SafeNet Authentication Service

Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Apache HTTP Server

gemalto
security to be free

Document Part Number: 007-012925-001, Rev. C

Release Date: June 2016

Contents

Third-Party Software Acknowledgement

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

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

Description

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

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

The Apache HTTP Server, colloquially called Apache, is the world's most widely-used web server software. Apache is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation. Most commonly used on a UNIX-like system, the software is available for a wide variety of operating systems, including UNIX, FreeBSD, Linux, Solaris, Novell NetWare, OS X, Microsoft Windows, OS/2, TPF, OpenVMS, and eComStation.

This document describes how to:

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

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

Apache HTTP Server can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet's cloud-based authentication service
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization

Environment

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

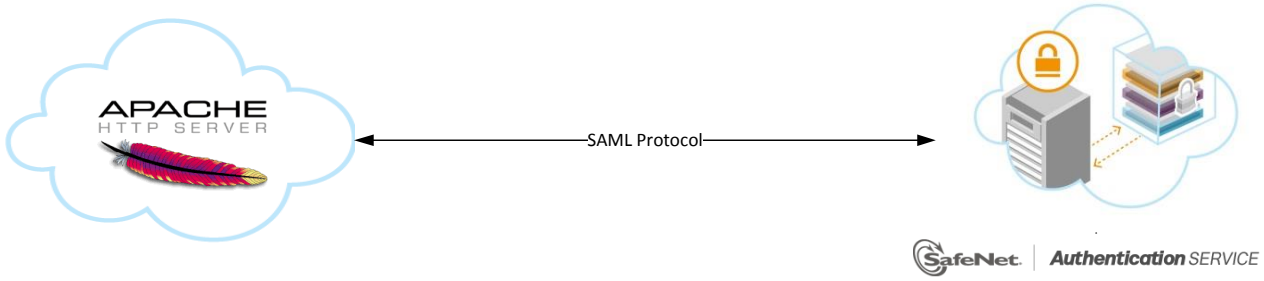
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)** — Mention only if SAS-PCE is relevant. Add version number to the SAS-PCE.
- **Apache HTTP Server 2.2.15**
- **Shibboleth SP 2.5.6 on CentOS 6.3**

Audience

This document is targeted to system administrators who are familiar with Apache HTTP Server, 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.

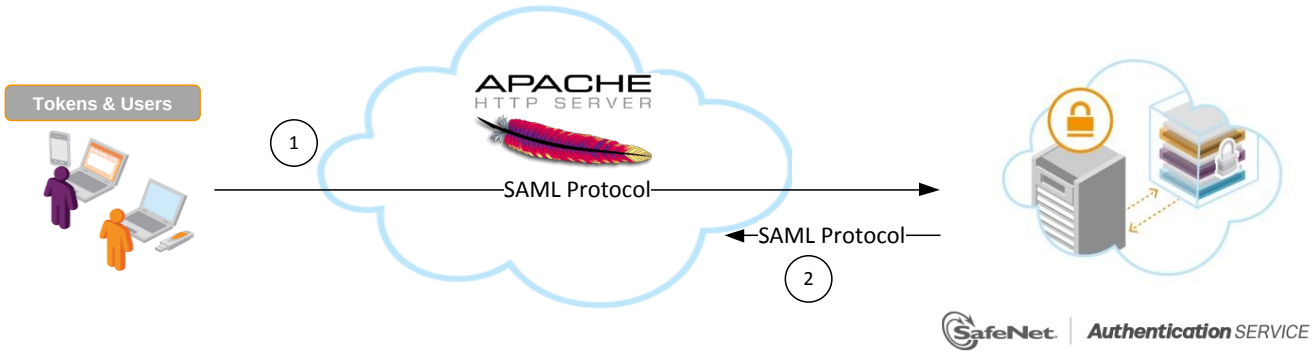
For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

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 Apache HTTP Server.



1. A user attempts to log on to Apache HTTP Server. The user is redirected to SafeNet Authentication Service. SAS collects and evaluates the user's credentials.
2. SAS returns a response to Apache HTTP Server, accepting or rejecting the user`s authentication request.

SAML Prerequisites

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

Configuring Apache HTTP Server

To add SafeNet Authentication Service (SAS) as an Identity Provider in Apache HTTP Server:

- Installing the Shibboleth Service Provider
- Configuring the Shibboleth Service Provider

Installing the Shibboleth Service Provider

The Apache HTTP Server itself cannot act as a Service Provider for SAML. Therefore, you need to install the Shibboleth Service Provider.

1. Log in to Apache HTTP Server as a root user.
2. Run the following commands:

cd /etc/yum.repos.d

wget http://download.opensuse.org/repositories/security://shibboleth/CentOS_CentOS-6/security:shibboleth.repo

yum install -y shibboleth

Configuring the Shibboleth Service Provider

Configure the Shibboleth Service Provider and add SAS as an Identity Provider.

To configure the Shibboleth Service Provider:

1. From the /etc/httpd/conf.d location, edit the shib.conf file as follows:

   ```
   LoadModule mod_shib /usr/lib/shibboleth/mod_shib_22.so
   UseCanonicalName On
   <IfModule mod_alias.c>
     <Location /shibboleth-sp>
       Allow from all
     </Location>
     Alias /shibboleth-sp/main.css /usr/share/shibboleth/main.css
   </IfModule>
   <Location /secure>
   AuthType shibboleth
   ShibRequestSetting requireSession 1
   require valid-user
   </Location>
   ```

   where, in <Location /secure>, secure is the location of the web page (including the filename) on which SAML authentication is applied. For example, if /var/www/html is the location where the website is hosted, and you replaced secure with my_secure/my_website.html, the resultant path will be /var/www/html/my_secure/my_website.html on which SAML authentication will be applied. In this case, my_website.html is the name of the web page.

