SafeNet Authentication Service
Integration Guide

Using SAS SAML-based Authentication with Citrix NetScaler Gateway 10.1
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012548-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>April 2014</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Overview</td>
<td>4</td>
</tr>
<tr>
<td>Audience</td>
<td>4</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>5</td>
</tr>
<tr>
<td>Security Assertion Markup Language</td>
<td>5</td>
</tr>
<tr>
<td>SAML Authentication Flow</td>
<td>5</td>
</tr>
<tr>
<td>Authentication using SAS-SPE and SAS-PCE</td>
<td>6</td>
</tr>
<tr>
<td>Configuring Citrix NetScaler Gateway as a Service Provider</td>
<td>6</td>
</tr>
<tr>
<td>Viewing SAS SAML Settings</td>
<td>6</td>
</tr>
<tr>
<td>Creating a SAML Authentication Policy</td>
<td>7</td>
</tr>
<tr>
<td>Attaching the SAML Policy to the NetScaler Virtual Server</td>
<td>11</td>
</tr>
<tr>
<td>SAML Authentication Configuration in SAS</td>
<td>12</td>
</tr>
<tr>
<td>Configuring the SAML Service Provider</td>
<td>12</td>
</tr>
<tr>
<td>Configuring SAML Services</td>
<td>14</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>18</td>
</tr>
<tr>
<td>User Authentication Scenario</td>
<td>18</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>19</td>
</tr>
</tbody>
</table>
Introduction

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 the 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.

Overview

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 choices, and integration APIs.

Citrix NetScaler Gateway is a secure application and data access solution that gives IT administrators a single point for managing access control and limiting 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 provides guidance for deploying the SAML authentication option in Citrix NetScaler Gateway 10.1, and describes how to set up NetScaler to work with SafeNet Authentication Service using SAML authentication.

Audience

This document is targeted to system administrators who are familiar with Citrix NetScaler 10.1 Gateway and are interested in adding SAML Authentication capabilities using SafeNet Authentication Service.

Prerequisites

This document assumes that Citrix NetScaler Gateway 10.1 is deployed in the organization. It will guide you through the process of adding SAML authentication capabilities to Citrix NetScaler Gateway by using SafeNet Authentication Service.

The deployment of SAML Authentication support using SafeNet Authentication Service with Citrix NetScaler Gateway requires these major steps:

- Synchronize Citrix NetScaler Gateway user store with SafeNet Authentication Service user store
- Assign authenticators to users
- Test the authentication solutions

NOTE: This document assumes that the Citrix NetScaler Gateway 10.1 VPX environment is already configured and working with static passwords prior to implementing multi-factor-authentication using SafeNet Authentication Service.
Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet's cloud-based delivered 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.

**NOTE:** For the purpose of this guide, Citrix NetScaler Gateway 10.1 was tested in a Citrix NetScaler VPX configuration based on virtual appliance deployment. The server version of Citrix NetScaler Gateway 10.1 should work by using the same process.

Security Assertion Markup Language

Security Assertion Markup Language (SAML) 2.0 is a standard for exchanging authentication and authorization data between security domains. SAML 2.0 is an XML-based protocol that uses security tokens (information packets) containing assertions to pass information about a principal (usually an end user) between an identity provider (IdP) and a web service. SAML 2.0 enables web-based scenarios, including single sign-on (SSO) authentication.

SAML 2.0 is supported by Citrix NetScaler Gateway 10.1. In this SAML scenario, Citrix NetScaler Gateway 10.1 is the service provider, and SafeNet Authentication Service (SAS) is the identity provider. Citrix NetScaler Gateway 10.1 implements the authentication result determined by SAS.

SAML Authentication Flow

Secure access to Citrix NetScaler Gateway using SafeNet Authentication Service with SAML occurs as follows:
Authentication using SAS-SPE and SAS-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service 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 SafeNet Authentication Service 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 SafeNet Authentication Service in their private cloud environment.

For both on-premises versions, SafeNet Authentication Service can be integrated with Microsoft Network Policy Server (MS-NPS) or with the legacy Microsoft Internet Authentication Service (MS-IAS). Both solutions serve as local RADIUS servers. SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SafeNet NPS Agent.

For more information on how to install and configure SafeNet Agent for NPS, refer to the *SafeNet Authentication Service Agent Configuration Guide for Microsoft IAS and NPS*.

Configuring Citrix NetScaler Gateway as a Service Provider

Viewing SAS SAML Settings

Display the SAS data that will be needed for Citrix NetScaler Gateway configuration when creating an authentication SAML policy.

To access the SAS SAML settings required for Citrix NetScaler Gateway configuration:

1. In the SAS console, click **Virtual Server**, and then click the **COMMS** tab.
2. Under **SAML Service Providers**, click the **SAML 2.0 Settings** link. The following is an example of these settings.

![SAML Service Providers settings](image)

Creating a SAML Authentication Policy

Use the SAS SAML settings to configure Citrix NetScaler Gateway as a SAS SAML service provider.

To create an authentication server:

1. In the Citrix NetScaler Gateway administrator’s console, in the left pane, click **NetScaler Gateway > Policies > Authentication > SAML**.

![Citrix NetScaler Gateway configuration](image)

*(The screen image above is from Citrix® software. Trademarks are the property of their respective owners.)*
2. On the Policies tab, click Add.

