SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for CA SiteMinder
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.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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:** 007-012793-001, Rev. B

**Release Date:** June 2016
## 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-PCE5
SAML Authentication Flow using SafeNet Authentication Service ................................................................. 6
SAML Prerequisites ............................................................................................................................................. 6
Configuring CA SiteMinder .................................................................................................................................. 6
Configuring SafeNet Authentication Service ..................................................................................................... 66
    Synchronizing Users Stores to SafeNet Authentication Service ................................................................. 66
    Assigning an Authenticator in SafeNet Authentication Service ............................................................... 67
    Adding CA SiteMinder as a Service Provider (SP) in SafeNet Authentication Service ......................... 67
    Enabling SAML Services in SafeNet Authentication Service ................................................................. 71
Running the Solution ........................................................................................................................................ 76
Support Contacts ............................................................................................................................................... 77
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as CA SiteMinder.

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 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.

CA SiteMinder solution is a web access management system that provides secure single sign-on and flexible access management to applications and web services either on-premises, in the cloud, from a mobile device, or at a partner’s site.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in CA SiteMinder using SafeNet OTP authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in CA SiteMinder using SafeNet Authentication Service as an identity provider.

It is assumed that the CA SiteMinder environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

CA SiteMinder 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 – Private Cloud Edition (SAS-PCE)** — Mention only if SAS-PCE is relevant. Add version number to the SAS-PCE.
- **CA SiteMinder** version 12.5.1
Audience

This document is targeted to system administrators who are familiar with CA SiteMinder, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

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 Protocol

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 CA SiteMinder.

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

SAML Prerequisites

To enable SafeNet Authentication Service (SAS) to receive SAML authentication requests from CA SiteMinder, ensure that the end users can authenticate from the CA SiteMinder environment with a static password.

Configuring CA SiteMinder

To configure SAML Federation authentication in the CA SiteMinder Policy Server, perform the following steps:

1. Configuring and Installing the Web Agent Option Pack
2. Installing the Servletexec extension
3. Configuring the ServletExec Extension
4. Configuring a Trust Certificate
5. Creating a Local Service Provider
6. Creating a Remote Identity Provider
7. Creating a Partnership
8. Creating an Authentication Scheme
9. Configuring a SAML Protected Realm
10. Creating a Domain Policy
Configuring and Installing the Web Agent Option Pack

To configure and work with SAML authentication (SP-initiated), the Web Agent Option pack must be installed on the IIS server hosting the protected website. The Policy Server Option Pack and the Web Agent Option Pack are stand-alone products. The Policy Server Option Pack is installed on the same system you install the SiteMinder Policy Server and includes (among others) the Federation Security Services, which enables the exchange of user identity information in a secure fashion. This exchange enables single sign-on across partner websites in multiple domains.

To install the Web Agent Option pack:

1. Run the installation of the Web Agent Option Pack as administrator.
2. In the Introduction page, click Next.
3. Read the terms of license agreement and select I accept the terms of the License Agreement. Click Next.

4. In the **Choose Java Virtual Machine** window, select `jdk\jre\java.exe` and click **Next**.

   **NOTE:** Java JDK package must be installed.
5. Click **Install** to start the installation process.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
6. When the **Install Complete** window appears, select **Yes, restart my system** and then click **Done**.

![Install Complete window](image)

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

7. After the machine restarts, browse to `<web agent installation directory>\affwebservices\web-inf\classes`:

   a. Edit the **Affwebservices.properties** file: set the **AgentConfigLocation** so it points to the location of the webagent.conf file (for example, `AgentConfigLocation=C:\CA\webagent\win64\bin\iis\webagent.conf`).