2. From the **/etc/selinux** location, edit the config file, and set the following:

   SELINUX=permissive

3. Save and close the **config** file, and then run the following command:

   setenforce 0

4. From the /etc/shibboleth location, edit the **attribute-map.xml** file as follows:

   configure the id tag with a uid (can be any value)

   ```
   <Attribute name="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" id="sasuid">
      <AttributeDecoder xsi:type="NameIDAttributeDecoder"
            formatter="$NameQualifier!$SPNameQualifier!$Name" defaultQualifiers="true"/>
   </Attribute>
   ```

5. From the /etc/shibboleth location, edit the **shibboleth2.xml** file as follows:

    a. Update the ApplicationDefaults element as below. Replace DNS or IP of Apache with the DNS or IP address of the Apache HTTP Server. Configure the **REMOTE_USER** field with the **uid** created previously in section 4:

    <ApplicationDefaults entityID="**Error! Hyperlink reference not valid.**"
    REMOTE_USER="sasuid">

    <SSO entityID="https://idp1.cryptocard.com/idp/shibboleth">
    SAML2 SAML1
    </SSO>

    b. Uncomment the MetadataProvider element and update as below. The **SafeNet-Idp-Metadata.xml** file is the SAS metadata file present at **/etc/shibboleth**. To download the SAS metadata, go to **https://idp1.cryptocard.com/idp/shibboleth**:

    <MetadataProvider type="XML" file="SafeNet-Idp-Metadata.xml" reloadInterval="7200">
    </MetadataProvider>

6. Save and close the **shibboleth2.xml** file.

7. Run the following commands to restart the Apache and Shibboleth services:

    service httpd restart

    service shibd restart

Downloading the SafeNet Authentication Service Metadata

Browse to the **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** URL. The SafeNet identity provider certificate will automatically download. Save it locally on your machine.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Apache HTTP Server using SAML authentication requires:

- Enabling SAML Services in SafeNet Authentication Service, page 14

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*:

http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/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 Apache HTTP Server.

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.

http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Account_Operator_Guide/

Adding Apache HTTP Server as a Service Provider (SP) in SafeNet Authentication Service

Add a service provider entry in the SafeNet Authentication Service (SAS) **SAML Service Providers** module to prepare it to receive SAML authentication requests from Apache HTTP Server. You will need the metadata of Apache HTTP Server.

To download the Apache HTTP Server metadata:

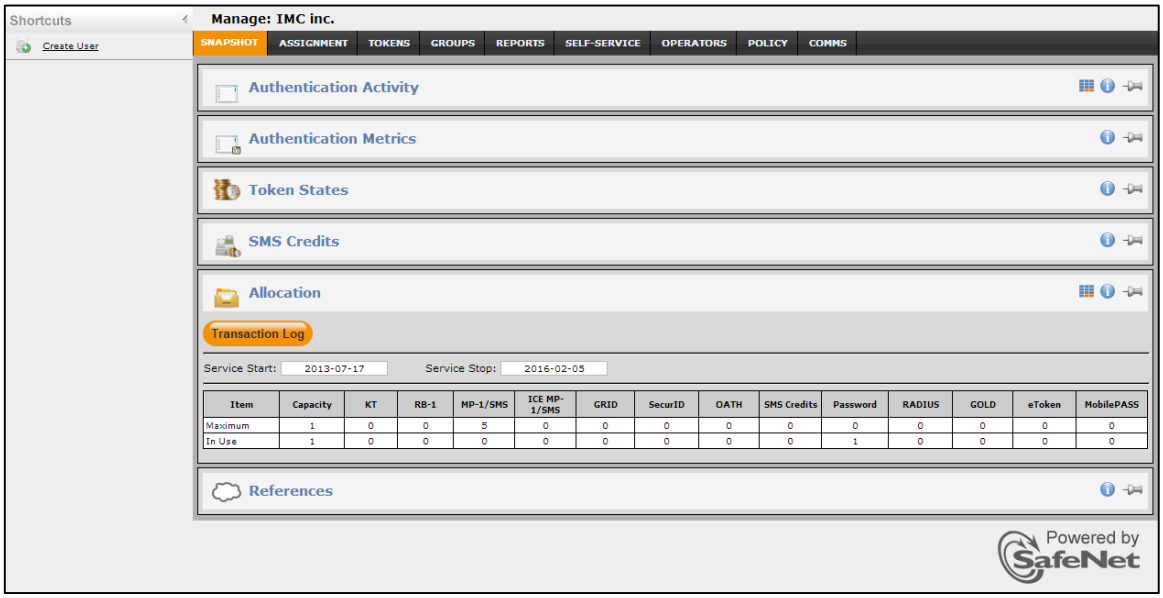
You can download the Apache HTTP Server metadata using one of the following methods:

- If the website to be protected is hosted on **HTTPS**, browse to the following URL: **https://<DNS or IP of Apache>/Shibboleth.sso/Metadata**
- If the website to be protected is hosted on **HTTP**, browse to the following URL: **http://<DNS or IP of Apache>/Shibboleth.sso/Metadata**

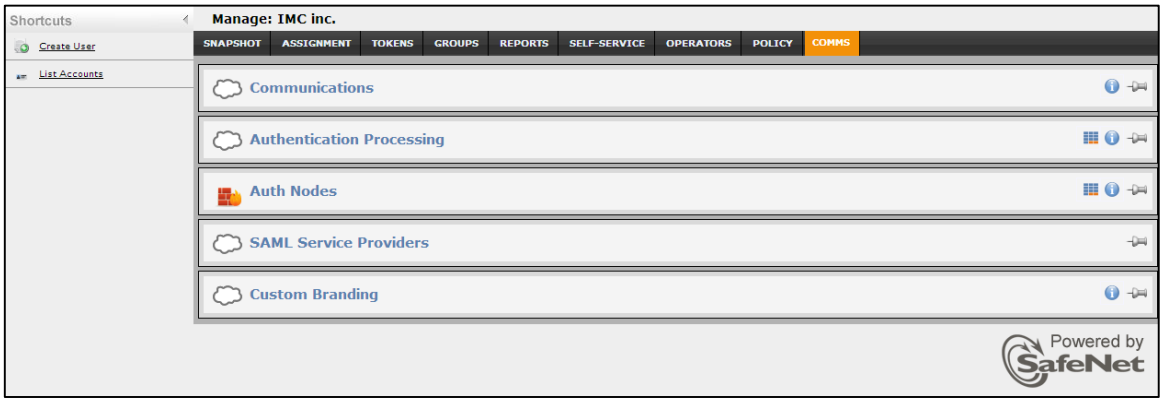
Replace **DNS** or **IP** of Apache with the DNS or IP address of the Apache HTTP Server. The metadata will get downloaded automatically. Save it with the **.xml** extension (for example, **metadata.xml**).

