SafeNet Authentication Service

Integration Guide

Using SAS as an Identity Provider for PingOne

Document Information

Document Part Number	007-012994-001, Rev. A
Release Date	April 2015

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Third-Party Software Acknowledgement

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

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.

PingOne® is an Identity-as-a-Service (IDaaS) solution that enables organizations to deliver single sign-on (SSO) for users with just one user name and password—eliminating multiple password security problems. PingOne delivers SSO to all of the applications your users need while increasing security for your organization.

This document describes how to:

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

This document assumes that the PingOne environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

PingOne can be configured to support multi-factor authentication in several modes. 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**—SafeNet's cloud-based authentication service.

Environment

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

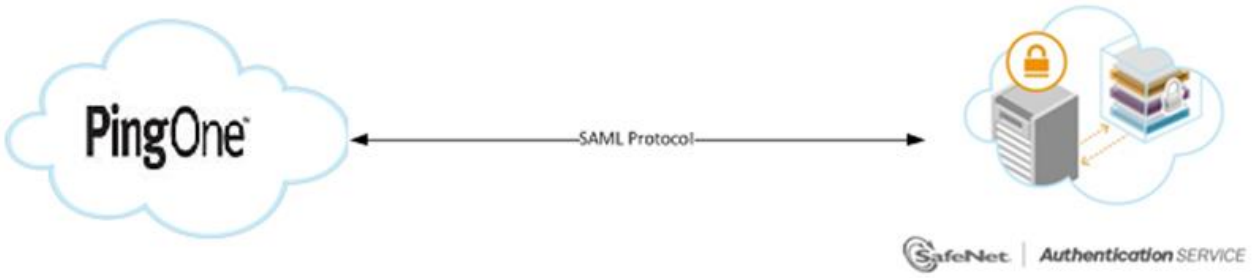
- **SafeNet Authentication Service**
- **PingOne** (**on cloud)**

Audience

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

SAML Authentication using SAS Cloud

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 Dataflow using SAS

SafeNet Authentication Service communicates with a large number of Service Providers and cloud-based service solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for PingOne.

1. A user attempts to log on to PingOne. The user is asked to enter the Active Directory credentials.
2. After successful authentication of Active Directory credentials, the user is redirected to SafeNet Authentication Service (SAS). SAS collects and evaluates the user's credentials.
3. SAS returns a response to PingOne, accepting or rejecting the user's authentication request.

SAML Prerequisites

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

Configuring PingOne

Configuring PingOne requires the following:

- Configuring SAS for Secondary Authentication, page 6
- Downloading the PingOne Metadata File, page 9

Configuring SAS for Secondary Authentication

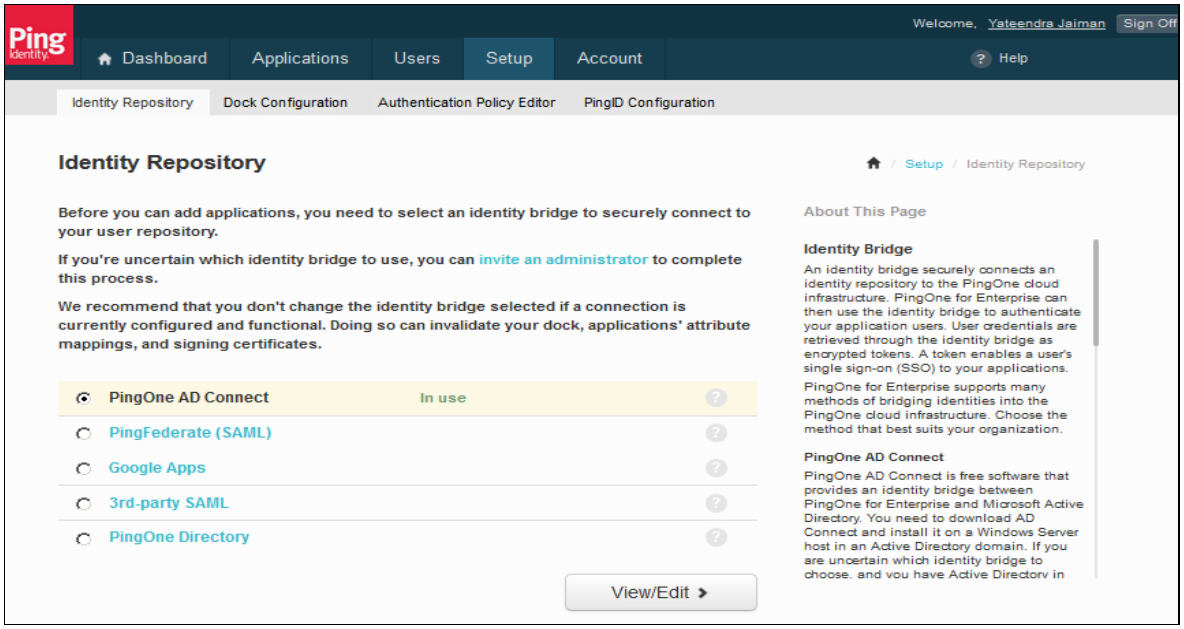
To configure SAS for secondary authentication, PingOne should be configured for primary authentication with any of the supported identity bridges.

PingOne for Enterprise supports many methods of bridging identities into the PingOne cloud infrastructure. Choose the method that best suits your organization. In this integration guide, we have chosen PingOne AD Connect for primary authentication.

NOTE: To configure Active Directory as the primary level of authentication in PingOne, refer to the PingOne documentation for AD Connect installation: http://documentation.pingidentity.com/pingone/employeeSsoAdminGuide/#connectAdcAgent.html