   ```
   //tunnel library type. valid values are 'c' and 'java'
   NotificationLibraryType=java
   //NotificationLibraryType=c
   //In case of java tunnel library provide the fully qualified classname of the provider. Else
   //Library name followed by a space and then the function name
   NotificationLibraryDetails=com.netegrity.affiliateminder.webservices.NotificationEventAdapter
   //NotificationLibraryDetails=libName funName
   //SiteMinder server that will process the request at the time of the tunnel call.
   // Valid values are:
   // 0 - for the authorization server port number.
   // 1 - for the authentication server port number.
   // 2 - for the accounting server port number.
   SMserverPort=0
   //In case of 4.x IIS web agent, please leave its value empty. Else provide the full path
   //of the WebAgent.conf file.
   //AgentConfigLocation=D:\netscape\server4\https-webserv1\config\WebAgent.conf
   AgentConfigLocation=C:\CA\webagent\win64\bin\IIS\WebAgent.conf
   ```
b. Edit the **LoggerConfig.properties** file: set **TracingOn=Y**

```java
// Log and trace configuration parameters for com.netegrity.affiliateminder.webservices

// LoggingOn can be Y, N
LoggingOn=Y

// If LogFileName is set Log output will go to the file named
LogFileName=C:\CA\webagent\win64\log\affwebserv.log

// LogLocalTime can be Y, N. Y will log timestamps in local time rather than GMT.
LogLocalTime=Y

// TraceRollover defines the type of rollover functionality desired for trace output files.
// Please choose from the following valid values:
// 0  - [default]. No rollover is performed. Existing files are overwritten at startup.
// 2  - Rollover now. Rollover is only performed at startup..
// 1  - Append. No rollover is performed. Existing files are appended to at startup.
// 3  - Rollover. Files rollover when they grow to the limit set by LogSize.
// 4  - Rollover now with size. Files rollover at startup and then grow to the limit set by LogSize.
LogRollover=4

// LogSize dictates the maximum file size in megabytes when rolling over by size
LogSize=10

// LogCount defines how many log output files to leave around when rollover is enabled.
LogCount=10

// TracingOn can be Y, N
**TracingOn=Y**

// EnableDNSLookUp can be Y, N
EnableDNSLookUp=Y

...```
Installing the Servletexec extension

To enable authentication with SAML, the Servletexec extension must be installed on SiteMinder, making Federation Configuration available.

1. Copy the ServletExec installation file (Servletexec_AS_60a.exe) from the Policy Server installation files (under thirdparty-tools\servletexec folder) to a local folder.

2. Start the installation of the Servletexec extension under the Servletexec-6.0\win32 directory, with administrator privileges.

3. Click Next.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
4. Select **Install a Servletexec AS instance** and then click Next.

5. Read the **License Agreement** screen, and then click **Yes**.
6. Click **Next**.

7. To keep the displayed destination folder, click **Next**. To change the destination folder, first click **Browse** and then browse to the required location.
8. Enter a name for the instance and click **Next**.

9. Select **Microsoft IIS** and then click **Next**.

(The screen image above is from New Atlanta. Trademarks are the property of their respective owners.)
10. Set the location of the virtual directory (by default it is automatically created by the installation), and then click **Next**.

![Image of the ServletExec 6.0 Application Server Setup screen](image.png)

*The screen image above is from New Atlanta. Trademarks are the property of their respective owners.*
11. Enter the port on which the instance will be running and then click **Next**.

![ServletExec 6.0 Application Server Setup](image1)

*The screen image above is from New Atlanta. Trademarks are the property of their respective owners.*

12. Click **Next**.

![ServletExec 6.0 Application Server Setup](image2)

*The screen image above is from New Atlanta. Trademarks are the property of their respective owners.*
13. Enter a username, password and a password confirmation for the ServletExec administrator, and then click **Next**.

14. Click **OK** on the message window to start the installation process.
15. Clear the **Display the README file** option and then click **Finish**.

*The screen image above is from New Atlanta. Trademarks are the property of their respective owners.*
Configuring the ServletExec Extension

To update the ServletExec extension to the most updated version, some dll files need to be replaced with newer versions:

1. Browse to `C:\Program Files\New Atlanta\ServletExec AS\se-iis\`
   a. Edit the `StopServletExec.bat` file and make sure that first sePort value is set to the port you selected during the installation process.
   b. Edit the `StartServletExec.bat` file and make sure that first sePort value is set to the port you selected during the installation process.

2. Run the command line as an administrator and execute the `StopServletExec.bat` file (from the `<ServletExec extension folder>\se-iis` folder).

3. Make sure that `StopServletExec` has been stopped message appears.

4. Replace the `C:\Program Files\New Atlanta\ServletExec AS\installerFiles\StopServletExec.class` file with the file under `Servletexec-6.0.0.2_39\win32` directory.

5. Rename the `C:\Program Files\New Atlanta\ServletExec AS\bin\isapi\ServletExec_Adapter.dll` file to `ServletExec_Adapter.bak` then copy the `ServletExec_Adapter.dll.IIS_32bit` file to the same location and rename it `ServletExec_Adapter.dll`.

6. Rename the `C:\Program Files\New Atlanta\ServletExec AS\bin\isapi\ServletExec_Adapter64.dll` file to `ServletExec_Adapter64.bak`. Then copy the `ServletExec_Adapter.dll.IIS_64bit` file to the same location and rename it `ServletExec_Adapter64.dll`.

7. Rename the `C:\Program Files\New Atlanta\ServletExec AS\bin\apache\ApacheModuleServletExec.dll` file to `ApacheModuleServletExec.bak`. Then copy the `ApacheModuleServletExec.dll.APACHE2.0.x` file to same location and rename it `ApacheModuleServletExec.dll`.

8. Rename the `C:\Program Files\New Atlanta\ServletExec AS\bin\apache\ApacheModuleServletExec_2.2.x.dll` file to `ApacheModuleServletExec_2.2.x.bak`. Then copy the `ApacheModuleServletExec.dll.APACHE2.2.x` file to same location and rename it `ApacheModuleServletExec_2.2.x.dll`.

9. Run the command line as an administrator and execute the `StartServletExec.bat` file (from the `C:\Program Files\New Atlanta\ServletExec AS\se-iis` folder).
Make sure that the **ServletExec 6.0 initialized in [x] seconds** message appears.

10. **Log in to ServletExec by browsing to** http://localhost/servletexec/admin. **Fill in the Username and Password** and then click Login.

![ServletExec login screen](image)

*(The screen image above is from New Atlanta. Trademarks are the property of their respective owners.)*
11. In the left pane, under **Web Application** click **Manage** and then, in the right pane, click **Add a web application**.

![Manage Web Applications](image1)

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

12. Complete the following and then click **Submit**:

<table>
<thead>
<tr>
<th>Application Name</th>
<th>servletexec</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Context path</td>
<td>/servletexec/</td>
</tr>
<tr>
<td>Location</td>
<td>Click <strong>Browse</strong> and choose <strong>C:\CA\webagent\win64\affwebservices</strong></td>
</tr>
</tbody>
</table>

![Add a Web Application](image2)

(The screen image above is from New Atlanta. Trademarks are the property of their respective owners.)
13. Restart the server to apply all the new configurations.
Configuring a Trust Certificate

In this section, a certificate will be imported to the CA SiteMinder Policy Server and configured as a Trusted Certificate, in order to sign the SAML communication.

1. **Log in to the SiteMinder Administrative UI window:**

![SiteMinder Administrative UI](image)

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

2. **Click on the Infrastructure tab.**

3. **Click the X509 Certificate Management tab.**

![SiteMinder X509 Certificate Management](image)

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
4. In the left pane, click Trusted Certificates and Private Keys.

![Image of SiteMinder Administrative UI with Trusted Certificates and Private Keys](https://example.com/image.png)

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

5. Click Import New to import a new certificate to the SiteMinder server.

![Image of SiteMinder Administrative UI showing Import New certificate](https://example.com/image.png)

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


![Image of SiteMinder Administrative UI showing Certificate Import](https://example.com/image.png)

*(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)*
7. Verify that the entry is correct and then click Next.

8. Click Finish.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
Creating a Local Service Provider

In this section, CA SiteMinder Policy Server will be configured as a Service Provider in order to enable SAML authentication to a secure website.

1. Log in to the SiteMinder Administrative UI window.

2. Click the Federation tab.

