SafeNet Authentication Manager
Integration Guide

Using SafeNet Authentication Manager as an Identity Provider for Citrix NetScaler Gateway
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.
Third-Party Software Acknowledgement

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

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.

Citrix NetScaler Gateway is a secure application and data access solution that gives IT administrators a single point to manage access control and limit actions within sessions based on both user identity and the endpoint device. New threats, risks, and vulnerabilities as well as evolving business requirements underscore the need for a strong authentication approach based on Multi-Factor Authentication.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Citrix NetScaler Gateway using SafeNet tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in Citrix NetScaler Gateway using SafeNet Authentication Manager as an identity provider.

It is assumed that the Citrix NetScaler Gateway environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

Citrix NetScaler Gateway can be configured to support multi-factor authentication in several modes. The SAML authentication 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
- **Citrix NetScaler Gateway**—Version 11.0


**Audience**

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

**SAML Authentication using SafeNet Authentication Manager**

SafeNet Authentication Manager (SAM) provides a SAML authentication option that is already implemented in the SAM environment and can be used without any installation.

![Diagram of SAML Authentication using SafeNet Authentication Manager](image)

**Authentication Flow using SafeNet Authentication Manager**

SafeNet Authentication Manager (SAM) communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Citrix NetScaler Gateway.

![Diagram of Authentication Flow using SafeNet Authentication Manager](image)

1. A user attempts to log on to Citrix NetScaler Gateway. The user is redirected to SafeNet Authentication Manager (SAM). SAM collects and evaluates the user's credentials.
2. SAM returns a response to Citrix NetScaler Gateway, accepting or rejecting the user's authentication request.
SAML Prerequisites

To enable SafeNet Authentication Manager (SAM) to receive SAML authentication requests from Citrix NetScaler Gateway, ensure that the end users can authenticate from the Citrix NetScaler Gateway environment with a static password.

Configuring SafeNet Authentication Manager

Using SafeNet Authentication Manager (SAM) as an identity provider for Citrix NetScaler Gateway requires the following:

- Synchronizing User Stores to SafeNet Authentication Manager, page 6
- Assigning Tokens in SafeNet Authentication Manager, page 6
- Configuring SafeNet Authentication Manager as an Identity Provider, page 7
- Exporting the SafeNet Authentication Manager Certificate, page 9
- Configuring SafeNet Authentication Manager for SAML-based User Federation, page 10

Synchronizing User Stores to SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) manages and maintains tokens information in its data store, including the tokens status 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

Assigning Tokens in SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) supports a number of token methods that can be used as a second authentication factor for users authenticating through Citrix NetScaler Gateway.

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*.

### Configuring SafeNet Authentication Manager as an Identity Provider

To use Citrix NetScaler Gateway as a service provider and SafeNet Authentication Manager (SAM) as an identity provider, SAM must be configured as an identity provider.

1. From the Windows **Start** menu, click **Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager**.

   ![Configuration Manager Screen](image)

   *(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*
2. Click the **Action** tab and then click **Cloud Configuration**.

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

3. On the **Info for Service Provider** tab, in the **Domain URL** field, enter the web address of the SAM portal server.

The remaining fields are generated according to the Domain URL that was entered.

4. Click **OK**.
Exporting the SafeNet Authentication Manager Certificate

SafeNet Authentication Manager’s certificate is shared between SAM and Citrix NetScaler Gateway. The certificate will be used to sign the authentication requests.

1. From the Windows Start menu, click Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager.

2. Click the Action tab, and then click Cloud Configuration.

3. On the Info for Service Provider tab, perform the following steps:
   a. Click Export Certificate and save the certificate file. The certificate file will be imported into Citrix NetScaler Gateway later.
b. Copy the values of the Sign-in page URL, Sign-out page URL, and Change password URL fields, and then save them in a text file. These URLs will be required while configuring Citrix NetScaler Gateway.

4. Click OK.

Configuring SafeNet Authentication Manager for SAML-based User Federation

SafeNet Authentication Manager’s Token Policy Object (TPO) policies include application authentication settings for SAML service providers. These settings are used by SAM’s portal to communicate with service providers.

For general portal configuration, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

To edit the TPO for SAM’s portal configuration:

1. Open the Token Policy Object Editor for the appropriate group. See the SafeNet Authentication Manager 8.2 Administrator’s Guide for more information.

2. In the left pane, click Protected Application Settings > User Authentication.

3. In the right pane, double-click Application Authentication Settings.
4. On the **Application Authentication Settings Properties** window, perform the following steps:
   a. Select **Define this policy setting**.
   b. Select **Enabled**.
   c. Click **Definitions**.

