SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol for FortiGate-VM
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:** 007-013503-001, Rev. A  
**Release Date:** May 2016
Third-Party Software Acknowledgement

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

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.

Fortinet FortiGate-VM firewall technology delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features. Application control, antivirus, IPS, Web filtering and VPN along with advanced features such as an extreme threat database, vulnerability management and flow-based inspection work in concert to identify and mitigate the latest complex security threats. The security-hardened FortiOS operating system is purpose-built for inspection and identification of malware.

This document describes how to:

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

It is assumed that the FortiGate-VM 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.

FortiGate-VM 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
- **FortiGate-VM**—Version 5.0.9 build8070 (GA Patch 9)
Audience

This document is targeted to system administrators who are familiar with FortiGate-VM, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager (SAM).

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 FortiGate-VM.

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

To enable SafeNet Authentication Manager (SAM) to receive RADIUS requests from FortiGate-VM, ensure the following:

- End users can authenticate from the FortiGate-VM environment with a static password before configuring the FortiGate-VM to use RADIUS authentication.
- Ports 1812/1813 are open to and from FortiGate-VM.
- 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 FortiGate-VM 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 7
- Adding FortiGate-VM 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 FortiGate-VM.

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 FortiGate-VM 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 FortiGate-VM.

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 FortiGate-VM.

FortiGate-VM must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize FortiGate-VM 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**.

   ![Network Policy Server](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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this RADIUS client</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Friendly name</td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td>Address (IP or DNS)</td>
<td>Enter the FortiGate-VM IP address or DNS.</td>
</tr>
<tr>
<td>Manual/Generate</td>
<td>Select <strong>Manual</strong>.</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 FortiGate-VM.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>

![New RADIUS Client](image)

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

4. Click **OK**.

FortiGate-VM 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 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 FortiGate-VM

Configuring the FortiGate-VM multi-factor authentication using SafeNet Authentication Manager (SAM) requires:

- Creating a RADIUS Server, page 10
- Creating a User on the RADIUS Server, page 12
- Creating an SSL VPN Security Policy, page 15

Creating a RADIUS Server

Create a RADIUS server to use RADIUS authentication with FortiGate-VM.

1. In a web browser, open the following URL:
   https://<Public DNS Address of FortiGate-VM>
2. On the FortiGate-VM login window, enter the administrator’s user name and password, and then click Login.

(The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)
3. On the FortiGate-VM administrator console, in the left pane, under User & Device, click Authentication > RADIUS Servers.

4. In right pane, click Create New.

5. On the New RADIUS Server window, complete the following fields, and then click OK.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the RADIUS server (for example, SAM).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Server Name/IP</td>
<td>Enter an IP address for the RADIUS server.</td>
</tr>
<tr>
<td>Primary Server Secret</td>
<td>Enter the shared secret that you entered earlier in step 3 of “Adding FortiGate-VM as a RADIUS Client in IAS/NPS” on page 8.</td>
</tr>
<tr>
<td>Authentication Scheme</td>
<td>Select the Use Default Authentication Scheme option.</td>
</tr>
</tbody>
</table>

(The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)
On the FortiGate-VM administrator console, in the right pane, the newly created RADIUS server is added.

![RADIUS Server Added](image)

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

**Creating a User on the RADIUS Server**

Create a user on the RADIUS server that will be authenticated using SafeNet Authentication Manager (SAM).

1. On the FortiGate-VM administrator console, in the left pane, under **User & Device**, click **User > User Definition**.

![User Definition](image)

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

2. In the right pane, click **Create New**.
3. On the **User Creation Wizard** window, under **Choose User Type**, select the **Remote RADIUS User** option, and then click **Next**.

   ![User Creation Wizard](image1.png)

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

4. Under **Specify RADIUS Server**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter a user name (for example, <strong>Alice</strong>).</td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>Select the RADIUS server (for example, <strong>SAM</strong>) that you created earlier in step 5 of “Creating a RADIUS Server” on page 10.</td>
</tr>
</tbody>
</table>

   ![User Creation Wizard](image2.png)

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

5. Under **Provide Contact Info**, click **Next**.

   ![User Creation Wizard](image3.png)

   *(The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)*
6. Under **Provide Extra Info**, select **Enable**, and then click **Done**.

**NOTE:** Ensure that **Two-factor Authentication** and **User Group** options are not selected.

On the FortiGate-VM administrator console, in the right pane, the newly created RADIUS user is listed.

