SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for IBM Security Access Manager (ISAM) for Web
All information herein is either public information or is the property of and owned solely by Gemalto 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.

© 2016 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:** 007-013542-001, Rev. A  
**Release Date:** August 2016
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>5</td>
</tr>
<tr>
<td>Description</td>
<td>5</td>
</tr>
<tr>
<td>Applicability</td>
<td>5</td>
</tr>
<tr>
<td>Environment</td>
<td>6</td>
</tr>
<tr>
<td>Audience</td>
<td>6</td>
</tr>
<tr>
<td>SAML Authentication using SafeNet Authentication Service Cloud</td>
<td>6</td>
</tr>
<tr>
<td>SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE</td>
<td>6</td>
</tr>
<tr>
<td>SAML Authentication Flow using SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>SAML Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>8</td>
</tr>
<tr>
<td>Synchronizing Users Stores to SafeNet Authentication Service</td>
<td>8</td>
</tr>
<tr>
<td>Assigning an Authenticator in SafeNet Authentication Service</td>
<td>8</td>
</tr>
<tr>
<td>Adding IBM Security Access Manager (ISAM) for Web 9.0 Service Provider (SP) in SafeNet Authentication Service</td>
<td>9</td>
</tr>
<tr>
<td>Enabling SAML Services in SafeNet Authentication Service</td>
<td>12</td>
</tr>
<tr>
<td>Downloading the SafeNet Authentication Service Metadata</td>
<td>16</td>
</tr>
<tr>
<td>Download the SafeNet Identity Provider Certificate</td>
<td>16</td>
</tr>
<tr>
<td>Configuring ISAM for Web</td>
<td>16</td>
</tr>
<tr>
<td>Uploading the SAS IDP Certificate Keystore Files</td>
<td>17</td>
</tr>
<tr>
<td>Uploading the ISAM SP Certificate Keystore Files</td>
<td>20</td>
</tr>
<tr>
<td>Updating the Hosts File on the Appliance</td>
<td>23</td>
</tr>
<tr>
<td>Creating a Reverse Proxy Instance</td>
<td>24</td>
</tr>
<tr>
<td>Modifying the Configuration Settings of the Reverse Proxy Instance</td>
<td>26</td>
</tr>
<tr>
<td>Configuring the Load Runtime SSL Certificate in the pdsrv Trust Store</td>
<td>28</td>
</tr>
<tr>
<td>Configuring the Runtime Junction as the Default ISAM Junction for the Service Provider</td>
<td>30</td>
</tr>
<tr>
<td>Creating a Junction in Reverse Proxy/WebSEAL</td>
<td>33</td>
</tr>
<tr>
<td>Creating and Uploading the Sample One to One Mapping Rule for the Federation</td>
<td>36</td>
</tr>
<tr>
<td>Creating a User Registry in the ISAM Local Data Store</td>
<td>39</td>
</tr>
<tr>
<td>Configuring Federation Partners</td>
<td>41</td>
</tr>
<tr>
<td>Configuring the ACL Policy for the Service Provider</td>
<td>49</td>
</tr>
<tr>
<td>Configure SafeNet Authentication Service as an IDP Partner in Federation on ISAM for Web</td>
<td>54</td>
</tr>
<tr>
<td>Configuring Protected Object Policy (POP) for Multi-Step Authentication to the Particular Junction</td>
<td>64</td>
</tr>
<tr>
<td>Modifying the step-uplogin.html file to Perform the Multi-Factor Authentication</td>
<td>67</td>
</tr>
</tbody>
</table>
Running the Solution .................................................................................................................................................. 70
Support Contacts .................................................................................................................................................... 71
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as IBM Security Access Manager (ISAM) for Web 9.0.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service (SAS) delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

IBM Security Access Manager (ISAM) for Web provides an integrated security management platform for authentication services, access control, authorization services, identity mapping, web single sign-on, entitlements, and audit services across the enterprise resources. ISAM for Web provides integrated, policy-based security management for the extended enterprise that enables customers, business partners, employees, suppliers, and distributors to securely access enterprise resources in a trusted manner.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in IBM Security Access Manager (ISAM) for Web 9.0 using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in IBM Security Access Manager (ISAM) for Web 9.0 using SafeNet Authentication Service as an identity provider.

It is assumed that the IBM Security Access Manager (ISAM) for Web 9.0 environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

IBM Security Access Manager (ISAM) for Web 9.0 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)**—Version 3.5.2912.32855
- **IBM Security Access Manager (ISAM) for Web**—Version 9.0.1

Audience

This document is targeted to system administrators who are familiar with IBM Security Access Manager (ISAM) for Web 9.0, 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 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 IBM Security Access Manager (ISAM) for Web 9.0.

1. A user attempts to log on to IBM Security Access Manager (ISAM) for Web 9.0 to access protected resources. The user is redirected to SafeNet Authentication Service. SAS collects and evaluates the user's credentials.
2. SAS returns a response to IBM Security Access Manager (ISAM) for Web 9.0, accepting or rejecting the user's authentication request.

SAML Prerequisites

To enable SafeNet Authentication Service (SAS) to receive SAML authentication requests from IBM Security Access Manager (ISAM) for Web 9.0, ensure that the end users can authenticate from the IBM Security Access Manager (ISAM) for Web 9.0 environment with a static password.

