SafeNet Authentication Manager
Integration Guide

Using SAM SAML-based Authentication with Citrix NetScaler Gateway 10.1
## Contents

- **Introduction** ................................................................. 4
- **Third-Party Software Acknowledgement** ........................................ 4
- **Overview** ........................................................................... 4
- **Audience** ........................................................................ 4
- **Prerequisites** ...................................................................... 4
- **Applicability** ...................................................................... 5
- **Security Assertion Markup Language** ........................................... 5
- **SAML Authentication Flow** ....................................................... 5
- **SAML Authentication Configuration in SAM** ................................... 6
  - Configuring SAM as an Identity Provider ........................................ 6
  - Configuring SAM for SAML-based User Federation ............................ 7
- **Configuring Citrix NetScaler Gateway as a Service Provider** .................. 10
  - Creating a SAML Authentication Policy ......................................... 10
  - Attaching the SAML Policy to the NetScaler Virtual Server .................. 13
- **Running the Solution** ............................................................ 13
  - User Authentication Scenario ................................................... 13
- **Support Contacts** .................................................................. 15
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 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 Manager (SAM) enables complete user authenticator lifecycle management. SAM links tokens with users, organizational rules, and security applications to enable streamlined handling of users’ needs throughout the various user authenticator lifecycle stages.

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 Manager 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 Manager.

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 Manager.

The deployment of SAML authentication support using SafeNet Authentication Manager with Citrix NetScaler Gateway requires these prerequisite steps:

- Synchronize the Citrix NetScaler Gateway user store with the SafeNet Authentication Manager 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 Manager.
Applicability

The information in this document applies to SafeNet Authentication Manager (SAM) 8.2.

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 Manager (SAM) is the identity provider. Citrix NetScaler Gateway 10.1 implements the authentication result determined by SAM.

SAML Authentication Flow

Secure access to Citrix NetScaler Gateway using SafeNet Authentication Service with SAML occurs as follows:

1. Bob, a user, wants to log in to Citrix NetScaler 10.1. Bob leverages the single sign-on capabilities embedded in the organization’s SafeNet Authentication Manager (SAM) solution.
2. SafeNet Authentication Manager’s external portal collects Bob’s credentials and passes them to SafeNet Authentication Manager for authentication. SAM evaluates Bob’s credentials and returns an “accept” or “reject” response to the external portal.
3. The portal uses SAM’s response to return an “accept” or “error” assertion to Citrix NetScaler 10.1.
SAML Authentication Configuration in SAM

Configuring SAM as an Identity Provider

The SAM Configuration Manager and TPO settings are used for setting SafeNet Authentication Manager (SAM) as the Citrix NetScaler identity provider.

To configure SAM as an identity provider:

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

2. On the Configuration Manager page, click Action > Cloud Configuration.

3. On the Cloud Settings page, click the Info for Service Provider tab. In the Domain URL field, enter the URL of your organization’s external SAM portal. The Single Sign-On fields will be filled in automatically.

   ![Cloud Settings](image)

   Do not close the Cloud Settings window. You will return here later during NetScaler SAML policy configuration.

4. Click Export Certificate and save the certificate file. This file will be needed later for NetScaler SAML policy configuration.
Configuring SAM for SAML-based User Federation

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

**NOTE:** See the *SafeNet Authentication Manager Version 8.2 Administrator’s Guide* for general portal configuration.

To edit the TPO policies for SAM’s portal configuration:

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

2. In the left pane, expand **Protected Application Settings** and then click **User Authentication**. The property’s policies are displayed in the right pane.

3. In the right pane, double-click **Application Authentication Settings**.

4. On the **Application Authentication Settings Properties** page, on the **User Authentication** tab, select the **Define this policy setting** check box and then select **Enabled**.
5. Click the **Definitions** button.

6. On the **Application Authentication Settings** page, in the left pane, right-click **Application Authentication Settings** and select **Create a new profile**. A new profile is created.
   a. In the left pane, right-click the new profile and select **Rename**.
   b. Rename the profile to **CAG**.

7. In the left pane, double-click the new profile named **CAG**. The profile’s policies are displayed in the right pane.
8. In the right pane, double-click the following policies, and enter the appropriate information:

- **Application Issuer**: Enter the NetScaler Issuer/Entity ID. The value should be the NetScaler virtual server URL (for example, https://<NetScaler virtual server>.com).

- **SAM issuer**: Type a unique SAM issuer ID (for example, SAM).

- **Application’s login URL**: Type https://<NetScaler virtual server>/csg/samlauth.

9. Enable the appropriate authentication methods for your organization. See the *SafeNet Authentication Manager Version 8.2 Administrator’s Guide* for additional information.

The following is an example of completed fields in the **Application Authentication Settings** window:

![Application Authentication Settings](image)

10. Click **OK** until all of the TPO Editor pages are closed.
Configuring Citrix NetScaler Gateway as a Service Provider

Creating a SAML Authentication Policy

Use the SAM SAML settings to configure Citrix NetScaler Gateway as a SAM 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**.

2. On the **Policies** tab, click **Add**.

3. On the **Create Authentication Policy** dialog box, in the **Name** box, type a name for the new policy.

(The screen image above is from Citrix® software. Trademarks are the property of their respective owners.)
4. Click the **New** button to the right of the **Server** field.

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

![Create Authentication Server dialog box](image)

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

6. Complete the **Install Certificate** dialog box as follows:

<table>
<thead>
<tr>
<th>Certificate-Key Pair Name</th>
<th>Type 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 SAM IDP certificate that was exported in previous section (see “Configuring SAM as an Identity Provider”, section 5). Click <strong>Install</strong> to install the certificate.</td>
</tr>
</tbody>
</table>

![Install Certificate dialog box](image)

(The screen image above is from Citrix® software. Trademarks are the property of their respective owners.)
7. On the Create Authentication Server dialog box, in the Redirect URL field, enter the sign-in page URL (see “Configuring SAM as an Identity Provider” on page 6).

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 dialog box.

10. In the Expression section, 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.

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.

![NetScaler Gateway Virtual Server Configuration](image)

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

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

Running the Solution

User Authentication Scenario

In this example, a user named Bob authenticates to NetScaler using a messaging token.

1. Bob opens a web browser and goes to the NetScaler site (for example, https://cag.safenetdemos.com).
2. NetScaler redirects the authentication request to the SAM authentication portal. The authentication portal’s **Login** page is displayed.

![SAM Authentication Portal](image)
3. Bob enters his user name and then clicks OK. The **OTP Authentication** page is displayed.

![OTP Authentication Page](image)

4. In this example, an SMS with the OTP passcode (688074) was sent to Bob’s mobile phone.

![SMS with OTP Passcode](image)

5. Bob types the passcode in the **OTP Authentication Code** field on the **OTP Authentication** page and then clicks OK.

6. After successful authentication, Bob is redirected to the Citrix Web Interface.

![Citrix Web Interface](image)

*(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>Address</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>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>Email</td>
<td><a href="mailto:support@safenet-inc.com">support@safenet-inc.com</a></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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>