To add Apache HTTP Server as a Service Provider in SafeNet Authentication Service**:**

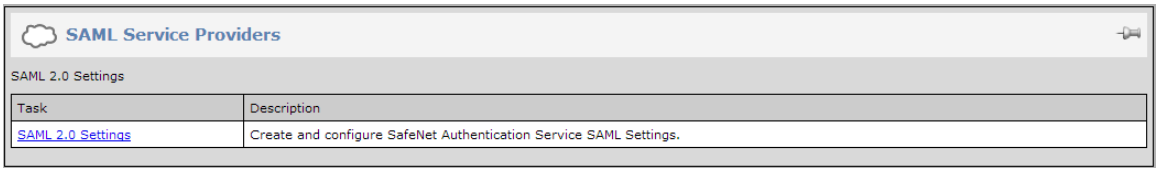
1. Log in to the SafeNet Authentication Service console with an Operator account.



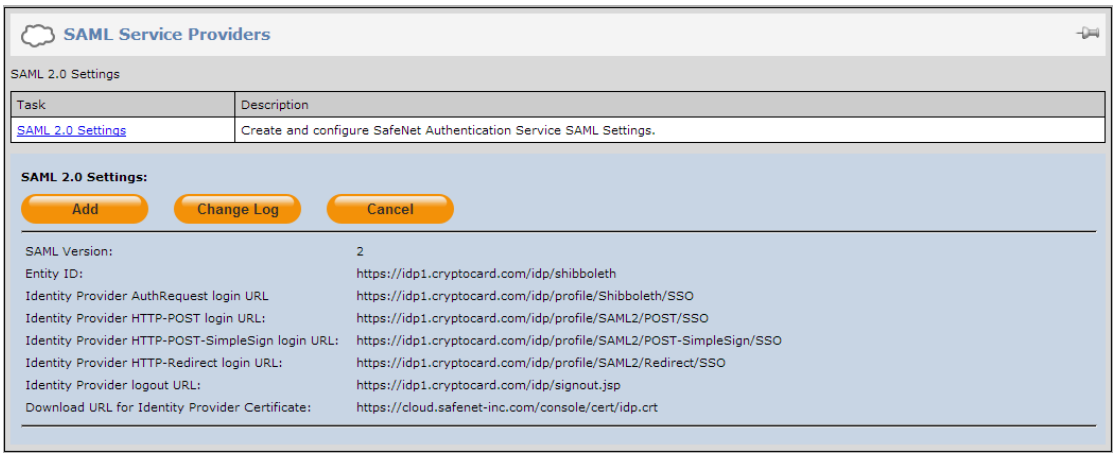
2. Click the **COMMS** tab, and then click **SAML Service Providers**.



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

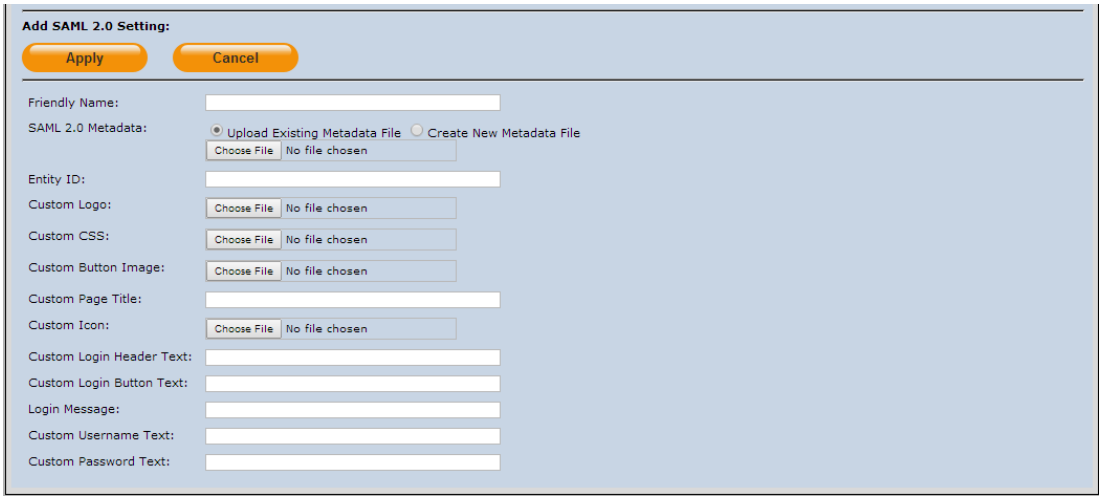


4. Click **Add**.



5. Under **Add SAML 2.0 Settings**, complete the following fields:

Friendly Name	Enter the Apache HTTP Server name.
SAML 2.0 Metadata	Select **Upload Existing Metadata File**. Click the **Choose File** button, select the Service Provider`s metadata file, and then click **Open**.