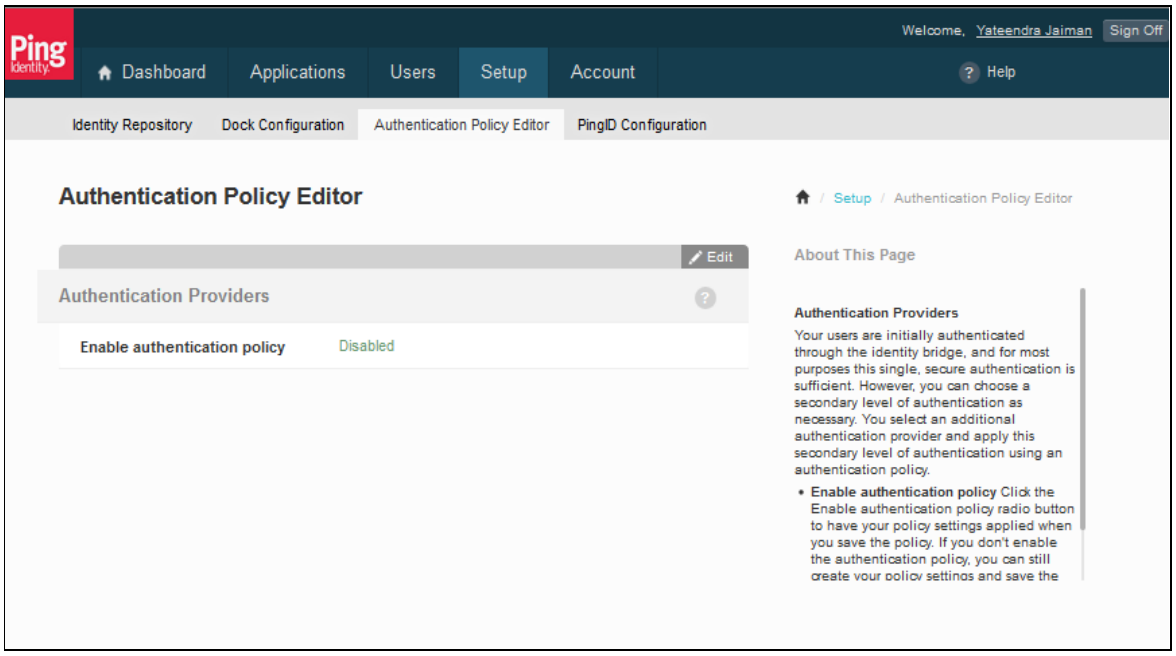
1. In a web browser, open the following URL and log in with administrator credentials:

   https://admin.pingone.com



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

2. Click **Setup** > **Authentication Policy Editor**.



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

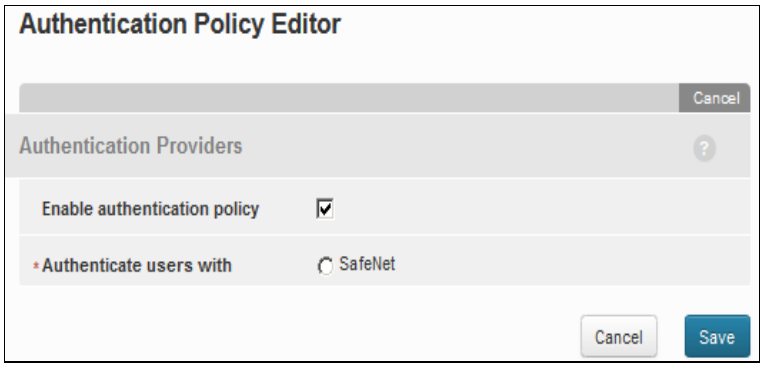
3. On the **Authentication Policy Editor** window, in the **Authentication Providers** section, click **Edit**

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

4. Select **Enable authentication policy**.

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

5. The **Authenticate users with** option is displayed. Select **SafeNet**.



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

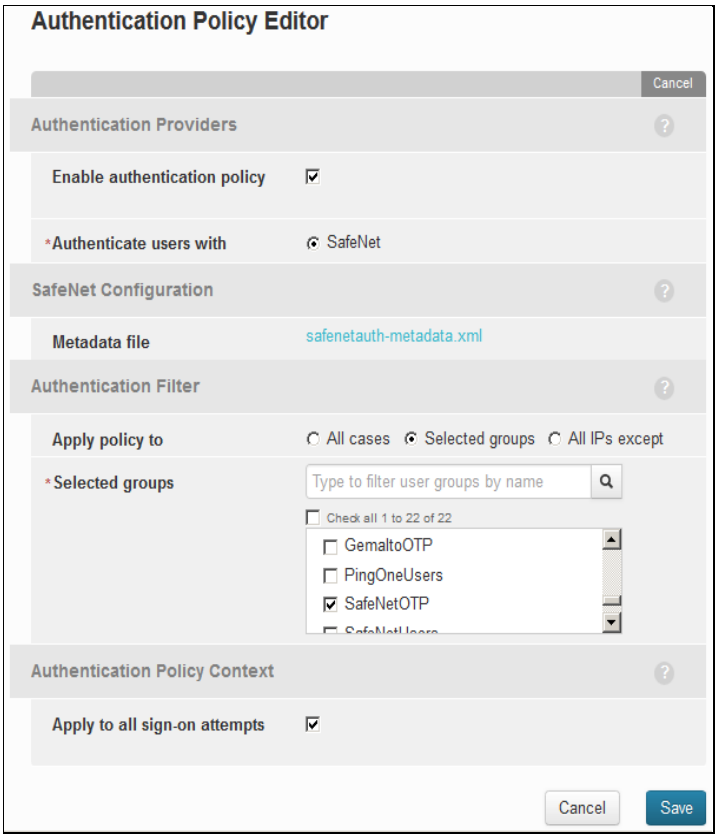
6. More sections are displayed under **Authentication Policy Editor**. Perform the following steps:

   a. In the **Authentication Filter** section, select a filter to define how the policy is to be applied as per user needs.

      For this integration, select **Selected groups**, and then select **SafeNetOTP**.

   b. In the **Authentication Policy Context** section, select the user context in which the policy is to be applied.

      For this integration, select **Apply to all Sign-on attempts**. Refer to the PingOne documentation for more details.



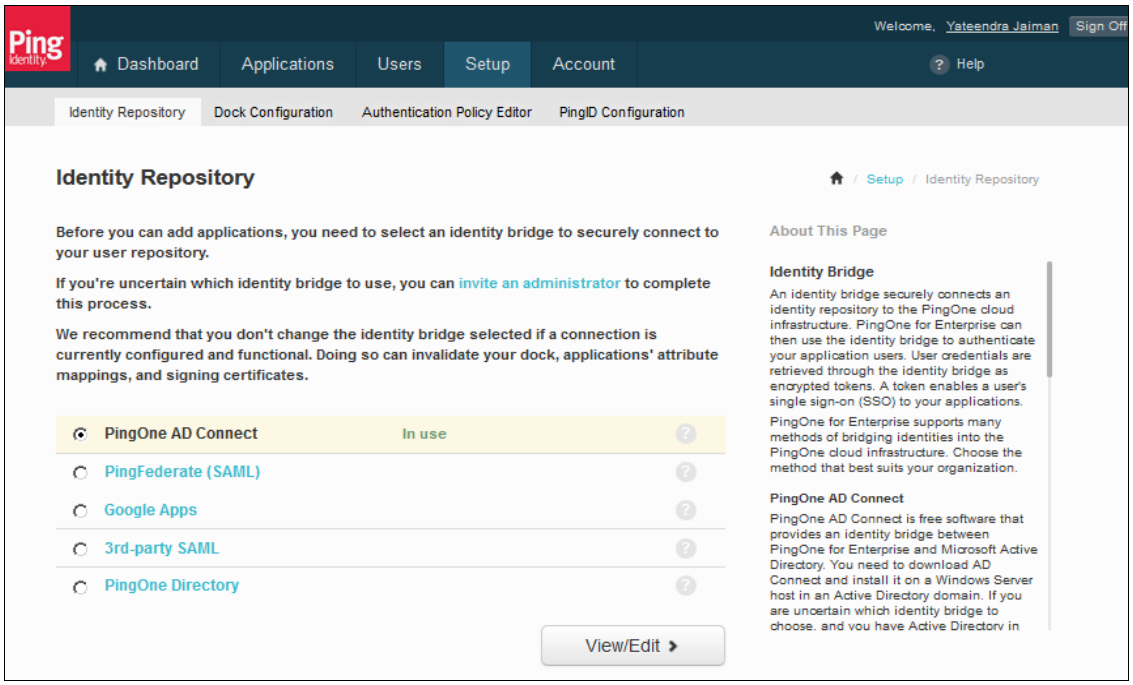
(The screen image above is from Ping Identity® software. Trademarks are the property of their respective owners.)