3. In the left pane, under Partnership Federation, click Entities.
4. Click **Create Entity**.

![Screen Image](image1.png)

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

5. Select **Entity Location** as **Local** and **New Entity Type** as **SAML2 SP**. Click **Next**.

![Screen Image](image2.png)

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
6. Enter the fields as follows and then click **Next**:

<table>
<thead>
<tr>
<th><strong>Entity ID</strong></th>
<th>Enter an Entity ID that will identify SiteMinder in the SAML authentication (f.e. <code>&lt;WebAgent public hostname&gt;</code>)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entity Name</strong></td>
<td>Enter an Entity Name that will identify the SP in SiteMinder GUI (f.e. <code>&lt;WebAgent public hostname&gt;</code>)</td>
</tr>
<tr>
<td><strong>Base URL</strong></td>
<td>Enter the host name of the web agent server which is visible and resolvable by the SP’s DNS service (f.e. http://&lt;WebAgent public hostname&gt;)</td>
</tr>
<tr>
<td><strong>Supported Name ID Formats</strong></td>
<td>Select <strong>Email Address</strong></td>
</tr>
</tbody>
</table>

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
7. Review the configurations and write down the **Assertion Consumer Service URL** (this will be needed later). Click **Finish**.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
Creating a Remote Identity Provider

In this section, SAS will be configured in the CA SiteMinder Policy Server as an Identity Provider in order to enable SAML authentication to a secure website.

1. Log in to the SiteMinder Administrative UI window:

2. Select the Federation tab.

3. In the left pane, under Partnership Federation, click Entities.
4. Click Create Entity.

5. Select Entity Location as Remote and New Entity Type as SAML2 IDP, and then click Next.
6. Complete the fields as follows (all information appears in the SAS metadata file can be downloaded by browsing to https://idp1.cryptocard.com/idp/shibboleth/). If more than one row is required, click **Add Row**.

| **Entity ID** | Enter the Entity ID (https://idp1.cryptocard.com/idp/shibboleth/) |
| **Entity Name** | Enter an Entity Name (for example, Safenet-Idp) |
| **Remote SSO Service URLs** | **Binding (HTTP-Redirect)** Enter the IDP HTTP-redirect login URL (https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO)  
**Binding (SOAP)** Enter the IDP HTTP-POST login URL (https://idp1.cryptocard.com/idp/profile/SAML2/Post/SSO)  
**Binding (SOAP)** Enter the ArtifactResolutionService Binding Location URL (https://idp1.cryptocard.com/idp/profile/SAML2/SOAP/ArtifactResolution) |
| **Remote SOAP Artifact Resolution URLs** | **Index (1)** Enter the ArtifactResolutionService Binding Location URL (https://idp1.cryptocard.com/idp/profile/SAML1/SOAP/ArtifactResolution)  
**Index (2)** Enter the ArtifactResolutionService Binding Location URL (https://idp1.cryptocard.com/idp/profile/SAML2/SOAP/ArtifactResolution) |
| **Remote SLO Service URLs** | **Binding (HTTP-Redirect)** Enter the IDP logout URL (https://idp1.cryptocard.com/idp/signout.jsp) |
| **Remote Attributes Service URLs** | **Location URL** Enter the AttributeService Binding Location URL (https://idp1.cryptocard.com/idp/profile/SAML1/SOAP/AttributeQuery)  
**Location URL** Enter the AttributeService Binding Location URL (https://idp1.cryptocard.com/idp/profile/SAML2/SOAP/AttributeQuery) |
| **Signature and Encryption Options** | Select the ‘Verification Certificate Alias’ imported in “Configuring a Trust Certificate” section and select and enable the ‘Signed Authentication Requests Required’ checkbox. |
| **Supported Name ID Formats and Attributes** | Select the ‘Email Address’ checkbox. |
| **Option/Field 1** | Use this option to enable option 1 behavior. |
| **Option/Field 2** | Use this option to enable option 2 behavior. |
7. Click Next.
8. Review the configuration and then click **Finish** to close the window.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
Creating a Partnership

In this section, a partnership between SAS and CA SiteMinder Policy Server will be configured, and as a result a Remote Entity ID (required for the SP initiated URL) will be created.

1. Log in to the SiteMinder Administrative UI window.

2. Click the Federation tab.

3. In the left pane, under Partnership Federation, click Partnerships.
4. Click Create Partnership.

5. Click **SAML2 SP -> IDP**.
6. Enter the fields as follows, and then click **Next**:

<table>
<thead>
<tr>
<th>Partnership Name</th>
<th>Enter a partnership name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local SP</strong></td>
