SafeNet Authentication Service

Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Google Apps

gemalto
security to be free

Document Part Number: 007-013094-001, Rev. B

Release Date: May 2016

Contents

Third-Party Software Acknowledgement

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

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.

Google Apps is a suite of cloud computing productivity and collaboration software tools and software offered on a subscription basis by Google. It includes Google's popular web applications including Gmail, Google Drive, Google Hangouts, Google Calendar, and Google Docs.

This document describes how to:

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

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

Google Apps 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:

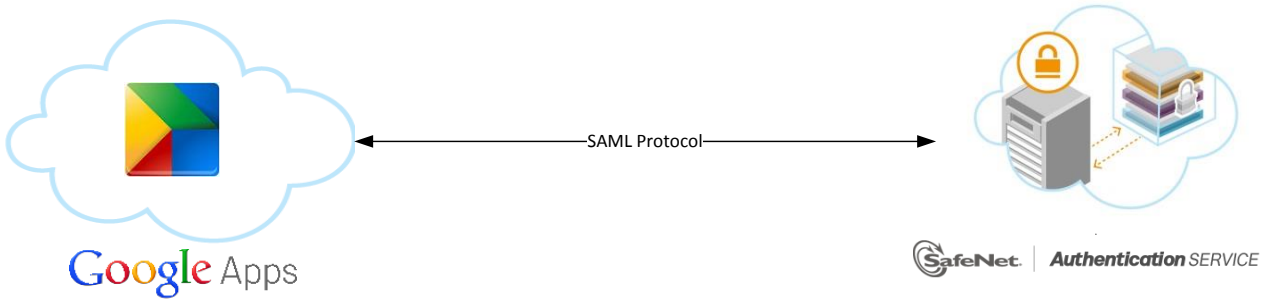
- **SafeNet Authentication Service - Service Provider Edition (SAS-SPE)**
- **Google Apps**

Audience

This document is targeted to system administrators who are familiar with Google Apps, 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.

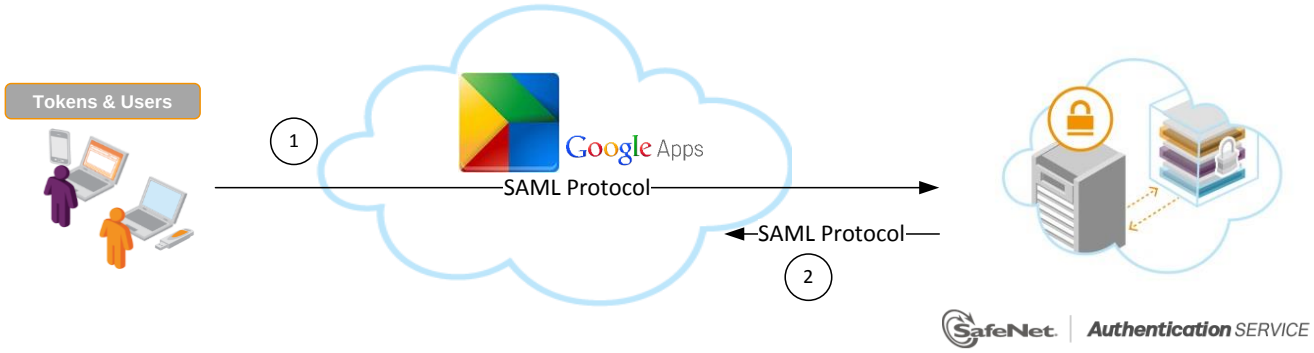
For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

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 Google Apps.



