SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Citrix NetScaler Gateway
## Contents

- Third-Party Software Acknowledgement ................................................................. 4
- Description ............................................................................................................... 4
- Applicability ............................................................................................................ 4
- Environment ............................................................................................................. 4
- Audience .................................................................................................................. 5
- SAML Authentication using SafeNet Authentication Service Cloud ...................... 5
- SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE ................................................................. 5
- SAML Authentication Flow using SafeNet Authentication Service ......................... 6
- SAML Prerequisites .................................................................................................. 6
- Configuring Citrix NetScaler Gateway ...................................................................... 6
  - Creating Authentication Server .............................................................................. 7
  - Creating Authentication Policy ............................................................................. 9
  - Assigning the SAML Policy to the Netscaler Virtual Server .................................. 10
  - Download the SafeNet Identity Provider Certificate ............................................ 12
- Configuring SafeNet Authentication Service ........................................................... 12
  - Synchronizing Users Stores to SafeNet Authentication Service ......................... 12
  - Assigning an Authenticator in SafeNet Authentication Service .......................... 12
  - Adding Citrix NetScaler Gateway as a Service Provider (SP) in SafeNet Authentication Service ................................................................. 13
  - Enabling SAML Services in SafeNet Authentication Service ............................... 16
- Running the Solution ............................................................................................... 21
- Support Contacts ...................................................................................................... 22
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet 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 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.

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 one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in Citrix NetScaler Gateway using SafeNet Authentication Service 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 Service.

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 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**
- **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 Service (SAS).

SAML Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides a service for SAML authentication that is already implemented in the SAS Cloud environment and can be used without any installation.

SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service (SAS) comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.

- **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

For more information on how to install and configure the SafeNet Authentication Service Agent for Shibboleth, refer to the SafeNet Support Portal.
SAML Authentication Flow using SafeNet Authentication Service

SafeNet Authentication Service (SAS) 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.

1. A user attempts to log on to Citrix NetScaler Gateway. The user is redirected to SafeNet Authentication Service. SAS collects and evaluates the user’s credentials.
2. SAS returns a response to Citrix NetScaler Gateway, accepting or rejecting the user’s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Service (SAS) 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 Citrix NetScaler Gateway

Adding SafeNet Authentication Service (SAS) as an Identity Provider in Citrix NetScaler Gateway requires:

- Creating Authentication Server, page 7
- Creating Authentication Policy, page 9
- Assigning the SAML Policy to the Netscaler Virtual Server, page 12
- Download the SafeNet Identity Provider Certificate, page 12
Creating Authentication Server

1. Log in 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.

3. 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, SAS 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**.

<table>
<thead>
<tr>
<th>Certificate-key Pair Name</th>
<th>Enter a name for the certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate File Name</strong></td>
<td>Click <strong>Browse</strong> to search for and select the SAS IDP certificate (refer to “Download the SafeNet Identity Provider Certificate” on page 12).</td>
</tr>
</tbody>
</table>

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

d. In the **Redirect URL** field, enter the Identity Provider HTTP-POST login URL (for example, `https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO`).

e. In the **Issuer Name** field, enter the NetScaler login page url (for example, `https://cag.safenetdemos.com`).

f. Click **Create**.

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

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

   ![Image of Citrix NetScaler administrator console](image1.png)

   *(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**.

   ![Image of Citrix NetScaler Policy Editor](image2.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, <code>ns_true</code>).</td>
</tr>
</tbody>
</table>

(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.

(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.**

![NetScaler Gateway Virtual Servers](image)

(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.

![NetScaler Gateway virtual server settings](image)

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

5. Click **Done.**

6. Click **Save.**
Download the SafeNet Identity Provider Certificate

Browse to the https://cloud.safenet-inc.com/console/cert/idp.crt URL. The SafeNet identity provider certificate will be automatically downloaded. Save it locally on your machine.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Citrix NetScaler Gateway using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 12
- Assigning an Authenticator in SafeNet Authentication Service, page 12
- Adding Citrix NetScaler Gateway as a Service Provider (SP) in SafeNet Authentication Service, page 13
- Enabling SAML Services in SafeNet Authentication Service, page 16

Synchronizing Users Stores to 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 further 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 authenticating through Citrix NetScaler Gateway.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
• MP-1 software token
• GrIDsure
• 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” 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 Citrix NetScaler Gateway as a Service Provider (SP) in SafeNet Authentication Service

Add a service provider entry in the SafeNet Authentication Service (SAS) **SAML Service Providers** module to prepare it to receive SAML authentication requests from Citrix NetScaler Gateway. You will need the Issuer ID and assertion consumer URL location of Citrix NetScaler Gateway.

**To add Citrix NetScaler Gateway as a Service Provider in SafeNet Authentication Service:**

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

![SafeNet Authentication Service console screenshot](image)
2. Click the **COMMS** tab, and then click **SAML Service Providers**.

