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: 007-013504-001, Rev. A
Release Date: September 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 Service (SAS) 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.

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 (OTP) authenticators managed by SafeNet Authentication Service.
- Configure FortiGate-VM to work with SafeNet Authentication Service 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 Service.

FortiGate-VM 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 – Private Cloud Edition (SAS-PCE)**
- **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 Service (SAS).

RADIUS-based Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (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.gemalto.com/sas-downloads/docs/007-012390-002_SAS_Agent_for_NPS_1.30_ConfigurationGuide_RevD.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 SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

For both on-premises versions, SafeNet Authentication Service (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 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 data flow of a multi-factor authentication transaction for FortiGate-VM.

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

To enable SafeNet Authentication Service (SAS) 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.
- A token is enrolled to a user in SAS.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with FortiGate-VM using RADIUS protocol requires the following:

- Creating Users Stores in , page 7
- Assigning an Authenticator in SAS, page 8
- Adding FortiGate-VM as an Authentication Node in , page 8
- Checking the SafeNet Authentication Service RADIUS Address, page 11

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 SAS

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 FortiGate-VM.

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 FortiGate-VM 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 FortiGate-VM. You will need the IP address of FortiGate-VM and the shared secret to be used by both SAS and FortiGate-VM.

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.

![Auth Nodes module](image)

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><strong>Agent Description</strong></td>
<td>Enter a host description.</td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td><strong>Low IP Address In Range</strong></td>
<td>Enter the IP address of the host.</td>
</tr>
<tr>
<td><strong>High IP Address In Range</strong></td>
<td>Leave this field blank.</td>
</tr>
<tr>
<td><strong>Configure FreeRADIUS</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Synchronization</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td><strong>Confirm Shared Secret</strong></td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>
The authentication node is added to the system.

Checking the SafeNet Authentication Service RADIUS Address

Before adding SafeNet Authentication Service (SAS) as a RADIUS server in FortiGate-VM, check its IP address. The IP address will then be added to FortiGate-VM 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.

![Auth Nodes module screenshot](image)

### Configuring FortiGate-VM

Configuring the FortiGate-VM multi-factor authentication using SafeNet Authentication Service (SAS) requires:

- Creating a RADIUS Server, page 12
- Creating a User on the RADIUS Server, page 14
- Creating an SSL-VPN Security Policy, 17

### Creating a RADIUS Server

Create a RADIUS Server with the RADIUS credentials to use the RADIUS authentication with the FortiGate Firewall VPN connection.

1. In a web browser, open the following URL:
   
   [https://<Public DNS Address of FortiGate-VM>](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**.

![Login screen](image)

*(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**.

![RADIUS Server Configuration](image)

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

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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the RADIUS server (for example, SAS).</td>
</tr>
<tr>
<td><strong>Primary Server Name/IP</strong></td>
<td>Enter an IP address for the RADIUS server.</td>
</tr>
<tr>
<td><strong>Primary Server Secret</strong></td>
<td>Enter the shared secret that you entered earlier in step 5 of “Adding FortiGate-VM as an Authentication Node in SafeNet Authentication Service” on page 9.</td>
</tr>
<tr>
<td><strong>Authentication Scheme</strong></td>
<td>Select the <strong>Use Default Authentication Scheme</strong> 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.

![FortiGate console screen](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 Service (SAS).

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

![FortiGate user definition screen](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)

*(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><strong>User Name</strong></td>
<td>Enter a user name.</td>
</tr>
<tr>
<td><strong>RADIUS Server</strong></td>
<td>Select the RADIUS server (for example, SAS) that you created earlier in step 5 of “Creating a RADIUS Server” on page 12.</td>
</tr>
</tbody>
</table>

![Specify RADIUS Server](image2)

*(The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)*
5. Under **Provide Contact Info**, in the **Email Address** field, enter the user's email address, and then click **Next**.

6. Under **Provide Extra Info**, select **Enable**, and then click **Done**.

---

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

A success message is displayed.

(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.

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>

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

| **User(s)** | Select and add the required user who will be allowed to connect to the SSL-VPN. |
| **SSL-VPN Portal** | Select a portal configuration (for example, **full-access**) that will be used when connected. |

![New SSL VPN Authentication Rule](image)

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

If a user is assigned a GrIDsure token, the user needs to select a grid pattern as a password. To fetch a grid for the user, the administrator needs to configure several settings on the Fortigate-VM management portal. For settings, refer to “Appendix B: Modifying Login Page for a GridSure Token” on page 23. When an administrator completes the configuration, the Get Grid button displays on the SSL VPN login page.

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>:<SSL VPN port>

2. On the login window, in the Name field, enter your user name, and then click Get GrID.

3. In the Password field, enter your Personal Identification Pattern (PIP), and then click Login.

![Login Screen](image)
After successful authentication, you will be logged in to the FortiGate Firewall SSL VPN portal.

Connecting to FortiGate-VM Using FortiClient

Configure FortiClient (refer to “Appendix A: Configuring FortiClient” on page 21) and then connect to FortiGate Firewall SSL VPN using FortiClient.

1. Open FortiClient.
2. On the login window, complete the following fields, and then click Connect.
   a. Select the VPN profile (for example, Test)
   b. In the Username field, enter your user name.
   c. In the Password field, enter the OTP.
If the authentication is successful, you will be successfully logged in to the FortiGate Firewall SSL VPN.

![FortiGate SSL VPN login screen](The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)

**Appendix A: Configuring FortiClient**

Configuring FortiClient requires:

- Installing FortiClient, page 21
- Creating an SSL VPN Connection, page 22

**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.

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

3. Install FortiClient using the installer file.
Creating an SSL VPN Connection

1. Open FortiClient.

2. On the FortiClient login window, click the icon, and then click Add a new connection.

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

<table>
<thead>
<tr>
<th><strong>Connection Name</strong></th>
<th>Enter a name for the connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Gateway</strong></td>
<td>Enter the IP address of the FortiGate server.</td>
</tr>
<tr>
<td><strong>Authentication</strong></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.)
Appendix B: Modifying Login Page for a GridSure Token

1. On the FortiGate-VM administrator console, under System, click Config > Replacement Messages.

2. In the right pane, scroll down, click SSL VPN login Page, and then paste the below mentioned code in the highlighted area.

```
<!DOCTYPE html>
<html lang="en">
<head>

</head>
```

**NOTE:** The below code is available in Inquira at the "http://bel1web002:9876/Files/1f0edbc9976946f1a6b6c450276a8832" URL.
3. Click Save.

(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><strong>Address</strong></td>
<td>Gemalto</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>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><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></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>