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

SAML Prerequisites

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

Download the SafeNet Identity Provider Certificate

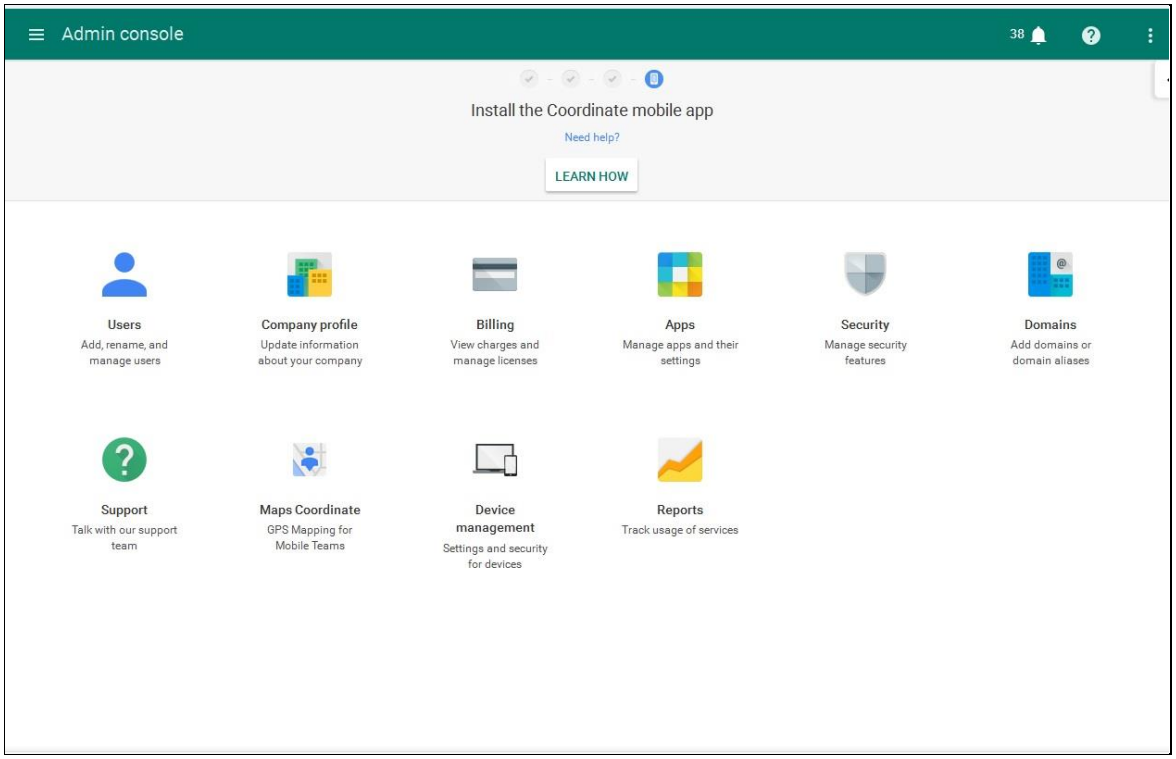
Browse to the **https://cloud.safenet-inc.com/console/cert/idp.crt** URL. The SafeNet identity provider certificate will automatically download. Save it locally on your machine.

Configuring Google Apps

To add SafeNet Authentication Service (SAS) as an Identity Provider in Google Apps:

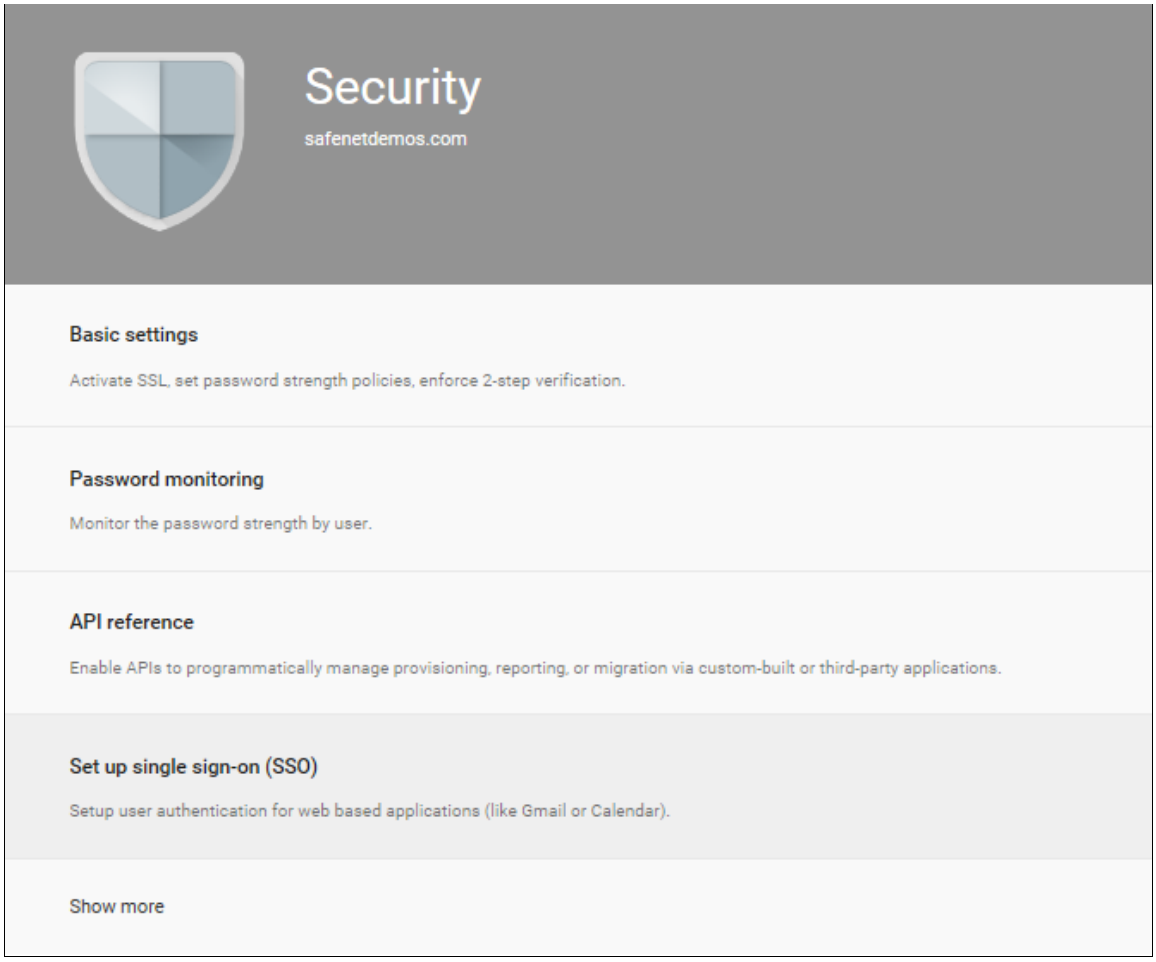
Add SafeNet Authentication Service as an Identity Provider in Google Apps.

