SafeNet Authentication Manager
Integration Guide

Using SAM as an Identity Provider for CA SiteMinder
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012794-001, Rev A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>October 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>
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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

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 tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in CA SiteMinder using SafeNet Authentication Manager 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 Manager.

CA SiteMinder can be configured to support multi-factor authentication in several modes. SAML authentication will be used for the purpose of working with SafeNet Authentication Manager.

Applicability

The information in this document applies to:

- SafeNet Authentication Manager - a server-based authentication management platform deployed as an on-premises solution within the organization.
Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Manager 8.2 HF 539** - a server based authentication management platform deployed as an on-premises solution within the organization.
- **CA SiteMinder** version 12.5.1

Audience

This document is intended for system administrators who are familiar with CA SiteMinder and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager.

SAML Authentication using SAM

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

The image below describes the data flow of a multi-factor authentication transaction for CA SiteMinder.
Authentication Flow using SAM

SafeNet Authentication Manager 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 loads the Idp Initiated URL to login to the SiteMinder’s secured website using SAML authentication.
2. The user enters his credentials, which SAM collects and evaluates.
3. SAM sends a SAML response to CA SiteMinder, accepting or rejecting the user’s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Manager to receive SAML authentication requests from CA SiteMinder, ensure that the end users can authenticate to the CA SiteMinder environment with a static password.
SAM SAML Configuration

The SAM Configuration Manager Settings are used to establish SafeNet Authentication Manager (SAM) as the identity provider for CA SiteMinder.

To configure SAM SAML:

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

2. On the menu bar, click Action > Cloud Configuration.

   The Cloud Settings window opens

3. Click the Info for Service Provider tab.
4. In the **Domain URL** field, enter the domain URL of your organization’s SAM external portal.

![Cloud Settings](image)

The **Single Sign-On** fields are automatically filled.

The displayed values will be needed when creating a remote identity provider section of *Configuring CA SiteMinder*. See “*Error! Reference source not found.*” on page *Error! Bookmark not defined.*.
Configuring CA SiteMinder

Configuring SAML Federation authentication in CA SiteMinder Policy Server requires the following:

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

Installing and Configuring 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 to exchange 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. On the Introduction page, click Next.

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

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

![Installation Summary](image)

*(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](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`).

```java
//tunnel library type. valid values are 'c' and 'java'
NotificationLibraryType=java

//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

//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`

```plaintext
// 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\servlethenec 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 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 then 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**.

*(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**.
12. Click **Next**.

(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**.

![ServletExec 6.0 Application Server Setup](image)

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

14. Click **OK** on the message window to start the installation process.

![ServletExec 6.0 Application Server Setup](image)

(The screen image above is from New Atlanta. Trademarks are the property of their respective owners.)
15. Clear the **Display the README** file option and then click **Finish**.
Configuring the ServletExec Extension

To update the ServletExec extension to the most updated version, several 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 command line as an administrator and execute the `StopServletExec.bat` file (from the `<ServletExec extension folder>\se-iis\` folder).

3. Make sure that the “StopServletExec has been stopped” message appears.
4. Replace the `C:\Program Files\New Atlanta\ServletExec AS\installerFiles\StopServletExec.class` file with the file under the `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` and then copy the `ServletExec_Adapter.dll.IIS_32bit` file to the same location. Rename the file to `ServletExec_Adapter.dll`.

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

7. Rename the `C:\Program Files\New Atlanta\ServletExec AS\bin\apache\ApacheModuleServletExec.dll` file to `ApacheModuleServletExec.bak` and then copy the `ApacheModuleServletExec.dll.APACHE2.0.x` file to same location. Rename it to `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` and then copy the `ApacheModuleServletExec.dll.APACHE2.2.x` file to same location. Rename the file to `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\sei-isis\` folder).

10. Make sure that the “ServletExec 6.0 initialized in [x] seconds” message appears.

![Initialization message](image)
11. Log in to ServletExec by browsing to http://localhost/servletexec/admin. Enter 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.)*

12. In the left pane, under **Web Application**, click **Manage** and then, in the right pane, click **Add a web application**.

![ServletExec manage web applications](image)

*(The screen image above is from New Atlanta. Trademarks are the property of their respective owners.)*
13. 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>Press ‘Browse’ button and choose ‘C:\CA\webagent\win64\affwebservices’</td>
</tr>
</tbody>
</table>

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

14. 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 CA Administrative UI:

![Image](image1.png)

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

2. Click on the Infrastructure tab.

![Image](image2.png)

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


![Image](image3.png)

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
4. Click **Import New** to import a new certificate to the SiteMinder server.

   ![SiteMinder Administrative UI](image1)

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

5. Click **Browse** and choose the certificate you want to import. Click **Next**.

   ![SiteMinder Administrative UI](image2)

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

6. Enter the certificate password, if it exists, and click **Next**.

   ![SiteMinder Administrative UI](image3)

   *(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)*
7. Verify the entry is correct (and this is the correct certificate) and 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, 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.

