box</td>
</tr>
<tr>
<td></td>
<td>• Dropbox</td>
</tr>
<tr>
<td></td>
<td>• Google Drive</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SkyDrive</td>
</tr>
<tr>
<td></td>
<td>By default, all services are selected.</td>
</tr>
</tbody>
</table>
Decrypt cloud storage data manually

When you cannot use Web Gateway to decrypt cloud storage data, you can perform the decryption manually by running a suitable command if you know the algorithm and password that were used for the encryption.

**Task**

1. Download the data in encrypted format from the cloud storage service that stored the data to your system.

2. Run the following command to decrypt the data:

   ```bash
   openssl enc -<cipher> -d -in <encrypted file> -out <decrypted file> -k <password> -md sha256
   ```

   where the variable parameters have the following meanings:

   - `<cipher>`: Algorithm used to encrypt the data
   - `<encrypted file>`: Path and file name for the file that contains the encrypted data
   - `<decrypted file>`: Path and file name for the file the decrypted data should be written to
   - `<password>`: Password used when the data was encrypted

   The data is decrypted and written to the specified file.

Cloud Storage Encryption rule set

The Cloud Storage Encryption rule set is a library rule set for encrypting and decrypting data that is uploaded to and downloaded from cloud storage services.

<table>
<thead>
<tr>
<th>Library rule set – Cloud Storage Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
<tr>
<td>Cycles – Requests (and IM), Responses</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.

**Set encryption password**

*Always* → Continue – Set User-Defined.Encryption Password = "webgateway"

The rule uses an event to set the default password for Web Gateway as the password that is used when data is encrypted.

**Enable encryption**

*CloudEncryption.IsEncryptionSupported<Default> equals true* → Continue –


The rule uses the CloudEncryption.IsEncryptionSupported property to check whether encryption of data can be performed. If this is the case, an event is used to perform the encryption.

**Enable decryption**

*CloudEncryption.IsDecryptionSupported<Default> equals true* → Continue –

CloudEncryption.Decrypt(User-Defined.Encryption Password)<Default>

The rule uses the CloudEncryption.IsDecryptionSupported property to check whether decryption of data can be performed. If this is the case, an event is used to perform the decryption.
Fix content type after decryption

CloudEncryption.IsDecryptionSupported<Default> equals true –> Continue –
MediaType.Header.FixContentType

The rule uses the CloudEncryption.IsDecryptionSupported property to check whether a decryption of cloud storage data was performed.

If this is the case, an event is used to modify the Content-Type field in the header of the response that was sent to deliver the data to Web Gateway. Cloud storage services set this field by default to application/octet-stream, as they are not able to recognize real media types when data is encrypted. The MediaType.Header.FixContentType event sets the field to a value for a real media type.set to the value

This rule fixes the issue that cloud storage services set this field by default to application/octet-stream, as they cannot recognize different media types when data is encrypted. The MediaType.Header.FixContentType event sets the field to a value for the real media type.

The rule is not enabled by default.

Log encryption password

CloudEncryption.IsEncryptionSupported<Default> equals true –> Continue –
Set User-Defined.encrypt-log. =
DateTime.ToGMTString
+ ", User: "
+ Authentication.UserName
+ ", IP: "
+ IP.ToString (Client.IP)
+ ", Service: "
+ CloudEncryption.ServiceName
+ ", Cipher: "
+ CloudEncryption.CipherName<Default>
+ ", Password: "
+ User-Defined.EncryptionPassword
FileSystemLogging.WriteLogEntry (User-Defined.encrypt-log)<Encryption Log>

The rule uses an event to create a log entry for an encryption.

A second event is used to write this entry into the log called Encryption Log, which is specified by the event settings. Since data is written into the log in encrypted format, you need a password to access it (default password: webgateway).

The rule is not enabled by default.
Hybrid solution

A hybrid solution that extends security to web usage when it happens outside your local network can be implemented on Web Gateway. McAfee® SaaS Web Protection runs in an integrated process with Web Gateway to enable this solution.

The following are key concepts of this solution:

- **Hybrid policy** — The solution allows you to apply the same policy to web usage inside and outside your local network.

- **Hybrid synchronization** — The policy is synchronized to ensure it is consistently applied to both kinds of web usage.

A legacy solution is also available that allows you to synchronize several policy elements, such as host names, IP addresses, and URL categories.

Contents

- Working with the hybrid solution
- Restrictions of the hybrid solution
- Configure a hybrid solution
- Configure settings for the hybrid solution
- Select a rule set for the hybrid solution
- Perform synchronization manually
- Web Hybrid settings
- Legacy hybrid solution

**Working with the hybrid solution**

Working with the hybrid solution allows you to ensure web security under the same policy for users inside and outside your local network.

The users of your organization can access the web while they are working on systems that are physically installed within your local network. The term "on premise" is often used to refer to working in this way. It can be extended to users who are connected to this network by a Virtual Private Network (VPN) interface.

Other users of your organization work on systems that are not connected to your local network in this way, for example, when they travel or work at home.

Under the hybrid solution, web usage of your on-premise users is protected by Web Gateway, for the other users it is protected by McAfee SaaS Web Protection. When users work with this product to access the web, they perform what is known as in-the-cloud communication.
The hybrid solution allows you to enforce the same security policy on the web usage of both kinds of users.

- From the policy that you have configured on Web Gateway, you can select the rule sets that you also want to apply on McAfee SaaS Web Protection.
- The policy is synchronized in configured intervals to ensure that rule sets remain the same on both products, including changes that you have incorporated on Web Gateway.
- You can also perform synchronization manually, regardless of the configured interval.

If additional features are made available in a new version of Web Gateway, you can immediately include them in the hybrid solution.

There are some restrictions to the hybrid solution, as not all policy elements that are used on Web Gateway can be made to apply on McAfee SaaS Web Protection. Warnings on the user interface of Web Gateway inform you about these restrictions.

**Products for the hybrid solution**

The hybrid solution is mainly based on the integrated operation of:

- **Web Gateway** — To protect the web usage of your on-premise users
- ** McAfee SaaS Web Protection** — To protect the web usage of your cloud users

For more information about McAfee SaaS Web Protection, refer to the *Web Protection Services Setup Guide*. Web Gateway and McAfee SaaS Web Protection are part of the *McAfee Web Protection* product suite. The hybrid solution is, therefore, also known as *McAfee Web Protection – Hybrid*.

For information about the solution as a whole, refer to the *McAfee Web Protection – Hybrid Deployment Guide*. This document also provides information on products that can optionally be run with the solution, for example, McAfee ePolicy Orchestrator or McAfee Client Proxy.

We recommend McAfee Client Proxy for use with the hybrid solution. It recognizes whether systems send requests for web access from inside or outside your network. For inside requests, it lets Web Gateway do its web security job, while outside requests are redirected to McAfee SaaS Web Protection.

**Configuring the hybrid solution on Web Gateway**

When configuring the hybrid solution on Web Gateway, you need to configure settings for this solution and select the rule sets of your web security policy that you also want to apply on McAfee SaaS Web Protection.

If warnings inform you about issues with policy elements that cannot be included in the solution, you need to take suitable measures for removing these issues.

**Restrictions of the hybrid solution**

There are some restrictions to letting a web security policy that you have configured on Web Gateway also apply on McAfee SaaS Web Protection.

For example, users can be authenticated under the NTLM authentication method when sending requests for web access from within your network. If an NTLM server is available for applying this method,
Since an NTLM server is not available for authenticating users when they send the requests for web access that are handled by McAfee SaaS Web Protection, use of the NTLM authentication method is a policy part that cannot be included in a hybrid solution.

Also, not all properties in web security rules on Web Gateway can be used in a hybrid solution. Similarly, not all events can be used, for example, events that increase counters, send emails to an administrator, or write entries into log files.

In general, policy elements cannot be used in a hybrid solution if they:

- Rely on particular network components or external services
  
  This applies, for example, to properties for configuring mail services, as these require that a mail server is available, for example, an SMTP server.

  It also applies to SNMP properties, which require the availability of a trap sink, or to next-hop proxy properties, which require next-hop proxy servers.

- Are related to functions that are not yet available for use in the hybrid solution

  This applies to quota management and PDStorage functions, as well as to other functions that require exchange of run-time data, for example, between multiple Web Gateway appliances in a Central Management configuration.

Warnings on the user interface of Web Gateway inform you about restrictions.

- Warnings on events can be ignored, as the hybrid solution is not impacted if they are not executed

- Warnings on properties that are set to their default values, might be followed by unexpected behavior. Properties are set to default values if no meaningful use can be made of them in a hybrid solution.

  We recommend that you check whether rules that contain such properties work correctly on McAfee SaaS Web Protection.

### Authentication restrictions

In a hybrid solution, authentication for users outside your local network is performed by McAfee SaaS Web Protection. Consequently, what you configure for authentication on Web Gateway must be compatible to the method that is applied for these users.

The `Authentication.UserName` and `Authentication.UserGroups` properties can be used when configuring a hybrid solution on Web Gateway. The values that they are set to depend, however, on the authentication method used by McAfee SaaS Web Protection.

The following methods are mainly used here:

- Using the IP addresses of clients, without providing information on individual users
- Using McAfee Client Proxy, with clients providing information about user names and groups
- Basic authentication, which means users must be provisioned within McAfee SaaS Web Protection
Sample warnings about restrictions of the hybrid solution

The following are sample warnings, appearing to indicate restrictions of the hybrid solution.

• A property in a rule on Web Gateway cannot be used on McAfee SaaS Web Protection.
  A warning informs you of the issue, identifying the rule and the property. It also contains a sentence like this:
  
  Property PDStorage.GetAllData must not be used in SaaS.

• An event in a rule on Web Gateway cannot be used on McAfee SaaS Web Protection.
  A warning informs you of the issue, identifying the rule and the event. It also contains a sentence like this:
  
  Event SNMP.Trap.Send.User(Number, String) must not be used in SaaS.

Configure a hybrid solution

To configure a hybrid solution that lets a Web Gateway security policy also apply on McAfee SaaS Web Protection, complete the following high-level steps.

Task

1 Configure settings for the hybrid solution.
   This includes configuring an address for connecting to McAfee SaaS Web Protection, credentials that must be submitted for communication between the two products, and other parameters.

   It also includes configuring a time interval for synchronization to let policy changes on Web Gateway be also incorporated on McAfee SaaS Web Protection. You can also perform synchronization manually, regardless of the configured synchronization interval.

2 Select the rule sets that you want to include in the hybrid solution.
   This includes considering restrictions of the hybrid solution and handling issues that might arise, as not all policy elements are available for this solution.

3 Save your changes.

Configure settings for the hybrid solution

To configure settings for the hybrid solution, complete the following steps.

Task

1 Select Configuration | Appliances.

2 On the Cluster branch of the appliances tree, click Web Hybrid.
   The settings for the hybrid solution appear on the configuration pane.

3 Configure these settings as needed.

4 Click Save Changes.

See also

Web Hybrid settings on page 562
Select a rule set for the hybrid solution

To select a rule set for the hybrid solution, select it on the user interface of Web Gateway and enable the appropriate option.

**Task**

1. Select **Policy | Rule Sets**.

2. On the rule sets tree, select the rule set that you want to include in the hybrid solution.

   The rule set appears in the key elements view.

3. At the top of this view, select **Enable in Cloud**.

   To perform this step, you can alternatively:

   - Select a rule set, right-click, and select **Enable in Cloud** on the context menu that is displayed.
   - Leave the key elements view and select **Enable in Cloud** in the complete rule sets view.

   If a restriction prevents the rule set from being included in the hybrid solution, a warning appears. Then solve the problem, for example, by removing an event that cannot be used in the solution or by leaving out a complete rule set.

   Nested rule sets are included in the hybrid solution if you use **Enable in Cloud** for their nesting rule set within the key elements view.

   If you use **Enable in Cloud** in the complete rules view, nested rule sets are included as follows:

   - Using the context menu — Nested rule sets are included
   - Clicking the button — Nested rule sets are not included

   To include them, click the button for each nested rule set.

   When using the context menu, you can also select multiple rule sets with or without nested rule sets and include them in the hybrid solution at once.

4. Click **Save Changes**.

   The rule set is now part of the hybrid solution and also applies on McAfee SaaS Web Protection.

   To remove a rule set from the solution, deselect the **Enable in Cloud** option or select **Disable in Cloud** on the context menu.

**See also**

*Restrictions of the hybrid solution on page 558*
Perform synchronization manually

To synchronize the web security policy for a hybrid solution manually, complete the following steps.
You can perform manual synchronization regardless of the configured synchronization interval.

**Task**

1. Select Troubleshooting.
2. On the troubleshooting tree, select SaaS Synchronization.
3. Under SaaS Synchronization on the configuration pane, click Synchronize.

Your web security policy is synchronized to let changes that you made on Web Gateway be also incorporated on McAfee SaaS Web Protection.

While individual policy elements are synchronized, messages about them appear under Results. If there are issues, you are also informed about them in corresponding messages.

Web Hybrid settings

The Web Hybrid settings are used for configuring a hybrid solution to let a web security policy that is implemented on Web Gateway also apply on McAfee SaaS Web Protection.

Web Hybrid Configuration

Settings for configuring a hybrid solution

Table 16-1  Web Hybrid Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize policy to SaaS</td>
<td>When selected, a web security policy that you have configured on Web Gateway is synchronized to let changes be also incorporated on McAfee SaaS Web Protection.</td>
</tr>
<tr>
<td></td>
<td>Synchronization is performed in regular intervals, according to the time that you configure under Local policy changes will be uploaded within the same interval as mentioned below.</td>
</tr>
<tr>
<td></td>
<td>You can also perform synchronization manually, regardless of the configured interval, but the Synchronize policy to SaaS option must also be enabled for this type of synchronization.</td>
</tr>
<tr>
<td></td>
<td>This means that when you perform synchronization manually, scheduled synchronization will still go on.</td>
</tr>
<tr>
<td>Appliance for synchronization</td>
<td>Identifies the Web Gateway appliance that synchronization data is transferred from.</td>
</tr>
<tr>
<td></td>
<td>Using this option ensures that synchronization data is always taken from the same appliance when you have multiple appliances running in a Central Management configuration.</td>
</tr>
<tr>
<td>SaaS address</td>
<td>Specifies the address for accessing McAfee SaaS Web Protection.</td>
</tr>
<tr>
<td></td>
<td>The address format is: (http</td>
</tr>
<tr>
<td></td>
<td>For example: <a href="https://msg.mcafeesaas.com">https://msg.mcafeesaas.com</a></td>
</tr>
</tbody>
</table>
### Table 16-1  Web Hybrid Configuration (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS administrator account name</td>
<td>Specifies the user name for the administrator of McAfee SaaS Web Protection. For example: <a href="mailto:saasadmin@mcafee.com">saasadmin@mcafee.com</a> This user name must correspond to the user name of the user on McAfee SaaS Web Protection who has been assigned the role of Customer Admin.</td>
</tr>
<tr>
<td>SaaS administrator account password</td>
<td>Sets a password for an administrator. The same password must be set for the user on McAfee SaaS Web Protection who has been assigned the role of Customer Admin. Clicking Change opens a window for setting a password.</td>
</tr>
<tr>
<td>SaaS customer ID</td>
<td>Identifies a customer who has purchased McAfee SaaS Web Protection to run it in a hybrid solution with Web Gateway.</td>
</tr>
<tr>
<td>Local policy changes will be uploaded within the same interval as mentioned below</td>
<td>Sets the time (in minutes) that elapses before the next synchronization run is performed to let policy changes on Web Gateway also apply on McAfee SaaS Web Protection. The time can range from 10 to 60 minutes. Policy changes are synchronized according to the interval that you configure here, not after every change that you apply, unless you perform manual synchronization each time.</td>
</tr>
</tbody>
</table>

### Advanced Synchronization Settings

Advanced settings for configuring a hybrid solution

### Table 16-2  Advanced Synchronization Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a proxy for synchronization</td>
<td>When selected, a proxy is used for transferring synchronization data.</td>
</tr>
<tr>
<td>Proxy host</td>
<td>Specifies the IP address or host name of the server that is used as a proxy.</td>
</tr>
<tr>
<td>Proxy port</td>
<td>Specifies the port on the proxy server that listens to requests for transferring synchronization data.</td>
</tr>
<tr>
<td>Proxy user</td>
<td>Specifies the user name that Web Gateway submits to the proxy when transferring synchronization data.</td>
</tr>
<tr>
<td>Proxy password</td>
<td>Sets a password for the user name. Clicking Set opens a window for setting a password.</td>
</tr>
</tbody>
</table>

### Legacy hybrid solution

A legacy solution is available for synchronizing web security policies to protect web access of your users when they are working on-premise and in-the-cloud.
Synchronizing settings for the legacy hybrid solution

When Web Gateway and McAfee SaaS Web Protection work together in the hybrid legacy solution, web filtering settings can be synchronized between the products to allow for a common web security policy.

The McAfee Web Protection solution enables you to enforce a common web security policy for users who are working on systems within your corporate network, as well as for those who are working on their systems from home or when traveling.

For this purpose, the solution uses a combination of on-premise products, such as Web Gateway and cloud-based products, such as McAfee SaaS Web Protection service.

The synchronization of web filtering settings between the two products works both ways. When you apply changes to the web filtering settings on Web Gateway, these changes are also applied on McAfee SaaS Web Protection.

In the same way, changes that the administrator for McAfee SaaS Web Protection applies on that product are also applied on Web Gateway.

An internal interface known as REST (Representational State Transfer) interface handles the data transfer.

To let the synchronization become effective, you need to configure several settings on the side of McAfee Web Gateway, for example, the host name or IP address of the portal that provides access to McAfee SaaS Web Protection Service.

If you are administering multiple Web Gateway appliances as nodes in a Central Management configuration, you can perform the synchronization on any node of the configuration.

Web filtering settings for synchronization

Different types of web filtering settings can be synchronized between McAfee Web Gateway and McAfee SaaS Web Protection Service.

Web filtering settings for synchronization between the two products include:

- **Policy settings** — Settings that specify parameters of web security policies, such as host names or URL categories

- **User group settings** — Settings that specify user groups

Different ways of handling these settings are possible on a McAfee Web Gateway appliance.

Policy settings for synchronization

Particular web filtering settings are combined on McAfee SaaS Web Protection Service to create a web security policy. These are settings for the following parameters:

- Name of a policy
- Description of a policy
- Enable/disable SafeSearch filtering
- Allowed URL categories
- Blocked URL categories
- Trusted web sites by host names
- Blocked web sites by host names
- Trusted web sites by IP addresses
- Blocked web sites by IP addresses

Settings for these parameters can be changed on both McAfee Web Gateway and McAfee SaaS Web Protection Service and the changes are synchronized between the two products.
User group settings for synchronization

User group settings include the groups of users that particular web security policies have been assigned to on McAfee SaaS Web Protection Service.

These settings can be changed on McAfee SaaS Web Protection Service. Users can be added to a group and new groups can be created. On McAfee Web Gateway, these settings can only be viewed, not changed.

However, any change on McAfee SaaS Web Protection Service is synchronized, so the current settings can always be viewed on McAfee Web Gateway.

Configure synchronization settings

To enable use of a synchronized policy for Web Gateway and McAfee SaaS Web Protection Service, you need to configure synchronization settings.

Task

1. Select Configuration | Appliances.
2. Select the appliance you want to configure synchronization settings on and click Web Hybrid Legacy.
   The synchronization settings appear on the settings pane.
3. Configure these settings as needed.
4. Click Save Changes.

Web Hybrid Legacy settings

The Web Hybrid Legacy settings are used for configuring synchronization of the web security policy on Web Gateway and McAfee SaaS Web Protection.

Web Hybrid Configuration

Settings for synchronizing a web security policy

Table 16-3 Web Hybrid Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS address</td>
<td>Specifies the IP address or host name of the portal that provides access to the McAfee SaaS Web Protection.</td>
</tr>
<tr>
<td>SaaS customer ID</td>
<td>Identifies a customer who runs the McAfee SaaS Web Protection.</td>
</tr>
<tr>
<td>SaaS administrator account name</td>
<td>Specifies the user name of the account for the administrator who manages McAfee SaaS Web Protection.</td>
</tr>
<tr>
<td>SaaS administrator account password</td>
<td>Sets a password for an administrator account.</td>
</tr>
<tr>
<td>Enable synchronization to SaaS</td>
<td>When selected, changes in the web filtering settings on Web Gateway are applied to the corresponding settings on McAfee SaaS Web Protection.</td>
</tr>
</tbody>
</table>
Table 16-3  Web Hybrid Configuration (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable synchronization from SaaS</td>
<td>When selected, changes in the web filtering settings on McAfee SaaS Web Protection are applied to the corresponding settings on McAfee Web Gateway.</td>
</tr>
<tr>
<td>Local policy changes will be uploaded immediately to SaaS</td>
<td>When selected, changes in the policy settings that you apply on Web Gateway are immediately uploaded to Web Gateway.</td>
</tr>
<tr>
<td>Local policy changes will be uploaded within the same interval as defined below</td>
<td>When selected, changes in the policy settings that you apply on Web Gateway are uploaded to McAfee SaaS Web Protection after the time interval configured below has elapsed.</td>
</tr>
<tr>
<td></td>
<td>Allowed values for the time interval range between 10 and 60 minutes.</td>
</tr>
<tr>
<td></td>
<td>The time interval is set on a slider scale.</td>
</tr>
</tbody>
</table>

Web Hybrid Actions
Options for performing the synchronization of web filtering settings

Table 16-4  Web Hybrid Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize to SaaS</td>
<td>Performs the immediate synchronization of web filtering settings on Web Gateway with the corresponding settings on McAfee SaaS Web Protection.</td>
</tr>
<tr>
<td>Synchronize from SaaS</td>
<td>Performs the immediate synchronization of web filtering settings on McAfee SaaS Web Protection with the corresponding settings on Web Gateway</td>
</tr>
</tbody>
</table>
17 Monitoring

You can monitor an appliance when it executes the filtering that ensures web security for your network.

Monitoring is performed in different ways. Default monitoring on an appliance includes:

- **Dashboard** — Displays key information on the appliance system and activities
- **Logging** — Writes information about important events on an appliance into log files
- **Error handling** — Takes measures when incidents and errors occur on an appliance

You can measure the performance of appliance functions and also use external devices for monitoring, such as a McAfee ePO server or an SNMP Agent.

**Contents**
- Dashboard
- Logging
- Error handling
- Performance measurement
- Event monitoring with SNMP
- Transferring data for McAfee ePO monitoring
- Best practices - Sending access log data to a syslog server
- Sending syslog data to McAfee Enterprise Security Manager

**Dashboard**

The dashboard on the user interface of the appliance allows you to monitor key events and parameters, such as alerts, filtering activities, status, web usage, and system behavior.

Information is provided on the following two tabs:

- **Alerts** — Shows status and alerts
- **Charts and Tables** — Shows web usage, filtering activities, and system behavior

If the appliance is a node in a Central Management configuration, statuses and alerts are also shown for the other nodes.
Access the dashboard
You can access the dashboard on the user interface of an appliance.

Task
1. Select the Dashboard top-level menu.
2. Select one of the following two tabs, according to what you want to view:
   - Alerts — Shows status and alerts
   - Charts and Tables — Shows web usage, filtering activities, and system behavior

See also
View status and alerts information on page 568
View charts and tables information on page 571

Alerts tab
The Alerts tab displays information on the status and alerts for an appliance and, in case the appliance is a node in a Central Management configuration, also of the other appliances.

View status and alerts information
On the alerts tab, you can view information on the status of an appliance and on alerts that occur.

Task
1. Select Dashboard | Alerts.
2. [Optional] Refresh information on alerts using one of the following two options:
   - Automatic refresh — Performs an automatic refresh in regular intervals
     This option is enabled by default.
   - Refresh now — Performs an immediate refresh

See also
Overview of status information on page 568
Alert filtering options on page 569

Overview of status information
Information about the status of an appliance is displayed under Appliances Status on the Alerts tab of the dashboard.

If an appliance is a node in a Central Management configuration, information on the the other nodes is also displayed.

The following table provides an overview of this information.
Table 17-1 Overview of status information

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance</td>
<td>Provides basic appliance information.</td>
</tr>
<tr>
<td></td>
<td>• Name — Specifies the name of an appliance.</td>
</tr>
<tr>
<td>Performance</td>
<td>Provides key performance parameters.</td>
</tr>
<tr>
<td></td>
<td>• Alert peaks, last 7 days — Indicates the most severe alert on an appliance for each of the last seven days.</td>
</tr>
<tr>
<td></td>
<td>A colored field is displayed for each day (right-most field is today):</td>
</tr>
<tr>
<td></td>
<td>• Gray — No alert during the day</td>
</tr>
<tr>
<td></td>
<td>• Green — Most severe alert during the day was an information</td>
</tr>
<tr>
<td></td>
<td>• Yellow — Most severe alert during the day was a warning</td>
</tr>
<tr>
<td></td>
<td>• Red — Most severe alert during the day was an error</td>
</tr>
<tr>
<td></td>
<td>• Requests per second — Provides a diagram showing how number of web requests in HTTP and HTTPS mode received on the appliance evolved over the last 30 minutes</td>
</tr>
<tr>
<td></td>
<td>The value to the right of the diagram is the average number of requests per second over the last ten minutes.</td>
</tr>
<tr>
<td>McAfee Anti-Malware Versions</td>
<td>Provides update and version information on modules used in virus and malware filtering.</td>
</tr>
<tr>
<td></td>
<td>• Last update — Shows the number of minutes since the modules were last updated.</td>
</tr>
<tr>
<td></td>
<td>• Gateway Engine — Shows the version number of the McAfee Web Gateway Anti-Malware engine.</td>
</tr>
<tr>
<td></td>
<td>• Proactive Database — Shows the version number of the Proactive Database.</td>
</tr>
<tr>
<td></td>
<td>• DATs — Shows the version number of the DAT files (containing virus signatures).</td>
</tr>
<tr>
<td>URL Filter</td>
<td>Provides update and version information for the module used in URL filtering.</td>
</tr>
<tr>
<td></td>
<td>• Last update — Shows the number of days since the module was last updated.</td>
</tr>
<tr>
<td></td>
<td>• Version — Shows the version number of the module.</td>
</tr>
</tbody>
</table>

Alert filtering options

Information about alerts on an appliance is provided under Alerts on the Alerts tab of the dashboard. You can filter this information using several filtering options.

If an appliance is a node in a Central Management configuration, alerts for the other nodes are also shown. Then you can also filter the nodes you want to view alerts for.

The following table describes the filtering options.
### Table 17-2 Alert filtering options

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Appliance Filter| Filters alerts according to the nodes they occurred on in a Central Management configuration.  
Clicking this button opens a window for selecting the nodes you want to view alerts for.  
The filter applies as soon as you close the window. |
| Date Filter     | Filters alerts according to the period of time they occurred in.  
Clicking this button displays a menu for selecting the time period you want to view alerts for.  
You can select one of the following:  
- All  
- Today  
- Yesterday  
- Last week  
- Custom  
  Under Custom, you can set a start and end date on two calendars and type a start and end time in two filter fields. The time format is hh:mm:ss, using the 24-hours notation, for example, 1 p.m. is 13:00:00.  
When an appliance is a node in a Central Management configuration and you have selected several nodes of this configuration in the Appliance Filter, alerts are shown for these nodes.  
They are shown, however, according to the date and time shown on the user interface you have been working with on a particular node to set the Date Filter.  
For example, you select Today in the Date Filter on a node in Amsterdam at 7 p.m. local time.  
This means all alerts that occurred during the last 19 hours are shown. For a node in New York, local time is 1 p.m. at the time you set the filter.  
Alerts that occurred on the New York node are then shown for the last 19 hours, not for the last 13 hours, which would correspond to what Today is for the New York node. |
| Message Filter  | Filters alerts according to alert message types and strings within the message texts.  
The filter applies as soon as you have set the filter options.  
Set these options in the following way:  
- Error, Warning, Information — Select the alert message type you want to view or any combination of types.  
- Filter — Optionally type a filtering term in this field. Only alerts with message texts matching this term and the selected type or types are shown.  
The search for matching terms is performed on alert entries as they are stored in an internal database on an appliance, not as they appear on the user interface.  
When alerts appear on the user interface, the alert message text can include additional parts.  
For example, the word origin is added to the name of the component that is the origin of an alert. You can, however, not use origin or other added terms to filter alerts. |
Charts and Tables tab
The Charts and Tables tab displays statistical data on web usage, filtering activities, and system behavior of an appliance. If the appliance is a node in a Central Management configuration, it displays also statistical data for the other nodes.

View charts and tables information
On the Charts and Tables tab, you can view information on web usage, filtering activities, and system behavior.

Task
1 Select Dashboard | Charts and Tables.
2 From the Appliance drop-down list, select the appliance you want to view chart and tables information for.
3 [Optional] Click Update to ensure you see the most recent information.
4 From the list on the navigation pane, select the type of information you want to view, for example Web Traffic Summary.

See also
Charts and tables display options on page 571
Overview of charts and tables information on page 572

Charts and tables display options
There are several options for displaying the information on the Charts and Tables tab, depending on the type of information that is provided.

Types of information are as follows:

• **Evolving data** — Shows how particular parameters evolved over a selected time interval

  For example, you can view how the number of blocked or allowed URL requests evolved over a selected time interval.

• **Top scores** — Shows top numbers for activities or byte volumes related to key items of the filtering process up to the moment when you view them

  What you see then is these numbers, but not how they evolved over time.

  For example, you can view the URL categories that have been most often requested. Or you can view media types ranked according to the volumes transferred when web objects of these types were downloaded.

  The maximum number of items stored on an appliance for presenting top scores at a given point in time is 1500. When this number is exceeded, items that have the lowest occurrence or byte volumes are removed.

• **Other information** — Shows other information presented on tables

  For example, you can view the current versions of key modules (also known as engines) on an appliance, such as the Anti-Malware module or the URL Filter module.

  The following table shows the display options for the different types of information.
Table 17-3  Charts and tables display options

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show last</td>
<td>Provides a drop-down list for selecting a time interval: 1 hour</td>
</tr>
</tbody>
</table>
| Resolution| Displays the time unit used for the diagram that shows the evolution of a parameter over the selected interval.  
Resolution varies with the interval.  
For example, when 1 hour is selected, the diagram uses 1 minute as the time unit, when 1 year is selected, the diagram uses 1 day. |
| View     | Provides a drop-down list for selecting:  
• Display mode: Line | Stacked  
• Average values |
| Refresh icon | Refreshes the view. |
| Top      | Provides a drop-down list for selecting how many of the items with the highest scores are shown: 10 | 25 | ... | 1000  
For example, the 25 URL categories that the most-often requested URLs fall in can be shown. |
| Refresh icon | Refreshes the view. |

Overview of charts and tables information

Information about web usage, filtering activities, and system behavior for an appliance is displayed on the Charts and Tables tab of the dashboard.

The following tables provide an overview of this information.

Table 17-4  Executive Summary

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
</table>
| URL Executive Summary     | Shows how numbers of requests evolved during the selected interval.  
Requests are sorted into allowed ("good") requests and such that were blocked.  
Blocked requests are additionally sorted according to the filtering modules that caused the blocking, such as the Anti-Malware engine, the URL engine, and others.  
Clicking Edit Choosable Data Series opens a window for editing the selection of good and blocked requests that is shown. |
| Categories by Hits        | Shows the categories that the most-often requested URLs belonged to. |
| Malwares by Hits          | Shows the virus and malware types that were requested most often. |

Table 17-5  System Summary

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Utilization</td>
<td>Shows how numbers of requests sent and received evolved during the selected interval.</td>
</tr>
<tr>
<td>System Utilization</td>
<td>Shows how usage of hard disk, CPU, physical memory of the appliance system, and the physical memories of the core and coordinator subsystems evolved during the selected interval.</td>
</tr>
<tr>
<td>Update Status</td>
<td>Shows the versions of several modules and filter information files that are implemented on an appliance, for example, of the Gateway Anti-Malware engine or of the malware signature files.</td>
</tr>
<tr>
<td>Last Update</td>
<td>Shows when several modules of an appliance were last updated, for example, the URL Filter module.</td>
</tr>
</tbody>
</table>
### Table 17-5 System Summary (continued)

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Ports</td>
<td>Lists the ports on an appliance that are currently listening to requests.</td>
</tr>
<tr>
<td>WCCP Services</td>
<td>Shows the status of WCCP services used to redirect traffic to an appliance.</td>
</tr>
<tr>
<td>Active Proxy Connections</td>
<td>Shows how numbers of connections evolved during the selected interval.</td>
</tr>
</tbody>
</table>

### Table 17-6 Web Traffic Summary

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic per Protocol</td>
<td>Shows how volumes of web traffic under the HTTP, HTTPS, and FTP protocols evolved during the selected interval.</td>
</tr>
<tr>
<td>Requests per Protocol</td>
<td>Shows how numbers of requests under the HTTP, HTTPS, and FTP protocols evolved during the selected interval.</td>
</tr>
</tbody>
</table>

### Table 17-7 ICAP Traffic Summary

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICAP Traffic with ICAP Clients</td>
<td>Shows how volumes of traffic occurring during communication with ICAP clients in REQMOD and RESPMOD modes evolved during the selected interval.</td>
</tr>
<tr>
<td>ICAP Requests from ICAP clients</td>
<td>Shows how numbers of requests sent by ICAP clients in REQMOD and RESPMOD modes evolved during the selected interval.</td>
</tr>
</tbody>
</table>

### Table 17-8 SOCKS Traffic Summary

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOCKS Traffic</td>
<td>Shows how volumes of traffic going on under versions 4 and 5 of the SOCKS protocol evolved during the selected interval.</td>
</tr>
<tr>
<td>SOCKS Connections</td>
<td>Shows how numbers of connections for traffic going on under versions 4 and 5 of the SOCKS protocol evolved during the selected interval.</td>
</tr>
</tbody>
</table>
| Traffic per Protocol         | Shows how volumes of traffic going on under the SOCKS protocol evolved during the selected interval.  
                                | Volumes are shown for UDP and the protocols that could be detected as underlying the SOCKS protocol: HTTP and HTTPS.  
                                | Volume is also shown for all other underlying protocols, which remained unfiltered, as filtering underlying protocols of the SOCKS protocol other than HTTP or HTTPS is not performed on Web Gateway. |
| Connections per Protocol     | Shows how numbers of connections for traffic going on under the SOCKS protocol evolved during the selected interval.  
                                | Connection numbers are shown for the UDP protocol and the protocols that could be detected as underlying the SOCKS protocol: HTTP and HTTPS.  
                                | The number of connections is also shown for all other underlying protocols, which remained unfiltered, as filtering underlying protocols of the SOCKS protocol other than HTTP or HTTPS is not performed on Web Gateway. |
| Protocol Detection per Connection | Lists the underlying protocols of the SOCKS protocol that were most often detected for an individual connection together with these connections. |
### Table 17-9 IM Traffic Summary

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Messaging Traffic</td>
<td>Shows how volumes of instant messaging requests evolved for different services during the selected interval.</td>
</tr>
<tr>
<td>Instant Messaging Requests</td>
<td>Shows how numbers of instant messaging requests evolved for different services during the selected interval.</td>
</tr>
<tr>
<td>Instant Messaging Clients</td>
<td>Shows how numbers of instant messaging clients evolved for different services during the selected interval.</td>
</tr>
</tbody>
</table>

### Table 17-10 Traffic Volume

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top-Level Domains by Bytes Transferred</td>
<td>Lists the domains that were requested most according to the number of bytes transferred from them.</td>
</tr>
<tr>
<td>Top-Level Domains by Number of Requests</td>
<td>Lists the domains that were requested most often according to the number of requests for them.</td>
</tr>
<tr>
<td>Destinations by Bytes Transferred</td>
<td>Lists the destinations that were requested most according to the number of bytes transferred from them.</td>
</tr>
<tr>
<td>Destinations by Number of Requests</td>
<td>Lists the domains that were requested most often according to the number of requests for them.</td>
</tr>
<tr>
<td>Source IPs by Bytes Transferred</td>
<td>Lists the source IP addresses that most volume was transferred to.</td>
</tr>
<tr>
<td>Source IPs by Number of Requests</td>
<td>Lists the source IP addresses that most requests were made from.</td>
</tr>
</tbody>
</table>

### Table 17-11 Web Cache Statistics

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Cache Efficiency</td>
<td>Shows how numbers of caching requests evolved during the selected interval and sorts them into hits and misses.</td>
</tr>
<tr>
<td>Web Cache Object Count</td>
<td>Shows how numbers of objects in the cache evolved during the selected interval.</td>
</tr>
<tr>
<td>Web Cache Usage</td>
<td>Shows how usage of the cache evolved during the selected interval.</td>
</tr>
</tbody>
</table>

### Table 17-12 Malware Statistics

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware URLs by Hits</td>
<td>Lists the URLs infected by viruses and other malware that were requested most often.</td>
</tr>
<tr>
<td>Malware by Hits</td>
<td>Lists the malware types that were requested most often.</td>
</tr>
<tr>
<td>Advanced Threat Defense Requests</td>
<td>Shows how numbers of requests for web objects that were passed on to McAfee® Advanced Threat Defense for scanning evolved during the selected interval.</td>
</tr>
<tr>
<td></td>
<td>Shows also how numbers of requests that were blocked due to the scanning results evolved during the selected interval.</td>
</tr>
<tr>
<td>Advanced Threat Defense Scanning Time</td>
<td>Shows how the time consumed for scanning web objects by McAfee Advanced Threat Defense evolved during the selected interval.</td>
</tr>
</tbody>
</table>

### Table 17-13 URL Filter Statistics

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Shows how numbers of requested URL categories evolved during the selected interval.</td>
</tr>
<tr>
<td>Reputation</td>
<td>Shows how numbers of requests evolved during the selected interval and sorts them according to the reputation of the requested URLs.</td>
</tr>
</tbody>
</table>
### Table 17-13  URL Filter Statistics (continued)

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories by Hits</td>
<td>Lists the URL categories that were requested most often.</td>
</tr>
<tr>
<td>Sites Not Categorized by Hits</td>
<td>Lists among the sites that are not categorized those that were requested most often.</td>
</tr>
<tr>
<td>Malicious Sites by Hits</td>
<td>Lists among the sites that were found to be infected those that were requested most often.</td>
</tr>
<tr>
<td>Top Blocked URLs</td>
<td>Lists among the blocked sites those that were requested most often.</td>
</tr>
</tbody>
</table>

### Table 17-14  Media Type Statistics

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Type Groups by Hits</td>
<td>Shows how numbers of requested media type groups evolved during the selected interval. Types are sorted into audio files, images, and others.</td>
</tr>
<tr>
<td>Media Types by Bytes</td>
<td>Lists the media types that were requested most according to the number of bytes transferred.</td>
</tr>
<tr>
<td>Media Types by Hits</td>
<td>Lists the media types that were requested most often according to the numbers of successful requests for them.</td>
</tr>
</tbody>
</table>

### Table 17-15  DLP Filter Statistics

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Classification</td>
<td>Shows how numbers of classifications for content that should not leave your network evolved during the selected interval.</td>
</tr>
<tr>
<td>DLP Classification by Hits</td>
<td>Lists the classifications that were most often used for content that should not leave your network.</td>
</tr>
</tbody>
</table>

### Table 17-16  SSL Scanner Statistics

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Incidents</td>
<td>Shows how numbers of incidents evolved during the selected interval. Incidents are sorted according to the types of the events that caused them, for example, expired certificates or common name mismatches.</td>
</tr>
<tr>
<td>Remote Private Key Operations</td>
<td>Shows how numbers of remote private key operations for encrypting and decrypting data evolved during the selected interval.</td>
</tr>
<tr>
<td>Remote Private Key Operations</td>
<td>Lists the remote private key operations that were executed most often, providing information on the keys used, the functions that were performed, and the types of operation.</td>
</tr>
</tbody>
</table>

### Table 17-17  Application Control Statistics

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories</td>
<td>Shows how numbers of the different categories that requested applications belonged to evolved during the selected interval.</td>
</tr>
<tr>
<td>Reputation</td>
<td>Shows how numbers of the reputation levels that were assigned to requested applications evolved during the selected interval.</td>
</tr>
<tr>
<td>Categories by Hits</td>
<td>Lists the categories that occurred most often for applications that access to was requested.belonged.</td>
</tr>
<tr>
<td>High Risk Applications byHits</td>
<td>Lists the applications with high-risk reputation that were most often requested for access.</td>
</tr>
</tbody>
</table>
### Table 17-18  Single Sign On Statistics

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Logins</td>
<td>Shows how numbers of logons to cloud applications (services) evolved during the selected interval.</td>
</tr>
<tr>
<td>Logins per Service</td>
<td>Shows how numbers of logons evolved during the selected interval and sorts them according to the cloud applications (services) that logon was performed to.</td>
</tr>
<tr>
<td>Logins per Service</td>
<td>Lists the cloud applications (services) that most logons were performed to.</td>
</tr>
<tr>
<td>Number of Invalid Tokens</td>
<td>Shows how numbers of invalid tokens evolved during the selected interval.</td>
</tr>
</tbody>
</table>

### Table 17-19  Encryption Statistics

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations</td>
<td>Shows how numbers of encryption and decryption operations for cloud storage data and numbers of errors that occurred during these operations evolved during the selected interval.</td>
</tr>
<tr>
<td>Volume</td>
<td>Shows how volumes of encrypted and decrypted data evolved during the selected interval.</td>
</tr>
<tr>
<td>Encryption Operations</td>
<td>Lists the cloud storage services that were involved most often when data was encrypted and uploaded.</td>
</tr>
<tr>
<td>Decryption Operations</td>
<td>Lists the cloud storage services that were involved most often when data was decrypted and downloaded.</td>
</tr>
<tr>
<td>Encryption Volume</td>
<td>Lists the cloud storage services that were involved most when data was encrypted according to the volume of encrypted data.</td>
</tr>
<tr>
<td>Decryption Volume</td>
<td>Lists the cloud storage services that were involved most when data was decrypted according to the volume of decrypted data.</td>
</tr>
<tr>
<td>Encryption Errors</td>
<td>Lists the cloud storage services that were involved most often when errors in encrypting data occurred.</td>
</tr>
<tr>
<td>Decryption Errors</td>
<td>Lists the cloud storage services that were involved most often when errors in decrypting data occurred.</td>
</tr>
</tbody>
</table>

### Table 17-20  System Details

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Utilization</td>
<td>Shows how numbers of requests sent and received evolved during the selected interval.</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Shows how CPU usage evolved during the selected interval.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>Shows how usage of memory evolved during the selected interval.</td>
</tr>
<tr>
<td>MWG Processes Virtual Memory Usage</td>
<td>Shows how usage of virtual memory by processes running on Web Gateway evolved during the selected interval.</td>
</tr>
<tr>
<td>Average System Load per CPU</td>
<td>Shows how average load on individual CPUs evolved during the selected interval.</td>
</tr>
<tr>
<td>Swap Space Usage</td>
<td>Shows how usage of memory available for swapping data evolved during the selected interval.</td>
</tr>
<tr>
<td>File System Utilization</td>
<td>Shows how usage of the file system evolved during the selected interval.</td>
</tr>
<tr>
<td>File System Utilization</td>
<td>Shows usage of the file system per partition.</td>
</tr>
<tr>
<td>Open TCP Ports</td>
<td>Shows open TCP ports with IP addresses and port numbers.</td>
</tr>
</tbody>
</table>
### Table 17-21 Authentication Statistics

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Requests</td>
<td>Shows how numbers of requests processed remotely, locally, or found in the cache evolved under each authentication method during the selected interval.</td>
</tr>
<tr>
<td>Average Request Processing Time per Method in ms</td>
<td>Shows how average processing time for requests sent to a server evolved under each authentication method during the selected interval.</td>
</tr>
<tr>
<td>Current Requests Report</td>
<td>Shows numbers of requests, cache hits, as well as minimum, maximum, and average processing time for requests sent to a server.</td>
</tr>
<tr>
<td>Current Connections Status</td>
<td>Shows the connections that are currently active under each authentication method.</td>
</tr>
</tbody>
</table>

### Table 17-22 Performance Information

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Performance</td>
<td>Shows how the processing time consumed on average for completing particular tasks evolved during the selected interval.</td>
</tr>
<tr>
<td></td>
<td>These tasks include performing a DNS lookup, connecting to a given web server, and the work done by the rule engine to process a request throughout all cycles.</td>
</tr>
<tr>
<td></td>
<td>When measuring the time consumed for DNS lookups, only lookups on external servers are considered. Cache lookups are disregarded.</td>
</tr>
<tr>
<td>Detailed HTTP Performance</td>
<td>Shows how the time consumed on average for processing a request throughout all cycles evolved during the selected interval.</td>
</tr>
<tr>
<td></td>
<td>This performance information is only measured and displayed for web traffic that uses HTTP and HTTPS connections.</td>
</tr>
<tr>
<td></td>
<td>The processing of a request throughout all cycles (request, response, and embedded object cycles) is considered to be one transaction.</td>
</tr>
<tr>
<td></td>
<td>Average processing time is shown for complete transactions, but also for particular data transfers going on during a transaction:</td>
</tr>
<tr>
<td></td>
<td>• First Byte Received from Client until First Byte Sent to Client — Shows the average processing time consumed between receiving the first byte from a client on an appliance and sending the first byte to this client within a transaction</td>
</tr>
<tr>
<td></td>
<td>• Last Byte Received from Client until Last Byte Sent to Client — Shows the average processing time consumed between receiving the last byte received from a client on an appliance and sending the last byte to this client within a transaction</td>
</tr>
<tr>
<td></td>
<td>• First Byte Sent to Server until First Byte Received from Server — Shows the average processing time consumed between sending the first byte from an appliance to a web server and receiving the first byte from this server within a transaction</td>
</tr>
<tr>
<td></td>
<td>• Last Byte Sent to Server until Last Byte Received from Server — Shows the average processing time consumed between sending the last byte from an appliance to a web server and receiving the last byte from this server within a transaction</td>
</tr>
</tbody>
</table>
Logging

Logging enables you to record web filtering and other processes on an appliance. Reviewing the log files that contain the recordings allows you to find reasons for failures and solve problems.

The following elements are involved in logging:

- Log files that entries recording web filtering and other processes are written into
- System functions that write entries into log files
- Modules that write entries into log files
- Logging rules that write entries into log files
- Log file management modules that rotate, delete, and push log files

Log files

Log files contain entries on web filtering and other processes. Log files with the same kind of content are stored in folders, which are called logs. You can view all logs and log files on the user interface of an appliance.

Depending on their content, log files are maintained by functions of the appliance system, modules, or logging rules. Accordingly, you can perform some or all kinds of activities for these log files, such as viewing, editing, rotating, and others.

Logging by system functions

For some content, log file entries are written by functions of the appliance system. You can view these files on the user interface, but not edit or delete them. The files are also rotated in regular intervals by system functions.

Logging by modules

For some content, log file entries are written by particular modules, such as the proxy module or the Anti-Malware module.

You can view these files on the user interface, but not edit or delete them. Rotation and deletion of these files and pushing them to another location is handled by the Log File Manager, which you can configure settings for.

Logging by rules

A logging rule uses events to create a log file entry and write it into a log file if its criteria matches.

Like other rules, logging rules are contained in rule sets. Logging rule sets are nested in top-level rule sets, which are known as Log Handlers. A default Log Handler rule set is available after the initial setup of an appliance. This rule set includes the following nested rule sets by default.

- **Access Log** — Contains a rule that writes entries about access to a Web Gateway appliance into the log
- **Access Denied Log** — Contains a rule that writes entries about attempts to access a Web Gateway appliance that were denied into the log
- **Found Viruses Log** — Contains a rule that writes entries about viruses that were found when requests were processed on a Web Gateway appliance into the log

To these default rule sets, you can add rule sets that you import from the rule set library, for example, the Proxy Error Log rule set. These rule sets are located in the Logging rule set group of the library.
Logging rules are processed in a separate logging cycle after the request, response, and embedded object cycles have been completed for a request that is received on an appliance.

Rotation and deletion of these files and pushing them to another location is handled by the File System Logging module, which you can configure settings for.

**Log file management modules**

There are two modules for performing management activities on log files, including rotation, deletion, and pushing to other locations.

These modules are the Log File Manager for log files that are maintained by modules and the File System Logging module (also known as engine) for log files maintained by logging rules.

You can configure settings for these modules to adapt the rotation, deletion, and pushing of log files to the requirements of your network.

**Administrater logging**

You can administer the logging functions of an appliance to monitor how it performs filtering and other activities that ensure web security for your network.

Complete the following high-level steps.

**Task**

1. View the log files that are maintained on an appliance.
2. Modify the implemented log file system as needed.
   
   You can, for example, do the following:
   
   - Enable, disable, or delete logging rules
   - Modify logging rules
   - Add logging rules of your own
   - Configure the settings of the logging modules for:
     - Log file rotation
     - Log file pushing
     - Log file deletion
3. Save your changes.

**View log files**

You can view log files on the user interface of an appliance.

**Task**

1. Select the Troubleshooting top-level menu.
2. On the appliances tree, select the appliance you want to view log files for and click Log Files.
   
   A list of log file folders appears, some of which contain subfolders.
3. Double-click the folder or subfolder with the log files you want to view.
   
   The folder opens to display its log files.
4. Select the log file you want to view and click View on the toolbar above the list.
Log file types
There are several types of log files on an appliance. They differ in the kind of content that is recorded and in the way the recording is done.

Log files that record the same kind of content are stored in the same folder. A folder for storing log files with the same kind of content is called a log.

Depending on their content, log files are maintained by system functions, modules, or logging rules.

System-maintained log files
Some log files are maintained by functions of the appliance system, which includes the operating system and several system-related services.

You can view these files on the user interface, but not edit or delete them. However, when system log files are unreadable, they are not displayed on the user interface.

The files are also rotated in regular intervals by system functions. There are no options for configuring this rotation.

Module-maintained log files
Other log files are maintained by particular modules of the appliance, such as the proxy module or the Anti-Malware module.

You can view these files on the user interface, but not edit or delete them. The files are stored in subfolders that are located on the appliance under:

/opt/mwg/log

Rotation, deletion, and pushing of these files in regular intervals is handled by the Log File Manager, which you can configure settings for.

All files in these folders are handled by the Log File Manager, except those that have mwgResInfo as a part of their names.

The folders with the following names are also not handled by the Log File Manager: cores, feedbacks, tcpdump, migration, system, ruleengine_tracing, connection_tracing, message_tracing.

Logs for module-maintained log files include the following:

- **Audit log** — Stores log files that record changes to the appliance configuration
- **Debug log** — Stores log files that record debugging information
- **Migration log** — Stores log files that record migration activities
- **MWG errors logs** — Stores log files that record errors occurring in appliance components
  - There are separate errors logs for the core and coordinator subsystems, the Anti-Malware module, the user interface, and the system configuration daemon.
- **Update log** — Stores log files that record updates of modules and files

Rule-maintained log files
There are also log files that are maintained by logging rules. The recording of data is executed by events that are triggered when these rules apply.
For example, a rule triggers an event when an object that a user requested is infected by a virus. The triggered event writes an entry with information on the user, the infected object, date and time of the request, and other parameters, to the log file.

You can work with the rules for this type of log files in the same way as with any other rules.

Rotation, deletion, and pushing of these files in regular intervals is handled by the File System Logging module, which you can configure settings for.

The following rule-maintained log files are provided on an appliance by default:

- **Access log** — Stores log files that record requests and related information, including date and time, user name, requested object, infection of an object, blocking of an object

- **Found viruses log** — Stores log files that record the names of viruses and other malware that were found to infect requested objects

  The log also records date and time, user name, requested URL, and the IP address of the client a request was sent from.

- **Incident logs** — Store log files that record incidents concerning various functions, such as licensing, monitoring, or updates

To these default logs, you can add logs that you have created yourself.

**Configure log file settings**

You can configure settings for the log file management modules to modify the way log files are rotated, deleted, and pushed.

The log file management modules handle rotation, deletion, and pushing for module-maintained and rule-maintained log files.

Log file management for system-maintained log files cannot be configured.

**Tasks**

- **Configure settings for module-maintained log files on page 581**
  You can configure settings for rotation, deletion, and pushing of module-maintained log files. These activities are handled by the Log File Manager.

- **Configure settings for rule-maintained log files on page 582**
  You can configure settings for rotation, deletion, and pushing of rule-maintained log files. These activities are handled by the File System Logging module.

**Configure settings for module-maintained log files**

You can configure settings for rotation, deletion, and pushing of module-maintained log files. These activities are handled by the Log File Manager.

The settings for module-maintained log files are system settings that are configured for the Log File Manager.

**Task**

1. Select **Configuration | Appliances**.

2. On the appliances tree, select the appliance you want to configure log file settings for and click **Log File Manager**.

   The Log File Manager settings appear on the settings pane.

3. Configure these settings as needed.

4. Click **Save Changes**.
See also
Log File Manager settings on page 582

Configure settings for rule-maintained log files
You can configure settings for rotation, deletion, and pushing of rule-maintained log files. These activities are handled by the File System Logging module.

Task
1. Select Policy | Settings.
2. On the settings tree, expand File System Logging and select the log file settings you want to configure, for example, Found Viruses Log.
3. Configure these settings as needed:
4. Click Save Changes.

See also
File System Logging settings on page 584

Log File Manager settings
The Log File Manager settings are used for configuring the rotation, deletion, and pushing of log files that are maintained by particular modules of an appliance.

Settings can be configured for log files in general and for two important types of log files, which are stored in the Update Log and the Audit Log.

Global Log File Settings
Settings for log files in general
These settings include options for rotation and deletion of log files and for pushing them to another location.