7. Click **Save**.

Downloading the PingOne Metadata File

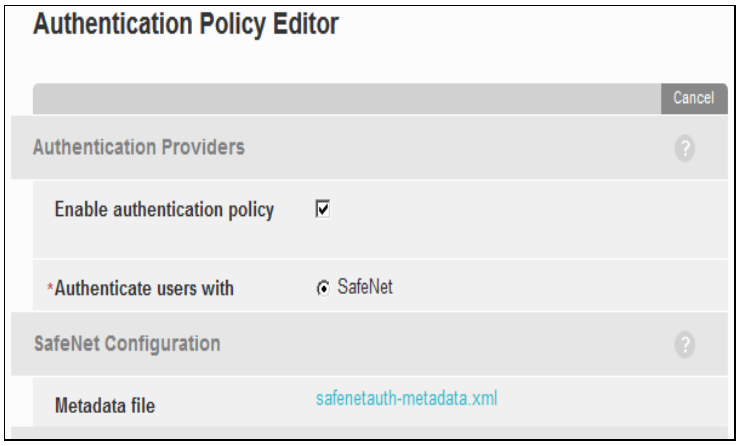
1. In a web browser, open the following URL and log in with administrator credentials:

   https://admin.pingone.com



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

2. Click **Setup** > **Authentication Policy Editor**.
3. On the **Authentication Policy Editor** window, in the **SafeNet Configuration** section, click the **safenetauth-metadata.xml** link to download the PingOne metadata file. This metadata file will be required during SAS configuration.



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

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with PingOne using SAML authentication requires:

- Synchronizing Users Stores to SAS, page 10
- Assigning Authenticators in SAS, page 10
- Adding PingOne as a Service Provider (SP) in SAS, page 11
- Enabling SAML Services in SAS, page 13

Synchronizing Users Stores to SAS

Before 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 SAS, refer to creating users in the *SafeNet Authentication Service Subscriber Account Operator Guide*:

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

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

Assigning Authenticators in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users authenticating through PingOne.

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:

- **Manually provision** – 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 rules” in the *SafeNet Authentication Service - Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SafeNet Authentication Service user store.

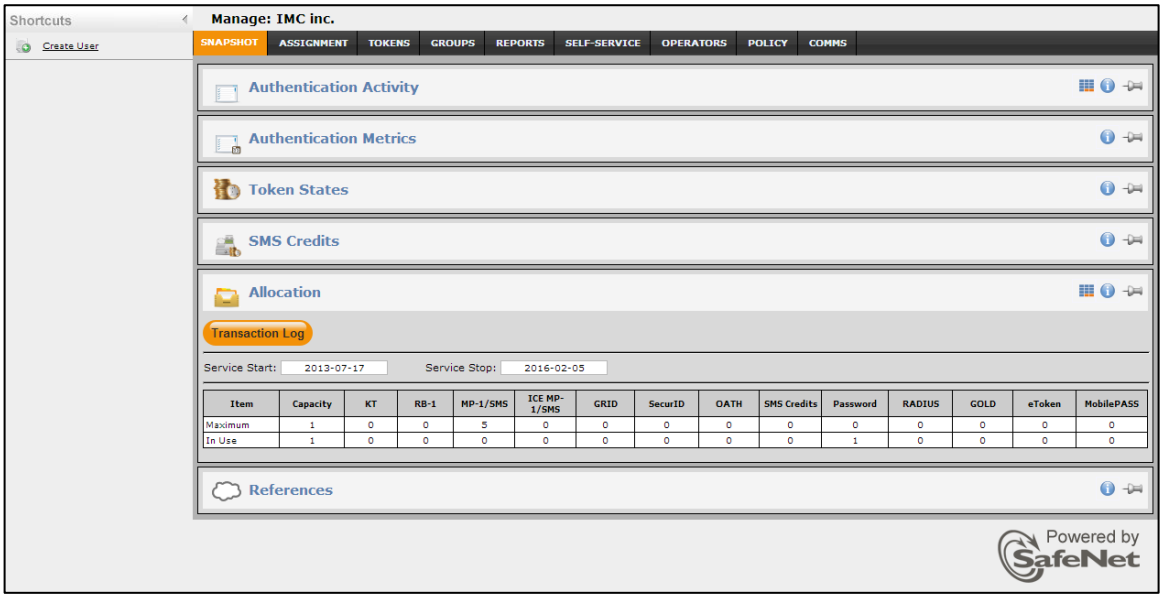
http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

Adding PingOne as a Service Provider (SP) in SAS

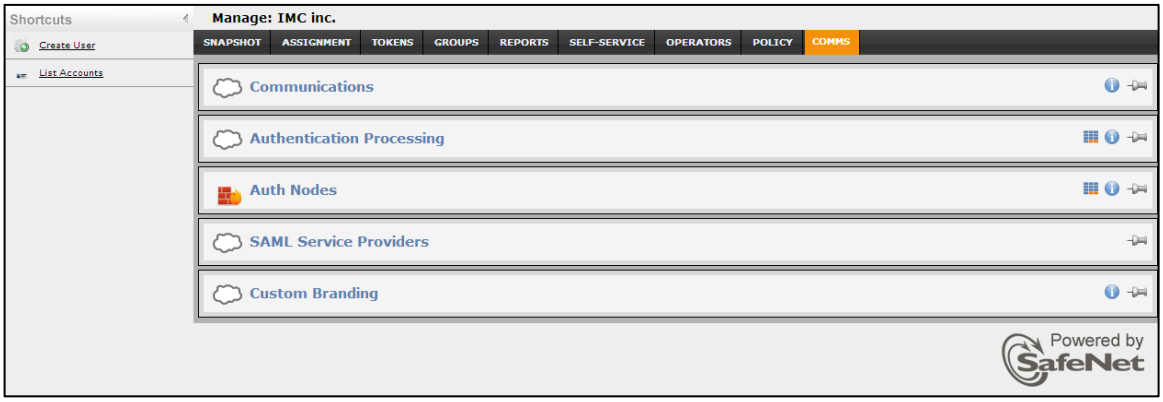
Add a Service Provider entry in the SAS **SAML Service Providers** module to prepare it to receive SAML authentication requests from PingOne.