1. In your Google Apps account, log in as an administrator.
2. Under **Admin console**, click **Security**.



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

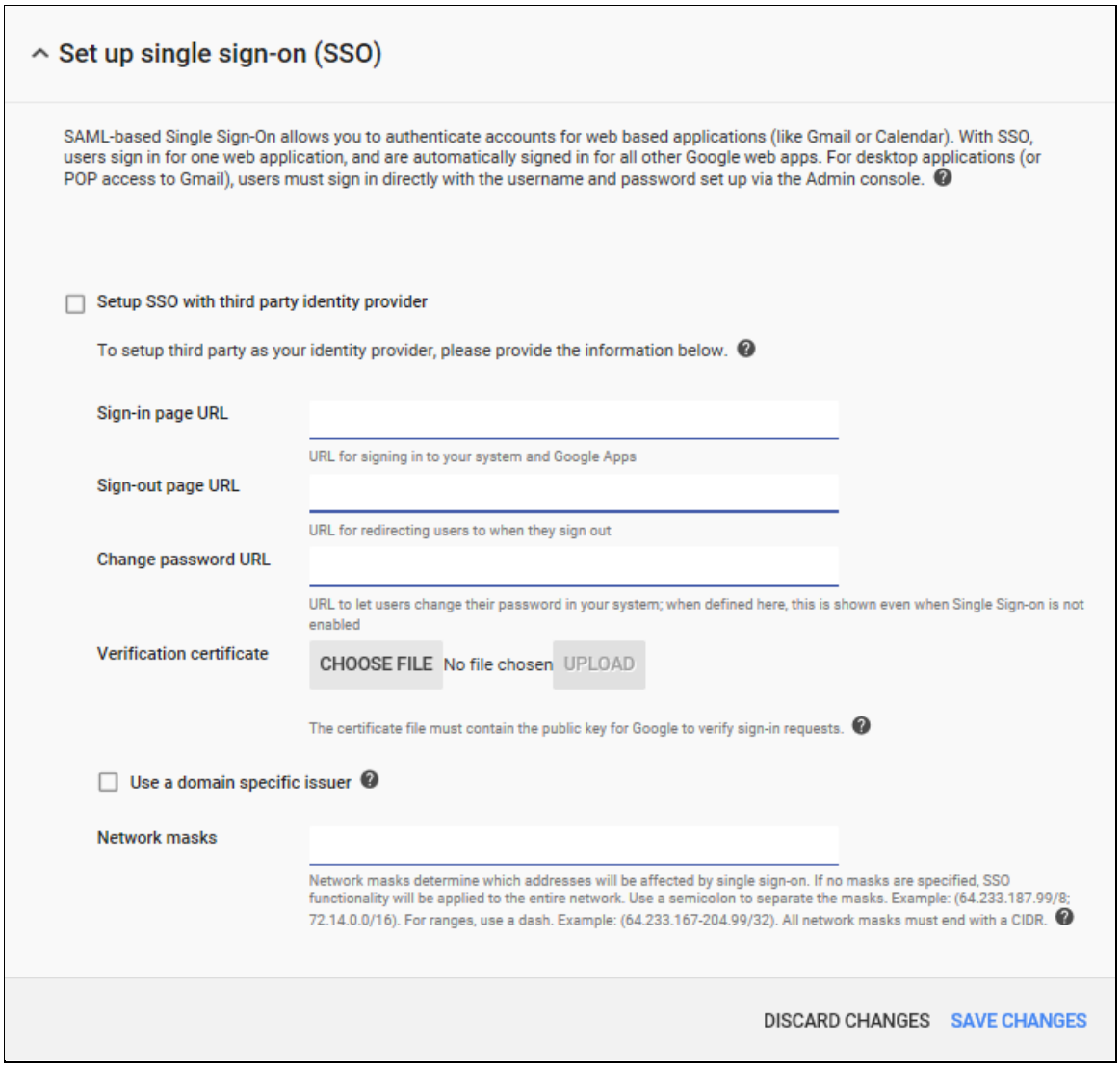
3. On the **Security** window, click **Set up single sign-on (SSO)**.