Auto Rotation
Settings for rotating log files automatically according to their size and the time of day

<table>
<thead>
<tr>
<th>Table 17-23  Auto Rotation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
</tr>
<tr>
<td>Enable auto rotation</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Enable log file rotation if log file size exceeds</td>
</tr>
<tr>
<td>Enable scheduling of log file rotation</td>
</tr>
</tbody>
</table>

Auto Deletion
Settings for deleting log files automatically according to their size and the last time of modification
### Table 17-24 Auto Deletion

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable auto deletion</td>
<td>When selected, log files are deleted according to the following options. You can configure one of the two options or both.</td>
</tr>
<tr>
<td>Enable log file deletion if log file size</td>
<td>When selected, log files are deleted according to their size (in MiB), as specified in the input field that is provided.</td>
</tr>
<tr>
<td>exceeds</td>
<td></td>
</tr>
<tr>
<td>Enable autodeletion of unchanged files</td>
<td>When selected, log files are deleted after the period of time (in days) specified in the input field that is provided.</td>
</tr>
</tbody>
</table>

### Auto Pushing

Settings for pushing rotated log files automatically to another location

### Table 17-25 Auto Pushing

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable auto pushing</td>
<td>When selected, rotated log files are pushed from the local database on an appliance to the server that is specified using the following options.</td>
</tr>
</tbody>
</table>
| Destination                                 | Specifies the network protocol, host name, and path of a server. A variable can be added to the path name to specify the pushing process more precisely. For example, `%h` can be added for the host name of the appliance that log files are pushed from. The destination could then be specified as follows: `ftp://myftp.com/%h` When the log files are pushed, the variable is replaced with the appropriate value, which is a host name in this example. The variables you can use here include:  
  - `%h` — Host name of an appliance  
  - `%y` — Current year (four digits)  
  - `%m` — Current month (one or two digits)  
  - `%%` — Used for specifying the `%` character (if it is to occur in a host name) |
| User name                                   | Specifies the name of a user who is authorized to push log files to a server. The variable `%h` can be specified for the user name. It is replaced by the host name of the current appliance at run time. |
| Enable pushing log files directly after rotation | When selected, pushing follows rotation immediately.                                                                                   |
| Push interval                               | Limits the time (in hours) that elapses before the next log files are pushed if not pushed immediately after rotation to the specified value. |

### Settings for the Update Log

Specific settings for the Update Log

You can configure these settings if you want them to differ from the global log file settings.
Table 17-26 Settings for the Update Log

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable specific update log settings</td>
<td>When selected, the settings configured in the following apply to the Update Log. Otherwise the global log file settings apply.</td>
</tr>
<tr>
<td>Auto Rotation, Auto Deletion, Auto Pushing</td>
<td>These settings include the same options and are configured in the same way as the global log file settings.</td>
</tr>
</tbody>
</table>

Settings for the Audit Log

Specific settings for the Audit Log

You can configure these settings if you want them to differ from the global log file settings.

Table 17-27 Settings for the Audit Log

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable specific audit log settings</td>
<td>When selected, the settings configured in the following apply to the Audit Log. Otherwise the global log file settings apply.</td>
</tr>
<tr>
<td>Auto Rotation, Auto Deletion, Auto Pushing</td>
<td>These settings include the same options and are configured in the same way as the global log file settings.</td>
</tr>
</tbody>
</table>

Advanced

Settings for auto-deletion of core and feedback files

Table 17-28 Advanced

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable auto-deletion of core files</td>
<td>When selected, core files are automatically deleted according to the settings you configure. You can specify a number, a time interval, and a volume to let core files that exist in excess of these values be automatically deleted.</td>
</tr>
<tr>
<td>Enable auto-deletion of feedback files</td>
<td>When selected, feedback files are automatically deleted according to the settings you configure. You can specify a number, a time interval, and a volume in the same way as for core files.</td>
</tr>
</tbody>
</table>

File System Logging settings

The File System Logging settings are used for configuring the rotation, deletion, and pushing of log files that are maintained by logging rules.

File System Logging Settings

Settings for the log that stores rule-maintained log files
**Table 17-29 File System Logging Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the log</td>
<td>Specifies the name of a log.</td>
</tr>
<tr>
<td>Enable log buffering</td>
<td>When selected, the log is buffered. The buffer interval is 30 seconds.</td>
</tr>
<tr>
<td>Enable header writing</td>
<td>When selected, the header below is added to all log files.</td>
</tr>
<tr>
<td>Log header</td>
<td>Specifies a header for all log files.</td>
</tr>
<tr>
<td>Encrypt the log file</td>
<td>When selected, log files are stored encrypted.</td>
</tr>
<tr>
<td>First password, Repeat password</td>
<td>Sets a password for access to encrypted log files.</td>
</tr>
<tr>
<td>[Optional] Second password, Repeat password</td>
<td>Sets a second password for access to encrypted log files.</td>
</tr>
</tbody>
</table>

**Settings for Rotation, Deletion, and Pushing**

Settings for log file management

The settings for rotating, deleting, and pushing rule-maintained log files include the same options and are configured in the same way as the corresponding settings for module-maintained log files, which are configured as part of the Log File Manager settings.

**See also**

*Log File Manager settings on page 582*

**Create a log**

You can create a log that can be used by a logging rule to write entries into its log files. When you create a log, you do not create it separately, but as a part of creating new settings for the File System Settings module.

**Task**

1. Select **Policy | Settings**.
2. Expand **File System Logging** and select one of the existing settings, for example, **Access Log Configuration**. This will serve as a starting point for creating new settings, including the creation of a new log.
3. Click **Add** above the settings tree.
   - The **Add Settings** window opens.
4. In the **Name** field, type a name for the settings.
5. [Optional] In the **Comment** field, type a plain-text comment on the settings.
6. [Optional] Select the **Permission** tab and configure who is allowed to access the settings.
7. Under **Name of the log**, type the name of the new log.
8. Configure other settings items, such as rotation or deletion, as needed.
9. Click **OK**.
   - The **Add Settings** window closes and the new settings appear under **File System Logging** on the settings tree.
10. Click **Save Changes**.
Create a log handler

When you create new logging rules, you can insert them into existing logging rule sets or create new rule sets for them. These must be nested themselves in top-level rule sets known as log handlers. You can also use the Default log handler for inserting new logging rule sets.

Task

2. From the Rule Sets menu, select Log Handler.
3. Click Add above the log handler tree, and from the drop-down list that appears, select Log Handler.
   The Add New Log Handler window opens.
4. In the Name field, type a name for the log handler.
5. Make sure Enable is selected.
6. [Optional] In the Comment field, type a plain-text comment on the log handler.
7. [Optional] Click the Permissions tab and configure who is allowed to access the log handler.
8. Click OK to close the Add New Log Handler window.
   The new log handler appears on the log handler tree.
9. Click Save Changes.

Elements of a logging rule

A logging rule handles the writing of log file entries into a particular log. Its elements are of the same types as with other rules.

Name

Write Found Viruses Log

Criteria        Action        Events
Antimalware.Infected equals true   ->  Continue   –  Set User-Defined.LogLine =

+ DateTime.ToWebReporterString
+ “ ”
+ Authentication.Username
+ “ ”
+ String.ReplaceIf Equals (IP.ToString(Client.IP), “”, “”)
+ “ ”
+ List.OfString.ToString (Antimalware.VirusNames)
+ “ ”
+ URL
+ “ ”

FileSystemLogging.WriteLogEntry
(User-Defined.logLine)<Found Viruses Log>
The elements of this rule have the following meanings:

- **Criteria** — `Antimalware.Infected equals true`
  
  The criteria of the rule uses the `Antimalware.Infected` property. It is matched when the value of this property is `true`. This means that the rule applies when a filtered object is infected.

- **Action** — Continue
  
  When the rule applies, it executes the the Continue action. This action lets processing continue with the next rule after the events of the current rule have also been executed.

- **Events** — When the rule applies, it also executes two events:
  
  - **Set User-Defined.logLine = ...** — Sets the parameter values that are logged.
    
    Theses values are as follows:
  
  - **FileSystemLogging.WriteLogEntry ...** — Executes the write event
    
    The entry that is to be written and the log file it is written into are specified with the event:
  
    - `(User-Defined.logLine)` — Event parameter specifying the entry
      
      This is a log file line with the parameter values that have been set by the other event of the rule.
    
    - `<Found Viruses Log>` — Event settings specifying the log file

**Best practices - Adding a log file field**

Adding a log file field to the entries that are written in the log files of a log allows you to record additional information about activities that are performed on Web Gateway.

When you add a log file field, you might also want to adapt the log header and configure an entry for the new log file field. This way you ensure that the header, which is written into every log file, also includes information on this field.

### Add a log file field

To add a log file field to an entry for a log file, append an appropriate element to the configuration for writing log file entries.

In this sample procedure, the destination IP address of a client request that is received on Web Gateway is added to the rule for writing log file entries into the default access log.

**Task**

1. Select **Policy | Rule Sets**.

2. Select **Log Handler**, expand the **Default** rule set on the log handler tree, and select **Access Log**.

3. Add an element for writing log file entries.
   
   a. Select the **Write access log** rule and click **Edit** immediately above.
   
   b. Select **Events**, then select the event **Set User-Defined.logLine** and click **Edit**.
   
   c. Under **To concatenation of these strings**, click **Add**.
Click Parameter property, select IP.ToString from the properties list, and click Parameters next to the property name.

To search for the property, you can type a suitable combination of characters in the filter field above the list, for example, ip.tos.

The Parameters For Property window opens.

e Click Parameter property and select URL.Destination.IP.

f Click OK in the Parameters For Property window, then in the Enter a String window.

The new element appears in the Edit Set Property window, behind the last of the old elements, as shown here:

+ Number.ToString(Block.ID)
+ " "
+ Application.ToString(Application.Name)
+ " "+ IP.ToString(URL.Destination.IP)

4 Insert a delimiter to let the new log file field be separated from the preceding.

a Select the line with the three double quotes and click Edit.

b Enter a blank next to the double quote that appears in the window, then click OK.

The Enter a String window closes. In the Edit Set Property window, the line between the two elements should now look like this:

+ Application.ToString(Application.Name)
+ " "
+ IP.ToString(URL.Destination.IP)

c Click OK in the Enter a String and Edit Set Property windows, then click Finish in the Edit Rule window.

5 Click Finish in the Edit Rule window, then click Save Changes.

Adapt the log header

Adapt the access log header by adding a header entry for the new element that you appended to the elements for log file writing.

Task
1 Select Policy | Settings.

2 On the settings tree, expand File System Logging and select the Access Log Configuration settings.

3 Under File System Logging Settings, make sure Enable header writing is selected, and at the end of the text string in the Log header field leave a blank after the last element and type server_ip.

Header field names, such as server_ip, must not include blanks inside them, so always use underscores.

4 Click Save Changes.

Best practices - Creating a log

Creating a log allows you to log particular activities that are performed on Web Gateway. For example, you want to log all requests that were sent from a particular client and were either invalid or blocked.
The logging is performed by a logging rule. This rule applies when a request of the kind that you want to log is received on Web Gateway. It does the following:

- Record information about the request in a log file entry (also known as *log line*)
  
  This entry can include the time when a request was sent, the name of the user who sent it, and other information.

- Write the entry into a log file
  
  Log files are stored in a log. To avoid excessive memory consumption, log files can be rotated and deleted after some time.

Like any other rule on Web Gateway, the logging rule must be contained in a rule set, which is termed a log rule set.

So creating a log that logs what you want to record includes the following activities:

- Creating a log rule set
- Creating a logging rule

To create the logging rule you need to configure:

- The rule criteria
- An event that builds log file entries
- An event that writes log file entries into a log file

When the write event is configured, the log that stores the log files is also specified.

**Configuring a log file entry**

When creating a logging rule, you need to configure an event within this rule that builds the log file entries.

A log file entry provides information about an activity that is performed on Web Gateway, for example, receiving and filtering a request.

Properties are used to store this information, for example, the Authentication.Username property is used to store the name of a user who sent a request.

To configure an event that builds log file entries, you need to specify all the properties you want to use for storing information. The event combines the values of these properties to the value of a single property, which is named *User-Defined.logLine*.

The value of the User-Defined-logLine property is then written by a write event into a log file.

When specifying the properties for the event that builds the log file entries, you need to consider some requirements.

**String format**

A log file entry is a chain of data in string format. This means that the properties that are used for building an entry must have this format. Otherwise they need to be converted.

For example, to log a client IP address, the Client.IP property is used. The values of this property have a special IP address format, which can be converted using the *IP.ToString* property.
IP.ToString is specified as an element of the log file entry with Client.IP (in parentheses) as its parameter: IP.ToString(Client.IP). When this term is processed, it delivers a value that is an IP address in string format.

**Empty elements**

When a logging rule is processed, not all properties might be filled with values for a particular request. Accordingly, a log file entry can contain empty elements.

For example, the Authentication.Username property has no value if no authentication was performed for a user who sent a request. You can insert a placeholder, such as a dash, in this case.

The String.ReplaceIfEqual property is available for this purpose. It takes three parameters:

- The value that is actually recorded for a property
- A value to compare value 1 with
- A value to replace value 2 if 1 matches 2

For example, Authentication.Username, a blank, and a dash as parameters of the String.ReplaceIfEqual property, result in a dash for the user-name element of a log file entry if no user name is recorded.

**Delimiters**

To improve the readability of log file entries, configure delimiters between the elements of a log file entry. Delimiters can be blanks, quotes, and other characters.

Delimiters are specified in the same way as the main elements of an entry and are also interpreted as strings.

**Create a log rule set with a logging rule**

To create a logging rule that lets entries be written into log files and stored in a log, create a log rule set for it and configure rule criteria and events.

The purpose of the sample rule described here is to log all requests that are received from a client with a particular ID if the following also applies:

- A request is not valid under the HTTP protocol (response 403) or
- A request is blocked by the web security rules on Web Gateway (block ID is not 0)

**Task**

2. Select Log Handler and on the log handler tree, expand the Default log handler rule set.
3. Create a rule set for the logging rule.
   - This rule set will be nested in the Default rule set.
     a. Click Add, then Rule Set.
     b. In the Name field, type a suitable name for the new log rule set, for example, Troubleshooting Log.
     c. Click OK.

   The window closes and the new log rule set appears on the log handler tree.
4 Add a logging rule and name it.
   a On the settings pane, click Add Rule.
   b In the Name field, type a suitable name for the logging rule, for example, Log requests that caused issues.

5 Configure the rule criteria.
   a Select Rule Criteria. then click Add and select Advanced Criteria.
   b Select Client.IP as the property, equals as the operator, and in the field below Compare with, type an IP address as the operand, for example, 10.149.33.8.
   c Click OK.
      The Add Criteria window closes and the configured rule criteria appears in the Add Rule window.
   d Click Add again for the second part of the criteria.
   e In the same way as for the first part, configure Response.StatusCode, equals, and 403, then click OK.
   f In the same way configure Block.ID, does not equal, and 0, then click OK.

6 Configure the event that builds the log file entry.
   a Select Events and click Add, then select Set Property Value.
   b From the properties list, select User-Defined.logLine and below To concatenation of these strings click Add.
   c Click Parameter property and from the properties list, select DateTime.ToWebReporterString, as the first element of the log file entry. Then click OK.
      The Enter a String window closes and the configured element appears in the Add Set Property window.
   d Click Add, make sure Parameter value is selected, and type a blank followed by a double quote. Then click OK.
      The Enter a String window closes and the configured delimiters appear in the Add Set Property window.
   e Add the next element of the log file entry.
      • Click Add, then Parameter property.
      • Select String.ReplaceIfEquals and click Parameters next to the property name.
         The Parameters For Property window opens.
      • For the first parameter, click Parameter property, and select Authentication.Username.
      • Select the second parameter and do not enter anything in the input field on the right.
         This creates a blank as the parameter value.
      • Select the third parameter and type a dash in the input field.
      • Click OK in the Parameters For Property, then in the Enter a String window.
         The element appears in the Add Set Property window.
   f Click Add and type a double quote, a blank, and a double quote. Then click OK.
      The Enter a String window closes and the configured delimiters appear in the Add Set Property window.
Add the remaining elements by selecting the properties listed in the following. Insert delimiters between the elements, as shown in substep f.

- **Client.IP**
  For this element, configure the `IP.ToString` property with the `Client.IP` property as its parameter.
  Add the parameter as shown in substep e.

- **Request.Header.First.Line**

- **Header.Request.Get**
  Configure a parameter for this element by typing `user-agent` as the parameter value.

- **Rules.CurrentRuleSet.Name**

- **Rules.CurrentRule.Name**

- **Block.ID**
  For this element, configure the `Number.ToString` property with the `Block.ID` property as its parameter.

- **Block.Reason**
  After this last element, only use one double quote as the delimiter.

Click **OK** to close the Add Set Property window.

The event that creates the log file entry appears in the Add Rule window.

It should look like this:

```csharp
Set User-Defined.logLine =
DateTime.ToWebReporterString
+ " "
+ String.ReplaceIfEquals
(Authentication.UserName, "", "-"
+ " "
+ IP.ToString(Client.IP)
+ " "
+ Request.Header.First.Line
+ " "
+ Header.Request.Get("user-agent")
+ " "
+ Rules.CurrentRuleSet.Name
+ " "
+ Rules.CurrentRule.Name
+ " "
+ Number.ToString(Block.ID)
+ " "
+ Block.Reason
+ ""
```

If you need to make changes, select the event, click **Edit**, and work with the Edit Set Property window.

In the representation of the event, the + symbols are added by the program.

Double quotes before and after a string value are also added. So, for example, the " " for the first delimiter represents a blank and a double quote.
Configure the event that writes the log file entries into a log file.

a) Under Events in the Add Rule window (or Edit Rule window if you made changes), click Add and select Event.

b) From the events list, select FileSystemLogging.WriteLogEntry and click Parameters.

c) Click Parameter property and from the list below, select User-Defined.logLine, then click OK.

The Parameters for Execute Action window closes.

d) In the Add Event window, click Add below the Settings field.

e) Create new settings.

These settings will be used by the File System Logging module (or engine) to handle the new log you are creating.

- In the Name field, type a suitable name for the new settings, for example, Troubleshooting Log Settings.

- Under Name of the log, type troubleshooting.log.

- Select Enable header writing and in the Log header field, type the elements of the log header.

  The log header will appear at the beginning of every log file in the new log. It should represent the elements of the log file entry that you configured in step 6.

  So the log header might look like this:

  ```
  time_stamp "auth_user" "src_ip" "req_line" "user_agent" "rule_set" "rule"
  "block_page_res"
  "block_res"
  ```

- Under Settings for Rotation, Pushing, and Deletion configure the following.
  
  - Select Enable specific settings for user-defined log.
  
  - Under Auto-Rotation, select GZIP log files after rotation to save memory space.
  
  - Configure the remaining settings under Auto-Rotation and those under Auto-Deletion as needed.

  Do not enable and configure the Auto-Pushing settings, as the log files for this new log are not pushed anywhere.

f) Click OK in the Add Settings window, then in the Add Event window.

The windows close and the event that writes the log file entries appears in the Add Rule (or Edit Rule) window.

g) Click Finish.

The window closes and the new logging rule appears as a rule of the Troubleshooting Log rule set on the Rule Sets tab.

You have now created a logging rule for recording a particular kind of requests.

The log files can be viewed in the log with the configured name. The log is accessible from the Troubleshooting top-level menu on the appliance you have configured the rule on.

The path to the log is Log files | user-defined logs.
Access log rule set

The Access Log rule set is a nested rule set in the Default Log Handler rule set.

<table>
<thead>
<tr>
<th>Nested default rule set – Access Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <strong>Always</strong></td>
</tr>
</tbody>
</table>

The rule set contains the following rule.

**Write access.log**

*Always* → Continue —

Set User-Defined.logLine = DateTime.ToWebReporterString + " " " ...  

FileSystemLogging.WriteLogEntry (User-Defined.logLine)<Access Log Configuration>

The rule uses an event to fill a log file entry with parameter values relating to requests sent by users, such as user names or request headers.

It uses another event to write this entry into a log file.

The log file entry is specified as a parameter in both events. The log that stores the log file is specified by the settings of the write event.

Values for the following parameters are set and logged by the events of the rule (properties used by the event that sets the values are shown in italics):

- Date and time — **DateTime.ToWebReporterString**
- User name — **Authentication.UserName**
- Client IP address — **String.ReplaceIfEquals (IP.ToString(Client.IP), ",", "-")**
- Response status — **String.ReplaceIfEquals (Number.ToString (Response.StatusCode), ",", "-")**
- Request header — **RequestHeader.FirstLine**
- URL category — **List.OfCategory.ToString (URL.Categories)**
- URL reputation — **String.ReplaceIfEquals (URL.ReputationString, "", "-")**  
  **(URL.Reputation<Default>)**
- Media type — **MediaType.ToString (MediaType.FromHeader)**
- Body size — **String.ReplaceIfEquals (Number.ToString (Body.Size), "", "-")**
- User agent — **Header.Request.Get("User-Agent")**
- Block action ID — **Number.ToString (Block.ID)**

The logging rule applies whenever a request for access to the web is received. The two rule events for filling and writing a log entry are then executed. Processing continues with the next rule or rule set.

Found Viruses Log rule set

The Found Viruses Log rule set is a nested rule set in the Default log handler rule set.

<table>
<thead>
<tr>
<th>Nested default rule set – Found Viruses Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <strong>Always</strong></td>
</tr>
</tbody>
</table>

The rule set contains the following rule.

**Write found viruses.log**

*Antimalware.Infected equals true* → Continue —
Set User-Defined.logLine = DateTime.ToWebReporterString + " " ...  
FileSystemLogging.WriteLogEntry (User-Defined.logLine)<Found Viruses Log>

The rule uses an event to fill a log file entry with parameter values relating to web objects that are infected by viruses or other malware, such as virus names or IP addresses.

It uses another event to write this entry into a log file.

The log file entry is specified as a parameter in both events. The log that stores the log file is specified by the settings of the write event.

Values for the following parameters are set and logged by the events of the rule (properties used by the set event are shown in italics):

- Date and time — DateTime.ToWebReporterString
- User name — Authentication.UserName
- Client IP address — String.ReplaceIfEquals (IP.ToString(Client.IP), "", ":")
- Virus and malware names — ListOfString.ToString (Antimalware.VirusNames)
- URL — URL

The logging rule applies whenever a requested web object has been found to be infected. The two rule events for filling and writing a log entry are then executed.

Processing continues with the next rule or rule set.

Error handling

When errors and incidents occur on an appliance, appropriate measures can be taken. Some of these measures are controlled by rules.

Error handling using error IDs

Errors that occur on an appliance are identified by error IDs. These can be used by rules to trigger particular methods of error handling.

To enable the use of error IDs in rules, the Error.ID property is available. A rule can trigger an action or event when this property has a particular value, for example, 14000, which indicates a failure to load the Anti-Malware module.

The action or event that is triggered uses a particular method of error handling, such as blocking access to a web object or creating an entry in a log file.

A rule that uses an error ID to trigger an error handling measure could, for example, look at follows

Name
Block if Anti-Malware engine cannot be loaded
Criteria
Error.ID equals 14000
Action
Block<Cannot Load Anti-Malware Engine>

Error handling using incident information

There is a group of activities and situations on an appliance that is termed incidents. Incident information can be used by rules to trigger particular methods of error handling.

Incidents can be related to the appliance system, as well as to its subsystems and modules. For example, a failure of the Log File Manager to push log files is recorded as an incident.
Incidents can be used by rules to trigger a particular method of error handling, such as sending a notification message or creating an entry in the system log. To enable the use of incidents in rules, key incident parameters, including the ID, severity, origin, and others, are made available as properties.

For example, there is the *Incident.ID* property. A rule can use this property to trigger an event that creates a syslog entry if the value of the property is a particular number.

**Rules using incidents**

The Default rule set for error handling contains a nested rule set providing rules that trigger a notification message and other error handling events when incidents concerning the Log File Manager occur. The name of this nested rule set is Log File Manager Incidents. Other nested rule sets handle incidents related to updates and licensing.

You can also create rules and rules sets of your own that use incidents for error handling.

**Incident parameters and properties**

Incidents are recorded on an appliance with their IDs and other parameters. For each parameter, there is a property, which can be used in an appropriate rule.

- **Incident ID** — Each incident is identified by a number. For example, the incident with ID 501 is a failure of the Log File Manager to push log files. The *Incident.ID* property can be used in a rule to check the ID of an incident.

- **Description** — An incident can be explained by a description in plain text. The name of the relevant property is *Incident.Description*.

- **Origin** — Each incident is assigned to the appliance component that is its origin. Origins are specified by numbers. For example, origin number 5 specifies the Log File Handler. The name of the relevant property is *Incident.Origin*.

- **OriginName** — The origin of an incident is further specified by the name of the appliance component that is involved in the incident. The name of the relevant property is *Incident.OriginName*.

  The origin name can specify a subcomponent that is a part of the component specified by the origin number. For example, origin number 2 (Core) can be further specified by the origin name as:

  - Core
  - Proxy
  - URL Filter
  - and other names of core subcomponents

- **Severity** — Each incident is classified according to its severity. Severity levels range from 0 to 7, with 0 indicating the highest level.

  These levels are the same as those used for entries in a syslog file.

  The name of the relevant property is *Incident.Severity*.

- **Affected host** — If there is an external system that is involved in an incident, for example, a server that the appliance cannot connect to, the IP address of this system is also recorded. The name of the relevant property is *Incident.AffectedHost*.

**Configure error handling**

You can configure error handling to adapt this process to the requirements of your network. Complete the following high-level steps.
**Task**

1. Review the rules in the nested rule sets of the default rule set for error handling. The name of this rule set is *Default*.

2. Modify these rules as needed. You can, for example, do the following:
   - Enable rules that take additional measures for error handling when a particular error or incident has occurred.
   - Create new rules and rule sets for handling additional errors and incidents.

3. Save your changes.

**View the error handling rule sets**

You can view the rule sets that are implemented for error handling on a rule set tree that is provided on the user interface in addition to the normal rule set tree for web filtering rules.

**Task**


2. Below the rule sets tree, select *Error Handler*.

3. Expand the *Default* top-level rule set.
   - The nested rule sets for error handling appear.

4. Select a nested rule set.
   - The rules of the nested rule set appear on the settings pane.

**See also**

*Default error handler rule set* on page 600

**Best practices - Working with the Error Handler**

Working with the rules in the Error Handler rule sets gives you control over what happens when errors occur with processing web traffic on Web Gateway.

There are two main strategies of responding to errors:

- **Fail-closed** — When an error occurs, the request that a user sent to the web and that is being processed on Web Gateway is not allowed to proceed. A block message is shown to the user.
  
  This strategy is the default for error handling on Web Gateway.

- **Fail-open** — When an error occurs, the request that a user sent to the web and that is being processed on Web Gateway is allowed to proceed.
  
  In addition to this, logging activities and notifications can be triggered.

  This strategy is widely used within the web security policies of enterprise organizations.
The following are benefits of adopting a fail-open strategy for your network:

- Prevents business interruptions, as unimpeded web access is one of the most critical aspects for many jobs today.
- Avoids unnecessary calls to help desks, as you might consider it sufficient if the Web Gateway administrator is aware and can fix the problem. There is no need then to alert users.

A fail-open strategy can also be appropriate if failed components are compensated within your network while internal alerts are triggered and action is taken.

The flexibility of the Error Handler allows you to create rules to implement the main strategies in various ways, for example, as follows:

- Strict fail-closed strategy on all errors
- Broad fail-open strategy to prevent any user impact
- Notifications to the Web Gateway administrator as part of a fail-closed or fail-open strategy
- Exceptions for requests from particular users and clients
  
  For example, a fail-open strategy is configured for executives and a fail-closed strategy for other users.

The default rule set for error handling includes the Block on All Errors rule set. This nested rule set is placed at the end of the default rule set. It blocks requests in all error situations that are not covered by the other nested rule sets.

When you configure a fail-open rule, make sure that this rule set is disabled or the rule set with the fail-open rule is placed before it.

**See also**
- Configure a general fail-open strategy on page 598
- Configure a fail-open strategy with a notification on page 599
- Configure a fail-open strategy for user groups on page 599

**Configure a general fail-open strategy**

Configure a general fail-open strategy to let processing continue after any processing error that occurs.

**Task**

2. Select Error Handler and expand the Default error handling rule set.
3. For all rules in the nested rule sets:
   - Select a rule and click Edit for this rule.
   - In the Edit Rule window, select Action, then select Continue as the rule action.
   - Click Finish.
4. Click Save Changes.

Processing of requests that users send to the web now continues on Web Gateway even when errors occur.
Configure a fail-open strategy with a notification

Configure a fail-open strategy with a notification to notify the administrator or another recipient when a particular error has occurred. For the notification, you add an event to a rule that handles a particular error.

**Task**

1. Locate an existing rule:
   b. Select Error Handler and expand the Default error handling rule set.
   c. Select a nested rule set, for example, Block on Anti-Malware Engine Errors. Then select one of its rules, for example, Block if anti-malware engine is overloaded, and click Edit for this rule.

2. In the Edit Rule window, select Action, then select Stop Rule Set as the rule action instead of Block.

3. Configure an event for notifying someone:
   a. Select Events and click Add.
   b. Select Event, then select Email.Send and click Parameters
   c. Type values for the three string parameters, for example, as follows:
      - **Recipient (an email address):** anyrecipient@samplecompany.com
        To configure more recipients, add their email addresses, separated by semicolons.
      - **Subject (message name):** Anti-Malware Overload
      - **Body (message text):** The anti-malware engines are overloaded, please inspect the mwg-antimalware-errors-log for more information.
   d. Click OK twice, then click Finish.

4. Click Save Changes.

When the error that is handled by this rule occurs, a notification is sent to the configured recipient. You can also configure multiple notification events for different recipients with varying message texts.

Make sure that the Block on All Errors set is disabled or the rule set with the fail-open rule is placed before it.

Configure a fail-open strategy for user groups

Configure a fail-open strategy with a notification that is only sent for errors with processing requests from users belonging to a particular user group.

**Task**

1. Locate the rule that you configured a fail-open strategy with a notification for:
   b. Select Error Handler and expand the Default error handling rule set.
   c. Select the Block on Anti-Malware Engine Errors nested rule set, then select the Block if anti-malware engine is overloaded rule and click Edit for this rule.
2 Configure an additional part for the rule criteria:
   a In the **Edit Rule** window, select **Rule Criteria**, then select the criteria of the rule and click **Add**.
   
b Select **User/Group criteria**, then select:
   
   - **Authentication.UserGroups** as the property
   - **at least one in list** as the operator
   
c At the bottom of the right column, click **Add List of String** to add a list of user groups, and in the **Add List** window:
   
   - **Name the list** Groups to bypass on anti-malware overloads, then click **OK**.
   - Click **Edit List** and under **List content**, add the following string to the list (without quotes):
     Executives, then click **OK** twice.
   
d In the **Edit Rule** window, select **AND** as the Boolean operator for this additional criteria part, then click **Finish**.
   
3 Click **Save Changes**.

When the error that is handled by this rule occurs, processing continues and a notification is sent to the configured recipient. It is only sent, however, if a user from the configured user group submitted the request that was processed when the error occurred.

**Important**: Make sure that the *Block on All Errors* set is disabled or the rule set with the fail-open rule is placed before it.

---

**Default error handler rule set**
The Default error handler rule set is the default rule set for error handling.

<table>
<thead>
<tr>
<th>Default error handler rule set – Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong> – Always</td>
</tr>
</tbody>
</table>

The following rule sets are nested in this rule set:

- Long Running Connections
- Monitoring
  - Check CPU Overload
  - Check Cache Partition
  - Check Request Overload
- Log File Manager Incidents
- Handle Update Incidents
- Handle License Incidents
- Block on Antimalware Engine Errors
- Block on URL Filter Errors
- Block on All Errors

**Long Running Connections**
This nested error handler rule set keeps connections alive when a proxy module error occurs.
**Nested error handler rule set – Long Running Connections**

| Criteria – Error.ID equals 20000 |

The rule set criteria specifies that the rule set applies when the value of the Error.ID property is 20000, which indicates a malfunction of the proxy module.

The rule set contains the following rule.

**Keep connection always alive**

*Always* → Stop Cycle

When the rule is executed, it stops the current processing cycle. The rule is always executed when the criteria of its rule set is matched. Stopping the processing cycle prevents the connection from being closed in the course of further rule processing.

The rule is not enabled by default.

---

**Monitoring**

This nested error handler rule set handles measures taken when an incident occurs that involves the appliance system.

**Nested error handler rule set – Monitoring**

| Criteria – Incident.ID equals 5 |

The rule set criteria specifies that the rule set applies when the value of the Incident.ID property is 5, which indicates an incident that involves the appliance system.

The following rule sets are nested in this rule set:

- Check CPU Overload
- Check Cache Partition
- Check Request Overload

**Check CPU Overload**

This nested error handler rule set handles measures that are taken when the CPU load exceeds a configured value.

**Nested error handler rule set – Check CPU Overload**

| Criteria – Statistics.Counter.GetCurrent("CPULoad")<Default> greater than or equals 95 |

The rule set criteria specifies that the rule set applies when the value of the Statistics.Counter.GetCurrent property for CPU load is 95 or higher. This value indicates the percentage of the maximum load that the CPU is currently running with.

The Statistics module, which provides the value, runs with default settings, as is specified after the CPU Load property parameter.

The rule set contains the following rules.

**Create notification message**

*Always* → Continue – Set User-Defined.loadMessage = "CPU load at " + Number.ToString (Statistics.Counter.GetCurrent("CPULoad")<Default>) + "%"
The rule is always executed when the criteria of its rule set is matched.
The rule then uses an event to set a user-defined property to a chain of values that make up a message text about the CPU overload.
The Continue action lets processing continue with the next rule.

**Send SNMP trap and other rules**

*Always → Continue → ...*

The Send SNMP trap rule and other rules in the rule set are always executed when the rule set criteria is matched.
The rules then use different events for taking measures to make the administrator aware of the CPU overload.
These rules are not enabled by default.

**Check Cache Partition**

This nested error handler rule set handles measures that are taken when the web cache usage exceeds a configured value.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Check Cache Partition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong> – <em>Statistics.Counter.GetCurrent(&quot;WebCacheDiskUsage&quot;)&lt;Default&gt;</em> greater than or equals 95</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when the value of the Statistics.Counter.GetCurrent property for web cache usage is 95 or higher. This value indicates the percentage of the maximum allowed usage of the web cache that is currently in use.

The Statistics module, which provides the value, runs with default settings, as is specified after the WebCacheDiskUsage property parameter.

The rule set contains the following rules.

**Create notification message**


The rule is always executed when the criteria of its rule set is matched.
The rule then uses two events to set user-defined properties. One of these properties is set to the number of requests that are currently processed on the appliance per second. The other is set to a chain of values that make up a message text about the web cache usage.
The Continue action lets processing continue with the next rule.

**Send SNMP trap and other rules**

*Always → Continue → ...*

The Send SNMP trap rule and other rules in the rule set are always executed when the rule set criteria is matched.
The rules then use different events for taking measures to make the administrator aware of the web cache usage.
These rules are not enabled by default.
Check Request Overload

This nested error handler rule set handles measures that are taken when the number of requests processed on an appliance per second exceeds a configured value.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Check Request Overload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Statistics.Counter.GetCurrent(&quot;HttpRequests&quot;)&lt;Default&gt; greater than or equals 480000</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when the value of the Statistics.Counter.GetCurrent property for requests is 480,000 or higher. This value is the number of requests that are currently processed on an appliance per second.

The Statistics module, which provides the value, runs with default settings, as is specified after the HttpRequests property parameter.

The rule set contains the following rules.

Create notification message

Always –> Continue – Set User-Defined.requestsPerSecond = Statistics.Counter.GetCurrent("HttpRequests")<Default>) / 60

Set User-Defined.requestLoadMessage = "detected high load: " + Number.ToString (User-Defined.requestsPerSecond) + "requests per second"

The rule is always executed when the criteria of its rule set is matched.

The rule then uses two events to set user-defined properties. One of these properties is set to the number of requests that are currently processed on an appliance per second. The other is set to a chain of values that make up a message text about this number.

The Continue action lets processing continue with the next rule.

Send SNMP trap and other rules

Always –> Continue – ...

The Send SNMP trap rule and other rules in the rule set are always executed when the rule set criteria is matched.

The rules then use different events for taking measures to make the administrator aware of the request overload.

These rules are not enabled by default.

Log File Manager Incidents

This nested error handler rule set handles measures taken when an incident occurs that involves the Log File Manager.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Log File Manager Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Incident.ID greater than or equals 501 AND Incident ID less than or equals 600</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when the value of the Incident.ID property is within the range of incidents that involve the Log File Manager.

The rule set contains the following rules.
Create notification message

*Incident.ID equals 501 →* Continue – Set User-Defined.notificationMessage = "License expires in " + Number.ToString (License.RemainingDays) + " days"

The rule is always executed when the criteria of its rule set is matched.
The rule then uses an event to set a user-defined property to a chain of values that make up a message text on the remaining number of days for your license.
The Continue action lets processing continue with the next rule.

Create syslog entry

*Always →* Continue – ...

The Create syslog entry rule and other rules in the rule set check the value of the Incident.ID property in the same way as the Create notification message rule and use different events to take measures if this value is 501.

These rules are not enabled by default.

Handle Update Incidents

This nested error handler rule set handles measures taken when an incident occurs that involves the Log File Manager.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Handle Update Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – <em>IIncident.OriginName equals “Updater” OR Incident.ID equals 850 OR Incident.ID equals 851 OR Incident.ID equals 940 OR Incident.ID equals 941 OR Incident.ID equals 1050 OR Incident.ID equals 1051 OR Incident.ID equals 1650 OR Incident.ID equals 1651</em></td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when the update module is specified by the value of the Incident.OriginName property or the value of the Incident.ID property is one of those that involve the update module.

The rule set contains the following rules.

Create update incident message

*Always →* Continue – Set User-Defined.eventMessage = "Update Event triggered [" + Incident.Description + "]:
+ "; origin:" + Incident.OriginName + "; severity:" + Number.ToString (Incident.Severity) + 

The rule is always executed when the criteria of its rule set is matched.
The rule then uses an event to set a user-defined property to a chain of values that make up a message text about the update incident. The message includes values for several incident properties.
The Continue action lets processing continue with the next rule.
Create syslog entry

Always -> Continue - ...

The Create syslog entry rule and other rules in the rule set use different events to take measures if the respective rule criteria is matched.
These rules are not enabled by default.

Handle License Incidents

This nested error handler rule set handles measures taken when an incident occurs that involves the expiration date of the license for your appliance.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Handle License Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Incident.ID equals 200</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when the value of the Incident.ID property is 200, which indicates that the remaining number of days for your licence has been checked.

The rule set contains the following rules.

Create license incident message

Always -> Continue – Set User-Defined.notificationMessage =

"A log file cannot be pushed. Please have a look at the mwg-logfilemanager errors log (/opt/mwg/log/mwg-errors/mwg-logmanager.errors.log)."

The rule checks whether the value of the Incident.ID property is 501, which indicates that the Log File manager could not push a log file.

If this is the case, the rule uses an event to set a user-defined property for sending a notification message to a string value that is the text of this message.

The Continue action lets processing continue with the next rule.

Create syslog entry

Always -> Continue - ...

The Create syslog entry rule and other rules in the rule set use different events to take measures if the respective rule criteria is matched.
These rules are not enabled by default.

Block on Anti-Malware Errors

This nested error handler rule set blocks access to all web objects when the Anti-Malware module cannot be loaded or is overloaded.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Block on Anti-Malware Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria – Always</td>
</tr>
</tbody>
</table>

The rule set contains the following rules.

Block if Anti-Malware engine cannot be loaded

Error.ID equals 14000 -> Block<Cannot Load Anti-Malware>

The rule blocks access to all web objects when the value of the Error.ID property is 14000, which indicates an error that prevents the Anti-Malware module (also known as engine) from loading.

The action settings specify a message to a requesting user.
Block if Anti-Malware engine is overloaded

*Error.ID equals 14001 → Block<Anti-Malware Engine Overloaded>*

The rule blocks access to all web objects when the value of the Error.ID property is 14001, which indicates all connections to the Anti-Malware module (also known as *engine*) are currently in use and the module is overloaded.

The action settings specify a message to a requesting user.

Block on URL Filter Errors

This nested error handler rule set blocks access to all web objects when the URL Filter module cannot be loaded or another error regarding this module occurs.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Block on URL Filter Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong> – <em>Error.ID greater than or equals 15000 AND Error.ID less than or equals 15999</em></td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when the value of the Error.ID property lies within the specified range, which is the range for errors related to URL filtering.

The rule set contains the following rules.

Block if the URL Filter engine cannot be loaded

*Error.ID equals 15000 OR Error.ID equals 15002 OR Error.ID equals 15004 OR Error.ID equals 15005 → Block<Cannot Load URL Filter>*

The rule blocks all requests for web access when the value of the Error.ID property is one of those specified in the rule criteria. These values indicate errors that prevent the URL Filter module (also known as *engine*) from loading.

The action settings specify a message to a requesting user.

Block all other internal URL Filter errors

*Always → Block<Internal URL Filter Error>*

The rule is always executed when its rule set applies and the rule preceding it in the rule set has not been executed. The rule then blocks all requests for web access.

The action settings specify a message to a requesting user.

Block on All Errors

This nested error handler rule set blocks access to all web objects when an internal error occurs on the appliance.

<table>
<thead>
<tr>
<th>Nested error handler rule set – Block on All Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong> – <em>Always</em></td>
</tr>
</tbody>
</table>

The rule set contains the following rule.

**Always block**

*Always → Block<Internal Error>*

The rule blocks access to all web objects when an internal error occurs.

The action settings specify a message to a user who requested access.

The rule in this rule set is for handling internal errors on the appliance. It is executed at the time when an internal error occurs, which can, of course, not be predicted and can happen at any time during the filtering process or not at all. In this sense, processing the rule is not part of the normal process flow.
After executing the blocking, the rule stops all further processing of rules for the requests, responses, or embedded objects that were being filtered when the internal error occurred.

This way it is ensured that no malicious or inappropriate web objects enter your network or leave it while the appliance is not fully available.

The process flow continues when the next request is received if the internal error did not lead to a general interruption of the appliance functions.

Performance measurement

Processing time for several appliance functions is measured and shown as performance information on the dashboard. You can record this information in log files and also measure and record processing time for individual rule sets.

Performance is measured on an appliance, for example, with regard to the average time it takes to resolve host names by looking up names on a DNS server. You can view this and other performance information on the dashboard. Additionally, you can measure the time needed for processing individual rule sets.

You can also log all performance information, the one shown on the dashboard and the one you have measured yourself.

The following elements are involved when you measure and log performance information:

- Properties for logging performance information
- Logging rules that use these properties to log performance information
- Events that measure processing time for individual rule sets
- Rule sets that include rules with events to have their processing time measured

Logging properties

Several properties are available that correspond to performance information shown on the dashboard and can be used in logging rules.

For example, the property `Timer.ResolveHostNameViaDNS` corresponds to the dashboard information on the average time for looking up host names on a DNS server.

Two properties are available for logging the time that has been measured for processing an individual rule set. The `Stopwatch.GetMilliseconds` property records this time in milliseconds, the `Stopwatch.GetMicroSeconds` records it in microseconds.

Logging rules

The default logging rules on an appliance use one event to create log lines and another to write these lines into a log file.

If you add properties for logging performance information to the elements of the log lines, they are written into the log file together with the other elements of the log line.

You can use default rules for logging performance information or create rules of your own.

Events for measuring processing time

Two events are available for measuring the time consumed for processing individual rule sets. The `Stopwatch.Start` event starts the internal stopwatch that measures this time. The `Stopwatch.Stop` event stops the watch, so the time that has elapsed can be recorded.
**Measured rule sets**

To measure the time consumed for processing a particular rule set, you need to create a rule with the event for starting the internal stopwatch at the beginning of the rule set and another at the end with the stopping event.

You need to insert the stopping event also into existing rules of the rule set if they have actions that stop processing of the rule set. Otherwise, the watch would not be stopped because the rule with the stopping event at the end of the rule set is skipped.

**View performance information**

You can view performance information about several appliance functions on the dashboard.

**Task**

1. Select Dashboard | Charts and Tables.
2. Select Performance Information.
   
   Performance information appears on the tab.

**See also**

*Overview of charts and tables information on page 572*

**Configure performance measurement**

You can configure performance measurement to measure and log the performance of functions on an appliance.

Complete the following high-level steps.

**Task**

1. View the performance information shown on the dashboard and decide what kind of information you want to record in a log file.
   
   For example, you might want to record the average time consumed for looking up host names on a DNS server. This information is shown by the *DNS Lookup* feature of the dashboard.
2. Use the properties that are available for logging performance information in existing logging rules or new logging rules that you create.
   
   For example, insert the *Timer.ResolveHostNameviaDNS* property into the event that creates a log line in the *Write access.log* rule of the default *Access Log* rule set.
3. Measure the time consumed for processing particular rule sets.
   
   a. Insert a rule with an event that starts the internal stopwatch at the beginning of a rule set.
   b. To stop the watch and measure the time consumed:
      
      • Insert a rule with an event that performs these activities at the end of the rule set.
      • Insert an event that performs these activities into each of the existing rules that is capable of stopping the rule set before all its rules are processed.

   For example, to measure the processing time consumed by a URL filtering rule set:
   
   • insert a rule with the *Stopwatch.Start (URL Filtering)* event at the beginning of the rule set.
   • Insert a rule with the *Stopwatch.Stop (URL Filtering)* event at the end.
   • Insert the *Stopwatch.Stop (URL Filtering)* event into each of the whitelisting and blocking rules of the rule set because they all can stop the processing of further rules.
4 Use the properties that are available for logging the measured processing time in existing logging rules or new logging rules that you create.

For example, insert the `Stopwatch.GetMILLiseconds (URL Filtering)` property into the event that creates a log line in the `Write access.log` rule of the default Access Log rule set.

**Using properties in rules to log performance information**

You can insert performance logging properties into logging rules to let performance information be logged.

For each type of performance information that is shown on the dashboard, a logging property is available.

For example, the dashboard shows the average time it takes to resolve host names by looking up names on a DNS server. The property `Timer.ResolveHostNameViaDNS` corresponds to this information. The value of the property is the time consumed for looking up a host name in a request that was processed on an appliance. The time is measured in milliseconds.

Other performance logging properties are `Timer.HandleConnect ToServer` for measuring the time needed to connect to external servers or `Timer.TimeConsumedByRule Engine` or the time the rule engine consumes for processing when a request is received on an appliance.

All properties that make dashboard performance information available for logging have the element `Timer` at the beginning of their names.

**Measuring processing time for a transaction**

The time that is measured and made available by a property for logging performance information shown on the dashboard is the time needed for a particular activity, for example, connecting to external servers, as long as processing for an individual request is continued throughout the relevant processing cycles.

Processing one individual request throughout the relevant cycles is considered one transaction.

It is not required for a transaction to include all three cycles (request, response, and embedded objects).

For example, if a user sends a request for a web page that falls into a blocked category, a block message is returned to this user, the request is not forwarded to the web server in question, and processing does not enter the response cycle.

Then the transaction includes only the request cycle, the response cycle is not relevant in this case.

**Rule for logging performance information**

An Access Log exists by default on an appliance with log files into which a log entry is written whenever a transaction has been completed for a request. This log is an appropriate device for recording performance information.

Writing log entries into the log files of the Access Log is performed by a logging rule. This rule uses one event to create a log file entry and another to write this entry into a log file.

Name

**Write access.log**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>-&gt;</td>
<td>Continue</td>
</tr>
</tbody>
</table>
|          |        | Set User-Defined.logLine = DateTime.ToWebReporterString + ""
A log entry is composed of several elements, each of which adds a particular piece of information, for example, the date and time when a request was received on the appliance. By adding an element providing performance information to the entry you can let this information be logged.

To log performance information, for example, on the processing time consumed by DNS lookups, you need to add the following two elements:

- + Number.ToString (Timer.ResolveHostNameViaDNS)
- + ""

Since the log entry is a string, the numerical value for the processing time must be converted to string format before it can be logged.

This is done by the Number.ToString property, which takes the Timer.ResolveHostNameViaDNS property as a parameter.

### Using events in rules to measure rule set processing time

You can measure the time it takes to process an individual rule set by inserting rules with measuring events into it.

The reason for measuring processing time could be that you want to know whether performance is improved or reduced after you have applied changes to a rule set.

The events for measuring rule set processing time control an internal stopwatch on an appliance. The following events are available:

- **Stopwatch.Start** — Starts the internal stopwatch
- **Stopwatch.Stop** — Stops the watch
- **Stopwatch.Reset** — Resets the watch

Each of these events takes a string parameter to indicate which rule set it measures. For example, an event that starts the internal watch to measure the processing time of the URL Filtering rule set, would appear in a rule as follows: **Stopwatch.Start ("URLFiltering")**.

### Rules for measuring processing time

A rule that uses, for example, the Stopwatch.Start event to start measuring processing time for the URL Filtering rule set could look as follows:

#### Name

**Start stopwatch for rule set**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>Continue</td>
<td>Stopwatch.Start (&quot;URLFiltering&quot;)</td>
</tr>
</tbody>
</table>

To measure the time consumed for processing the rule set, you need to place a rule with the starting event at the beginning of the rule set and another one that contains the stopping event at the end.

However, if you have rules in a rule set that can execute a Stop Rule Set, Stop Cycle, or Block action, you also need to insert a stopping event into each of these rules.
A URL filtering rule with an event to stop the internal watch inserted would look as follows:

Name

**Allow URLs in URL Whitelist**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Event</th>
</tr>
</thead>
</table>
| *URL matches in URL Whitelist*   | Continue| `Stopwatch.Stop ("URLFiltering")`

When this rule is applied, it stops processing the URL Filtering rule set because the URL that a user requested access for has been found to be on the list of allowed URLs. The stopping event must therefore be inserted into this rule.

This is required because the rule with the stopping event at the end of the rule set is then not processed as the whitelisting rule stops processing of the rule set before this rule is reached.

**Logging measured processing time**

You can log the time that has been measured for rule set processing. Two properties are available for this purpose, which you can use in logging rules.

- `Stopwatch.GetMilliseconds` — Time measured for rule set processing in milliseconds
- `Stopwatch.GetMicroSeconds` — Time measured for rule set processing in microseconds

Both properties have a string parameter, which indicates the rule set that processing time was measured for.

For example, a property for logging the processing time of the URL Filtering rule set in milliseconds would appear in a logging rule as follows: `Stopwatch.GetMilliseconds ("URL Filtering")`.

---

**Event monitoring with SNMP**

Events that occur on the appliance system can be monitored using SNMP.

When monitoring is performed under SNMP (Simple Network Management Protocol), an SNMP agent that runs on a host system sends messages about events that occur on this system to other host systems that are its clients.

The messages are known as *traps* under SNMP, while the host system that the SNMP agent runs on is known as *management station*. The host systems that receive messages from the agent are also management stations, in addition to this, they are known as *trap sinks*.

Particular users or user communities are given permission to view the information sent with the traps. System information is also provided in the Management Information Base (MIB), which uses a tree structure to present the information.

**Configure the SNMP settings**

You can configure the SNMP settings to enable the monitoring of system events on an appliance.

**Task**

1. Select **Configuration | Appliances**.

2. On the appliances tree, select the appliance you want to configure SNMP monitoring on and click **SNMP**.
3 Configure the SNMP settings as needed.

4 Click Save Changes.

See also
SNMP settings on page 612

SNMP settings
The SNMP settings are settings for configuring the monitoring of system events under SNMP.

SNMP Port Settings
Settings for the ports of the SNMP agent on an appliance that listen to client requests

Table 17-30 SNMP Port Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listener address list</td>
<td>Provides a list for entering the ports that listen to client requests.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the listener address list.

Table 17-31 Listener address – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Specifies the protocol used for the communication between a port and the clients that it listens to.</td>
</tr>
<tr>
<td>Listener address</td>
<td>Specifies the IP address and port number of a listener port.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a listener port.</td>
</tr>
</tbody>
</table>

The following two listener ports are available on an appliance and entered in this list by default.

- UDP — 0.0.0.0:161
- UDP — 0.0.0.0:9161

SNMP System Information
Settings for the appliance that is the monitored system

Table 17-32 SNMP System Information

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Identifies the monitored system.</td>
</tr>
<tr>
<td>Object ID</td>
<td>Specifies the ID of the object in the Management Information Base (MIB) where information on the monitored system begins. For example: .1.3.6.1.4.1.1230.2.7.1.1</td>
</tr>
<tr>
<td>Contact person</td>
<td>Specifies the name of the person who administers the SNMP functions of the monitored system.</td>
</tr>
<tr>
<td>Physical location</td>
<td>Specifies the location of the monitored system.</td>
</tr>
</tbody>
</table>

SNMP Protocol Options
Settings for SNMP protocol versions and user access to SNMP information
Table 17-33 SNMP Protocol Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP v1</td>
<td>When selected, system events are monitored under version 1 of SNMP.</td>
</tr>
<tr>
<td>SNMP v2c</td>
<td>When selected, system events are monitored under version 2c of SNMP.</td>
</tr>
<tr>
<td>Communities for SNMPv1 and SNMPv2c access</td>
<td>Provides a list for entering the user communities who are allowed access to SNMP information under versions 1 and 2c of SNMP.</td>
</tr>
<tr>
<td>SNMP v3c</td>
<td>When selected, system events are monitored under version 3 of SNMP.</td>
</tr>
<tr>
<td>SNMP v3 users</td>
<td>Provides a list for entering the users who are allowed access to SNMP information under version 3 of SNMP</td>
</tr>
</tbody>
</table>

The following tables describe the entries in the list of user communities and the list of SNMP v3 users.

