SafeNet Authentication Service
Push OTP 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 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:** 007-013536-001, Rev. A  
**Release Date:** June 2016
Contents

Third-Party Software Acknowledgement ........................................................................................................... 4
Description ............................................................................................................................................................ 4
Applicability .......................................................................................................................................................... 5
Environment .......................................................................................................................................................... 5
Audience ................................................................................................................................................................. 5
RADIUS-based Authentication using SafeNet Authentication Service Cloud ....................................................... 5
RADIUS Authentication Flow using SafeNet Authentication Service ............................................................... 6
RADIUS Prerequisites ......................................................................................................................................... 6
Push OTP Prerequisites ........................................................................................................................................ 6
Configuring SafeNet Authentication Service ..................................................................................................... 7
  Creating Users Stores in SafeNet Authentication Service ................................................................................ 7
  Assigning an Authenticator in SafeNet Authentication Service ........................................................................ 7
  Adding FortiGate-VM as an Authentication Node in SafeNet Authentication Service ..................................... 8
  Checking the SafeNet Authentication Service RADIUS Address ................................................................. 10
  Enabling the Software Token Push OTP Setting ............................................................................................. 11
  Enabling the Allowed Targets Policy ............................................................................................................. 12
Configuring FortiGate-VM .................................................................................................................................. 13
  Creating a RADIUS server ............................................................................................................................... 13
  Creating a User on the RADIUS Server ............................................................................................................. 16
  Creating an SSL VPN Security Policy ............................................................................................................. 19
Running the Solution ........................................................................................................................................... 21
  Connecting to the FortiGate Secure Portal Using the Hybrid Mode ............................................................... 24
Appendix: Modifying the Login Window (Hybrid Mode) ..................................................................................... 27
  Downloading the HTML Code and the loading_spinner.gif File .................................................................... 27
  Uploading the HTML Code to FortiGate-VM .................................................................................................. 28
  Uploading the loading_spinner.gif File to FortiGate-VM ................................................................................ 29
Support Contacts ................................................................................................................................................. 30
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 Push one-time password (OTP) solution managed by SafeNet Authentication Service.

- Configure FortiGate-VM to work with SafeNet Authentication Service in the 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 Push OTP solution.

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

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

- Receive authentication requests in real-time via push notifications to his or her smart phone.

- Assess the validity of the request with the information displayed on the screen.

- Respond quickly with a one-tap response to approve or deny the authentication.
Applicability

The information in this document applies to:

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

Environment

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

- **SafeNet Authentication Service (SAS)**
- **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.

RADIUS-based Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides the following RADIUS topology that supports Push OTP tokens:

**SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.
**RADIUS Authentication Flow using SafeNet Authentication Service**

SafeNet Authentication Service (SAS) communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for FortiGate-VM.

1. A user attempts to log on to FortiGate-VM using a Push OTP authenticator.
2. FortiGate-VM sends a RADIUS request with the user's credentials to SafeNet Authentication Service (SAS) for validation.
3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
   - SAS will directly trigger a Push OTP authentication request.
   - The user receives a push notification on the configured mobile device to indicate that there is a login request pending.
   - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token's PIN code).
4. The SAS authentication reply is sent back to FortiGate-VM.
5. The user is granted or denied access to 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.
- On the client machine, set the RADIUS timeout value at least 60 seconds.
Push OTP Prerequisites

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

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

Configuring SafeNet Authentication Service

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

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 7
- Adding FortiGate-VM as an Authentication Node in SafeNet Authentication Service, page 8
- Checking the SafeNet Authentication Service RADIUS Address, page 10
- Enabling the Software Token Push OTP Setting, page 11
- Enabling the Allowed Targets Policy, page 12

Creating Users Stores in SafeNet Authentication Service

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the **Create User** shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through FortiGate-VM.

The following authenticators are supported:

- **MobilePASS**
Authenticators can be assigned to users in two ways:

- **Manual provisioning** — Assign an authenticator to users one at a time.
- **Provisioning rules** — The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.


**Adding 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 click **Auth Nodes**.
3. In the **Auth Nodes** module, click the **Auth Nodes** link, and then click **Add**.

![Auth Nodes module](image)

**Auth Nodes**: Create and configure SafeNet Authentication Service Authentication Nodes

Using the RADIUS protocol over the Internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security and for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.

- Primary RADIUS Server IP: 64.20.164.68:1812
- Primary SafeNet Authentication Service Agent DNS: safenetagent.safenet-inc.com:443
- Failover RADIUS Server IP: 64.20.164.68:1812
- Failover SafeNet Authentication Service Agent DNS: safenetagent.safenet-inc.com:443
- Max. Auth Nodes: 10

No Records

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

- **Auth Node Name**: Enter a host description.
- **Resource Name**: Enter a resource name which will identify in a push notification which authentication node it relates to.
- **Low IP Address In Range**: Enter the IP address of the host.
- **Configure FreeRADIUS Synchronization**: Select this option.
- **Shared Secret**: Enter the shared secret key.
- **Confirm Shared Secret**: Re-enter the shared secret key.

![Add Auth Node form](image)

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 click Auth Nodes.