<td>Select the Local SP created in the <em>Creating a Local Service Provider</em> section (page 27)</td>
</tr>
<tr>
<td><strong>Remote IDP</strong></td>
<td>Select the Remote IDP created in the <em>Creating a Remote Identity Provider</em> section (page 31)</td>
</tr>
<tr>
<td><strong>Available Directories</strong></td>
<td>Click on the organization directory and click on the arrow to move it to the Selected Directories.</td>
</tr>
</tbody>
</table>

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
7. Enter the fields as follows, and then click **Next**:

| **Choose Identity Attribute from Assertion** | Leave as default – Use Name ID. |
| **Map Identity Attribute from Assertion** | Enter the AD Search Specification - sAMAccountName=%s |
| **Federated Users** | Click Add Row. Verify that the Directory is your directory and that All Users in Directory is chosen. |

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
8. Enter the fields as follows, and then click **Next**:

<table>
<thead>
<tr>
<th><strong>SSO Profile</strong></th>
<th>Select the <strong>HTTP-Post</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transactions Allowed</strong></td>
<td>Select <strong>SP initiated only</strong></td>
</tr>
<tr>
<td><strong>Remote SSO Service URLs</strong></td>
<td>Leave default settings</td>
</tr>
<tr>
<td><strong>Remote SOAP Artifact Resolution URLs</strong></td>
<td>Select the SAML2 URL (line 2) – <a href="https://idp1.cryptocard.com/idp/profile/SAML2/SOAP/ArtifactResolution">https://idp1.cryptocard.com/idp/profile/SAML2/SOAP/ArtifactResolution</a></td>
</tr>
<tr>
<td><strong>Attribute Requester Service</strong></td>
<td>Select the SAML2 URL (line 2) – <a href="https://idp1.cryptocard.com/idp/profile/SAML2/SOAP/AttributeQuery">https://idp1.cryptocard.com/idp/profile/SAML2/SOAP/AttributeQuery</a></td>
</tr>
</tbody>
</table>
Using SafeNet Authentication Service as an Identity Provider for CA SiteMinder

The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
9. Click **Next**.

10. Under Signature, select **Disable Signature Processing**, and then click **Next**.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
11. Enter the fields as follows and click **Next**:

<table>
<thead>
<tr>
<th>Redirect Mode</th>
<th>Select <strong>Cookie Data</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target</strong></td>
<td>enter the target Website/Web Application you want to protect (example: <a href="http://ca.safenetdemos.com/saml/demo.aspx">http://ca.safenetdemos.com/saml/demo.aspx</a>)</td>
</tr>
<tr>
<td><strong>Relay State Overrides Target</strong></td>
<td>Select t if a redirection option is required (optional).</td>
</tr>
</tbody>
</table>

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
12. Review the details and then click **Finish** to close this window.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
Using SafeNet Authentication Service as an Identity Provider for CA SiteMinder

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
13. Back in the **Partnerships** window, activate the partnership by clicking its **Action** button (next to its name) and then click **Activate**.

![Partnerships window with partnership activated](image1.png)

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

14. Click **Yes** when prompted for confirmation.

![Confirm activation dialog](image2.png)

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

15. Copy the **Remote Entity ID URL** as displayed in the **Federation Partnership List** and use it to configure the **SP initiated URL**:

Creating an Authentication Scheme

In this section, the Authentication Scheme creation is described, where SAS SAML is configured on the CA SiteMinder Policy Server.

1. Log in to the **SiteMinder Administrative UI** window:

   ![SiteMinder Administrative UI](image)

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

2. Click the **Infrastructure** tab.

   ![SiteMinder Administrative UI](image)

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

3. Click the **Authentication** tab. In the left pane, click **Authentication Schemes**.

   ![SiteMinder Administrative UI](image)

   *(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)*
4. In the right pane, click **Create Authentication Scheme**.

5. Select **Create a new object of type Authentication Scheme**, and then click **OK**.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
6. Fill in the required fields as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Scheme Type</td>
<td>Select <strong>SAML 2.0 Template</strong>.</td>
</tr>
</tbody>
</table>