Table 17-34 User communities – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community string</td>
<td>Provides a string used for authenticating a user community to let it access SNMP information, for example, public.</td>
</tr>
<tr>
<td>Allowed root OID</td>
<td>Identifies the item on the MIB tree that is the beginning of the information with allowed access. If * or no value is specified here, access to all information is allowed.</td>
</tr>
<tr>
<td>Allowed from</td>
<td>Specifies the host name or IP address of a host system that access to SNMP information is allowed from.</td>
</tr>
<tr>
<td>Read-only access</td>
<td>When selected, only reading access to SNMP information is allowed.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a user community.</td>
</tr>
</tbody>
</table>

Table 17-35 SNMP v3 users – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specifies the name of a user who is allowed access to SNMP information.</td>
</tr>
<tr>
<td>Allowed root OID</td>
<td>Identifies the item on the MIB tree that is the beginning of the information with allowed access. If * or no value is specified here, access to all information is allowed.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Sets the authentication method used when SNMP information is accessed by a user.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Sets the encryption method used when SNMP information is accessed by a user.</td>
</tr>
<tr>
<td>Read-only access</td>
<td>When selected, only reading access to SNMP information is allowed.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a user.</td>
</tr>
</tbody>
</table>

SNMP Trap Sinks

Settings for the host systems that receive SNMP messages

Table 17-36 SNMP Trap Sinks

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap sinks</td>
<td>Provides a list for entering the host systems, known as trap sinks, that receive messages about system events from the SNMP agent on an appliance.</td>
</tr>
</tbody>
</table>

The following table describes an entry in the list of trap sinks.
### Table 17-37  Trap sinks – List entry

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name or IP address</td>
<td>Specifies the host name or IP address of a host system that receives SNMP messages, which are known as traps.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port on a host system that listens to SNMP messages.</td>
</tr>
<tr>
<td>Community string</td>
<td>Specifies the string used for authenticating a user community to let it access SNMP information, for example, public.</td>
</tr>
<tr>
<td>Send SNMP v2c traps</td>
<td>When selected, messages can be sent under version v2c of the SNMP protocol.</td>
</tr>
<tr>
<td>Comment</td>
<td>Provides a plain-text comment on a host system that receives SNMP messages.</td>
</tr>
</tbody>
</table>

### SNMP MIB Files

Files in txt format providing additional information about SNMP monitoring on an appliance

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAFEE-SMI.txt</td>
<td>Provides Structure of Management Information (SMI) on McAfee, including contact information for the McAfee customer service.</td>
</tr>
<tr>
<td>MCAFEE-MWG-MIB.txt</td>
<td>Provides descriptions of the items in the Management Information Base (MIB) that you can do SNMP monitoring for on an appliance</td>
</tr>
</tbody>
</table>

---

### Transferring data for McAfee ePO monitoring

Transferring data from an appliance to the McAfee ePolicy Orchestrator® (McAfee ePO®) console allows you to monitor the appliance from the console.

The McAfee ePolicy Orchestrator console is a device for performing security management on different McAfee products, including the McAfee Web Gateway appliance.

If you configure the McAfee ePO console and an appliance accordingly, you can log on to the appliance from the console and have monitoring data transferred from the appliance to the server that the console is running on. This server is also referred to as the McAfee ePO server.

The McAfee ePO server sends SSL-secured requests to retrieve the monitoring data that has been collected on the appliance in regular intervals. Then you need to allow the CONNECT request that the SSL-secured communication begins with to bypass the normal processing of web security rules, so it does not get blocked on the appliance.

For example, if you have authentication rules implemented, this would lead to blocking because the server does not support the authentication method used by these rules.

You can import an appropriate rule set from the library to enable the bypassing or create a rule set of your own.

### Configure the ePolicy Orchestrator settings

You can configure the ePolicy Orchestrator settings to enable the transfer of monitoring data from an appliance to a McAfee ePO server.

**Task**

1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to transfer monitoring data from and click ePolicy Orchestrator.
Configure the ePolicy Orchestrator settings as needed.

Click **Save Changes**.

See also

*ePolicy Orchestrator settings* on page 615

**ePolicy Orchestrator settings**

The ePolicy Orchestrator settings are used for configuring the transfer of monitoring and other data from a Web Gateway appliance to a McAfee ePO server.

**ePolicy Orchestrator Settings**

Settings for transferring monitoring data to a McAfee ePO server

**Table 17-39 ePolicy Orchestrator Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePO user account</td>
<td>Specifies a user name for the account that allows the retrieval of monitoring data from an appliance.</td>
</tr>
<tr>
<td>Password</td>
<td>Sets a password for a user.</td>
</tr>
<tr>
<td>Change</td>
<td>Opens a window to create a new password.</td>
</tr>
<tr>
<td>Enable data collection for ePO</td>
<td>When selected, monitoring data for the McAfee ePO server is collected on an appliance.</td>
</tr>
<tr>
<td>Data collection interval in minutes</td>
<td>Limits the time (in minutes) that elapse between data collections. The time is set on a slider scale, ranging from 10 minutes to 6 hours.</td>
</tr>
</tbody>
</table>

**ePo DXL Settings**

Settings for configuring the credentials submitted by Web Gateway when connecting to a McAfee ePO server to enable DXL messaging

**Table 17-40 ePo DXL Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePO host name</td>
<td>Specifies the host name that Web Gateway uses when connecting to a McAfee ePO server.</td>
</tr>
<tr>
<td>ePO user account</td>
<td>Specifies a name for the user account that Web Gateway submits when connecting to a McAfee ePO server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password that Web Gateway submits when connecting to a McAfee ePO server. Clicking <strong>Set</strong> opens a window for setting a new password.</td>
</tr>
</tbody>
</table>

**Bypass ePO Requests rule set**

The Bypass ePO Requests rule set is a library rule set for allowing requests from a McAfee ePO server to bypass filtering rules on an appliance.

**Library rule set – Bypass ePO Requests**

<table>
<thead>
<tr>
<th>Criteria – Command.Name equals “CONNECT”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycles – Requests (and IM)</td>
</tr>
</tbody>
</table>

The rule set criteria specifies that the rule set applies when the SSL-secured communication between an ePO server and an appliance begins with a request from the server to connect to the appliance.
The rule set contains the following rule.

**Skip subsequent rules for ePO requests**

```
URL.Host equals "127.0.0.1" OR URL.Host equals "[::1]" -> Stop Cycle – Enable SSL Client
Context<Default CA> – Enable SSL Scanner <Certificate verification without edh>
```

The rule uses the URL.Host property to identify the host of a requested URL, based on the IP address of the host.

If this address is 127.0.0.1, the host of the requested URL is the appliance. When the ePO server sends a request to connect to the appliance, it uses this address.

So if 127.0.0.1 is the requested address, the rule applies and stops all further processing in the request cycle. This way the CONNECT request is allowed to pass through.

The next step in this process is sending and verifying certificates. The rule includes an event to enable the sending of a client certificate that is issued by the default certificate authority.

You can modify the event settings to have the certificate issued by another authority.

When certificate verification has been completed, the SSL-secured communication can go ahead.

---

**Best practices - Sending access log data to a syslog server**

You can configure Web Gateway to send data that is recorded in the access log to a syslog server. Data about requests for web access that Web Gateway receives from its clients is recorded in the access log. The recording is performed by a rule in a rule set for log handling, which is enabled by default. By adding another rule this data can be made available to a daemon, which sends it to a particular syslog server.

The recorded data includes date and time of a request, the user name of the user who sent the request, the requested URL, and other information. You can modify the configuration to record more or different information about web access.

The data can be sent under different protocols and in different formats. You can also configure a severity level to send, for example, only data about emergencies.

To send the data, you must complete the following:

- Add a rule that makes access log data available to the syslog daemon.
- Adapt the `rsyslog.conf` system file to let the daemon send data to a syslog server.

These activities must be completed on every Web Gateway appliance that access log data are to be sent from. In a similar way, you can also configure the sending of other log data.

**Protocols for sending data**

Data can be sent to a syslog server under the UDP or TCP protocol. Some syslog servers have no TCP listener ports, however. The most common UDP listener port is 514, whereas under TCP the port varies from application to application.
**Data formats**

Data is sent to syslog servers in different formats, depending on the server type. If in doubt, ask the administrator who is responsible for the syslog server.

- **Default format** — The default log handling rule uses this format to record access log data.
  
  The format and modified versions of it are also accepted by McAfee Content Security Reporter, version 2.0.

- **SIEM (Nitro) format** — This format is required if the syslog server is provided by McAfee Enterprise Security Manager (McAfee ESM) (SIEM, formerly known as Nitro).
  
  You can import the *SIEM Nitro Integration* rule set from the online rule set library. This rule set contains a rule that uses the SIEM (Nitro) format to record access log data.

- **CEF format** — This format is required if the syslog server is provided by an ArcSight security manager or a similar program.
  
  You can import the *CEF Syslog* rule set from the online rule set library. This rule set contains a rule that uses the CEF format to record access log data.

**Severity levels**

Data with differing severity can be sent to a syslog server. The severity levels are listed in the following. Severity level 6 is recommended.

- 0: Emergency (emerg) — System unusable
- 1: Alert (alert) — Action to be taken immediately
- 2: Critical (critical) — Critical condition
- 3: Error (error) — Error condition
- 4: Warning (warning) — Warning condition
- 5: Notice (notice) — Normal, but significant condition
- 6: Information (info) — Informational message
- 7: Debug (debug) — Message for debugging

**Add a rule for sending access log data**

To send access log data from Web Gateway to a syslog server, add a rule to the rule for recording data in the Access Log rule set.

**Task**

1. Select **Policy | Rule Sets**.

2. Click **Log Handler**, expand the **Default** rule set, and select the nested **Access Log** rule set.

   The content of the nested rule set appears on the configuration pane. By default the rule set contains a rule that writes data about web access to a log line.
Add the following rule to make access log data available to the daemon that sends it to the syslog server.

<table>
<thead>
<tr>
<th>Name</th>
<th>Make access log data available to syslog daemon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Action Event</td>
<td>Always Continue Syslog (6, User-Defined.logLine)</td>
</tr>
</tbody>
</table>

The rule uses an event to make the access data that has been written to a user-defined log line before to the syslog daemon. The syslog daemon sends it to the syslog server. The daemon is configured in the `rsyslog.conf` system file.

The first event parameter specifies the severity level of the access log data.

Click **Save Changes**.

The rule is for making available data that the preceding rule records in default format. If the syslog server requires a different format, replace the preceding rule with a rule that uses the required format.

You can import rule sets with rules that write data in SIEM or CEF format from the online rule set library.

### Adapt the rsyslog.conf system file for sending access log data

Adapt the `rsyslog.conf` system file to ensure that access log data is successfully sent to a syslog server.

Work with the **File Editor** on the user interface of Web Gateway to adapt the system file. If you use commands from a system console, your changes will be overwritten by future updates.

**Task**

1. Select **Configuration | File Editor**.
2. On the files tree, select **rsyslog.conf**.
   The file content appears on the configuration pane.
3. Edit the file to adapt it for sending access log data.
   a. Look for the following line:
      ```
      *.info;mail.none;authpriv.none;cron.none /var/log/messages
      ```
      The line is part of a section on rules.
      ```
      # Include config files in /etc/rsyslog.d
      $IncludeConfig /etc/rsyslog.d/*.conf
      #######RULES####
      # Log all kernel messages to the console.
      # Logging much else clutters up the screen.
      #kern.*
      /dev/console
      
      # Log anything (except mail) of level info or higher.
      # Don't log private authentication messages!
      *.info;mail.none;authpriv.none;cron.none /var/log/messages
      ```
b. Replace `mail` with `daemon` in this line and insert a `-` (dash) before the path information.

```
*.info;daemon.none;authpriv.none;cron.none                -/var/log/messages
```

This modification prevents the syslog daemon from sending data to the `var/log/messages` partition on the disk of the Web Gateway appliance system.

### Information

The `info` before `daemon` specifies the severity level of the data.

You can now direct the data to the intended destination.

c. To send data to a syslog server under the UDP protocol, insert:

```
daemon.info.@x.x.x.x:514
```

`x.x.x.x` must be substituted with the IP address of the syslog server.

To send messages to a syslog server under TCP, insert:

```
daemon.info.@@x.x.x.x:<port number>
```

4. Click **Save Changes**.

### Resolving issues with sending access log data

Several measures can be taken to resolve issues with sending access log data from Web Gateway to a syslog server.

- If access log data is not received on the syslog server, it might still be written to the `var/log/messages` partition on the disk of the Web Gateway appliance system.

  Run the following command from a system console to verify that data is not written to disk:

  ```
tail -f /var/log/messages
```

- If access log data is not received on the syslog server, it might be due to restrictions that are, for example, imposed by a firewall. You can perform a tcpdump to see whether Web Gateway sends data packets to the syslog server at all.

  Run the following command from a system console to see the data packets, for example, when they are sent to the syslog server under the UDP protocol:

  ```
tcpdump port 514
```

  You should also review the `rsyslog.conf` system file to make sure that sending data to the syslog server is configured correctly.

- Web Gateway truncates a data packet that is sent to the syslog server by default if it has more than 2000 characters.

  Add the following line to the `rsyslog.conf` system file to adjust the packet length:

  ```
$MaxMessageSize <maximum number of characters>
```
Sending syslog data to McAfee Enterprise Security Manager

Data that is logged on Web Gateway in syslog log files can be sent to McAfee Enterprise Security Manager (McAfee ESM).

The data transfer is controlled by a rule in a rule set that is available in the online rule set library for Web Gateway. The component of McAfee ESM that the data is sent to is the McAfee SIEM Receiver.

To enable the transfer, you adapt a system file for remote use of syslog data on Web Gateway. The name of this system file is rsyslog (the r in the file name stands for remote). You must also configure the McAfee SIEM Receiver to let Web Gateway be included as a data source in the McAfee ESM environment.

Version 9.3.2 or a later version of McAfee ESM is required for the data transfer to work.

Configure the sending of syslog data

To send syslog data that is collected on Web Gateway to McAfee ESM, complete the following high-level steps.

Task

1. Import the McAfee SIEM rule set from the online rule set library for Web Gateway. Place it as a nested rule set in the default Log Handler rule set.
   In the online rule set library, this rule set is available under SIEM (Nitro) Integration.

2. In the imported rule set, enable the Send to syslog rule and disable the Send to nitro.log rule.

3. Use the File Editor to adapt the rsyslog system file for the data transfer.
   If you are running multiple Web Gateway appliances in a Central Management cluster, adapt the system file on every appliance within the cluster.

4. On McAfee ESM, configure the McAfee SIEM Receiver to let Web Gateway be added as a data source.
   For more information, see the documentation for McAfee ESM and the Data Source Configuration Guide. The guide is provided in the online rule set library under SIEM (Nitro) Integration.

Adapt the rsyslog system file for the data transfer

Adapt the rsyslog system file on Web Gateway to ensure that syslog data is successfully sent to McAfee ESM.

Task

1. Select Configuration | File Editor.

2. On the files tree, select rsyslog.conf.
   The file content appears on the configuration pane.
3  Edit the file to adapt it for the data transfer.

The edited file should look as shown in the following. The modified lines are in the paragraph that begins with: The below will direct all daemon.info messages to the remote syslog server ...

![The information that you provide here includes the IP address of the McAfee SIEM Receiver.]

```bash
# default parameters
$DirCreateMode 0755
$FileCreateMode 0640
$FileGroup adm
$umask 0026

# Include config files in /etc/rsyslog.d
$IncludeConfig /etc/rsyslog.d/*.conf

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*
/dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
# The following directs all daemon.info messages to the
# remote syslog server at [IP_OF_MCAFEE_EVENT_RECEIVER]
# add @@ for TCP syslog for example
daemon.info @192.168.1.1
*.info;daemon.!=info;mail.none;authpriv.none;cron.none
-/var/log/messages

# The authpriv file has restricted access.
authpriv.*
/var/log/secure

# Log all the mail messages in one place.
mail.*
/var/log/maillog

# Log cron stuff
cron.*
/var/log/cron

# Everybody gets emergency messages
*.emerg

# Save news errors of level crit and higher in a special file.
news.crit
/var/log/spooler

# Save boot messages also to boot.log
local7.*
/var/log/boot.log
```

4  Click Save Changes.

**Fine-tuning the collection and evaluation of syslog data**

Several fine-tuning activities can be performed to ensure that relevant syslog data is collected on Web Gateway and efficiently evaluated on McAfee ESM.

The amount of syslog data that is collected can be throttled by excluding less relevant data and restricting the process to logging only important events. Relevant data can also be added, however, to the syslog data by implementing additional logging activities.

On McAfee ESM, data aggregation can be disabled to ensure that no relevant data is overlooked.
**Throttling the amount of syslog data**

The amount of syslog data that Web Gateway sends to McAfee ESM can be throttled by taking, for example, the following measures.

- **Excluding Authentication Required (status code 407) responses** — These are standard responses that do not require much attention regarding web security.

  To exclude these responses from the syslog data that is transferred, add a rule in the rule set that you imported.

  The rule must be placed, together with other throttling rules that you might implement, at the top of the rule set. It should look as follows:

  Name
  
  **Exclude 407 responses**

  Criteria                              Action
  Response.StatusCode equals 407       -> Stop Rule Set

- **Sending only logged Block actions** — Block actions are crucial in maintaining web security, but usually account for only a small proportion of web traffic.

  To restrict the syslog data that is transferred to log files for these actions, add a rule in the rule set that you imported.

  The rule must be placed, together with other throttling rules that you might implement, at the top of the rule set. It should look as follows:

  Name
  
  **Send only logged Block actions**

  Criteria                              Action
  Block.ID equals 0                     -> Stop Rule Set

**Adding hashes of infected files to the syslog data**

To the syslog data can be added the hash values of files that were processed on Web Gateway and found to be infected. File hashes can be useful for tracking infections and possible outbreaks.

As hashing consumes a large amount of resources, we recommend using it only for important issues. If in doubt, consult McAfee support.

To enable the calculation and logging of file hashes, add an event to the rule that detects and blocks infected files. By default, this rule is *Block if virus was found* in the Gateway Anti-Malware rule set.

The event should look as follows:

```
```

The `Header.Block.Add` event is a preconfigured event that you can select from the list of available events. It adds an entry to the syslog log when the rule that it is inserted in applies.
The event takes two parameters, which you must configure:

- **X-Hash-MD5** — Name of the log entry
- **Body.Hash("md5")** — Value of the log entry

This parameter is a property for calculating the hash value of a file. Here it calculates the hash value of the infected file that was sent to Web Gateway as the body of a request or response.

The property takes itself a parameter, which determines the method for calculating the hash.

If you are working with the key elements view for rule sets, you must switch to the complete rules view to add the event.

After adding the event, the blocking rule should look as follows.

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block if virus was found</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antimalware.Infected&lt;Gateway Anti-Malware&gt;equals true</td>
<td>Block&lt;Virus Found&gt;</td>
<td>Statistics.Counter.Increment (&quot;BlockedByAntiMalware&quot;, 1)&lt;Default&gt;</td>
</tr>
</tbody>
</table>

Disabling the aggregation of syslog data

When the McAfee SIEM Receiver receives syslog data from Web Gateway, this data is by default aggregated into a single record. While aggregation can be useful for many data sources, it could be undesirable for Web Gateway, as critical information might get lost during aggregation.

You can disable aggregation for Web Gateway data on McAfee ESM.

For more information, see the documentation for McAfee ESM and the **Data Source Configuration Guide**. The guide is provided in the online rule set library under **SIEM (Nitro) Integration**.

Resolving issues with the transfer of syslog data

To resolve issues with sending syslog data from Web Gateway to McAfee ESM, several measures can be taken.

- Review the configuration on Web Gateway and make sure that the following applies:
  - The **Send syslog** rule is enabled.
  - The IP address of the McAfee SIEM Receiver is correctly specified in the **rsyslog** system file.
- Review the configuration on McAfee ESM.
  For more information on this step and on others that are performed on McAfee ESM, see the documentation on McAfee ESM and the **Data Source Configuration Guide**. The guide is provided in the online rule set library under **SIEM (Nitro) Integration**.
- Verify that syslog data is generated on Web Gateway, for example, by running the following command from a system console:

  tcpdump -s 0 -I any port 514
- Verify that syslog data is received on the McAfee SIEM Receiver.
- Verify that the syslog log is generated on Web Gateway in proper format.

Entries in the syslog log usually look as follows:

```
url_port=80|status_code=200|bytes_from_client=187|bytes_to_client=272|
media_type=|application_name=|user_agent=Mozilla/4.0 (compatible; Synapse)|
block_res=0|block_reason=|virus_name=|hash=|

url_port=80|status_code=200|bytes_from_client=376|bytes_to_client=200|
categories=|rep_level=|method=GET|url=http://www.nitroguard.com/ngdb.dll?NG:DoIt:0:Info=D8BC0B7C97D2C352AFE4643FEA44AE4D4C70F79271D4620B64294729E046CB607B5458AC24BA31B061A12313E016EBF62ED267DC6FE9A02A552681347EF796303514934EEO08F0DA76B27F5EEA225B0DB274367AF4FEA574EA6137728|
media_type=|application_name=|user_agent=Mozilla/4.0 (compatible; Synapse)|block_res=0|block_reason=|virus_name=|hash=|
```
Several methods and tools are available for troubleshooting problems on an appliance.

Contents
- Troubleshooting methods
- Rule tracing
- Create a feedback file
- Enable the creation of core files
- Enable the creation of connection tracing files
- Create a packet tracing file
- Work with system and network tools
- Restart a service of the operating system
- Display running AV threads
- Back up and restore an appliance configuration
- Troubleshooting settings

Troubleshooting methods

When problems arise on an appliance, you can use different methods to solve them.

Rule tracing

You can create and review rule traces on the user interface. The traces record how rules were processed to deal with requests sent from clients of Web Gateway, as well as with the responses to these requests that were received from the Web.

Reviewing these traces enables you to find out which rules were processed and what actions, for example, block actions, they executed for a particular request.

Tracing information is shown on the user interface for:

- **Cycles** — Request, response, or embedded objects cycle that a rule action was executed in
- **Rules** — Rules that were processed in these cycles
- **Rule sets** — Rule sets that these rules belong to
- **Rule Criteria** — Criteria that matched to let a rule action be executed
- **Properties** — Properties and the values they had when the rule criteria matched
- **Actions** — Actions that were executed when the rule criteria matched
- **Events** — Events that were executed when the rule criteria matched
Recording and inspecting data in files
You can record data on appliance behavior in files and inspect them. The following types of files can be created for this purpose:

- **Log files** — Log events and functions, such as access to an appliance or updates of files
- **Rule tracing files** — Record the processing of rules
- **Feedback files** — Backtrace processes that went on before the failure of a function
- **Core files** — Record memory content after the failure of a function has caused an appliance to terminate operation
- **Connection tracing files** — Record activities on connections between an appliance and other network components
- **Packet tracing files** — Record network activities of an appliance

Using network tools
You might need to test whether connections from an appliance to other network components still work. Several tools are available for this purpose, including **ping**, **nslookup**, **ipneigh**, and others.

Using system tools
You can use system tools to perform a service restart on Web Gateway and also to display the AV threads that are currently running.

Restoring a configuration
When other troubleshooting methods do not work, it might be necessary to remove a faulty appliance configuration and replace it with a backup.

Having a backup available can also help in other situations, for example, when you want to discard changes applied to an existing configuration.

Options are provided for creating backups and using them to restore configurations.

Rule tracing
To debug issues with rule processing, you can use rule tracing functions on the user interface. Rule traces can be created, which record the activities that were completed to process the implemented rules when users of your network sent requests for web access from particular clients.

You can filter these traces according to the date of creation, the URL that was sent with a request, or the rule action, such as Block, Redirect, or Continue, and others, that was executed when a rule was processed.

Tracing covers all activities in the different processing cycles that were performed for a request, including the request, response, and embedded object cycles. Tracing results can be viewed separately for different cycles.

Properties in the criteria of the rules that were involved in the processing can also be viewed separately, together with the values they were set to when the rules were processed.
Three panes are provided on the rule tracing page of the user interface to let you complete rule tracing activities.

- **Traces pane** — Allows you to create traces, filter, and remove them
  You can also export and store traces and import them again for viewing later on or import traces that have been created on other Web Gateway appliances.

- **Rules pane** — Allows you to select a processing cycle and view the rule sets and individual rules that were processed in this cycle

- **Details pane** — Allows you to view the rule criteria of individual rules with their properties and the values the properties have been set to

**Cycles in rule tracing**
Processing starts when a request for web access has been received from a client of Web Gateway. It is performed in different cycles, beginning with the request cycle, in which rules are processed that are related to the elements of the request itself, for example, to a URL that was sent with a request.

If none of the rules in this cycle forbids a forwarding of the request to the web, for example, due to a negative categorization of a URL, the request is forwarded. Processing then waits for a response from the web.

When the response arrives, the rules of the response cycle are processed. For example, when a file that was requested for downloading is sent in response, it is scanned for virus and other malware infections according to a particular rule and eventually passed on or not to the client that requested the download.

Other processing cycles are performed for embedded objects sent with requests or responses. Processing activities can also be logged according to the configured logging rules.

All processing that is performed in the different cycles for an initial request from a client of Web Gateway can be viewed as an entity, which is termed a transaction.

To debug an issue with rule processing, you can analyze the complete rule trace of a transaction or focus on a particular cycle that seems interesting with regard to problem solving.

**Properties in rule tracing**
Whether a rule applies and executes a particular action, for example, a Block action that blocks a request for web access, depends on the rule criteria, which contains properties that are set to particular values during the processing.

For example, the `Antimalware.Infected` property, which is contained in the rule criteria of a default anti-malware rule, is set to `true` when a scanned web object has been found to be infected by viruses or other malware. Then the criteria of this rule matches, and a Block action is executed.

When analyzing a rule trace, it can be useful to look at the properties that were involved in rule processing and the values they were set to. Therefore, properties and their values can also be viewed separately.

**Deleting and restoring rule traces**
Rule traces can be removed from the panes of the rule tracing page, but not deleted on that page.

To delete rule traces, you need to access the Rule tracing files section, which is provided for every individual appliance under the Troubleshooting top-level menu.
In this section, you can also restore traces to the rule tracing panes that you have previously removed.

Up to 5000 traces can be stored on an appliance. When this number is exceeded, the oldest traces are deleted.

The deletion is not reflected on the rule tracing panes, so you might see entries for traces that you cannot access because the traces have already been deleted.

**Debug rule processing issues using rule tracing**

Use the options of the rule tracing panes to create rule traces and review them to debug issues with rule processing.

**Task**

1. Select Troubleshooting.

2. On the troubleshooting tree, select Rule Tracing Central.

   The rule tracing panes appear.

3. Work with the rule tracing panes to debug rule processing issues.

**Rule tracing panes**

The rule tracing panes allow you to create, review, and manage rule traces.
The following table describes the main functions of the rule tracing panes.

**Table 18-1  Main functions of the rule tracing panes**

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traces pane</td>
<td>Allows you to create and manage rule traces.</td>
</tr>
<tr>
<td>Rules pane</td>
<td>Allows you to view the rules that were processed.</td>
</tr>
<tr>
<td>Details pane</td>
<td>Allows you to view details with regard to properties used in rule criteria.</td>
</tr>
</tbody>
</table>

You can expand and hide panes by clicking the small black triangles between them.

**Traces pane**

The traces pane provides the following options.

**Table 18-2  Traces pane**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Appliance names list</strong></td>
<td>Lets you select a Web Gateway appliance within your network that you want to import rule traces from or create, review, and manage rule traces on.</td>
</tr>
<tr>
<td><strong>Import</strong></td>
<td>Opens a menu for importing rule traces.</td>
</tr>
<tr>
<td>• <strong>Import from appliance directory</strong></td>
<td>Lets you import all rule traces that are recorded on the appliance you selected from the list.</td>
</tr>
<tr>
<td>• <strong>Import from local directory</strong></td>
<td>Opens the local file manager to let you import the rule traces that are recorded on the appliance you are currently logged on to.</td>
</tr>
<tr>
<td><strong>Client IP address field</strong></td>
<td>Lets you enter the IP address of the client that is the source of the requests rule processing is traced for.</td>
</tr>
<tr>
<td><strong>Go / Stop icon (cross)</strong></td>
<td>Starts or stops the creation of rule traces.</td>
</tr>
<tr>
<td>• <strong>Go</strong></td>
<td>Starts the creation of rule traces for the latest requests received from the client specified by the address in the client IP address field.</td>
</tr>
<tr>
<td>• <strong>Stop icon</strong></td>
<td>Stops the creation of rule traces.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Lets you select the source of rule traces that entries should be shown for on the traces pane.</td>
</tr>
<tr>
<td>Clicking the button displays a list of the zipped rule tracing files that you have imported.</td>
<td></td>
</tr>
<tr>
<td>After selecting a file, entries for the rule traces contained in the file appear on the traces pane. The button then shows the name of the selected file.</td>
<td></td>
</tr>
<tr>
<td>If you do not select a file, entries for the rule traces that were created in the latest tracing are shown.</td>
<td></td>
</tr>
</tbody>
</table>
**Table 18-2  Traces pane (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action icons bar</strong></td>
<td>When clicked, provides a menu of the actions that can be executed by rules.</td>
</tr>
<tr>
<td></td>
<td>Selecting an action filters the rule traces accordingly.</td>
</tr>
<tr>
<td></td>
<td>For example, if you select the Block action, only entries for rule traces are shown that recorded an execution of this action.</td>
</tr>
<tr>
<td></td>
<td>You can select any combination of actions and also view the entries for all rule traces, regardless of a particular action.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Show all</strong> — Selects all actions and lets rule traces be shown for them.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Invert selection</strong> — Lets rule traces be shown for all actions that are not selected.</td>
</tr>
<tr>
<td></td>
<td>Subsequently, these actions appear in the menu as selected.</td>
</tr>
<tr>
<td><strong>Time or URL filtering field</strong></td>
<td>Lets you enter a time or URL for filtering traces.</td>
</tr>
<tr>
<td></td>
<td>Clicking the icon (cross) at the right end of the field clears the filter.</td>
</tr>
<tr>
<td><strong>Export</strong></td>
<td>Opens a menu for exporting rule traces.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Export visible traces</strong> — Opens the local file manager to let you export the rule traces that entries are currently shown for on the traces pane.</td>
</tr>
<tr>
<td></td>
<td>The rule traces are stored in a zipped file for exporting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Export selected traces</strong> — Opens the local file manager to let you export the currently selected rule traces.</td>
</tr>
<tr>
<td></td>
<td>Rule traces are stored in a zipped file for exporting.</td>
</tr>
</tbody>
</table>
Table 18-2  Traces pane (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>Opens a menu for clearing rule traces from the traces pane.</td>
</tr>
<tr>
<td></td>
<td>• Clear visible traces — Clears the rule traces that entries are currently shown for on the traces pane.</td>
</tr>
<tr>
<td></td>
<td>• Clear selected traces — Clears the rule traces that are currently selected on the rule tracing pane.</td>
</tr>
<tr>
<td></td>
<td>• Clear all — Clears all rule traces from the rule tracing pane.</td>
</tr>
</tbody>
</table>

Clearing traces from the traces pane does not delete them. You can delete rule traces in the Rule tracing files section, which is accessible from the Troubleshooting top-level menu.

Traces field
Shows entries for individual rule traces, depending on the specified filtering information.
When you select a trace, the rule that contains the most impacting action is shown with neighboring rules in the cycles pane and with its criteria, action, and events in the details pane.
Impact is attributed to actions in the following order:
Block (greatest impact) — Redirect — Authenticate — Remove — Stop Cycle — Stop Rule Set — Continue
However, a Stop Cycle, Stop Rule Set, and Continue action is only attributed impact if it was the last action in a cycle before rule processing stopped.
The following is provided for each trace:
• Action icon — Icon for the last action that was executed when rule processing was performed for a request
  The meanings of the icons can be viewed in the menu that appears when clicking the action icons bar.
• Time — Time when a trace was created on a particular day
• URL — URL sent with the request that a trace was created for

Rules pane
The rules pane provides the following options.

Table 18-3  Rules pane

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracing information field</td>
<td>Provides information about a selected trace.</td>
</tr>
<tr>
<td></td>
<td>The following is shown for a selected trace:</td>
</tr>
<tr>
<td></td>
<td>• URL sent with the request that the trace was created for</td>
</tr>
<tr>
<td></td>
<td>• Time stamp indicating the time when the trace was created</td>
</tr>
<tr>
<td></td>
<td>• Name of the file that stores the rule trace</td>
</tr>
<tr>
<td>Cycle</td>
<td>Lets you select a cycle to display information recorded in a trace about the rule processing that was performed in this cycle.</td>
</tr>
<tr>
<td></td>
<td>If you select All, summarized information is displayed about the processing in all cycles that were recorded in a trace.</td>
</tr>
</tbody>
</table>
### Table 18-3 Rules pane *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search</strong></td>
<td>Lets you type a term that is searched for within the information provided on rule sets and rules.</td>
</tr>
<tr>
<td></td>
<td>A match can be found:</td>
</tr>
<tr>
<td></td>
<td>• In the name of rule set or rule</td>
</tr>
<tr>
<td></td>
<td>• In the name of a property, action, or event</td>
</tr>
<tr>
<td></td>
<td>• In a list name</td>
</tr>
<tr>
<td></td>
<td>• In the value of a property</td>
</tr>
<tr>
<td></td>
<td>• In a constant value</td>
</tr>
<tr>
<td></td>
<td>• In other text portions that appear on the user interface</td>
</tr>
<tr>
<td></td>
<td>The first match is highlighted. Using the arrows next to the search field, you can navigate to the next or previous matches.</td>
</tr>
<tr>
<td></td>
<td>After selecting a new rule set or rule, the first match is again highlighted.</td>
</tr>
</tbody>
</table>

**Rule sets and rules field**

Shows the rule sets and rules that were executed when rule processing was performed in the selected cycle. For each rule set and rule, the information listed below is provided in the rules pane. More information can be viewed in the details pane after selecting a rule set or rule.

- **Cycle** — Cycle in which a rule set or rule was processed
  - Request and response cycles are represented by arrows in different colors
  - The meanings of these arrows are as follows:
    - *Arrow pointing to the right* — Request cycle
    - *Arrow pointing to the left* — Response cycle
    - *No arrow pointing to the right (left)* — No processing in the request (response) cycle
    - *Hollow arrow* — Rule set or rule processed, but no action executed (criteria did not match)
    - *Gray arrow* — Action executed, but not as the most impacting action in the rule trace
    - *Green arrow* — Stop Rule Set, Stop Cycle, or Continue executed as the most impacting action in the rule trace
Table 18-3 Rules pane (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An action of this type can only be the most impacting action if it was the last action in a cycle before processing stopped.</td>
</tr>
<tr>
<td></td>
<td>• Yellow arrow — Remove executed as the most impacting action</td>
</tr>
<tr>
<td></td>
<td>• Blue arrow — Authenticate executed as the most impacting action</td>
</tr>
<tr>
<td></td>
<td>• Dark green arrow — Redirect executed as the most impacting action</td>
</tr>
<tr>
<td></td>
<td>• Red arrow — Block executed as the most impacting action</td>
</tr>
<tr>
<td></td>
<td>If a rule set or rule was also processed in an embedded objects cycle, this is indicated by a small box with a number inside.</td>
</tr>
<tr>
<td></td>
<td>The box appears in the same line as the arrows for a rule set or rule. The box can be filled with a color that corresponds to the colors of the arrows.</td>
</tr>
<tr>
<td></td>
<td>Accordingly, the meanings that a box with a number can have are as follows:</td>
</tr>
<tr>
<td></td>
<td>• No box in the line for a rule set or rule — Rule set or rule not processed in an embedded objects cycle</td>
</tr>
<tr>
<td></td>
<td>• Box with number in the line for a rule set or rule — Rule set or rule processed in as many embedded object cycles as is shown by the number</td>
</tr>
<tr>
<td></td>
<td>• Hollow box not colored — Rule set or rule processed in an embedded cycle, but no action executed during this cycle (criteria did not match)</td>
</tr>
<tr>
<td></td>
<td>• Gray box — Action executed during an embedded objects cycle, but not as the most impacting action in the rule trace</td>
</tr>
<tr>
<td></td>
<td>• Green box — Stop Rule Set, Stop Cycle, or Continue executed during an embedded objects cycle as the most impacting action in the rule trace</td>
</tr>
<tr>
<td></td>
<td>An action of this type can only be the most impacting action if it was the last action in a cycle before processing stopped.</td>
</tr>
<tr>
<td></td>
<td>• Yellow box — Remove executed as the most impacting action during an embedded objects cycle</td>
</tr>
<tr>
<td></td>
<td>• Blue box — Authenticate executed as the most impacting action during an embedded objects cycle</td>
</tr>
<tr>
<td></td>
<td>• Dark green box — Redirect executed as the most impacting action during an embedded objects cycle</td>
</tr>
<tr>
<td></td>
<td>• Red box — Block executed as the most impacting action during an embedded objects cycle</td>
</tr>
<tr>
<td></td>
<td>• Name — Name of a rule set or rule</td>
</tr>
<tr>
<td></td>
<td>If a rule set or rule uses a list in its criteria, the criteria is shown below the name. The link to the list is then provided in the details pane.</td>
</tr>
</tbody>
</table>

Details pane

The details pane provides the following options.
**Table 18-4  Details pane**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Top Properties tab** | Displays a list of connection-related properties that are used by the rules of the currently selected rule trace and processing cycle. For each property, the following information is provided:  
  • Property — Name of the property  
  • Value — Value of the property at the time when a trace was created  
  Â few properties are always recorded by rule tracing and on shown this tab, as they are always processed. Others are only recorded and shown if they have been processed.  
  • URL — Always  
  • Client.IP — Always  
  • URL.Host — Always  
  • Authentication.Username — Only if processed  
  • Authentication.Usergroups — Only if processed  
  • URL.Categories — Only if processed  
  • Response.StatusCode — Only if processed  
  • Block.Reason — Only if processed  
  • Command.Name — Only if processed |
| **Details tab**    | Shows the criteria of the rule set or rule that is currently selected in the rules pane. The criteria is shown with the value its property was set to in the processing cycle that is currently selected in the rules pane. If All is selected in the rules pane, criteria is shown for every cycle in which processing was performed. For each criteria, the following information is provided:  
  • Cycle — Cycle in which the rule with the displayed criteria was processed and name of the rule  
  • Criteria — Criteria of the rule  
  If the criteria has matched, it is preceded by a marker icon (hook).  
  • Evaluated — Property of the criteria  
  If the criteria contains a list, the list name is repeated below the property name and a link to the list is provided under Value.  
  • Value — Value for the property at the time when a trace was created  
  The value depends on the property type. For example, a Boolean property has true or false as its values, a String property has a string, a Number property a number, and so on. If the criteria contains a list, a link to the list is provided. |
Use rule tracing to find out why a request was blocked

When a request for web access that a user sent from a client of Web Gateway has been blocked, you can use rule tracing to find the rule that blocked the request and the reason why it was done.

This is a sample procedure that describes one of several ways to use rule tracing for recording and analyzing rule processing on Web Gateway.

Task

1. Select Troubleshooting and on the appliances tree, select Rule Tracing Central.

   The rule tracing panes appear.

2. Create rule traces.

   a. In the traces pane, leave the name of the current appliance, which appears in the appliances names field.

      In this sample procedure, you will perform rule tracing for requests that were processed on this appliance.

   b. In the client IP address field, enter the IP address of the client that sent the request you want to do rule tracing for.

   c. Click Go.

      Rule traces for the latest requests received from the client are created. When trace creation is completed, entries for the traces appear in the traces field.

3. Filter the rule traces.

   a. In the time and URL filtering field, enter the URL that was sent with the blocked request.

      The rule traces are filtered to show only entries for traces that were performed for requests to access a web object with this URL.

      Let us assume that a request with this URL was only submitted once by the client in question. This would mean only one entry is shown as the filtering result.

   b. Select the entry.

      Detailed information from the trace that recorded rule processing for the request with this URL is shown in the rules and details panes.
4 Review a rule trace.
   a Review the tracing information in the rules pane.
      The rules that were processed to deal with the request are shown with their rule sets.
      The rule that blocked the request is selected and marked by a red arrow. If the arrow points to
      the right, the rule blocked the request in the request cycle. If the arrow points to the left, it was
      in the response cycle.
   b Review the tracing information in the details pane.
      • The cycle in which the rule blocked the request, the name of the rule, its criteria, action, and
        event are shown.
      The criteria is marked with a grey hook, which means it has matched.
      • Under Evaluat in the field below the criteria with the hook, the criteria is repeated.
        Under Value in the same field the value is shown that the property had at the time when the
        criteria matched and the rule blocked the request.

Let us assume that, for example, the details pane shows the following details for the rule that
blocked the request.

- Cycle — Response
- Rule name — Block if virus was found
- Criteria — Antimalware.Infected<Gateway Anti.Malware> equals true
- Evaluat — Antimalware.Infected equals true, Value — true
- Action — Block<Virus found>
- Event — Statistics.Counter.Increment<Default>("BlockedByAntiMalware", 1>

This means that rule tracing showed the request was blocked because the requested object had been
found to be infected by a virus or other malware.

The blocking action was performed by a virus and malware filtering rule, which was processed in the
response cycle when the object was received from a particular web server in response to the request.

The criteria of this rule included the Antimalware.Infected property. To find out what this property
must be set to, the Anti-Malware engine on Web Gateway was called. It scanned the requested web
object and detected an infection, so the property could be set to true and the rule criteria matched.

**Best practices - Find out why a web page displays no images**

Use rule tracing to find out why a requested web page appears on a client system, but with text only
and without displaying any images.

Imagine a sample issue, where a user requests access to the CNN channel homepage from a browser
on a client of Web Gateway. The page appears, but displays only text.

You can use rule tracing to see whether a CNN server that provides the images on the homepage
might have been blocked and why this happened.

**Task**
1 On the user interface of Web Gateway, select Troubleshooting.

If you are using several Web Gateway appliances in a Central Management configuration, make
sure you are logged on to the appliance that the client in question is connected to.
2 On the troubleshooting tree, select Rule Tracing Central.

3 Create a trace.
   a In the input field on the top left, type the IP address of the client system that had a request blocked, then click Go on the toggle button next to the input field.

   Requests for web access sent from the client are now traced and entries for trace files are displayed in the output field on the lower left.

   The Go on the toggle button turns into a cross to let you stop the process when no more tracing is needed.

   b On the client system, refresh the browser or click or enter ccn.com again to reproduce the issue.

   Trace file entries appear in the output field on Web Gateway.

   ![Information](Depending on the amount of data that is being transferred, it can take a while until the trace file entries appear.)

   c When you have reproduced the issue and the trace file entries have appeared, click the toggle button again to stop the tracing.

4 Review the trace file entries.
   For every request that has been traced, a time stamp and the requested URL are shown.

   At the beginning of an entry, a symbol for the most impacting action that was executed when processing the request is also shown. The most impacting of all actions is the Block action.

   When reviewing the trace file entries, you will see several entries with the blocking symbol and a URL beginning with cdn.turner.com/ccn. These are probably trace files for requests to access the CCN server that provides the images.

5 Select a trace file entry with cdn.turner.com/ccn.
   Information on this trace appears in the rules and details panes on the right.

6 Review the rules pane.
   The pane shows the rules that were processed for the request that was traced. The view stops at the last rule that applied before rule processing stopped. The rule is highlighted.

   This way you can see that Block URLs whose category is in Category Block List is the last rule that applied.

7 Review the details pane.
   On the two tabs of the details pane, more tracing information is shown.

   On the Top Properties tab, you will see, among other information, that the URL.Categories property had the value Business when the rule mentioned above was processed.

   This completes your rule tracing activities for this issue. Images from the CNN server were not displayed because the URLs that were submitted for accessing this server have fallen into the Business category and this category is on a blocklist.

   If you want to see the images displayed, you need to reconfigure the web security policy for your network and put, for example, cdn.turner.com/ccn/* on a URL whitelist.
Restore removed rule traces to the rule tracing panes

To restore rule traces that you have removed from the rule tracing panes, supply them from the rule traces directory of an appliance or import them in a source file.

How removed rule traces can be restored to the rule tracing panes depends on whether they were created on the appliance you are currently logged on to or were imported to this appliance.

Accordingly, you can supply them from the rule traces directory of the appliance or repeat the import of the source file.

Tasks

• Restore removed rule traces from an appliance directory on page 638
  When rule traces that you have removed from the rule tracing panes had been created on the current appliance, you can restore them from the directory of rule tracing files on that appliance.

• Restore removed rule traces by importing a source file on page 638
  When rule traces that you have removed from the rule tracing panes had previously been imported, you can restore them by importing the source file once again.

Restore removed rule traces from an appliance directory

When rule traces that you have removed from the rule tracing panes had been created on the current appliance, you can restore them from the directory of rule tracing files on that appliance.

Task

1. Select Troubleshooting.
2. On the troubleshooting tree, expand the appliance you want to restore rule traces on.
3. Select Rule tracing files.
   The directory of the rule tracing files appears on the right side of the troubleshooting page.
4. Under Trace files, select the rule tracing files you want to restore.
5. Click Analyze.

The rule traces are accessible again in the rule tracing panes.

Restore removed rule traces by importing a source file

When rule traces that you have removed from the rule tracing panes had previously been imported, you can restore them by importing the source file once again.

Task

1. Select Troubleshooting.
2. On the troubleshooting tree, select Rule Tracing Central.
3. Click Traces and then Import.
   The local file manager opens.
4. Browse to the location where you stored the zipped file that is the source for the rule traces you want to restore, select the file, and import it.

The rule traces are accessible again on the rule tracing panes.
Delete rule traces
To delete rule traces, access the directory of rule tracing files on an appliance and use the delete option that is provided.

**Task**
1. Select Troubleshooting.
2. On the troubleshooting tree, select the appliance you want to delete rule traces on, then click Rule tracing files.
   - The directory of rule tracing files appears on the right side of the troubleshooting page.
3. Under Trace files, select the rule tracing files you want to delete and click Delete.
4. In the window that opens, confirm the deletion.

Create a feedback file
You can create a feedback file to backtrace processes after the failure of a function.

**Task**
1. Select the Troubleshooting top-level menu.
2. On the appliances tree, select the appliance you want to backtrace processes on and click Feedback.
3. Select or deselect Pause running McAfee Web Gateway to create a backtrace as needed.
   - We recommend that you select the checkbox.
4. Click Create Feedback File.
   - A feedback file is created and appears with its name, size, and date in the list under Feedback file.
   - Using the items on the toolbar, you can perform several file-related activities, such as view or download a file.

Enable the creation of core files
You can enable the creation of core files to record memory content after the failure of a function has caused an appliance to terminate operation.

**Task**
1. Select Configuration | Appliances.
2. On the appliances tree, select the appliance you want to record memory content on and click Troubleshooting.
3. In the Troubleshooting section, select Enable core file creation.
4. Click Save Changes.
   - Core files are now created whenever the appliance terminates due to the failure of a particular function.
You can view the core files, after selecting the appliance under the **Troubleshooting** top-level menu and clicking **Core Files**. The files are then displayed in a list.

Using the items on the toolbar, you can perform several file-related activities, such as view or download a file.

---

### Enable the creation of connection tracing files

You can enable the creation of trace files to record activities occurring on connections between an appliance and other network components.

**Task**

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to record connection activities on and click **Troubleshooting**.
3. In the **Troubleshooting** section, select **Enable connection tracing**.
4. [Optional] To trace only activities on a connection to a particular client of the appliance, select **Restrict tracing to only one IP** and type the IP address of the client in the **Client IP** field.
5. Click **Save Changes**.

Connection tracing files are now created.

You can view the connection tracing files, after selecting the appliance under the **Troubleshooting** top-level menu and clicking **Connection Tracing**. The files are then displayed in a list.

Using the items on the toolbar, you can perform several file-related activities, such as view or download a file.

---

### Create a packet tracing file

You can create a packet tracing file to record the network activities of an appliance.

**Task**

1. Select the **Troubleshooting** top-level menu.
2. On the appliances tree, select the appliance you want to record network activities on and click **Packet tracing**.
3. In the **Command line parameters** field, type parameters for the packet tracing as needed.
4. Click **tcpdump start**.

A packet tracing file is generated and appears with its name, size, and date in the list under **Results (dump)**.

To stop the ongoing generation of a packet tracing file, click **tcpdump stop**.

Using the items on the toolbar of the list, you can perform several file-related activities, such as view or download a file.
Work with system and network tools

You can work with several system and network tools to troubleshoot problems on an appliance.

Task

1. Select the Troubleshooting top-level menu.

2. On the appliances tree, select the appliance you want to use a tool on and click System Tools or Network Tools.

   The available system tools are:
   - service restart
   - AV threads

   The available network tools are:
   - ping and ping6
   - nslookup
   - traceroute and traceroute6
   - ipneigh
   - ntp

3. In the Command line parameters field, type the parameters for a command that can be executed by a particular tool.
   
   For example, type the name of a host you want to connect to using the ping network tool.

4. Click the button for the tool that you want to use.

   The corresponding command is executed and the resulting output displayed under Results.

   The following could, for example, be displayed:

   Ping: Unknown host testhost

   To export the results to a location within your file system, click Export and specify the location in the window that opens.

See also

Restart a service of the operating system on page 641
Display running AV threads on page 642

Restart a service of the operating system

Using the restart tool, you can stop a service of the operating system that is currently running and restart it again. If a service is not running at the time when the tool is applied to it, the service is started.

You cannot restart the main mwg service and the sysconfd service, which is a daemon for implementing manual configuration changes, using this system tool.
**Task**
1. Select the **Troubleshooting** top-level menu.
2. On the appliances tree, select the appliance you want to start a service on and click **System Tools**.
3. In the **Command line parameters** field, type the service name and parameters as required.
4. Click **service restart**.

The service is restarted and the executed service activities are displayed in the **Results** field.

The following could, for example, be displayed after restarting the `ip6tables` service.

```
Flushing firewall rules: [OK]
Unloading ip6tables modules: [OK]
Applying ip6tables firewall rules: [OK]
```

To export the results to a location within your file system, click **Export** and specify the location in the window that opens.

**Display running AV threads**

You can display the threads that are currently running to perform anti-malware scanning activities. Seeing many threads lets you know that scanning a particular request or response is consuming a high amount of resources.

The list of threads that is shown includes the threads that actually perform scanning activities, as well as the threads that deliver requests and responses to the scanning modules. Both kinds of threads are referred to as anti-malware working threads or simply as **AV threads**.

**Task**
1. Select the **Troubleshooting** top-level menu.
2. On the troubleshooting tree, select **System Tools**, then click **AV threads**.

A list of the AV threads appears under **Results**.

For each thread, an ID number is shown, the time when the thread was started, its current status, and other information.

To export the thread list to a location within your file system, click **Export** and specify the location in the window that opens.

**Back up and restore an appliance configuration**

You can store an appliance configuration in a backup file and use this file to restore the appliance configuration.

When backing up the appliance configuration, you have the option of including the SSO credentials in the credential store in the backup file. Likewise, when restoring, you have the option of restoring the SSO credentials from the backup file to the credential store.
When restoring a backup, you have the option of restoring all configurations and accounts or only the data configured under the Policy top-level menu, which includes data on rules, lists, and settings.

Make sure the UTF-8 character format is used on your administration system for Web Gateway if you want to insert special characters, for example, German umlaut (ä, ö, ü), in the passwords that are required for encrypting and decrypting a backup.

**Task**

1. On the dashboard, select **Troubleshooting**.

2. On the appliances tree, select the appliance whose configuration you want to back up or restore, then click **Backup/Restore**.

3. To back up the appliance configuration:
   a. To include SSO credentials in the backup, select the **SSO Credentials** check box.
   b. Click **Back up to file**.
   c. In your local file manager, create or select the backup file.

4. To restore the appliance configuration:
   a. To include all configurations and accounts in the restore, select the **Configurations and Accounts** check box.
   b. To include SSO credentials in the restore, select the **SSO Credentials** check box.
   c. Click **Restore from file**.
   d. Confirm the message stating that you will be logged off during the restore.
   e. In your local file manager, select the backup file to use for restoring the appliance configuration.

---

**Troubleshooting settings**

The **Troubleshooting** settings are system settings that are used for configuring the troubleshooting functions on an appliance.

**Troubleshooting**

Settings for general troubleshooting functions

<table>
<thead>
<tr>
<th>Table 18-5  Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td>Enable core file generation</td>
</tr>
<tr>
<td>Enable connection tracing</td>
</tr>
<tr>
<td>Restrict connection tracing to one IP</td>
</tr>
<tr>
<td>Client IP</td>
</tr>
<tr>
<td>Reduce connection trace size</td>
</tr>
<tr>
<td>Content bytes included for each send and receive operation</td>
</tr>
</tbody>
</table>
Table 18-5  Troubleshooting (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable tracing for Coordinator (e.g. Central Management)</td>
<td>When selected, tracing is enabled for activities that are performed by the Coordinator subsystem on Web Gateway, for example, activities that are related to Central Management.</td>
</tr>
<tr>
<td>Write full message body into log</td>
<td>When selected, the complete body of a message is written into a log file.</td>
</tr>
<tr>
<td>Enable tracing for DXL</td>
<td>When selected, DXL messaging can be traced.</td>
</tr>
<tr>
<td>Write full message body into log</td>
<td>When selected, the complete body of a message is written into a log file.</td>
</tr>
</tbody>
</table>

Authentication Troubleshooting
Settings for authentication-related troubleshooting

Table 18-6  Authentication Troubleshooting

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log management events</td>
<td>When selected, management events are logged.</td>
</tr>
<tr>
<td>Log authentication events</td>
<td>When selected, authentication events are logged.</td>
</tr>
<tr>
<td>Restrict connection tracing to one IP</td>
<td>When selected, connection tracing is restricted to processing for requests that are sent from one particular client, which is identified by its IP address.</td>
</tr>
<tr>
<td>Client IP</td>
<td>IP address of the client that connection tracing is restricted to.</td>
</tr>
</tbody>
</table>

Quota Troubleshooting
Settings for troubleshooting that is related to quota restrictions

Table 18-7  Quota Troubleshooting

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log quota events</td>
<td>When selected, quota events are logged.</td>
</tr>
</tbody>
</table>

PDStorage Troubleshooting
Settings for troubleshooting that is related to the PDStorage function

Table 18-8  PDStorage Troubleshooting

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log PDStorage events</td>
<td>When selected, PDStorage events are logged.</td>
</tr>
</tbody>
</table>

SAML Processing Troubleshooting
Settings for troubleshooting that is related to the SAML processing

Table 18-9  SAML Processing Troubleshooting

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable logging</td>
<td>When selected, SAML processing events are logged.</td>
</tr>
</tbody>
</table>
Configuration lists

The following lists describe items you can use to configure web security rules.

Contents
- List of actions
- List of block reason IDs
- List of error IDs
- List of events
- List of incident IDs
- List of properties
- Wildcard expressions

List of actions

The following table provides a list of the actions you can use in rules. The actions are listed in alphabetical order.