To add PingOne as a Service Provider in SAS:

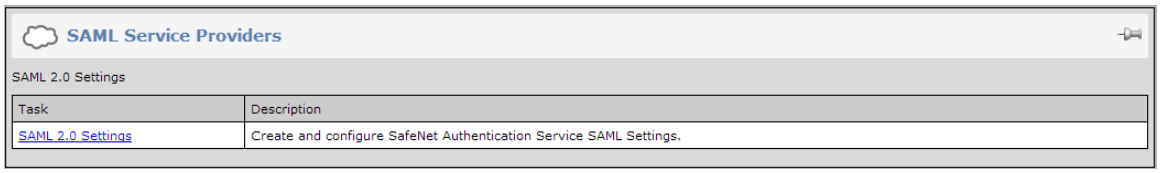
1. Log in to the SAS console with an Operator account.



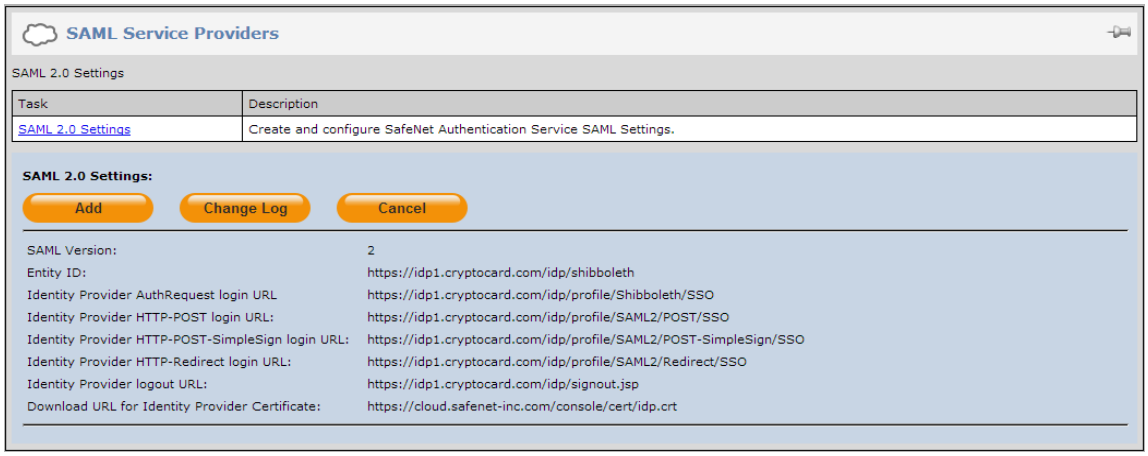
2. Click the **COMMS** tab, and then click **SAML Service Providers**.



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

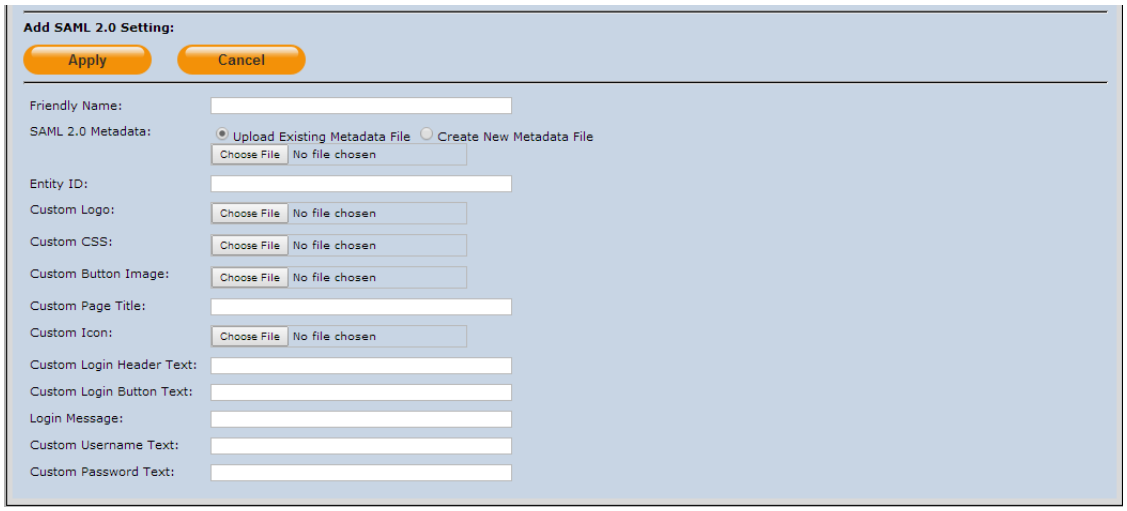


4. Under **SAML 2.0 Settings**, click **Add**.



5. In the **Add SAML 2.0 Settings** section, complete the following fields, and then click **Apply**:

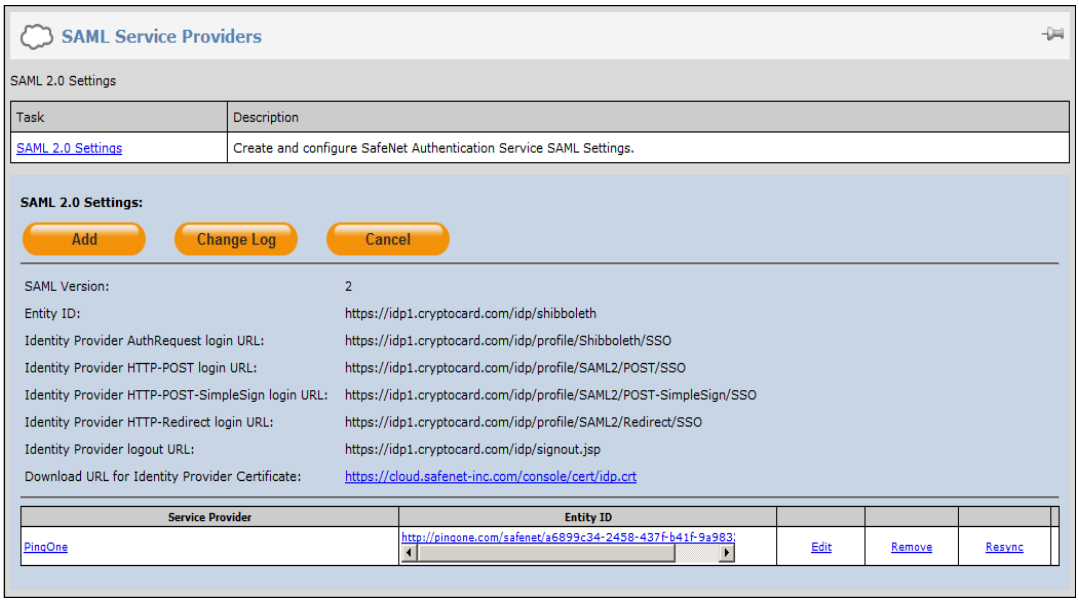
Friendly Name	Enter the PingOne name.
SAML 2.0 Metadata	You have downloaded the PingOne metadata file in the section “Downloading the PingOne Metadata File” on page 9. Select **Upload Existing Metadata File**. Click the **Choose File** button, select the Service Provider`s (PingOne) metadata file, and then click **Open**.