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
Ignore the alert **SAML2 configuration is missing.** It will be configured next.

7. Click **SAML 2.0 configuration.**

   a. Enter the names of the SP ID and Idp ID in the appropriate fields and leave all other as default settings and click **Next.**

   ![SiteMinder Administrative UI](image)

   (The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
b. In the SSO tab:
   - Select the **Relay State Overrides Target**.
   - Click **Next**.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
c. On the SLO tab, leave the default settings and then click **Next**.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
d. On the **Attribute** tab:

- Select **Enabled**.
- Enter **Attribute Service** (the AttributeService Binding Location URL from metadata file - https://idp1.cryptocard.com/idp/profile/SAML2/SOAP/AttributeQuery).
- Select **Email Address** as Name ID Format.
- Enter **mail** as an Attribute Name.
- Click **Next**.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
e. On the **Encryption & Signing** tab:

- Select **Disable Signature Processing**.
- Under **Backchannel**, enter **Basic** in the **Authentication** field. Enter and then confirm a password.
- Click **Next**.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
f. On the **Advanced** tab, leave the default settings, and then click **Finish**.

![Image of SiteMinder Administrative UI](image)

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

8. Click **Submit**.

The new Authentication Scheme has been added.

![Image of SiteMinder Administrative UI](image)

*(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)*
Configuring a SAML Protected Realm

This section describes the SAML-protected realm configuration, where the resource to be protected by SAML authentication is configured.

1. Log in to the SiteMinder Administrative UI window:

2. Click the Policies tab.

3. Click the Domain tab.
4. In the left pane, click **Domains**.

5. To modify a domain, click the pencil icon to the right of the domain name.

6. Click the **Realms** tab.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
7. Click **Create Realm** to create a new realm.

8. Fill in the required fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Choose a name for the realm.</td>
</tr>
<tr>
<td>Agent</td>
<td>Choose a web agent (if it doesn't exist you need to create one by clicking <strong>Lookup Agent/Agent Group</strong> and then clicking <strong>Create Agent</strong>).</td>
</tr>
<tr>
<td>Resource Filter</td>
<td>Choose the virtual directory to be secured by this realm.</td>
</tr>
<tr>
<td>Authentication Scheme</td>
<td>Choose the authentication scheme that was created in the <strong>Creating an Authentication Scheme</strong> section.</td>
</tr>
<tr>
<td>Rules</td>
<td>Click <strong>Create</strong> to create a new rule.</td>
</tr>
</tbody>
</table>

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
9. Fill in the fields as follows, and then click **OK** to save the rule:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Choose a name for the rule.</td>
</tr>
<tr>
<td><strong>Resource</strong></td>
<td>Enter a resource (Can stay as default '**'')</td>
</tr>
<tr>
<td><strong>Allow/Deny and Enable/Disable</strong></td>
<td>Can stay as default</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Select <strong>Web Agent actions</strong> and highlight <strong>Get</strong> and <strong>Post</strong> actions</td>
</tr>
</tbody>
</table>

![Image of SiteMinder Administrative UI](image)

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

10. Click **OK**.
11. Verify that the new realm is now added to the realms list of your domain.

12. Click **Submit** to submit the changes to the Policy Server.
Creating a Domain Policy

This section describes how to create a Domain Policy, where the SAML authentication policy is being assigned to users in the domain.

1. Log in to the SiteMinder Administrative UI window.

2. Click the Policies tab.

3. Click the Domain tab.
4. In the left pane, click **Domains**.

![Domain Administration UI](image1)

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

5. To modify a domain, click the pencil icon to the right of the required domain.

6. Click the **Policies** tab.

![Policy Administration UI](image2)

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
7. Click **Create**.

![SiteMinder Administrative UI](image)

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

8. Click the **General** tab.

![SiteMinder Administrative UI](image)

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