Table A-1  List of actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>Stops processing the rules in the current cycle. Sends an authentication request to the client of the user who requested access to a web object. Continues processing with the next cycle.</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks access to a requested web object. Stops processing rules. Continues when the next request is received on the appliance.</td>
</tr>
<tr>
<td>Continue</td>
<td>Continues processing with the next rule.</td>
</tr>
<tr>
<td>Redirect</td>
<td>Redirects a client that requested access to a web object to another object.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes a requested web object. Stops processing the rules in the current cycle. Continues processing with the next cycle.</td>
</tr>
</tbody>
</table>
Table A-1  List of actions (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop Cycle</td>
<td>Stops processing the rules in the current cycle.</td>
</tr>
<tr>
<td></td>
<td>Does not block access to a requested web object.</td>
</tr>
<tr>
<td></td>
<td>Continues processing with the next cycle.</td>
</tr>
<tr>
<td>Stop Rule Set</td>
<td>Stops processing the rules of the current rule set.</td>
</tr>
<tr>
<td></td>
<td>Continues processing with the next rule set.</td>
</tr>
</tbody>
</table>

List of block reason IDs

The following table provides a list of block reason IDs with descriptions of their meanings.

You can configure block reason IDs in user message templates to provide a value that identifies a block reason for logging by McAfee® Web Reporter.

Table A-2  List of block reason IDs

<table>
<thead>
<tr>
<th>Block reason ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Allowed</td>
</tr>
<tr>
<td>1</td>
<td>Internal error</td>
</tr>
<tr>
<td>2</td>
<td>Default message template being used for an action</td>
</tr>
<tr>
<td>3</td>
<td>Internal URL filter error</td>
</tr>
<tr>
<td>10</td>
<td>Blocked due to an entry in the URL filter database</td>
</tr>
<tr>
<td>14</td>
<td>Blocked according to URL filtering by expression</td>
</tr>
<tr>
<td>15</td>
<td>Blocked by the Real-Time Classifier</td>
</tr>
<tr>
<td>20</td>
<td>Blocked due to lack of content type</td>
</tr>
<tr>
<td>22</td>
<td>Blocked due to the media type</td>
</tr>
<tr>
<td>30</td>
<td>Blocked due to a multi-part archive having been found</td>
</tr>
<tr>
<td>35</td>
<td>Blocked due to an archive not handled by the Archive Handler</td>
</tr>
<tr>
<td>80</td>
<td>Blocked due to a virus having been found</td>
</tr>
<tr>
<td>81</td>
<td>Blocked due to unauthorized access</td>
</tr>
<tr>
<td>82</td>
<td>Blocked due to a bad request</td>
</tr>
<tr>
<td>85</td>
<td>Blocked due to an internal anti-malware error</td>
</tr>
<tr>
<td>92</td>
<td>Blocked due to expiration of a certificate</td>
</tr>
<tr>
<td>93</td>
<td>Blocked due to a revoked certificate</td>
</tr>
<tr>
<td>94</td>
<td>Blocked due to a forbidden certificate authority (CA)</td>
</tr>
<tr>
<td>95</td>
<td>Blocked due to an unknown certificate authority (CA)</td>
</tr>
<tr>
<td>97</td>
<td>Blocked due to a self-signed certificate</td>
</tr>
<tr>
<td>98</td>
<td>Blocked due to a common name mismatch</td>
</tr>
<tr>
<td>102</td>
<td>Blocked due to an unspecified certificate incident</td>
</tr>
<tr>
<td>103</td>
<td>Blocked due to CONNECT not allowed</td>
</tr>
<tr>
<td>104</td>
<td>Blocked due to the reverse proxy destination not being allowed</td>
</tr>
<tr>
<td>140</td>
<td>Blocked due to an internal DLP filter error</td>
</tr>
</tbody>
</table>
Table A-2 List of block reason IDs (continued)

<table>
<thead>
<tr>
<th>Block reason ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>150</td>
<td>Blocked due to an internal Application Control filter error</td>
</tr>
<tr>
<td>151</td>
<td>Blocked due to a request belonging to an application that is not allowed</td>
</tr>
<tr>
<td>160</td>
<td>Blocked due to missing policy for Web Hybrid</td>
</tr>
<tr>
<td>161</td>
<td>Blocked due to web access not being allowed by Web Hybrid</td>
</tr>
<tr>
<td>162</td>
<td>Blocked due to URL filtering by Web Hybrid</td>
</tr>
<tr>
<td>200</td>
<td>Blocked due to the coaching session of a user having been exceeded</td>
</tr>
<tr>
<td>201</td>
<td>Blocked due to the time quota session of a user having been exceeded</td>
</tr>
<tr>
<td>202</td>
<td>Blocked due to the time quota for a user having been exceeded</td>
</tr>
<tr>
<td>203</td>
<td>Blocked due to the volume quota session of a user having been exceeded</td>
</tr>
<tr>
<td>204</td>
<td>Blocked due to the volume quota for a user having been exceeded</td>
</tr>
<tr>
<td>205</td>
<td>Blocked due to the authorized override session of a user having been exceeded</td>
</tr>
<tr>
<td>206</td>
<td>Blocked due to the blocking session of a user being active</td>
</tr>
<tr>
<td>300</td>
<td>Blocked due to a quota redirect</td>
</tr>
<tr>
<td>301</td>
<td>Blocked due to an authentication redirect</td>
</tr>
<tr>
<td>400</td>
<td>Blocked due to an authorized override redirect</td>
</tr>
</tbody>
</table>

List of error IDs

The following table provides a list of the error IDs you can use in rules.

The error IDs are grouped in numerical ranges as follows.

10000–10049 Incorrect usage of properties or events
10050–10099 Errors of the rule processing module
10100–10199 General errors
11000–11999 License Manager errors
12000–12999 Errors related to the appliance system
13000–13999 Persistent Database (PDStore) errors
14000–14999 Virus and malware filtering errors
15000–15999 URL filtering errors
16000–16999 ICAP client errors
20000–21000 Proxy module errors
25000–25999 External lists errors
26000–26999 Data loss prevention (DLP) errors
32000–32999 Cloud storage encryption errors
34000–34999 Single sign-on errors
35000–35999 DXL errors
### Table A-3 List of error IDs

<table>
<thead>
<tr>
<th>Error ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000</td>
<td>WrongPropParams</td>
<td>$onPosition$: Wrong parameters or types for property $propName$.</td>
</tr>
<tr>
<td>10001</td>
<td>UnknownProperty</td>
<td>$onPosition$: Error in rule '$ruleName$': Property dispatcher does not know property $propName$.</td>
</tr>
<tr>
<td>10002</td>
<td>NoPropParam</td>
<td>$onPosition$: No parameter for property $propName$ given.</td>
</tr>
<tr>
<td>10003</td>
<td>WrongThirdPropParam</td>
<td>$onPosition$: Wrong type of third parameter for property $propName$.</td>
</tr>
<tr>
<td>10004</td>
<td>InvalidPropertyParameter</td>
<td>$onPosition$: Parameters for property $propName$ are invalid, reason: $reason$.</td>
</tr>
<tr>
<td>10005</td>
<td>InvalidPropertyParameter2</td>
<td>Parameters are invalid. Reason: $reason$.</td>
</tr>
<tr>
<td>10005</td>
<td>UnknownProperty2</td>
<td>$onPosition$: Unknown property $propName$.</td>
</tr>
<tr>
<td>10050</td>
<td>WrongOperator</td>
<td>$onPosition$: Error in rule '$ruleName$': wrong operator '$operator$' used on left hand side type $typeLeft$ and right hand side type $typeRight$.</td>
</tr>
<tr>
<td>10051</td>
<td>WrongOperatorNoNames</td>
<td>$onPosition$: $action$ failed. Type of $property$ is $typeName$, but it has to be $formatType$.</td>
</tr>
<tr>
<td>10052</td>
<td>FormatError</td>
<td>$onPosition$: User-defined property '$propName$' could not be found. Reason: it was not yet set (not initialized).</td>
</tr>
<tr>
<td>10053</td>
<td>UserDefinedPropertyNotFound</td>
<td>$onPosition$: User-defined property '$propName$' could not be found. Reason: it was not yet set (not initialized).</td>
</tr>
<tr>
<td>10054</td>
<td>PropertyNotFound</td>
<td>$onPosition$: Property '$propName$' could not be found. Reason: it was not yet set (not initialized).</td>
</tr>
<tr>
<td>10055</td>
<td>NeedMoreDataOnLastCall</td>
<td>On computing property '$propName$' the filter returned 'NeedMoreData' though there is no more data.</td>
</tr>
<tr>
<td>10056</td>
<td>WrongPropState</td>
<td>$onPosition$: State of Property $propName$ is $propState$.</td>
</tr>
<tr>
<td>10057</td>
<td>ZombieRuleElemIsExecuted</td>
<td>$rule$ (name: '$name$', id: '$id$') could not be executed because it is a zombie. Reason: '$reason$'.</td>
</tr>
<tr>
<td>10058</td>
<td>SetPropertyFailed</td>
<td>$onPosition$: Error in Rule '$ruleName$': Event could not be evaluated. Reason: $reason$.</td>
</tr>
<tr>
<td>10059</td>
<td>EventError</td>
<td>$onPosition$: Error while $operation$ the $objName$. Reason: $reason$.</td>
</tr>
<tr>
<td>10100</td>
<td>ErrorDuringOperation</td>
<td>$onPosition$: Error while $operation$ the $objName$. Reason: $reason$.</td>
</tr>
<tr>
<td>11000</td>
<td>NoLicense</td>
<td>The requested functionality '$func$' is not covered by your license.</td>
</tr>
<tr>
<td>12000</td>
<td>CannotOpenPipe</td>
<td>Cannot open pipe.</td>
</tr>
<tr>
<td>12001</td>
<td>CannotOpenFile</td>
<td>Cannot open file '$name$' in mode '$mode$' with errno '$errno$'.</td>
</tr>
</tbody>
</table>
Table A-3  List of error IDs (continued)

<table>
<thead>
<tr>
<th>Error ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13000</td>
<td>NoUser</td>
<td>No user available.</td>
</tr>
<tr>
<td>14000</td>
<td>AVError</td>
<td>Error in AntivirusFilter: $reason$.</td>
</tr>
<tr>
<td>14001</td>
<td>AVScanFailedFull</td>
<td>Cannot call McAfee Gateway Anti-Malware engine. All connections in use.</td>
</tr>
<tr>
<td>14002</td>
<td>AVError</td>
<td>Internal error in Anti-Malware filter.</td>
</tr>
<tr>
<td>14003</td>
<td>AVError</td>
<td>Timeout occurred while filtering.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See also the note on error message 14002.</td>
</tr>
<tr>
<td>14004</td>
<td>AVError</td>
<td>Cannot filter because a special update is performed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See also the note on error message 14002.</td>
</tr>
<tr>
<td>14005</td>
<td>AVError</td>
<td>Scanning failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See also the note on error message 14002.</td>
</tr>
<tr>
<td>14010</td>
<td>ATDError</td>
<td>Communication failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication to a server that Advanced Threat Defense runs on failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This can be due to several reasons, including network problems (the server is offline, a request timed out), to an issue with the HTTP protocol, or an unexpected or malformed server reply.</td>
</tr>
<tr>
<td>14011</td>
<td>ATDError</td>
<td>Timeout occurred while filtering.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced Threat Defense took longer to scan a web object than is allowed according to the configured time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The time allowed by default is 10 minutes.</td>
</tr>
<tr>
<td>14012</td>
<td>ATDError</td>
<td>File cannot be scanned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced Threat Defense was not able to scan a web object.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In the scanning report that is returned by Advanced Threat Defense, the value for Severity is set to N/A.</td>
</tr>
<tr>
<td>15000</td>
<td>TSDatabaseExpired</td>
<td>Global Threat Intelligence system database expired error: Database is expired. <code>$desc$</code>.</td>
</tr>
</tbody>
</table>
### Table A-3  List of error IDs (continued)

<table>
<thead>
<tr>
<th>Error ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15001</td>
<td>TSInvalidURL</td>
<td>The URL '$url$' is invalid. In function $func$.</td>
</tr>
<tr>
<td>15002</td>
<td>TSBinaryNotProperlyLoaded</td>
<td>Binary could not be loaded from '$path$'. In function $func$.</td>
</tr>
<tr>
<td>15003</td>
<td>TSCommon</td>
<td>Global Threat Intelligence system error (code: $errorCode$). In function $func$.</td>
</tr>
<tr>
<td>15004</td>
<td>TSBinaryDoesNotExist</td>
<td>Global Threat Intelligence system library is not yet available. In function $func$.</td>
</tr>
<tr>
<td>15005</td>
<td>TSDatabaseNotProperlyLoaded</td>
<td>Database was not properly loaded. In function $func$.</td>
</tr>
<tr>
<td>15006</td>
<td>TSNoMem</td>
<td>Global Threat Intelligence system is out of memory. In function $func$.</td>
</tr>
<tr>
<td>15007</td>
<td>TSInsufficientSpace</td>
<td>Insufficient space in buffer for Global Threat Intelligence system. In function $func$.</td>
</tr>
<tr>
<td>15008</td>
<td>TSNetLookup</td>
<td>Global Threat Intelligence system net error (code: TS_NET_ERROR). In function $func$.</td>
</tr>
<tr>
<td>15009</td>
<td>TSCommonNetLookup</td>
<td>Global Threat Intelligence system net error (code: $errorCode$). In function $func$.</td>
</tr>
<tr>
<td>15010</td>
<td>TSPipe</td>
<td>Cannot open Global Threat Intelligence system pipe. In function $func$.</td>
</tr>
<tr>
<td>16000</td>
<td>NoICAPServerAvailable</td>
<td>No ICAP server available from list: $list$$.</td>
</tr>
<tr>
<td>16001</td>
<td>NoRespModPropInReqMod</td>
<td>Property $propName$ cannot be calculated in request cycle.</td>
</tr>
<tr>
<td>16002</td>
<td>ICAPBadResponse</td>
<td>ICAP client filter error: ICAP server sent bad response.</td>
</tr>
<tr>
<td>16003</td>
<td>ICAPMaxConnectionLimit</td>
<td>ICAP client filter error: Maximum number of connections reached.</td>
</tr>
<tr>
<td>16004</td>
<td>ICAPCannotConnectToServer</td>
<td>ICAP client filter error: Cannot connect to ICAP server.</td>
</tr>
<tr>
<td>16005</td>
<td>ICAPCommunicationFailure</td>
<td>ICAP client filter error: Failure in communication with ICAP server.</td>
</tr>
<tr>
<td>20000</td>
<td>CheckLongRunningConnection</td>
<td>A timeout occurred on a long-running connection.</td>
</tr>
<tr>
<td>20001</td>
<td>CheckSizeOfConnection</td>
<td>The maximum amount of data that can be sent on a long-running connection has been exceeded.</td>
</tr>
<tr>
<td>25000</td>
<td>Unknown error happened</td>
<td>An uncategorized error was encountered by the External Lists module.</td>
</tr>
<tr>
<td>25001</td>
<td>Error during data fetch</td>
<td>An uncategorized error was encountered by the External Lists module during the data fetch.</td>
</tr>
<tr>
<td>25002</td>
<td>Error during data conversion</td>
<td>An error occurred while external list data was converted.</td>
</tr>
<tr>
<td>25003</td>
<td>Too much data</td>
<td>The configured limit for the number of list entries that can be retrieved from an external source has been exceeded.</td>
</tr>
<tr>
<td>25004</td>
<td>Timeout during data fetch</td>
<td>The configured timeout for retrieving external list data has expired.</td>
</tr>
<tr>
<td>25005</td>
<td>Data access denied</td>
<td>The rights required for accessing a source of external list data have not been granted to the appliance.</td>
</tr>
</tbody>
</table>
### Table A-3  List of error IDs (continued)

<table>
<thead>
<tr>
<th>Error ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>25006</td>
<td>No such resource</td>
<td>A source of external list data, for example, a file or web server, could not be found.</td>
</tr>
<tr>
<td>26001</td>
<td>DLP engine not loaded</td>
<td>The DLP engine could not be loaded.</td>
</tr>
<tr>
<td>32002</td>
<td>Empty password is not allowed</td>
<td>An empty password was submitted, for example, when passwords were retrieved from an external data source.</td>
</tr>
<tr>
<td>32003</td>
<td>Invalid configuration for filter</td>
<td>The settings of the module for encryption and decryption are invalid. This error occurs very rarely.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It could be caused by a general issue with policy configuration on Web Gateway.</td>
</tr>
<tr>
<td>32004</td>
<td>Encryption failed: Unknown content type</td>
<td>Data could not be encrypted because it was of an unknown type. This could be caused by an invalid description for a cloud storage service.</td>
</tr>
<tr>
<td>32005</td>
<td>Encryption failed: Parsing of message body failed</td>
<td>The data sent in the body of an upload request is in multi-part/form data format. Parsing this type of data, which is required for encryption, is not supported on Web Gateway.</td>
</tr>
<tr>
<td>32006</td>
<td>Encryption failed: Fetching of file name failed</td>
<td>The name of a file containing data that should be encrypted could not be fetched.</td>
</tr>
<tr>
<td>32007</td>
<td>Encryption failed: Cipher NNNN is not supported</td>
<td>The cipher that is provided for encrypting data is invalid. This is very unlikely to happen, as the administrator selects the encryption cipher from a pre-configured list.</td>
</tr>
<tr>
<td>32008</td>
<td>Encryption failed: Generation of salt failed</td>
<td>The process of salt generation, which is required for encrypting data, could not be performed successfully. This is usually caused by an internal OpenSSL error.</td>
</tr>
<tr>
<td>32009</td>
<td>Encryption failed: Fetching of key failed</td>
<td>The key that is required for encrypting data could not be fetched.</td>
</tr>
<tr>
<td>32010</td>
<td>Encryption failed: Initialization of encryption failed</td>
<td>The encryption process could not be initialized.</td>
</tr>
<tr>
<td>32011</td>
<td>Encryption failed: Data encryption failed</td>
<td>An error occurred during the encryption process.</td>
</tr>
<tr>
<td>32012</td>
<td>Encryption failed: Finalization of decryption failed</td>
<td>The encryption process could not be completed.</td>
</tr>
<tr>
<td>32013</td>
<td>Encryption failed: Generic error</td>
<td>Other encryption-related error</td>
</tr>
<tr>
<td>32014</td>
<td>Encryption failed: Unknown content type</td>
<td>Data could not be decrypted because it was of an unknown type. This could be caused by an invalid description for a cloud storage service.</td>
</tr>
<tr>
<td>32015</td>
<td>Decryption failed: Multi-part message body is not supported</td>
<td>A cloud storage service sent data in the body of its response to a download request that is in multi-part/form data format. Decrypting this type of data is not supported on Web Gateway.</td>
</tr>
<tr>
<td>32016</td>
<td>Decryption failed: Cipher NNNN is not supported</td>
<td>The cipher that is provided for decrypting data is invalid. This is very unlikely to happen, as the administrator selects the decryption cipher from a pre-configured list.</td>
</tr>
<tr>
<td>32017</td>
<td>Decryption failed: Fetching of key failed</td>
<td>The key that is required for decrypting data could not be fetched.</td>
</tr>
<tr>
<td>32018</td>
<td>Decryption failed: Initialization of decryption failed</td>
<td>The decryption process could not be initialized.</td>
</tr>
</tbody>
</table>
Table A-3  List of error IDs (continued)

<table>
<thead>
<tr>
<th>Error ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32019</td>
<td>Decryption failed: Data decryption failed</td>
<td>An error occurred during the decryption process.</td>
</tr>
<tr>
<td>32020</td>
<td>Decryption failed: Finalization of decryption failed</td>
<td>The decryption process could not be completed.</td>
</tr>
<tr>
<td>32021</td>
<td>Decryption failed: Generic error</td>
<td>Other decryption-related error</td>
</tr>
<tr>
<td>34000</td>
<td>Generic SSO filter error</td>
<td>An error happened during the single sign-on process. Reason: 'General error...'</td>
</tr>
<tr>
<td>34001</td>
<td>Generic SSO filter error</td>
<td>A user tried to get single sign-on access using a non-existing cloud connector. Reason: 'No such connector'</td>
</tr>
<tr>
<td>34003</td>
<td>Generic SSO filter error</td>
<td>No cloud connector was configured for the single sign-on process. Reason: 'There is no connector catalog'</td>
</tr>
<tr>
<td>34004</td>
<td>SSO service mismatch error</td>
<td>The value for a token did not match the value that was stored in a cloud connector: Service mismatch. Token ID: ´$tokenid$`, Service ID: ´$serviceid$´.</td>
</tr>
<tr>
<td>34005</td>
<td>SSO service not enabled</td>
<td>A cloud application was not available for a user: Realm: ´$realm$´, user: ´$userid$´, service ID: ´$serviceid$´.</td>
</tr>
<tr>
<td>34006</td>
<td>SSO non-inline mode error</td>
<td>A cloud application was not available in the non-proxy (non-inline) mode of the single sign-on process: Service ID: ´$serviceid$´.</td>
</tr>
<tr>
<td>34050</td>
<td>Credential store generic error</td>
<td>See the error log for details.</td>
</tr>
<tr>
<td>34051</td>
<td>Credential store generic error</td>
<td>This request is not allowed for current user.</td>
</tr>
<tr>
<td>34052</td>
<td>Credential store generic error</td>
<td>The credential store request could not be created.</td>
</tr>
<tr>
<td>34060</td>
<td>Credential store server HTTP error</td>
<td>The credential store server responded to a request with an HTTP error. See the error log for details.</td>
</tr>
<tr>
<td>34070</td>
<td>Credential store server error</td>
<td>The credential store server responded with an error. See the error log for details. The log includes the error code returned by the credential store server.</td>
</tr>
<tr>
<td>34080</td>
<td>Credential store connection error</td>
<td>A credential store request failed because of a connection error. See the error log for details.</td>
</tr>
<tr>
<td>34090</td>
<td>Credential store request error</td>
<td>An internal error occurred while a credential store request was performed. See the error log for details.</td>
</tr>
<tr>
<td>35000</td>
<td>DXLNotAvailable</td>
<td>No DXL messages can currently be sent.</td>
</tr>
</tbody>
</table>

List of events

The following table provides a list of the events you can use in rules.

The events are listed in alphabetical order.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication.AddMethod</td>
<td>Adds an authentication method.</td>
<td>1 String: Name of an authentication method&lt;br&gt;2 String: Value for an authentication method&lt;br&gt;3 Boolean: If true, an existing method is overwritten.</td>
</tr>
<tr>
<td>Authentication.ClearCache</td>
<td>Clears the cache.</td>
<td></td>
</tr>
<tr>
<td>Authentication.ClearMethodList</td>
<td>Clears the authentication methods list.</td>
<td></td>
</tr>
<tr>
<td>Authentication.ClearNTMLCache</td>
<td>Clears the NTML cache.</td>
<td></td>
</tr>
<tr>
<td>Authentication.GenerateICEResponse</td>
<td>Generates a token that is sent in response to McAfee Cloud Identity Manager to enable seamless authentication.</td>
<td></td>
</tr>
<tr>
<td>Authentication.SendOTP</td>
<td>Sends a one-time password to an authenticated user.</td>
<td></td>
</tr>
<tr>
<td>BlockingSession.Activate</td>
<td>Activates a blocking session.</td>
<td></td>
</tr>
<tr>
<td>Body.Insert</td>
<td>Inserts a string into the body of the request or response that is currently processed.</td>
<td>1 Number: Byte position where insertion begins&lt;br&gt;2 String: Pattern&lt;br&gt;a. string embedded in double quotes (“ ...”, can also contain hex values preceded by \)&lt;br&gt;or:&lt;br&gt;b. sequence of hex values</td>
</tr>
<tr>
<td>Body.Remove</td>
<td>Removes a number of bytes from the body of the request or response that is currently processed.</td>
<td>1 Number: Byte position where the removal begins&lt;br&gt;2 Number: Number of bytes to remove</td>
</tr>
</tbody>
</table>
### Table A-4  List of events (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| Body.Replace                | Replaces a portion from the body of the request or response that is currently processed with a string. | 1  Number: Byte position where replacement begins  
                          |                                                                             | 2  String: Pattern  
                          |                                                                             | a. string embedded in double quotes ("...", can also contain hex values preceded by \\)  
                          |                                                                             | or:  
                          |                                                                             | b. sequence of hex values |
| Body.ToFile                 | Writes the body of the request or response that is currently processed to the specified file. | String: Name of the file that the body is written to  
                          |                                                                             | The file is stored in the directory /opt/mwg/log/debug/BodyFilterDumps.  
                          |                                                                             | The body is written to the file only after it has been completely loaded, even if the Body.ToFile event occurred when only one or more chunks of the body had been loaded.  
                          |                                                                             | To prevent the stored files from filling up the hard disk of an appliance, enable their auto-deletion on the user interface under Configuration | <appliance> | Log File Manager | Advanced.  
<p>| | |
|                                                                             | |
| CloudEncryption.Encrypt     | Performs the encryption of cloud storage data using the encryption algorithm configured in the settings and the password specified as a parameter of the event. | This event can be triggered several times with different settings and passwords, so encryption is also performed several times. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudEncryption.Decrypt</td>
<td>Performs the decryption of data using the decryption algorithm specified in the settings and the password specified as a parameter of the event. This event can be triggered several times with different settings and passwords, so decryption is also performed several times. Order of calls to this event should be the reverse of calls to the encryption event.</td>
<td></td>
</tr>
<tr>
<td>Connection.Mark</td>
<td>Sets a connection mark.</td>
<td>Number: Number of a connection</td>
</tr>
<tr>
<td>DSCP.Mark.Request</td>
<td>Sets an IP header field. The field is known as DSCP header field. It can be evaluated by network devices supporting DSCP (Differentiated Services Code Point) when data packets are sent from Web Gateway to the requested web server. The value that the field is set to can be a number ranging from 0 to 63. The field can only be set for requests that are sent using an HTTP(S) connection. The option to set this field by an event allows the administrator to provide information for network devices that support DSCP, such as routers and others, depending on a Web Gateway rule that applies. Using the header field in this way requires that the network devices are configured accordingly. For example, when a rule for handling streaming media applies, setting the header field to a particular value would let routers direct data packets in a way that leads to a throttling of the connection. Another option would be to use the header field for letting network devices perform some kind of load balancing.</td>
<td>Number: Value of the DSCP header field</td>
</tr>
</tbody>
</table>
### Table A-4 List of events (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP.Mark.Response</td>
<td>Sets an IP header field. The field is known as DSCP header field. It can be evaluated by network devices supporting DSCP (Differentiated Services Code Point) when data packets are sent back in response from Web Gateway to a client. The value that the header field is set to can be a number ranging from 0 to 63. The header field can only be set for responses that are sent using an HTTP(S) connection. The option to set this header field by an event allows the administrator to provide information for network devices that support DSCP, such as routers and others, depending on a Web Gateway rule that applies. Using the header field in this way requires that the network devices are configured accordingly.</td>
<td>Number: Value of the DSCP header field</td>
</tr>
<tr>
<td>DXL.Event</td>
<td>Sends a DXL message with information about a web security topic to the subscribers.</td>
<td>1 String: Topic to send information about 2 String: Information to send about topic</td>
</tr>
<tr>
<td>Email.Send</td>
<td>Sends an email.</td>
<td>1 String: Recipient 2 String: Subject 3 String: Body</td>
</tr>
<tr>
<td>Enable Cache</td>
<td>Enables the web cache.</td>
<td></td>
</tr>
<tr>
<td>Enable CompositeOpener</td>
<td>Enables the composite opener.</td>
<td></td>
</tr>
<tr>
<td>Enable Data Trickling</td>
<td>Enables data trickling.</td>
<td></td>
</tr>
<tr>
<td>Enable FTP Upload Progress Indication</td>
<td>Enables the sending of responses to an FTP client, stating that processing of a file that has been sent for uploading to the web is still in progress. This is intended to prevent a timeout on the FTP client when processing on Web Gateway takes more time, for example, due to scanning the file that should be uploaded for infections by viruses and other malware.</td>
<td></td>
</tr>
<tr>
<td>Enable HTML Opener</td>
<td>Enables the HTML opener.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Media Stream Scanner</td>
<td>Enables the Media Stream Scanner, which is provided by the McAfee Gateway Anti-Malware engine.</td>
<td></td>
</tr>
<tr>
<td>Enable Next Hop Proxy</td>
<td>Enables use of next-hop proxies.</td>
<td></td>
</tr>
<tr>
<td>Enable Outbound Source IP Override</td>
<td>Enables the replacement of different outbound source IP addresses by a single IP address.</td>
<td>List of string: List of IP addresses for replacing other IP addresses in string format</td>
</tr>
<tr>
<td>Enable Progress Page</td>
<td>Enables display of a progress page.</td>
<td></td>
</tr>
<tr>
<td>Enable RuleEngine Tracing</td>
<td>Enables tracing of the activities that are completed by the rule processing module (rule engine).</td>
<td></td>
</tr>
<tr>
<td>Enable SSL Client Context with CA</td>
<td>Enables sending of client certificates issued by a certificate authority.</td>
<td></td>
</tr>
<tr>
<td>Enable SSL Client Context without CA</td>
<td>Enables sending of client certificates not issued by a certificate authority.</td>
<td></td>
</tr>
<tr>
<td>Enable SSL Scanner</td>
<td>Enables module for SSL scanning.</td>
<td></td>
</tr>
<tr>
<td>Enable SafeSearchEnforcer</td>
<td>Enables the SafeSearchEnforcer.</td>
<td></td>
</tr>
<tr>
<td>Enable Proxy Control</td>
<td>Enables proxy control</td>
<td></td>
</tr>
<tr>
<td>FileSystemLogging.WriteDebugEntry</td>
<td>Writes a debugging entry.</td>
<td>1 String: Debugging entry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Boolean: If true, entry is written to stdout</td>
</tr>
<tr>
<td>FileSystemLogging.WriteLogEntry</td>
<td>Writes an entry into a log.</td>
<td>String: Log entry</td>
</tr>
<tr>
<td>HTMLElement.InsertAttribute</td>
<td>Inserts an attribute into an HTML element.</td>
<td>1 String: Attribute name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 String: Attribute value</td>
</tr>
<tr>
<td>HTMLElement.RemoveAttribute</td>
<td>Removes an attribute from an HTML element.</td>
<td>String: Attribute name</td>
</tr>
<tr>
<td>HTMLElement.SetAttributeValue</td>
<td>Sets an attribute to a value.</td>
<td>1 String: Attribute name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 String: Value to set attribute to</td>
</tr>
<tr>
<td>Header.Add</td>
<td>Adds a header to a request or response.</td>
<td>1 String: Header name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 String: Header value</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Header.AddMultiple</td>
<td>Adds a header with a list of values to a request or response.</td>
<td>1 String: Header name&lt;br&gt;2 List of string: List of header values</td>
</tr>
<tr>
<td>Header.Block.Add</td>
<td>Adds a block header to a request or response.</td>
<td>1 String: Header name&lt;br&gt;2 String: Header value</td>
</tr>
<tr>
<td>Header.Block.AddMultiple</td>
<td>Adds a block header with a list of values to a request or response.</td>
<td>1 String: Header name&lt;br&gt;2 List of string: List of header values</td>
</tr>
<tr>
<td>Header.Block.RemoveAll</td>
<td>Removes all block headers with a given name from a request or response.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.ICAP.Response.Add</td>
<td>Adds a header to an ICAP response.</td>
<td>1 String: Header name&lt;br&gt;2 String: Header value</td>
</tr>
<tr>
<td>Header.ICAP.Response.AddMultiple</td>
<td>Adds a header with a list of values to an ICAP response.</td>
<td>1 String: Header name&lt;br&gt;2 List of string: List of header values</td>
</tr>
<tr>
<td>Header.ICAP.Response.RemoveAll</td>
<td>Removes all headers with a given name from an ICAP response.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.RemoveAll</td>
<td>Removes all headers with a given name from a request or response.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.Response.Add</td>
<td>Adds a header to the page generated by a block action.</td>
<td></td>
</tr>
<tr>
<td>HTTP.GenerateResponse</td>
<td>Generates a response to the request made in the request cycle.</td>
<td>String: Response body</td>
</tr>
<tr>
<td>HTTP.SetStatus</td>
<td>Sets the HTTP status code at the end of the response cycle.</td>
<td>Number: HTTP status code</td>
</tr>
<tr>
<td>ICAP.AddRequestInformation</td>
<td>Adds information to an ICAP request.</td>
<td>1 String: Name of the request&lt;br&gt;2 String: Added information</td>
</tr>
<tr>
<td>MediaType.Header.FixContentType</td>
<td>Replaces a media type header with an appropriate header when it is found after inspection of the media body that the original header does not match the body.</td>
<td></td>
</tr>
<tr>
<td>Notice</td>
<td>Writes an entry with notice level into syslog.</td>
<td>String: Log entry</td>
</tr>
<tr>
<td>PDStorage.AddGlobalData.Bool</td>
<td>Adds global variable of type Boolean.</td>
<td>1 String: Variable key&lt;br&gt;2 Boolean: Variable value</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>PDStorage.AddGlobalData.Category</td>
<td>Adds global variable of type Category.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Category: Variable value</td>
</tr>
<tr>
<td>PDStorage.AddGlobalData.Dimension</td>
<td>Adds global variable of type Dimension.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Dimension: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData.Hex</td>
<td>Adds global variable of type Hex.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Hex: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData.IP</td>
<td>Adds global variable of type IP.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 IP: Variable value</td>
</tr>
<tr>
<td>PDStorage.AddGlobalData.IPRange</td>
<td>Adds global variable of type IPRange.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 IPRange: Variable value</td>
</tr>
<tr>
<td>PDStorage.AddGlobalData.List.Category</td>
<td>Adds global variable of type List of Category.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of Category: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData.List.Dimension</td>
<td>Adds global variable of type List of Dimension.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of Dimension: Variable value</td>
</tr>
<tr>
<td>PDStorage.AddGlobalData.List.Hex</td>
<td>Adds global variable of type List of Hex.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of Hex: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData.List.IP</td>
<td>Adds global variable of type List of IP.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of IP: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData.List.IPRange</td>
<td>Adds global variable of type List of IPRange.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of IPRange: Variable value</td>
</tr>
<tr>
<td>PDStorage.AddGlobalData.List.MediaType</td>
<td>Adds global variable of type List of MediaType.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of MediaType: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData.List.Number</td>
<td>Adds global variable of type List of Number.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of Number: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData.List.String</td>
<td>Adds global variable of type List of String.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of String: Variable value</td>
</tr>
</tbody>
</table>

**Table A-4 List of events (continued)**
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDStorage. AddGlobalData.List. Wildcard</td>
<td>Adds global variable of type List of Wildcard Expression.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of Wildcard Expression: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData. MediaType</td>
<td>Adds global variable of type MediaType.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 MediaType: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData.Number</td>
<td>Adds global variable of type Number.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Number: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData.String</td>
<td>Adds global variable of type String.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 String: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddGlobalData.Wildcard</td>
<td>Adds global variable of type Wildcard Expression.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Wildcard Expression: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.Bool</td>
<td>Adds user variable of type Boolean.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Boolean: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.Category</td>
<td>Adds user variable of type Category.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Category: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.Dimension</td>
<td>Adds user variable of type Dimension.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Dimension: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.Hex</td>
<td>Adds user variable of type Hex.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Hex: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.IP</td>
<td>Adds user variable of type IP.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 IP: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.IPRange</td>
<td>Adds user variable of type IPRange.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 IPRange: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.List. Category</td>
<td>Adds user variable of type List of Category.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of Category: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.List. Dimension</td>
<td>Adds user variable of type List of Dimension.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of Dimension: Variable value</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>PDStorage. AddUserData.List.Hex</td>
<td>Adds user variable of type List of Hex.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of Hex: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.List.IP</td>
<td>Adds user variable of type List of IP.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of IP: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.List.IPRange</td>
<td>Adds user variable of type List of IPRange.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of IPRange: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.List.MediaType</td>
<td>Adds user variable of type List of MediaType.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of MediaType: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.List.Number</td>
<td>Adds user variable of type List of Number.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of Number: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.List.String</td>
<td>Adds user variable of type List of String.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of String: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.List.Wildcard</td>
<td>Adds user variable of type List of Wildcard Expression.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 List of Wildcard Expression: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.MediaType</td>
<td>Adds user variable of type MediaType.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 MediaType: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.Number</td>
<td>Adds user variable of type Number.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Number: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.String</td>
<td>Adds user variable of type String.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 String: Variable value</td>
</tr>
<tr>
<td>PDStorage. AddUserData.Wildcard</td>
<td>Adds user variable of type Wildcard Expression.</td>
<td>1 String: Variable key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Wildcard Expression: Variable value</td>
</tr>
<tr>
<td>PDStorage. Cleanup</td>
<td>Cleans up persistently stored data.</td>
<td></td>
</tr>
<tr>
<td>PDStorage. DeleteAllUserData</td>
<td>Deletes all permanently stored user data.</td>
<td></td>
</tr>
<tr>
<td>PDStorage. DeleteGlobalData</td>
<td>Deletes all permanently stored global variables of a given type.</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>PDStorage.DeleteUserData</td>
<td>Deletes all permanently stored user variables of a given type.</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>ProtocolDetector.ApplyFiltering</td>
<td>Applies processing of web filtering rules on web traffic that has been found to follow a protocol that is supported on Web Gateway.</td>
<td></td>
</tr>
<tr>
<td>SNMP.Send.Trap.Application</td>
<td>Sends an SNMP trap message with application information.</td>
<td></td>
</tr>
<tr>
<td>SNMP.Send.Trap.System</td>
<td>Sends an SNMP trap message with system information.</td>
<td></td>
</tr>
<tr>
<td>SNMP.Send.Trap.User</td>
<td>Sends an SNMP trap message with user information.</td>
<td>1 Number: User ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 String: Message body</td>
</tr>
<tr>
<td>SNMP.Send.Trap.UserHost</td>
<td>Sends an SNMP trap message with information on the host of a user.</td>
<td>1 Number: User ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 String: Message body</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 IP: IP address of the host</td>
</tr>
<tr>
<td>SSO.AddCredentials</td>
<td>Creates new credentials for a user who attempts to log on in a single sign-on process to a cloud application.</td>
<td>1 String: Identity provider</td>
</tr>
<tr>
<td></td>
<td>To authenticate a user, the credentials are evaluated by an authentication instance, which is also known as identity provider (IdP), for example, an LDAP or NTLM database.</td>
<td>2 String: User name</td>
</tr>
<tr>
<td></td>
<td>The new credentials are stored in the database of the identity provider.</td>
<td>3 String: Cloud application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 JSON: Credentials in JSON format</td>
</tr>
<tr>
<td>SSO.AddServices</td>
<td>Prepares the availability of cloud applications for a user who attempts to select one of them for logon in a single sign-on process.</td>
<td>1 String: Identity provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 String: User name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 List: List of cloud applications</td>
</tr>
</tbody>
</table>

A cloud application is also referred to as cloud service.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| SSO.DeleteCredentials | Deletes credentials of a user who attempts to logon in a single sign-on process to a cloud application.                                                                                                                         | 1 String: Identity provider  
2 String: User name  
3 String: Cloud application  
4 JSON: Credentials in JSON format |
|                     | To authenticate a user the credentials are evaluated by an authentication instance, which is also known as identity provider (IdP), for example, an LDAP or NTLM database.                                                          |                                                                                               |
|                     | The new credentials are stored in the database of the identity provider.                                                                                                                                                         |                                                                                               |
| SSO.ProcessFormLogin | Processes the data that was submitted for a user in a form on a logon page to perform logon to a cloud application in a single sign-on process.                                                                                   |                                                                                               |
|                     | One of the following is executed for the logon form:                                                                                                                                                                               |                                                                                               |
|                     | • When a logon form is sent with a POST request to a cloud application, the password token that had been inserted into the logon form before is replaced by the real password of the user who requests single sign-on access. |                                                                                               |
|                     | • When a logon form is requested for a user with a GET request that is sent from a browser, script code is inserted into the form to fill it out and forward it to the cloud application.                                           |                                                                                               |
|                     | This event is only executed when the proxy (inline) mode is configured for the single sign-on process.                                                                                                                             |                                                                                               |
| SSO.UpdateCredentials | Updates credentials of a user who attempts to log on in a single sign-on process to a cloud application.                                                                                                                       | 1 String: Identity provider  
2 String: User name  
3 String: Cloud application  
4 JSON: Credentials in JSON format |
|                     | To authenticate a user, the credentials are evaluated by an authentication instance, which is also known as identity provider (IdP), for example, an LDAP or NTLM database.                                                            |                                                                                               |
|                     | The new credentials are stored in the database of the identity provider.                                                                                                                                                         |                                                                                               |
Table A-4 List of events (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistics.Counter.Reset</td>
<td>Resets a counter.</td>
<td>String: Counter name</td>
</tr>
<tr>
<td>Stopwatch.Reset</td>
<td>Sets an internal watch that measures processing time for rule sets.</td>
<td>String: Rule set name</td>
</tr>
<tr>
<td>Stopwatch.Start</td>
<td>Starts an internal watch that measures processing time for rule sets.</td>
<td>String: Rule set name</td>
</tr>
<tr>
<td>Stopwatch.Stop</td>
<td>Stops an internal watch that measures processing time for rule sets.</td>
<td>String: Rule set name</td>
</tr>
<tr>
<td>Syslog</td>
<td>Writes an entry into syslog.</td>
<td>1 Number: Log level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 – Emergency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Alert</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 – Critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 – Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 – Warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 – Notice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 – Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 – Debugging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 String: Log entry</td>
</tr>
</tbody>
</table>

List of incident IDs

The following table provides a list of the incident IDs you can use in rules.

The incident IDs are grouped in numerical ranges as follows.

1-199 Incidents related to the appliance system
200-299 Core subsystem incidents
300-399 Update module incidents
400-499 Virus and malware filtering incidents
500-599 Log File Manager incidents
600-699 sysconfd daemon incidents
700-799 Proxy module incidents
800-899 Virus and malware filtering incidents
900-999 Authentication incidents
1000-1099 URL filtering incidents
1100-1199 Quota management incidents
1200-1299 SSL certificate incidents
1300-1399 ICAP client incidents
1400-1499 Media type filtering incidents
1500-1599 Opener incidents
1600-1699 SSL certificate chain incidents
<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Description</th>
<th>Origin number and name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>A rule that uses an incident property was executed.</td>
<td>1 System</td>
<td>7</td>
</tr>
<tr>
<td>20</td>
<td>RAID monitoring reported critical status or failure of one or more hard disks.</td>
<td>1 Health Monitor</td>
<td>4 (or 3 for hard-disk failure)</td>
</tr>
<tr>
<td>21</td>
<td>S.M.A.R.T health check reported an error on an HDD hard disk.</td>
<td>1 Health Monitor</td>
<td>4</td>
</tr>
<tr>
<td>22</td>
<td>File system usage has exceeded a configured limit.</td>
<td>1 Health Monitor</td>
<td>4</td>
</tr>
<tr>
<td>23</td>
<td>Memory usage has exceeded a configured limit.</td>
<td>1 Health Monitor</td>
<td>4</td>
</tr>
<tr>
<td>24</td>
<td>System load has exceeded a configured limit.</td>
<td>1 Health Monitor</td>
<td>4</td>
</tr>
<tr>
<td>26</td>
<td>A check has been executed to detect a BBU RAID error. The checking interval is 30 minutes.</td>
<td>1 Health Monitor</td>
<td>4</td>
</tr>
<tr>
<td>200</td>
<td>The license expiration date has been checked.</td>
<td>2 Core</td>
<td>6</td>
</tr>
<tr>
<td>201</td>
<td>The appliance has successfully completed all FIPS 140-2 self-tests.</td>
<td>2 Core</td>
<td>6</td>
</tr>
<tr>
<td>211</td>
<td>The maximum number of entries in dashboard report x has been exceeded.</td>
<td>2 Statistics</td>
<td>4</td>
</tr>
<tr>
<td>298</td>
<td>Update of product x succeeded.</td>
<td>2 Core</td>
<td>6</td>
</tr>
<tr>
<td>299</td>
<td>Update of product x failed.</td>
<td>2 Core</td>
<td>3</td>
</tr>
<tr>
<td>250</td>
<td>An entry in a list is invalid and will be ignored.</td>
<td>2 Core</td>
<td>3</td>
</tr>
<tr>
<td>301</td>
<td>Download of update files was stopped because there is not enough disk space.</td>
<td>3 Updater</td>
<td>3</td>
</tr>
</tbody>
</table>
### Table A-5  List of incident IDs (continued)