The following prerequisite tasks must also be completed:

- Ensure the prerequisites required for installing the IBM Security Access Manager (ISAM) components are met. Refer to the following link:
  

- Install the following:
  - IBM ISAM for Web 9.0
  - Reverse Proxy
    - The Reverse Proxy must be up and running after configuration.
    - Protected Resource is to be add under the Reverse Proxy.
  - Federation License is uploaded in IBM ISAM for Web 9.0 for Federated Authentication

- Create an account in SAS Cloud. For more information, refer to: http://www.safenet-inc.com/request-information/
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with IBM Security Access Manager (ISAM) for Web 9.0 using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 8
- Assigning an Authenticator in SafeNet Authentication Service, page 8
- Adding IBM Security Access Manager (ISAM) for Web 9.0 Service Provider (SP) in SafeNet Authentication Service, page 9
- Enabling SAML Services in , page 12
- Downloading the SafeNet Authentication Service Metadata, page 16
- Download the SafeNet Identity Provider Certificate, page 16

Synchronizing Users Stores to SafeNet Authentication Service

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time using the Create User shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory/LDAP server using the SAS Synchronization Agent

For further details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users authenticating through IBM Security Access Manager (ISAM) for Web 9.0. 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 IBM Security Access Manager (ISAM) for Web 9.0 Service Provider (SP) in SafeNet Authentication Service**

To add SafeNet Authentication Service (SAS) as an Identity Provider in IBM Security Access Manager (ISAM) for Web 9.0:

Add a service provider entry in the SAS **SAML Service Providers** module to prepare it to receive SAML authentication requests from ISAM for Web. To import metadata of ISAM for Web refer to “Exporting the Service Provider’s Metadata” on page 48.

**To add IBM Security Access Manager (ISAM) for Web 9.0 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**.

![COMMS Tab](image1)

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

![SAML Service Providers](image2)

4. Click **Add**.

![Add SAML Service Provider](image3)
5. Under **Add SAML 2.0 Settings** section, complete the following fields, and then click **Apply**:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Enter the ISAM SP name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML 2.0 Metadata</td>
<td>Select <strong>Upload Existing Metadata File</strong>. Click the <strong>Choose File</strong> button, select the Service Provider’s metadata file, and then click <strong>Open</strong>.</td>
</tr>
</tbody>
</table>

**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

IBM Security Access Manager (ISAM) for Web 9.0 is added as a service provider in the system.
Enabling SAML Services in SafeNet Authentication Service

After IBM Security Access Manager (ISAM) for Web 9.0 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**, perform the following steps:
   a. From the **Service** menu, select the ISAM service provider.
b. In **SAML Login ID** field, select the type of login ID (**User ID, E-mail, or Custom**) to be sent as a User ID to ISAM in the response.

c. Click **Add**.

![Add SAML Service](image)

The user can now authenticate to ISAM using SAML authentication.

![SAML Services](image)

**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.

![SafeNet Authentication Service Console](image)
2. Click the **POLICY** tab, and then click **Automation Policies**.

3. Click the **SAML Provisioning Rules** link.

4. Click **New Rule**.

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

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Enter a name for the rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is in container</td>
<td>Users affected by this rule must be in the selected container.</td>
</tr>
<tr>
<td>Groups</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

Select **User ID**. The **User ID** will be returned to the service provider in the SAML assertion.

---

**Downloading the SafeNet Authentication Service Metadata**

Browse to the [https://idp1.cryptocard.com/idp/shibboleth](https://idp1.cryptocard.com/idp/shibboleth) URL. The SafeNet Authentication Service metadata will automatically download. Save it locally on your machine.

**Download the SafeNet Identity Provider Certificate**

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

**Configuring ISAM for Web**

Configuring ISAM for Web requires:

- Uploading the SAS IDP Certificate Keystore Files, page 17
- Uploading the ISAM SP Certificate Keystore Files, page 20
- Updating the Hosts File on the Appliance, page 23
- Creating a Reverse Proxy Instance, page 24
- Modifying the Configuration Settings of the Reverse Proxy Instance, page 26
Uploading the SAS IDP Certificate Keystore Files

Upload the SAS IDP Certificate keystore in the ISAM pdsrv database.

1. In a web browser, open any of the following URLs:
   - https://IP Address of ISAM Management Virtual Appliance/core/login
   - https://<FQDN_of_ISAM_Virtual Appliance>/core/login

   Where, FQDN_of_ISAM_Virtual Appliance is the complete domain name of the ISAM Virtual appliance.

2. On the ISAM login window, enter the administrator user name and password, and then click Login.

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
3. On the ISAM administrator console, click the Manage System Setting menu, and then under Secure Settings, click SSL Certificates.

![IBM Security Access Manager](image)

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

4. On the SSL Certificates window, perform the following steps:
   a. In the Certificate Database Name list, select pdsrv.
   b. In the Manage list, click Edit SSL Certificate Database.

![SSL Certificates](image)

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

5. On Edit SSL Certificate Database window, in the Manage list, click Import.

![Edit SSL Certificate Database - pdsrv](image)

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
6. On the **Import Signer Certificate** window, perform the following steps:
   
a. In the **Certificate File** field, click **Browse** to search and select the SAS IDP certificate stored on the local machine.
   
b. In the **Certificate Label** field, enter a label for the certificate (for example, **SAS Cert**).
   
c. Click **Import**.

   ![Import Signer Certificate](image)

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

6. On the **Edit SSL Certificate Database** window, on the **Signer Certificates** tab, the imported SAS IDP certificate (for example, **SAS Cert**) is listed.

   ![Edit SSL Certificate Database](image)

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

7. Click **Click here to review the changes or apply them to the system** link to deploy the changes.

   ![Click here to review the changes or apply them to the system](image)

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

8. On the **Deploy Pending Changes** window, click **Deploy** to deploy the changes.

   ![Deploy Pending Changes](image)

   (The screen image above is from IBM. Trademarks are the property of their respective owners.)
9. A warning message is displayed to restart the runtime component. Restart the component to make the changes come into effect.

10. On the ISAM administrator console, click the Secure Web Settings menu, and then under Manage, click Runtime Component.

11. On the Runtime Component window, click the Restart tab.

A system notification is displayed that the runtime component is restarted successfully.

Uploading the ISAM SP Certificate Keystore Files

NOTE: This environment is tested with the sample keystore and stash files for the service provider (SP) that is available in the providedfiles/myspkeys directory or location, provided by the IBM support. The keystore file contains ISAM Virtual Appliance certificate that is issued by the IBM CA server which is required for an SP initiated SAML flow.
1. On the ISAM administrator console, click the **Manage System Settings** menu, and then under **Secure Settings**, click **SSL Certificates**.