5. Select Entity Location as Local and New Entity Type as SAML2 SP. Click Next.
6. Enter the fields as follows and then click **Next**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entity ID</strong></td>
<td>Enter an Entity ID that will identify SiteMinder in the SAML authentication (for example <code>&lt;WebAgent public hostname&gt;</code>)</td>
</tr>
<tr>
<td><strong>Entity Name</strong></td>
<td>Enter an Entity Name that will identify the SP in SiteMinder GUI (for example <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 (for example <code>http://&lt;WebAgent public hostname&gt;</code>)</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, SAM 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:

   ![SiteMinder Administrative UI](image1)

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

2. Select the Federation tab.

   ![SiteMinder Administrative UI](image2)

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

3. In the left pane, under Partnership Federation, click Entities.

   ![SiteMinder Administrative UI](image3)

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

5. For Entity Location, select Remote, and for New Entity Type select SAML2 IDP. Click Next.

6. Fill in the fields as follows (all information appears in Cloud Settings window of your SAM server).

   If more than one row is needed to be added, click Add Row.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity ID</td>
<td>Enter the Entity ID (for example http:&lt;SAM_machine_name&gt;)</td>
</tr>
<tr>
<td>Entity Name</td>
<td>Enter an Entity Name (for example http:&lt;SAM_machine_name&gt;)</td>
</tr>
<tr>
<td>Remote SSO Service URLs &gt; Binding (HTTP-Redirect)</td>
<td>Enter the SAM Sign-in page URL.</td>
</tr>
<tr>
<td>Remote SOAP Artifact Resolution URLs</td>
<td>Leave default settings</td>
</tr>
<tr>
<td>Remote SLO Service URLs &gt; Binding (HTTP-Redirect)</td>
<td>Enter the SAM Sign-out URL.</td>
</tr>
<tr>
<td>Remote Attributes Service URLs</td>
<td>Leave default settings</td>
</tr>
<tr>
<td>Supported Name ID Formats and Attributes</td>
<td>Select Email Address.</td>
</tr>
</tbody>
</table>
Please note changes to an entity will not be automatically reflected in any partnership associated with this entity. To update the partnership with the latest changes from the entity, please modify the partnership and click on “Get Updates” next to the entity that has been changed.

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

(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>Partnership Name</strong></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 <a href="#">Creating a Local Service Provider section</a></td>
</tr>
<tr>
<td><strong>Remote IDP</strong></td>
<td>Select the Remote IDP created in the <a href="#">Creating a Remote Identity Provider section</a></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 <a href="#">Selected Directories</a></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**:

<table>
<thead>
<tr>
<th>Choose Identity Attribute from Assertion</th>
<th>Leave as the default settings – Use Name ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map Identity Attribute from Assertion</td>
<td>Enter the AD Search Specification - sAMAccountName=%s</td>
</tr>
<tr>
<td>Federated Users</td>
<td>Click <strong>Add Row</strong>. Verify that the directory is your directory and that <strong>All Users in Directory</strong> is selected.</td>
</tr>
</tbody>
</table>

(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>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSO Profile</strong></td>
<td>Select <strong>HTTP-Post</strong></td>
</tr>
<tr>
<td><strong>Audience</strong></td>
<td>Enter the <strong>SAM Entity ID</strong> configured previously</td>
</tr>
<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>
</tbody>
</table>

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

10. Under the **Signature** section, enable the **Disable Signature Processing** option and click the **Next** button.
11. Enter the fields as follows:

<table>
<thead>
<tr>
<th>Redirect Mode</th>
<th>Select Cookie Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</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>Optional</td>
<td>Select Relay State Overrides Target where a redirection option needs to be available.</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 click **Finish** to close this window.
13. On the **Partnerships** window, click **Action** (next to its name) and then click **Activate**.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
14. Click **Yes** when prompted for confirmation.

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 SAM SAML is configured on the CA SiteMinder Policy Server.

1. Log in to the SiteMinder Administrative UI window:

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

2. Click the Infrastructure tab.

   (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.

   (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**.
6. Complete the following fields:

<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 SAML 2.0 Template.</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 fields with default settings. Click **Next to continue**.

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

- Enter the SSO service (the IDP HTTP-POST login URL - https://idp1.cryptocard.com/idp/profile/SAML2/Post/SSO)
- Select and enable the **Relay State Overrides Target** option.
- 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**.
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.)
1. On the **Advanced** tab, leave default settings, and then click **Finish**.

8. Click **Submit**.

The new Authentication Scheme was added.
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:

   ![SiteMinder Administrative UI](image)

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

2. Click on the Policies tab.

   ![SiteMinder Administrative UI](image)

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

3. Click on the Domain tab.

   ![SiteMinder Administrative UI](image)

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

   ![Domains](image1.png)

   *(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 domain name.