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

4. Under **Set up single sign-on (SSO)**, complete the following fields, and then click **SAVE CHANGES**.

Setup SSO with third party identity provider	Select this option.
Sign-in page URL	Enter **https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO**.
Sign-out page URL	Enter **https://idp1.cryptocard.com/idp/signout.jsp**.
Change password URL	Enter **https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO**.
Verification certificate	Click **CHOOSE FILE**, and then select the SafeNet Identity Provider Certificate you have downloaded. Click **UPLOAD** to upload the certificate.
Use a domain specific issuer	Select this option.



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

5. Under **Set up single sign-on (SSO)** -> **Setup SSO with Google identity provider**, click on option 2 and download the **IDP metadata**.

Configuring SafeNet Authentication Service

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

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 Google Apps.

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.

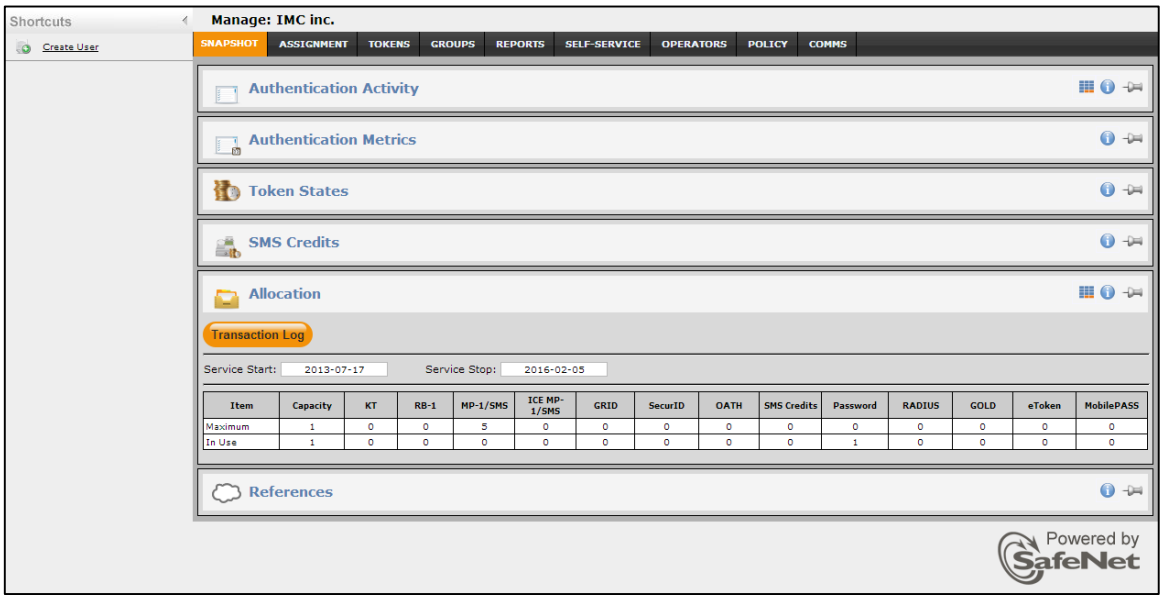
http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Account_Operator_Guide/