   ![Application Authentication Settings Properties](image)

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

5. On the **Application Authentication Settings** window, in the left pane, right-click **Application Authentication Settings**, and then select **Create a new profile**.

   ![Application Authentication Settings](image)

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

6. Right-click the new profile, and then rename it to a user-friendly name.
7. Click the new profile.

8. In the right pane, double-click on the following policies, and enter the appropriate information:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application issuer</td>
<td>Not Defined</td>
</tr>
<tr>
<td>SAM issuer</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Application’s login URL</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audience URL</td>
<td>Not Defined</td>
</tr>
<tr>
<td>User mapping</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Automatic Windows auth.</td>
<td>Not Defined</td>
</tr>
<tr>
<td>OTP auth.</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Certificate-based auth.</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Network password auth.</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Always require auth.</td>
<td>Not Defined</td>
</tr>
<tr>
<td>End SSO session on signout</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Context-based auth.</td>
<td>Not Defined</td>
</tr>
</tbody>
</table>


The following is an example of the completed policy settings in the Application Authentication Settings window:

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
10. Click OK until all of the Token Policy Object Editor windows are closed.

**Configuring Citrix NetScaler Gateway**

Adding SafeNet Authentication Manager (SAM) as an Identity Provider in Citrix NetScaler Gateway requires:

- Creating an Authentication Server, page 13
- Creating an Authentication Policy, page 15
- Assigning the SAML Policy to the NetScaler Virtual Server, page 17

**Creating an Authentication Server**

1. Login to the Citrix NetScaler administrator console.
2. On the Citrix NetScaler administrator console, on the Configuration tab, in the left pane, click **NetScaler Gateway > Policies > Authentication > SAML**.

*(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)*
3. In the right pane, on the **Servers** tab, click **Add**.

4. On the **Create Authentication SAML Server** window, perform the following steps:
   a. In the **Name** field, enter a name for the server (for example, **SAM SAML**).
   b. In the **IDP Certificate Name** field, click the **[ ]** icon.
   c. On the **Install Certificate** window, complete the following fields, and then click **Install**.

   ![Certificate installation screen](image)

   **Certificate-Key Pair Name**: Enter a name for the certificate.

   **Certificate File Name**: Click **Browse** to search for and select the SAM IDP certificate (refer to “Exporting the SafeNet Authentication Manager Certificate” on page 9).

   ![Certificate installation screen](image)

   **Redirect URL**: Enter the sign-in page URL (for example, [http://2008-SAM-Serv.samserver.com/samcloud/default.aspx](http://2008-SAM-Serv.samserver.com/samcloud/default.aspx)).
e. In the **Issuer Name** field, enter the NetScaler login page URL (for example, https://cag.safenetdemos.com).

f. Click **Create**.

![NetScaler VPS AWS BYOL](image)

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

### Creating an Authentication Policy

1. On the Citrix NetScaler administrator console, click the **Configuration** tab.

![NetScaler VPS AWS BYOL](image)

*(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)*
2. In the left pane, click **NetScaler Gateway > Policies > Authentication > SAML**.

   ![NetScaler Gateway Interface](image1.png)

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

3. Click **Add**.

4. On the **Create Authentication SAML Policy** window, complete the following fields, and then click **Create**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the policy</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>Select the server you previously created</td>
</tr>
<tr>
<td><strong>Expression</strong></td>
<td>Enter the logical expression you want to use (for example, <strong>ns_true</strong>).</td>
</tr>
</tbody>
</table>

   ![Create SAML Policy Interface](image2.png)

   *(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)*
Assigning the SAML Policy to the NetScaler Virtual Server

1. On the Citrix NetScaler administrator console, click the **Configuration** tab.

![Configuration Tab](image1)

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

2. In the left pane, click **NetScaler Gateway > Virtual Servers**.

![Virtual Servers](image2)

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

3. Select your virtual server (for example, cag), and then click **Edit**.
4. Under **Authentication**, select the SAML policy you created earlier.

5. Click **Done**.

6. Click **Save**.

---

### Running the Solution

1. In a web browser, open the Citrix NetScaler Access Gateway login page.
2. You will be redirected to the SAM IDP login page. Enter your username, and then click **OK**.

(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)
3. On the **OTP Authentication** window, in the **OTP Authentication Code** field, enter the OTP, and then click **OK**.

![OTP Authentication Window](image1.png)

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

After a successful authentication, you will be redirected to the Citrix Netscaler Access Gateway page.

![Citrix Netscaler Access Gateway](image2.png)

*(The screen image above is from Citrix®. 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</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 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 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 Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>