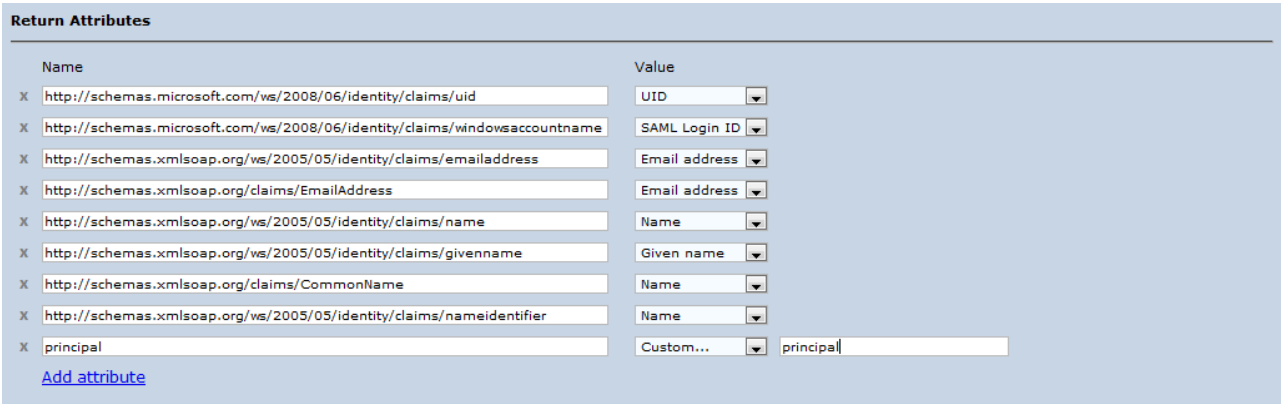


NOTE: The remaining options are used to customize the appearance of the logon page presented to the user. For more information on logon page customization, refer “Configure SAML Service” in the *SAML Configuration Guide*:

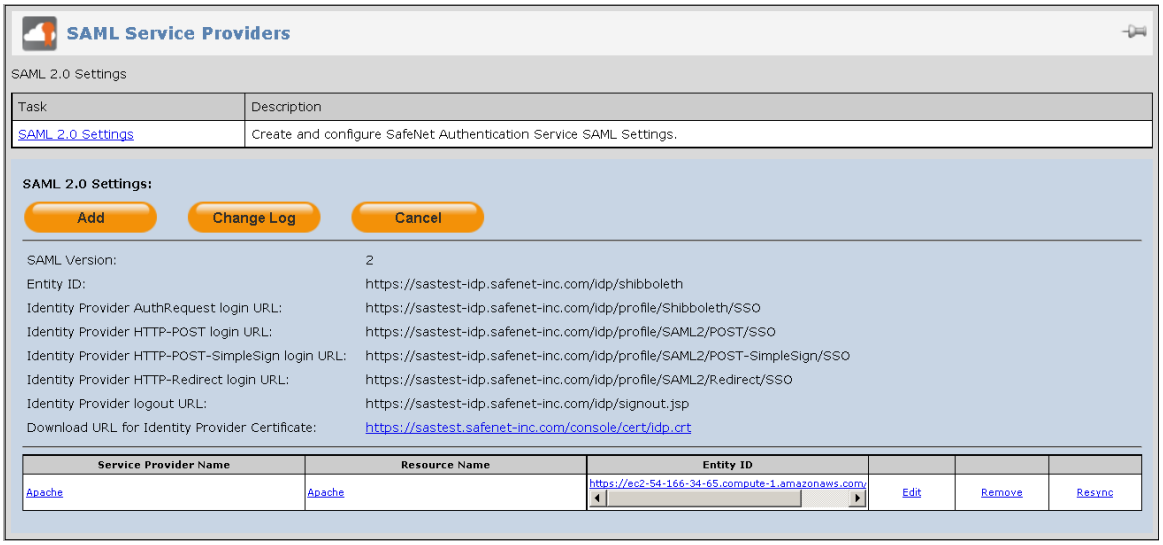
http://www2.safenet-inc.com/sas/implementation-guides/sas-on-prem/SAS-QS-SAML.pdf

Under **Return Attributes**, add the following attributes, and then click **Apply:**

Name	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/uid	According to ThirdParty Product Requirements
http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname	According to ThirdParty Product Requirements
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	According to ThirdParty Product Requirements
http://schemas.xmlsoap.org/claims/EmailAddress	According to ThirdParty Product Requirements
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	According to ThirdParty Product Requirements
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	According to ThirdParty Product Requirements
http://schemas.xmlsoap.org/claims/CommonName	According to ThirdParty Product Requirements
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	According to ThirdParty Product Requirements
principal	According to ThirdParty Product Requirements



Apache HTTP Server is added as a service provider in the system.



Enabling SAML Services in SafeNet Authentication Service

After Apache HTTP Server has been added to SafeNet Authentication Service (SAS) as a service provider, the users should be granted permission to use this service provider with SAML authentication.

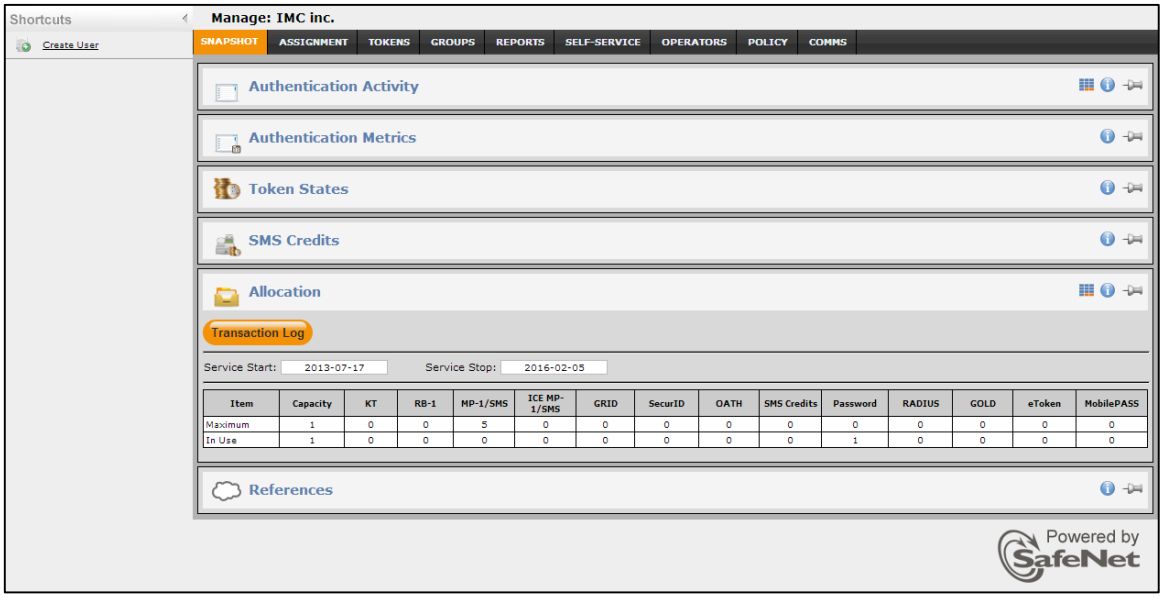
There are two methods to enable the user to use the service provider:

- Manually, one user at a time, using SAML Services module
- Automatically, by defining groups of users, using SAML Provisioning Rules

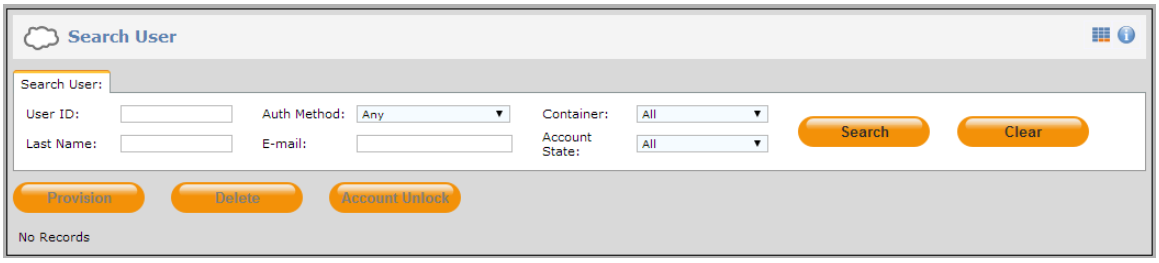
Using the SAML Services Module

Manually enable a single user to authenticate against one or more configured SAML Service providers.

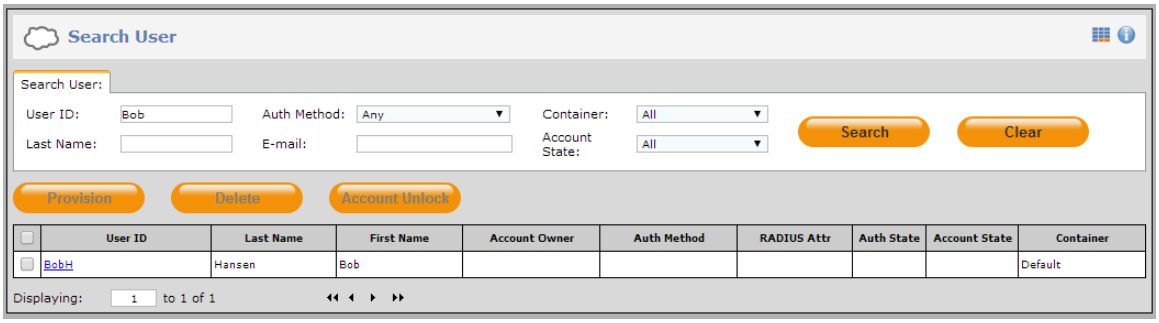
1. Log in to the SafeNet Authentication Service console with an Operator account.



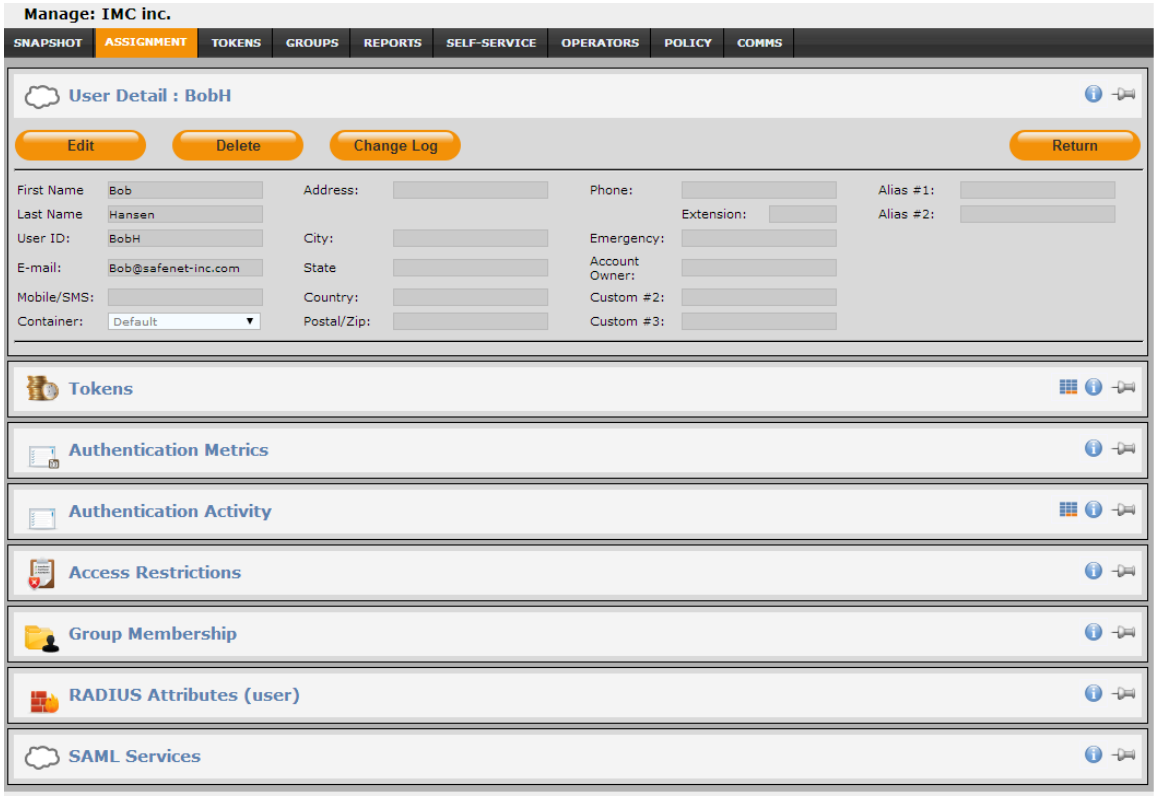
2. Click the **ASSIGNMENT** tab, and then search for the required user.