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 to “Configure SAML Service” in the *SAML Configuration Guide*:

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

PingOne is added as a Service Provider in the system.



Enabling SAML Services in SAS

After PingOne has been added to SAS as a Service Provider, users should be granted permission to use this Service Provider with SAML authentication.

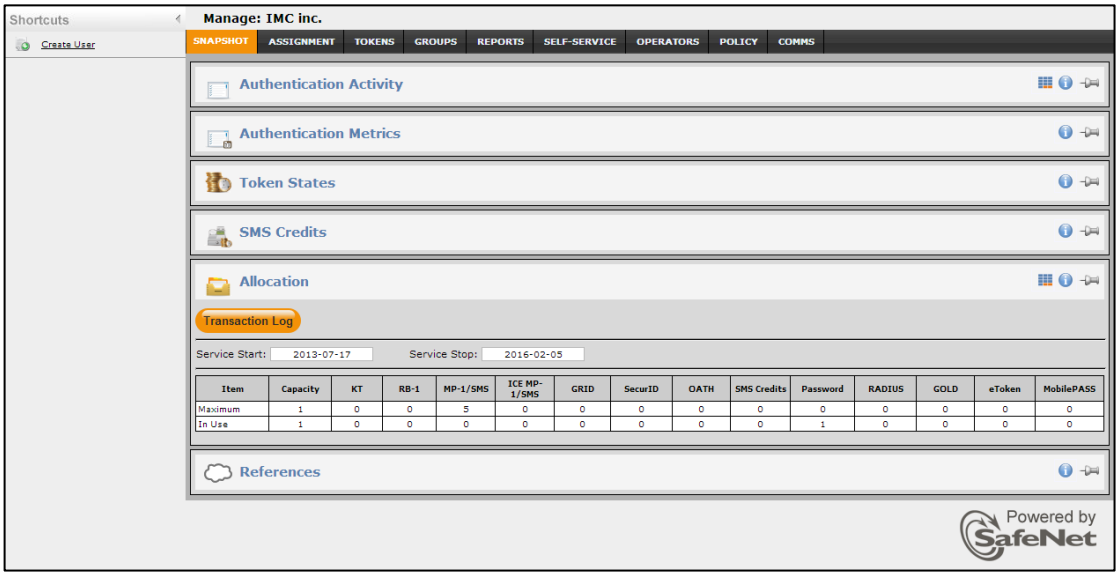
There are two methods to enable the user to use the Service Provider:

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

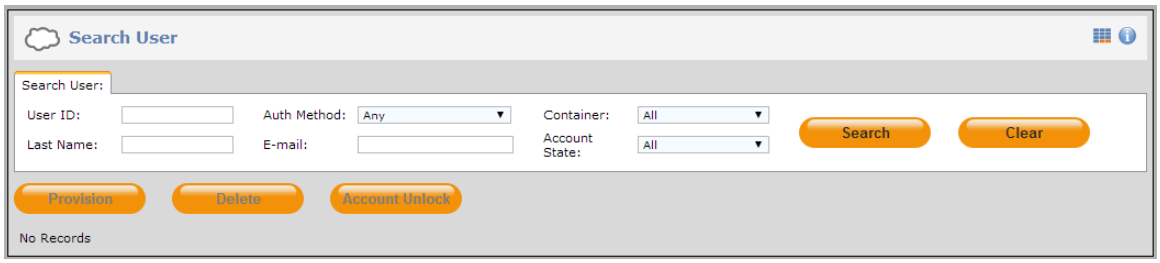
Using the SAML Services Module

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

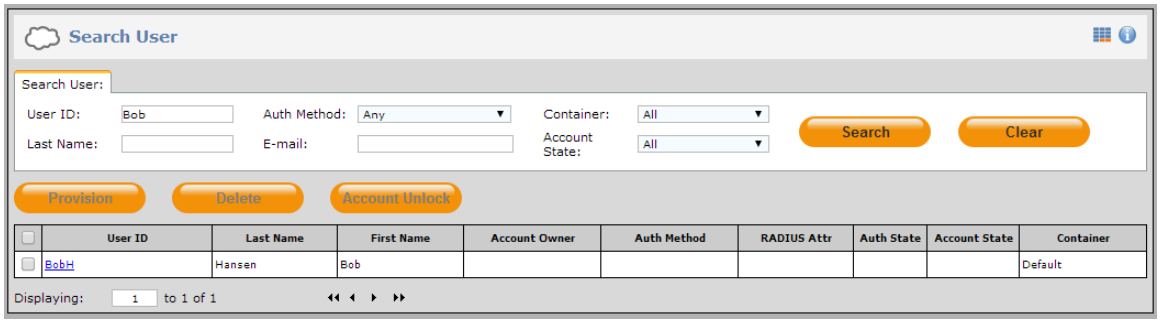
1. Log in to the SAS console with an Operator account.



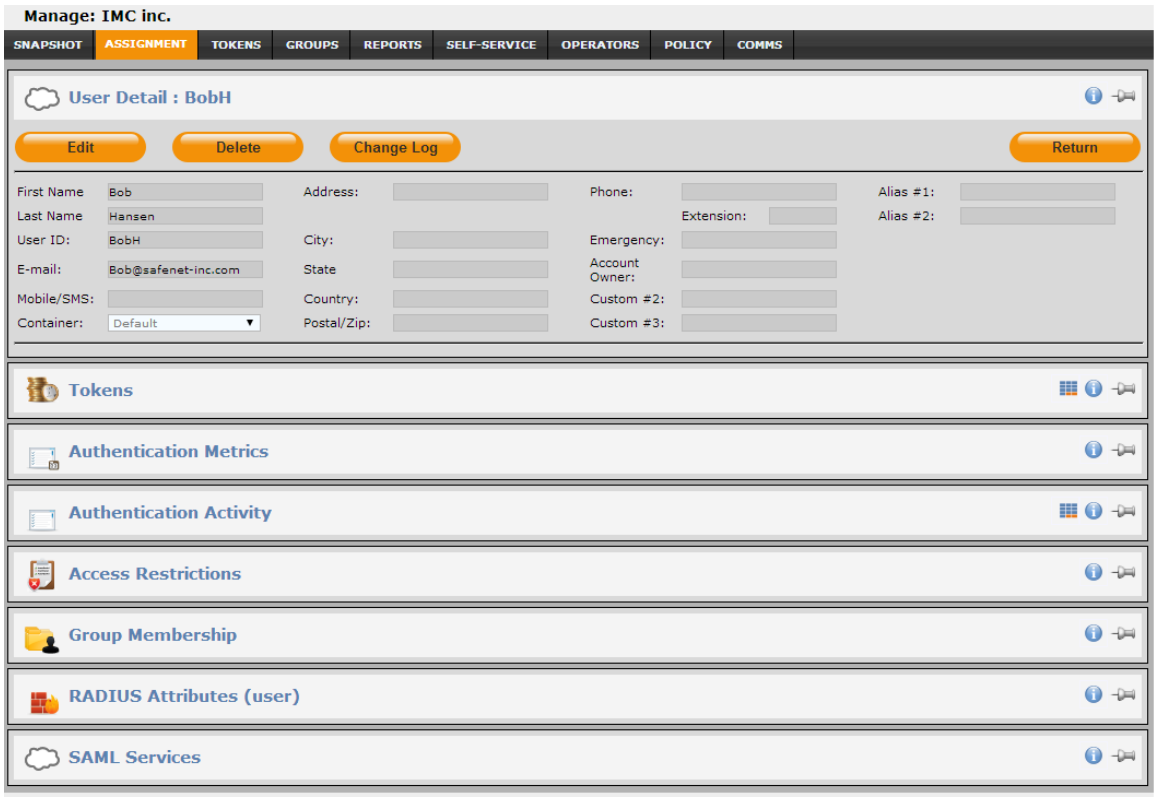
2. Click the **Assignment** tab and search for the required user.