![Image of ISAM administrator console with Manage System Settings highlighted](image)

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

2. On the **SSL Certificates** window, in the **Manage** list, click **Import**.

![Image of SSL Certificates window with Import highlighted](image)

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

3. On the **Import SSL Certificate Database** window, perform the following steps:
   a. In the **Certificate Database File** field, click **Browse** to search and select the server provider certificate database file.
   
   ![Image of SSL Certificate Database window](image)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
   
   b. In the **Stash File** field, click **Browse** to search and select the stash file.
   
   ![Image of Stash File selection](image)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
   
   c. Click **Import**.

   ![Image of Import button](image)

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

4. Click **Click here to review the changes or apply them to the system** link to deploy the changes.

![Warning message for undeployed changes](image)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
5. On the **Deploy Pending Changes** window, click **Deploy** to deploy the changes.

![Deploy Pending Changes](image)

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

6. A warning message is displayed to restart the runtime component. Restart the component to make the changes come into effect.

![System Warning](image)

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

7. On the ISAM administrator console, click the **Secure Web Settings** menu, and then under **Manage**, click **Runtime Component**.

![Secure Web Settings](image)

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

8. On the **Runtime Component** window, click the **Restart** tab.

![Runtime Component](image)

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

A system notification is displayed that the runtime component is restarted successfully.

![System Notification](image)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
Updating the Hosts File on the Appliance

1. On the ISAM administrator console, click the **Manage System Settings** menu, and then under **Network Settings**, click **Hosts File**.

   ![Network Settings](image)

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

2. On the **Manage Hosts File** window, select **Host Records**, and then click **New**.

   ![Manage Hosts File](image)

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

3. On the **Create Host Record** window, complete the following fields, and then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Enter the IP address of the ISAM management interface.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter the hostname (for example, <code>isam.mysp.ibm.com</code>) for the ISAM management interface.</td>
</tr>
</tbody>
</table>

   ![Create Host Record](image)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
Creating a Reverse Proxy Instance

1. On the ISAM administrator console, click the **Secure Web Settings** menu, and then under **Manage**, click **Reverse Proxy**.

   ![Secure Web Settings](image1)

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

2. On the **Reverse Proxy** window, click **New**.

   ![Revers Proxy](image2)

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

3. On the **New Reverse Proxy Instance** window, on the **Instance** tab, complete the following fields, and then click **Next**.

   - **Instance Name**: Enter a name for the instance (for example **default**).
   - **IP Address for the Primary Interface**: Select the IP address of the reverse proxy interface.

   ![New Reverse Proxy Instance](image3)

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

   **NOTE**: Ensure that the **Host name** and **Listening Port** are correct.
4. On the **IBM Security Access Manager** tab, in the **Administrator Password** field, enter the ISAM administrator password, and then click **Next**.

5. On the **Transport** tab, perform the following steps:
   a. Select **Enable HTTPS**.
   b. In the **HTTPS Port** field, enter **443**.
   c. Click **Finish**.

The newly created reverse proxy instance is now configured and started.
Modifying the Configuration Settings of the Reverse Proxy Instance

**NOTE:** Ensure that the reverse proxy instance is up and running before modifying its configuration settings.

1. On the ISAM administrator console, click the **Secure Web Settings** menu, and then under **Manage**, click **Reverse Proxy**.

   ![ISAM Administrator Console Secure Web Settings Menu](image1)

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

2. On the **Reverse Proxy** window, select the reverse proxy instance (for example, **default**), and then click **Manage > Configuration > Edit Configuration File**.

   ![ISAM Administrator Console Reverse Proxy Configuration Menu](image2)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
3. In the configuration file, search the following variables and set their values:

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>web-host-name</td>
<td>Enter the hostname of reverse proxy. Here, hostname of reverse proxy is the FQDN of reverse proxy interface (for example, <a href="http://www.mysp.ibm.com">www.mysp.ibm.com</a>).</td>
</tr>
<tr>
<td>worker-threads</td>
<td>600</td>
</tr>
<tr>
<td>reset-cookies-list</td>
<td>*ac.uuid,*JSESSIONID</td>
</tr>
<tr>
<td>user-session-ids</td>
<td>yes</td>
</tr>
<tr>
<td>inactive-timeout</td>
<td>1800</td>
</tr>
<tr>
<td>create-unauth-sessions</td>
<td>yes</td>
</tr>
<tr>
<td>show-all-auth-prompts</td>
<td>yes</td>
</tr>
<tr>
<td>verify-step-up-user</td>
<td>yes</td>
</tr>
<tr>
<td>step-up-at-higher-level</td>
<td>no</td>
</tr>
</tbody>
</table>

4. In the configuration file, search the following variables and uncomment it.

```ini
#web-http-port = 443
#web-http-protocol = https
```

For example,

```ini
web-http-port = 443
web-http-protocol = https
```

5. Save the configuration file.

6. A warning message is displayed. Click Click here to review the changes or apply them to the system link to deploy the changes.
7. On the **Deploy Pending Changes** window, click **Deploy** to deploy the changes to the master copy of the configuration files.

![Deploy Pending Changes](image_url)

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

8. A warning message is displayed to restart the reverse proxy instance. Restart the reverse proxy instance to make the changes come into effect.

![System Warning](image_url)

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

9. On the **Reverse Proxy** window, select the reverse proxy instance (for example, **default**) that you created earlier in step 3 of “Creating a Reverse Proxy Instance” on page 24, and then click **Restart**.

![Reverse Proxy](image_url)

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

**Configuring the Load Runtime SSL Certificate in the pdsrv Trust Store**

1. On the ISAM administrator console, click the **Manage System Settings** menu, and then under **Secure Settings**, click **SSL Certificates**.

![Manage System Settings](image_url)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
2. On the **SSL Certificates** window, select the **pdsrv** certificate database, and then in the **Manage** list, click **Edit SSL Certificate Database**.

3. On the **Edit SSL Certificate Database** window, on the **Signer Certificates** tab, in the **Manage** list, click **Load**.