3. On the Create Authentication Policy window, in the Name field, enter a name for the new policy.

4. Click the New button to the right of the Server field.

5. On the Create Authentication Server window, next to the IDP Certificate Name field, click the Install button.

(The screen image above is from Citrix® software. Trademarks are the property of their respective owners.)
6. Complete the **Install Certificate** window as follows:

<table>
<thead>
<tr>
<th>Certificate-Key Pair Name</th>
<th>Enter a name for the certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate File Name</td>
<td>Click the <strong>Browse</strong> button to locate and select the SAS IDP certificate that can be found in the SAS SAML Settings (see “Viewing SAS SAML Settings” on page 66). Click <strong>Install</strong> to install the certificate.</td>
</tr>
</tbody>
</table>

7. On the **Create Authentication Server** window, in the **Redirect URL** field, enter the Identity Provider HTTP-POST login URL from the SAS SAML 2.0 dashboard (see “Viewing SAS SAML Settings” on page 66).

8. In the **SAML Issuer Name** field, enter the NetScaler login URL.

9. Click **OK** to add the server to the policy. You are returned to the **Create Authentication Policy** window.
10. Under **Expression**, do the following:
   a. From the **Named Expression** list, select **General**.
   b. From the adjacent list, select **True Value**.
   c. Click **Add Expression**. The **ns_root** value will be added to **Expression** box.

   ![Configuration screen](image.png)

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

11. Click **OK**.
Attaching the SAML Policy to the NetScaler Virtual Server

1. In the Citrix NetScaler Gateway administrator console, click **NetScaler Gateway > Virtual Servers**.

2. Double-click the virtual server, and then click the **Authentication** tab.

3. On the **Primary** policy tab, click **Insert Policy**, and then select the SAML policy you created in the previous section.
SAML Authentication Configuration in SAS

The following steps are used to configure SAML authentication in SAS:

- “Configuring the SAML Service Provider” – see below
- “Configuring SAML Services” - page 14

Configuring the SAML Service Provider

Configure the virtual server to process authentication requests received from a specific SAML service provider.

To configure the virtual server:

1. In the SAS console, click Virtual Server, and then click the COMMS tab.

2. Under SAML Service Providers, click SAML 2.0 Settings. The SAML 2.0 settings are displayed.
3. Click **Add** to add a new service provider. Complete the **Add SAML 2.0 Setting** window as follows:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Enter a name for the NetScaler service provider. You will need this value when configuring SAML services.</th>
</tr>
</thead>
</table>
| SAML 2.0 Metadata | Select **Create New Metadata File**.  
- **Entity ID**: Enter the NetScaler login URL (for example, https://cag.safenetdemos.com).  
- **Location**: Enter the location of the metadata file, which is the Entity ID URL plus /cgi/samlauth (for example, https://cag.safenetdemos.com/cgi/samlauth). |

4. Click **Apply**. The new service provider is added to the **Entity ID** list.
Configuring SAML Services

Enable or disable SAML authentication services for individual users or user groups. SAML services are enabled and disabled using either of the following methods:

- “Manually Enabling User Authentication” – see below
- “Using SAML Provisioning Rules to Enable User Authentication” – page 15

Manually Enabling User Authentication

Enable an individual user to authenticate against the NetScaler service provider.

To manually enable authentication for a user:

1. In the SAS console, click Virtual Server, and then click the ASSIGNMENT tab.
2. Complete the search fields to locate the user for whom you want to enable SAML authentication, and then click Search. When located, click the User ID. The user options are displayed.
3. Click SAML Services. The SAML Services options are displayed.
4. Click **Add**.

5. On the **Add SAML Service** window:
   a. Click the **Service** list, and then select the NetScaler service provider.
   b. In the **SAML Login ID** field, select **User ID**.
   c. Click **Add**. The service name is added as the user’s SAML service provider.

### Using SAML Provisioning Rules to Enable User Authentication

Use SAML provisioning rules to automatically enable or disable user authentication to SAML service providers. The provisioning rules can be used instead of or in addition to manual authentication configuration.

To set SAML provisioning rules for users:

1. In the SAS console, click **Virtual Server**, and then click the **POLICY** tab.
2. Click **Automation Policies > SAML Provisioning Rules**.

3. Click **New Rule**.
4. Complete the **SAML Provisioning Rules** window as follows.

<table>
<thead>
<tr>
<th><strong>Rule Name</strong></th>
<th>Enter a name for the new rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Groups</strong></td>
<td>In the Virtual Server groups list, click the group to be authenticated against NetScaler, and then click the right arrow to move the group to the Used by rule list.</td>
</tr>
<tr>
<td><strong>Parties</strong></td>
<td>In the Relying Parties list, click the NetScaler service provider, and then click the right arrow to move the service provider to the Rule Parties list.</td>
</tr>
<tr>
<td><strong>SAML Login ID</strong></td>
<td>Select User ID.</td>
</tr>
</tbody>
</table>

5. Click **Add**. The new rule is displayed under **SAML Provisioning Rules**.
Running the Solution

User Authentication Scenario

In this example, a user named Walter authenticates to NetScaler using his enrolled password.

1. Walter opens a web browser and goes to the NetScaler site (in this example, https://cag.safenetdemos.com).
2. NetScaler redirects the authentication request to the SAS authentication portal. The authentication portal’s Login window is displayed.

3. Walter enters his user name and password, and then clicks Login.
4. After successful authentication, Walter is redirected to the Citrix Web Interface.

(The screen image above is from Citrix® 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 SafeNet Customer Support. SafeNet 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 SafeNet 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 1: Support Contacts

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>SafeNet, Inc.</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></td>
</tr>
<tr>
<td>United States</td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>