SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol for McAfee NGFW
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:** 007-013413-001, Rev. A  
**Release Date:** February 2016
## Contents

Third-Party Software Acknowledgement ................................................................. 4  
Description ............................................................................................................. 4  
Applicability .......................................................................................................... 4  
Environment ......................................................................................................... 4  
Audience .................................................................................................................. 5  
RADIUS-based Authentication using SAM .............................................................. 5  
RADIUS Authentication Flow using SAM ............................................................... 5  
RADIUS Prerequisites ............................................................................................ 6  
Configuring SafeNet Authentication Manager ....................................................... 6  
  Synchronizing Users Stores to SAM .................................................................. 6  
  Configuring SAM’s Connector for OTP Authentication ...................................... 7  
  Assigning a Token in SAM .................................................................................. 7  
  Adding McAfee NGFW as a RADIUS Client in IAS/NPS ................................. 8  
  Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client ....................... 9  
Configuring McAfee NGFW .................................................................................. 10  
  Configuring the Authentication Server ............................................................ 10  
  Configuring an Authentication Method for the Authentication Server .......... 13  
  Adding Users to the LDAP Domain ................................................................. 15  
  Adding a User Group to the SSL VPN Portal Policy .................................... 17  
  Refreshing the Firewall Policy ......................................................................... 21  
Running the Solution ............................................................................................. 23  
Support Contacts .................................................................................................. 24
Third-Party Software Acknowledgement

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

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.

The McAfee NGFW engine in the firewall/VPN role is part of the McAfee Next Generation Firewall solution, which is especially well-suited to complex and distributed network environments. In addition to firewalls and virtual private networking, the McAfee NGFW solution also provides intrusion detection and prevention. The configuration, monitoring, and control of the system is done through a centralized Security Management Center (SMC) that provides a single point of contact for a large number of geographically distributed administrators.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in McAfee NGFW using SafeNet one-time password (OTP) tokens managed by SafeNet Authentication Manager.
- Configure McAfee NGFW to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the McAfee NGFW 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 NGFW 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**—Version 8.2 HF 493
- **McAfee NGFW**—Version 5.8.0.12042
- **McAfee Security Management Center**—Version 5.8.1[8817]
**Audience**

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

**RADIUS-based Authentication using SAM**

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 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 SAM**

SafeNet Authentication Manager 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 NGFW.

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

To enable SafeNet Authentication Manager to receive RADIUS requests from McAfee NGFW, ensure the following:

- End users can authenticate from the McAfee NGFW environment with a static password before configuring McAfee NGFW to use RADIUS authentication.
- Ports 1812/1813 are open to and from McAfee NGFW.
- 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 SAM with McAfee NGFW using the RADIUS protocol requires the following:

- Synchronizing Users Stores to SAM, page 6
- Configuring SAM’s Connector for OTP Authentication, page 7
- Assigning a Token in SAM, page 7
- Adding McAfee NGFW as a RADIUS Client in IAS/NPS, page 8
- Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client, page 9

Synchronizing Users Stores to SAM

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 SAM’s Connector for OTP Authentication

SafeNet Authentication Manager 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 SAM

SAM supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through McAfee NGFW.

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 NGFW as a RADIUS Client in IAS/NPS

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

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 NGFW.

McAfee NGFW must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize McAfee NGFW 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 on **RADIUS Clients** and then click **New**.

![Network Policy Server](image-url)  
*(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><strong>Friendly name</strong></td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td><strong>Address (IP or DNS)</strong></td>
<td>Enter the McAfee NGFW IP address or DNS.</td>
</tr>
<tr>
<td><strong>Manual/Generate</strong></td>
<td>Select <strong>Manual</strong>.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></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 NGFW.</td>
</tr>
<tr>
<td><strong>Confirm shared secret</strong></td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

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

4. Click **OK**.

   McAfee NGFW is added as a RADIUS client in NPS.

**Configuring SAM’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.

SAM’s 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 NGFW**

For this integration, McAfee NGFW is used for the web-based SSL VPN connection. Configuring McAfee NGFW multi-factor authentication requires the following:

- Configuring the Authentication Server, page 10
- Configuring an Authentication Method for the Authentication Server, page 13
- Adding Users to the LDAP Domain, page 15
- Adding a User Group to the SSL VPN Portal Policy, page 17
- Refreshing the Firewall Policy, page 21

**Configuring the Authentication Server**

You can authenticate end-user access through firewalls and administrator logins to the SMC against external authentication servers that support either the RADIUS or TACACS+ protocol.

In addition to the server element configuration, you must configure the external authentication server to allow the firewalls to use the authentication services. The Authentication Server component automatically allows single firewalls with static IP addresses to use the authentication services.

1. From the Windows Start menu, click All Programs > McAfee Security Management Center > Management Client.
2. On the McAfee Security Management Center login window, complete the following fields, and then click Log in.

<table>
<thead>
<tr>
<th><strong>User Name</strong></th>
<th>Enter your SMC user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Enter your SMC password.</td>
</tr>
<tr>
<td><strong>Server Address</strong></td>
<td>Enter the IP address of the SMC server.</td>
</tr>
</tbody>
</table>

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
After a successful login, the following window is displayed.