4. On the **Load Signer Certificate** window, complete the following fields, and then click **Load**.

   | **Server** | Enter the loopback IP address. |
   | **Port** | Enter the port number (for example, 443). |
   | **Certificate Label** | Enter a name for the certificate label (for example **Local Runtime**). |

5. A warning message is displayed. Click **Click here to review the changes or apply them to the system** link to deploy the changes.
6. On the **Deploy Pending Changes** window, click **Deploy** to deploy the changes to the master copy of the configuration files.

   ![Deploy Pending Changes](image)

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

7. A warning message is displayed to restart the reverse proxy instance. Restart the reverse proxy instance to make the changes come into effect.

   ![System Warning](image)

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

8. On the **Reverse Proxy** window, select the reverse proxy instance (for example, **default**) that you created earlier in step 3 of “Creating a Reverse Proxy Instance” on page 24, and then click **Restart**.

   ![Reverse Proxy](image)

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

**Configuring the Runtime Junction as the Default ISAM Junction for the Service Provider**

1. On the ISAM administrator console, click the **Secure Web Settings** menu, and then under **Manage**, click **Reverse Proxy**.

   ![Secure Web Settings](image)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
2. On the Reverse Proxy window, select the reverse proxy instance (for example, **default**), and then in the Manage list, click Junction Management.

![Reverse Proxy](image)

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

3. On the Junction Management window, click **New > Standard Junction**.

![Junction Management - default](image)

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

4. On the Create a Standard Junction window, on the Junction tab, perform the following steps:
   a. In the Junction Point Name field, enter the name of the junction (for example, `/isam`).
   b. Select Stateful Junction.
   c. Select the Junction Type as **SSL**.

![Create a Standard Junction](image)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
5. On the **Servers** tab, click **New**.

![Target Backend Servers. At least one serve](image)

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

6. On the **Add TCP or SSL Servers** window, complete the following fields, and then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Enter <strong>localhost</strong>.</td>
</tr>
<tr>
<td>TCP or SSL Port</td>
<td>Enter <strong>443</strong>.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Enter the IP address of the reverse proxy interface.</td>
</tr>
</tbody>
</table>

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
7. On the **Identity** tab, perform the following steps:
   a. In the **HTTP Basic Authentication Header** field, select **Ignore**.
   b. Under **HTTP Header Identity Information**, select **IV-USER**, **IV-GROUPS**, and **IV-CREDS**.
   c. Select **Junction Cookie**.
   d. In the **Junction Cookie JavaScript Block** field, select **Inhead**.
   e. Select **Insert client IP address**.
   f. Click **Save**.

![Image of Identity tab](image.png)

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

**Creating a Junction in Reverse Proxy/WebSEAL**

1. On the ISAM administrator console, click the **Secure Web Settings** menu, and then under **Manage**, click **Reverse Proxy**.

![Image of Secure Web Settings](image.png)

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

2. On the **Reverse Proxy** window, select the reverse proxy instance (for example, **default**), and then in the **Manage** list, click **Junction Management**.

![Image of Reverse Proxy window](image.png)

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

![Junction Management window](image)

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

4. On the Junction tab, perform the following steps:
   a. In the Junction Point Name field, enter the name of the junction (for example, /Safenet).
   b. Select Stateful Junction.
   c. Select the Junction Type as SSL.

![Create a Standard Junction](image)

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

5. On the Servers tab, click New.

![Target Backend Servers](image)

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

6. On the Add TCP or SSL Servers window, complete the following fields, and then click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname*</td>
<td>Enter the FQDN or IP address of application.</td>
</tr>
<tr>
<td>TCP or SSL Port*</td>
<td>Enter the port number (for example, 80 or 443) of the application.</td>
</tr>
<tr>
<td>Virtual Host</td>
<td>Enter the IP address of the Internet application, which you can host under the ISAM protected resource.</td>
</tr>
</tbody>
</table>
Virtual Host Port | Enter 80 if the Internet application is hosted as HTTP or enter 443 if the Internet application is hosted as HTTPS.

Local Address | Enter the IP address of the reverse proxy interface.

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

7. On the Identity tab, perform the following steps:
   a. In the HTTP Basic Authentication Header field, select Ignore.
   b. Under HTTP Header Identity Information, select IV-USER, IV-GROUPS, and IV-CREDS.
   c. Select Junction Cookie.
   d. In the Junction Cookie JavaScript Block field, select Inhead.
   e. Select Insert client IP address.
   f. Click Save.

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
Creating and Uploading the Sample One to One Mapping Rule for the Federation

Use the following Java script to create a sample one to one mapping rule for the federation:

```java
// SAML20 SP Mapping rule JavaScript
importPackage(Packages.com.tivoli.am.fim.trustserver.sts);
importPackage(Packages.com.tivoli.am.fim.trustserver.sts.uuser);
importPackage(Packages.com.tivoli.am.fim.trustserver.sts.utilities);
IDMappingExtUtils.traceString("sp mapping rule called with stsuu: " + stsuu.toString());
// Create the new principal attribute that's
// appropriate for a TAM Credential.
//var prinValues = java.lang.reflect.Array.newInstance(java.lang.String, 1);
var uname = stsuu.getPrincipalName();
// Clear the stsuu. We don't need any of the existing data.
stsuu.clear();
//var index=prinValues[0].indexOf("@");
//the above is need as I am getting the username from email address, you can use a fixed user
//var uname=prinValues[0].substr(0,index);
var principalAttr = new Attribute("name","urn:ibm:names:ITFIM:5.1:accessmanager",uname);
//stsuu.addAttribute(testRegAttr);
stsuu.addPrincipalAttribute(principalAttr);
var attributeAuthenticationLevel = new Attribute("AUTHENTICATION_LEVEL",
"urn:ibm:names:ITFIM:5.1:accessmanager", "2");
stsuu.addAttribute(attributeAuthenticationLevel);
// copy all the attributes from the idp, found in the AdditionalAttributeStatement, into this STSUU
for (var i = stsuu.getAttributeStatements(); i.hasNext(); ) {
    var attrStatement = i.next();
    var attrs = attrStatement.getAttributes();
    if (attrs != null & attrs.length > 0) {
        for (var j = 0; j < attrs.length; j++) {
            stsuu.addAttribute(attrs[j]);
        }
    }
}
var testAttr = new Attribute("testattr_sp","urn:mytype", "myvalue_sp");
stsuu.addAttribute(testAttr);
```
1. On the ISAM administrator console, click the **Secure Federation** menu, and then under **Global Settings**, click **Mapping Rules**.

