SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for McAfee Web Gateway
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms’ resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013468-001, Rev. A
Release Date: April 2016
Contents

Third-Party Software Acknowledgement ................................................................. 4
Description ................................................................................................................. 4
Applicability ............................................................................................................... 4
Environment .............................................................................................................. 4
Audience ..................................................................................................................... 5
RADIUS-based Authentication using SafeNet Authentication Service Cloud................. 5
RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE .......................................................... 6
RADIUS Authentication Flow using SafeNet Authentication Service ......................... 6
RADIUS Prerequisites ............................................................................................. 7
Configuring SafeNet Authentication Service ............................................................. 7
  Creating Users Stores in SafeNet Authentication Service ....................................... 7
  Assigning an Authenticator in SafeNet Authentication Service ............................ 7
  Adding McAfee Web Gateway as an Authentication Node in SafeNet Authentication Service .......................................................... 8
  Checking the SafeNet Authentication Service RADIUS Address ......................... 10
Configuring McAfee Web Gateway .......................................................................... 11
  Configuring McAfee Web Gateway to Use RADIUS for Authentication ............. 11
  Modifying the Rule Set for Direct Proxy Authentication for RADIUS ............... 16
Configuring Proxy Server Settings on the Client Machine ......................................... 20
Running the Solution ............................................................................................... 22
Support Contacts .................................................................................................... 23
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as McAfee Web Gateway.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

McAfee Web Gateway is a web security product that protects your network against threats arising from the web, such as viruses and other malware, inappropriate content, data leaks, and related issues. It also insures regulatory compliance and a productive work environment.

McAfee Web Gateway connects your network to the web, filtering the traffic that leaves and enters your network. Malicious and inappropriate content is blocked, while the useful content is allowed to pass through the network.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in McAfee Web Gateway using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure McAfee Web Gateway to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the McAfee Web Gateway environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

McAfee Web Gateway can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**
- **McAfee Web Gateway**—Version 7.5.2.3.0
• **Windows Client Machine**—Version 7.0 with Internet Explorer (IE) 9.0.

**Audience**

This document is targeted to system administrators who are familiar with McAfee Web Gateway, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

**RADIUS-based Authentication using SafeNet Authentication Service Cloud**

SafeNet Authentication Service (SAS) Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

![SAS Cloud Hosted RADIUS Service Diagram]

- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

![Local RADIUS Hosted on-premises Diagram]

This document demonstrates the solution using the SAS cloud hosted RADIUS service.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to:

For more details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.
RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

For both on-premises versions, SafeNet Authentication Service (SAS) can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS)** or the legacy **Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.
  
  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:
  

- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.
  
  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

RADIUS Authentication Flow using SafeNet Authentication Service

SafeNet Authentication Service (SAS) communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the data flow of a multi-factor authentication transaction for McAfee Web Gateway.

1. A user attempts to log on to McAfee Web Gateway using an OTP authenticator.
2. McAfee Web Gateway sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to McAfee Web Gateway.
4. The user is granted or denied access to McAfee Web Gateway based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from McAfee Web Gateway, ensure the following:

- End users can authenticate from the McAfee Web Gateway environment with a static password before configuring the McAfee Web Gateway to use RADIUS authentication.
- Ports 1812/1813 are open to and from McAfee Web Gateway.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with McAfee Web Gateway using RADIUS protocol requires the following:

- Creating User Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 7
- Adding McAfee Web Gateway as an Authentication Node in SafeNet Authentication Service, page 8
- Checking the SafeNet Authentication Service RADIUS Address, page 10

Creating User Stores in SafeNet Authentication Service

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the Create User shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through McAfee Web Gateway.

The following authenticators are supported:

- eToken PASS
Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.


### Adding McAfee Web Gateway as an Authentication Node in SafeNet Authentication Service

Add a RADIUS entry in the SafeNet Authentication Service (SAS) **Auth Nodes** module to prepare it to receive RADIUS authentication requests from McAfee Web Gateway. You will need the IP address of McAfee Web Gateway and the shared secret to be used by both SAS and McAfee Web Gateway.

1. Log in to the SAS console with an Operator account.
2. Click the **COMMS** tab, and then select **Auth Nodes**.

3. In the **Auth Nodes** module, click the **Auth Nodes** link.

4. Under **Auth Nodes**, click **Add**.

5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent Description</strong></td>
<td>Enter a host description.</td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td><strong>Low IP Address In Range</strong></td>
<td>Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS</td>
</tr>
<tr>
<td><strong>Configure FreeRADIUS Synchronization</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td><strong>Confirm Shared Secret</strong></td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>
The authentication node is added to the system.

Checking the SafeNet Authentication Service RADIUS Address

Before adding SafeNet Authentication Service (SAS) as a RADIUS server in McAfee Web Gateway, check its IP address. The IP address will then be added to McAfee Web Gateway as a RADIUS server at a later stage.