<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Description</th>
<th>Origin number and name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>302</td>
<td>Download of product x failed on node y.</td>
<td>3 Updater</td>
<td>3</td>
</tr>
<tr>
<td>303</td>
<td>Update of product x failed on node y.</td>
<td>3 Updater</td>
<td>3</td>
</tr>
<tr>
<td>304</td>
<td>Status of product x on node y is up to date.</td>
<td>3 Updater</td>
<td>3</td>
</tr>
<tr>
<td>305</td>
<td>The update module could not connect to an update server.</td>
<td>3 Updater</td>
<td>3</td>
</tr>
<tr>
<td>321</td>
<td>Download of product x succeeded on node y.</td>
<td>3 Updater</td>
<td>6</td>
</tr>
<tr>
<td>322</td>
<td>Download of product x succeeded on node y.</td>
<td>3 Updater</td>
<td>6</td>
</tr>
<tr>
<td>323</td>
<td>Update of customer subscribed list x succeeded on node y.</td>
<td>3 Customer Subscribed List Manager</td>
<td>6</td>
</tr>
<tr>
<td>324</td>
<td>Update of customer subscribed list x failed on nodes y, z, ...</td>
<td>3 Customer Subscribed List Manager</td>
<td>3</td>
</tr>
<tr>
<td>325</td>
<td>Status of customer subscribed list x on node y is up to date.</td>
<td>3 Customer Subscribed List Manager</td>
<td>6</td>
</tr>
<tr>
<td>326</td>
<td>Download of customer subscribed list x failed on nodes y, z, ...</td>
<td>3 Customer Subscribed List Manager</td>
<td>3</td>
</tr>
<tr>
<td>327</td>
<td>Download of McAfee subscribed list x failed on nodes y, z, ...</td>
<td>3 Updater</td>
<td>3</td>
</tr>
<tr>
<td>328</td>
<td>Update of McAfee subscribed list x failed on nodes y, z, ...</td>
<td>3 Updater</td>
<td>3</td>
</tr>
<tr>
<td>329</td>
<td>Status of McAfee subscribed list x on nodes y, z, ... is up to date.</td>
<td>3 Updater</td>
<td>6</td>
</tr>
<tr>
<td>330</td>
<td>Update of McAfee subscribed list x succeeded on node y.</td>
<td>3 Updater</td>
<td>6</td>
</tr>
<tr>
<td>331</td>
<td>Processing scheduled job x succeeded</td>
<td>3 Scheduled Job Manager</td>
<td>6</td>
</tr>
<tr>
<td>332</td>
<td>Processing scheduled job x failed.</td>
<td>3 Scheduled Job Manager</td>
<td>3</td>
</tr>
<tr>
<td>333</td>
<td>Update of updatable system lists failed on node y.</td>
<td>3 Central Updater</td>
<td>3</td>
</tr>
<tr>
<td>334</td>
<td>Update of updatable system lists succeeded on node y.</td>
<td>3 Central Updater</td>
<td>6</td>
</tr>
<tr>
<td>335</td>
<td>Status of updatable system lists on node y is up to date.</td>
<td>3 Central Updater</td>
<td>6</td>
</tr>
<tr>
<td>340-349</td>
<td>Migration failed for different reasons.</td>
<td>3 Migration</td>
<td>6</td>
</tr>
<tr>
<td>500</td>
<td>The log manager experienced an unrecoverable internal error and will terminate.</td>
<td>5 Log File Manager</td>
<td>2</td>
</tr>
<tr>
<td>501</td>
<td>Log File Manager failed to push log files.</td>
<td>5 Log File Manager</td>
<td>3</td>
</tr>
<tr>
<td>600</td>
<td>A yum update contained packages that require a restart of the appliance to become effective.</td>
<td>6 mwg-update</td>
<td>4</td>
</tr>
<tr>
<td>601</td>
<td>A yum update was successfully completed.</td>
<td>6 mwg-update</td>
<td>5</td>
</tr>
<tr>
<td>602</td>
<td>A yum update failed.</td>
<td>6 mwg-update</td>
<td>3</td>
</tr>
<tr>
<td>620</td>
<td>A major distribution upgrade was successfully completed.</td>
<td>6 mwg-dist-upgrade</td>
<td>5</td>
</tr>
<tr>
<td>621</td>
<td>A major distribution upgrade is in progress. The appliance will restart automatically.</td>
<td>6 mwg-dist-upgrade</td>
<td>4</td>
</tr>
<tr>
<td>Incident ID</td>
<td>Description</td>
<td>Origin number and name</td>
<td>Severity</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>622</td>
<td>A major distribution upgrade failed. Check the upgrade log file.</td>
<td>6 mwg-dist-upgrade</td>
<td>3</td>
</tr>
<tr>
<td>666</td>
<td>A FIPS 140-2 self-test failed on node y. The node is running in non-FIPS mode.</td>
<td>1 FIPS</td>
<td>0</td>
</tr>
<tr>
<td>700</td>
<td>The number of concurrent connections has exceeded the configured overload limit. The appliance has entered overload status. Requests sent to the appliance are accepted with delay.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>701</td>
<td>The appliance is in overload status for more than 30 seconds. Requests sent to the appliance are accepted with delay.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>702</td>
<td>The appliance has left overload status. Requests sent to the appliance are again accepted without delay.</td>
<td>2 Proxy</td>
<td>4</td>
</tr>
<tr>
<td>703</td>
<td>The number of concurrent connections has exceeded the configured high-load limit. The appliance has entered high-load status. Requests sent to the appliance are accepted with a delay.</td>
<td>2 Proxy</td>
<td>4</td>
</tr>
<tr>
<td>704</td>
<td>The appliance is in high-load status for more than 30 seconds. Requests sent to the appliance are accepted with a delay.</td>
<td>2 Proxy</td>
<td>4</td>
</tr>
<tr>
<td>705</td>
<td>The number of concurrent connections has dropped below 85% of the configured high-load limit. The appliance is still in high-load status. Requests sent to the appliance are accepted with a delay.</td>
<td>2 Proxy</td>
<td>6</td>
</tr>
<tr>
<td>710</td>
<td>A next-hop proxy server is down and will not be available for n seconds.</td>
<td>2 Proxy</td>
<td>4</td>
</tr>
<tr>
<td>711</td>
<td>The appliance could not connect to a next-hop proxy server.</td>
<td>2 Proxy</td>
<td>4</td>
</tr>
<tr>
<td>712</td>
<td>A next-hop proxy server has moved back from error status to normal operation.</td>
<td>2 Proxy</td>
<td>6</td>
</tr>
<tr>
<td>720</td>
<td>The listener on IP address x, port y could not be opened.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>730</td>
<td>A changed proxy mode configuration requires a restart of the appliance.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>740</td>
<td>The number of concurrent connections has exceeded the overload limit that is configured for an IFP proxy. Overload status has been entered. New requests are not processed.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>741</td>
<td>Overload status lasts more than 30 seconds for an IFP proxy. New requests are not processed.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>742</td>
<td>Overload status has been left for an IFP proxy. Requests are again accepted without delay.</td>
<td>2 Proxy</td>
<td>4</td>
</tr>
<tr>
<td>Incident ID</td>
<td>Description</td>
<td>Origin number and name</td>
<td>Severity</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>743</td>
<td>The number of concurrent connections has exceeded the high-load limit that is configured for an IFP proxy. High-load status has been entered. New requests are not processed.</td>
<td>2 Proxy</td>
<td>4</td>
</tr>
<tr>
<td>744</td>
<td>High-load status lasts more than 30 seconds for an IFP proxy. New requests are not processed.</td>
<td>2 Proxy</td>
<td>4</td>
</tr>
<tr>
<td>745</td>
<td>The number of concurrent connections has dropped below 85% of the high-load limit that is configured for an IFP proxy. High-load status is still on. Requests are accepted with a delay.</td>
<td>2 Proxy</td>
<td>6</td>
</tr>
<tr>
<td>750</td>
<td>A key for the HSM Agent could not be loaded due to an error on the appliance side.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>751</td>
<td>A key for the HSM Agent could not be loaded due to an error on the agent side.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>752</td>
<td>The ID of a key for an HSM Agent could not be retrieved due to an error on the appliance side.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>753</td>
<td>The ID of a key for an HSM Agent could not be retrieved due to an error on the agent side.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>760</td>
<td>The WCCP listener could not be started.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>761</td>
<td>WCCP could not start send and listerner threads.</td>
<td>2 Proxy</td>
<td>2</td>
</tr>
<tr>
<td>762</td>
<td>WCCP could not resolve the router address &lt;host&gt;</td>
<td>2 Proxy</td>
<td>3</td>
</tr>
<tr>
<td>763</td>
<td>WCCP could not join the multicast group &lt;host&gt;</td>
<td>2 Proxy</td>
<td>3</td>
</tr>
<tr>
<td>764</td>
<td>An error occurred when reading WCCP sockets or writing to them.</td>
<td>2 Proxy</td>
<td>3</td>
</tr>
<tr>
<td>765</td>
<td>Authentication with the WCCP router &lt;host&gt; failed.</td>
<td>2 Proxy</td>
<td>3</td>
</tr>
<tr>
<td>766</td>
<td>WCCP message parsing failed and malformed packets were created.</td>
<td>2 Proxy</td>
<td>3</td>
</tr>
<tr>
<td>767</td>
<td>The WCCP service ID or group could not be found</td>
<td>2 Proxy</td>
<td>3</td>
</tr>
<tr>
<td>768</td>
<td>A WCCP router for a service ID was added.</td>
<td>2 Proxy</td>
<td>6</td>
</tr>
<tr>
<td>769</td>
<td>A WCCP router for a service ID was removed.</td>
<td>2 Proxy</td>
<td>6</td>
</tr>
<tr>
<td>850</td>
<td>An update of the MGAM module for virus and malware filtering was successfully completed.</td>
<td>2 Anti-Malware Filter</td>
<td>6</td>
</tr>
<tr>
<td>851</td>
<td>An update of the MGAM module for virus and malware filtering failed.</td>
<td>2 Anti-Malware Filter</td>
<td>3</td>
</tr>
<tr>
<td>852</td>
<td>Download or verification of the update files for the MGAM module failed.</td>
<td>2 Anti-Malware Filter</td>
<td>3</td>
</tr>
<tr>
<td>Incident ID</td>
<td>Description</td>
<td>Origin number and name</td>
<td>Severity</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>853</td>
<td>The version of the MGAM module for virus and malware filtering is up to date.</td>
<td>2 Anti-Malware Filter</td>
<td>6</td>
</tr>
<tr>
<td>854</td>
<td>An update of the Avira module for virus and malware filtering was successfully completed.</td>
<td>2 Anti-Malware Filter</td>
<td>6</td>
</tr>
<tr>
<td>855</td>
<td>An update of the Avira module for virus and malware filtering failed.</td>
<td>2 Anti-Malware Filter</td>
<td>3</td>
</tr>
<tr>
<td>856</td>
<td>Download or verification of the update files for the Avira module failed.</td>
<td>2 Anti-Malware Filter</td>
<td>3</td>
</tr>
<tr>
<td>857</td>
<td>The version of the Avira module for virus and malware filtering is up to date.</td>
<td>2 Anti-Malware Filter</td>
<td>6</td>
</tr>
<tr>
<td>901</td>
<td>The appliance is connected to n servers for NTLM authentication in Windows domain x.</td>
<td>2 NTLM Authentication Filter</td>
<td>6</td>
</tr>
<tr>
<td>902</td>
<td>The appliance could not connect to n servers for NTLM authentication in Windows domain x.</td>
<td>2 NTLM Authentication Filter</td>
<td>4</td>
</tr>
<tr>
<td>903</td>
<td>The appliance could not contact Windows domain x for NTLM authentication.</td>
<td>2 NTLM Authentication Filter</td>
<td>3</td>
</tr>
<tr>
<td>910</td>
<td>The appliance is connected to the LDAP server with configuration ID n.</td>
<td>2 LDAP Authentication Filter</td>
<td>6</td>
</tr>
<tr>
<td>912</td>
<td>The appliance was disconnected from the LDAP server with configuration ID n.</td>
<td>2 LDAP Authentication Filter</td>
<td>4</td>
</tr>
<tr>
<td>913</td>
<td>The appliance could not connect to any LDAP server with configuration ID n.</td>
<td>2 LDAP Authentication Filter</td>
<td>3</td>
</tr>
<tr>
<td>920</td>
<td>A response has been received from RADIUS server x after attempting to start communication to retrieve information for authenticating users.</td>
<td>2 RADIUS Authentication Filter</td>
<td>6</td>
</tr>
<tr>
<td>921</td>
<td>A response has again been received from RADIUS server x after communication had been interrupted.</td>
<td>2 RADIUS Authentication Filter</td>
<td>6</td>
</tr>
<tr>
<td>923</td>
<td>An authentication request sent to RADIUS server x has led to a timeout.</td>
<td>2 RADIUS Authentication Filter</td>
<td>3</td>
</tr>
<tr>
<td>931</td>
<td>The appliance is connected to NTLM-Agent server x.</td>
<td>2 NTLM-Agent Authentication Filter</td>
<td>6</td>
</tr>
<tr>
<td>932</td>
<td>The appliance has been disconnected from NTLM-Agent server x.</td>
<td>2 NTLM-Agent Authentication Filter</td>
<td>3</td>
</tr>
<tr>
<td>933</td>
<td>The appliance could not connect to NTLM-Agent server x.</td>
<td>2 NTLM-Agent Authentication Filter</td>
<td>3</td>
</tr>
<tr>
<td>940</td>
<td>An update of a Certificate Revocation List was successfully completed.</td>
<td>2 Authentication Filter</td>
<td>6</td>
</tr>
<tr>
<td>941</td>
<td>An update of a Certificate Revocation List failed.</td>
<td>2 Authentication Filter</td>
<td>4</td>
</tr>
<tr>
<td>942</td>
<td>A download of a Certificate Revocation List failed.</td>
<td>2 Authentication Filter</td>
<td>4</td>
</tr>
<tr>
<td>943</td>
<td>The status of a Certificate Revocation List is up to date.</td>
<td>2 Authentication Filter</td>
<td>6</td>
</tr>
<tr>
<td>Incident ID</td>
<td>Description</td>
<td>Origin number and name</td>
<td>Severity</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>1050</td>
<td>An update of the URL Filter module was successfully completed.</td>
<td>2 URL Filter</td>
<td>6</td>
</tr>
<tr>
<td>1051</td>
<td>An update of the URL Filter module failed.</td>
<td>2 URL Filter</td>
<td>3</td>
</tr>
<tr>
<td>1052</td>
<td>Download or verification of update files for the URL Filter module failed.</td>
<td>2 URL Filter</td>
<td>3</td>
</tr>
<tr>
<td>1053</td>
<td>Status of the URL Filter module is up to date.</td>
<td>2 URL Filter</td>
<td>6</td>
</tr>
<tr>
<td>1650</td>
<td>An updated Certificate Revocation List was downloaded and loaded successfully.</td>
<td>2 Certificate Chain Filter</td>
<td>6</td>
</tr>
<tr>
<td>1651</td>
<td>An updated Certificate Revocation List was downloaded, but could not be loaded.</td>
<td>2 Certificate Chain Filter</td>
<td>4</td>
</tr>
<tr>
<td>1652</td>
<td>An updated Certificate Revocation List could not be downloaded.</td>
<td>2 Certificate Chain Filter</td>
<td>3</td>
</tr>
<tr>
<td>1653</td>
<td>Status of all Certificate Revocation Lists is up to date.</td>
<td>2 Certificate Chain Filter</td>
<td>6</td>
</tr>
<tr>
<td>1700</td>
<td>An admin user logged on successfully to the user interface.</td>
<td>7 User interface</td>
<td>4</td>
</tr>
<tr>
<td>1701</td>
<td>Logon of an admin user to the user interface failed.</td>
<td>7 User interface</td>
<td>3</td>
</tr>
<tr>
<td>1702</td>
<td>The IP address of a client that an end user sent a request from changed.</td>
<td>7 User interface</td>
<td>4</td>
</tr>
<tr>
<td>1703</td>
<td>An admin user logged off successfully from the user interface.</td>
<td>7 User interface</td>
<td>6</td>
</tr>
<tr>
<td>1704</td>
<td>A logoff from the user interface was forced upon an admin user after a restart of an appliance, a timeout, or a similar incident had occurred.</td>
<td>7 User interface</td>
<td>6</td>
</tr>
<tr>
<td>1710</td>
<td>An admin user saved changes successfully.</td>
<td>7 User interface</td>
<td>6</td>
</tr>
<tr>
<td>1711</td>
<td>An attempt by an admin user to save changes failed.</td>
<td>7 User interface</td>
<td>3</td>
</tr>
<tr>
<td>1800</td>
<td>The number of entries that can be retrieved from an external list has exceeded the configured limit.</td>
<td>2 External Lists Filter</td>
<td>4</td>
</tr>
<tr>
<td>1801</td>
<td>The amount of data of entries that can be retrieved from an external list has exceeded the configured limit.</td>
<td>2 External Lists Filter</td>
<td>4</td>
</tr>
<tr>
<td>1802</td>
<td>An error occurred when data was retrieved from an external list.</td>
<td>2 External Lists Filter</td>
<td>4</td>
</tr>
<tr>
<td>1803</td>
<td>An error occurred when data that had been retrieved from an external list was converted.</td>
<td>2 External Lists Filter</td>
<td>4</td>
</tr>
<tr>
<td>1804</td>
<td>A time-out occurred when data was retrieved from an external list.</td>
<td>2 External Lists Filter</td>
<td>4</td>
</tr>
<tr>
<td>1805</td>
<td>Permission to retrieve data from an external list was denied.</td>
<td>2 External Lists Filter</td>
<td>4</td>
</tr>
<tr>
<td>1806</td>
<td>A resource for retrieving external list data could not be found.</td>
<td>2 External Lists Filter</td>
<td>4</td>
</tr>
<tr>
<td>1850</td>
<td>An update of the database for application filtering was successfully completed.</td>
<td>2 Application Control</td>
<td>6</td>
</tr>
<tr>
<td>Incident ID</td>
<td>Description</td>
<td>Origin number and name</td>
<td>Severity</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>1851</td>
<td>An update of the database for application filtering failed.</td>
<td>2 Application Control</td>
<td>3</td>
</tr>
<tr>
<td>1852</td>
<td>A download of the database for application filtering failed.</td>
<td>2 Application Control</td>
<td>3</td>
</tr>
<tr>
<td>1853</td>
<td>Status of the database for application filtering is up to date.</td>
<td>2 Application Control</td>
<td>6</td>
</tr>
<tr>
<td>1854</td>
<td>Loading the database for application filtering failed.</td>
<td>2 Application Control</td>
<td>3</td>
</tr>
<tr>
<td>1855</td>
<td>Loading the database for application filtering was successfully completed.</td>
<td>2 Application Control</td>
<td>6</td>
</tr>
<tr>
<td>1950</td>
<td>An update of the Data Loss Prevention (DLP) module was successfully completed.</td>
<td>2 Data Loss Prevention</td>
<td>6</td>
</tr>
<tr>
<td>1951</td>
<td>An update of the Data Loss Prevention (DLP) module failed.</td>
<td>2 Data Loss Prevention</td>
<td>3</td>
</tr>
<tr>
<td>1952</td>
<td>Download or verification of the update files for the Data Loss Prevention (DLP) module failed.</td>
<td>2 Data Loss Prevention</td>
<td>3</td>
</tr>
<tr>
<td>1953</td>
<td>Status of the Data Loss Prevention (DLP) is up to date.</td>
<td>2 Data Loss Prevention</td>
<td>6</td>
</tr>
<tr>
<td>2001</td>
<td>An error occurred with the Stream Detector module.</td>
<td>2 Stream Detector</td>
<td>2</td>
</tr>
<tr>
<td>2101</td>
<td>The database for media type filtering could not be loaded.</td>
<td>2 Media Type Filter</td>
<td>2</td>
</tr>
<tr>
<td>2200</td>
<td>An update of the Dynamic Content Classifier was successfully completed.</td>
<td>2 Dynamic Content Classifier</td>
<td>6</td>
</tr>
<tr>
<td>2201</td>
<td>An update of the Dynamic Content Classifier failed.</td>
<td>2 Dynamic Content Classifier</td>
<td>3</td>
</tr>
<tr>
<td>2202</td>
<td>A download or verification of the update files for the Dynamic Content Classifier failed.</td>
<td>2 Dynamic Content Classifier</td>
<td>3</td>
</tr>
<tr>
<td>2203</td>
<td>Status of the Dynamic Content Classifier is up to date.</td>
<td>2 Dynamic Content Classifier</td>
<td>6</td>
</tr>
<tr>
<td>2350</td>
<td>An update of the files for the single sign-on process was successfully completed.</td>
<td>3 Single Sign On Service</td>
<td>6</td>
</tr>
<tr>
<td>2351</td>
<td>An update of the files for the single sign-on process failed.</td>
<td>3 Single Sign On Service</td>
<td>3</td>
</tr>
<tr>
<td>2352</td>
<td>A download or verification of the updated files for the single sign-on process failed.</td>
<td>3 Single Sign On Service</td>
<td>3</td>
</tr>
<tr>
<td>2353</td>
<td>Status of the files for the single sign-on process are up to date.</td>
<td>3 Single Sign On Service</td>
<td></td>
</tr>
<tr>
<td>2401</td>
<td>Failed to load services database. This incident is reported when the Cloud Storage Encryption module cannot load files with a description of supported cloud storage services.</td>
<td>3 Cloud Storage Encryption</td>
<td>2</td>
</tr>
<tr>
<td>2502</td>
<td>Credential store export incident Export of data from the credential store failed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table A-5  List of incident IDs (continued)

<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Description</th>
<th>Origin number and name</th>
<th>Severity</th>
</tr>
</thead>
</table>
| 2503        | Credential store import incident  
Import of data into the credential store failed. |                         |          |
| 2510        | Credential store incident  
A credential store error occurred. See the message in the incident report and more details in the error log. |                         |          |
| 2550        | SSO update success  
The SSO module was successfully updated. |                         |          |
| 2551        | SSO update failure  
The SSO module could not successfully be updated.  
See the errors log for more details. |                         |          |
| 2552        | SSO download failed  
Files could not successfully be downloaded from the SSO server. |                         |          |
| 2553        | SSO catalog up to date  
There is no new version of the SSO files on the update server. |                         |          |
| 2650        | SSO catalog update success  
The SSO connector catalog was successfully updated. |                         |          |
| 2651        | SSO catalog update failure  
The SSO connector catalog could not successfully be updated.  
See the errors log for more details. |                         |          |
| 2652        | SSO catalog download failed  
SSO connector catalog files could not successfully be downloaded from the update server. |                         |          |
| 2653        | SSO catalog up to date  
There is no new version of the SSO connector catalog files on the update server. |                         |          |
| 3000        | At least one node in a Central Management configuration is not in synchronized status (with regard to storage and configuration).  
The number of unsynchronized nodes changes.  
This incident is only recorded on the root node. | 3 Central Management | 3        |
<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Description</th>
<th>Origin number and name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>3001</td>
<td>After incident 3000 occurred, all nodes in a Central Management configuration are again in synchronized status (with regard to storage and configuration).</td>
<td>3 Central Management</td>
<td>6</td>
</tr>
<tr>
<td>3005</td>
<td>At least one node in a Central Management configuration did not respond properly after shared data had been sent out. The number of nodes not properly responding changes. This incident is only recorded on the root node and only if the shared data was intended for all nodes.</td>
<td>3 Central Management</td>
<td>3</td>
</tr>
<tr>
<td>3006</td>
<td>After incident 3004 occurred, all nodes in a Central Management configuration responded properly again to the sending of shared data.</td>
<td>3 Central Management</td>
<td>6</td>
</tr>
<tr>
<td>3200</td>
<td>Sending lists to McAfee SaaS Web Protection was successfully completed.</td>
<td>3 Web Hybrid</td>
<td>6</td>
</tr>
<tr>
<td>3201</td>
<td>Sending lists to McAfee SaaS Web Protection failed.</td>
<td>3 Web Hybrid</td>
<td>3</td>
</tr>
<tr>
<td>3205</td>
<td>Lists were successfully downloaded from McAfee SaaS Web Protection and stored.</td>
<td>3 Web Hybrid</td>
<td>6</td>
</tr>
<tr>
<td>3206</td>
<td>Lists could not be downloaded from McAfee SaaS Web Protection and stored.</td>
<td>3 Web Hybrid</td>
<td>3</td>
</tr>
<tr>
<td>3210</td>
<td>Synchronization status could not be determined.</td>
<td>3 Web Hybrid</td>
<td>3</td>
</tr>
<tr>
<td>3211</td>
<td>An error occurred with the API for McAfee SaaS Web Protection, for example, a mismatch of the API version.</td>
<td>3 Web Hybrid</td>
<td>3</td>
</tr>
<tr>
<td>3250</td>
<td>Status of synchronization with McAfee SaaS Web Protection is OK.</td>
<td>3 Web Hybrid</td>
<td>6</td>
</tr>
<tr>
<td>3300</td>
<td>The list for Web Service Access is not available for an unknown reason.</td>
<td>2 Web Hybrid</td>
<td>2</td>
</tr>
<tr>
<td>3301</td>
<td>The list for Web Service Access does not exist.</td>
<td>2 Web Hybrid</td>
<td>2</td>
</tr>
<tr>
<td>3302</td>
<td>The settings for Web Service Access are not available for an unknown reason.</td>
<td>2 Web Hybrid</td>
<td>2</td>
</tr>
<tr>
<td>3303</td>
<td>The settings for Web Service Access do not exist.</td>
<td>2 Web Hybrid</td>
<td>2</td>
</tr>
<tr>
<td>3400</td>
<td>A policy could not be synchronized to McAfee SaaS Web Protection.</td>
<td>8 SaaS Connector</td>
<td>3</td>
</tr>
<tr>
<td>3500</td>
<td>The Protocol Detector rule set could not be found and loaded.</td>
<td>2 Protocol Detector Filter</td>
<td>2</td>
</tr>
<tr>
<td>3501</td>
<td>The Protocol Detector rule set was broken or corrupt and could not be loaded.</td>
<td>2 Protocol Detector Filter</td>
<td>2</td>
</tr>
</tbody>
</table>
List of properties

The following tables provides a list of the properties you can use in rules.

Order of properties

The properties are listed in alphabetical order. However, the listing takes into consideration the parts of the property names. Name parts begin with a capital letter, in many cases they are also separated by periods.

For example, `Body.HasMimeHeaderParameter` is listed before `Body.Hash`.

There are no properties with names that begin with K, O, V, X, Y, or Z.

Properties in context

You can easily find out about the rules and rule sets that use a property.

1. On the user interface, click Search, and under Search for objects referring to, select Property and the property you are interested in.

   The rules that use the property are shown. For example, for Antimalware.Infected, the rule Block if virus was found is shown.

2. Select a rule and click Show in context.

   The rule and the property are shown within its rule set. For example, the rule for Antimalware.Infected is shown within the Gateway Anti-Malware rule set.

Properties - A

The following table describes the properties that have names beginning with A.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action.Names</td>
<td>List of String</td>
<td>List with names of the actions that were performed when processing a request, including the response received upon the request</td>
<td></td>
</tr>
<tr>
<td>Antimalware.Avira.VersionString</td>
<td>String</td>
<td>Version of the Avira engine that was used to perform a scanning job</td>
<td></td>
</tr>
<tr>
<td>Antimalware.Infected</td>
<td>Boolean</td>
<td>If true, a web object has been found to be infected.</td>
<td></td>
</tr>
<tr>
<td>Antimalware.Proactive.Probability</td>
<td>Number</td>
<td>Probability that a web object is malware</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The probability is a percentage, indicated by a number from 1 to 100.</td>
<td></td>
</tr>
<tr>
<td>Antimalware.MATD.GetReport</td>
<td>Boolean</td>
<td>If true, a scanning report exists already for a web object that is to be scanned by Advanced Threat Defense.</td>
<td></td>
</tr>
<tr>
<td>Antimalware.MATD.Hash</td>
<td>String</td>
<td>Hash value used to identify a file that was received from a web server in response to a download request and scanned by Advanced Threat Defense.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameter</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Antimalware.MATD.InitBackgroundScan</td>
<td>Boolean</td>
<td>If true, data for the current transaction is recorded, including data that is related to a request for web access and the response from the web server. The data is recorded in preparation of the scanning that is performed by Advanced Threat Defense when the web object that should be scanned has already been forwarded to the user who requested it. An internal request is also sent to initiate the scanning. If this request is not accepted before the timeout (in seconds) has elapsed that is configured as a parameter of the property, the attempt to let additional scanning be performed by Advanced Threat Defense has failed.</td>
<td>Number:</td>
</tr>
<tr>
<td>Antimalware.MATD.IsBackgroundScan</td>
<td>Boolean</td>
<td>If true, the data that was recorded in preparation of the additional scanning is used by Advanced Threat Defense to scan the web object specified by the data.</td>
<td></td>
</tr>
<tr>
<td>Antimalware.MATD.Probability</td>
<td>Number</td>
<td>Severity grade indicating how malicious a web object is on a scale from 1 (low severity grade) to 5 The severity grade is found when an object is scanned by Advanced Threat Defense.</td>
<td></td>
</tr>
<tr>
<td>Antimalware.MATD.Report</td>
<td>String</td>
<td>Report for a web object that was scanned by Advanced Threat Defense The report is provided in JSON data format.</td>
<td></td>
</tr>
<tr>
<td>Antimalware.MATD.Server</td>
<td>String</td>
<td>Server that Advanced Threat Defense was running on when scanning a web object The server is identified by a URL, for example, <a href="http://matdserver300">http://matdserver300</a>.</td>
<td></td>
</tr>
<tr>
<td>Antimalware.MATD.TaskID</td>
<td>String</td>
<td>Identifier for the task that was performed by Advanced Threat Defense when scanning a web object</td>
<td></td>
</tr>
<tr>
<td>Antimalware.MATD.VersionString</td>
<td>String</td>
<td>Version of Advanced Threat Defense that was used to perform a scanning job</td>
<td></td>
</tr>
<tr>
<td>Antimalware.MGAM.VersionString</td>
<td>String</td>
<td>Version of the McAfee Gateway Anti-Malware engine that was used to perform a scanning job</td>
<td></td>
</tr>
<tr>
<td>Antimalware.VersionString</td>
<td>String</td>
<td>Version information referring to all engines for virus and malware filtering that were used by Web Gateway to perform a scanning job</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Antimalware.VirusNames</td>
<td>List of String</td>
<td>List with names of the viruses that a web object has been found to be infected with</td>
<td></td>
</tr>
<tr>
<td>AnyText.Language</td>
<td>String</td>
<td>Name of the language that a given text is written in The languages are identified according to ISO-639-1.</td>
<td></td>
</tr>
<tr>
<td>Application.IsHighRisk</td>
<td>Boolean</td>
<td>If true, access to an application is considered to be a high risk for web security.</td>
<td></td>
</tr>
<tr>
<td>Application.IsMediumRisk</td>
<td>Boolean</td>
<td>If true, access to an application is considered to be a medium risk for web security.</td>
<td></td>
</tr>
<tr>
<td>Application.IsMinimalRisk</td>
<td>Boolean</td>
<td>If true, access to an application is considered to be a minimal risk for web security.</td>
<td></td>
</tr>
<tr>
<td>Application.IsUnverified</td>
<td>Boolean</td>
<td>If true, it has not been verified that access to an application is a risk for web security</td>
<td></td>
</tr>
<tr>
<td>Application.Name</td>
<td>Applcontrol</td>
<td>Name of an application</td>
<td></td>
</tr>
<tr>
<td>Application.Reputation</td>
<td>Number</td>
<td>Reputation score for an application</td>
<td>Applname</td>
</tr>
<tr>
<td>Application.ToString</td>
<td>String</td>
<td>Name of an application converted into a string</td>
<td>Applname</td>
</tr>
<tr>
<td>Authentication.Authenticate</td>
<td>Boolean</td>
<td>If true, the authentication engine has been called to apply the configured method, for example, NTLM, to the credentials of a user and the user has been authenticated successfully. Values have also been set for the Authentication.IsAuthenticated and Authentication.UserName properties. If false, it was not possible to apply the configured authentication method successfully, for example, because no credentials or incorrect credentials were submitted.</td>
<td></td>
</tr>
<tr>
<td>Authentication.CacheRemainingTime</td>
<td>Number</td>
<td>Time (in seconds) that remains until authentication credentials are cleared from the cache</td>
<td></td>
</tr>
<tr>
<td>Authentication.Failed</td>
<td>Boolean</td>
<td>If true, credentials were provided by a user, but authentication has failed.</td>
<td></td>
</tr>
<tr>
<td>Authentication.FailureReason.ID</td>
<td>Number</td>
<td>Number identifying the reason why authentication has failed for a user</td>
<td></td>
</tr>
<tr>
<td>Authentication.FailureReason.Message</td>
<td>String</td>
<td>Message text explaining the reason why authentication has failed for a user</td>
<td></td>
</tr>
<tr>
<td>Authentication.GetUserGroups</td>
<td>List of String</td>
<td>List of user groups that the authentication process is applied to</td>
<td></td>
</tr>
</tbody>
</table>
### Table A-6 Properties – A (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication.GetUserGroups.JSON</td>
<td>JSON</td>
<td>List of user groups that the authentication process is applied to provided as a JSON object</td>
<td></td>
</tr>
<tr>
<td>Authentication.ICEToken.Attributes</td>
<td>List</td>
<td>List of additional attributes that are retrieved from an ICE token</td>
<td></td>
</tr>
<tr>
<td>Authentication.ICEToken.Audiences</td>
<td>List</td>
<td>List of audiences that are retrieved from an ICE token</td>
<td></td>
</tr>
<tr>
<td>Authentication.ICEToken.Subject</td>
<td>String</td>
<td>Subject that is retrieved from an ICE token</td>
<td></td>
</tr>
<tr>
<td>Authentication.IsAuthenticated</td>
<td>Boolean</td>
<td>If true, a user has been successfully authenticated.</td>
<td></td>
</tr>
<tr>
<td>Authentication.IsLandingOnServer</td>
<td>Boolean</td>
<td>If true, cookie authentication has been applied for a user.</td>
<td></td>
</tr>
<tr>
<td>Authentication.IsServerRequest</td>
<td>Boolean</td>
<td>If true, authentication has been requested for a user under the Authentication Server method.</td>
<td></td>
</tr>
<tr>
<td>Authentication.Method</td>
<td>String</td>
<td>Method used for authenticating a user, for example, LDAP</td>
<td></td>
</tr>
<tr>
<td>Authentication.OTP.Context</td>
<td>String</td>
<td>Information required for verifying a one-time password user in encrypted format</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The property is set to this value when the Authentication.SendOTP event is executed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>When the rules of the Authentication Server (Time/IP Based Session or Authorized Override with OTP library rule sets are processed, the information is sent in the header of a response under the HTTP protocol.</td>
<td></td>
</tr>
<tr>
<td>Authentication.RawCredentials</td>
<td>String</td>
<td>Credentials of a user in the format originally received on the appliance from a client or other instances of the network</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using this property for rule configuration will speed up processing because it saves the time used for converting user credentials to a human readable format, as it is done for the simple Authentication.UserName property.</td>
<td></td>
</tr>
<tr>
<td>Authentication.RawUserName</td>
<td>String</td>
<td>Name of a user in the format originally received on the appliance from a client or other instances of the network</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using this property for rule configuration will speed up processing because it saves the time used for converting the user name to a human readable format, as it is done for the simple Authentication.UserName property.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Authentication.Realm</td>
<td>String</td>
<td>Authentication realm, for example, a Windows domain</td>
<td></td>
</tr>
<tr>
<td>Authentication.SAML.Attributes</td>
<td>List of String</td>
<td>Stores a list of attribute name-value pairs extracted from the <a href="">saml2:Attribute</a> tag in the SAML response. When there are multiple values for one attribute name, the values are separated by commas.</td>
<td></td>
</tr>
<tr>
<td>Authentication.SAML.CreateAuthnRequest</td>
<td>HTTP POST form</td>
<td>Creates the SAML authentication request which is sent to the external Identity Provider and sets the Authentication.SAML.IDPSSOEndpoint property to the URL of the external Identity Provider.</td>
<td></td>
</tr>
<tr>
<td>Authentication.SAML.Error</td>
<td>String</td>
<td>Describes the error that occurred when the authentication server failed to validate the SAML response.</td>
<td>Errors messages are provided by the OpenSAML library.</td>
</tr>
<tr>
<td>Authentication.SAML.IDPSSOEndpoint</td>
<td>String</td>
<td>Specifies the SSO URL of the external Identity Provider. If an error occurs, the user is redirected to this URL.</td>
<td></td>
</tr>
<tr>
<td>Authentication.SAML.ParseAuthnResponse</td>
<td>String</td>
<td>Parses the SAML authentication response that is received from the external Identity Provider. If the response is valid, this property returns a list of attribute name-value pairs in the Authentication.SAML.Attributes property. If the response is invalid, this property returns an error in the property Authentication.SAML.Error.</td>
<td></td>
</tr>
<tr>
<td>Authentication.SAML.RelayState</td>
<td>String</td>
<td>Stores the value of the ACS URL at the time that the authentication server creates the SAML authentication request. The authentication server sends the RelayState parameter to the external Identity Provider in the authentication request. The Identity Provider returns the parameter unchanged in the authentication response. The proxy can use the value stored in the RelayState to construct the ACS URL when the external Identity Provider does not support dynamic URLs.</td>
<td></td>
</tr>
<tr>
<td>Authentication.SOCKSKerberosProtectionLevelToken</td>
<td>Number</td>
<td>Number representing the protection level that is used when the SOCKS Kerberos authentication method is configured</td>
<td></td>
</tr>
<tr>
<td>Authentication.Token</td>
<td>String</td>
<td>Stores the SAML assertion returned by the external Identity Provider.</td>
<td></td>
</tr>
</tbody>
</table>
### Table A-6 Properties – A (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication.UserGroups</td>
<td>List of string</td>
<td>List of user groups that the authentication process is applied to</td>
<td></td>
</tr>
<tr>
<td>Authentication.UserName</td>
<td>String</td>
<td>Name of a user that the authentication process is applied to</td>
<td></td>
</tr>
</tbody>
</table>

### Properties - B

The following table describes the properties that have names beginning with B.

### Table A-7 Properties – B

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block.ID</td>
<td>Number</td>
<td>ID of an action that blocked a request</td>
<td></td>
</tr>
<tr>
<td>Block.Reason</td>
<td>String</td>
<td>Name of the reason for an action that blocked a request</td>
<td></td>
</tr>
<tr>
<td>BlockingSession.IsBlocked</td>
<td>Boolean</td>
<td>If true, a blocking session has been activated for a user.</td>
<td></td>
</tr>
<tr>
<td>BlockingSession.RemainingSession</td>
<td>Number</td>
<td>Remaining time of a blocking session (in minutes)</td>
<td></td>
</tr>
<tr>
<td>BlockingSession.SessionLength</td>
<td>Number</td>
<td>Time length of a blocking session (in minutes)</td>
<td></td>
</tr>
<tr>
<td>Body.ChangeHeaderMime</td>
<td>Boolean</td>
<td>If true, the header sent in MIME format with the body of a web object has been changed.</td>
<td></td>
</tr>
<tr>
<td>Body.ClassID</td>
<td>String</td>
<td>ID for a class of web objects</td>
<td></td>
</tr>
<tr>
<td>Body.Equals</td>
<td>Boolean</td>
<td>If true, the body of a web object matches the pattern specified by the property parameters.</td>
<td>1 Number: Position of byte where pattern begins 2 String: Pattern a. String embedded in double quotes (“ ...”, can also contain hex values preceded by ) or: b. Sequence of hex values</td>
</tr>
<tr>
<td>Body.FileName</td>
<td>String</td>
<td>Name of a file that is embedded in the body of a web object, for example, an archived file</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Body.FullFileName</td>
<td>String</td>
<td>Name of a file that is embedded in the body of a web object, including also the names of the embedding entities, such as documents or archives. Name parts are separated by the</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Body.HasMimeHeader</td>
<td>Boolean</td>
<td>If true, the body of an extracted multi-part object sent in MIME format has a specified header.</td>
<td></td>
</tr>
<tr>
<td>Body.HasMimeHeaderParameter</td>
<td>Boolean</td>
<td>If true, the body of an extracted multi-part object sent in MIME format has a specified header parameter.</td>
<td>1 String: Header name 2 String: Header parameter name</td>
</tr>
<tr>
<td>Body.Hash</td>
<td>String</td>
<td>Hash value of the type specified by the property parameter for the body of a web object. Hash types can be md5, sha1, sha256, sha512, and others.</td>
<td>String: Hash type</td>
</tr>
<tr>
<td>Body.IsAboveSizeLimit</td>
<td>Boolean</td>
<td>If true, the body of a web object is above a size limit.</td>
<td></td>
</tr>
<tr>
<td>Body.IsCompleteWithTimeout</td>
<td>Boolean</td>
<td>If true, the body of a web object has been completely sent to the appliance before the time (in milliseconds) specified by the property parameter has elapsed.</td>
<td>Number: Time allowed to send object completely</td>
</tr>
<tr>
<td>Body.IsCorruptedObject</td>
<td>Boolean</td>
<td>If true, an archive contained in the body of a web object is corrupted.</td>
<td></td>
</tr>
<tr>
<td>Body.IsEncryptedObject</td>
<td>Boolean</td>
<td>If true, an archive contained in the body of a web object is encrypted.</td>
<td></td>
</tr>
<tr>
<td>Body.IsMultiPartObject</td>
<td>Boolean</td>
<td>If true, an archive contained in the body of a web object is complex, including multiple parts.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Body.IsSupportedByOpener</td>
<td>Boolean</td>
<td>If true, an opener device is available on the appliance for the body of a web object that is composite, for example, the body of an archive.</td>
<td></td>
</tr>
<tr>
<td>Body.MimeHeaderParameter1Value</td>
<td>String</td>
<td>Value of a header parameter in the body of a web object sent in MIME format</td>
<td>1 String: Header name&lt;br&gt;2 String: Header parameter value</td>
</tr>
<tr>
<td>Body.MimeHeaderValue</td>
<td>String</td>
<td>Value of a header in the body of a web object sent in MIME format</td>
<td>String: Header value</td>
</tr>
<tr>
<td>Body.Modified</td>
<td>Boolean</td>
<td>If true, an appliance module has modified the body of a web object.</td>
<td></td>
</tr>
<tr>
<td>Body.NestedArchive Level</td>
<td>Number</td>
<td>Current level of an archive part in an archive</td>
<td></td>
</tr>
<tr>
<td>Body.NotEquals</td>
<td>Boolean</td>
<td>If false, the body of a web object matches the pattern specified by the property parameters.</td>
<td>1 Number: Position of byte where pattern begins&lt;br&gt;2 String: Pattern&lt;br&gt;a. String embedded in double quotes (“ ...”, can also contain hex values preceded by )&lt;br&gt;or:&lt;br&gt;b. Sequence of hex values</td>
</tr>
<tr>
<td>Body.NumberOfChildren</td>
<td>Number</td>
<td>Number of objects embedded in the body of a web object</td>
<td></td>
</tr>
<tr>
<td>Body.PositionOfPattern</td>
<td>Number</td>
<td>Position of the byte where the search for a pattern in the body of a web object begins. Returns -1 if the pattern is not found.</td>
<td>1 String: Pattern to search for&lt;br&gt;a. String embedded in double quotes (“ ...”, can also contain hex values preceded by )&lt;br&gt;or:&lt;br&gt;b. Sequence of hex values&lt;br&gt;2 Number: Position of byte where search for pattern begins&lt;br&gt;3 Number: Search length (in bytes, 0 means search from offset to end of object)</td>
</tr>
<tr>
<td>Body.Size</td>
<td>Number</td>
<td>Size of the body of a web object (in bytes)</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Body.Text</td>
<td>String</td>
<td>Text in the body of a web object</td>
<td></td>
</tr>
<tr>
<td>Body.ToNumber</td>
<td>Number</td>
<td>Part of the body of a web object converted into a number (maximum 8 bytes beginning at a specified position)</td>
<td>1 Number: Position of byte where converted part begins</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Length of converted part (in bytes, maximum 8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 for the first parameter and the respective value of the Body.Size property for the second means the whole body is converted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Boolean: If true, little-endian format is used for conversion, otherwise big-endian</td>
</tr>
<tr>
<td>Body.ToString</td>
<td>String</td>
<td>Part of the body of a web object converted into a string</td>
<td>1 Number: Position of byte where converted part begins</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Length of converted part (in bytes)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 for the first parameter and the respective value of the Body.Size property for the second means the whole body is converted.</td>
</tr>
<tr>
<td>Body.UncompressedSize</td>
<td>Number</td>
<td>Size of the body of an archived web object (in bytes) after having been extracted from the archive</td>
<td></td>
</tr>
<tr>
<td>BooleanToString</td>
<td>String</td>
<td>Boolean value converted into a string</td>
<td>Boolean: Boolean value to convert</td>
</tr>
<tr>
<td>BytesFromClient</td>
<td>Number</td>
<td>Number of bytes received in a request from a client</td>
<td></td>
</tr>
<tr>
<td>BytesFromServer</td>
<td>Number</td>
<td>Number of bytes received in a response from a web server</td>
<td></td>
</tr>
<tr>
<td>BytesToClient</td>
<td>Number</td>
<td>Number of bytes in a web server response that is forwarded to a client</td>
<td></td>
</tr>
<tr>
<td>BytesToServer</td>
<td>Number</td>
<td>Number of bytes in a client request that is forwarded to a web server</td>
<td></td>
</tr>
</tbody>
</table>
Properties - C
The following table describes the properties that have names beginning with C.

**Table A-8  Properties – C**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache.IsCacheable</td>
<td>Boolean</td>
<td>If true, an object sent in response from a web server can be stored in the web cache.</td>
<td></td>
</tr>
<tr>
<td>Cache.IsFresh</td>
<td>Boolean</td>
<td>If true, an object stored in the web cache has either been downloaded from the web or has been verified.</td>
<td></td>
</tr>
<tr>
<td>Cache.Status</td>
<td>String</td>
<td>Cache status for a web object</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>TCP_HIT</strong> – A web object was requested by a user and found in the cache.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>TCP_MISS</strong> – A web object was requested by a user and not found in the cache.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>TCP_MISS_RELOAD</strong> – A web object was requested by a user, but was not taken from the cache because the user required it to be fetched directly from the web server in question by clicking the Refresh button. The object was then entered into the cache again.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>TCP_MISS_VERIFY</strong> – A web object was requested by a user and existed in the cache, but verification information from the web server in question showed it was outdated. An updated version of the object was received from the server and entered into the cache.</td>
<td></td>
</tr>
<tr>
<td>Category.ToShortString</td>
<td>String</td>
<td>URL category converted into a string that is the category abbreviation</td>
<td></td>
</tr>
<tr>
<td>Category.ToString</td>
<td>String</td>
<td>URL category converted into a string</td>
<td></td>
</tr>
<tr>
<td>Client.IM.Login</td>
<td>String</td>
<td>ID used by a client to log on to the appliance under an instant messaging protocol</td>
<td></td>
</tr>
<tr>
<td>Client.IM.ScreenName</td>
<td>String</td>
<td>Screen name of of a client communicating with the appliance under an instant messaging protocol</td>
<td></td>
</tr>
<tr>
<td>Client.IP</td>
<td>IP</td>
<td>IP address of a client</td>
<td></td>
</tr>
<tr>
<td>Client.NumberOfConnections</td>
<td>Number</td>
<td>Number of connections from a client to the appliance that are open at the same time</td>
<td></td>
</tr>
</tbody>
</table>
Table A-8 Properties – C (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudEncryption.IsEncryptionSupported</td>
<td>Boolean</td>
<td>If true, encryption can be performed for the data that is uploaded to a cloud storage service with the request that is currently processed. The Cloud Storage Encryption module finds out whether this is true by evaluating service description files for cloud storage services and the settings that are configured on Web Gateway, for example, the Cloud Storage Encryption Support settings, which specify the supported cloud storage services.</td>
<td></td>
</tr>
<tr>
<td>CloudEncryption.IsDecryptionSupported</td>
<td>Boolean</td>
<td>If true, decryption can be performed for the data that is downloaded from a cloud storage service with the request that is currently processed. For the method of finding out whether this is true, see the description of the CloudEncryption.IsEncryptionSupported property.</td>
<td></td>
</tr>
<tr>
<td>CloudEncryption.ServiceName</td>
<td>String</td>
<td>Name of the cloud storage service that data is uploaded to or downloaded from with the request that is currently processed. The property is always filled with a value when request are received on Web Gateway for uploading or downloading cloud storage data. However, the property should not be used in rule criteria to trigger an encryption or decryption event upon a match of the criteria. For this purpose, the CloudEncryption.IsEncryptionSupported and CloudEncryption.IsDecryptionSupported properties are provided.</td>
<td></td>
</tr>
<tr>
<td>CloudEncryption.CipherName</td>
<td>String</td>
<td>Name of the algorithm (cipher) used for encrypting or decrypting the cloud storage data that is uploaded or downloaded with the request that is currently processed.</td>
<td></td>
</tr>
<tr>
<td>Command.Categories</td>
<td>List of String</td>
<td>List of categories that a command belongs to, for example, to the FTP command category</td>
<td></td>
</tr>
<tr>
<td>Command.Name</td>
<td>String</td>
<td>Name of a command</td>
<td></td>
</tr>
<tr>
<td>Command.Parameter</td>
<td>String</td>
<td>Parameter of a command</td>
<td></td>
</tr>
<tr>
<td>Connection.Aborted</td>
<td>Boolean</td>
<td>If true, communication on a connection has finally failed and the connection is closed.</td>
<td></td>
</tr>
</tbody>
</table>
## Properties – C (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection.IP</td>
<td>IP</td>
<td>IP address used on a connection</td>
<td></td>
</tr>
<tr>
<td>Connection.OriginalDestinationIP</td>
<td>IP</td>
<td>IP address of the destination that a request was originally sent to over a given connection</td>
<td></td>
</tr>
<tr>
<td>Connection.Port</td>
<td>Number</td>
<td>Port number of the port that a request sent by a client over a given connection is received on</td>
<td></td>
</tr>
<tr>
<td>Connection.Protocol</td>
<td>String</td>
<td>Protocol used for communication on a connection, for example, HTTP</td>
<td></td>
</tr>
<tr>
<td>Connection.Protocol.IsIM</td>
<td>Boolean</td>
<td>If true, communication on a connection uses an instant messaging protocol.</td>
<td></td>
</tr>
<tr>
<td>Connection.Protocol.Parent</td>
<td>String</td>
<td>The embedding protocol for the protocols that are used in communication with the clients when Web Gateway runs as a proxy under the SOCKS protocol. This protocol is the SOCKS protocol, while various protocols can be embedded, for example, HTTP or HTTPS.</td>
<td></td>
</tr>
<tr>
<td>Connection.RunTime</td>
<td>Number</td>
<td>Time (in seconds) that a connection has been running since it was opened until the current second</td>
<td></td>
</tr>
<tr>
<td>Connection.SSL.TransparentCNHandling</td>
<td>Boolean</td>
<td>If true, communication on a connection is SSL-secured and runs in transparent mode.</td>
<td></td>
</tr>
<tr>
<td>Connection.VlanID</td>
<td>Number</td>
<td>VLAN ID of the network that a client uses to communicate with Web Gateway</td>
<td></td>
</tr>
<tr>
<td>Cycle.LastCall</td>
<td>Boolean</td>
<td>If true, processing of data is complete for a cycle.</td>
<td></td>
</tr>
<tr>
<td>Cycle.Name</td>
<td>String</td>
<td>Name of a processing cycle</td>
<td></td>
</tr>
<tr>
<td>Cycle.TopName</td>
<td>String</td>
<td>Name of a cycle (Requests or Responses) that is processed before a web object is processed in the Embedded Objects cycle</td>
<td></td>
</tr>
</tbody>
</table>

### Properties - D

The following table describes the properties that have names beginning with D.

## Table A-9 Properties – D

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataTrickling.Enabled</td>
<td>Boolean</td>
<td>If true, data trickling is used for downloading web objects.</td>
<td></td>
</tr>
<tr>
<td>DateTime.Date.MonthDayNumber</td>
<td>Number</td>
<td>Number of day in month</td>
<td></td>
</tr>
<tr>
<td>DateTime.Date.MonthNumber</td>
<td>Number</td>
<td>Number of month</td>
<td></td>
</tr>
</tbody>
</table>
**Table A-9  Properties – D (continued)**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>DateTime.Date.ToString</td>
<td>String</td>
<td>String representing current date (in the format specified by the property parameters)</td>
<td>String including the following three parts:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1  1. %YYYY (for the year)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>%YY (last two digits)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>%Y (last two digits, but only one digit if the last two digits begin with 0, for example, 9 for 2009)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2  %MM (for the month number with 0 inserted before one-digit numbers)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>%M (0 is not inserted, for example, 3 for March and 12 for December)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3  %DD (for the day)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>or:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>%D</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If no parameter is specified, the format is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>%YYYY/%MM /%DD</td>
</tr>
<tr>
<td>DateTime.Date.WeekDayNumber</td>
<td>Number</td>
<td>Number of day in week (1 is Sunday)</td>
<td></td>
</tr>
<tr>
<td>DateTime.Date.Year</td>
<td>Number</td>
<td>Year (four digits)</td>
<td></td>
</tr>
<tr>
<td>DateTime.Date.YearTwoDigits</td>
<td>Number</td>
<td>Year (last two digits)</td>
<td></td>
</tr>
<tr>
<td>DateTime.Time.Hour</td>
<td>Number</td>
<td>Hour (in 24-hours format, for example, 1 p. m. is 13)</td>
<td></td>
</tr>
<tr>
<td>DateTime.Time.Minute</td>
<td>Number</td>
<td>Minute in hour</td>
<td></td>
</tr>
<tr>
<td>DateTime.Time.Second</td>
<td>Number</td>
<td>Second in minute</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| DateTime.Time.ToString        | String  | String representing current time (in the format specified by the property parameters) | String including the following three parts:  
1 %h (for the hour)  
   or:  
   %hh (with 0 inserted before a one-digit hour)  
2 %m (for the minute)  
   or:  
   %mm  
3 %s (for the second)  
   or:  
   %ss  
If no parameter is specified, the format is:  
%hh:%mm:%ss |
| DateTime.ToGMTString          | String  | String representing current date and time in Greenwich Mean Time format   | For example, “Mon, 22 March 2012 11:45:36 GMT”                               |
| DateTime.ToISOString          | String  | String representing current date and time in ISO format                   | For example, “2012-03-22 11:45:12”                                            |
| DateTime.ToNumber             | Number  | Number of seconds since beginning of 1/1/1970 (UNIX epoch time)           |                                                                            |
| DateTime.ToString             | String  | String representing current date and time (in the format specified by the property parameters) | String including the part of the DateTime.Date.ToString and DateTime.Time.ToString properties  
If no parameter is specified, the format is:  
%YYYY/%MM/%DD  
%hh:%mm:%ss |
<p>| DateTime.ToWebReporterString  | String  | String representing current date and time in Web Reporter format           | For example, “29/Oct/2012:14:28:15 +0000”                                      |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>DecimalNumber.ToString</td>
<td>String</td>
<td>Decimal number converted to a string</td>
<td>1 Number: Decimal number to convert</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The string is truncated according to a parameter.</td>
<td>2 Number: Number of places after the decimal point</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, 10.12345 is truncated to 10.12 if this parameter is 2.</td>
<td></td>
</tr>
<tr>
<td>Dimension.ToString</td>
<td>String</td>
<td>Dimension converted into a string</td>
<td>Dimension: Dimension to convert</td>
</tr>
<tr>
<td>DLP.Classification.AnyText.Matched</td>
<td>Boolean</td>
<td>If true, a given text string is specified as sensitive or inappropriate content by one or more entries in classification lists.</td>
<td>String: Text checked for being sensitive or inappropriate</td>
</tr>
<tr>
<td>DLP.Classification.AnyText.MatchedClassifications</td>
<td>List of String</td>
<td>List of entries in classification lists that specify a given text string as sensitive or inappropriate</td>
<td>String: Text checked for being sensitive or inappropriate</td>
</tr>
<tr>
<td>DLP.Classification.AnyText.MatchedTerms</td>
<td>List of String</td>
<td>List of terms including a given text string that is specified as sensitive or inappropriate by one or more entries in classification lists.</td>
<td>String: Text checked for being sensitive or inappropriate</td>
</tr>
<tr>
<td>DLP.Classification.BodyText.Matched</td>
<td>Boolean</td>
<td>If true, the text of a request or response body includes content that is specified as sensitive or inappropriate by one or more entries in classification lists.</td>
<td></td>
</tr>
<tr>
<td>DLP.Classification.BodyText.MatchedClassifications</td>
<td>List of String</td>
<td>List of entries in classification lists that specify the sensitive or inappropriate content found in the body text of requests or responses</td>
<td></td>
</tr>
<tr>
<td>DLP.Classification.BodyText.MatchedTerms</td>
<td>List of String</td>
<td>List of terms in request or response body text that are sensitive or inappropriate content according to one or more entries in classification lists.</td>
<td></td>
</tr>
</tbody>
</table>
### Table A-9  Properties – D (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP.Dictionary.AnyText.Matched</td>
<td>Boolean</td>
<td>If true, a given text string is specified as sensitive or inappropriate content on a dictionary list.</td>
<td>String: Text checked for being sensitive or inappropriate</td>
</tr>
<tr>
<td>DLP.Dictionary.AnyText.MatchedTerms</td>
<td>List of String</td>
<td>List of terms including a given text string that is specified as sensitive or inappropriate on a dictionary list</td>
<td>String: Text checked for being sensitive or inappropriate</td>
</tr>
<tr>
<td>DLP.Dictionary.BodyText.Matched</td>
<td>Boolean</td>
<td>If true, the text of a request or response body includes content that is specified as sensitive or inappropriate by an entry you made in a dictionary list.</td>
<td></td>
</tr>
<tr>
<td>DLP.Dictionary.BodyText.MatchedTerms</td>
<td>List of String</td>
<td>List of the terms in request or response body text that are sensitive or inappropriate content according to the entries you made in a dictionary list</td>
<td>String: Text checked for being sensitive or inappropriate</td>
</tr>
<tr>
<td>DNS.Lookup</td>
<td>List of IP</td>
<td>List of IP addresses found in a DNS lookup for a host name</td>
<td>String: Host name</td>
</tr>
<tr>
<td>DNS.Lookup.Reverse</td>
<td>List of String</td>
<td>List of host names found in a reverse DNS lookup for an IP address</td>
<td>IP: IP address</td>
</tr>
<tr>
<td>DXL.Query</td>
<td>String</td>
<td>Information retrieved about a topic by sending a DXL query to a service</td>
<td>1 String: Topic that the query is about</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 String: Information about the topic that the query retrieves as response</td>
</tr>
</tbody>
</table>

### Properties - E

The following table describes the properties that have names beginning with E.

### Table A-10  Properties – E

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error.ID</td>
<td>Number</td>
<td>ID of an error</td>
<td></td>
</tr>
<tr>
<td>Error.Message</td>
<td>String</td>
<td>Message text describing an error</td>
<td></td>
</tr>
</tbody>
</table>
Table A-10 Properties – E (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExtLists.Boolean</td>
<td>Boolean</td>
<td>Boolean value</td>
<td>1 String: Value holding the place of a term that identifies an external list source, for example, in a URL</td>
</tr>
<tr>
<td>String: Value holding the place of a term that identifies an external list source, for example, in a URL</td>
<td>2 String: as above</td>
<td></td>
<td></td>
</tr>
<tr>
<td>String: as above</td>
<td>3 String: as above</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ExtLists.Category</td>
<td>Category</td>
<td>URL category</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.CategoryList</td>
<td>List of Category</td>
<td>List of URL categories</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.Double</td>
<td>Double</td>
<td>Double value</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.DoubleList</td>
<td>List of Double</td>
<td>List of Double values</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.Integer</td>
<td>Integer</td>
<td>Integer</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.IntegerList</td>
<td>List of Integer</td>
<td>List of integers</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.IP</td>
<td>IP</td>
<td>IP address</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.IPList</td>
<td>List of IP</td>
<td>List of IP addresses</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.IPRange</td>
<td>IPRange</td>
<td>IP address range</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.IPRangeList</td>
<td>List of IPRange</td>
<td>List of IP address ranges</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.JSON</td>
<td>JSON</td>
<td>List of JSON elements</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.LastUsedListName</td>
<td>String</td>
<td>String representing name of settings for the External Lists module that were used last</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.MediaType</td>
<td>MediaType</td>
<td>Media type</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.MediaTypeList</td>
<td>List of MediaType</td>
<td>List of media types</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.String</td>
<td>String</td>
<td>String</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.StringList</td>
<td>List of String</td>
<td>List of strings</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.StringMap</td>
<td>List of String</td>
<td>List of strings representing map type pairs of keys and values</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.Wildcard</td>
<td>Wildcard Expression</td>
<td>Wildcard (regular) expression</td>
<td>as above</td>
</tr>
<tr>
<td>ExtLists.WildcardList</td>
<td>List of Wildcard Expression</td>
<td>List of wildcard (regular) expressions</td>
<td>as above</td>
</tr>
</tbody>
</table>

Properties - F

The following table describes the properties that have names beginning with F.

Table A-11 Properties – F

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileSystemLogging.MakeAnonymous</td>
<td>String</td>
<td>String made anonymous by encryption</td>
<td>String: String to encrypt</td>
</tr>
</tbody>
</table>
**Properties - G**

The following table describes the properties that have names beginning with G.

**Table A-12 Properties – G**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTI.RequestSentToCloud</td>
<td>Boolean</td>
<td>If true, a lookup request for URL category information was sent to the Global Threat Intelligence server.</td>
<td></td>
</tr>
</tbody>
</table>

**Properties - H**

The following table describes the properties that have names beginning with H.

**Table A-13 Properties – H**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header.Block.Exists</td>
<td>Boolean</td>
<td>If true, a specified block header exists.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.Block.Get</td>
<td>String</td>
<td>First value found for a specified block header</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.Block.GetMultiple</td>
<td>List of String</td>
<td>List of values found for a specified block header</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.Exists</td>
<td>Boolean</td>
<td>If true, a specified header is contained in a request or response that is processed on the appliance. It depends on the current processing cycle whether it is actually a request or response that contains the header.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.Get</td>
<td>String</td>
<td>First value found for the specified header in a request or response that is processed on the appliance. It depends on the current processing cycle whether it is actually a request or response that contains the header.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.GetMultiple</td>
<td>List of String</td>
<td>List of values found for a specified header in a request or response that is processed on the appliance. It depends on the current processing cycle whether it is actually a request or response that contains the header.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.ICAP.Request.Exists</td>
<td>Boolean</td>
<td>If true, a specified header is contained in a request sent in ICAP communication.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.ICAP.Request.Get</td>
<td>String</td>
<td>First value found for a specified header in a request sent in ICAP communication</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.ICAP.Response.Equals</td>
<td>Boolean</td>
<td>If true, a specified header is contained in a response received in ICAP communication.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.ICAP.Response.Get</td>
<td>String</td>
<td>First value found for a specified header in a response received in ICAP communication.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.Request.Exists</td>
<td>Boolean</td>
<td>If true, a specified header is contained in a request.</td>
<td>String: Header name</td>
</tr>
</tbody>
</table>
Table A-13 Properties – H (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header.Request.Get</td>
<td>String</td>
<td>First value found for a specified header in a request</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.Request.GetMultiple</td>
<td>List of String</td>
<td>List of values found for a specified header in a request</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.Response.Exists</td>
<td>Boolean</td>
<td>If true, a specified header is contained in a response.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.Response.Get</td>
<td>String</td>
<td>First value found for a specified header in a response</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Header.Response.GetMultiple</td>
<td>List of String</td>
<td>List of values found for a specified header in a response</td>
<td>String: Header name</td>
</tr>
<tr>
<td>Hex.ToString</td>
<td>String</td>
<td>Hex value converted into a string</td>
<td>Hex: Hex value to convert</td>
</tr>
<tr>
<td>HTML.Element.Attribute</td>
<td>String</td>
<td>String representing an attribute of an HTML element</td>
<td></td>
</tr>
<tr>
<td>HTML.Element.Dimension</td>
<td>Dimension</td>
<td>Dimension of an HTML element (width and height)</td>
<td></td>
</tr>
<tr>
<td>HTML.Element.HasAttribute</td>
<td>Boolean</td>
<td>If true, an HTML element has a specified attribute.</td>
<td>String: Attribute name</td>
</tr>
<tr>
<td>HTML.Element.Name</td>
<td>String</td>
<td>Name of an HTML element</td>
<td></td>
</tr>
<tr>
<td>HTML.Element.ScriptType</td>
<td>String</td>
<td>Script type of an HTML element, for example, JavaScript or Visual Basic Script</td>
<td></td>
</tr>
</tbody>
</table>

Properties - I

The following table describes the properties that have names beginning with I.