Adding Google Apps as a Service Provider (SP) in SafeNet Authentication Service

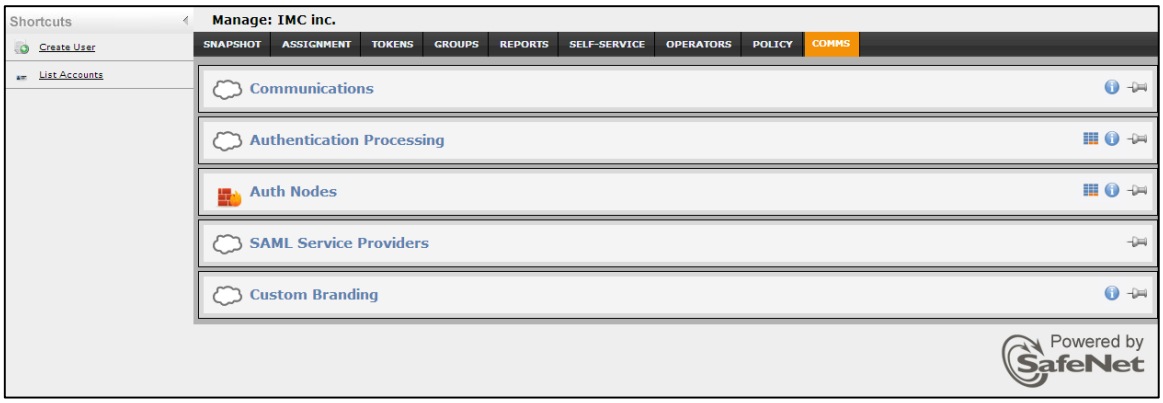
Add a service provider entry in the SafeNet Authentication Service (SAS) **SAML Service Providers** module to prepare it to receive SAML authentication requests from Google Apps. You will need the Issuer ID and assertion consumer URL location of Google Apps.

To add Google Apps as a Service Provider in SafeNet Authentication Service**:**

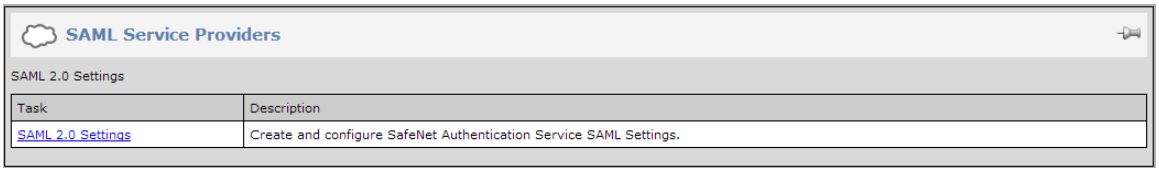
1. Log in to the SafeNet Authentication Service console with an Operator account.



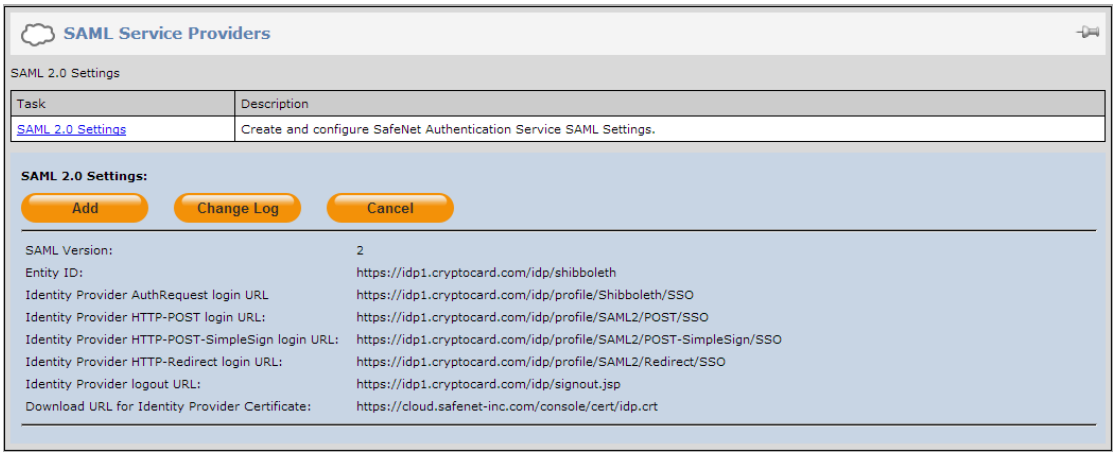
2. Click the **COMMS** tab, and then click **SAML Service Providers**.