9. Enter a name for the policy.
10. Click the **Users** tab.

11. Select the users to whom you want to apply the policy (for example, select **Add All**).

12. Click the **Rules** tab.

13. Click **Add Rule**.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
14. Select the SAML rule that was created when the SAML protected realm was added, and then click OK.

15. Click OK to save the changes.
16. Click Submit to submit the changes to the Policy Server.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with CA SiteMinder using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 66
- Assigning an Authenticator in SafeNet Authentication Service, page 67
- Adding CA SiteMinder as a Service Provider (SP) in SafeNet Authentication Service, page 67
- Enabling SAML Services in SafeNet Authentication Service, page 71

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:

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 CA SiteMinder.

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 CA SiteMinder 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 CA SiteMinder. You will need the Issuer ID and Assertion Consumer Service URL location of CA SiteMinder.

**To add CA SiteMinder as a Service Provider in SafeNet Authentication Service:**

1. Log in to the SafeNet Authentication Service console with an Operator account.
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**.
5. In the **Add SAML 2.0 Settings** section, complete the following fields, and then click **Apply**:

- **Friendly Name**: Enter a friendly name for the CA SiteMinder provider.
- **SAML 2.0 Metadata**: Select **Create New Metadata File**.
- **Entity ID**: Enter the same Entity ID configured in CA SiteMinder Policy Server (For example, `ca.safenetdemos.com`).
- **Location**: Enter the **Assertion Consumer Service URL** from the Local SP Entity configuration of the CA SiteMinder Policy Server. The ACS URL was configured in **Create a local Service Provider** section (For example, `http://ca.safenetdemos.com/affwebservices/public/saml2assertionconsumer`).

---

**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](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>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/CommonName">http://schemas.xmlsoap.org/claims/CommonName</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td>principal</td>
<td>According to ThirdParty Product Requirements</td>
</tr>
</tbody>
</table>

CA SiteMinder is added as a service provider in the system.
Enabling SAML Services in SafeNet Authentication Service

After CA SiteMinder 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**.

5. Click **Add**.
6. Under **Add SAML Service**, do the following:
   g. From the **Service** menu, select the CA SiteMinder service provider.
   h. In **SAML Login ID** field, select the **User ID** to be sent as a UserID to CA SiteMinder in the SAML response.
   i. Click **Add**.

   ![Image of SAML Services](image1)

   The user can now authenticate to CA SiteMinder using SAML authentication.

   ![Image of SAML Services](image2)

**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.

   ![Image of SafeNet Authentication Service](image3)

2. Click the **POLICY** tab, and then click **Automation Policies**.

   ![Image of Automation Policies](image4)
3. Click the **SAML Provisioning Rules** link.

4. Click **New Rule**.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rule Name</strong></td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td><strong>User is in container</strong></td>
<td>Users affected by this rule must be in the selected container.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>The <strong>Virtual Server groups</strong> 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 <strong>Used by rule</strong> box.</td>
</tr>
</tbody>
</table>
**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**

This is the User ID that will be returned to the Service Provider in the SAML assertion. Select **User ID**.
Running the Solution

The example below demonstrates how to authenticate to a website protected by SiteMinder using SafeNet SAS SMS token.


2. The browser redirects Bob to the SAS SAML login page:

3. Bob enters his username and generates an OTP using his token for the password field.

4. After a successful authentication, Bob is forwarded to the requested website/web application.
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><strong>Address</strong></td>
<td>Gemalto, 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>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></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>