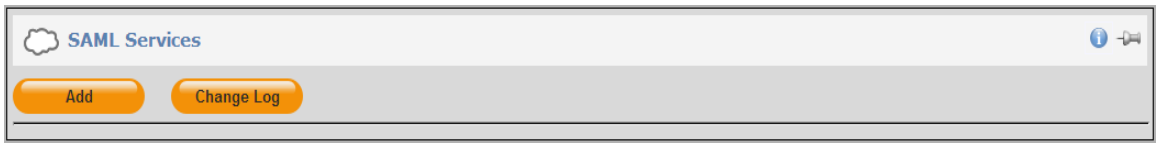
3. Click the appropriate User ID.



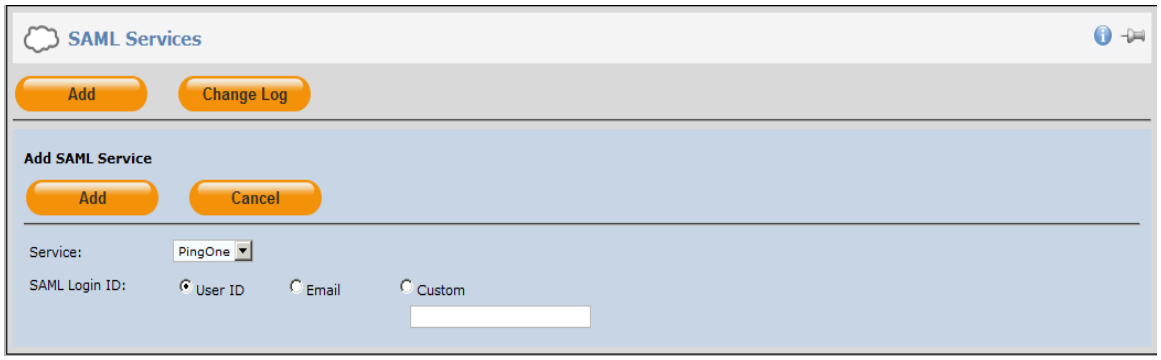
4. Click **SAML Services**.



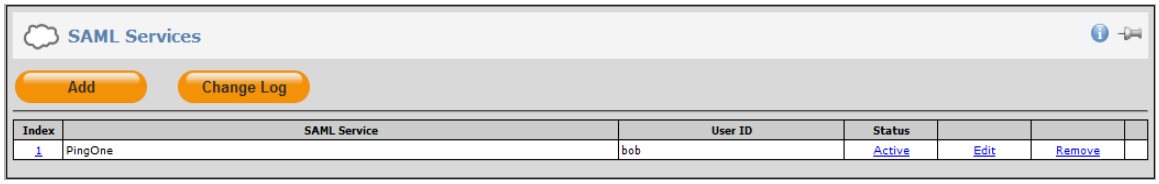
5. Click **Add**.



6. Under **Add SAML Service**, do the following:
   a. In the **Service** field, select the PingOne Service Provider.
   b. In **SAML Login ID** field, select the appropriate option (**User ID**, **Email**, or **Custom**) to be sent as a User ID to PingOne in the response.
   c. Click the **Add** button above the **Service** field.



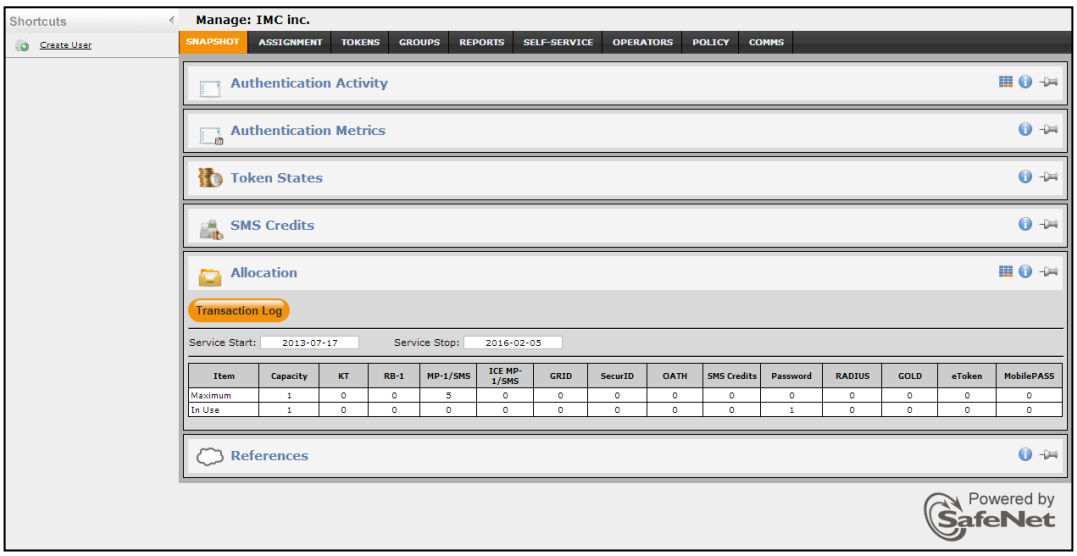
The user can now authenticate to PingOne using SAML authentication.



