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:** 007-013479-001, Rev. A  
**Release Date:** May 2016
Contents

Third-Party Software Acknowledgement ........................................................................................................... 4
Description ........................................................................................................................................................... 4
Applicability .......................................................................................................................................................... 4
Environment .......................................................................................................................................................... 4
Audience ............................................................................................................................................................... 5
RADIUS-based Authentication using SafeNet Authentication Manager ................................................................. 5
RADIUS Authentication Flow using SafeNet Authentication Manager ............................................................... 5
RADIUS Prerequisites ......................................................................................................................................... 6
Configuring SafeNet Authentication Manager .................................................................................................. 6
  Synchronizing Users Stores to SafeNet Authentication Manager ................................................................. 6
  Configuring SafeNet Authentication Manager’s Connector for OTP Authentication .................................... 7
  Assigning a Token in SafeNet Authentication Manager ................................................................................... 7
  Adding McAfee Web Gateway as a RADIUS Client in IAS/NPS ..................................................................... 8
  Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client ........................ 10
Configuring McAfee Web Gateway .................................................................................................................. 10
  Configuring Web Gateway to Use RADIUS for Authentication ................................................................ 10
  Modifying the Rule Set for Direct Proxy Authentication for RADIUS ......................................................... 15
Configuring Proxy server setting in Client Machine ............................................................................................ 19
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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

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) tokens managed by SafeNet Authentication Manager.
- Configure McAfee Web Gateway to work with SafeNet Authentication Manager 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 Manager, and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

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

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager**—A server version of SAM 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 Manager 8.2 HF 493**
- **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 Manager.

RADIUS-based Authentication using SafeNet Authentication Manager

SafeNet's OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SafeNet Authentication Manager (SAM).

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

RADIUS Authentication Flow using SafeNet Authentication Manager

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

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

1. A user attempts to log on to McAfee Web Gateway using an OTP token.
2. McAfee Web Gateway sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
3. The SAM 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 SAM and is connected to McAfee Web Gateway.

RADIUS Prerequisites

To enable SafeNet Authentication Manager 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 Manager

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

- Synchronizing Users Stores to SafeNet Authentication Manager, page 6
- Configuring SafeNet Authentication Manager’s Connector for OTP Authentication, page 7
- Assigning a Token in SafeNet Authentication Manager, page 4
- Adding McAfee Web Gateway as a RADIUS Client in IAS/NPS, page 8
- Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client, page 10

Synchronizing Users Stores to SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server
Configuring SafeNet Authentication Manager’s Connector for OTP Authentication

SafeNet Authentication Manager (SAM) is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the Simplified OTP-only configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The Simplified OTP-only configuration is as follows:

- **Connectors**—SAM Connector for OTP Authentication is installed
- **SAM Back-end Service**—Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the **Token Initialization** settings.
- The **SAM Connector for OTP Authentication** is set, by default, to enable enrollment of OTP tokens without requiring changes in the Token Policy Object (TPO) settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

Assigning a Token in SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through McAfee Web Gateway.

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 3400
- SafeNet eToken 3500

Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and helpdesk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.
For more information on SafeNet’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**Adding McAfee Web Gateway as a RADIUS Client in IAS/NPS**

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in McAfee Web Gateway.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in McAfee Web Gateway.

McAfee Web Gateway must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize McAfee Web Gateway for authentication.

---

**NOTE:** This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

The details below refer to NPS, and are very similar to IAS.

1. Click *Start > Administrative Tools > Network Policy Server*.
2. From the NPS web console, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients** and then click **New**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. On the **New RADIUS Client** window, complete the following fields on the **Settings** tab:

<table>
<thead>
<tr>
<th>Enable this RADIUS client</th>
<th>Select this option.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly name</td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td>Address (IP or FQDN)</td>
<td>Enter the McAfee Web Gateway IP address or FQDN.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in McAfee Web Gateway.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

McAfee Web Gateway is added as a RADIUS client in NPS.
Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SafeNet Authentication Manager’s (SAM) OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Configuring McAfee Web Gateway

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

- Configuring Web Gateway to Use RADIUS for Authentication, page 10
- Modifying the Rule Set for Direct Proxy Authentication for RADIUS, page 15

Configuring Web Gateway to Use RADIUS for Authentication

1. Log in to the McAfee Web Gateway console.

2. Click Policy.

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
3. Click the **Settings** tab and then in the left pane, expand **Engines**.

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

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, **SafeNet Authentication Manager**).
   b. In the right pane, in the **Authentication method** field, select **Radius**.
c. Under **Common Authentication Parameters**, complete the following fields:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy realm</td>
<td>Enter a name for the proxy realm (for example, SafeNet).</td>
</tr>
<tr>
<td>Authentication attempt timeout</td>
<td>Enter the maximum time (in seconds) for which the McAfee Web Gateway waits to process an authentication request.</td>
</tr>
<tr>
<td>Use Authentication cache</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Authentication cache entry TTL</td>
<td>Enter the maximum time (in minutes) for which the authentication information is stored in the cache.</td>
</tr>
</tbody>
</table>

d. Under **RADIUS Specific Parameters**, click the **add** 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**.

8. 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 3 of &quot;Adding McAfee Web Gateway as a RADIUS Client in IAS/NPS&quot; on page 8.</td>
</tr>
<tr>
<td>Repeat Password</td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
9. 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.

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

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

(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.
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)

(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)

(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](image1)

(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 the engine (for example 
*SafeNet Authentication Manager*) that you created earlier in step 5 of "Configuring Web Gateway to Use 
RADIUS for Authentication" on page 10.

![Screen Image](image2)

(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**.

![Screen Image](image3)

(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**.

![Image of Action field settings](image1)

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

11. Click **Next**.

![Image of Action field settings](image2)

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

12. Click **Finish**.

![Image of Action field settings](image3)

(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**.

![Screen image of McAfee Web Gateway console](image)

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

### Configuring Proxy server setting in 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**.

![Screen image of Internet Option in Control Panel](image)

(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.

   ![Internet Options window](image)

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

5. Click **LAN settings**.

   ![Internet Options window - LAN settings](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**.

   ![Internet Options](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>

(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>Address</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>Phone</td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</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>