![Secure Federation menu](image)

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

2. On the **Mapping Rules** window, click **Add**.

![Mapping Rules window](image)

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

3. On the **Create Mapping Rule** window, complete the following fields, and then click **Save**.

<table>
<thead>
<tr>
<th><strong>Content</strong></th>
<th>Copy and paste the sample Java script.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the mapping rule (for example, <strong>sp_saml20</strong>).</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Select <strong>SAML2_0</strong>.</td>
</tr>
</tbody>
</table>

![Create Mapping Rule window](image)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
4. A warning message is displayed. Click Click here to review the changes or apply them to the system to deploy the changes.

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

5. On the **Deploy Pending Changes** window, click **Deploy** to deploy the changes to the master copy of the configuration files.

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

6. A warning message is displayed to restart the reverse proxy instance. Restart the reverse proxy instance to make the changes come into effect.

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

7. On the **Reverse Proxy** window, select the reverse proxy instance (for example, **default**) that you created earlier in step 3 of “Creating a Reverse Proxy Instance” on page 24, and then click **Restart**.

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
Creating a User Registry in the ISAM Local Data Store

**NOTE:** ISAM local user registry User-ID must match with SAS on Cloud User-ID

1. On the ISAM administrator console, click the **Secure Web Settings** menu, and then under **Manage**, click **Policy Administration**.

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

2. On the login window, complete the following fields, and then click **Sign On**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Id</strong></td>
<td>Enter the Reverse Proxy/WebSEAL administrator user ID.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the administrator password.</td>
</tr>
</tbody>
</table>

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

After successful login, the **Task List** is listed.

   (The screen image above is from IBM. Trademarks are the property of their respective owners.)
3. In the left pane, click **User > Create User**, and then in the right pane, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Id</td>
<td>Enter the user ID. The user ID must match with the SAS user ID.</td>
</tr>
<tr>
<td>Common Name</td>
<td>Enter a common name for the user.</td>
</tr>
<tr>
<td>Surname</td>
<td>Enter a surname for the user.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a user password.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Re-enter the user password.</td>
</tr>
<tr>
<td>Registry UID</td>
<td>Enter the registry user ID. The registry user ID refers to the user domain (for example <code>cn=Bod,dc=iswga</code>)</td>
</tr>
<tr>
<td>Account Valid</td>
<td>Select this option.</td>
</tr>
<tr>
<td>GSO User</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Password Valid</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

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

4. A success message is displayed. Click **Done**.

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
Configuring Federation Partners

Configuring federation partners requires:

- Configuring ISAM as a Service Provider’s Partner in Federation, page 41
- Exporting the Service Provider’s Metadata, page 48

Configuring ISAM as a Service Provider’s Partner in Federation

1. On the ISAM administrator console, click the **Secure Federation** menu, and then under **Manage**, click **Federations**.

   ![Secure Federation menu](image1)

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

2. On the **Federation Management** window, click **Add**.

   ![Federation Management window](image2)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
3. On the **Update Federation** window, in the right pane, under **Federation Protocol**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th>Federation Name</th>
<th>Enter a name for the SAML 2.0 federation (for example, saml20sp).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the protocol for this federation</td>
<td>Select <strong>SAML 2.0</strong>.</td>
</tr>
</tbody>
</table>

![Update Federation window](image)

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

4. On the **Create New Federation** window, in the right pane, under **Template**, select **SAML 2.0**, and then click **Next**.

![Create New Federation window](image)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
5. Under **General Information**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th><strong>Company Name</strong></th>
<th>Enter a name for the company (for example, ISAM).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identify your role</strong></td>
<td>Select <strong>Service Provider</strong>.</td>
</tr>
</tbody>
</table>

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

6. Under **Point of Contact Server**, in the **Point of Contact** field, enter **https://<Interface IP address or domain name of the reverse proxy>/isam**, and then click **Next**.

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
7. Under **Profile Selection**, select the following SAML 2.0 profiles, and then click **Next**.
   - **Web Browser Single Sign-on**
   - **Single Logout**

8. Under **Single Sign-on Settings**, perform the following steps:
   a. Select the following supported bindings:
      - **HTTP POST**
      - **HTTP Redirect**
   b. Select **Require signature on incoming SAML assertions**.
   c. Select **Require outgoing SAML authentication requests to be signed**.
   d. Click **Next**.
9. Under **Single Logout Settings**, perform the following steps:
   a. Select the following supported bindings:
      - HTTP POST
      - HTTP Redirect
   b. Select the following outgoing SAML messages that require a signature:
      - Single Logout requests
      - Single Logout responses
   c. Click **Next**.

   ![Image of Single Logout Settings](image)

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

10. Under **Signature Options**, perform the following steps:
   a. In the **Certificate Database** field, select **myspkeys**.
   b. In the **Certificate Label** field, select **myspkey**.
   c. Select the **X509 Certificate Data** KeyInfo element.
   d. Click **Next**.

   ![Image of Signature Options](image)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
11. Under **Encryption Options**, perform the following steps:
   a. In the **Certificate Database** field, select **myspkeys**.
   b. In the **Certificate Label** field, select **myspkey**.
   c. Click **Next**.

   ![Encryption Options](image1)

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

12. Under **SAML Message Settings**, do not change the default values. Click **Next**.

   ![SAML Message Settings](image2)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
13. Under **Identity Mapping**, select the **Use JavaScript transformation for identity mapping** option, and then click **Next**.