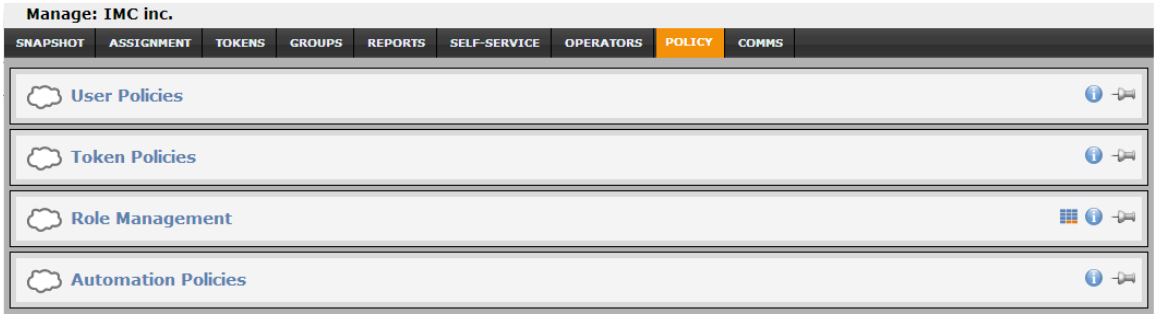
Using SAML Provisioning Rules

Use this module to enable groups of users to authenticate to SAML Service Providers.

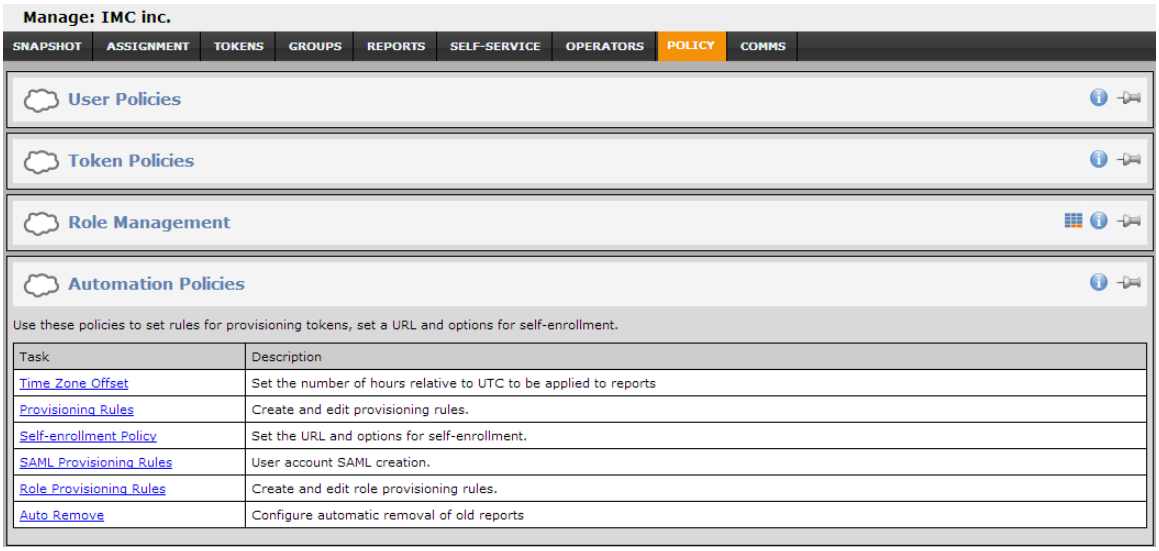
1. Log in to the SAS console with an Operator account.



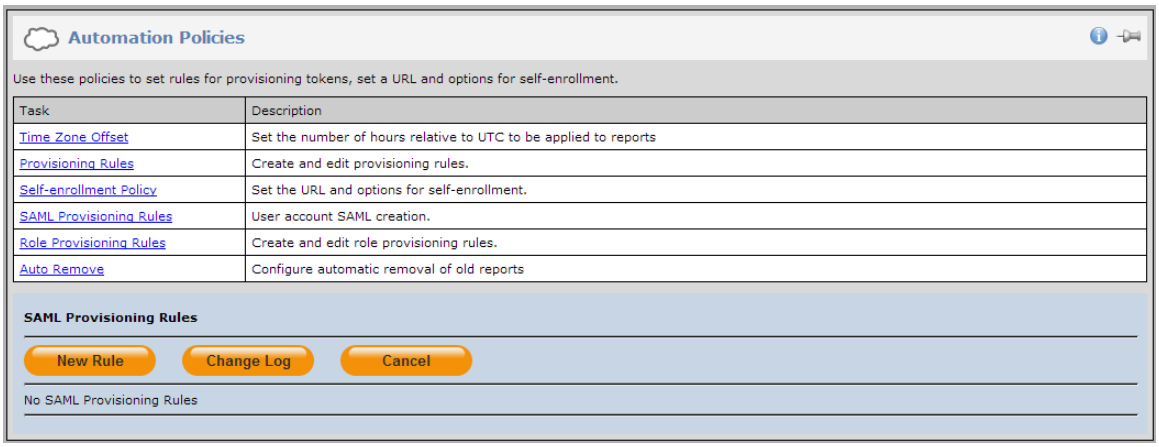
2. Click the **Policy** tab, and then click **Automation Policies**.