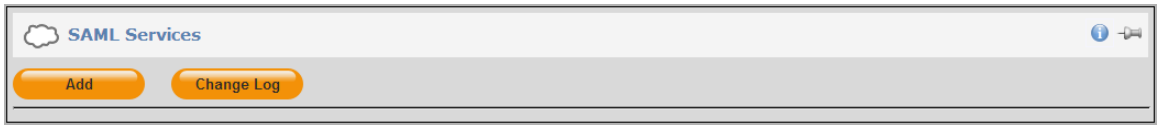
3. Click the appropriate user in the **User ID** column.



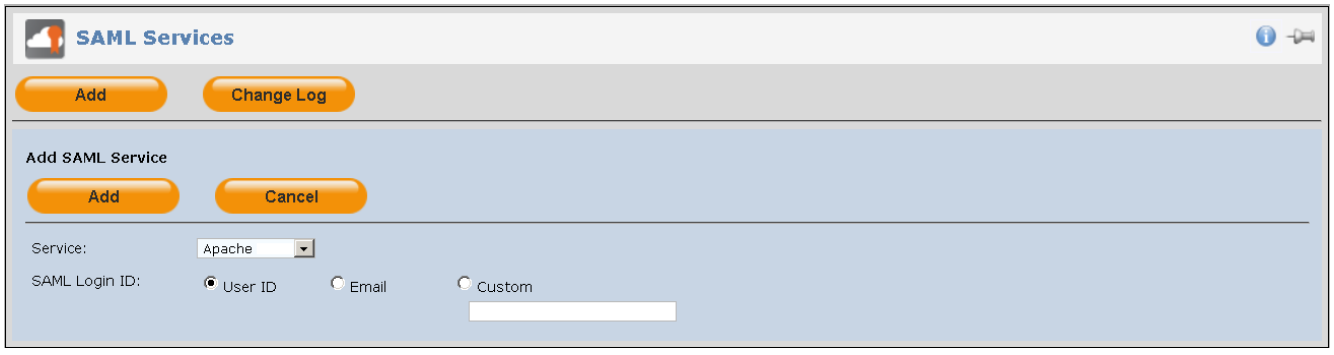
4. Click **SAML Services**.



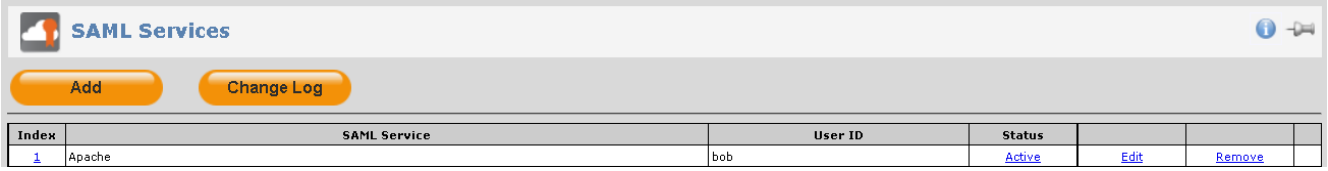
5. Click **Add**.



6. Under **Add SAML Service**, do the following:
   a. From the **Service** menu, select the Apache HTTP Server 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 UserID to Apache HTTP Server in the response.
   c. Click **Add**.



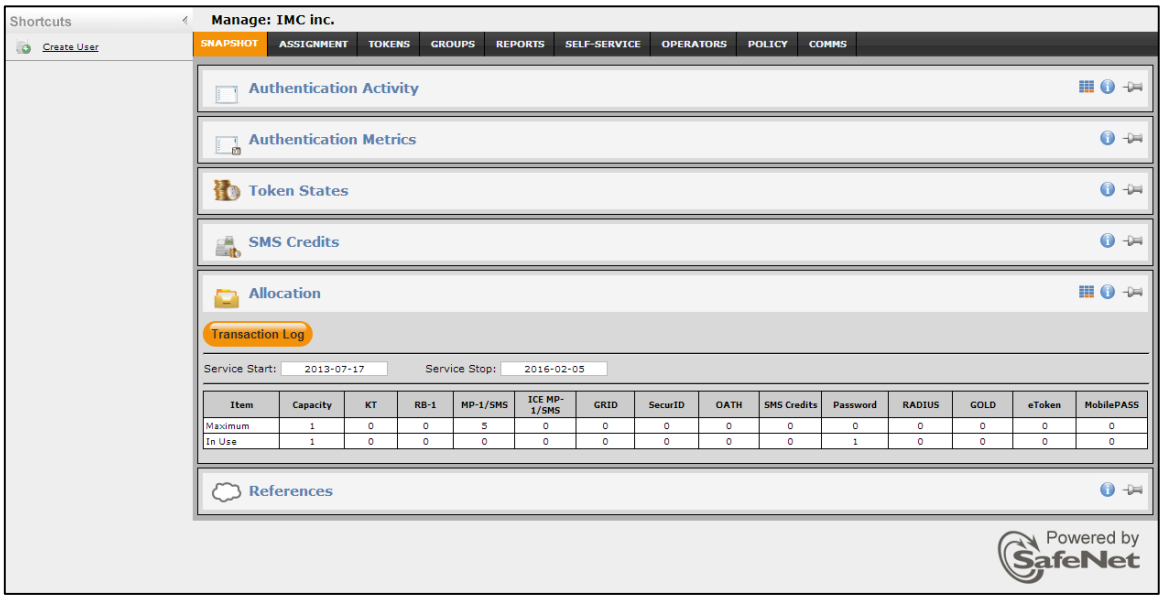
The user can now authenticate to Apache HTTP Server using SAML authentication.