![Image of Identity Mapping screen](image_url)

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

14. Under **Identity Mapping Rule**, select the identity mapping rule (for example, **sp_saml20**) that you uploaded earlier in step 3 of "Creating and Uploading the Sample One to One Mapping Rule for the Federation" on page 36, and then click **Next**.

![Image of Identity Mapping Rule screen](image_url)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
15. Under **Summary**, click **OK**.

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

On the **Federations Management** window, the newly created service provider federation is listed.

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

**Exporting the Service Provider’s Metadata**

1. On the ISAM administrator console, click the **Secure Federation** menu, and then under **Manage**, click **Federations**.

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
2. On the **Federation Management** window, in the **Federation Name** column, select the newly created federation (for example `saml20sp`), and then click **Export** to download the `federation_metadata.xml` file.

![Federation Management Window](image)

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

### Configuring the ACL Policy for the Service Provider

Configuring the ACL policy for the service provider requires:

- Configuring the SP Reverse Proxy, page 49
- Creating an ACL Policy for SP, page 51
- Configuring the Point of Contact (POC) Sign in Callback settings, page 53

#### Configuring the SP Reverse Proxy

1. On the ISAM administrator console, click the **Secure Web Settings** menu, and then under **Manage**, click **Reverse Proxy**.

![Secure Web Settings](image)

*The screen image above is from IBM. Trademarks are the property of their respective owners.*
2. On the Reverse Proxy window, select the reverse proxy instance (for example, default), and then click Manage > Configuration > Edit Configuration File.

![IBM Security Access Manager](image)

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

The isam configuration file is opened.

3. In the configuration file, under [authentication-levels], set the values of the variables as given below:
   - level = unauthenticated
   - level = password
   - level = ext-auth-interface

4. In the configuration file, under # EXTERNAL AUTHENTICATION INTERFACE, search for the following variables, and then set their values as given below.

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai-auth</td>
<td>both</td>
</tr>
<tr>
<td>eai-user-id-header</td>
<td>am-eai-user-id</td>
</tr>
<tr>
<td>eai-auth-level-header</td>
<td>am-eai-auth-level</td>
</tr>
<tr>
<td>eai-xattrs-header</td>
<td>am-eai-xattrs</td>
</tr>
<tr>
<td>eai-pac-header</td>
<td>am-eai-pac</td>
</tr>
<tr>
<td>eai-redir-url-priority</td>
<td>yes</td>
</tr>
<tr>
<td>eai-ext-user-id-header</td>
<td>am-eai-ext-user-id</td>
</tr>
<tr>
<td>eai-ext-user-groups-header</td>
<td>am-eai-ext-user-groups</td>
</tr>
<tr>
<td>eai-session-id-header</td>
<td>am-eai-session-id</td>
</tr>
</tbody>
</table>

5. In the configuration file, under [eai-trigger-urls], add the following:
   - trigger = /isam/sps/auth*
   - trigger = /isam/sps/saml20sp/saml20/soap*
   - trigger = /isam/sps/saml20sp/saml20/slo*
   - trigger = /isam/sps/saml20sp/saml20/login*

Where,
- `<federation name>`, is the SP federation name (for example, saml20sp) that you created earlier in step 3 of “Configuring ISAM as a Service Provider’s Partner in Federation” on page 41.
6. Save the file.
7. Restart the reverse proxy instance to make the changes come into effect. Ensure that all the changes are in place.

**Creating an ACL Policy for SP**

1. Open a putty terminal or use the appliance console, and then log in to the appliance interface. Here, putty terminal is used.
2. Connect to **ISAM Management IP Address** or **ISAM FQDN** (for example isam.mysp.ibm.com) using the **SSH** command, and then use the administrator credentials for authentication.

```plaintext
10.164.44.235 - PuTTY
login as: admin
admin@10.164.44.235's password:
Last login: Fri May 13 17:04:01 2016
Welcome to the IBM Security Access Manager
Welcome to the IBM Security Access Manager appliance
Enter "help" for a list of available commands
isam.mysp.ibm.com> 
```

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

3. Go to **isam**.

```
isam.mysp.ibm.com> isam
isam.mysp.ibm.com:isam> 
```

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

4. Go to **admin**.

```
isam.mysp.ibm.com:isam> admin
pdadmin> 
```

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

5. Login to the pdadmin console using the following command:

```
login -a sec_master -p passw0rd
```

Where,

- **sec_master** is reverse proxy administrator username.
- **passw0rd** is reverse proxy administrator password.

```
pdadmin> login -a sec_master -p Passw0rd
pdadmin sec master> 
```

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

6. Create ACLs using the following commands, and then attach the ACLs to the SAML endpoints.

```
acl create <federation name>-unauth
acl modify <federation name>-unauth set group iv-admin TcmdbsvaBRrxl
acl modify <federation name>-unauth set group webseal-servers Tgmdbsrxl
acl modify <federation name>-unauth set user sec_master TcmdbsvaBRrxl
acl modify <federation name>-unauth set any-other Tr
```
acl modify <federation name>-unauth set unauthenticated Tr
acl attach /WebSEAL/<Management Interface FQDN>-<instance name>/favicon.ico <federation name>-unauth
acl attach /WebSEAL/<Management Interface FQDN>-<instance name>/isam/sps/<federation name>/saml20/login saml20sp-unauth
acl attach /WebSEAL/<Management Interface FQDN>-<instance name>/isam/sps/<federation name>/saml20/logininitial <federation name>-unauth
acl attach /WebSEAL/<Management Interface FQDN>-<instance name>/isam/sps/<federation name>/saml20/slo <federation name>-unauth
acl attach /WebSEAL/<Management Interface FQDN>-<instance name>/isam/sps/<federation name>/saml20/sloinitial <federation name>-unauth
acl attach /WebSEAL/<Management Interface FQDN>-<instance name>/isam/sps/static <federation name>-unauth
acl create <federation name>-anyauth
acl modify <federation name>-set group iv-admin TcmdbsvaBRrxl
acl modify <federation name>-set group webseal-servers Tgmdbsrxl
acl modify <federation name>-set user sec_master TcmdbsvaBRrxl
acl modify <federation name>-set any-other Tr
acl modify <federation name>-anyauth set unauthenticated T
acl attach /WebSEAL/<Management Interface FQDN>-<instance name>/isam/sps/<federation name>/saml20/auth <federation name>-anyauth