3. In the **SAML Service Providers** module, click the **SAML 2.0 Settings** link.

4. Click **Add**.

   ![SAML Service Providers Module](image)

   **SAML Service Providers Module**

   - **Task**: SAML 2.0 Settings
   - **Description**: Create and configure SafeNet Authentication Service SAML Settings.

   **SAML 2.0 Settings**

   - **Entity ID**: https://idp1.cryptoaid.com/idp/whidbalek
   - **Identity Provider Authentication Provider**: https://idp1.cryptoaid.com/idp/profile/SAML2/POST/SSO
   - **Identity Provider HTTP-POST SimpleSign Provider**: https://idp1.cryptoaid.com/idp/profile/SAML2/POST-SimpleSign/SSO
   - **Identity Provider HTTP-Redirect Provider**: https://idp1.cryptoaid.com/idp/profile/SAML2/Redirect/SSO
   - **Identity Provider Logout Provider**: https://idp1.cryptoaid.com/idp/security.jsp
   - **Download URL for Identity Provider Certificate**: https://idp1.safenet.com/compute/sid/sid.crt
5. Under **Add SAML 2.0 Settings**, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Friendly Name</strong></td>
<td>Enter the Citrix NetScaler Gateway name.</td>
</tr>
<tr>
<td><strong>SAML 2.0 Metadata</strong></td>
<td>Select <strong>Create New Metadata File</strong>.</td>
</tr>
<tr>
<td><strong>Entity ID</strong></td>
<td>Enter the Service Provider IssuerID/EntityID (for example, <a href="https://cag.safenetdemos.com">https://cag.safenetdemos.com</a>).</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Enter the Assertion Consumer URL (for example, <a href="https://cag.safenetdemos.com/cgi/samlauth">https://cag.safenetdemos.com/cgi/samlauth</a>).</td>
</tr>
</tbody>
</table>

![Add SAML 2.0 Settings](image)

**NOTE:** The remaining options are used to customize the appearance of the logon page presented to the user. For more information on logon page customization, refer “Configure SAML Service” in the **SAML Configuration Guide**: http://www2.safenet-inc.com/sas/implementation-guides/sas-on-prem/SAS-QS-SAML.pdf

Under **Return Attributes**, add the following attributes, and then click **Apply**:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/EmailAddress">http://schemas.xmlsoap.org/claims/EmailAddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
</tbody>
</table>
Citrix NetScaler Gateway is added as a service provider in the system.

Enabling SAML Services in SafeNet Authentication Service

After Citrix NetScaler Gateway has been added to SafeNet Authentication Service (SAS) as a service provider, the users should be granted permission to use this service provider with SAML authentication.

There are two methods to enable the user to use the service provider:

Enabling SAML Services in SafeNet Authentication Service

After Citrix NetScaler Gateway has been added to SafeNet Authentication Service (SAS) as a service provider, the users should be granted permission to use this service provider with SAML authentication.

There are two methods to enable the user to use the service provider:
- Manually, one user at a time, using SAML Services module
- Automatically, by defining groups of users, using SAML Provisioning Rules

**Using the SAML Services Module**

Manually enable a single user to authenticate against one or more configured SAML Service providers.

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

2. Click the **ASSIGNMENT** tab, and then search for the required user.

3. Click the appropriate user in the **User ID** column.
4. Click **SAML Services**.

![Image of SAML Services](image)

5. Click **Add**.

![Image of Add SAML Service](image)

6. Under **Add SAML Service**, do the following:
   a. From the **Service** menu, select the Citrix NetScaler Gateway service provider.
   b. In **SAML Login ID** field, select the type of login ID (User ID, E-mail, or Custom) to be sent as a UserID to Citrix NetScaler Gateway in the response.
   c. Click **Add**.
The user can now authenticate to Citrix NetScaler Gateway using SAML authentication.

Using SAML Provisioning Rules

Use this module to enable groups of users to authenticate to SAML service providers.

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

2. Click the POLICY tab, and then click Automation Policies.
3. Click the SAML Provisioning Rules link.

![Image of SAML Provisioning Rules](image)


5. Configure the following fields, and then click Add:

   - **Rule Name**: Enter a name for the rule.
   - **User is in container**: Users affected by this rule must be in the selected container.
   - **Groups**: The Virtual Server groups box lists all groups. Click the user groups that will be affected by the rule, and then click the right arrow to move it to the Used by rule box.
   - **Parties**: The Relying Parties box lists all service providers. Click the service providers that the groups of users will authenticate to, and then click the right arrow to move it to Rule Parties box.
   - **SAML Login ID**: Select User ID. The User ID will be returned to the service provider in the SAML assertion.
Running the Solution

1. In a web browser, open the Citrix NetScaler Access Gateway login page.
2. You will be redirected to the SAS IDP login page. Enter your username and token passcode.

3. After a successful authentication, you will be redirected to access Citrix StoreFront.

(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</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></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>