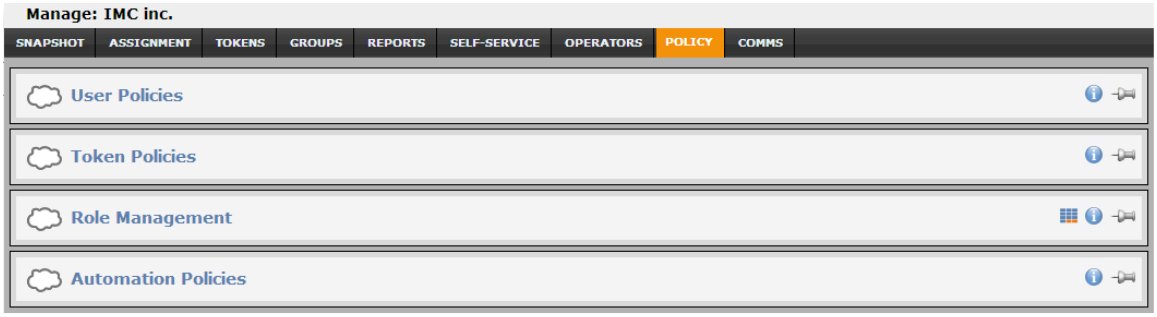
Using SAML Provisioning Rules

Use this module to enable groups of users to authenticate to SAML service providers.

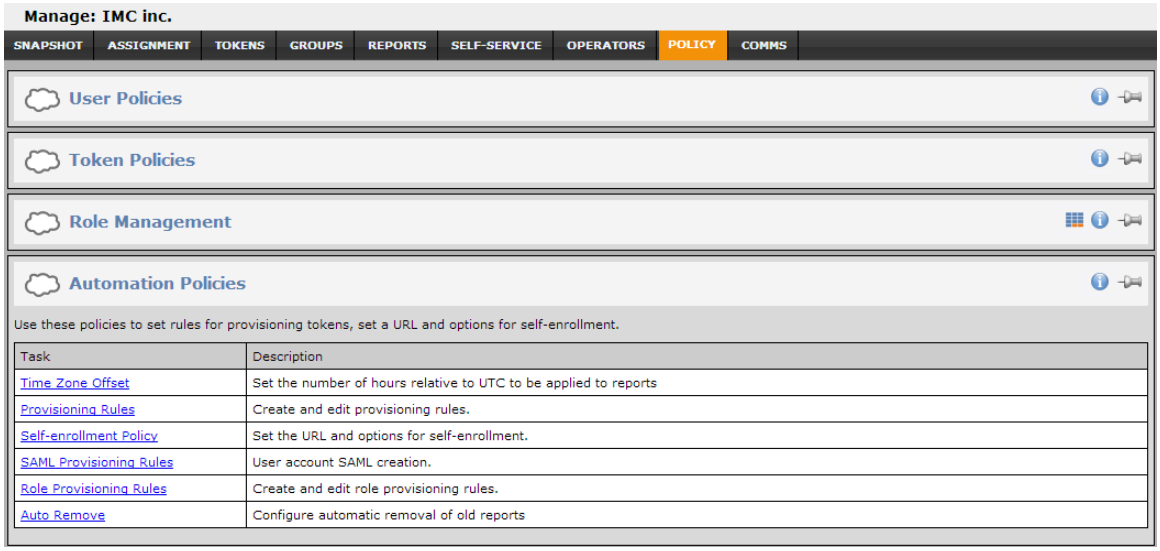
1. Log in to the SafeNet Authentication Service console with an Operator account.



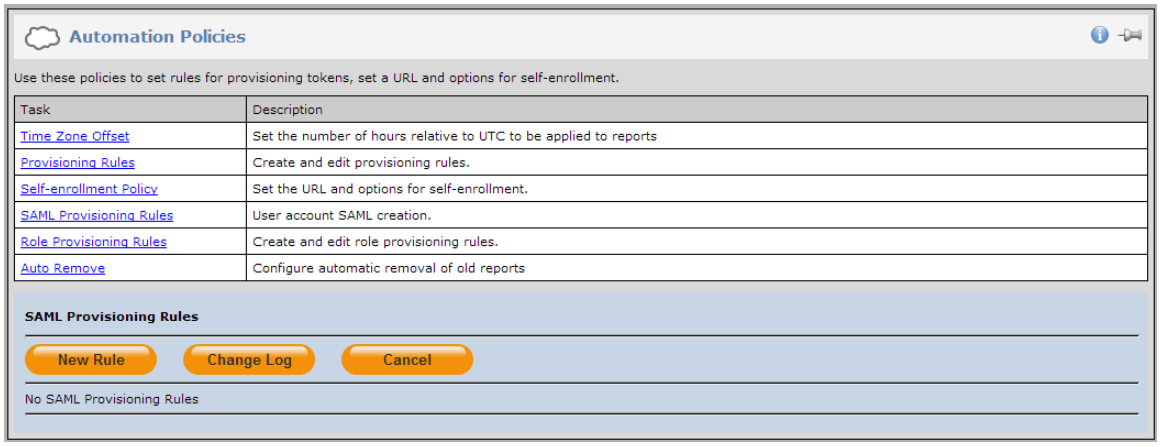
2. Click the **POLICY** tab, and then click **Automation Policies**.