Object modify /WebSEAL/<Management Interface FQDN>-<instance name>/isam/ set attribute HTTP-Tag-Value user_session_id=user_session_id

Where,
- <federation name>, is the SP federation name (for example, saml20sp) that you created earlier in step 3 of “Configuring ISAM as a Service Provider’s Partner in Federation” on page 41.
- <instance name>, is the reverse proxy instance name (for example, default) that you created earlier in step 3 of “Creating a Reverse Proxy Instance” on page 24.
- <Management Interface FQDN>, is the management interface FQDN (for example isam.mysp.ibm.com) that you created earlier in step 3 of “Updating the Hosts File on the Appliance” on page 23.

7. Run the following command to save the changes:

Server replicate
Configuring the Point of Contact (POC) Sign in Callback settings

1. On the ISAM administrator console, click the **Secure Federation** menu, and then under **Global Settings**, click **Advanced Configuration**.

   ![Secure Federation menu](image)

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

   The **Advance Configuration** window is displayed.

   ![Advanced Configuration window](image)

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

2. On the **Advanced Configuration** window, perform the following steps:
   a. In the **Filter** box, enter the **poc.signIn.authenticationLevelResponseHeader** variable. The variable is listed in the table.
   b. In the table, against the variable name, click the ![icon](image) icon to change the value of the variable.

   ![Advanced Configuration window](image)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
c. In the box, enter the new value for the variable, **am-eai-auth-level**, and then click **Save**.

![Advanced Configuration](image)

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

3. Follow step 2 to set the values of the following remaining variables.

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>poc.signIn.groupsResponseHeader</td>
<td>fim.groups</td>
</tr>
<tr>
<td>poc.signIn.serverResponseHeader</td>
<td>fim.server</td>
</tr>
<tr>
<td>poc.signIn.targetResponseHeader</td>
<td>am-eai-redir-url</td>
</tr>
<tr>
<td>poc.signIn.urlEncodingEnabled</td>
<td>false</td>
</tr>
<tr>
<td>poc.signIn.userRequestHeader</td>
<td>iv-user</td>
</tr>
<tr>
<td>poc.signIn.userResponseHeader</td>
<td>am-eai-user-id</td>
</tr>
<tr>
<td>poc.localIdentity.attributesRequestHeader</td>
<td>user_session_id</td>
</tr>
<tr>
<td>poc.localIdentity.credRequestHeader</td>
<td>iv-creds</td>
</tr>
<tr>
<td>poc.localIdentity.groupsRequestHeader</td>
<td>iv-groups</td>
</tr>
<tr>
<td>poc.localIdentity.userRequestHeader</td>
<td>iv-user</td>
</tr>
<tr>
<td>poc.websealAuth.authLevel</td>
<td>1</td>
</tr>
<tr>
<td>poc.websealAuth.authenticationMacros</td>
<td>%PARTNERID%,%TARGET%</td>
</tr>
<tr>
<td>poc.websealAuth.userRequestHeader</td>
<td>iv-user</td>
</tr>
</tbody>
</table>

**Configure SafeNet Authentication Service as an IDP Partner in Federation on ISAM for Web**

1. On the ISAM administrator console, click the **Secure Federation** menu, and then under **Manage**, click **Federations**.

![IBM Security Access Manager](image)

*The screen image above is from IBM. Trademarks are the property of their respective owners.*
2. On the **Federation Management** window, in the table, in the **Federation Name** column, select the SP Federation (for example *saml_sp*), and then click **Partners**.

![Federation Management Window](image)

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

3. On the **Partners** window, click **Add** to import **SAS IDP** as a partner.

![Partners Window](image)

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

4. On the **Create New Partner** window, in the right pane, click **Browse** to search and select the SAS metadata file that is exported from IDP earlier.

![Create New Partner Window](image)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
5. Under Single Sign-on Settings, select Force authentication to achieve account linkage and Include federation ID when performing alias service operations, and then click Next.

6. Under SOAP SSL Connection Settings, complete the following fields, and then click Next:

<table>
<thead>
<tr>
<th>Certificate Database</th>
<th>Select the certificate database (for example, pdsrv).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Label</td>
<td>Select the SAS IDP Certificate as the certificate label (for example, SAS Cert) that you uploaded earlier step 6 of “Uploading the SAS IDP Certificate Keystore Files” on page 17.</td>
</tr>
</tbody>
</table>

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
7. Under Identity Mapping, select the **Use JavaScript transformation for identity mapping** option, and then click **Next**.

   ![Identity Mapping](image1.png)

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

8. Select the mapping rule (for example, **sp_saml20**), and then click **Next**.

   ![Mapping Rule](image2.png)

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

9. Verify the summary details, and then click **OK**.

   ![Summary](image3.png)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
An error message is displayed.

```
System Error
FBTRBA098E The value [null] for [binding] is not valid. Valid values are: [artifact, post, redirect, soap]
```

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

10. On the **Partners** window, select the IDP Partner, and then click **Edit** to specify the IDP redirect and post URLs.

![Partners Window](image)

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

11. Under **General Information**, in the **Name** field, enter the name for IDP Federation (for example **https://idp1.cryptocard.com/idp/shibboleth**), and then click **Next**.