(The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)
Creating an SSL VPN Security Policy

Create an SSL VPN security policy that will allow specific users or user groups to access SSL VPN.

1. On the FortiGate-VM administrator console, in the left pane, under Policy, click Policy > Policy.

   ![政策界面](The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)

2. In the right pane, click Create New.

3. On the New Policy window, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Type</td>
<td>Select the VPN option.</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>Select the external port number.</td>
</tr>
<tr>
<td>Remote Address</td>
<td>Select All.</td>
</tr>
<tr>
<td>Local Interface</td>
<td>Select the internal port number.</td>
</tr>
<tr>
<td>Local Protected Subnet</td>
<td>Select the SSL VPN tunnel IP range.</td>
</tr>
</tbody>
</table>

   ![新政策界面](The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)

SafeNet Authentication Manager: Integration Guide
Using RADIUS Protocol for FortiGate-VM
Document PN: 007-013503-001, Rev. A, Copyright © 2016 Gemalto, Inc., All rights reserved.
4. Under **Configure SSL-VPN Authentication Rules**, click **Create New**.

![Configure SSL-VPN Authentication Rules](image)

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

5. On the **New SSL VPN Authentication Rule** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>User(s)</strong></th>
<th>Select the user (for example, <strong>Alice</strong>) that you created earlier in step 4 of “Creating a User on the RADIUS Server” on page 12. The user can connect to the SSL VPN tunnel.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSL-VPN Portal</strong></td>
<td>Select a portal configuration (for example, <strong>full-access</strong>) for the user.</td>
</tr>
</tbody>
</table>

![New SSL VPN Authentication Rule](image)

*(The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)*
6. On the FortiGate-VM administrator console, in the right pane, under Configure SSL-VPN Authentication Rules, the user (for example Alice) is added. Click OK.

![Configuration Screen](image)

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

**Running the Solution**

For this integration, SafeNet eToken PASS token is configured for authentication with the SafeNet Authentication Manager (SAM) solution.

**Connecting to FortiGate-VM Using a Web Browser**

1. In a web browser, open the following URL:
   
   https://<external FQDN or IP address of FortiGate-VM>

2. On the login window, complete the following fields, and then click Login.

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

   ![Login Screen](image)

   (The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)
If the authentication is successful, you are successfully logged in to the FortiGate Firewall SSL VPN portal.

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

Connecting to FortiGate-VM Using FortiClient

Configure FortiClient (refer to “Appendix: Configuring FortiClient” on page 19) and then connect to FortiGate Firewall SSL VPN using FortiClient.

1. Double-click the FortiClient icon.

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

2. On FortiClient, perform the following steps:
   a. Select the SSL VPN connection (for example, connection1)
   b. In the Username field, enter the username.
   c. Generate an OTP using the SafeNet eToken PASS token and then in the Password field, enter that OTP.
   d. Click Connect.

(The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)
If the authentication is successful, you are successfully connected to FortiGate Firewall SSL VPN.

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

Appendix: Configuring FortiClient

Configuring FortiClient requires:

- Installing FortiClient, page 19
- Creating an SSL VPN Connection, page 20

Installing FortiClient

1. Connect to the FortiGate SSL VPN web portal.
2. Under FortiClient Download, click a link (for example, FortiClient Windows) to download the FortiClient installer file.

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

3. After the download is complete, double-click the FortiClient installer file to install FortiClient.
Creating an SSL VPN Connection

1. Double-click the FortiClient icon.

2. On FortiClient, click Configure VPN.

3. On the New VPN Connection window, on the SSL-VPN tab, complete the following fields, and then click Apply.

<table>
<thead>
<tr>
<th>Connection Name</th>
<th>Enter a name for the connection (for example connection1).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Gateway</td>
<td>Enter the IP address of the FortiGate server.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select the Prompt on login option.</td>
</tr>
</tbody>
</table>

(The screen image above is from FortiGate® software. 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>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</td>
</tr>
<tr>
<td></td>
<td>Customer Portal account can log in to</td>
</tr>
<tr>
<td></td>
<td>manage incidents, get the latest software</td>
</tr>
<tr>
<td></td>
<td>upgrades, and access the Gemalto Knowledge</td>
</tr>
<tr>
<td></td>
<td>Base.</td>
</tr>
</tbody>
</table>