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

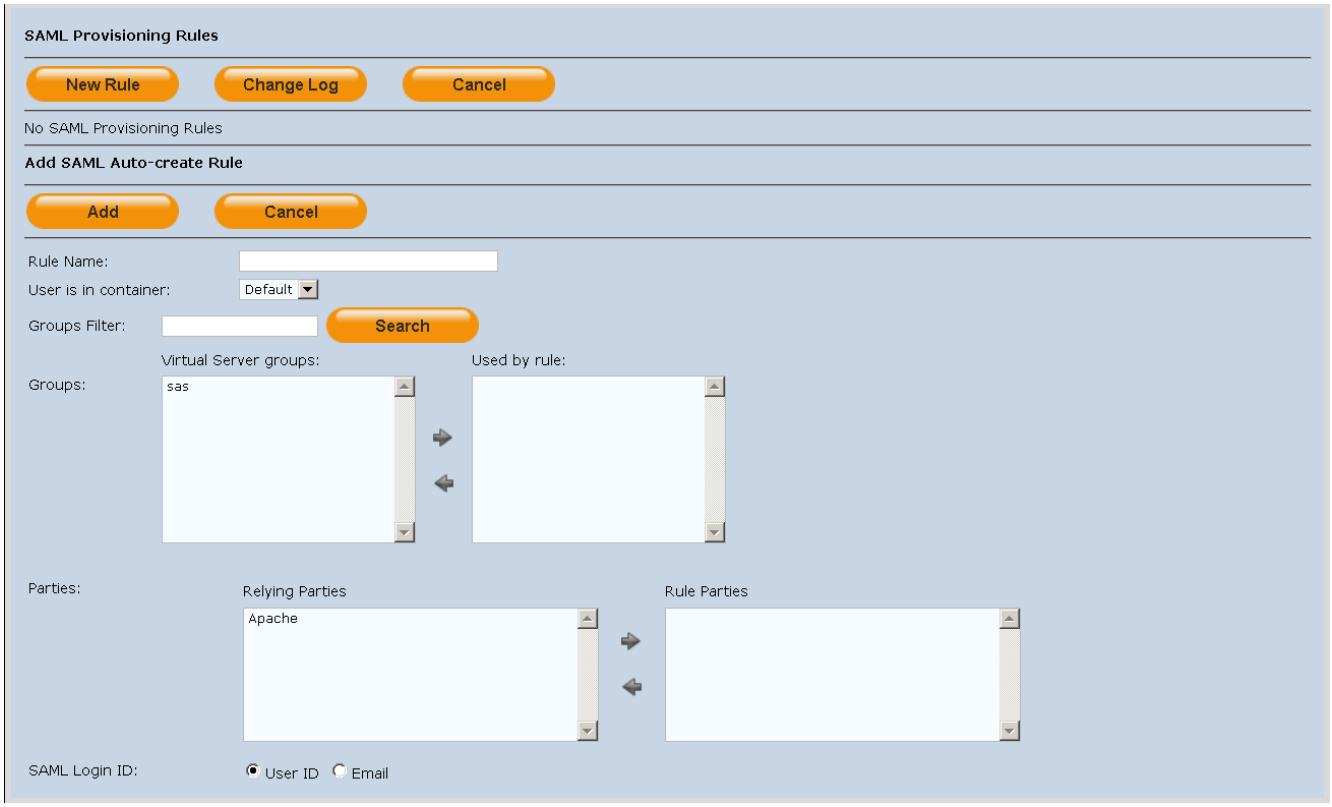


4. Click **New Rule**.



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

Rule Name	Enter a name for the rule.
User is in container	Users affected by this rule must be in the selected container.
Groups	The **Virtual Server groups** 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 **Used by rule** box.
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.

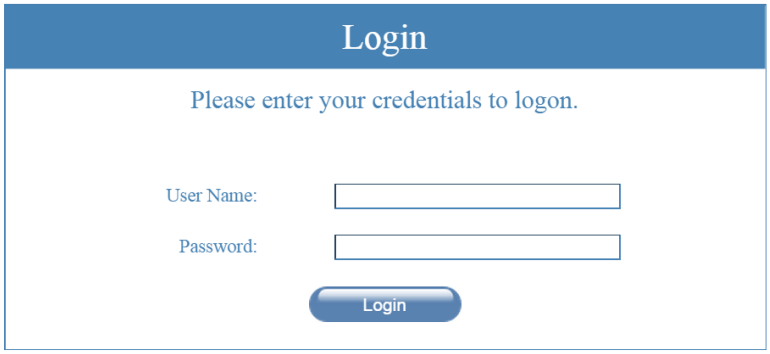


Running the Solution

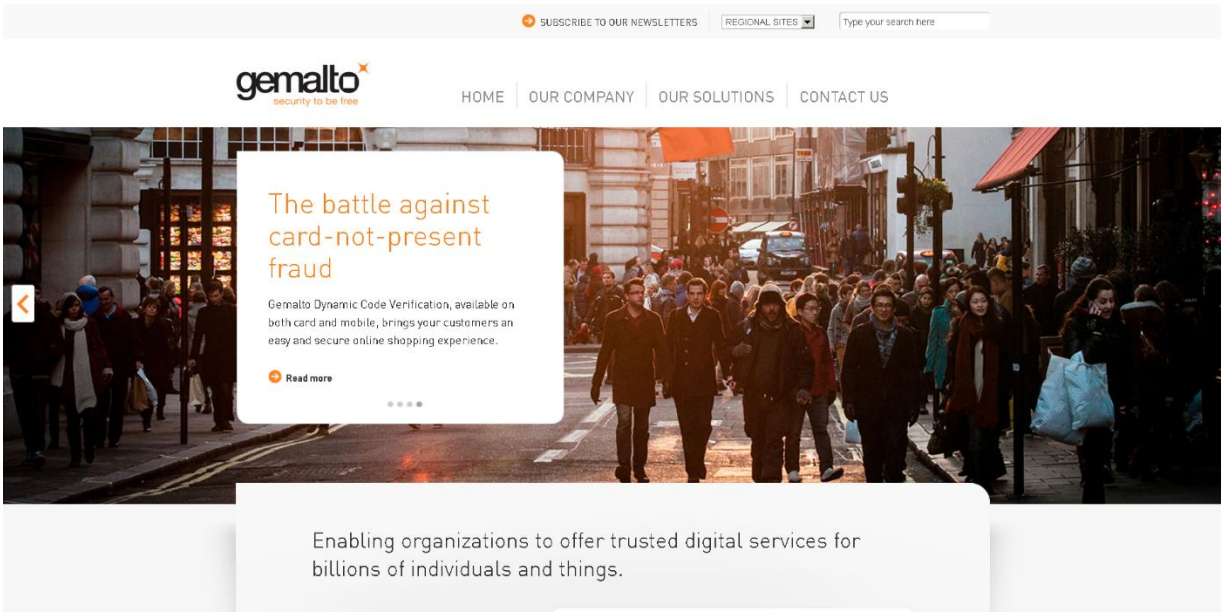
After successfully installing the Shibboleth Service Provider and configuring the Apache HTTP Server for SAML authentication, verify the integration solution.

For this integration, the SafeNet eToken PASS is configured for authentication with the SAS solution.

1. In a web browser, open the website you have protected. You will be redirected to the SAS Login page.
2. On the SAS **Login** page, in the **User Name** field, enter your user name.



3. Using the SafeNet eToken PASS, generate an OTP, and then enter it in the **Password** field.
4. Click **Login**.
   If the credentials are valid, you will be redirected to the protected website.



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.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com 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.	