SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for McAfee NGFW
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-013236-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>July 2015</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
## Contents

Third-Party Software Acknowledgement................................................................. 4
Description............................................................................................................... 4
Applicability ........................................................................................................... 4
Environment .......................................................................................................... 5
Audience .................................................................................................................. 5
RADIUS-based Authentication using SAS Cloud...................................................... 5
RADIUS-based Authentication using SAS-SPE and SAS-PCE................................. 6
RADIUS Authentication Flow using SAS ............................................................... 6
RADIUS Prerequisites........................................................................................... 7
Configuring SafeNet Authentication Service ........................................................... 7
  Synchronizing Users Stores in SAS ................................................................. 7
  Assigning an Authenticator in SAS ................................................................. 8
  Adding McAfee NGFW as an Authentication Node in SAS ............................... 9
  Checking the SAS RADIUS Server’s IP Address ............................................. 11
Configuring McAfee NGFW................................................................................. 12
  Configuring the Authentication Server ............................................................ 12
  Configuring an Authentication Method for the Authentication Server ......... 16
  Adding Users to the LDAP Domain ................................................................. 17
  Adding a User Group to the SSL VPN Portal Policy ................................... 20
  Refreshing the Firewall Policy ........................................................................ 24
Running the Solution ............................................................................................ 27
Support Contacts.................................................................................................... 28
**Third-Party Software Acknowledgement**

This document is intended to help users of SafeNet 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 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.

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) authenticators managed by SafeNet Authentication Service.
- Configure McAfee NGFW to work with SafeNet Authentication Service 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 Service.

McAfee NGFW 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 (SAS)**—SafeNet’s cloud-based authentication service
- **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 Service.

RADIUS-based Authentication using SAS Cloud

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.

- **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.

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: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

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

For both on-premises versions, 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 SAS

SafeNet Authentication Service 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 NGFW.

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

To enable SafeNet Authentication Service 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 the 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 Service

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

- Synchronizing Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding McAfee NGFW as an Authentication Node in SAS, page 9
Synchronizing Users Stores in SAS

Before SAS can authenticate any user in your organization, you must 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 be found on the SafeNet Knowledge Base site.
Assigning an Authenticator in SAS

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

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet GOLD
- SMS Token
- MP-1 Software Token
- 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 NGFW as an Authentication Node in SAS

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

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>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host that will authenticate with SAS (in this case, a range of IP addresses is being used).</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>

The authentication node is added to the system.
Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in McAfee NGFW, check its IP address. The IP address will then be added to McAfee NGFW 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 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 12
- Configuring an Authentication Method for the Authentication Server, page 16
- Adding Users to the LDAP Domain, page 17
- Adding a User Group to the SSL VPN Portal Policy, page 20
- Refreshing the Firewall Policy, page 24

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, select All Programs > McAfee Security Management Center > Management Client.

   ![Login Screen](image)

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

2. Complete the following fields, and then click Log in.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter your SMC user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter your SMC password.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Enter the IP address of the SMC server.</td>
</tr>
</tbody>
</table>
After a successful login, the following window is displayed.

3. Click the System Status tab.

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
4. Select **Configuration > Configuration > User Authentication.**

![Image](image_url)

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

5. In the left pane, click **User Authentication.**

![Image](image_url)

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

6. In the left pane, right-click on **Servers**, and then click **New > RADIUS Authentication Server.**

![Image](image_url)

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
7. 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 this server.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Enter the SAS RADIUS IP address.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the RADIUS authentication port number. The default is 1812.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the secret key for communication with the SAS RADIUS server. This entry must match the shared secret that was configured in &quot;Adding McAfee NGFW as an Authentication Node in SAS,&quot; on page 9.</td>
</tr>
</tbody>
</table>

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

A RADIUS authentication server is now added in **McAfee Security Management Center**.

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

1. From the Windows Start menu, launch the McAfee Security Management Center, and then log in.
2. Click the System Status tab, and then select Configuration > Configuration > User Authentication.

3. In the left pane, right-click on Authentication Methods, and then click New Authentication Method.

4. 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 server that you configured in “Configuring the Authentication Server,” on page 12.</td>
</tr>
</tbody>
</table>
An authentication method for user authentication is now added.