![Update Partner](image)

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
12. Under **Common Data**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th>Provider ID</th>
<th>Enter the provider ID (for example, <a href="https://idp1.cryptocard.com/idp/shibboleth">https://idp1.cryptocard.com/idp/shibboleth</a>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Partner role</strong></td>
<td>Select <strong>Identity Provider</strong>.</td>
</tr>
</tbody>
</table>

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

13. Under **Profile selection**, select **Web Browser Single Sign-on** and **Single Logout**, and then click **Next**.

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

14. Under **Single Sign-on Settings**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th><strong>Binding</strong></th>
<th>Select <strong>redirect</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>Select the redirect SSO URL of IDP (for example, <a href="https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO">https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO</a>).</td>
</tr>
<tr>
<td><strong>Force authentication to achieve account linkage</strong></td>
<td>Select this option.</td>
</tr>
</tbody>
</table>
15. Under **Single Logout Settings**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th>Binding</th>
<th>Select <em>redirect</em></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>Select the redirect SLO URL of IDP (for example, <a href="https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SLO">https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SLO</a>).</td>
</tr>
<tr>
<td><strong>Single logout requests</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Single logout responses</strong></td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

(Images of the user interface for updating partner and single logout settings are shown.)

(Images are from IBM. Trademarks are the property of their respective owners.)
16. Under **SOAP SSL Connection Settings**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th><strong>Certificate Database</strong></th>
<th>Select the IDP certificate database (for example, <code>pdsrv</code>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate Label</strong></td>
<td>Select the certificate label as SAS IDP Certificate (for example, <code>SAS Cert</code>) that you uploaded earlier in step 6 of “Uploading the SAS IDP Certificate Keystore Files” on page 17.</td>
</tr>
</tbody>
</table>

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

17. Under **Signature Options**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th><strong>Certificate Database</strong></th>
<th>Select the IDP certificate database (for example, <code>pdsrv</code>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate Label</strong></td>
<td>Select the certificate label as SAS IDP Certificate (for example <code>SAS Cert</code>) that you uploaded earlier step 6 of “Uploading the SAS IDP Certificate Keystore Files” on page 17.</td>
</tr>
</tbody>
</table>

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
18. Under **Encryption Options**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th><strong>Certificate Database</strong></th>
<th>Select the IDP certificate database (for example, <code>pdsrv</code>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate Label</strong></td>
<td>Select the SAS IDP Certificate as the certificate label (for example <code>SAS Cert</code>) that you uploaded earlier step 6 of “Uploading the SAS IDP Certificate Keystore Files” on page 17.</td>
</tr>
</tbody>
</table>

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

19. Under **Identity Mapping**, select **Use JavaScript transformation for identity mapping**, and then click **Next**.

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
20. Under **Identity Mapping Rule**, select `sp_saml20` that you created and uploaded earlier step 2 of “Creating and Uploading the Sample One to One Mapping Rule for the Federation” on page 36, and then click **Next**.

![Identity Mapping Rule](image)

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

21. Verify the summary details, and then click **OK**.

![Summary](image)

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

A success message is displayed.

![System Notification](image)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
Configuring Protected Object Policy (POP) for Multi-Step Authentication to the Particular Junction

1. On the ISAM administrator console, click the **Secure Web Settings** menu, and then under **Manage**, click **Policy Administration**.

   ![ISAM Console Screen](image)

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

2. On the login window, complete the following fields, and then click **Sign On**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Id</strong></td>
<td>Enter the administrator user ID.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the administrator password.</td>
</tr>
</tbody>
</table>

   ![Login Window](image)

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

3. After successful login, the **Task List** is listed. Expand **POP**, and then click **Create POP**.

   ![Task List](image)

   *(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
4. In the right pane, under Create POP, in the POP Name field, enter the POP name (for example, step-up2), and then click Create.

5. Under Manage POPs, click step-up2.

6. Under POP Properties, click the Attach tab, and then click Attach.
7. Under **Attach POP**, in the **Protected Object Path** field, enter the junction that you want to use as multi-factor authentication (for example, `/WebSEAL/isam.mysp.ibm.com-default/safenet`), and then click **Attach**.

   **NOTE:** Here, `/WebSEAL/isam.mysp.ibm.com-default/safenet` = `/WebSEAL/FQDN of the reverse proxy interface-reverse proxy/Junction Name`

8. Under **POP Properties**, click the **IP Auth** tab, and then click **Create**.

9. Under **Create IP Authentication**, select **Any Other Network**, and then in the **Authentication Level** field, enter **2**.

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

11. Under POP Properties, click the General tab, and then click Apply.

![POP Properties](image)

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

Modifying the step-uplogin.html file to Perform the Multi-Factor Authentication

1. On the ISAM administrator console, click the Secure Web Settings menu, and then under Manage, click Reverse Proxy.

![IBM Security Access Manager](image)

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
2. On the **Reverse Proxy** window, select the reverse proxy instance (for example, **default**), and then click **Manage > Management Root**.

![Reverse Proxy Window](image1)

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

3. On the **Manage Reverse Proxy Management Root** window, click **Management > C > stepuplogin.html**.

![Manage Reverse Proxy Management Root](image2)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
4. Click File > Open to open the stepuplogin.html file.

5. On the View Reverse Proxy Management Root File window, enter a value for URL as highlighted in the following code.

   ```html
   <head>
   <title>IU Webmaster redirect</title>
   </head>
   ```
6. Save the file and then close the View Reverse Proxy Management Root File window.

7. On the Deploy Pending Changes window, click Deploy to deploy the changes.

## Running the Solution

For this integration, SafeNet eToken PASS token is configured for authentication with the SAS solution. Before running the solution, ensure that Reverse Proxy/WebSEAL with Junction is up and running.

1. In a web browser, open the following reverse proxy protected resource URL:
   
   https://reverse proxy interface IP Address or FQDN of reverse proxy>/junction name

2. The IBM Security Access Manager login window is displayed. Enter your username and password which you crated in the local ISAM user registry.

3. After successful authentication, you will be redirected to the SafeNet Authentication Service login window. Complete the following fields, and then click Login.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Enter your user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passcode</td>
<td>Enter the SafeNet MobilePASS passcode.</td>
</tr>
</tbody>
</table>

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
4. After successful authentication, you will be redirected to the junction URL (for example, IP address of Reverse Proxy/WebSEAL>/safenet).

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>
</table>
| Address                     | Gemalto  
4690 Millennium Drive  
Belcamp, Maryland  21017 USA                                                 |
| Phone                       | United States  
1-800-545-6608  
International  
1-410-931-7520              |
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. |