3. Click the **System Status** tab.

4. Click **Configuration > Configuration > User Authentication**.
5. In the left pane, under **User Authentication**, right-click on **Servers**, and then click **New > RADIUS Authentication Server**.

![Image of RADIUS Authentication Server creation](image)

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

6. Complete the following fields, and then click **OK**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the server.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Enter the SAM RADIUS server IP address.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the RADIUS authentication port number. The default is <strong>1812</strong>.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret same as entered in step 3 of &quot;Adding McAfee NGFW as a RADIUS Client in IAS/NPS&quot; on page 8.</td>
</tr>
</tbody>
</table>

![Image of RADIUS Authentication Server properties](image)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
In the right pane, a RADIUS authentication server is added.

Configuring an Authentication Method for the Authentication Server

Define the authentication method used by particular authentication servers, users, and user groups. For this integration, external authentication is provided by servers that support the RADIUS protocol.

1. On the McAfee Security Management Center main window, click Configuration > Configuration > User Authentication.

2. In the left pane, under User Authentication, right-click on Authentication Methods, and then click New Authentication Method.
3. On Authentication Method Properties window, complete the following fields, and then click OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the authentication method (for example, SafenetMethod).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select RADIUS.</td>
</tr>
<tr>
<td>Authentication Servers</td>
<td>Click Add, and then select the IP address of the authentication server that you added earlier in step 6 of “Configuring the Authentication Server” on page 10.</td>
</tr>
</tbody>
</table>

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

In the right pane, an authentication method for user authentication is added.

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
Adding Users to the LDAP Domain

The Users element defines who your users are, and how they can identify themselves to gain access to certain networks and services as defined in your firewall access rules. When using the internal user database, you can create users one by one, or import multiple users from a .ldif file. For this integration, you will create a user in the default LDAP domain. (The InternalDomain domain is present by default in McAfee Security Management Center.)

1. On the McAfee Security Management Center main window, click Configuration > Configuration > User Authentication.

2. In the left pane, expand Users, and then click InternalDomain.

3. In the right pane, expand stonegate, right-click on Mobile VPN users, and then click New Internal User.
4. On the **Internal User Properties** window, on the **General** tab, in the **Name** field, enter the user name.

![Internal User Properties window](image)

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

5. Click the **Authentication** tab, and then perform the following steps:
   
   a. Click **Add** and then select the authentication method that you configured in step 3 of “Configuring an Authentication Method for the Authentication Server” on page 13.
   
   b. Click **OK**.

![Authentication tab](image)

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

In the right pane, users are added.

![Users added](image)

*(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)*
Adding a User Group to the SSL VPN Portal Policy

The portal policies authorize users or group of users access to a set of services.

Make sure you have created an SSL VPN portal policy (for example, ngfwsslpolicy) and added the appropriate web service (for example, firewallngfwservice) to the policy.

1. On the McAfee Security Management Center main window, click Configuration > Configuration > VPN.

2. In the left pane, click SSL VPN Portal Policies.

3. In the right pane, right-click on a policy (for example, ngfwsslpolicy), and then click Edit SSL VPN Portal Policy.
4. On the SSL VPN Portal Policies tab, in the right pane, in the Web Service column, select the appropriate policy (for example, firewallngfwservice).

5. In the Authentication column, right-click on the selected row, and then click Edit Authentication.
6. On the **Authentication Parameters** window, under **Name**, click **Users**.

   ![Authentication Parameters window](image1)

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

7. Click **InternalDomain**.

   ![InternalDomain window](image2)

   *(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)*
8. Expand **stonegate**, select **Mobile VPN users**, and then click **Add**.

![Authentication Parameters](image1)

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

9. Click **OK**.

10. On the McAfee Security Management Center main window, click the icon.

![Highlevelpolicy](image2)

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

After creating or modifying a firewall policy, you must transfer the changes to the engine using McAfee Security Management Center. You can either install the policy (which transfers a selected policy), or refresh the policy (which transfers the most recent version of the policy that the engine currently uses).

It is assumed that the policy (for example, test) with the appropriate rules is already installed on the firewall.

1. On the McAfee Security Management Center main window, click the System Status tab.

2. Click the icon, and then in the left pane, expand Firewalls.

3. Right-click on the appropriate firewall (for example, ngfwsllvpn), and then click Current Policy > Refresh.
4. On the **Refresh Policy Task Properties** window, perform the following steps:
   a. In the **Policy** field, ensure that the correct policy (for example, **test**) is selected.
   b. Select **Validate Policy before Upload**.
   c. Click **OK**.

   ![Refresh Policy Task Properties](image)

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

   The following window is displayed if the policy is successfully updated.

   ![Uploaded Policy Test](image)

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

For this integration, SafeNet eToken PASS is configured for authentication with the SAM solution.

1. In a web browser, open the following URL:
   
   https://<McAfee SSL VPN Domain>

   Where, McAfee SSL VPN Domain is domain that will be used to connect to McAfee SSL VPN.

2. On the McAfee login page, complete the following fields, and then click Submit.

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>Enter your Mobile VPN user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD</td>
<td>Generate an OTP using SafeNet eToken PASS, and then enter it in this field.</td>
</tr>
</tbody>
</table>

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

If the login credentials are validated, you are provided access to the service and application.

   (The screen image above is from McAfee®. 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</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></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>