1. Log in to the SAS console with an Operator account.

2. Click the COMMS tab, and then select Auth Nodes.
3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

### Configuring McAfee Web Gateway

Configuring McAfee Web Gateway to use the RADIUS protocol as a secondary authentication method requires:

- Configuring McAfee Web Gateway to Use RADIUS for Authentication, page 11
- Modifying the Rule Set for Direct Proxy Authentication for RADIUS, page 16

#### Configuring McAfee Web Gateway to Use RADIUS for Authentication

1. Log in to the McAfee Web Gateway console.

   ![McAfee Web Gateway Console](image)

   *(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)*

2. Click **Policy**.
3. Click the **Settings** tab and then in the left pane, expand **Engines**.

![McAfee Web Gateway Settings](image1.png)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)

4. Right-click **Authentication** and then click **Add**.

![McAfee Web Gateway Authentication Add](image2.png)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
5. On the **Add Settings** window, on the **Add Settings** tab, perform the following steps:
   a. In the **Name** field, enter a name for the engine (for example, **RADIUS**).
   b. In the right pane, in the **Authentication method** field, select **Radius**.
   c. Under **Common Authentication Parameters**, complete the following fields:
      | Proxy realm | Enter a name for the proxy realm (for example, **Safenet**). |
      | Authentication attempt timeout | Enter the maximum time (in seconds) for which the McAfee Web Gateway waits to process an authentication request. |
      | Use Authentication cache | Select this option. |
      | Authentication cache entry TTL | Enter the maximum time (in minutes) for which the authentication information is stored in the cache. |
   d. Under **RADIUS Specific Parameters**, click the icon to add a RADIUS server.

6. On the **Add String** window, in the **String** field, enter IP/FQDN for the RADIUS server, and then click **OK**.

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
7. On the Add Settings window, on the Add Settings tab, in the right pane, under RADIUS Specific Parameters, the newly added string is listed. Click Set.

![Add Settings window with RADIUS Specific Parameters](image)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)

10. On the New Password window, complete the following fields, and then click OK.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter the shared secret that you entered earlier in step 5 of “Adding McAfee Web Gateway as an Authentication Node in SafeNet Authentication Service” on page 8.</td>
</tr>
<tr>
<td>Repeat Password</td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

![New Password window](image)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
8. On the **Add Settings** window, on the **Add Settings** tab, in the right pane, under **RADIUS Specific Parameters**, in the **RADIUS connection timeout** field, enter the RADIUS connection timeout (in seconds) according to your preferred configuration, and then click **OK**.

![Image of the Add Settings window with RADIUS Specific Parameters](image)

*(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)*

9. On the McAfee Web Gateway console, in the upper-right corner, click **Save Changes**.

![Image of the McAfee Web Gateway console with Save Changes button highlighted](image)

*(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)*
Modifying the Rule Set for Direct Proxy Authentication for RADIUS

In the direct proxy authentication mode, the client or browser is aware of the proxy (the address and port of the proxy) in order to send the network traffic to the McAfee Web Gateway.

It is assumed that the direct proxy setup (with authentication) is configured on McAfee Web Gateway with appropriate rules.

1. Log in to the McAfee Web Gateway console.

2. Click Policy.

3. On the Rule Sets tab, in the left pane, expand Direct Proxy Authentication, and then click Authentication Method.

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
4. In the right pane, under **Rules in “Authentication Method”**, in the **Enabled** column, select the box to select an appropriate rule (for example, **Authentication Method**), and then click **Edit**.

![Screen Image](image1.png)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)

5. The **Edit Rule** window is displayed. Click **Next**.

![Screen Image](image2.png)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)

6. In the right pane, in the **Property** column, select the appropriate rule criteria (for example, **Authentication.Authenticate<User Database>**), and then click **Edit**.

![Screen Image](image3.png)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
7. On the **Edit Criteria** window, in the left box, select the rule criteria (for example, `Authentication.Authenticate`), click **Settings: User Database**, and then select **RADIUS**.

![Edit Criteria Window](image)

*(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)*

8. Click **OK**.

9. On the **Edit Rule** window, click **Next**.

![Edit Rule Window](image)

*(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)*

10. In the right pane, in the **Action** field, ensure that **Authenticate** is selected. In the **Settings** field, select an appropriate setting (for example, **Default**) and then click **Next**.

![Edit Rule Window](image)

*(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)*
11. Click **Next**.

![Image of Next button](image1)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)

12. Click **Finish**.

![Image of Finish button](image2)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)

13. On the McAfee Web Gateway console, in the upper-right corner, click **Save Changes**.

![Image of Save Changes button](image3)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
Configuring Proxy Server Settings on the Client Machine

Proxy server settings are used to tell Internet Explorer the network address of an intermediary server (known as a proxy server) that is used between the browser and the Internet on some networks.

1. Log in to the client machine.
2. Click **Start > Control Panel**.
3. On Control Panel, click **Internet Option**.

![Configuring Proxy Server Settings on the Client Machine](image1)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

4. On the **Internet Options** window, click the **Connections** tab.

![Configuring Proxy Server Settings on the Client Machine](image2)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
5. Click **LAN settings**.

![Internet Options](image)

*(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*

6. On **Local Area Network (LAN) Settings** window, perform the following steps:
   a. Under **Automatic configuration**, ensure that the following are not selected:
      - Automatically detect setting
      - Use automatic configuration script
   b. Under **Proxy server**, complete the following fields:
      | **Use a proxy server for your LAN** | Select this option. |
      | **Address**                      | Enter the IP address of the proxy server. |
      | **Port**                        | Enter the port number of the proxy server. |
      | **Bypass proxy server for local addresses** | Do not select this option. |
   c. **Click OK**.

![Local Area Network (LAN) Settings](image)

*(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*
7. On the **Internet Options** window, click **OK**.

7. On the **Internet Options** window, click **OK**.

![Internet Options window](image)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

## Running the Solution

For this integration, the SafeNet MobilePASS token is configured for authentication with the SAS solution.

1. In **Internet Explorer (IE)**, try to open a website.
2. The **Windows Security** window is displayed. Complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Username</strong></th>
<th>Enter your user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Generate an OTP using the SafeNet MobilePASS token and then enter that OTP in this field.</td>
</tr>
</tbody>
</table>

![Windows Security window](image)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
If the authentication is successful, you are successfully logged in, and you can access the Internet.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>