Table A-14 Properties – I

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICAP.Policy</td>
<td>String</td>
<td>Name of a policy included in an ICAP request for a URL</td>
<td></td>
</tr>
<tr>
<td>ICAP.ReqMod.ResponseHeader.Exists</td>
<td>Boolean</td>
<td>If true, a response sent from an ICAP server in REQMOD mode contains a specified header.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>ICAP.ReqMod.ResponseHeader.Get</td>
<td>String</td>
<td>First value found for a specified header in a REQMOD response</td>
<td>String: Header name</td>
</tr>
<tr>
<td>ICAP.ReqMod.ResponseHeader.GetMultiple</td>
<td>List of String</td>
<td>List of values found for a specified header in a REQMOD response</td>
<td>String: Header name</td>
</tr>
<tr>
<td>ICAP.ReqMod.Satisfaction</td>
<td>Boolean</td>
<td>If true, an ICAP server has replaced a request with a response. The ICAP server does this after sending a message that a particular request is blocked.</td>
<td></td>
</tr>
<tr>
<td>ICAP.RespMod.EncapsulatedHTTPChanged</td>
<td>Boolean</td>
<td>If true, an ICAP server has changed the HTTP state for a response sent in RESPMOD mode.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ICAP.RespMod.ResponseHeader.Exists</td>
<td>Boolean</td>
<td>If true, a response sent from an ICAP server in RESPMOD mode contains a specified header.</td>
<td>String: Header name</td>
</tr>
<tr>
<td>ICAP.RespMod.ResponseHeader.Get</td>
<td>String</td>
<td>First value found for a specified header in a RESPMOD response</td>
<td>String: Header name</td>
</tr>
<tr>
<td>ICAP.RespMod.ResponseHeader.GetMultiple</td>
<td>List of String</td>
<td>List of values found for a specified header in a RESPMOD response</td>
<td>String: Header name</td>
</tr>
<tr>
<td>IM.Direction</td>
<td>String</td>
<td>Direction of a chat message sent or a file transferred under an instant messaging protocol and processed on the appliance. If a chat message sent from a client to the appliance, the direction could, for example, be specified as out, for a message sent from a server to the appliance it could be specified as in.</td>
<td></td>
</tr>
<tr>
<td>IM.FileName</td>
<td>String</td>
<td>Name of a file transferred under an instant messaging protocol</td>
<td></td>
</tr>
<tr>
<td>IM.FileSize</td>
<td>Number</td>
<td>Size of a file transferred under an instant messaging protocol (in bytes)</td>
<td></td>
</tr>
<tr>
<td>IM.MessageCanSendBack</td>
<td>Boolean</td>
<td>If true, a block message or other message can be sent from the appliance to a user of an instant messaging service. A block message is, for example, sent back to a user who submitted a chat message during a time interval that is not allowed for chatting. A message can typically not be sent before a user has completed the procedure for logging on to the instant messaging service.</td>
<td></td>
</tr>
<tr>
<td>IM.Notification</td>
<td>String</td>
<td>Name of a template used for sending a notification from the appliance to a user of an instant messaging service, for example, a block message</td>
<td></td>
</tr>
<tr>
<td>IM.Recipient</td>
<td>String</td>
<td>Name of a client that receives a chat message or file under an instant messaging protocol. This name can also be a group name (group ID) when a chat message is sent to a group of recipients.</td>
<td></td>
</tr>
</tbody>
</table>
### Table A-14 Properties – I (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM.Sender</td>
<td>String</td>
<td>Name of a client that sends a chat message or file under an instant messaging protocol</td>
<td></td>
</tr>
<tr>
<td>Incident.AffectedHost</td>
<td>IP</td>
<td>IP address of a host that is involved in an incident, for example, a web server that the appliance cannot connect to</td>
<td></td>
</tr>
<tr>
<td>Incident.Description</td>
<td>String</td>
<td>Plain-text description of an incident</td>
<td></td>
</tr>
<tr>
<td>Incident.ID</td>
<td>Number</td>
<td>ID of an incident</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For a list of these IDs, refer to the List of incident IDs.</td>
<td></td>
</tr>
<tr>
<td>Incident.Origin</td>
<td>Number</td>
<td>Number specifying the appliance component that is the origin of an incident</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 – Appliance system</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 – Core subsystem</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 – Coordinator subsystem</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 – Anti-Malware process</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 – Log File Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 – sysconf daemon</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 – User interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 – SaaS connector</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 – Unidentified origin</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The origin of an incident is further specified by the Incident.OriginName property.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the origin of an incident with a particular ID, refer to the List of incident IDs.</td>
<td></td>
</tr>
<tr>
<td>Incident.OriginName</td>
<td>String</td>
<td>Name of an appliance component that is the origin of an incident, for example, Core or Log File Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The name can be that of one of the main components that are listed under Incident.Origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>It can also be the name of a subcomponent, which appears together with the Incident.Origin number for the related main component.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, the value of Incident.OriginName could be 2 Proxy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the origin name of an incident with a particular ID, refer to the List of incident IDs.</td>
<td></td>
</tr>
</tbody>
</table>
### Table A-14 Properties – I (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident.Severity</td>
<td>Number</td>
<td>Severity of an incident</td>
<td>IP: Severity levels:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 - Emergency</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - Alert</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - Critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - Warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 - Notice</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6 - Informational</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7 - Debug</td>
</tr>
<tr>
<td></td>
<td></td>
<td>These levels are the same as those</td>
<td>For the severity level of an incident with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>used in syslog entries.</td>
<td>a particular ID, refer to the List of incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IDs.</td>
</tr>
<tr>
<td>IP.ToString</td>
<td>String</td>
<td>IP address converted into a string</td>
<td>IP: IP address to convert</td>
</tr>
<tr>
<td>IPRange.ToString</td>
<td>String</td>
<td>Range of IP addresses converted into</td>
<td>IPRange: Range of IP addresses to convert</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a string</td>
<td></td>
</tr>
</tbody>
</table>

### Properties – J

The following table describes the properties that have names beginning with J.

### Table A-15 Properties – J

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSON.ArrayAppend</td>
<td>JSON</td>
<td>JSON array with specified element appended</td>
<td>1 JSON: Array</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 JSON: Element to append</td>
</tr>
<tr>
<td>JSON.AsBool</td>
<td>Boolean</td>
<td>Value of specified JSON element returned as Boolean value</td>
<td>JSON: Element</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The element value must be a Boolean value.</td>
</tr>
<tr>
<td>JSON.AsNumber</td>
<td>Number</td>
<td>Value of specified JSON element returned as number</td>
<td>JSON: Element</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The element value must be a number in Long, Double, or Hexadecimal format.</td>
</tr>
<tr>
<td>JSON.AsString</td>
<td>String</td>
<td>Value of specified JSON element returned as string</td>
<td>JSON: Element</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The element value must be a string.</td>
</tr>
</tbody>
</table>
# Table A-15 Properties – J (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSON.CreateArray</td>
<td>JSON</td>
<td>New empty JSON array</td>
<td></td>
</tr>
<tr>
<td>JSON.CreateObject</td>
<td>JSON</td>
<td>New empty JSON object</td>
<td></td>
</tr>
<tr>
<td>JSON.CreateNull</td>
<td>JSON</td>
<td>JSON element value null</td>
<td></td>
</tr>
<tr>
<td>JSON.FromBool</td>
<td>JSON</td>
<td>JSON element value created from Boolean value</td>
<td>Boolean: Boolean value to create JSON element value from</td>
</tr>
<tr>
<td>JSON.FromNumber</td>
<td>JSON</td>
<td>JSON element value created from number</td>
<td>Number: Number to create JSON element value from</td>
</tr>
<tr>
<td>JSON.FromNumberList</td>
<td>String</td>
<td>JSON element value created from number list</td>
<td>List of Number: Number list to create JSON element value from</td>
</tr>
<tr>
<td>JSON.FromString</td>
<td>JSON</td>
<td>JSON element value created from string</td>
<td>String: String to create JSON element value from</td>
</tr>
<tr>
<td>JSON.FromStringList</td>
<td>JSON</td>
<td>JSON element value created from string list</td>
<td>List of String: String list to create JSON element value from</td>
</tr>
</tbody>
</table>
| JSON.GetAt            | JSON    | JSON element value retrieved from specified position in specified array | 1 JSON: Array  
2 Number: Position of element |
| JSON.GetName         | JSON    | JSON object identified by key retrieved from specified object | 1 JSON: Object  
2 String: Element key |
| JSON.GetType         | String  | Type of specified JSON element                        | JSON: Element                                                             |
| JSON.PutAt            | JSON    | JSON array with element inserted in specified position | 1 JSON: Array  
2 Number: Position of element  
3 JSON: Element |
| JSON.ReadString       | JSON    | JSON element created from specified string           | String: String to create element from                                     |
| JSON.RemoveAt         | JSON    | JSON array with element at specified position removed  | 1 JSON: Array  
2 Number: Position of element |
| JSON.RemoveByName     | JSON    | JSON object with element identified by specified key removed | 1 JSON: Object  
2 String: Element key |
| JSON.Size             | Number  | Number of elements in specified JSON object or array  | JSON: Object or array                                                     |
### Table A-15 Properties – J (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSON.StoreByName</td>
<td>JSON</td>
<td>JSON object with element value stored under specified key</td>
<td>1 JSON: Object</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 String: Element key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 JSON: Element value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the object does not exist yet, it is created under the name that is specified for the object.</td>
<td></td>
</tr>
<tr>
<td>JSON.ToString</td>
<td>String</td>
<td>JSON element value converted into a string</td>
<td>JSON: Element value to convert</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The element value can be a string or in any of the other data formats for element values.</td>
<td></td>
</tr>
</tbody>
</table>
## Properties - L

The following table describes the properties that have names beginning with L.

**Table A-16 Properties – L**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License.RemainingDays</td>
<td>Number</td>
<td>Remaining time until a license expires (in days)</td>
</tr>
</tbody>
</table>
| List.LastMatches    | String  | String containing all elements that have been found to match when two lists are compared using an operator such as at least one in list or all in list. Matches are only added to the list as long it has not yet been decided whether the relationship between the lists that the operator evaluates exists or not. For example, list A contains the elements 1, 2, 3, whereas list B contains 1, 2, 4. Both lists are compared using the at least one in list operator. To find out that list A actually contains at least one element of list B, the operator only needs to compare element 1 in both lists and detect that they match. List.LastMatches then contains 1 because it has been found to be a match. 2 is also a match in the two lists, but is not contained in List.LastMatches because it was not evaluated by the operator and found to be a match. It was not evaluated because the operator had already found out after evaluating the 1
Table A-16  Properties – L (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>in both lists that at least one element of list A was also in list B.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the property String.BelongsToDomains has &quot;true&quot; as its value, the string that is specified as its first parameter is set as the value of List.LastMatches.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This means List.LastMatches then provides a string that matched in a list of domain names, being either the name of a domain or a subdomain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The same applies for the property URL.Host.BelongsToDomains and List.LastMatches.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfCategory.Append</td>
<td>List of Category</td>
<td>List of URL categories that a category is appended to</td>
<td>1 List of Category: List to append category to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Category: Category to append</td>
</tr>
<tr>
<td>List.OfCategory.ByName</td>
<td>List of Category</td>
<td>List of URL categories (specified by its name)</td>
<td>String: List name</td>
</tr>
<tr>
<td>List.OfCategory.Erase</td>
<td>List of Category</td>
<td>List of URL categories with specified category erased</td>
<td>1 List of Category: List with category to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of category to erase</td>
</tr>
<tr>
<td>List.OfCategory.EraseElementRange</td>
<td>List of Category</td>
<td>List of URL categories with specified range of categories erased</td>
<td>1 List of Category: List with categories to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first category to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last category to erase</td>
</tr>
<tr>
<td>List.OfCategory.EraseList</td>
<td>List of Category</td>
<td>List of URL categories with categories that are also on other list erased</td>
<td>1 List of Category: List with categories to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of Category: List of categories to erase on first list</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List.OfCategory.Find</td>
<td>Number</td>
<td>Position of a URL category on a list</td>
<td>1 List of Category: List with category to find position for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Category: Category to find position for</td>
</tr>
<tr>
<td>List.OfCategory.Get</td>
<td>Category</td>
<td>URL category specified by its position on a list</td>
<td>1 List of Category: List containing category</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of category on list</td>
</tr>
<tr>
<td>List.OfCategory.GetElementRange</td>
<td>List of Category</td>
<td>List of URL categories extracted from other list</td>
<td>1 List of Category: List with categories to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first category to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last category to extract</td>
</tr>
<tr>
<td>List.OfCategory.Insert</td>
<td>List of Category</td>
<td>List of URL categories with specified category inserted</td>
<td>1 List of Category: List to insert category in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Category: Category to insert</td>
</tr>
<tr>
<td>List.OfCategory.IsEmpty</td>
<td>Boolean</td>
<td>If true, the specified list is empty.</td>
<td>List of Category: List to check for being empty</td>
</tr>
<tr>
<td>List.OfCategory.Join</td>
<td>List of Category</td>
<td>List of URL categories created by joining two lists</td>
<td>1 List of Category: First list to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of Category: Second list to join</td>
</tr>
<tr>
<td>List.OfCategory.Reverse</td>
<td>List of Category</td>
<td>List of URL categories that has its original order reverted</td>
<td>List of Category: List in original order</td>
</tr>
<tr>
<td>List.OfCategory.Size</td>
<td>Number</td>
<td>Number of URL categories on a list</td>
<td>List of Category: List to provide number of categories for</td>
</tr>
<tr>
<td>List.OfCategory.Sort</td>
<td>List of Category</td>
<td>List of URL categories sorted in alphabetical order</td>
<td>List of Category: List to sort</td>
</tr>
<tr>
<td>List.OfCategory.ToShortString</td>
<td>String</td>
<td>List of URL categories converted into a list of their abbreviated name forms</td>
<td>List of Category: List to convert</td>
</tr>
<tr>
<td>List.OfCategory.ToString</td>
<td>String</td>
<td>List of URL categories converted into a string</td>
<td>List of Category: List to convert</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List.OfDimension.Append</td>
<td>List of Dimension</td>
<td>List of dimensions that a dimension is appended to</td>
<td>1 List of Dimension: List to append dimension to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Dimension: Dimension to append</td>
</tr>
<tr>
<td>List.OfDimension.ByName</td>
<td>List of</td>
<td>List of dimensions specified by its name</td>
<td>String: List name</td>
</tr>
<tr>
<td></td>
<td>Dimension</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfDimension.Erase</td>
<td>List of</td>
<td>List of dimensions with specified dimension erased</td>
<td>1 List of Dimension: List with dimension to erase</td>
</tr>
<tr>
<td></td>
<td>Dimension</td>
<td></td>
<td>2 Number: Position of dimension to erase</td>
</tr>
<tr>
<td>List.OfDimension.EraseElementRange</td>
<td>List of Dimension</td>
<td>List of dimensions with specified range of dimensions erased</td>
<td>1 List of Dimension: List with dimension range to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first dimension to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last dimension to erase</td>
</tr>
<tr>
<td>List.OfDimension.EraseList</td>
<td>List of</td>
<td>List of dimensions with dimensions that are also on other list erased</td>
<td>1 List of Dimension: List with dimensions to erase</td>
</tr>
<tr>
<td></td>
<td>Dimension</td>
<td></td>
<td>2 List of Dimension: List of dimensions to erase on first list</td>
</tr>
<tr>
<td>List.OfDimension.Find</td>
<td>Number</td>
<td>Position of a dimension on a list</td>
<td>1 List of Dimension: List with dimension to find position for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Dimension: Dimension to find position for</td>
</tr>
<tr>
<td>List.OfDimension.Get</td>
<td>Dimension</td>
<td>Dimension specified by its position on a list</td>
<td>1 List of Dimension: List containing dimension</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of dimension on list</td>
</tr>
</tbody>
</table>
Table A-16 Properties – L (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>List.OfDimension.GetElementRange</td>
<td>List of Dimension</td>
<td>List of dimensions extracted from other list</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>List of Dimension: List with dimensions to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Number: Position of first dimension to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Number: Position of last dimension to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Dimension: Dimension to insert</td>
</tr>
<tr>
<td>List.OfDimension.Insert</td>
<td>List of Dimension</td>
<td>List of dimensions with specified dimension inserted</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>List of Dimension: List to insert dimension in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Dimension: Dimension to insert</td>
</tr>
<tr>
<td>List.OfDimension.IsEmpty</td>
<td>Boolean</td>
<td>If true, the specified list is empty.</td>
<td>List of Dimension: List to check for being empty</td>
</tr>
<tr>
<td>List.OfDimension.Join</td>
<td>List of Dimension</td>
<td>List of dimensions created by joining two lists</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>List of Dimension: First list to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>List of Dimension: Second list to join</td>
</tr>
<tr>
<td>List.OfDimension.Reverse</td>
<td>List of Dimension</td>
<td>List of dimensions that has its original order reverted</td>
<td>List of Dimension: List in original order</td>
</tr>
<tr>
<td>List.OfDimension.Size</td>
<td>Number</td>
<td>Number of dimensions on a list</td>
<td>List of Dimension: List to provide number of dimensions for</td>
</tr>
<tr>
<td>List.OfDimension.Sort</td>
<td>List of Dimension</td>
<td>List of dimensions sorted in alphabetical order</td>
<td>List of Dimension: List to sort</td>
</tr>
<tr>
<td>List.OfDimension.ToString</td>
<td>String</td>
<td>List of dimensions converted into a string</td>
<td>List of Dimension: List to convert</td>
</tr>
<tr>
<td>List.OfHex.Append</td>
<td>List of Hex</td>
<td>List of hex values that a hex value is appended to</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>List of Hex: List to append Hex value to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hex: Hex value to append</td>
</tr>
<tr>
<td>List.OfHex.ByName</td>
<td>List of Hex</td>
<td>List of hex values specified by its name</td>
<td>String: List name</td>
</tr>
<tr>
<td>List.OfHex.Erase</td>
<td>List of Hex</td>
<td>List of hex values with specified value erased</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>List of Hex: List with hex value to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Number: Position of hex value to erase</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List.OfHex.EraseElementRange</td>
<td>List of Hex</td>
<td>List of hex values with specified range of values erased</td>
<td>1 List of Hex: List with hex values to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first hex value to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last hex value to erase</td>
</tr>
<tr>
<td>List.OfHex.EraseList</td>
<td>List of Hex</td>
<td>List of hex values with values that are also on other list erased</td>
<td>1 List of Hex: List with hex values to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of Hex: List of hex values to erase on first list</td>
</tr>
<tr>
<td>List.OfHex.Find</td>
<td>Number</td>
<td>Position of a hex value on a list</td>
<td>1 List of Hex: List with hex value to find position for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Hex: Hex value to find position for</td>
</tr>
<tr>
<td>List.OfHex.Get</td>
<td>Hex</td>
<td>Hex value specified by its position on a list</td>
<td>1 List of Hex: List containing hex value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of hex value on list</td>
</tr>
<tr>
<td>List.OfHex.GetElementRange</td>
<td>List of Hex</td>
<td>List of hex values extracted from other list</td>
<td>1 List of Hex: List with hex values to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first hex value to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last hex value to extract</td>
</tr>
<tr>
<td>List.OfHex.Insert</td>
<td>List of Hex</td>
<td>List of hex values with specified value inserted</td>
<td>1 List of Hex: List to insert hex value in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Hex: Hex value to insert</td>
</tr>
<tr>
<td>List.OfHex.IsEmpty</td>
<td>Boolean</td>
<td>If true, the specified list is empty.</td>
<td>List of Hex: List to check for being empty</td>
</tr>
<tr>
<td>List.OfHex.Join</td>
<td>List of Hex</td>
<td>List of hex values created by joining two lists</td>
<td>1 List of Hex: First list to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of Hex: Second list to join</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List.OfHex.Reverse</td>
<td>List of Hex</td>
<td>List of hex values that has its original order reverted</td>
<td>List of Hex: List in original order</td>
</tr>
<tr>
<td>List.OfHex.Size</td>
<td>Number</td>
<td>Number of hex values on a list</td>
<td>List of Hex: List to provide number of hex values for</td>
</tr>
<tr>
<td>List.OfHex.Sort</td>
<td>List of Hex</td>
<td>List of sorted hex values</td>
<td>List of Hex: List to sort</td>
</tr>
<tr>
<td>List.OfHex.ToString</td>
<td>String</td>
<td>List of hex values converted into a string</td>
<td>List of Hex: List to convert</td>
</tr>
<tr>
<td>List.OfIP.Append</td>
<td>List of IP</td>
<td>List of IP addresses that an IP address is appended to</td>
<td>1 List of IP: List to append IP address to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 IP: IP address to append</td>
</tr>
<tr>
<td>List.OfIP.ByName</td>
<td>List of IP</td>
<td>List of IP addresses (specified by its name)</td>
<td>String: List name</td>
</tr>
<tr>
<td>List.OfIP.Erase</td>
<td>List of IP</td>
<td>List of IP addresses with specified address erased</td>
<td>1 List of IP: List with IP address to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of IP address to erase</td>
</tr>
<tr>
<td>List.OfIP.EraseElementRange</td>
<td>List of IP</td>
<td>List of IP addresses with specified range of addresses erased</td>
<td>1 List of IP: List with IP addresses to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first IP address to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last IP address to erase</td>
</tr>
<tr>
<td>List.OfIP.EraseList</td>
<td>List of IP</td>
<td>List of IP addresses with addresses that are also on other list erased</td>
<td>1 List of IP: List with IP addresses to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of IP: List of IP addresses to erase on first list</td>
</tr>
<tr>
<td>List.OfIP.Find</td>
<td>Number</td>
<td>Position of an IP address on a list</td>
<td>1 List of IP: List with IP address to find position for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 IP: IP address to find position for</td>
</tr>
<tr>
<td>List.OfIP.Get</td>
<td>IP</td>
<td>IP address specified by its position on a list</td>
<td>1 List of IP: List containing IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of IP address on list</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List.OfIP.GetElementRange</td>
<td>List of IP</td>
<td>List of IP addresses extracted from another list</td>
<td>1 List of IP: List with IP addresses to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first IP address to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last IP address to extract</td>
</tr>
<tr>
<td>List.OfIP.Insert</td>
<td>List of IP</td>
<td>List of IP addresses with specified address inserted</td>
<td>1 List of IP: List to insert IP address in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 IP: IP address to insert</td>
</tr>
<tr>
<td>List.OfIP.IsEmpty</td>
<td>Boolean</td>
<td>If true, the specified list is empty</td>
<td>List of IP: List to check for being empty</td>
</tr>
<tr>
<td>List.OfIP.Join</td>
<td>List of IP</td>
<td>List of IP addresses created by joining two lists</td>
<td>1 List of IP: First list to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of IP: Second list to join</td>
</tr>
<tr>
<td>List.OfIP.Reverse</td>
<td>List of IP</td>
<td>List of IP addresses that has its original order reverted</td>
<td>List of IP: List in original order</td>
</tr>
<tr>
<td>List.OfIP.Size</td>
<td>Number</td>
<td>Number of IP addresses on a list</td>
<td>List of IP: List to provide number of IP addresses for</td>
</tr>
<tr>
<td>List.OfIP.Sort</td>
<td>List of IP</td>
<td>List of sorted IP addresses</td>
<td>List of IP: List to sort</td>
</tr>
<tr>
<td>List.OfIP.ToString</td>
<td>String</td>
<td>List of IP addresses converted into a string</td>
<td>List of IP: List to convert</td>
</tr>
<tr>
<td>List.OfIPRange.Append</td>
<td>List of IPRange</td>
<td>List of IP address ranges that an IP address range is appended to</td>
<td>1 List of IPRange: List to append IP address range to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 IPRange: IP address range to append</td>
</tr>
<tr>
<td>List.OfIPRange.ByName</td>
<td>List of IPRange</td>
<td>List of IP address ranges specified by its name</td>
<td>String: List name</td>
</tr>
<tr>
<td>List.OfIPRange.Erase</td>
<td>List of IPRange</td>
<td>List of IP address ranges with specified range erased</td>
<td>1 List of IPRange: List with IP address range to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of IP address range to erase</td>
</tr>
</tbody>
</table>
### Table A-16 Properties – L (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>List.OfIPRange.EraseElementRange</td>
<td>List of IPRange</td>
<td>List of IP address ranges with specified ranges erased</td>
<td>1 List of IPRange: List with IP address ranges to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first IP address range to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last IP address range to erase</td>
</tr>
<tr>
<td>List.OfIPRange.EraseList</td>
<td>List of IPRange</td>
<td>List of IP address ranges with ranges that are also on other list erased</td>
<td>1 List of IPRange: List with IP address ranges to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of IPRange: List of IP address ranges to erase on first list</td>
</tr>
<tr>
<td>List.OfIPRange.Find</td>
<td>Number</td>
<td>Position of an IP address range on a list</td>
<td>1 List of IPRange: List with IP address range to find position for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 IPRange: IP address range to find position for</td>
</tr>
<tr>
<td>List.OfIPRange.Get</td>
<td>IPRange</td>
<td>IP address range specified by its position on a list</td>
<td>1 List of IPRange: List containing IP address range</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of IP address range on list</td>
</tr>
<tr>
<td>List.OfIPRange.GetElementRange</td>
<td>List of IPRange</td>
<td>List of IP address ranges extracted from other list</td>
<td>1 List of IPRange: List with IP address ranges to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first IP address range to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last IP address range to extract</td>
</tr>
<tr>
<td>List.OfIPRange.Insert</td>
<td>List of IPRange</td>
<td>List of IP address ranges with specified range inserted</td>
<td>1 List of IPRange: List to insert IP address range in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 IPRange: IP address range to insert</td>
</tr>
<tr>
<td>List.OfIPRange.IsEmpty</td>
<td>Boolean</td>
<td>If true, the specified list is empty.</td>
<td>List of IPRange: List to check for being empty</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List.OfIPRange.Join</td>
<td>List of IPRange</td>
<td>List of IP address ranges created by joining two lists</td>
<td>1 List of IPRange: First list to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of IPRange: Second list to join</td>
</tr>
<tr>
<td>List.OfIPRange.Reverse</td>
<td>List of IPRange</td>
<td>List of IP address ranges that has its original order reverted</td>
<td>List of IPRange: List in original order</td>
</tr>
<tr>
<td>List.OfIPRange.Size</td>
<td>Number</td>
<td>Number of IP address ranges on a list</td>
<td>List of IPRange: List to provide number of IP address ranges for</td>
</tr>
<tr>
<td>List.OfIPRange.Sort</td>
<td>List of IPRange</td>
<td>List of sorted IP address ranges</td>
<td>List of IPRange: List to sort</td>
</tr>
<tr>
<td>List.OfIPRange.ToString</td>
<td>String</td>
<td>List of IP address ranges converted into a string</td>
<td>List of IPRange: List to convert</td>
</tr>
<tr>
<td>List.OfMediaType.Append</td>
<td>List of MediaType</td>
<td>List of media types that a media type is appended to</td>
<td>1 List of MediaType: List to append media type to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 MediaType: Media type to append</td>
</tr>
<tr>
<td>List.OfMediaType.ByName</td>
<td>List of MediaType</td>
<td>List of media types specified by its name</td>
<td>String: List name</td>
</tr>
<tr>
<td>List.OfMediaType.Erase</td>
<td>List of MediaType</td>
<td>List of media types with specified type erased</td>
<td>1 List of MediaType: List with media type to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of media type to erase</td>
</tr>
<tr>
<td>List.OfMediaType.EraseElementRange</td>
<td>List of MediaType</td>
<td>List of media types with specified range of types erased</td>
<td>1 List of MediaType: List with media types to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first media type to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last media type to erase</td>
</tr>
<tr>
<td>List.OfMediaType.EraseList</td>
<td>List of MediaType</td>
<td>List of media types with types that are also on other list erased</td>
<td>1 List of MediaType: List with media types to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of MediaType: List of media types to erase on first list</td>
</tr>
</tbody>
</table>
### Table A-16  Properties – L (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>List.OfMediaType.Find</td>
<td>Number</td>
<td>Position of a media type on a list</td>
<td>1 List of MediaType: List with media type to find position for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 MediaType: Media type to find position for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfMediaType.Get</td>
<td>MediaType</td>
<td>Media type specified by its position on a list</td>
<td>1 List of MediaType: List containing media type</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of media type on list</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfMediaType.GetElems</td>
<td>List of MediaType</td>
<td>List of media types extracted from other list</td>
<td>1 List of MediaType: List with media types to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first media type to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last media type to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfMediaType.Insert</td>
<td>List of MediaType</td>
<td>List of media types with specified type inserted</td>
<td>1 List of MediaType: List to insert media type in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 MediaType: Media type to insert</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfMediaType.IsEmpty</td>
<td>Boolean</td>
<td>If true, the specified list is empty.</td>
<td>List of MediaType: List to check for being empty</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfMediaType.Join</td>
<td>List of MediaType</td>
<td>List of media types created by joining two lists</td>
<td>1 List of MediaType: First list to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of MediaType: Second list to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfMediaType.Reverse</td>
<td>List of MediaType</td>
<td>List of media types that has its original order reverted</td>
<td>List of MediaType: List in original order</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfMediaType.Size</td>
<td>Number</td>
<td>Number of media types on a list</td>
<td>List of MediaType: List to provide number of media types for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfMediaType.Sort</td>
<td>List of MediaType</td>
<td>List of media types sorted in alphabetical order</td>
<td>List of MediaType: List to sort</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List.OfMediaType.ToString</td>
<td>String</td>
<td>List of media types converted into a string</td>
<td>List of MediaType: List to convert</td>
</tr>
</tbody>
</table>
### Table A-16  Properties – L (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>List.OfNumber.Append</td>
<td>List of Number</td>
<td>List of numbers that a number is appended to</td>
<td>1 List of Number: List to append number to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Number to append</td>
</tr>
<tr>
<td>List.OfNumber.ByName</td>
<td>List of Number</td>
<td>List of numbers specified by its name</td>
<td>String: List name</td>
</tr>
<tr>
<td>List.OfNumber.Erase</td>
<td>List of Number</td>
<td>List of numbers with specified number erased</td>
<td>1 List of Number: List with number to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of number to erase</td>
</tr>
<tr>
<td>List.OfNumber.EraseElementRange</td>
<td>List of Number</td>
<td>List of numbers with specified range of numbers erased</td>
<td>1 List of Number: List with numbers to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first number to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last number to erase</td>
</tr>
<tr>
<td>List.OfNumber.EraseList</td>
<td>List of Number</td>
<td>List of numbers with numbers that are also on other list erased</td>
<td>1 List of Number: List with numbers to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of Number: List of numbers to erase on first list</td>
</tr>
<tr>
<td>List.OfNumber.Find</td>
<td>Number</td>
<td>Position of a number on a list</td>
<td>1 List of Number: List with number to find position for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Number to find position for</td>
</tr>
<tr>
<td>List.OfNumber.Get</td>
<td>Number</td>
<td>Number specified by its position on a list</td>
<td>1 List of Number: List containing number</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of number on list</td>
</tr>
<tr>
<td>List.OfNumber.GetElementRange</td>
<td>List of Number</td>
<td>List of numbers extracted from other list</td>
<td>1 List of Number: List with numbers to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first number to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last number to extract</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------</td>
<td>-------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List.OfNumber.Insert</td>
<td>List of Number</td>
<td>List of numbers with specified number inserted</td>
<td>1 List of Number: List to insert number in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Number to insert</td>
</tr>
<tr>
<td>List.OfNumber.IsEmpty</td>
<td>Boolean</td>
<td>If true, the specified list is empty.</td>
<td>List of Number: List to check for being empty</td>
</tr>
<tr>
<td>List.OfNumber.Join</td>
<td>List of Number</td>
<td>List of numbers created by joining two lists</td>
<td>1 List of Number: First list to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of Number: Second list to join</td>
</tr>
<tr>
<td>List.OfNumber.Reverse</td>
<td>List of Number</td>
<td>List of numbers that has its original order reverted</td>
<td>List of Number: List in original order</td>
</tr>
<tr>
<td>List.OfNumber.Size</td>
<td>Number</td>
<td>Number of numbers on a list</td>
<td>List of Number: List to provide number of numbers for</td>
</tr>
<tr>
<td>List.OfNumber.Sort</td>
<td>List of Number</td>
<td>List of sorted numbers</td>
<td>List of Number: List to sort</td>
</tr>
<tr>
<td>List.OfNumber.ToString</td>
<td>String</td>
<td>List of numbers converted into a string</td>
<td>List of Number: List to convert</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Append</td>
<td>List of SSOConnector</td>
<td>List of cloud connectors with specified cloud connector appended</td>
<td>1 List of SSOConnector: List to append cloud connector to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 SSO Connector: Cloud connector to append</td>
</tr>
<tr>
<td>List.OfSSOConnectors.ByName</td>
<td>List of SSOConnector</td>
<td>List of cloud connectors specified by its name</td>
<td>String: List name</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Erase</td>
<td>List of SSOConnector</td>
<td>List of cloud connectors with specified connector erased</td>
<td>1 List of SSOConnector: List with cloud connector to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of cloud connector to erase</td>
</tr>
<tr>
<td>List.OfSSOConnectors.EraseElementRange</td>
<td>List of SSOConnector</td>
<td>List of cloud connectors with specified range of connectors erased</td>
<td>1 List of SSOConnector: List with range of cloud connectors to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first cloud connector to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last cloud connector to erase</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List.OfSSOConnectors.EraseList</td>
<td>List of SSOConnector</td>
<td>List of cloud connectors with connectors that are also on other list erased</td>
<td>1 List of SSOConnector: List with cloud connectors to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of SSOConnector: List of cloud connectors to erase on first list</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Exists</td>
<td>Boolean</td>
<td>If true, the list of cloud connectors with the specified name exists.</td>
<td>String: List name</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Find</td>
<td>Number</td>
<td>Position of cloud connector in a list</td>
<td>1 List of SSOConnector: List containing cloud connector</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 SSOConnector: Cloud connector to find position for</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Get</td>
<td>SSOConnector</td>
<td>Cloud connector specified by its position on a list</td>
<td>1 List of SSOConnector: List containing cloud connector</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of cloud connector on list</td>
</tr>
<tr>
<td>List.OfSSOConnectors.GetElementRange</td>
<td>List of SSOConnector</td>
<td>List of cloud connectors extracted from other list</td>
<td>1 List of SSOConnector: List with cloud connectors to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first cloud connector to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last cloud connector to extract</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Insert</td>
<td>List of SSOConnector</td>
<td>List of cloud connectors with specified connector inserted</td>
<td>1 List of SSOConnector: List to insert cloud connector in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 SSO Connector: Cloud connector to insert</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position to insert cloud connector in</td>
</tr>
<tr>
<td>List.OfSSOConnectors.IsEmpty</td>
<td>Boolean</td>
<td>If true, the specified list is empty.</td>
<td>List of SSOConnector: List to check for being empty</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Join</td>
<td>List of SSOConnector</td>
<td>List of single sign-on connectors created by joining two lists</td>
<td>1 List of SSOConnector: First list to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of SSOConnector: Second list to join</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Reverse</td>
<td>List of SSOConnector</td>
<td>List of cloud connectors that has its original order reverted</td>
<td>List of SSOConnector: List in original order</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Set</td>
<td>List of SSOConnector</td>
<td>List of cloud connectors with specified connector set</td>
<td>1 List of SSOConnector: List to set cloud connector on</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 SSOConnector: Cloud connector to set</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position to set cloud connector on</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Size</td>
<td>Number</td>
<td>Number of cloud connectors on a list</td>
<td>List of SSOConnector: List to provide number of cloud connectors for</td>
</tr>
<tr>
<td>List.OfSSOConnectors.Sort</td>
<td>List of SSOConnector</td>
<td>List of cloud connectors sorted in alphabetical order of names</td>
<td>List of SSOConnector: List to sort</td>
</tr>
<tr>
<td>List.OfSSOConnectors.ToString</td>
<td>String</td>
<td>List of cloud connectors converted into a string</td>
<td>List of SSOConnector: List to convert</td>
</tr>
<tr>
<td>List.OfString.Append</td>
<td>List of String</td>
<td>List of strings that a string is appended to</td>
<td>1 List of String: List to append string to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 String: String to append</td>
</tr>
<tr>
<td>List.OfString.ByName</td>
<td>List of String</td>
<td>List of strings specified by its name</td>
<td>String: List name</td>
</tr>
<tr>
<td>List.OfString.Erase</td>
<td>List of String</td>
<td>List of strings with specified string erased</td>
<td>1 List of String: List with string to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of string to erase</td>
</tr>
<tr>
<td>List.OfString.EraseElementRange</td>
<td>List of String</td>
<td>List of strings with specified range of strings erased</td>
<td>1 List of String: List with strings to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first string to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last string to erase</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List.OfString.EraseList</td>
<td>List of String</td>
<td>List of strings with strings that are also on other list erased</td>
<td>1 List of String: List with strings to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of String: List of strings to erase on first list</td>
</tr>
<tr>
<td>List.OfString.Find</td>
<td>Number</td>
<td>Position of a string on a list</td>
<td>1 List of String: List with string to find position for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 String: String to find position for</td>
</tr>
<tr>
<td>List.OfString.Get</td>
<td>String</td>
<td>String specified by its position on a list</td>
<td>1 List of String: List containing string</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of string on list</td>
</tr>
<tr>
<td>List.OfString.GetElementRange</td>
<td>List of String</td>
<td>List of strings extracted from other list</td>
<td>1 List of String: List with strings to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first string to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last string to extract</td>
</tr>
<tr>
<td>List.OfString.Insert</td>
<td>List of String</td>
<td>List of strings with specified string inserted</td>
<td>1 List of String: List to insert string in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 String: String to insert</td>
</tr>
<tr>
<td>List.OfString.IsEmpty</td>
<td>Boolean</td>
<td>If true, the specified list is empty.</td>
<td>List of String: List to check for being empty</td>
</tr>
<tr>
<td>List.OfString.Join</td>
<td>List of String</td>
<td>List of strings created by joining two lists</td>
<td>1 List of String: First list to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of String: Second list to join</td>
</tr>
<tr>
<td>List.OfString.JSON.AsStringList</td>
<td>List of String</td>
<td>List of strings created from the element values of a JSON array</td>
<td>JSON: Array</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If a value is null, an empty string is created.</td>
</tr>
</tbody>
</table>
### Table A-16 Properties – L (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| List.OfStringMapInList      | List of String      | String specified by a parameter and contained in a list with an index for the position this string has in another list. If the specified string is not contained in the first list or does not exist as a position in the second list, the string is empty. | 1 List of String: First list containing string  
2 List of String: Second list containing string  
3 String: String contained in first and second list or empty string |
| List.OfString.Reverse      | List of String      | List of strings that has its original order reverted                        | List of String: List in original order                                       |
| List.OfString.Size         | Number              | Number of strings on a specified list                                       | List of String: List to provide number of strings for                        |
| List.OfString.Sort         | List of String      | List of strings sorted in alphabetical order                               | List of String: List to sort                                                 |
| List.OfString.ToString     | String              | List of strings converted into a string                                    | List of String: List to convert                                              |
| List.OfWildcard.Append     | List of Wildcard Expression | List of wildcard expressions that an expression is appended to          | 1 List of Wildcard Expression: List to append wildcard expression to          
2 Wildcard Expression: Wildcard expression to append                                |
| List.OfWildcard.ByName     | List of Wildcard Expression | List of wildcard expressions specified by its name                      | String: List name                                                              |
| List.OfWildcard.Erase      | List of Wildcard Expression | List of wildcard expressions with specified expression erased             | 1 List of Wildcard Expression: List with wildcard expression to erase          
2 Number: Position of wildcard expression to erase                                    |
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>List.OfWildcard.EraseElementRange</td>
<td>List of Wildcard Expression</td>
<td>List of wildcard expressions with specified range of expressions erased</td>
<td>1 List of Wildcard Expression: List with wildcard expressions to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first wildcard expression to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last wildcard expression to erase</td>
</tr>
<tr>
<td>List.OfWildcard.EraseList</td>
<td>List of Wildcard Expression</td>
<td>List of wildcard expressions with expressions that are also on other list erased</td>
<td>1 List of Wildcard Expression: List with wildcard expressions to erase</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of Wildcard Expression: List of wildcard expressions to erase on first list</td>
</tr>
<tr>
<td>List.OfWildcard.Find</td>
<td>Number</td>
<td>Position of a wildcard expression on a list</td>
<td>1 List of Wildcard expression: List with wildcard expression to find position for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Wildcard expression: Wildcard expression to find position for</td>
</tr>
<tr>
<td>List.OfWildcard.Get</td>
<td>Wildcard Expression</td>
<td>Wildcard expression specified by its position on a list</td>
<td>1 List of Wildcard Expression: List containing wildcard expression</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of wildcard expression on list</td>
</tr>
<tr>
<td>List.OfWildcard.GetElementRange</td>
<td>List of Wildcard Expression</td>
<td>List of wildcard expressions extracted from other list</td>
<td>1 List of Wildcard Expression: List with wildcard expressions to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position of first wildcard expression to extract</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position of last wildcard expression to extract</td>
</tr>
</tbody>
</table>
### Table A-16 Properties – L (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>List.OfWildcard.Insert</td>
<td>List of Wildcard</td>
<td>List of wildcard expressions with specified expression inserted</td>
<td>1 List of Wildcard Expression: List to insert wildcard expression in</td>
</tr>
<tr>
<td></td>
<td>Expression</td>
<td></td>
<td>2 Wildcard Expression: Wildcard expression to insert</td>
</tr>
<tr>
<td>List.OfWildcard.IsEmpty</td>
<td>Boolean</td>
<td>If true, the specified list is empty.</td>
<td>List of Wildcard Expression: List to check for being empty</td>
</tr>
<tr>
<td>List.OfWildcard.Join</td>
<td>List of Wildcard</td>
<td>List of wildcard expressions created by joining two lists</td>
<td>1 List of Wildcard Expression: First list to join</td>
</tr>
<tr>
<td></td>
<td>Expression</td>
<td></td>
<td>2 List of Wildcard Expression: Second list to join</td>
</tr>
<tr>
<td>List.OfWildcard.Reverse</td>
<td>List of Wildcard</td>
<td>List of wildcard expressions that has its original order reverted</td>
<td>List of Wildcard Expression: List in original order</td>
</tr>
<tr>
<td>List.OfWildcard.Size</td>
<td>Number</td>
<td>Number of wildcard expressions on a list</td>
<td>List of Wildcard Expression: List to provide number of wildcard expressions for</td>
</tr>
<tr>
<td>List.OfWildcard.Sort</td>
<td>List of Wildcard</td>
<td>List of sorted wildcard expressions</td>
<td>List of Wildcard Expression: List to sort</td>
</tr>
<tr>
<td>List.OfWildcard.ToString</td>
<td>String</td>
<td>List of wildcard expressions converted into a string</td>
<td>List of Wildcard Expression: List to convert</td>
</tr>
</tbody>
</table>

### Properties – M

The following table describes the properties that have names beginning with M.

### Table A-17 Properties – M

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map.ByName</td>
<td>List of MapType</td>
<td>Already existing Map Type list that has the specified name</td>
<td>String: List name</td>
</tr>
<tr>
<td>Map.CreateStringMap</td>
<td>List of MapType</td>
<td>Newly created Map Type list The list is still empty.</td>
<td></td>
</tr>
<tr>
<td>Map.DeleteKey</td>
<td>List of MapType</td>
<td>Map Type list, in which the specified key and the related value are deleted</td>
<td>1 List of MapType: Map Type list</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 String: Key</td>
</tr>
<tr>
<td>Map.GetKeys</td>
<td>List of MapType</td>
<td>List of keys that are contained in the specified Map Type list</td>
<td>List of MapType: Map Type list</td>
</tr>
</tbody>
</table>
Table A-17 Properties – M (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map.GetStringValue</td>
<td>String</td>
<td>String that is the value for the specified key in the specified Map Type list</td>
<td>1 List of MapType: Map Type list 2 String: Key</td>
</tr>
<tr>
<td>Map.HasKey</td>
<td>Boolean</td>
<td>If true, the specified key exists in the specified Map Type list</td>
<td>1 List of MapType: Map Type list 2 String: Key</td>
</tr>
<tr>
<td>Map.SetStringValue</td>
<td>List of MapType</td>
<td>Map Type list, in which the specified value is set for the specified key</td>
<td>1 List of MapType: Map Type list 2 String: Key 3 String: Value</td>
</tr>
<tr>
<td>Map.Size</td>
<td>Number</td>
<td>Number of key-value pairs in the specified Map Type list</td>
<td>List of MapType: Map Type list</td>
</tr>
<tr>
<td>Map.ToString</td>
<td>String</td>
<td>Map Type list converted into a string</td>
<td>List of MapType: Map Type list</td>
</tr>
<tr>
<td>Math.Abs</td>
<td>Number</td>
<td>Absolute value of specified number</td>
<td>Number: Number that absolute value is provided for</td>
</tr>
<tr>
<td>Math.Modulo</td>
<td>Number</td>
<td>Integer that is the remainder after dividing integer a by integer b when only an integer is accepted as the resulting quotient.</td>
<td>1 Number: Value for a 2 Number: Value for b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, if a = 14 and b = 3, the value of Math.Modulo is 2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The integer that is the result of dividing 14 by 3 is 4 and, since 3 x 4 = 12, this leaves 2 as the remainder.</td>
<td></td>
</tr>
<tr>
<td>Math.Random</td>
<td>Number</td>
<td>Random number between specified minimum and maximum values (including these values)</td>
<td>1 Number: Minimum value 2 Number: Maximum value</td>
</tr>
<tr>
<td>MediaStreamProbability</td>
<td>Number</td>
<td>Probability that the streaming media in question matches the found media type (in percent)</td>
<td></td>
</tr>
<tr>
<td>MediaType.EnsureddTypes</td>
<td>List of MediaType</td>
<td>List of media types that are ensured for the respective media with a probability of more than 50%</td>
<td></td>
</tr>
<tr>
<td>MediaType.FromFileExtension</td>
<td>List of MediaType</td>
<td>List of media types that are found using the file name extension of the media</td>
<td></td>
</tr>
<tr>
<td>MediaType.FromHeader</td>
<td>List of MediaType</td>
<td>List of media types that are found using the content-type header sent with the media</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>MediaType.HasOpener</td>
<td>Boolean</td>
<td>If true, an opener module is available on the appliance for media of a given type.</td>
<td></td>
</tr>
<tr>
<td>MediaType.IsArchive</td>
<td>Boolean</td>
<td>If true, the media that is being processed is an archive.</td>
<td></td>
</tr>
<tr>
<td>MediaType.IsAudio</td>
<td>Boolean</td>
<td>If true, the media that is being processed is of the audio type.</td>
<td></td>
</tr>
<tr>
<td>MediaType.IsCompositeObject</td>
<td>Boolean</td>
<td>If true, the media that is being processed is a composite object.</td>
<td></td>
</tr>
<tr>
<td>MediaType.IsDatabase</td>
<td>Boolean</td>
<td>If true, the media that is being processed is a database.</td>
<td></td>
</tr>
<tr>
<td>MediaType.IsDocument</td>
<td>Boolean</td>
<td>If true, the media that is being processed is a document.</td>
<td></td>
</tr>
<tr>
<td>MediaType.IsExecutable</td>
<td>Boolean</td>
<td>If true, the media that is being processed is an executable file.</td>
<td></td>
</tr>
<tr>
<td>MediaType.IsImage</td>
<td>Boolean</td>
<td>If true, the media that is being processed is an image.</td>
<td></td>
</tr>
<tr>
<td>MediaType.IsText</td>
<td>Boolean</td>
<td>If true, the media that is being processed is of the text type.</td>
<td></td>
</tr>
<tr>
<td>MediaType.IsVideo</td>
<td>Boolean</td>
<td>If true, the media that is being processed is of the video type.</td>
<td></td>
</tr>
<tr>
<td>MediaType.MagicBytesMismatch</td>
<td>Boolean</td>
<td>If true, the media type specified in the header sent with the media does not match the type that was found on the appliance by examining the magic bytes actually contained in the media.</td>
<td></td>
</tr>
<tr>
<td>MediaType.NotEnsuredTypes</td>
<td>List of MediaType</td>
<td>List of media types that are ensured for the respective media with a probability of less than 50%</td>
<td></td>
</tr>
<tr>
<td>MediaType.ToString</td>
<td>String</td>
<td>Media type converted into a string</td>
<td>MediaType: MediaType to convert</td>
</tr>
<tr>
<td>Message.Language</td>
<td>String</td>
<td>Name of language for messages sent to users in short form, for example, en, de, ja</td>
<td></td>
</tr>
<tr>
<td>Message.TemplateName</td>
<td>String</td>
<td>Name of a template for messages sent to users</td>
<td></td>
</tr>
</tbody>
</table>
## Properties - N

The following table describes the properties that have names beginning with N.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHopProxy.StickinessAttribute</td>
<td>String</td>
<td>Part of a request that qualifies it for being handled in next-hop proxy stickiness mode</td>
<td></td>
</tr>
<tr>
<td>Number.ToDecimalNumber</td>
<td>Number</td>
<td>Integer converted into decimal format</td>
<td>Number: Integer to convert</td>
</tr>
<tr>
<td>Number.ToString</td>
<td>String</td>
<td>Number converted into a string</td>
<td>Number: Number to convert</td>
</tr>
<tr>
<td>Number.ToDoubleVolumeString</td>
<td>String</td>
<td>Number of bytes that a volume amounts to converted into a string</td>
<td>Number: Number of bytes to convert</td>
</tr>
<tr>
<td>NumberOfClientConnections</td>
<td>Number</td>
<td>Number of connections to clients that are open on an appliance at the same time</td>
<td></td>
</tr>
</tbody>
</table>

## Properties - P

The following table describes the properties that have names beginning with P.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDStorage.GetAllData</td>
<td>List of String</td>
<td>List containing all permanently stored data in string format</td>
<td></td>
</tr>
<tr>
<td>PDStorage.GetAllGlobalData</td>
<td>List of String</td>
<td>List containing all permanently stored global data in string format</td>
<td></td>
</tr>
<tr>
<td>PDStorage.GetAllUserData</td>
<td>List of String</td>
<td>List containing all permanently stored user data in string format</td>
<td></td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.Category</td>
<td>Category</td>
<td>Global variable of type Category</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.Dimension</td>
<td>Dimension</td>
<td>Global variable of type Dimension</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.Hex</td>
<td>Hex</td>
<td>Global variable of type Hex</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.IP</td>
<td>IP</td>
<td>Global variable of type IP</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.IPRange</td>
<td>IPRange</td>
<td>Global variable of type IPRange</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.List.Category</td>
<td>List of Category</td>
<td>Global variable of type List of Category</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.List.IP</td>
<td>List of IP</td>
<td>Global variable of type IP</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.List.IPRange</td>
<td>List of IPRange</td>
<td>Global variable of type IPRange</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.List.MediaType</td>
<td>List of MediaType</td>
<td>Global variable of type MediaType</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.List.Number</td>
<td>List of Number</td>
<td>Global variable of type Number</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.MediaType</td>
<td>MediaType</td>
<td>Global variable of type MediaType</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.Number</td>
<td>Number</td>
<td>Global variable of type Number</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.String</td>
<td>String</td>
<td>Global variable of type String</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetGlobalData.WildcardExpression</td>
<td>Wildcard Expression</td>
<td>Global variable of type WildcardExpression</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.Category</td>
<td>Category</td>
<td>User variable of type Category</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.Dimension</td>
<td>Dimension</td>
<td>User variable of type Dimension</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.Hex</td>
<td>Hex</td>
<td>User variable of type Hex</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.IP</td>
<td>IP</td>
<td>User variable of type IP</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.IPRange</td>
<td>IPRange</td>
<td>User variable of type IPRange</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.List.IP</td>
<td>List of IP</td>
<td>User variable of type List of IP</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.List.IPRange</td>
<td>List of IPRange</td>
<td>User variable of type List of IPRange</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.List.MediaType</td>
<td>List of MediaType</td>
<td>User variable of type List of MediaType</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>PDStorage.GetUserData.List.Number</td>
<td>List of Number</td>
<td>User variable of type List of Number</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.MediaType</td>
<td>MediaType</td>
<td>User variable of type MediaType</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.Number</td>
<td>Number</td>
<td>User variable of type Number</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.String</td>
<td>String</td>
<td>User variable of type String</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.GetUserData.WildcardExpression</td>
<td>Wildcard Expression</td>
<td>User variable of type WildcardExpression</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.HasGlobalData</td>
<td>Boolean</td>
<td>If true, permanently stored global data is available.</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>PDStorage.HasGlobalDataWait</td>
<td>Boolean</td>
<td>If true, a request is kept waiting until the requested global variable exists in the storage or the specified time interval has elapsed. The value of the property is then set to false. It is true by default.</td>
<td>1 String: Variable key 2 Number: Timeout (in seconds)</td>
</tr>
<tr>
<td>PDStorage.HasUserData</td>
<td>Boolean</td>
<td>If true, permanently stored user data is available.</td>
<td>String: Variable key</td>
</tr>
<tr>
<td>ProgressPage.Enabled</td>
<td>Boolean</td>
<td>If true, download progress is indicated to the user by a progress page.</td>
<td></td>
</tr>
<tr>
<td>ProgressPage.Sent</td>
<td>Boolean</td>
<td>If true, a progress page is displayed when a requested web object is downloaded.</td>
<td></td>
</tr>
<tr>
<td>ProtocolDetector.DetectedProtocol</td>
<td>String</td>
<td>String containing name of a protocol that has been detected as being used for traffic on a connection between Web Gateway and a client.</td>
<td></td>
</tr>
<tr>
<td>ProtocolDetector.ProtocolFilterable</td>
<td>Boolean</td>
<td>If true, filtering is supported for a protocol that has been detected as being used for web traffic.</td>
<td></td>
</tr>
</tbody>
</table>
### Table A-19 Properties – P (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol.FailureDescription</td>
<td>String</td>
<td>String containing description of a connection error under the current protocol</td>
<td></td>
</tr>
<tr>
<td>Proxy.EndUserURL</td>
<td>String</td>
<td>String representing URL for display to a user</td>
<td></td>
</tr>
<tr>
<td>Proxy.IP</td>
<td>IP</td>
<td>IP address of Web Gateway</td>
<td></td>
</tr>
<tr>
<td>Proxy.Outbound.IP</td>
<td>IP</td>
<td>Source IP address that Web Gateway uses when connecting to web servers or next-hop proxies</td>
<td>Do not confuse this property with the <code>Proxy.Outbound.IP</code> property, which has no dot before <code>IP</code>.</td>
</tr>
<tr>
<td>Proxy.Outbound.IPList</td>
<td>List of IP</td>
<td>List of source IP addresses that Web Gateway selects an address from when connecting to web servers or next-hop proxies.</td>
<td></td>
</tr>
<tr>
<td>Proxy.Outbound.Port</td>
<td>Number</td>
<td>Number of source port that Web Gateway uses when connecting to web servers or next-hop proxies</td>
<td>Number: Position of source IP address in list</td>
</tr>
<tr>
<td>Proxy.OutboundIP</td>
<td>IP</td>
<td>Source IP address for replacing multiple source IP addresses that Web Gateway might use when connecting to web servers or next-hop proxies. The address is selected from a list, using a number parameter to identify its position in the list.</td>
<td>Do not confuse this property with the <code>Proxy.Outbound.IP</code> property, which has a dot before <code>IP</code>.</td>
</tr>
<tr>
<td>Proxy.Port</td>
<td>Number</td>
<td>Number of a port used by Web Gateway</td>
<td></td>
</tr>
</tbody>
</table>
Properties - Q

The following table describes the properties that have names beginning with Q.