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

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

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

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

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

**Enabling the Allowed Targets Policy**

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

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

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

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

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

**Configuring FortiGate-VM**

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

- Creating a RADIUS server, page 13
- Creating a User on the RADIUS Server, page 16
- Creating an SSL VPN Security Policy, page 19

**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.

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, SAS).</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 4 of “Adding FortiGate-VM as an Authentication Node in SafeNet Authentication Service” on page 8.</td>
</tr>
<tr>
<td>Authentication Scheme</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.

(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.

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.

(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>User Name</th>
<th>Enter a user name (for example, <em>Alice</em>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Server</td>
<td>Select the RADIUS server (for example, <em>SAS</em>) that you created earlier in step 5 of “Creating a RADIUS server” on page 13.</td>
</tr>
</tbody>
</table>

5. Under **Provide Contact Info**, in the **Email Address** field, enter the user's email address, and then click **Next**.

(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**.

![Image of FortiGate VM administrator console](image_url)

*(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 user is listed.

![Image of FortiGate VM administrator console](image_url)

*(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><strong>Policy Type</strong></td>
<td>Select the <strong>VPN</strong> option.</td>
</tr>
<tr>
<td><strong>Incoming Interface</strong></td>
<td>Select the external port number.</td>
</tr>
<tr>
<td><strong>Remote Address</strong></td>
<td>Select <strong>All</strong>.</td>
</tr>
<tr>
<td><strong>Local Interface</strong></td>
<td>Select the internal port number.</td>
</tr>
<tr>
<td><strong>Local Protected Subnet</strong></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](image1)

*(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>User(s)</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 16. The user can connect to the SSL VPN tunnel.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL-VPN Portal</td>
<td>Select a portal configuration (for example, <strong>full-access</strong>) for the user.</td>
</tr>
</tbody>
</table>

![New SSL VPN Authentication Rule](image2)

*(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**.

![Image of FortiGate-VM administrator console](image)

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

---

**Running the Solution**

Connecting to the FortiGate Secure Portal Using the Simple Mode

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 **Login**.

![Image of FortiGate secure portal login screen](image)

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

SAS will trigger an on-the-go authentication request.
3. You will receive an authentication notification on the registered mobile device. On the mobile device screen, tap **APPROVE**.

![MobilePASS+ screen](image1)

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

4. On the **TOKEN AUTHENTICATION** window, enter the token PIN, and then tap **CONTINUE**.

![Token Authentication screen](image2)

*(The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)*
A success message is displayed on the mobile screen.

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

You will be 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 the FortiGate Secure Portal Using the Hybrid Mode

In this scenario, the hybrid mode login window is used, and you can choose any of the following options for authentication:

- Use my mobile to autosend a passcode
- Enter a passcode manually

1. In a web browser, open the following URL:
   https://<external FQDN or IP address of FortiGate-VM>:<SSL VPN port>
2. On the hybrid mode login window, in the Name field, enter your SAS user name, select the **Use my mobile to autosend a passcode** option, and then click **Submit**.

*(The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)*
SAS will trigger an on-the-go authentication request.

3. You will receive a push notification on the registered mobile device. On the mobile device screen, tap APPROVE.
4. On the **TOKEN AUTHENTICATION** window, enter the token PIN, and then tap **CONTINUE**.

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

A success message is displayed on the mobile screen.

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

Appendix: Modifying the Login Window (Hybrid Mode)

Modifying the login window for the hybrid mode requires:

- Downloading the HTML Code and the loading_spinner.gif File, page 27
- Uploading the HTML Code to FortiGate-VM, page 28
- Uploading the loading_spinner.gif File to FortiGate-VM, page 29

Downloading the HTML Code and the loading_spinner.gif File

1. In a web browser, open the following url to download the Fortigate SSLVPN with PushOTP HybridMode including spinner.zip file (containing the HTML code file and the loading_spinner.gif file) from Inquira: http://bel1web002:9876/Files/a0d6e1517e7d418fae049a474668d29c
2. Unzip the file.
Uploading the HTML Code to FortiGate-VM

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

![FortiGate VM64-AWSONDEMAND](image1)

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

2. In the right pane, scroll down, under SSLVPN, click SSLVPN Login Page. Then, paste the html code (given in the downloaded HTML file) in highlighted area.

![FortiGate VM64-AWSONDEMAND](image2)

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

3. Click Save.
Uploading the loading_spinner.gif File to FortiGate-VM

1. On the FortiGate-VM administrator console, in the left pane, under System, click Config > Replacement Messages, and then in the right pane, click Manage Images.

2. Click Create New.

(The screen image above is from FortiGate® software. Trademarks are the property of their respective owners.)
3. In the **Name** field, enter a name for the image, and then click **Browse** to search for and select the `loading_spinner.gif` file.

4. Click **OK**. The image will be uploaded to the FortiGate-VM.

**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>
</table>
| **Address**           | Gemalto  
4690 Millennium Drive  
Belcamp, Maryland 21017 USA |
| **Phone**             | United States  
1-800-545-6608  
International  
1-410-931-7520 |
| **Technical Support** |  
https://serviceportal.safenet-inc.com  
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.  

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