6. Click the **Realms** tab.

   ![Realms](image2.png)

   *(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><strong>Name</strong></td>
<td>Choose a name for the realm.</td>
</tr>
<tr>
<td><strong>Agent</strong></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><strong>Resource Filter</strong></td>
<td>Choose the virtual directory to be secured by this realm.</td>
</tr>
<tr>
<td><strong>Authentication Scheme</strong></td>
<td>Choose the authentication scheme that was created in the <strong>Creating an Authentication Scheme</strong> section</td>
</tr>
<tr>
<td><strong>Resource Filter</strong></td>
<td>Rules</td>
</tr>
</tbody>
</table>
### Using SAM as an Identity Provider for CA SiteMinder

#### General
- **Name**: [xml]
- **Description**: [xml]
- **Domain**: integ_domain

#### Resource
- **Agent**: [web]
- **Lookup Agent/Agent Group**: [xml]
- **Resource Filter**: [xml]
- **Effective Resource**: [xml]
- **Default Resource Protection**: [Protected]
- **Unprotected**
- **Authentication Scheme**: [SafeNet-fed]

#### Rules
- **Name**: [xml]
- **Description**: [xml]

#### Sub-Realms
- **Name**: Resource Filter
- **No results**.

#### Session
- **Maximum Timeout**
  - **Enabled**
  - **Hours**: [2]
  - **Minutes**: [2]
- **Idle Timeout**
  - **Enabled**
  - **Hours**: [1]
  - **Minutes**: [0]
- **Persistent Session**: [Non-persistent]
- **Synchronous Auditing**: [ ]

#### Advanced
- **Authorization Identity Mapping**
  - **Authorization Mapping**: [Default]
  - **Create Authorization Mapping**
- **Validation Identity Mapping**
  - **Validation Mapping**: [Default]
  - **Create Validation Mapping**
- **Legacy Authorization Directory Mapping**
  - **Directory Mapping**: [Default]
  - **Create Legacy Authorization Mapping**
- **Events**
  - **Process Authentication Events**
  - **Process Authorization Events**
- **Flush Resources in Realm**

---

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

---

SafeNet Authentication Manager: Integration Guide
Using SAM as an Identity Provider for CA SiteMinder
Document PN: 007-012794-001, Rev. A, Copyright © 2014 SafeNet, Inc., All rights reserved.
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>Enter 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>

(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.

![SiteMinder Administrative UI](image)

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

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. Login 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 **Policies** tab.

3. Click on the **Domain** tab.

4. In the left pane, click **Domains**.

(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.

7. Click **Create**.

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

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, choose **Add All**).
12. Click the **Rules** tab.

13. Click **Add Rule**.

14. Select the SAML rule that was created when creating a SAML-protected realm, and then click **OK**.

15. Click **OK** to save the changes.

16. Click **Submit** to submit the changes to the Policy Server.
Configuring SAML User Authentication in SAM

SafeNet Authentication Manager’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 Guide for general portal configuration.

To edit the required Token Policy Object:

1. Open the Token Policy Object Editor for the appropriate group.

   See the SafeNet Authentication Manager 8.2 Administrator Guide for more information.

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

   The property’s policies are displayed in the right pane.
3. In the right pane, double-click **Application Authentication Settings**.

4. Select Define this policy **setting**, select **Enabled**, and then click **Definitions**.
5. In the left pane, right-click **Application Authentication Settings** and select **Create a new profile**.
6. In the left pane, right-click the new profile and select **Rename**.
7. Rename the profile to **SiteMinder**.
8. In the left pane, click the new profile, **SiteMinder**.
9. In the right pane, double-click the following policies, and then enter the appropriate information:

<table>
<thead>
<tr>
<th>Application Issuer</th>
<th>Enter the SiteMinder’s Entity ID value (for example, ca.siteminder.com)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM issuer</td>
<td>Enter the Domain URL copied from the SAM Cloud Setting window.</td>
</tr>
<tr>
<td>Application’s login URL</td>
<td>Enter Entity’s Assertion Consumer Service URL. (for example:</td>
</tr>
<tr>
<td></td>
<td><a href="https://ca.safenetdemos.com/afw">https://ca.safenetdemos.com/afw</a> webservices/public/saml2assertioncons</td>
</tr>
<tr>
<td></td>
<td>umer</td>
</tr>
<tr>
<td>Audience URI</td>
<td>Enter the SiteMinder’s Entity ID value (for example ca.siteminder.com)</td>
</tr>
<tr>
<td>User mapping</td>
<td>Choose <strong>Account Name</strong></td>
</tr>
<tr>
<td>Automatic Windows</td>
<td>Enable the authentication methods as required for your organization</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>OTP Authentication</td>
<td></td>
</tr>
<tr>
<td>Certificate-based</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>Network password authentication</td>
<td></td>
</tr>
</tbody>
</table>

For detailed information about authentication methods, see the *SafeNet Authentication Manager Version 8.2 Administrator’s Guide*. 
The following is an example of completed fields in the **Application Authentication Settings** window:

10. Click **OK** to close the TPO Editor window
11. Click **OK** to close the **Application Authentication Settings** window
12. Click **OK** to close the user repository.

SiteMinder is now added as a SAML service provider.
Running the Solution

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


2. The browser redirects Bob to the SAM SAML login page:
3. Bob enters his username and generates an OTP using his token for the **Password** field.

![OTP Authentication](image)

3. **OTP Authentication**

   Enter the OTP Authentication Code using your OTP Passcode.

   Username: [Bob]

   OTP Authentication Code:

   **Send me another OTP passcode in a message**

   ![OK button]

4. After 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 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>
<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>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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>