3. Click **SAML Provisioning Rules**.

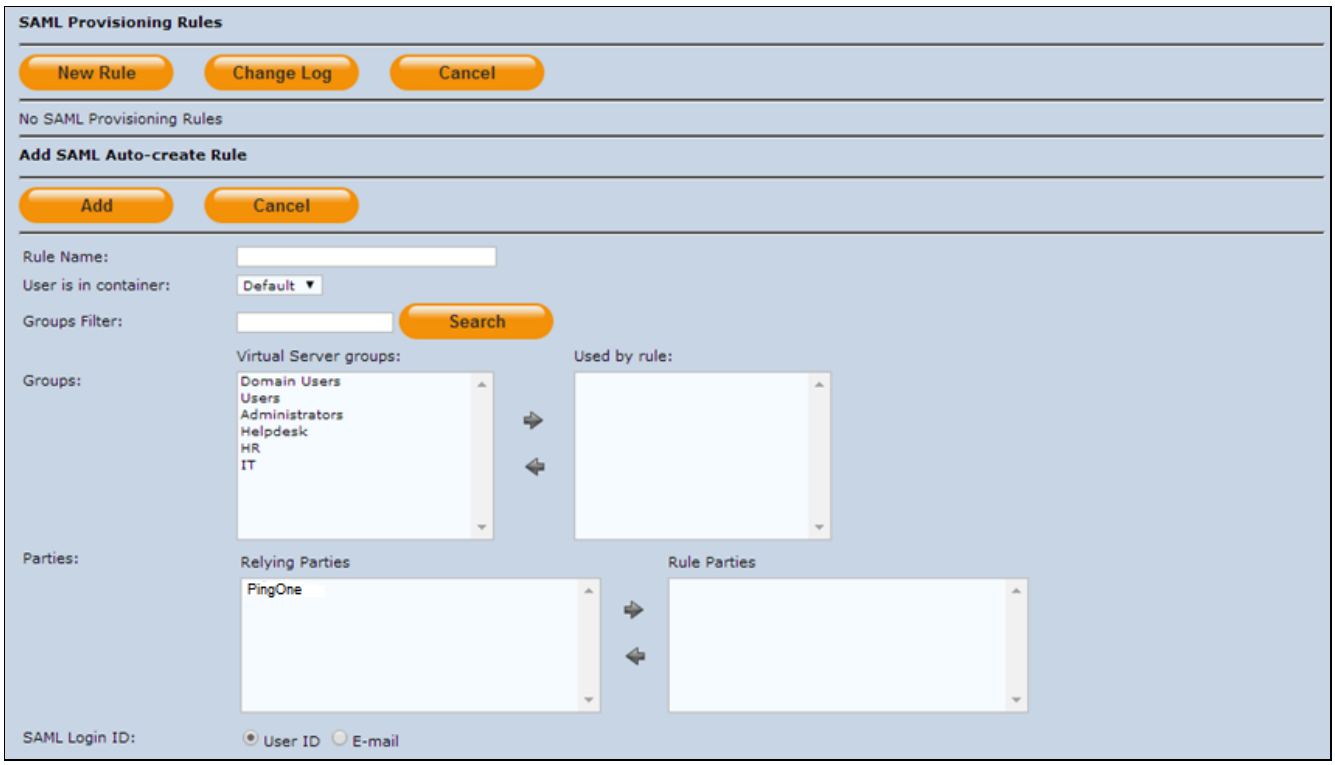


4. Click the **New Rule** button.



5. Configure the rule as follows:

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



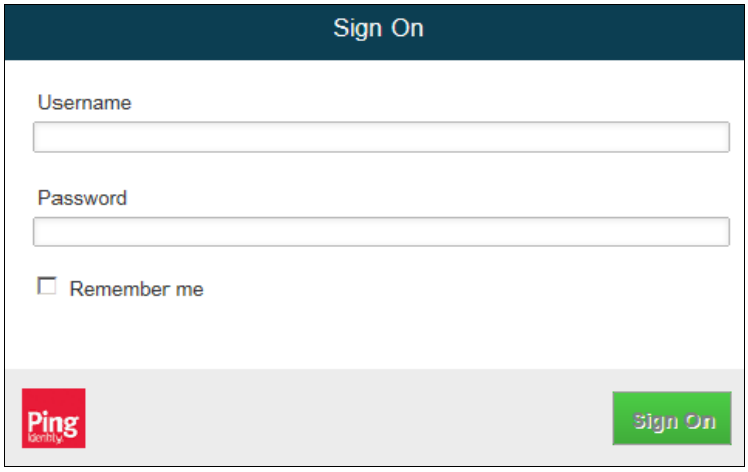
Running the Solution

PingOne dock is a graphical, browser-based interface to display your SaaS applications to users.

1. In a web browser, open the URL you have received from PingOne. Below is our specific URL used for this integration:

   https://desktop.pingone.eu/safenet-inc.com

2. On the PingOne **Sign On** window, enter your Active Directory **username** and **password** for primary authentication, and then click **Sign On**.



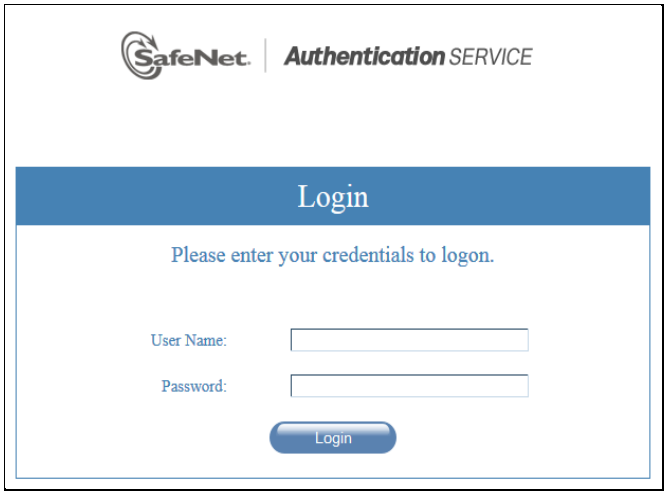
(The screen image above is from Ping Identity® software. Trademarks are the property of their respective owners.)

3. After successful authentication, the user is redirected to the SAS **Login** window for secondary authentication. Perform the following steps:

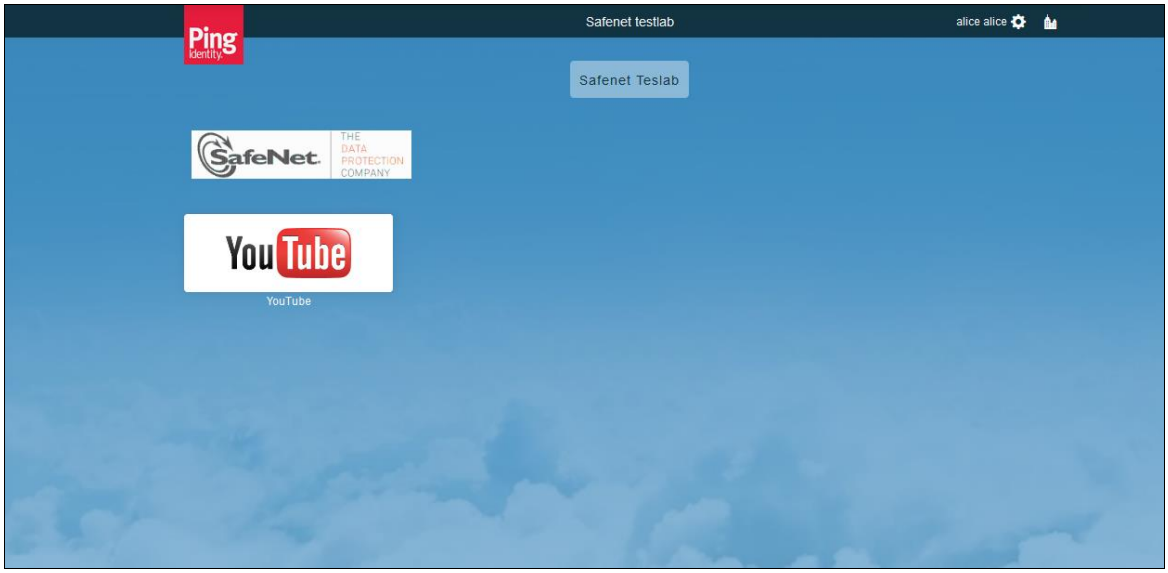
   a. In the **User Name** filed, enter you user name.

   b. In the **Password** field, enter the OTP for your enrolled token.

   c. Click **Login**.



After successful user authentication with SAS, the PingOne dock interface will display the user's SaaS applications.



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

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, 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 SafeNet Knowledge Base.	