Table A-20 Properties – Q

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota.AuthorizedOverride.GetLogin</td>
<td>String</td>
<td>User name submitted for performing an authorized override</td>
<td></td>
</tr>
<tr>
<td>Quota.AuthorizedOverride.IsActivationRequest</td>
<td>Boolean</td>
<td>If true, an authorized user has chosen to continue with a authorized override session after session time has been exceeded.</td>
<td></td>
</tr>
<tr>
<td>Quota.AuthorizedOverride.IsActivationRequest.Strict</td>
<td>Boolean</td>
<td>If true, an authorized user has chosen to continue with an Authorized Override session and the request for continuing the session applies to the current settings.</td>
<td></td>
</tr>
<tr>
<td>Quota.AuthorizedOverride.JS.ActivateSession</td>
<td>String</td>
<td>String in JavaScript code calling the function that is executed when an authorized user chooses to start a new session by clicking the appropriate button in the authorized override template. The code is provided when the template is created and displayed to the user.</td>
<td></td>
</tr>
<tr>
<td>Quota.AuthorizedOverride.LastAuthorizedPerson</td>
<td>String</td>
<td>User name of the last person who performed an authorized override to provide additional session time for a user</td>
<td></td>
</tr>
<tr>
<td>Quota.AuthorizedOverride.RemainingSession</td>
<td>Number</td>
<td>Remaining time (in seconds) for an authorized override session</td>
<td></td>
</tr>
<tr>
<td>Quota.AuthorizedOverride.SessionExceeded</td>
<td>Boolean</td>
<td>If true, the time allowed for an authorized override session has been exceeded.</td>
<td></td>
</tr>
<tr>
<td>Quota.AuthorizedOverride.SessionLength</td>
<td>Number</td>
<td>Time length (in seconds) for an authorized override session</td>
<td></td>
</tr>
<tr>
<td>Quota.Coaching.IsActivationRequest</td>
<td>Boolean</td>
<td>If true, a user has chosen to continue with a new coaching session after session time has been exceeded.</td>
<td></td>
</tr>
</tbody>
</table>
Table A-20 Properties – Q (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota.Coaching.IsActivationRequest.Strict</td>
<td>Boolean</td>
<td>If true, a user has chosen to continue with a Coaching session and the request for continuing the session applies to the current settings.</td>
<td></td>
</tr>
<tr>
<td>Quota.Coaching.JS.ActivateSession</td>
<td>String</td>
<td>String in JavaScript code calling the function that is executed when a user chooses to start a new session by clicking the appropriate button in the coaching session template. The code is provided when the template is created and displayed to the user.</td>
<td></td>
</tr>
<tr>
<td>Quota.Coaching.RemainingSession</td>
<td>Number</td>
<td>Remaining time (in seconds) for a coaching session</td>
<td></td>
</tr>
<tr>
<td>Quota.Coaching.SessionExceeded</td>
<td>Boolean</td>
<td>If true, the time allowed for a coaching session has been exceeded.</td>
<td></td>
</tr>
<tr>
<td>Quota.Coaching.SessionLength</td>
<td>Number</td>
<td>Time length (in seconds) for a coaching session</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.Exceeded</td>
<td>Boolean</td>
<td>If true, the time quota has been exceeded.</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.IsActivationRequest</td>
<td>Boolean</td>
<td>If true, a user has chosen to continue with a new time session after session time has been exceeded.</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.IsActivationRequest.Strict</td>
<td>Boolean</td>
<td>If true, a user has chosen to continue with a new Time session and the request for continuing the session applies to the current settings.</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.JS.ActivateSession</td>
<td>String</td>
<td>String in JavaScript code calling the function that is executed when a user chooses to start a new session by clicking the appropriate button in the time session template. The code is provided when the template is created and displayed to the user.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Quota.Time.RemainingDay</td>
<td>Number</td>
<td>Time (in seconds) remaining from the configured time quota for the current day</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.RemainingDay.ReducedAtActivation</td>
<td>Number</td>
<td>Time (in seconds) remaining from the configured time quota for the current day when a user has just started a session</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.RemainingDay.ReducedAtDeactivation</td>
<td>Number</td>
<td>Time (in seconds) remaining from the configured time quota for the current day when a user has just closed a session</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.RemainingMonth</td>
<td>Number</td>
<td>Time (in seconds) remaining from the configured time quota for the current month</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.RemainingMonth.ReducedAtActivation</td>
<td>Number</td>
<td>Time (in seconds) remaining from the configured time quota for the current month when a user has just started a session</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.RemainingMonth.ReducedAtDeactivation</td>
<td>Number</td>
<td>Time (in seconds) remaining from the configured time quota for the current month when a user has just closed a session</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.RemainingSession</td>
<td>Number</td>
<td>Remaining time (in seconds) for a time session</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.RemainingWeek</td>
<td>Number</td>
<td>Time (in seconds) remaining from the configured time quota for the current week</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.RemainingWeek.ReducedAtActivation</td>
<td>Number</td>
<td>Time (in seconds) remaining from the configured time quota for the current week when a user has just started a session</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.RemainingWeek.ReducedAtDeactivation</td>
<td>Number</td>
<td>Time (in seconds) remaining from the configured time quota for the current week when a user has just closed a session</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.SessionExceeded</td>
<td>Boolean</td>
<td>If true, the time allowed for a time session has been exceeded.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Quota.Time.SessionLength</td>
<td>Number</td>
<td>Time length (in seconds) for a time session</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.SizePerDay</td>
<td>Number</td>
<td>Time (in seconds) allowed per day under the configured quota</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.SizePerMonth</td>
<td>Number</td>
<td>Time (in seconds) allowed per month under the configured quota</td>
<td></td>
</tr>
<tr>
<td>Quota.Time.SizePerWeek</td>
<td>Number</td>
<td>Time (in seconds) allowed per week under the configured quota</td>
<td></td>
</tr>
<tr>
<td>Quota.Volume.Exceeded</td>
<td>Boolean</td>
<td>If true, the volume quota has been exceeded.</td>
<td></td>
</tr>
<tr>
<td>Quota.Volume.IsActivationRequest</td>
<td>Boolean</td>
<td>If true, a user has chosen to continue with a new volume session after session time has been exceeded.</td>
<td></td>
</tr>
<tr>
<td>Quota.Volume.IsActivationRequest.Strict</td>
<td>Boolean</td>
<td>If true, a user has chosen to continue a session when the configured volume has been exceeded and the request for continuing the session applies to the current settings.</td>
<td></td>
</tr>
<tr>
<td>Quota.Volume.JS.ActivateSession</td>
<td>String</td>
<td>String in JavaScript code calling the function that is executed when a user chooses to start a new session by clicking the appropriate button in the volume session template. The code is provided when the template is created and displayed to the user.</td>
<td></td>
</tr>
<tr>
<td>Quota.Volume.RemainingDay</td>
<td>Number</td>
<td>Volume (in bytes) remaining from the configured volume quota for the current day</td>
<td></td>
</tr>
<tr>
<td>Quota.Volume.RemainingMonth</td>
<td>Number</td>
<td>Volume (in bytes) remaining from the configured volume quota for the current month</td>
<td></td>
</tr>
<tr>
<td>Quota.Volume.RemainingSession</td>
<td>Number</td>
<td>Remaining time (in seconds) for a volume session</td>
<td></td>
</tr>
</tbody>
</table>
**Table A-20 Properties – Q (continued)**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota.Volume.RemainingWeek</td>
<td>Number</td>
<td>Volume (in bytes) remaining from the configured volume quota for the current week</td>
</tr>
<tr>
<td>Quota.Volume.SessionExceeded</td>
<td>Boolean</td>
<td>If true, the time allowed for a volume session has been exceeded.</td>
</tr>
<tr>
<td>Quota.Volume.SessionLength</td>
<td>Number</td>
<td>Time length (in seconds) for a volume session</td>
</tr>
<tr>
<td>Quota.Volume.SizePerDay</td>
<td>Number</td>
<td>Volume (in bytes) allowed per day under the configured quota</td>
</tr>
<tr>
<td>Quota.Volume.SizePerMonth</td>
<td>Number</td>
<td>Volume (in bytes) allowed per month under the configured quota</td>
</tr>
<tr>
<td>Quota.Volume.SizePerWeek</td>
<td>Number</td>
<td>Volume (in bytes) allowed per week under the configured quota</td>
</tr>
</tbody>
</table>

### Properties - R

The following table describes the properties that have names beginning with R.

**Table A-21 Properties – R**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect.URL</td>
<td>String</td>
<td>String representing a URL that a user is redirected to by an authentication or quota rule</td>
</tr>
<tr>
<td>Reporting.URL.Categories</td>
<td>List of Category</td>
<td>List of all URL categories used on the appliance</td>
</tr>
<tr>
<td>Reporting.URL.Reputation</td>
<td>List of Number</td>
<td>List of all reputation score values used on the appliance</td>
</tr>
<tr>
<td>Request.Header.FirstLine</td>
<td>String</td>
<td>First line of a header sent with a request</td>
</tr>
<tr>
<td>Request.POSTForm.Get</td>
<td>String</td>
<td>Retrieves URL encoded data in the POST form sent by the external Identity Provider.</td>
</tr>
<tr>
<td>Request.ProtocolAndVersion</td>
<td>String</td>
<td>Protocol and protocol version used when a request is sent</td>
</tr>
<tr>
<td>Response.ProtocolAndVersion</td>
<td>String</td>
<td>Protocol and protocol version used when a response is sent</td>
</tr>
<tr>
<td>Response.Redirect.URL</td>
<td>String</td>
<td>URL that a user is redirected to when a response is sent</td>
</tr>
<tr>
<td>Response.StatusCode</td>
<td>String</td>
<td>Status code of a response</td>
</tr>
<tr>
<td>Rules.CurrentRuleID</td>
<td>String</td>
<td>ID of the rule that is currently processed</td>
</tr>
<tr>
<td>Rules.CurrentRuleName</td>
<td>String</td>
<td>Name of the rule that is currently processed</td>
</tr>
</tbody>
</table>
Table A-21 Properties – R (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules.CurrentRuleSetName</td>
<td>String</td>
<td>Name of the rule set that is currently processed</td>
<td></td>
</tr>
<tr>
<td>Rules.EvaluatedRules</td>
<td>List of String</td>
<td>List of all rules that have been processed</td>
<td></td>
</tr>
<tr>
<td>Rules.EvaluatedRules.Names</td>
<td>List of String</td>
<td>List with names of all rules that have been processed</td>
<td></td>
</tr>
<tr>
<td>Rules.FiredRules</td>
<td>List of String</td>
<td>List of all rules that have applied</td>
<td></td>
</tr>
<tr>
<td>Rules.FiredRules.Names</td>
<td>List of String</td>
<td>List with names of all rules that have applied</td>
<td></td>
</tr>
</tbody>
</table>

Properties - S

The following table describes the properties that have names beginning with S.

Table A-22 Properties – S

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecureReverseProxy.EmbeddedHost</td>
<td>String</td>
<td>Host name of a URL in an HTTP request that is embedded in an HTTPS request</td>
<td></td>
</tr>
<tr>
<td>SecureReverseProxy.EmbeddedProtocol</td>
<td>String</td>
<td>Protocol of a URL in an HTTP request that is embedded in an HTTPS request</td>
<td></td>
</tr>
<tr>
<td>SecureReverseProxy.EmbeddedURL</td>
<td>String</td>
<td>URL in an HTTP request that is embedded in an HTTPS request</td>
<td>String: Host name of the URL</td>
</tr>
<tr>
<td>SecureReverseProxy.GetDomain</td>
<td>String</td>
<td>Domain specified in the settings for the SecureReverseProxy module</td>
<td></td>
</tr>
<tr>
<td>SecureReverseProxy.IsValidReverseProxyRequest</td>
<td>Boolean</td>
<td>If true, the URL submitted in a request has the format required in a SecureReverseProxy configuration.</td>
<td></td>
</tr>
<tr>
<td>SecureReverseProxy.URLToEmbed</td>
<td>String</td>
<td>URL submitted in a HTTP request that is embedded in an HTTPS request</td>
<td></td>
</tr>
<tr>
<td>SecureToken.CreateToken</td>
<td>String</td>
<td>Encrypted string</td>
<td>String: String to encrypt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This string serves as a token for securing an IP address. An AES-128-bit algorithm is used to create the token.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Depending on the value of a parameter in the settings of the SecureReverseProxy module, the string includes a time stamp.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SecureToken.IsValid</td>
<td>Boolean</td>
<td>If true, the specified token is valid and has not expired.</td>
<td>1  String: Token to be checked</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Depending on the value of a parameter in the settings of the SecureReverse</td>
<td>2  Number: Time (in seconds) elapse until token expires</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Proxy module, the token string includes no time stamp.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expiration of the token is then not checked.</td>
<td></td>
</tr>
<tr>
<td>SecureToken.GetString</td>
<td>String</td>
<td>String serving as a token for securing an IP address.</td>
<td>1  String: Token to be checked</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the token is invalid or has expired, the string is empty.</td>
<td>2  Number: Time (in seconds) elapse until token expires</td>
</tr>
<tr>
<td>SNMP.Trap.Additional</td>
<td>String</td>
<td>Additional message sent to a trap under the SNMP protocol</td>
<td></td>
</tr>
<tr>
<td>SOCKS.Version</td>
<td>String</td>
<td>Version of the SOCKS protocol that is used when a client requests access to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a web object under this protocol.</td>
<td></td>
</tr>
<tr>
<td>SSL.Certificate.CN.ToWildcard</td>
<td>Wildcard Expression</td>
<td>Common name in an SSL certificate converted into a wildcard expression</td>
<td>1  String: Common name to convert</td>
</tr>
<tr>
<td>SSL.Client.Certificate.Serial</td>
<td>String</td>
<td>Serial of a client certificate</td>
<td></td>
</tr>
<tr>
<td>SSL.ClientContext.IsApplied</td>
<td>Boolean</td>
<td>If true, parameters for setting the client context in SSL-secured</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>communication have been configured.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.Certificate.AlternativeCNs</td>
<td>List of Wildcard Expression</td>
<td>List of alternative common names for a web server as used in SSL certificates</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.Certificate.CN</td>
<td>String</td>
<td>Common name of a web server provided in a certificate for SSL-secured</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>communication.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.Certificate.CN.HasWildcards</td>
<td>Boolean</td>
<td>If true, the common name for a web server in an SSL certificate includes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>wildcards.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.Certificate.DaysExpired</td>
<td>Number</td>
<td>Number of days that an SSL certificate for a web server has expired</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.Certificate.HostAndCertificate</td>
<td>HostAndCertificate</td>
<td>Host name and certificate for connecting to a web server in SSL-secured communication</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>SSL.Server.Certificate.SelfSigned</td>
<td>Boolean</td>
<td>If true, an SSL certificate for a web server is self-signed.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.Certificate.SHA1Digest</td>
<td>String</td>
<td>String representing an SHA1Digest of a SSL certificate for a web server</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.CertificateChain.AllRevocationStatusesKnown</td>
<td>Boolean</td>
<td>If true, it is known of all SSL certificates in a certificate chain for a web server whether they are revoked or not.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.CertificateChain.ContainsExpiredCA</td>
<td>Boolean</td>
<td>If true, an SSL certificate in a certificate chain for a web server has expired.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.CertificateChain.ContainsRevoked</td>
<td>Boolean</td>
<td>If true, an SSL certificate in a certificate chain for a web server has been revoked.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.CertificateChain.FirstKnownCAIsTrusted</td>
<td>Boolean</td>
<td>If true, a the certificate authority for issuing SSL certificates that has been found first in a certificate chain for a web server is trusted.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.CertificateChain.FoundKnownCA</td>
<td>Boolean</td>
<td>If true, a known certificate authority for issuing SSL certificates has been found in a certificate chain for a web server.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.CertificateChain.IsComplete</td>
<td>Boolean</td>
<td>If true, the chain of SSL certificates for a web server is complete.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.CertificateChain.Length</td>
<td>Number</td>
<td>Number of SSL certificates in a certificate chain for a web server</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.CertificateChain.PathLengthExceeded</td>
<td>Boolean</td>
<td>If true, the chain of SSL certificates for a web server exceeds the allowed length.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.Cipher.KeyExchangeBits</td>
<td>Number</td>
<td>Normalized strength of the weakest link involved in a key exchange performed in SSL-secured communication.</td>
<td></td>
</tr>
<tr>
<td>SSL.Server.Handshake.CertificateIsRequested</td>
<td>Boolean</td>
<td>If true, a handshake is requested for setting up a connection to a web server in SSL-secured communication.</td>
<td></td>
</tr>
<tr>
<td>SSO.Action</td>
<td>String</td>
<td>Returns the name of an internal action performed in response to an SSO request.</td>
<td></td>
</tr>
<tr>
<td>SSO.Config</td>
<td>String</td>
<td>Returns the name of the settings used by an internal action performed in response to an SSO request.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SSO.Debug</td>
<td>String</td>
<td>Returns an SSO debug message.</td>
<td></td>
</tr>
<tr>
<td>SSO.GetConnectorInfo</td>
<td>Variable</td>
<td>Returns information about the SSO connector to the service the user is</td>
<td>String: Service ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>requesting. This information is stored as a JSON object in a local variable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>named sso-conn-info.</td>
<td></td>
</tr>
<tr>
<td>SSO.GetData</td>
<td>JSON object</td>
<td>Returns additional information needed for SAML single sign-on.</td>
<td></td>
</tr>
<tr>
<td>SSO.GetDatFile</td>
<td>String</td>
<td>Retrieves the specified DAT file from the update server and returns the</td>
<td>String: Name of the SSO DAT file</td>
</tr>
<tr>
<td></td>
<td></td>
<td>contents of the file in a string.</td>
<td></td>
</tr>
<tr>
<td>SSO.GetIceTokenLoginAction</td>
<td>String</td>
<td>Returns the user information needed to complete single sign-on to the</td>
<td>1 String: Service ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>requested service or application.</td>
<td>2 Variable: sso-user-data</td>
</tr>
<tr>
<td>SSO.GetPostLoginAction</td>
<td>String</td>
<td>Returns the information needed to complete single sign-on to the requested</td>
<td>1 String: Identity Provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTP service or application.</td>
<td>2 String: User name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 String: Service ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 String: User account</td>
</tr>
<tr>
<td>SSO.GetSAMLLoginAction</td>
<td>String</td>
<td>Returns the user information needed to complete single sign-on to the</td>
<td>1 String: Service ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>requested SAML service or application.</td>
<td>2 Variable: sso-user-data</td>
</tr>
<tr>
<td>SSO.GetServices</td>
<td>JSON object</td>
<td>Returns all information about the current user added by the SSO Select</td>
<td>Variable: &quot;conditions&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Services rule set. This information is returned in JSON format and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>includes the names of cloud services the user is allowed to access and all</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>account information.</td>
<td></td>
</tr>
<tr>
<td>SSO.GetTools</td>
<td>String</td>
<td>Returns a string of JavaScript tools.</td>
<td></td>
</tr>
<tr>
<td>SSO.IsManagementRequest</td>
<td>Boolean</td>
<td>Returns a true value if the current request is an SSO request and one or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>both of the following conditions are met:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web Gateway has received an SSO request.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The SSO.Action property is processed with valid settings.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>SSO.LogProperties</td>
<td>JSON object</td>
<td>Stores information about each SSO request that is used to generate the SSO access and SSO trace logs.</td>
<td></td>
</tr>
<tr>
<td>SSO.ManagementHost</td>
<td>String</td>
<td>Returns the host name of the SSO service specified in the configuration. Typically, this value is the name of the server hosting the SSO service provided by Web Gateway.</td>
<td></td>
</tr>
<tr>
<td>SSO.OTPRequired</td>
<td>Boolean</td>
<td>Returns a true value if the SSO action requires OTP authentication.</td>
<td></td>
</tr>
<tr>
<td>SSO.ProcessTask</td>
<td>Boolean</td>
<td>Processes common SSO tasks, such as credential management, using the Single Sign On settings. If the SSO tasks are processed successfully, this property returns a true value.</td>
<td></td>
</tr>
<tr>
<td>SSO.UserHasAccessToService</td>
<td>Boolean</td>
<td>Returns a true value if the user is allowed to access the cloud service or manage the account.</td>
<td></td>
</tr>
<tr>
<td>SSOConnector.ToString</td>
<td>String</td>
<td>Converts the name of a cloud connector to the Service ID that identifies the corresponding cloud service or application.</td>
<td>String: Name of cloud connector</td>
</tr>
<tr>
<td>Statistics.Counter.Get</td>
<td>Number</td>
<td>Number of occurrences of an activity or situation recorded on a counter.</td>
<td>String: Name of counter</td>
</tr>
<tr>
<td>Statistics.Counter.GetCurrent</td>
<td>Number</td>
<td>Number of occurrences of an activity or situation recorded on a counter (fully completed) during the last minute</td>
<td>String: Name of counter</td>
</tr>
<tr>
<td>Stopwatch.GetMicroSeconds</td>
<td>Number</td>
<td>Time measured for rule set processing in microseconds</td>
<td>String: Name of rule set</td>
</tr>
<tr>
<td>Stopwatch.GetMilliSeconds</td>
<td>Number</td>
<td>Time measured for rule set processing in milliseconds</td>
<td>String: Name of rule set</td>
</tr>
<tr>
<td>StreamDetector.IsMediaStream</td>
<td>Boolean</td>
<td>If true, a requested web object is streaming media. This is the basic property used in streaming media filtering.</td>
<td></td>
</tr>
<tr>
<td>StreamDetector.MatchedRule</td>
<td>String</td>
<td>Name of a streaming media filtering rule that has matched. This property is given a value if the StreamDetector.IsMediaStream property is set to true.</td>
<td></td>
</tr>
<tr>
<td>StreamDetector.Probability</td>
<td>Number</td>
<td>Probability for a web object that it is streaming media. Values range from 1 to 100. This property is given a value if the StreamDetector.IsMediaStream property is set to true.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>String.BackwardFind</td>
<td>Number</td>
<td>Position where a substring begins that is found in a string by a backward search.</td>
<td>1 String: String containing substring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 String: Substring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Position where backward search for substring begins.</td>
</tr>
<tr>
<td>String.Base64DecodeAsBinary</td>
<td>String</td>
<td>String of binary digits that is the result of decoding a base-64 encoded string.</td>
<td>String: String encoded format</td>
</tr>
<tr>
<td>String.Base64DecodeAsText</td>
<td>String</td>
<td>Text string that is the result of decoding a base-64 encoded string.</td>
<td>String: String encoded format</td>
</tr>
<tr>
<td>String.Base64Encode</td>
<td>String</td>
<td>String that is the result of using the base-64 encoding method to encode a string.</td>
<td>String: String to encode</td>
</tr>
<tr>
<td>String.BelongsToDomains</td>
<td>Boolean</td>
<td>If true, a specified string is found in a list of domain names</td>
<td>1 String: String to be found in list</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 List of string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value of the property is &quot;true&quot; if the string matches a list entry, which means it is a domain name.</td>
<td>List of domain names</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value of the property is also &quot;true&quot; if the string is a character or sequence of characters followed by a dot and a substring that matches a list entry (*.&lt;list entry&gt;), which means it is the name for a subdomain of a domain in the list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>In both cases the string is set as the value of the List.LastMatches property.</td>
<td></td>
</tr>
<tr>
<td>String.Concat</td>
<td>String</td>
<td>Concatenation of two specified strings</td>
<td>1 String: First string to concatenate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 String: Second string to concatenate</td>
</tr>
<tr>
<td>String.CRLF</td>
<td>String</td>
<td>Carriage-return line-feed</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| `String.Find`    | Number       | Position where a substring begins that is found in a string by a forward search | 1 String: String containing substring  
2 String: Substring  
3 Number: Position where forward search for substring begins |
| `String.FindFirstOf` | Number       | Position of the first character of a substring found in a string            | 1 String: String containing substring  
2 String: Substring  
3 Number: Position where search for substring begins |
| `String.FindLastOf` | Number       | Position of the last character of a substring found in a string             | 1 String: String containing substring  
2 String: Substring  
3 Number: Position where search for substring begins |
| `String.GetWordCount` | Number       | Number of words in a string                                                 | String: String get number of words for |
| `String.Hash`    | String       | Hash value of a particular type for a given string                          | 1 String: String find hash value for  
2 String: Hash type |
<p>| <code>String.IsEmpty</code> | Boolean      | If true, the specified string is empty.                                     | String: String checked for being empty |
| <code>String.Length</code>  | Number       | Number of characters in a string                                            | String: String count characters for |
| <code>String.LF</code>      | String       | Line-feed                                                                   |                                                                           |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>String.MakeAnonymous</td>
<td>String</td>
<td>String that has been made anonymous and requires one or two passwords for reverting anonymization</td>
<td>String: String to anonymize</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The string that is to be anonymized is specified as a parameter of the property.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The passwords are set within the Anonymization settings, which are provided as settings of the property.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can use the property in a rule to anonymize sensitive data, for example, the user name that is retrieved as the value of the Authentication.UserName property.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>An event in this rule sets the authentication property to the value of String.MakeAnonymous, which takes the authentication property as its parameter, so its value is the anonymized user name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>After the set event has been executed, the anonymized user name is also the value of Authentication.UserName. Sensitive information is protected this way.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the rule to work, a rule with the authentication property must have been processed before. Otherwise the string that is to be anonymized would not be known.</td>
<td></td>
</tr>
<tr>
<td>String.MatchWildcard</td>
<td>List of String</td>
<td>List of terms in a string that match a wildcard expression</td>
<td>1 String: String with matching terms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Wildcard Expression: Wildcard expression to match</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 Number: Position where search for substring begins</td>
<td></td>
</tr>
</tbody>
</table>
Table A-22 Properties – S (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| String.Replace        | String| String having a substring replaced by a string as specified | 1 String: String containing substring to replace  
  2 Number: Position where replacement begins  
  3 Number: Number of characters to replace  
  4 String: Replacing string |
| String.ReplaceAll     | String| String having each occurrence of a substring replaced by string as specified | 1 String: String containing substring to replace  
  2 String: Replacing substring  
  3 String: Substring to replace |
| String.ReplaceAllMatches | String| String having each occurrence of a substring that matches a wildcard expression replaced by a string as specified | 1 String: String containing substring to replace  
  2 Wildcard Expression: Wildcard expression to match  
  3 String: Substring to replace |
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>String.ReplaceFirst</td>
<td>String</td>
<td>String having first occurrence of a substring replaced by a string as specified</td>
<td>1 String: String containing substring to replace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 String: String: Substring to replace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 String: String: Replacing string</td>
</tr>
<tr>
<td>String.ReplaceFirstMatch</td>
<td>String</td>
<td>String having first occurrence of a substring that matches a wildcard expression replaced by a string as specified</td>
<td>1 String: String containing substring to replace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Wildcard Expression: String: Wildcard expression to match</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 String: String: Replacing substring</td>
</tr>
<tr>
<td>String.ReplaceIfEquals</td>
<td>String</td>
<td>String having every occurrence of a substring replaced by a string as specified</td>
<td>1 String: String containing substring to replace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 String: String: Substring to replace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 String: String: Replacing substring</td>
</tr>
<tr>
<td>String.Substring</td>
<td>String</td>
<td>Substring contained in a string specified by start position and length</td>
<td>1 String: String containing substring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 Number: Position where substring begins</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 Number: Number of characters in substring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If no number specified, the substring extends to the end of the original string</td>
</tr>
</tbody>
</table>
### Table A-22 Properties – S (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>String.SubStringBetween</td>
<td>String</td>
<td>Substring of string extending between two other substrings of this string</td>
<td>1 String: String containing substrings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The search for this substring begins with looking for the first of the</td>
<td>2 String: Substring ending immediately before the wanted substring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>other substrings. If this string is found, the search is continued with</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>looking for the second substring. If the first substring is not found, the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>search has no result. If the second substring is not found, the wanted</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>substring extends from the end of the first substring to the end of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>main string.</td>
<td></td>
</tr>
<tr>
<td>String.ToCategory</td>
<td>Category</td>
<td>String converted into a category</td>
<td>String: String convert</td>
</tr>
<tr>
<td>String.ToDimension</td>
<td>Dimension</td>
<td>String converted into a dimension</td>
<td>String: String convert</td>
</tr>
<tr>
<td>String.ToHex</td>
<td>Hex</td>
<td>String converted into a hex value</td>
<td>String: String convert</td>
</tr>
<tr>
<td>String.ToIP</td>
<td>IP</td>
<td>String converted into an IP address</td>
<td>String: String convert</td>
</tr>
<tr>
<td>String.ToIPRange</td>
<td>PRange</td>
<td>String converted into a range of IP addresses</td>
<td>String: String convert</td>
</tr>
<tr>
<td>String.ToMediaType</td>
<td>MediaType</td>
<td>String converted into a media type</td>
<td>String: String convert</td>
</tr>
<tr>
<td>String.ToNumber</td>
<td>Number</td>
<td>String converted into a number</td>
<td>String: String convert</td>
</tr>
<tr>
<td>String.ToSSOConnector</td>
<td>String</td>
<td>Converts the Service ID that identifies a cloud service or application to</td>
<td>String: Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the name of the corresponding cloud connector.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
</tbody>
</table>
| String.ToStringList | List of String | String converted into a string list. The string list is a list of the elements in the string to convert. For example, the string to convert can be a text and the string list a list of the words in this text. The delimiter is a substring that separates elements in the string to convert. For example, in a normal text, the delimiter is the whitespace. The substring can be a single character, such as the whitespace, or multiple characters. To specify the whitespace, hit the space bar. A trim character is a character that appears at the beginning or end of an element in the string to convert, but not in the string list. A trim character can, for example, be a comma, a period, or a single quotation mark. It can also be an “invisible” character, such as a tab stop or a line feed. To specify trim characters, type them in the input field that is provided on the user interface without separating them from each other. Use the following combinations to type invisible characters: \t – tab stop \r – carriage return \n – line feed \b – backspace \\ – backslash If you specify a character as a delimiter, it is also deleted from the resulting string list, so you need not specify it as a trim character. | 1 String: String convert  
2 String: Delimiter  
3 String: Substring beginning immediately after the wanted substring |
| String.ToWildcard | Wildcard Expression | String converted into a wildcard expression | String: String convert |
| String.URLDecode | String | Standard format of a URL that was specified in encoded format | String: URL in encoded format |
| String.URLEncode | String | Encoded format of a URL | String: URL to encode |
| System.HostName | String | Host name of an appliance | |
| System.UUID | String | UUID (Universal Unique Identifier) of an appliance | |
### Properties - T

The following table describes the properties that have names beginning with T.

**Table A-23  Properties – T**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIE.Filereputation</td>
<td>Number</td>
<td>File reputation score that has been retrieved from a TIE server</td>
<td></td>
</tr>
<tr>
<td>Timer.FirstReceivedFirstSentClient</td>
<td>Number</td>
<td>Processing time consumed between receiving the first byte from a client on the appliance and sending the first byte to this client within a transaction</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using this property is only supported when HTTP or HTTPS connections are involved, but not for FTP connections.</td>
<td></td>
</tr>
<tr>
<td>Timer.FirstSentFirstReceivedServer</td>
<td>Number</td>
<td>Processing time consumed between sending the first byte from the appliance to a web server and receiving the first byte from this server within a transaction</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using this property is only supported when HTTP or HTTPS connections are involved, but not for FTP connections.</td>
<td></td>
</tr>
<tr>
<td>Timer.HandleConnectToServer</td>
<td>Number</td>
<td>Processing time consumed for connecting to a web server within a transaction</td>
<td></td>
</tr>
<tr>
<td>Timer.LastReceivedLastSentClient</td>
<td>Number</td>
<td>Processing time consumed between receiving the last byte from a client on the appliance and sending the last byte to this client within a transaction</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using this property is only supported when HTTP or HTTPS connections are involved, but not for FTP connections.</td>
<td></td>
</tr>
<tr>
<td>Timer.LastSentLastReceivedServer</td>
<td>Number</td>
<td>Processing time consumed between sending the last byte from the appliance to a web server and receiving the last byte from this server within a transaction</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using this property is only supported when HTTP or HTTPS connections are involved, but not for FTP connections.</td>
<td></td>
</tr>
<tr>
<td>Timer.ResolveHostNameViaDNS</td>
<td>Number</td>
<td>Processing time consumed for looking up a host name on a DNS server within a transaction</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Only lookups on external servers are considered. Cache lookups are disregarded.</td>
<td></td>
</tr>
</tbody>
</table>
### Table A-23 Properties – T (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer.TimeInExternals</td>
<td>Number</td>
<td>Time (in milliseconds) consumed when processing a request in waiting for responses by components other than the rule engine that are involved in the process, for example, domain controllers or anti-malware scanning engines. This time is the time that has already been consumed in waiting when the property is evaluated. Waiting periods in all relevant processing cycles are considered when calculating this time.</td>
<td></td>
</tr>
<tr>
<td>Timer.TimeInRuleEngine</td>
<td>Number</td>
<td>Time (in milliseconds) consumed by the rule engine for processing a request, including activities in all relevant processing cycles, at the time when the property is evaluated. Processing a request through all relevant processing cycles is also referred to as a transaction. When the property is evaluated within a rule for log handling, its value is the time that was used by the rule engine for the complete transaction.</td>
<td></td>
</tr>
<tr>
<td>Timer.TimeInTransaction</td>
<td>Number</td>
<td>Time (in milliseconds) consumed for processing a request, including activities in all relevant processing cycles, at the time when the property is evaluated. Time used for rule engine activities and waiting times are summed up in this property value. Processing a request through all relevant processing cycles is also referred to as a transaction. When the property is evaluated within a rule for log handling, its value is the time that was used for the complete transaction.</td>
<td></td>
</tr>
<tr>
<td>Tunnel.Enabled</td>
<td>Boolean</td>
<td>If true, an HTTP or HTTPS tunnel is enabled</td>
<td></td>
</tr>
</tbody>
</table>

### Properties – U
The following table describes the properties that have names beginning with U.

### Table A-24 Properties – U

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>String</td>
<td>URL of a web object</td>
<td></td>
</tr>
<tr>
<td>URL.Categories</td>
<td>List of Category</td>
<td>List of URL categories that a URL belongs to</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>URL.CategoriesForURL</td>
<td>List of Category</td>
<td>List of URL categories that a specified URL belongs to</td>
<td>String: URL in string format</td>
</tr>
<tr>
<td>URL.CategorySetVersion</td>
<td>Number</td>
<td>Version number of the category set that is used for URL filtering</td>
<td></td>
</tr>
<tr>
<td>URL.CloudLookupLedToResult</td>
<td>Boolean</td>
<td>If true, the rating for a URL was retrieved by a cloud lookup that was performed using the Global Threat Intelligence service.</td>
<td></td>
</tr>
<tr>
<td>URL.DestinationIP</td>
<td>IP</td>
<td>IP address for a URL as found in a DNS lookup</td>
<td></td>
</tr>
<tr>
<td>URL.Domain</td>
<td>String</td>
<td>Name of the domain that access was requested to</td>
<td></td>
</tr>
<tr>
<td>URL.DomainSuffix</td>
<td>String</td>
<td>Suffix appended to the name of the domain that access was requested to</td>
<td></td>
</tr>
<tr>
<td>URL.FileExtension</td>
<td>String</td>
<td>Extension of the file name for a requested file</td>
<td></td>
</tr>
<tr>
<td>URL.FileName</td>
<td>String</td>
<td>Name of a file that can be accessed through a URL</td>
<td></td>
</tr>
<tr>
<td>URL.ForwardDNSLedToResult</td>
<td>Boolean</td>
<td>If true, the rating for a URL was retrieved by performing a forward DNS lookup.</td>
<td></td>
</tr>
<tr>
<td>URL.Geolocation</td>
<td>String</td>
<td>ISO 3166 code for the country where the host that a URL belongs to is located</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a value is to be assigned to this property, the following option of the settings for the URL Filter module must be enabled:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Only use online GTI web reputation and categorization services.</em></td>
<td></td>
</tr>
<tr>
<td>URL.Geolocation</td>
<td>String</td>
<td>Name of the country where the host that a given URL belongs to is located</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The URL is the URL that was sent with the request that is currently processed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The country is identified according to ISO 3166.</td>
<td></td>
</tr>
</tbody>
</table>

The name can only be found if the following option of the settings for URL filtering is selected: **Disable local GTI database**
### Table A-24  Properties – U (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL.GeolocationForURL</td>
<td>String</td>
<td>Name of the country where the host that a given URL belongs to is located</td>
<td>String: URL that country name is to be found for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The URL is specified as a parameter of the property.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The country is identified according to ISO 3166.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="https://example.com" alt="Note" /> The name can only be found if the following option of the settings for URL filtering is selected: Disable local GTI database</td>
<td></td>
</tr>
<tr>
<td>URL.GetParameter</td>
<td>String</td>
<td>Parameter of a URL in string format</td>
<td>String: Parameter name</td>
</tr>
<tr>
<td>URL.HasParameter</td>
<td>Boolean</td>
<td>If true, a specified parameter belongs to the parameters of a URL.</td>
<td>String: Parameter name</td>
</tr>
<tr>
<td>URL.Host</td>
<td>String</td>
<td>Host that a URL belongs to</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>URL.Host.BelongsToDomains</td>
<td>Boolean</td>
<td>If true, a host that access was requested to by submitting a particular URL belongs to one of the domains in a list.</td>
<td>List of string: List of domain names</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The name of a host that was found to belong to one of the domains is set as the value of the <code>List:LastMatches</code> property.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can use the <code>URL.Host.BelongsToDomains</code> property to match anything to the domain name in a URL or anything to the left of a dot of a domain name (<code>*.domain.com</code>). Terms including the domain name (<code>*domain.com</code>) are not counted as matches.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domain List is the string list specified as the property parameter. It contains the following entries (dots preceding a domain name in a URL are omitted):</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>twitter.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>mcafee.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>dell.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>k12.ga.us</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>xxx</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Then the criteria:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>URL.Host.BelongsToDomains(&quot;Domain List&quot;)</code> equals true</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>matches for the following URLs:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://twitter.com">http://twitter.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.twitter.com">http://www.twitter.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://my.mcafee.com">http://my.mcafee.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://my.support.dell.com">http://my.support.dell.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.dekalb.k12.ga.us">http://www.dekalb.k12.ga.us</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>any.site.xxx</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>but not for:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://malicious-twitter.com">http://malicious-twitter.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.my.mcafee.com">http://www.my.mcafee.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.treasury.ga.us">http://www.treasury.ga.us</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using this property avoids the effort of creating more complicated solutions to accomplish the same, for example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Using two entries in a list of wildcard expressions, such as:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>twitter.com</code> and <code>*twitter.com</code></td>
<td></td>
</tr>
</tbody>
</table>
### Table A-24 Properties – U (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL.HostIsIP</td>
<td>Boolean</td>
<td>If true, the URL that is submitted for access to a host is an IP address.</td>
<td></td>
</tr>
<tr>
<td>URL.IsHighRisk</td>
<td>Boolean</td>
<td>If true, the reputation score of a URL falls in the high risk range.</td>
<td></td>
</tr>
<tr>
<td>URL.IsMediumRisk</td>
<td>Boolean</td>
<td>If true, the reputation score of a URL falls in the medium risk range.</td>
<td></td>
</tr>
<tr>
<td>URL.IsMinimalRisk</td>
<td>Boolean</td>
<td>If true, the reputation score of a URL falls in the minimal risk range.</td>
<td></td>
</tr>
<tr>
<td>URL.IsUnverified</td>
<td>Boolean</td>
<td>If true, the reputation score of a URL falls in the unverified risk range.</td>
<td></td>
</tr>
<tr>
<td>URL.Parameters</td>
<td>List of String</td>
<td>List of URL parameters</td>
<td></td>
</tr>
<tr>
<td>URL.ParametersString</td>
<td>String</td>
<td>String containing the parameters of a URL.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the URL has parameters, the string begins with the ? character.</td>
<td></td>
</tr>
<tr>
<td>URL.Path</td>
<td>String</td>
<td>Path name for a URL</td>
<td></td>
</tr>
<tr>
<td>URL.Port</td>
<td>Number</td>
<td>Number of a port for a URL</td>
<td></td>
</tr>
<tr>
<td>URL.Protocol</td>
<td>String</td>
<td>Protocol for a URL</td>
<td></td>
</tr>
<tr>
<td>URL.Raw</td>
<td>String</td>
<td>URL in the format originally received on the appliance from a client or other network components. Using this property for rule configuration will speed up processing because it saves the time used for converting URL code to a human readable format, as it is done for the simple URL property.</td>
<td></td>
</tr>
<tr>
<td>URL.Reputation</td>
<td>Number</td>
<td>Reputation score for a given URL.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The URL is the URL sent with the request that is currently processed.</td>
<td></td>
</tr>
<tr>
<td>URL.ReputationForURL</td>
<td>Number</td>
<td>Reputation score for a given URL.</td>
<td>String: URL that reputation score is to be found for</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>URL.ReputationString</td>
<td>String</td>
<td>Reputation score for a given URL in string format</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The URL is the URL sent with the request that is currently processed.</td>
<td></td>
</tr>
<tr>
<td>URL.ReputationStringForURL</td>
<td>String</td>
<td>Reputation score for a given URL</td>
<td>String: URL that reputation score is to be found for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The URL is specified as a parameter of the property.</td>
<td></td>
</tr>
<tr>
<td>URL.ReverseDNSLedToResult</td>
<td>Boolean</td>
<td>If true, the rating for a URL was retrieved by performing a reverse DNS lookup.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Parameters</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>URL.SmartMatch</td>
<td>Boolean</td>
<td>If true, a URL matches one or more of the URL parts that are specified in string format in any of the entries in the list of URL parts that is given as the parameter of this property. An entry in this string list must specify at least the domain or the path part of a URL as a substring. It can specify both. The domain part matches also if a URL only contains a subdomain of the specified domain. For the path part, it is sufficient if the beginning of the path in a URL matches it. Additionally, a list entry can specify the protocol and port of a URL. The value of the property is true if a URL matches the domain or the path part (or both) in an entry of the string list and also matches the protocol part (if specified) and the port part (if specified). If a port is specified in an entry of the string list, but not in the URL, there is no match. For example, the string list contains the following entry: <a href="http://www.mycompany.com/samplepath/xyz">http://www.mycompany.com/samplepath/xyz</a> Then the URLs below will produce matches or not as follows: mycompany.com (match) <a href="http://mycompany.com">http://mycompany.com</a> (match) <a href="https://mycompany.com">https://mycompany.com</a> (no match) <a href="http://www.mycompany.com/">http://www.mycompany.com/</a> (match) host.mycompany.com (no match) <a href="http://www.mycompany.com:8080/">http://www.mycompany.com:8080/</a> (no match) <a href="http://www.mycompany.com/samplepath/">http://www.mycompany.com/samplepath/</a> (match) /samplepath/ (match) mycompany.com/samplepath/ (match) com (match) You can use this property to search for matches in a complex URL whitelist or blocklist, for example, in a list that contains both entries for URL hosts and for complete URLs.</td>
<td>List of String: List with parts of URLs in string format</td>
</tr>
</tbody>
</table>
### Table A-24 Properties – U (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>URLFilter.DatabaseVersion</td>
<td>Number</td>
<td>Version number of the database on an appliance</td>
<td></td>
</tr>
<tr>
<td>URLFilter.EngineVersion</td>
<td>String</td>
<td>String identifying the version of the URL filtering module (engine)</td>
<td></td>
</tr>
<tr>
<td>User-Defined.cacheMessage</td>
<td>String</td>
<td>Message text providing information on web cache usage</td>
<td></td>
</tr>
<tr>
<td>User-Defined.eventMessage</td>
<td>String</td>
<td>Message text providing information on an event</td>
<td></td>
</tr>
<tr>
<td>User-Defined.loadMessage</td>
<td>String</td>
<td>Message text providing information on CPU overload</td>
<td></td>
</tr>
<tr>
<td>User-Defined.logLine</td>
<td>String</td>
<td>Entry written into a log file</td>
<td></td>
</tr>
<tr>
<td>User-Defined.monitorLogMessage</td>
<td>String</td>
<td>Entry written into a log file</td>
<td></td>
</tr>
<tr>
<td>User-Defined.notificationMessage</td>
<td>String</td>
<td>Text of a notification message</td>
<td></td>
</tr>
<tr>
<td>User-Defined.requestLoadMessage</td>
<td>String</td>
<td>Message text providing information on request overload</td>
<td></td>
</tr>
<tr>
<td>User-Defined.requestsPerSecond</td>
<td>Number</td>
<td>Number of requests processed on an appliance per second</td>
<td></td>
</tr>
</tbody>
</table>

### Properties - W

The following table describes the properties that have names beginning with W.

### Table A-25 Properties – W

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wildcard.ToString</td>
<td>String</td>
<td>Wildcard expression converted into a string</td>
<td>Wildcard Expression: Wildcard expression to convert</td>
</tr>
</tbody>
</table>

### Wildcard expressions

When completing configuration activities on an appliance, you can use wildcard expressions for several purposes, for example, to match URLs on blocking lists and whitelists.

There are two types of wildcard expressions you can use:

- **Glob expressions** — Using these is the default.

  More information about this type of expressions is, for example, provided on the following Linux man page:

  ```
glob(7)
  ```

- **Regular expressions (Regex)** — If you want to use these, you need to type the term *regex* first and then include the regular expression in parentheses, for example:

  ```
regex(a*b)
  ```

  The regular expressions that are used on the McAfee Web Gateway appliance follow the Perl Regular Expression syntax. Information on this syntax is, for example, provided on the following Linux man page:

  ```
perlre(1)
  ```
Test a wildcard expression

When adding a wildcard expression to a list, you can test it before actually adding it.

**Task**

1. Select Policy | Lists.
2. On the lists tree, expand Wildcard Expressions and select a list.
3. Click the Add icon on the settings pane.
   
   The Add Wildcard Expression window opens.
4. Type a wildcard expression in the input field, then click Test.
   
   The Wildcard Expression Test window opens to display information on whether the expression is valid.

List of important special glob characters

The following table provides a list of important special characters you can use to create *glob* type wildcard expressions.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Matches any single character (if not between square brackets). For example, ?est matches: best rest test and others</td>
</tr>
<tr>
<td>*</td>
<td>Matches any string, including the empty string (if not between square brackets). For example, b* matches: b best binary and others</td>
</tr>
<tr>
<td>[...]</td>
<td>Matches any of the single characters included in the square brackets. ? and * are normal characters between square brackets. For example, [a5?] matches: a 5 ?</td>
</tr>
</tbody>
</table>

The first character must not be an ! (exclamation mark).
### Table A-26  List of important special glob characters (continued)

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Matches any single character except those following the exclamation mark. For example, <code>[!ab]</code> matches: c s % but not: a b</td>
</tr>
<tr>
<td>-</td>
<td>Is used to denote a range of characters. For example, <code>[a-f A-F 0-5]</code> matches: d F 3 and others</td>
</tr>
<tr>
<td>/</td>
<td>Is not matched by ? or * and cannot be included in [...] or be part of a range. This means, for example, that <code>http://linux.die.net/*</code> does not match the following pathname: <code>http://linux.die.net/man/7/glob</code> The pathname is, however, matched by: <code>http://linux.die.net/*/*/*</code></td>
</tr>
<tr>
<td>\</td>
<td>If preceding ?, *, or [, these are normal characters. For example, <code>[mn\*][]</code> matches: m n * [</td>
</tr>
<tr>
<td>.</td>
<td>A . (dot) at the beginning of a file name must be matched explicitly. For example, the command: <code>rm *</code> will not remove the file <code>.profile</code>. However, the following command will: <code>rm .*</code></td>
</tr>
</tbody>
</table>
List of important special regex characters

The following table provides a list of important special characters you can use to create regex type wildcard expressions.

The examples given here include the term regex and parentheses. You need to use both when working with these expressions on an appliance.

Table A-27  List of important special regex characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Matches any single character. For example, <code>regex(.est)</code> matches: best rest test and others</td>
</tr>
<tr>
<td>*</td>
<td>Matches the preceding character zero or more times. For example, <code>regex(a*b)</code> matches: b ab aaaaab and others</td>
</tr>
<tr>
<td>+</td>
<td>Matches the preceding character once or more times. For example, <code>regex(c+d)</code> matches: cd ccccd and others</td>
</tr>
<tr>
<td>?</td>
<td>Matches the preceding character zero times or once. For example, <code>regex(m?n)</code> matches: n mn</td>
</tr>
<tr>
<td>^</td>
<td>Matches the beginning of a line</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of a line</td>
</tr>
</tbody>
</table>
### Table A-27 List of important special regex characters (continued)

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
</table>
| {...}     | Are used to match a character as many times as specified.  
| **Options:** |  
| - \(a^n\) — Matches a character \(n\) times  
  | For example, \(\text{regex}(a\{3\})\) matches:  
  | aaa  
| - \(a^n\) — Matches a character \(n\) and more times  
  | For example, \(\text{regex}(p\{4,\})\) matches:  
  | pppp  
  | ppppp  
  | and others  
| - \(a^n, m\) — Matches between \(n\) and \(m\) times, including the limiting values  
  | For example, \(\text{regex}(q\{1,3\})\) matches:  
  | q  
  | qq  
  | qqq |
| | Separates expressions that match alternatively.  
| For example, \(\text{regex}(abc|klm)\) matches:  
| abc  
| klm |
| (...) | Delimits an alternative expression combined with another expression.  
| For example, \(\text{regex}(bi(n|rd))\) matches:  
| bin  
| bird |
| [...]] | Matches any of the single characters included in the square brackets.  
| For example, \(\text{regex}([bc3])\) matches:  
| b  
| c  
| 3 |
| - | Is used to denote a range of characters in a bracketed expression.  
| For example, \(\text{regex}([c-f C-F 3-5])\) matches:  
| d  
| F  
| 4  
| and others |
### Table A-27 List of important special regex characters *(continued)*

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
</table>
| ^         | Matches any single character in a bracketed expression except those following the accent circonflexe.  
For example, `regex([^a-d])` matches:  
e  
7  
&  
and others, but not  
a  
b  
c  
d  |
| \         | If preceding a special character, turns it into a normal character.  
For example, `regex(mn\+)` matches:  
\mn+  
If preceding some normal characters, matches a particular class of characters.  
For information on these classes, refer to the *perlre* man page or other documentation.  
The following are examples of frequently used character classes.  
`regex(\d)` matches numerical characters (digits), such as:  
\3  
\4  
7  
and others  
`regex(\w)` matches alphabetical characters, such as:  
\a  
F  
s  
and others  
`regex(\D)` matches all characters that are not digits, such as:  
\c  
T  
\%  
and others |
An interface is provided that allows you to administer an appliance without being logged on to its standard user interface. This alternative interface is known as the REST (Representational State Transfer) interface.

Using the REST interface, you can perform different kinds of activities on a particular appliance or on others that are connected to it.

- **Actions** — Turn off an appliance, restart it, flush the cache, create a configuration backup, and perform several other activities
- **File handling** — Access system, log, and troubleshooting files to perform activities such as downloading, modifying, deleting, and others
- **Policy configuration** — Configure settings for engines and rule actions, manage rule sets and lists by performing activities such as enabling, adding, deleting, exporting, importing, and others
- **Updates** — Perform manual engine updates and trigger automatic yum and engine updates

A suitable script is the usual way to perform these activities.

### Contents

- Prepare use of the REST interface
- Working with the REST interface
- Sample scripts for working with the REST interface

### Prepare use of the REST interface

To let users work with the REST interface, you need to enable it on the standard user interface of an appliance and permit access to it.

#### Tasks

- **Enable use of the interface on page 756**
  You can enable the use of the REST interface for completing administration activities on an appliance.

- **Give permission to access the interface on page 756**
  You must add permission to access the REST interface to an administrator role for those users who are supposed to work with the interface.
Enable use of the interface
You can enable the use of the REST interface for completing administration activities on an appliance.

**Task**
1. Select **Configuration** | **Appliances**.
2. On the appliances tree, select the appliance you want to administer using the REST interface and click **User Interface**.
3. Under **UI Access**, select **Enable REST interface over HTTP** or **Enable REST interface over HTTPS** as needed.
4. Click **Save Changes**.

Give permission to access the interface
You must add permission to access the REST interface to an administrator role for those users who are supposed to work with the interface.