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 the users one by one, or import multiple users from an .ldif file. For this integration, you will create a user in the default LDAP domain. (This is the “InternalDomain,” which is present by default in McAfee Security Management Center.)

1. From the Windows Start menu, launch the McAfee Security Management Center, and then log in.
2. Click the System Status tab, and then select Configuration > Configuration > User Authentication.

(The screen image above is from McAfee. Trademarks are the property of their respective owners.)
3. In the left pane, expand Users, and then select InternalDomain.

![Image of Users and InternalDomain expanded]

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

4. In the right pane, expand stonegate, right-click on Mobile VPN users, and then select New Internal User.

![Image of stonegate expanded]

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

5. On the Internal User Properties window, enter the user’s name in Name field, and then click the Authentication tab.

![Image of Internal User Properties]

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
6. On the Authentication tab, click Add, and then select the authentication method that you configured in “Configuring an Authentication Method for the Authentication Server,” on page 16, and then click OK.

![Image of Authentication setup](image1)

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

Users are now added to the LDAP Domain.

![Image of Users added](image2)

*(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.

Before you can complete this section, 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. From the Windows Start menu, launch the McAfee Security Management Center, and then log in.
2. Click the System Status tab, and then select Configuration > Configuration > VPN.

![Configuration view](image)

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

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

![SSL VPN Portal Policies](image)

(“The screen image above is from McAfee®. Trademarks are the property of their respective owners.”)
4. In the right pane, right-click on a policy (for example, `ngfwsslpolicy`), and then select **Edit SSL VPN Portal Policy**.

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

The following window is displayed.

5. In the right pane, under **Web Service**, select the appropriate policy (for example, `firewallngfwservice`).

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
6. Right-click the Authentication cell, and then select Edit Authentication.

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

7. On the Authentication Parameters window, click Users.

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

   ![InternalDomain](image1.png)

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

9. Expand **stonegate**, select **Mobile VPN users**, and then click **Add**.

   ![Mobile VPN users](image2.png)

   *(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)*
10. Click OK to close the Authentication Parameters window, and then click the Save icon.

(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 the Management Client. 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. From the Windows Start menu, launch the McAfee Security Management Center, and then log in.
2. Click the System Status tab, and then click the system Status icon.
3. In the left pane, expand Firewalls, and then select the appropriate firewall (for example, ngfwsslypn).

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
4. Right-click on the selected firewall, and then select **Current Policy > Refresh**.

5. On the **Refresh Policy Task Properties** window:
   a. Ensure that the correct policy (for example, **test**) is selected in the **Policy** field.
   b. Select the **Validate Policy before Upload** check box.
   c. Click **OK**.

(The screen image above is from McAfee®. Trademarks are the property of their respective owners.)
6. If the policy is successfully updated, the following window is displayed.

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

Verify the integration solution after you have successfully configured the McAfee NGFW solution.

In this solution, the SafeNet eToken PASS is used as the enrolled OTP token.

1. In a web browser, open the McAfee URL: \texttt{https://<McAfee SSL VPN Domain>}. 

2. On the login page, complete the following fields, and then click \textbf{Submit}.

\begin{tabular}{|l|l|}
\hline
\textbf{USERNAME} & Enter your Mobile VPN user name. \\
\hline
\textbf{PASSWORD} & Generate an OTP using SafeNet eToken PASS, and then enter it in this field. \\
\hline
\end{tabular}

3. If the credentials are validated, you will be successfully logged in, and you can access the configured service and application.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{login_screenshot.png}
\caption{The screen image above is from McAfee\textsuperscript{®}. Trademarks are the property of their respective owners.}
\end{figure}
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 SafeNet Customer Support. SafeNet 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 SafeNet 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>SafeNet, 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></td>
</tr>
<tr>
<td>United States</td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Existing customers</td>
<td>with a Technical Support Customer Portal account can log</td>
</tr>
<tr>
<td></td>
<td>in to manage incidents, get the latest software</td>
</tr>
<tr>
<td></td>
<td>upgrades, and access the SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>