SafeNet Authentication Service
Push OTP 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 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:** 007-013572-001, Rev. A  
**Release Date:** August 2016
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SafeNet Authentication Service Cloud</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SafeNet Authentication Service</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Push OTP Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>Creating Users Stores in SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>Assigning an Authenticator in SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>Adding McAfee Web Gateway as an Authentication Node in SafeNet</td>
<td>8</td>
</tr>
<tr>
<td>Authentication Service</td>
<td></td>
</tr>
<tr>
<td>Checking the SafeNet Authentication Service RADIUS Address</td>
<td>10</td>
</tr>
<tr>
<td>Enabling the Software Token Push OTP Setting</td>
<td>11</td>
</tr>
<tr>
<td>Enabling the Allowed Targets Policy</td>
<td>12</td>
</tr>
<tr>
<td>Configuring McAfee Web Gateway</td>
<td>14</td>
</tr>
<tr>
<td>Configuring Web Gateway to use RADIUS for Authentication</td>
<td>14</td>
</tr>
<tr>
<td>Modifying the Rule Set for Direct Proxy Authentication for RADIUS</td>
<td>18</td>
</tr>
<tr>
<td>Configuring Proxy Server Setting on the Client Machine</td>
<td>22</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>25</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>28</td>
</tr>
</tbody>
</table>
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:

- 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 Push OTP solution.

The primary objective of the Push OTP solution is to reduce the friction around two-factor authentication, and provide users with an improved two-factor authentication experience.

It’s likely that most users already own and always carry a device that can be used as a second factor of authentication. Using the mobile phone as an authenticator replaces the need for a user to carry any additional hardware. So, with Push OTP, a user can:

- Receive authentication requests in real-time via push notifications to his or her smart phone.
- Assess the validity of the request with the information displayed on the screen.
- Respond quickly with a one-tap response to approve or deny the authentication.

Applicability

The information in this document applies to:

- SafeNet Authentication Service (SAS)—SafeNet’s cloud-based authentication service
- MobilePASS+ application
Environment

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

- SafeNet Authentication Service (SAS)
- McAfee Web Gateway—Version 7.5.2.3.0
- Window 7 Client machine with IE 9

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 the following RADIUS topology that supports Push OTP tokens:

**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.

![Diagram](image)

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

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 dataflow of a multi-factor authentication transaction for McAfee Web Gateway.

![Diagram](image)
1. A user attempts to log on to McAfee Web Gateway using a Push OTP authenticator.

2. McAfee Web Gateway sends a RADIUS request with the user’s credentials to SafeNet Authentication Service (SAS) for validation.

3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
   - SAS will directly trigger a Push OTP authentication request.
   - The user receives a push notification on the configured mobile device to indicate there is a login request pending.
   - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token’s PIN code).

4. The SAS authentication reply is sent back to McAfee Web Gateway.

5. 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 (SAS) 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.
- On the RADIUS client machine, set the RADIUS timeout value at least 60 seconds.

**Push OTP Prerequisites**

In order to use SafeNet Authentication Service (SAS) Push OTP you will need:

- **SafeNet Authentication Service configured to enable Push OTP**
- **MobilePASS+ application**
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with McAfee Web Gateway using RADIUS protocol requires the following:

- Creating Users 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
- Enabling the Software Token Push OTP Setting, page 11
- Enabling the Allowed Targets Policy, page 12

Creating Users 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:

- MobilePASS

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, and then click **Add**.

![Auth Nodes module screenshot]

4. Under **Add Auth Nodes**, complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Node Name</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Resource Name</td>
<td>Enter a resource name which will identify in a push notification which authentication node it relates to.</td>
</tr>
<tr>
<td>Low IP Address In Range</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>Configure FreeRADIUS Synchronization</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

![Add Auth Node form]

The authentication node is added to the system.

![Authentication node added to system]

---

SafeNet Authentication Service: Push OTP Integration Guide
Using RADIUS Protocol for McAfee Web Gateway

Document PN: 007-013572-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.
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 click **Auth Nodes**.

3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.
Enabling the Software Token Push OTP Setting

To use Push OTP authentication, the Software Token Push OTP setting must be enabled in the SafeNet Authentication Service (SAS) token policy.

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

2. Click the POLICY tab, and then click Token Policies.

3. In the Token Policies module, click the Software Token Push OTP Setting link.
4. Select **Enable Push OTP communication with MobilePass+**, and then click **Apply**.

**Enabling the Allowed Targets Policy**

For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the self-enrollment of MobilePASS tokens. You can restrict the targets on which MobilePASS+ or MobilePASS 8 tokens are allowed to be activated or enrolled.

1. Log in to the SafeNet Authentication Service (SAS) console with an Operator account.

2. Click the **POLICY** tab, and then select **Token Policies**.
3. In the Token Policies module, click the **Allowed Targets Settings** link.

4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application for this virtual server, and then click **Apply**.
Configuring McAfee Web Gateway

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.

Configuring Web Gateway to use RADIUS for Authentication

1. Log in to the McAfee Web Gateway console.

2. Click Policy.

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

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

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
8. On the **New Password** window, complete the following fields, and then click **OK**.

| **Password** | Enter the shared secret that you entered earlier in step 3 of "Adding McAfee Web Gateway as an Authentication Node in SafeNet Authentication Service" on page 8. |
| **Repeat Password** | Re-enter the shared secret. |

(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**.

![McAfee Web Gateway console](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 number 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.

![McAfee Web Gateway rules](image)

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

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

![Screen Image](image1.png)

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

4. In the right pane, in the table, in the **Enabled** column, select the box to select an appropriate rule (for example, **Authentication Method**), and then click **Edit**.

![Screen Image](image2.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**.

![Edit Rule Window](image)

(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**.

![Property Selection](image)

(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 Service`) that you created earlier in step 5 of "Configuring Web Gateway to use RADIUS for Authentication" on page 14.

![Edit Criteria](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**.

![Edit Rule window](image)

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

![Finish button](image)

*(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**.

![Save Changes button](image)

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

### Configuring Proxy Server Setting 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.

**NOTE:** It is assumed that Microsoft Internet Explorer is installed in client Machine (Window 7).

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

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

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

![LAN setting screenshot](image)

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

6. On the **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**.

![Proxy server settings screenshot](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 enrolled as an OTP token 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>Username</th>
<th>Enter your SAS user ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter a character.</td>
</tr>
</tbody>
</table>

   ![Windows Security](image)

   *(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*
3. SAS will trigger an on-the-go authentication request. You will receive a push notification on the configured mobile device. Tap on **APPROVE**.

![MobilePASS+ app screen](image)

4. On the **TOKEN AUTHENTICATION** screen, enter the token PIN, and then tap **CONTINUE**.
After successful authentication, a success message is displayed on mobile screen.

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&lt;br&gt;4690 Millennium Drive&lt;br&gt;Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States 1-800-545-6608&lt;br&gt;International 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>&lt;br&gt;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>