**Task**
1. Select **Accounts** | **Administrator Accounts**.
2. In the **Roles** area, select an administrator role and click **Edit**.
   - The **Edit Role** window opens.
3. Select **REST interface accessible**.
4. Click **OK** to close the window.
5. Click **Save Changes**.

You can now assign this administrator role to the appropriate users.

Instead of adding access permission to an existing role, you can also create a new role with this permission and name it, for example, **REST Admin**.

---

**Working with the REST interface**

When working with the REST interface, you use it for sending HTTP or HTTPS requests to perform activities on one or several appliances.

You can send individual requests that are immediately processed or use requests in a script, for example, in a bash script. The latter is the typical use.

Requests are sent to the REST interface using a client of an appliance, which provides a server to process the requests and send responses. You are assigned a particular workspace on the server, so to apply some types of changes, you need to send a request to commit them to let them become effective.

When logging on to the REST interface on an appliance, you authenticate and are provided with a session ID in return. You can then send HTTP or HTTPS requests to execute actions and work with files and lists on the appliance. You can do the same on other appliances that are connected as nodes in a Central Management configuration to the one you are logged on to.

The REST interface is provided in a particular format known as the ATOM format.

As your client for communicating with the interface server, you can use a data transfer tool, for example, **curl** (Client for URLs).
Sample script for sending a request

The following is an example of a bash script that sends a request to the REST interface using curl. The purpose of the request is to create a configuration backup.

The script does basically the following:

- Logs on and authenticates to the REST interface on an appliance
- Sends a request to create a backup file
- Logs off again

The script also uses a variable for the URL that is specified in the request for logging on to the REST interface. The variable is set at the beginning.

```bash
# !bin/bash
# Set URL variable for access to REST interface
REST="http://localhost:4711/Konfigurator/REST"
## Log on and authenticate
curl -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/login"
## Create backup file
curl -b cookies.txt -X POST "$REST/backup" -o filename.backup
## Log off again
curl -b cookies.txt -X POST "$REST/logout"
```

Using curl as the data transfer tool

To send requests to the REST interface on an appliance, you can use curl as the data transfer tool. A request sent with curl usually has three main parts: the `curl` command, one or several options, and a URL.

For example, in the following backup request:

```bash
curl -b cookies.txt -X POST "$REST/backup" -o filename.backup
```

the `curl` command appears with the `-b` option for sending cookies that have been collected in a text file and the `-o` option, which stores the output of the request in another file. The `-X` option is for the request method.

The URL is specified as a variable that has the IP address, port number, and other information needed for access to the REST interface on an appliance as its value. It is followed by the name of the activity that should be performed.

Using these and other options of curl together with the appropriate URLs, you can send requests to the REST interface on an appliance to perform activities as needed.

The curl data transfer tool is available under Linux and other UNIX operating systems and described in full detail, for example, on the `curl` man page.

Request methods

The request method is specified in curl by the `-X` option. When working with the REST interface on an appliance, the GET, POST, PUT, and DELETE methods can be used, for example, as follows:

```bash
curl -X POST <URL>
```
If no request method is specified, GET is used as the default method.

**Headers**

When a header is sent with a request, it is specified by the `-H` option, for example, as follows:

```bash
curl -H <header name>:<header value> -X POST <URL>
```

You can send multiple headers within one request, repeating the `-H` option letter before each header.

```bash
curl -H <header name 1>:<header value 1> -H <header name 2>:<header value 2> <...> -X POST <URL>
```

A request normally includes an `Accept` header that has `application/atom+xml` as its value. In curl `Accept:` `/*` is sent as a default, which is accepted by the REST interface, so you can leave out this header in many cases.

However, if you send data in the body of a request, you need to include the `Content-Type` header with `application/atom+xml` as its value. Then you also need to include the `Content-Length` header and set it correctly. The latter is done in curl by default, so you need not do it explicitly when using this tool.

If you want to include the header of the response you get upon a request in its output, you need to insert the `-i` option.

```bash
curl -i -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/login"
```

The `-v` option creates verbose output, which means that also the request header is included.

**URLs**

A URL in a request specifies a protocol, which can be HTTP or HTTPS in communication with the REST interface, the IP address or host name and the port number of the appliance that a request is sent to, and the internal path on the appliance to the REST interface.

This is followed by the name of the activity that should be performed and further parameters if there are any.

As the REST interface is located within the configurator subsystem of an appliance, the internal name of this subsystem, which is `Konfigurator`, appears in the URL.

A URL in, for example, a logon request, could therefore look as follows:

```bash
curl -X POST "HTTP://localhost:4711/Konfigurator/REST/login?userName=myusername&pass=mypassword"
```

In this request, the URL also has query parameters for the logon credentials. Query parameters are introduced by a `?` (question mark) and separated by an `&` (ampersand), as shown. A URL can also have matrix parameters, which are introduced by a `;` (semicolon).

For correct URL encoding, spaces in a URL must be filled with the symbols `%20`. So, for example, *Bob Smith* becomes `Bob%20Smith`.

You can use a variable within a URL for easier code writing and reading. For example, if you have set the `$REST` variable accordingly, the above request could look as follows:

```bash
curl -X POST "$REST/login?userName=myusername&pass=mypassword"
```
**Sending data in the request body**

For sending data in the body of a request, the `-d` option is used, followed by the name of the file that contains the data.

```
curl -b cookies.txt -X POST -d "file.txt" "$REST/list?name=newlist&type=string"
```

If you are sending only binary data, the option to use is `- -data-binary`.

```
curl -b cookies.txt --data-binary @file.backup -X POST "$REST/restore" -H "Content-Type: text/plain; charset=UTF-8"
```

You can use the symbol `@` after the option name to indicate a file name.

**Authenticating to the interface**

Before you can use the REST interface to perform any activities on an appliance you need to authenticate.

To authenticate you submit username and password in the logon request that you send to the REST interface.

There are the following two ways to submit them:

- Using query parameters
- Using an authentication header

After a successful authentication, the response contains the session ID, which you must include in each of your following requests.

**Using query parameters for authentication**

You can submit your credentials with query parameters that you add to the URL in your logon request.

```
curl -i -X POST "$REST/login?userName=myusername&pass=mypassword"
```

**Using an authentication header**

You can also use the Basis Access Authentication method to authenticate, which requires you to submit your credentials in an authentication header.

```
curl -i -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/login"
```

In the authentication header, the string after `Authorization: Basic` is the Base64-encoded representation of your user name and password.

**Session ID**

The session ID is sent to you in the response to your logon request. The session ID looks, for example, as follows:

```
D0EFF1F50909466159728F28465CF763
```

It is either contained in the response body:

```
<entryxmlns="http://www.w3.org/2005/Atom"><contenttype="text">D0EFF1F50909466159728F28465CF763</content></entry>
```

or in a Set-Cookie header:

```
Set-Cookie: JSESSIONID=D0EFF1F50909466159728F28465CF763
```
In the requests of the session that follow the logon request, you need to include the session ID as JSESSIONID.

For easier code writing and reading, you can set a variable to the value of the ID and use it for including the ID.

```bash
export SESSIONID=D0EFF1F50909466159728F28465CF763
```

You can append the ID as a matrix parameter to the URL, preceded by a semicolon.

```bash
curl -i "$REST/appliances;jsessionid=$SESSIONID"
```

Alternatively, you can send the ID in a Cookie header.

```bash
curl -i -H "Cookie: JSESSIONID=$SESSIONID" "$REST/appliances"
```

The option `-c` in curl allows you to collect all cookies in a text file, which is then sent with subsequent requests.

```bash
curl -i -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/login"
```

For sending a cookie file with a request, the option `-b` is used:

```bash
curl -i -b cookies.txt "$REST/appliances"
```

**Requesting resources**

A request sent to the REST interface regarding system files, log files, lists, and some other items is considered to be a request for resources.

The response to a request for resources can be one of the following:

- **Entry** — An entry delivers information in xml format about an individual resource, such as its ID, name, or the URL that can be used to access it.

- **Feed** — A feed delivers information in xml format about a collection of resources.

  A feed can, for example, be a list of appliances that are available as nodes in a Central Management configuration, or a list of all lists that exist on an appliance, or a list of all lists of a particular type.

- **Binary data** — Binary data is delivered in a file that you requested for downloading.

A response can also be empty. This is the case when the requested data is not available.

**Reducing xml data overhead**

You can reduce the xml data overhead that you receive with a response, by including an appropriate Accept header in a request for resources. For this purpose, the header value must be `application/mwg+xml`.

Instead of an entry in the normal Atom format, you will then receive only the xml data from the content part of that format.

Instead of a feed in Atom format, you will only receive a list of IDs for the resources you asked for.

Similarly, you can reduce xml data overhead when working with the resources, for example, when modifying them. For this, you need to set the Content-Type header to `application/mwg+xml`. 
**Paging a feed**
When requesting a feed, you can use paging, which means you can ask for a feed that is divided into pages.

Paging information is specified by query parameters that are added to the URL in a request. The following two parameters can be used:

- **PageSize** — Maximum number of elements on a page
- **Page** — Page number

A request for a feed that uses paging could look as follows:

```bash
curl -i -b cookies.txt "$REST/list?pageSize=10&page=4"
```

If a feed is, for example, a list of 35 lists, the `pageSize` parameter in the above request divides it up into four pages, three of which contain ten lists, while the last one contains only five. The last page is also the one that is delivered.

**Navigating within a feed**
To allow navigation within a feed, the XML file that you receive contains appropriate links.

Using these links, you can go to the current, next, previous, first, and last page, respectively.

**Performing basic activities**
When working with the REST interface, you can perform several basic activities within your working environment, such as logging on and off, committing changes, creating a configuration backup, and others.

The POST request method is used for performing all these activities. A particular activity is specified by a parameter that is added to the URL of a request.

For example, the following is a request to log off from the REST interface on an appliance:

```bash
curl -i -b cookies.txt -X POST "$REST/logout"
```

Parameters for basic activities are as follows:

- **login** — Log on
- **discard** — Discard changes
- **logout** — Log off
- **backup** — Back up the configuration
- **restore** — Restore the configuration
- **commit** — Commit changes
- **heartbeat** — Keep a session alive

In addition to performing these activities, you can request information on the version of REST interface, as well as that of the standard user interface of the appliance you are currently working on.

**Logging on**
To log on to the REST interface on an appliance, the `login` parameter is used in a request. Within this request you also submit your credentials for authentication, for example, in the following way:

```bash
curl -i -X POST "$REST/login?userName=myusername&pass=mypassword"
```

If authentication is performed successfully, the response to the logon request provides a session ID.

**Logging off**
To log off from the REST interface on an appliance, the `logout` parameter is used.
REST interface
Working with the REST interface

curl -i -b cookies.txt -X POST "$REST/logout"

Logging off deletes the session information and discards the changes made in a session that would need to be, but have not been committed.

**Keeping a session alive**
Using the heartbeat parameter in a request keeps the session alive that you are currently working in.

curl -i -b cookies.txt -X POST "$REST/heartbeat"

**Committing changes**
To commit changes that have been made to items such as system files, log files, lists, and others on an appliance, the commit parameter is used.

curl -i -b cookies.txt -X POST "$REST/commit"

**Discarding changes**
To discard changes that have been made to items such as system files, log files, lists, and others on an appliance, the discard parameter is used.

curl -i -b cookies.txt -X POST "$REST/discard"

**Backing up the configuration**
To create a configuration backup for the appliance you are currently working on, the backup parameter is used.

curl -b cookies.txt -X POST "$REST/backup -o filename.backup"

When backing up or restoring a configuration, no response header is required as part of the output, so the -i option need not to be included in the request.

**Restoring the configuration**
To restore the configuration of the appliance you are currently working on, the restore parameter is used. You also need to specify a Content-Type header for the type of the backup file.

curl -b cookies.txt --data-binary @filename.backup -X POST "$REST/restore" -H "Content-Type: text/plain;charset=UTF-8"

**Requesting version information**
To request information on the version of the REST interface or the standard user interface of the appliance you are currently working on, you can use the version parameter.

Using the parameter alone in a request retrieves a feed in XML format with the versions of both interfaces.

curl -i -b cookies.txt -X GET "$REST/version"

If you are only interested in version information for one of the interfaces, you can send the following request for the REST interface:

curl -i -b cookies.txt -X GET "$REST/version/mwg-rest"

and this one for the standard user interface:

curl -i -b cookies.txt -X GET "$REST/version/mwg-ui"
Working on individual appliances

After logging on to the REST interface on one appliance, you can perform activities on any other appliance that is connected. Individual appliances are identified in requests by their UUIDs (Universal Unique Identifiers).

To find out about the UUID of an individual appliance, you can request a feed of all appliances that are connected as nodes in a Central Management configuration to the one you are currently working on.

The feed includes a list of the UUIDs for all nodes. A UUID looks, for example, as follows:

081EEDBC-7978-4611-9B96-CB388EEFC4BC

A GET request is sent to retrieve the feed, with the `appliances` parameter appended to the URL.

```
curl -i -b cookies.txt -X GET "$REST/appliances"
```

You can then identify an individual appliance by its UUID and, for example, shut down this appliance with a POST request, appending the `action` parameter and `shutdown` as the action name.

```
curl -i -b cookies.txt -X POST "$REST/appliances/<UUID>/action/shutdown"
```

You can repeat this action or any other activity on all individual appliances that the feed delivered UUIDs for, for example, by running an appropriate script.

Actions

When working with the REST interface, actions are those activities that are preceded by the `action` parameter in a request. They do not involve a modification of resources and are performed instantly, which means no request to commit them is required.

Action names are as follows:

- **restart** — Restart an appliance
- **shutdown** — Shut down an appliance
- **flushcache** — Flush the cache
- **rotateLogs** — Rotate log files
- **rotateAndPushLogs** — Rotate and push log files
- **license** — Import a license

Restarting an appliance

To restart an appliance, `restart` is used as the action name in a request.

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/action/restart"
```

Shutting down an appliance

To shut down an appliance, `shutdown` is used as the action name.

```
curl -i -b cookies.txt -X POST "$REST/appliances/<UUID>/action/shutdown"
```

Flush the cache

To flush the cache on an appliance, `flushcache` is used as the action name.

```
curl -i -b cookies.txt -X POST "$REST/appliances/<UUID>/action/flushcache"
```

Rotating log files

To rotate log files on an appliance, `rotateLogs` is used as the action name.

```
curl -i -b cookies.txt -X POST "$REST/appliances/<UUID>/action/rotateLogs"
```
Rotating and pushing log files

To rotate and push log files on an appliance, `rotateAndPushLogs` is used as the action name.

curl -i -b cookies.txt -X POST "${REST}/appliances/" <UUID>/action/rotateAndPushLogs"

Importing a license

To import a license onto an appliance, `license` is used as the action name. You also need to specify a Content-Type header for the type of the license file.

curl -i -b cookies.txt -H "Content-Type: text/plain; charset=UTF-8" -X POST "${REST}/appliances/" <UUID>/action/license" --data-binary @license.xml

Working with files and lists

When working with system files, log files, files uploaded for troubleshooting, and lists, the `system`, `log`, `files`, and `list` parameters are used in requests instead of the `action` parameter.

Changes made to system files and lists must be committed by sending an appropriate request.

Working with system files

You can use the REST interface to work with system files on an appliance.

Modifying system files in an inappropriate manner can impact the proper operation of an appliance.

In a request to access a system file, for example, the `/etc/hosts` file, on a particular appliance, you identify this appliance, using its UUID, and add the `system` parameter to the URL.

If you know the path to a system file and its name, you can include this information in a request to access the file directly.

Otherwise, you can request a feed to deliver a list of the system files that exist on an appliance as follows:

curl -i -b cookies.txt -X GET "${REST}/appliances/"<UUID>/system"

Like with any other feed request, you can also add query parameters for paging to the URL.

With system files, you can do the following:

• Download a system file
• Modify a system file

Unlike with log files and other files on an appliance, you must send a separate request to commit changes you have made to a system file.

When you are running an appliance in FIPS-compliant mode, you cannot modify system files.

Downloading a system file

When downloading a system file, you specify the `application/x-download` Accept header in the request and add the path and name of the system file to the URL.

curl -i -b cookies.txt -H "Accept:application/x-download" -X GET "${REST}/appliances/"<UUID>/system/etc/hosts" -O

The `-O` option stores the data in a local file under the name the file had on the appliance you downloaded it from.
Modifying a system file

When modifying a system file, you set the Content-Type header and add the path and name of the system file to the URL. You also provide a file as the request body containing the data for modifying the system file in binary format.

```
curl -i -b cookies.txt -H "Content-Type: */*" -X PUT "$REST/appliances/<UUID>/system/etc/hosts" --data-binary @binary.zip
```

Working with log files

You can use the REST interface to work with log files on an appliance.

In a request to access a log file on a particular appliance, you identify this appliance, using its UUID, and add the log parameter to the URL.

If you know the path to a log file and its name, you can include this information in a request to access the file directly.

Otherwise, you can request a feed that delivers a list of the files and directories stored in the root log directory on an appliance as follows:

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/log"
```

Like with any other feed request, you can also add query parameters for paging to the URL.

The xml file that you receive as a feed in response provides MIME type information to indicate for every element in the feed whether it is an individual log file or a directory.

- "application/x-download" — For an individual log file
- "application/atom+xml; type=feed" — For a directory

The xml file could, for example, indicate as follows that the root log directory includes the individual log file debug_1234.log.

```xml
```

It could also indicate that the directory connection_tracing is included, as follows.

```xml
<link href="http://localhost:4711/Konfigurator/REST/appliances/081EEDBC-7978-4611-9B96-CB388EEFC4BC/log/debug/connection_tracing" rel="self" type="application/atom+xml; type=feed"/>
```

Regarding individual log files, you can:

- Download a log file
- Delete a log file

**Downloading a log file**

When downloading a log file, you specify the `application/x-download` Accept header in the request and add the path and name of the log file to the URL.

```
curl -i -b cookies.txt -H "Accept:application/x-download" -X GET "$REST/appliances/<UUID>/log/debug/debug_1234.log" -O
```

The `-O` option stores the log file data in a local file under the name it had on the appliance you downloaded it from.
Deleting a log file

When deleting a log file, you add the path and name of the log file to the URL.

```
curl -i -b cookies.txt -X DELETE "$REST/appliances/<UUID>/log/debug/debug_1234.log"
```

Working with files uploaded for troubleshooting

You can use the REST interface to work with files that have been uploaded for troubleshooting purposes on an appliance.

On the standard user interface of an appliance, you can upload files for troubleshooting purposes under Files, which is a location that is accessible from the Troubleshooting top-level menu.

In a request to access one of these uploaded files on a particular appliance, you identify the appliance, using its UUID, and add the files parameter to the URL.

If you know the path to an uploaded file and its name, you can include this information in a request to access the file directly.

Otherwise, you can request a feed that delivers a list of these files as follows:

```
curl -i -b cookies.txt -X GET "$REST/appliances/<UUID>/files"
```

Like with any other feed request, you can also add query parameters for paging to the URL.

You can do the following with the uploaded files:

- Download an uploaded file
- Add a file to the uploaded files
- Modify an uploaded file
- Delete an uploaded file

Downloading an uploaded file

When downloading an uploaded file, you specify the application/x-download Accept header in the request and add the name of the file to the URL.

```
curl -i -b cookies.txt -H "Accept:application/x-download" -X GET "$REST/appliances/<UUID>/files/troubleshooting.zip" -O
```

The -O option stores the downloaded data in a local file under the name it had on the appliance you downloaded it from.

Adding a file to the uploaded files

When adding a file to the uploaded files, you set the Content-Type header and add the name of the file to the URL. You also provide this file with data in binary format as the request body.

```
curl -i -b cookies.txt -H "Content-Type: */*" -X PUT "$REST/appliances/<UUID>/files/moretroubleshooting.zip" --data-binary @moretroubleshooting.zip
```

Make sure that the content type is not application/x-www-form-urlencoded, as the curl tool will set the header to this value.

Modifying an uploaded file

When modifying an uploaded file, you set the Content-Type header and add the name of the file to the URL. You also provide a file as the request body containing data for modifying the file in binary format.
curl -i -b cookies.txt -H "Content-Type: */*" -X PUT "${REST}/appliances/<UUID>/files/troubleshooting.zip" --data-binary @binary.zip

**Deleting an uploaded file**

When deleting an uploaded file, you add the name of the file to the URL.

```bash
curl -i -b cookies.txt -X DELETE "${REST}/appliances/<UUID>/files/troubleshooting.zip"
```

**Working with lists**

You can use the REST interface to work with lists and their entries on an appliance.

In a request to access a list, you add the `list` parameter to the URL.

A request for a feed that delivers a list of all available lists on an appliance could, for example, look as follows:

```bash
curl -i -b cookies.txt -X GET "${REST}/appliances/list"
```

Like with any other feed request, you can add query parameters for paging to the URL. In addition to this you can add query parameters for the file name and type.

The following request retrieves a feed of all available string lists:

```bash
curl -i -b cookies.txt -X GET "${REST}/appliances/list?type=string"
```

The following request retrieves a feed of all lists with the name `Default`.

```bash
curl -i -b cookies.txt -X GET "${REST}/appliances/list?name=Default"
```

The xml file that you receive as a feed in response to your request provides a list ID for each list. You can use this ID to identify a list that you want to access. A list ID looks, for example, as follows:

```
com.scur.type.regex.11347
```

You can also use the list ID in a request for a feed of the entries in a particular list, together with the `entry` parameter. The following request retrieves a list entry feed:

```bash
curl -i -b cookies.txt -X GET "${REST}/appliances//list/<list ID>/entry"
```

The xml file that you receive as a feed in response to your request provides a number for each entry to indicate its position. You can use the position to identify an entry that you want to access.

With regard to a list, you can do the following:

- Add a list with content
- Add a list with name and type inside the content
- Add an empty list
- Delete a list
- Retrieve a list
- Modify a list
- Copy a list
- Delete a list
- Insert a list
- Move a list entry
- Modify a list entry
Adding a list with content

When adding a list with content, you specify the Content-Type header and provide the file in xml format as the request body, using the -d option. With the query parameters of the URL, you specify name and type of the list.

```
curl -i -b cookies.txt -H "Content-Type: application/xml" -X POST -d @listwithcontent.xml "$REST/list?name=newlist&type=category"
```

The response to this request includes the new list in xml format as the response body.

The xml file that you send with the request could, for example, look as follows:

```
<entry>
  <content type="application/xml">
    <list>
      <description/>
    </list>
    <content>
      <listEntry>
        <entry>com.scur.category.192</entry>
      </listEntry>
      <listEntry>
        <entry>com.scur.category.195</entry>
      </listEntry>
      <listEntry>
        <entry>com.scur.category.140</entry>
      </listEntry>
    </content>
  </content>
</entry>
```

Adding a list with name and type inside the content

When adding a list that has its name and type included in the content, you specify the Content-Type header and provide the file in xml format as the request body, using the -d option.

```
curl -i -b cookies.txt -H "Content-Type: application/xml" -X POST -d @nameandtypeinside.xml" "$REST/list"
```

The response to this request includes the new list in xml format as the response body.

The xml file that you send with the request could, for example, look as follows:

```
<entry>
  <content type="application/xml">
    <list name="Lifestyle" type=Id="com.scur.type.category">
    </list>
  </content>
</entry>
```
Adding an empty list

When adding an empty list, you specify its name and type with the query parameters of the URL.

curl -i -b cookies.txt -X POST "$REST/list?name=newlist&type=category"

The response to this request includes an empty list in xml format as the response body.

Retrieving a list

When retrieving a list with content, you add its list ID to the URL.

curl -i -b cookies.txt -X GET "$REST/list/ <list ID>"

The response to this request includes the requested list in xml format as the response body. It has the same structure as a new list that has been added.

Deleting a list

When deleting a list, you add its list ID to the URL.

curl -i -b cookies.txt -X DELETE "$REST/list/ <list ID>"

Modifying a list

When modifying a list, you replace it with modified content. You specify the Content-Type header and provide the modified content in XML format as the request body, using the -d option. You also add the list ID to the URL.

The structure of the modified content is the same as with the content of a list that is added without including its name and type inside the content.
curl -i -b cookies.txt -H "Content-Type: application/xml" -X PUT -d @modifiedlist.xml "$REST/list/<list ID>"

The response to this request includes the modified list in xml format as the response body.

**Copying a list**

When copying a list, you add the ID of the list you want to copy to the URL. You also add the `copy` parameter with a query parameter for the name that the copied list should have.

curl -i -b cookies.txt -X POST "$REST/list/<list ID>/copy/?newname"

The response to this request includes the modified list in xml format as the response body.

**Retrieving a list entry**

When retrieving a list entry, you add the list ID and `entry` parameter with the position of the entry to the URL.

curl -i -b cookies.txt -X GET "$REST/list/<list ID>/entry/3"

The response to this request includes the entry in xml format as the response body.

**Deleting a list entry**

When deleting a list entry, you add the list ID and `entry` parameter with the position of the entry to the URL.

curl -i -b cookies.txt -X DELETE "$REST/list/<list ID>/entry/4"

**Modifying a list entry**

When modifying a list entry, you replace it with modified content. You specify the Content-Type header and provide the modified content in xml format as the request body, using the `-d` option.

You also add the list ID, the `entry` parameter and the position of the entry to the URL.

curl -i -b cookies.txt -H "Content-Type: application/xml" -X PUT -d @modifiedentry.xml "$REST/list/<list ID>/entry/2"

The response to this request includes the modified entry in xml format as the response body.

The modified content that you send with the request could, for example, look as follows:

```xml
<entry xmlns="http://www.w3.org/2011/Atom">
  <content type="application/xml">
    <listEntry>
      <entry>com.scur.category.192</entry>
      <description />
    </listEntry>
  </content>
</entry>
```

**Moving a list entry**

When moving a list entry, you add the list ID, the `entry` parameter and the old position of the entry to the URL. You also add the `move` and the `newpos` query parameter with the new position.
curl -i -b cookies.txt -X POST "$REST/list/<list ID>/entry/4/move?newpos=3"

The response to this request includes the entry in xml format with its new position as the response body.

**Inserting a list entry**

When inserting a list entry, you specify the Content-Type header and provide the entry in xml format at the request body, using the `-d` option.

You also add the list ID, entry parameter, the position where you want to insert the entry, and the insert parameter to the URL.

curl -i -b cookies.txt -H "Content-Type: application/xml" -X POST -d @newentry.xml "$REST/list/<list ID>/entry/2/insert"

The response to this request includes the inserted entry in xml format as the response body.

---

**Sample scripts for working with the REST interface**

When working with the REST interface, you can use suitable scripts for sending requests to it.

The following scripts are bash scripts that use curl as the data transfer tool. They complete the following activities:

- Perform an action
- Download a log file
- Create a configuration backup
- Restore a configuration

**Perform an action**

The following bash script performs a particular action on each of several appliances.

```bash
#!/bin/bash
# Set URL variable for access to REST interface
REST="http://10.149.112.48:4711/Konfigurator/REST"
# Set action variable
action="flushcache"
## Log on and authenticate
curl -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "$REST/login"
## Write appliances feed to appliancesxml variable
appliancesxml=`curl -b cookies.txt "$REST/appliances"`
## Retrieve UUIDs from appliancesxml variable using xpath
uuids=`echo $appliancesxml|xpath -e "/feed/entry/id/text()"`'
## Perform action on all appliances, identifying them by their UUIDs
echo $uuids
for uuid in $uuids
do
```

---

McAfee Web Gateway 7.6.0  Product Guide  771
echo Sending $action to $uuid
curl -b cookies.txt -X POST "${REST}/appliances/$uuid/action/$action"
done

## Log off again
curl -b cookies.txt -X POST "${REST}/logout"

### Download a log file

The following bash script downloads a particular log file from each of several appliances.

```bash
#!/bin/bash
# Set URL variable for access to REST interface
REST="http://10.149.112.48:4711/Konfigurator/REST"
# Set log file variable
auditlog="/audit/audit.log"
## Log on and authenticate
curl -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "${REST}/login"
## Write appliances feed to appliancesxml variable
appliancesxml=`curl -b cookies.txt "${REST}/appliances"`
## Retrieve UUIDs from appliancesxml variable using xpath
uuids=`echo $appliancesxml|xpath -e "/feed/entry/id/text()"`
## Retrieve log file from all appliances, identifying them by their UUIDs
echo $uuids
for uuid in $uuids
do
echo Downloading $auditlog from $uuid
curl -b cookies.txt -H "Accept: application/x-download" -X POST "${REST}/appliances/$uuid/log/$auditlog" -o audit$uuid.log
done
## Log off again
curl -b cookies.txt -X POST "${REST}/logout"
```

### Create a configuration backup

The following bash script creates a configuration backup on an appliance.

```bash
#!/bin/bash
# Set URL variable for access to REST interface
REST="http://localhost:4711/Konfigurator/REST"
## Log on and authenticate
curl -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "${REST}/login"
## Create backup file
curl -b cookies.txt -X POST "${REST}/backup" -o file.backup
```
## Log off again

curl -b cookies.txt -X POST "${REST}/logout"

### Restore a configuration

The following bash script restores a configuration from a backup file on an appliance.

```bash
# !bin/bash
# Set URL variable for access to REST interface
REST="http://localhost:4711/Konfigurator/REST"
## Log on and authenticate
curl -c cookies.txt -H "Authorization: Basic YWRtaW46d2ViZ2F0ZXdheQ==" -X POST "${REST}/login"
## Restore configuration from backup file
curl -b cookies.txt --data-binary @file.backup -X POST "${REST}/restore" -H "Content-Type: text/plain; charset=UTF-8"
## Log off again
curl -b cookies.txt -X POST "${REST}/logout"
```
REST interface
Sample scripts for working with the REST interface
Third-party software

The following list provides information about third-party software used in developing the McAfee Web Gateway appliance software.

Third-party software list

Information on third-part software is provided in this list following the alphabetical order of names.

**Apache Jakarta Commons IO**
Used in portions
Made available under an Apache License, version 2.0
Copyright © 2002-2012 The Apache Software Foundation

**Apache log4j**
Used in portions
Made available under an Apache License, version 2.0
Copyright © 2007 The Apache Software Foundation.

**Apache ORO**
Used in portions
Made available under an Apache License, version 1.1
Copyright © 2002-2003 The Apache Software Foundation.

**Apache Tomcat**
Used in portions
Made available under an Apache License, version 2.0
Copyright © 2012 The Apache Software Foundation.

**Apache-Jakarta Codec**
Used in portions
Made available under an Apache License, version 2.0
Copyright © 2000-2009 The Apache Software Foundation
Apache-Jakarta Fileupload
Used in portions.
Made available under an Apache License, version 2.0
Copyright © 2002-2010 The Apache Software Foundation

Apache-Jakarta Lang
Used in portions
Made available under an Apache License, version 2.0
Copyright © 2001-2011 The Apache Software Foundation

Arabica XML and HTML Toolkit for C++
Made available under a Berkeley Software Distribution (BSD) License, version 2.0
Used in portions
Copyright © 2001-2013 Jez UK Ltd

ASM
Used in portions
Made available under a Berkeley Software Distribution (BSD) License, version 2.0
Copyright © 2000-2005 INRIA France Telekom.

Boost C++ Libraries
Used in portions
Made available under a Boost Software License, version 1.0
Copyright © miscellaneous

Bzip2
Used in portions
Made available under a Bzip2 License
Copyright © 1996-2013 julian@bzip.org

Chromium Source
Used in portions
Made available under a Berkeley Software Distribution (BSD) License, version 2.0
Copyright © 2010

Code Project - Walking the callstack
Used in portions
Made available under a Berkeley Software Distribution (BSD) License, version 2.0
Copyright © 2005 Jochen Kalmbach
Dynamic Drive - DD Tooltip
Used in portions
Made available under a Dynamic Drive DHTML Scripts License
Copyright © 1998-2004 Dynamic Drive

Eclipse
Used in portions
Made available under an Eclipse Public License, version 1.0, and a Common Public License
Copyright © 2005-2009 Eclipse contributors and others

ftpparse
Used in portions
Made available under an Ftp Parse License
Copyright © 2000 D. J. Bernstein

fugue icons
Used in portions
Made available under a Creative Commons Attribution License, version 3.0
Copyright © 2013 Yusuke Kamiyamane

Glazed Lists
Used in portions
Made available under a Mozilla Public License, version 1.1
Copyright © 2003-2006 publicobject.com O'Dell Engineering Ltd

googletest
Used in portions
Made available under a Berkeley Software Distribution (BSD) License, version 2.0
Copyright © 2008 Google Inc

Info-ZIP project - source-UnZip
Used in portions
Made available under an Info-ZIP Updated License
Copyright © 1999-2005 Greg Roelofs

Jackson JSON Processor Core Annotations
Used in portions
Made available under an Apache License, version 2.0
Copyright © 2000-2005 INRIA France Telecom
jersey-bundle
Used in portions
Made available under a Common Development and Distribution License, version 1.0
Copyright © 2000-2005 INRIA France Telecom

JFreeChart
Used in portions
Made available under a GNU Lesser General Public License, version 2.1
Copyright © 2000-2009 Object Refinery Limited and Contributors

JIDE Common Layer
Used in portions
Made available under a GNU Lesser General Public License, version 2.1
Copyright © 2002-2011 JIDE Software, Inc

JSON
Used in portions
Made available from a public domain

jsprogressBarHandler
Used in portions
Made available under a Creative Commons Attribution Share-Alike License, version 2.5
Copyright © 2007 - 2008 Bram Van Damme

JSR-311 - JAX-RS - The Java API for RESTful Web Services
Used in portions
Made available under a Common Development and Distribution License, version 1.0
Copyright © 2009 Sun Microsystems, Inc

jQuery
Used in portions
Made available under a Massachusetts Institute for Technology (MIT) License
Copyright © 2005, 2013 jQuery Foundation, Inc

jQuery UI
Used in portions
Made available under a Massachusetts Institute for Technology (MIT) License
Copyright © 2013 jQuery Foundation and other contributors
Kerberos 5
Used in portions
Made available under a Kerberos 5 Massachusetts Institute of Technology (MIT) License
Copyright © 1985-2013 Massachusetts Institute of Technology and contributors

libuuid
Used in portions
Made available under a Theodore Ts’o License
Copyright © 1999 Theodore Ts’o

Mozilla Rhino JavaScript for Java
Used in portions
Made available under a Mozilla Public License, version 1.1
Copyright © 2012 Mozilla Foundation

msgpack
Used in portions
Made available under an Apache License, version 2.0
Copyright © 2004 The Apache Software Foundation

Open BSD
Used in portions
Made available under a Berkeley Software Distribution (BSD) License, version 2.0

opencsv
Used in portions
Made available under an Apache License, version 2.0
Copyright © 2005 Bytecode Pty Ltd

OpenSSL
Used in portions
Made available under an OpenSSL License, version 1.1
Copyright © 1999-2011 The OpenSSL Project

Paho
Used in portions
Made available under an Eclipse Public License, version 1.0
POCO
Used in portions
Made available under a Boost Software License, version 1.0

Prototype JavaScript Framework
Used in portions
Made available under a Massachusetts Institute of Technology (MIT) License, version 2.0
Copyright © 2005-2010 Sam Stephenson

rapidjson
Used in portions
Made available under a Massachusetts Institute of Technology (MIT) License, version 2.0
Copyright © 2011 Milo Yip

RapidXml
Used in portions
Made available under a Massachusetts Institute of Technology (MIT) License, version 2.0
Copyright © 2008, 2006, 2007 Marcin Kalicinski

RARLAB-UnRAR
Used in portions
Made available under an unRAR License
Copyright ©1993-2012

RDialog
Used in portions
Made available under a Ruby License
Copyright © 2007 Aleks Clarks

RegExFormatter Tutorial
Used in portions
Made available under a Creative Commons Attribution License, version 2.5
Copyright © 2008, 2010, Oracle and/or its affiliates

Ruby
Used in portions
Made available under a Ruby License, version 2.5
Copyright © 1995-2013 Yukihiro Matsumoto
**Silk Icons**
Used in portions
Made available under a Creative Commons Attribution License, version 2.5
Copyright © 2008 Mark James

**StAX2**
Used in portions
Made available under an Apache License, version 2.0
Copyright © 2004 Alexander Slominski 2006 Chris Fry

**test/unit**
Used in portions
Made available under a Ruby License, version 2.0
Copyright © 2000-2003, Nathaniel Talbott

**The ASN.1 Compiler**
Used in portions
Made available under a Berkeley Software Distribution (BSD) Two Clause License (BSD -) License, version 2.0

**The Legion of the Bouncy Castle**
Used in portions
Made available under a Massachusetts Institute of Technology (MIT) License, version 2.0
Copyright © 2000-2012 2000 - 2012 The Legion Of The Bouncy Castle

**The prefuse visualization toolkit**
Used in portions
Made available under a Berkeley Software Distribution (BSD) License, version 2.0
Copyright © 2000-2012 Regents of the University of California

**Trove for Java**
Used in portions
Made available under a Massachusetts Institute of Technology (MIT) License, version 2.0
Copyright © 2000-2012 The Legion of the Bouncy Castle

**Valgrind Instrumentation Framework**
Used in portions
Made available under a Massachusetts Institute of Technology (MIT) License, version 2.0
Copyright © 2000-2012 The Legion of the Bouncy Castle
**Woodstox**
Used in portions
Made available under an Apache License, version 2.0
Copyright © 2000-2012 2004 Tatu Saloranta

**XStream Library**
Used in portions
Made available under a Berkeley Software Distribution (BSD) License, version 2.0
Index

A

about this guide 15
action
  add to rule 190
  list of actions 645
  rule element 177
  settings 237
  Settings tab 239
administrator
  accounts 302
  external accounts 305
  high-level activities 20
  roles 304
  test account 303
Advanced Threat Defense
  Advanced Threat Defenserule set 420
  ATD - Offline Scanning with Immediate File Availability rule set 421
  configuring 413
  Gateway ATD settings 418
  key elements 415
  monitoring 417
  monitoring with Content Security Reporter 417
  scanning criteria 408
  Use existing report 410
  use ongoing scanning run 411
  workflows 407
alerts 567
appliance
  administrator 302
  alerts 567
  Appliances tab 36
  back up configuration 642
  Central Management 152
  components 19
  configuration daemon 19
  configurator 19
  coordinator 19
  core 19
  dashboard 567
  deployment overview 20
  error handling 595
  filtering cycles 175
  high-level administration activities 20

appliance (continued)
  log off 23
  logging 578
  main functions 18
  operating system 19
  REST interface 756
  restore configuration 642
  rules 177
  system architecture 19
  system configuration 34
  system information line 23
  troubleshooting 625
  user interface 23
  web filtering 17
application filtering
  blocking lists 368
  individual functions 368
  process 368
  rule set 372
  rules 368
  system lists 368
authentication
  advanced settings 247
  Authentication Server settings 247
  common settings 247
  IM Authentication rule set 279
  implement different method 258
  instant messaging 276
  Kerberos Administration settings 258
  LDAP digest authentication 245
  LDAP method 268
  LDAP settings 247
  McAfee Pledge 281
  Novell eDirectory settings 247
  NTML Agent settings 247
  NTML settings 247
  One-Time Password settings 247
  one-time passwords 281
  RADIUS settings 247
  settings 247
  system settings 258
  User Database settings 247
  Windows Domain Membership settings 260
Index

B
back up configuration 642
backup encryption 642
bandwidth throttling 441
best practices
  adding a log file field 587
  configuring authentication for deployment types 261
  configuring LDAP authentication 268
  configuring node groups in Central Management 157
  configuring the explicit proxy mode with WCCP 79
  configuring the Proxy HA mode 74
  configuring the Stream Detector 376
  creating a log 588
  find reason for missing images 636
  fine-tuning a transparent bridge configuration 94
  High Availability size limits 78
  rule configuration 194
  sending access log data to syslog 616
  troubleshooting next-hop proxy issues 454
  using URL properties for whitelisting 348
  working with a McAfee-maintained subscribed list 213
  working with the error handler 597
  working with the user-agent header 128
block reason ID
  Authenticate settings 464
  Block settings 464
  list of block reason IDs 646
  Redirect settings 465
bonded interface 53
bonding interface 53
C
cache volume resizing 60
Central Management
  add node 154
  add scheduled job 160
  assign node to groups 155
  assign node to network groups 156
  assign node to runtime group 155
  assign node to update group 156
  best practices - configuring node groups 157
  configuration 152
  configuring node groups 157
  node communication protocols 122
  node groups 152
  nodes 152
  scheduled jobs 152
  settings 161
  update appliance in closed network 63
  update configuration 160
certificate keys 398
channel bonding 53
closed network updates 62
cloud connectors
  about 477
  custom 478
  custom, configuring 481
  custom, deleting 481
  generic HTTP 480
  generic HTTP settings 485
  generic HTTP, configuring 484
  generic IceToken 480
  generic IceToken settings 513
  generic IceToken, configuring 512
  generic SAML2 480
  generic SAML2 settings 493
  generic SAML2, configuring 492
  HTTP, configuring 484
  predefined 478
  SAML2 settings 491
  SAML2, configuring 491
templates 477
templates, generic vs. individual 480
cloud storage encryption
  Cloud Storage Encryption rule set 554
  Cloud Storage Encryption settings 553
  Cloud Storage Encryption Support settings 553
  configure data encryption and decryption 552
  configure settings 552
  decrypt storage data 549
  decrypt storage data manually 554
  encrypt storage data 549
  encryption algorithms 549
  high-level steps for data encryption and decryption 552
storage services 549
Common Catalog
  enable use 228
  list types 228
  user account 229
configuration daemon 19
configurator subsystem 19
Content Security Reporter 417
conventions and icons used in this guide 15
Cookie authentication with SAML back end and fixed ACS URL rule set
  about 506
  Authenticate clients with authentication server 509
  Authentication server request 510
  Cookie authentication at authentication server 509
  Cookie authentication at HTTP(S) proxy 508
  Intercept SAML assertion if IdP uses a fixed ACS URL 507
  Set cookie for authenticated clients 508
coordinator subsystem 19
core subsystem 19
criteria
  add to rule 189
  complex 179
  operand 177
criteria (continued)
    operator 177
    parameter 177
    property 177
    rule element 177

cycles
    embedded objects 175
    request 175
    response 175

D

dashboard
    access 568
    alerts 567
    charts and tables 567
    evolving data 571
    top scores 571
Data Exchange Layer, See DXL
data loss prevention
    classification settings 430
    dictionaries settings 431
    ICAP server 434
    logging 423
    process 423
    rule set 432
    rules 423
data trickling 437
Data Usage Statement 37
database updates
    automatic 61
    manual 61
DNS servers
    conditional forwarding 123
    reverse lookups 123
    settings 123
    use according to domains 123
documentation
    audience for this guide 15
    product-specific, finding 16
    typographical conventions and icons 15
DXL
    architecture 125
    configure settings for using a TIE server 127
    messages 125
    sample rules 125
    scenarios 125
    TIE server 125
Dynamic Content Classifier
    configure use 356
    URL categories 356

E

embedded objects cycle 175
End User License Agreement 37

Enterprise Security Manager 620
ePolicy Orchestrator 614
error handling
    list of error IDs 647
    list of incident IDs 664
    using error IDs 595
    using incident information 595
ESM 620
ethernet bonding 53
event
    add to rule 191
    list of events 652
    rule element 177
explicit proxy mode 66
external lists
    module 214
    module settings 218
    properties 214
    recommended use 214
    sources 214
    system settings 224

F

feedback collection 38
filtering
    embedded objects cycle 175
    process flow 175
    properties 174
    request cycle 175
    response cycle 175
    users 174

G

global whitelisting
    Global Whitelist rule set 378
    rule set 378
    rules 378
    whitelists 378

H

Hardware Security Module
    access 398
    administrator responsibilities 398
    configure local use 400
    configure remote use 401
    install 398
    log module operations 398
    Private Key Infrastructure 398
    settings 403
    store private keys 398
    Helix proxy 149
    help 23
hybrid solution
configure settings 560
enable synchronization 562
high-level steps 560
overview 557
products 557
select rule set 561
settings 562
synchronize manually 562
use proxy 562
Web Hybrid settings 562
work with 557

I
ICAP communication
  ICAP Client settings 434
  ICAP server list 434
  ICAP Server settings 106
  secure ICAP 97
  use ICAP server for data loss prevention 434
ICAP Token authentication
  about 477
  compared to SAML 512
inline lists 200
instant messaging
  ICQ settings 106
  process 101
  Windows Live Messenger settings 106
  XMPP settings 106
  Yahoo settings 106
isolated network updates 62

J
JavaScript Object Notation data (JSON) 231

L
launchpad
  customizing 516
  editing the Launchpad.html file 516
  providing custom logos 519
  style sheet, editing default 517
  style sheet, importing custom 519
LDAP
  authentication method 268
  digest authentication 245
License settings 37
licensing 37
list
  access in rule 204
  access on Lists tab 204
  Common Catalog 228
  create 204
  custom lists 200
  external lists 214
list (continued)
  inline lists 200
  Lists tab 202
  restrict access 198
  subscribed lists 208
  system lists 200
  types 200
  updatable system lists 200
log off 23
logging
  log files 578
  modules 578
  rules 578
long running connection handler
  ICAP server settings 106

M
McAfee Pledge 281
McAfee ServicePortal, accessing 16
media stream scanning 339
media type filtering
  blocking lists 363
  configure key elements 364
  key elements 364
  Media Type Filtering rule set 363
  rule set 363
  rules 363
monitoring
  dashboard 567
  ePolicy Orchestrator 614
  error handling 595
  logging 578
  performance measurement 607
  sending access log data to syslog 616
  sending syslog data to ESM 620
  SNMP agent 611

N
network interface bonding 53
next-hop proxies
  failover mode 447
  forward requests tp 446
  modes 446
  round-robin mode 446
  rule set 459
  settings 457
  SOCKS protocol 450
  stickiness 448
  troubleshooting 454
NIC bonding 53
node communication protocols 122
proxies (continued)
- transparent bridge mode 90
- transparent proxy 68
- transparent router mode 84
- UDP protocol 100
- UDP settings 106
- user-agent header 128
- using WCCP to redirect FTP traffic 120
- WCCP 79
- Windows Live Messenger settings 106
- XMPP settings 106
- XMPP with SSL scanner disabled 105
- Yahoo settings 106

Q
- quota management
  - authorized override 320
  - blocking sessions 323
  - coaching 317
  - system settings 325
  - time quota 310
  - volume quota 313

R
- request cycle 175
- response cycle 175
- REST interface
  - access permission 756
  - actions 763
  - authentication 759
  - basic activities 761
  - curl 757
  - enable use 756
  - lists 767
  - log files 765
  - prepare use 755
  - requesting resources 760
  - sample scripts 771
  - system files 764
  - uploaded files 766
  - working on individual appliances 763
  - working with the interface 756
- restore configuration 642
- rule
  - action 177
  - create 186
  - criteria 177
  - elements 177
  - event 177
  - flexibility 173
  - format on user interface 178
  - operand 177
  - operator 177
  - process flow 175

O
- one-time passwords
  - configure for authenticating users 282
  - configure for authorized overriding 282
- McAfee Pledge 281
- overview 281
- online help 23
- online rule set library 183
- operand 177
- operating system 19
- operator 177

P
- password change 23
- Periodic Rule Engine Trigger List 106
- Private Key Infrastructure 398
- private keys 398
- progress indication
  - data trickling 437
  - progress page 437
- property
  - add to rule 189
  - filtering process 174
  - list of properties 674
  - rule element 177
- proxies
  - advanced settings 106
  - auto-configuration 147
  - conditional DNS forwarding 123
  - Data Exchange Layer 106, 125
  - DNS settings 106
  - DXL 106, 125
  - explicit proxy mode 66
  - FTP settings 106
  - Helix 149
  - High Availability size limits 78
  - HTTP settings 106
  - ICAP Server settings 106
  - ICQ settings 106
  - IFP settings 106
  - instant messaging 101
  - network setup 106
  - node communication protocols 122
  - Office 365 bypassing 132
  - outbound source IP addresses 118
  - Periodic Rule Engine Trigger List 106
  - Proxy HA mode 74
  - Proxy HA settings 73
  - reverse HTTPS 135
  - settings 106
  - SOCKS proxy 98
  - SOCKS proxy settings 106
  - TCP window scaling 106
  - timeouts 106
Index

rule (continued)
property 177
representation in documentation text 179
Rule Sets tab 184
sets 181
rule set
create 191
criteria 181
cycles 181
default system 182
import 193
library 183
nested 181
online library 183
restrict access 198
Rule Sets tab 184
system 182
rule tracing
delete traces 639
find reason for missing images 636
lists 628
overview 626
restore traces 638
rule tracing panes 628
search 628

S
SAML authentication, external Identity Providers
about 499
configuring 501
Identity Provider URLs, adding to whitelists 504
process 499
requests, configuring settings 502, 503
responses, configuring settings 503
responses, validating 505
rule set 506
SAML attribute mapping 505
static ACS URLs, configuring 502
static ACS URLs, support for 500
SAML single sign-on
about 488
certificate management 490
configuring external data sources 496
Identity Provider (IdP) 488
initiating 488
Service Provider (SP) 488
SAML SSO data sources
LDAP authentication 496
using a database 498
using a web service 497
using an LDAP server 498
save changes 23
ServicePortal, finding product documentation 16
settings
access 240
access on Settings tab 240
acess in rule 240
action 237
create 241
module 237
restrict access 198
Settings tab 239
system 237
types 237
Single Sign On lists 536
Single Sign On rule set
about 523
Get Attributes in the Cloud 533
Get Attributes on Premise 532
Get Login Action 531
HTTPS Handling 527
Launchpad 528
OTP Authentication 529
Perform IceToken SSO 534
Perform SAML SSO 534
Perform SSO 535
Process Common Tasks 535
Select Services 524
Single Sign On settings
about 537
certificate and private key 539
single sign-on
cloud connectors 477
creating bookmarks 520
credential model for HTTP applications 484
data sources 477
dynamic HTTP applications 483
high-level configuration 474
key elements 521
lists and settings 536
monitoring logons 520
process in proxy and non-proxy modes 475
resolving issues 547
rule set reference 523
rule set summary 520
SSO Catalog 477
supported authentication methods 477
to .NET and Java web applications 512
to HTTP applications and services 483
to SAML applications and services 488
using the launchpad 514
viewing update status 482
SNMP monitoring 611
SOCK S protocol
Protocol Detector settings 458
SOCKS protocol
next-hop proxies 450
SOCKS proxy 98
SOCKS protocol (continued)
SOCKS Proxy rule set 101
SOCKS proxy
configure settings 99
source-based routing 56
SSL scanning
certificate keys 398
client certificate list 384
Hardware Security Module 398
lists 380
modules 380
private keys 398
rules 380
SSL Scanner rule set 393
whitelists 380
SSO Catalog
as a service 479
cloud connectors 477
technical note 478
viewing in the user interface 478
SSO Connector lists
adding connectors 483
configuring cloud access 482
viewing in the user interface 478
SSO logging
enabling 541
overview 540
rule set reference 542
rule set, SSO access log 543
rule set, SSO stop logging 546
rule set, SSO trace log 545
streaming media filtering
best practices 376
module settings 378
rule 374
subscribed lists
content settings 209
create 208
retrieving content 208
updates 210
system architecture 19
system configuration
after initial setup 34
Appliances tab 36
cache volume resizing 60
Data Usage Statement 37
database updates 61
Date and Time settings 40
End User License Agreement 37
feedback collection 38
File Editor tab 59
File Server settings 41
initial setup settings 33
License settings 37
licensing 37
system configuration (continued)
Network protection settings 49
Port Forwarding settings 50
Static Routes settings 51
system files 59
Telemetry settings 38
User Interface settings 42
system information line 23

T
tabs
Administrator Accounts 302
Alerts 568
Appliances 36
Charts and Tables 571
File Editor 59
Lists 202
Rule Sets 184
Settings 239
Templates 467
TCP window scaling 106
technical support, finding product information 16
Telemetry settings 38
templates
editor 467
tab 467
third-party software 775
TIE server 125
top-level menus
Accounts 23
Configuration 23
Dashboard 23
Policies 23
Troubleshooting 23
transparent modes
bridge 90
router 84
troubleshooting
AV threads 642
back up configuration 642
backup encryption 642
connection tracing files 640
core files 639
display running AV threads 642
feedback files 639
methods 625
network tools 641
packet tracing files 640
restart service 641
restore configuration 642
rule tracing 626
system tools 641
U

URL filtering
  - best practices - using URL properties for whitelisting 348
  - blocking lists 341
  - configure key elements 343
  - Dynamic Content Classifier 356
  - IFP proxy 358
  - key elements 343
  - module 341
  - own URL filter database 357
  - rule set 341
  - rules 341
  - URL Filter module 341
  - URL Filtering rule set 341
  - using URL properties for whitelisting 348
  - whitelists 341

user interface
  - complete rules view 30
  - configuration pane 23
  - configuring a web security policy 26
  - help 23
  - key elements 26
  - key elements view 28
  - log off 23
  - main elements 23
  - navigation pane 23
  - password change 23
  - sample screen capture 23
  - save changes 23
  - search 23
  - Settings tab 239
  - supporting configuration functions 25
  - system information line 23
  - system settings 42
  - tab bar 23
  - toolbar 23
  - top-level menus 23
  - user preferences 23

user message (continued)
  - variables 461
  - user-agent header 128

V

virus and malware filtering
  - Anti-Malware module 327
  - anti-malware queue 340
  - configure key elements 329
  - Gateway Anti-Malware rule set 327, 337
  - key elements 329
  - media stream scanning 339
  - module 327
  - module settings 333
  - rule set 327
  - rules 327
  - system settings 340
  - whitelists 327

W

WCCP 79
  - web cache
    - enabling 444
    - rule set 444
    - rules 444
    - Web Cache rule set 444
  - web filtering
    - Advanced Threat Defense 406
    - application filtering 368
    - data loss prevention 423
    - global whitelisting 378
    - media type filtering 363
    - SSL scanning 380
    - streaming media filtering 374
    - URL filtering 341
    - virus and malware filtering 327
  - what's in this guide 15
  - wildcard expressions
    - glob expressions 748
    - list of important special glob characters 749
    - list of important special regular expression characters 751
    - regular expressions 748
    - test 749

X

XMPP with SSL scanner disabled 105