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



4. Click **Add**.

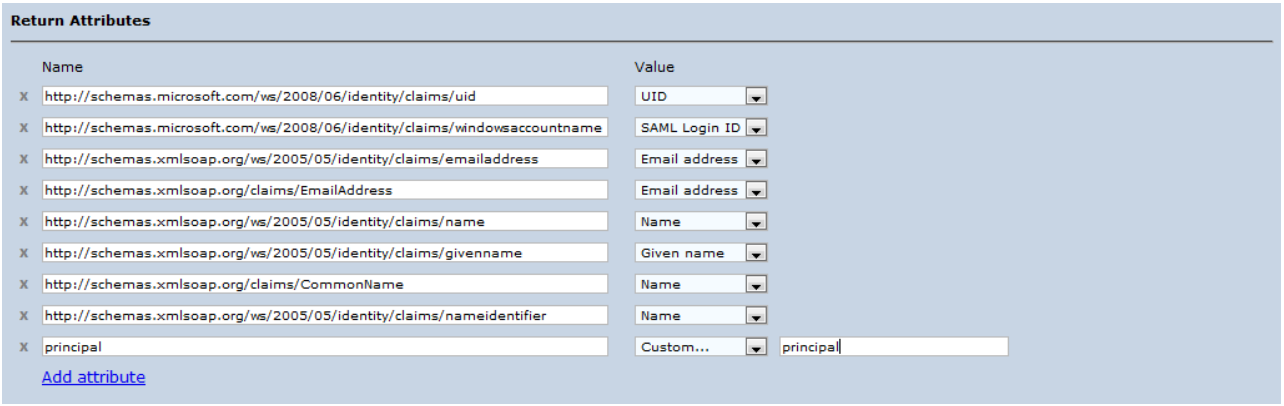


5. In the **Add SAML 2.0 Settings** section, complete the following fields:

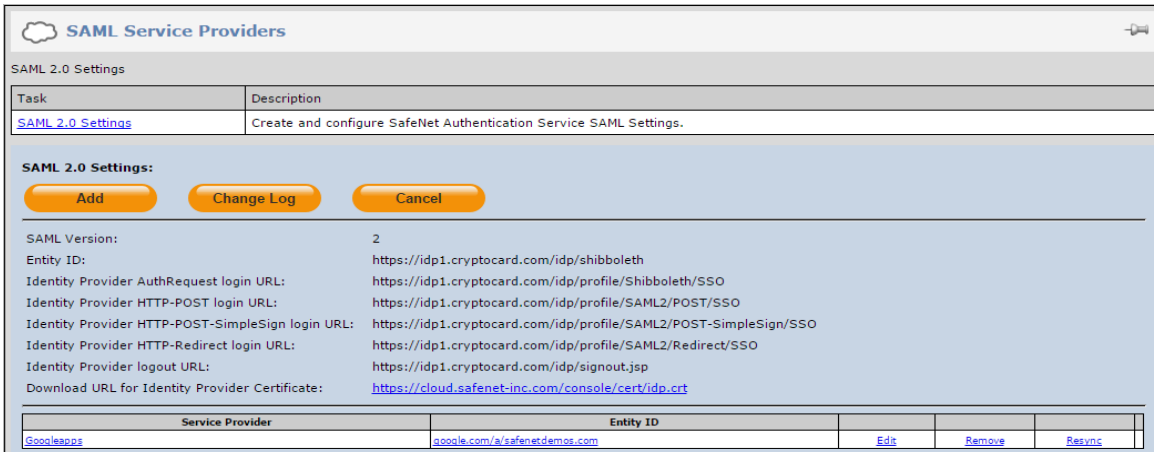
Friendly Name	Enter the Google Apps name.
SAML 2.0 Metadata	a. Select **Create New Metadata File**. b. In the **Entity ID** field, enter the Service Provider EntityID (for example, **google.com/a/mycompany**, where **mycompany** is your domain registered in Google Apps). In the **Location** field, enter the Assertion Consumer URL (for example, https://www.google.com/a/mycompany/acs, where **mycompany** is your domain registered in Google Apps).

Under **Return Attributes**, add 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



Google Apps is added as a service provider in the system.



Enabling SAML Services in SafeNet Authentication Service

After Google Apps 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.

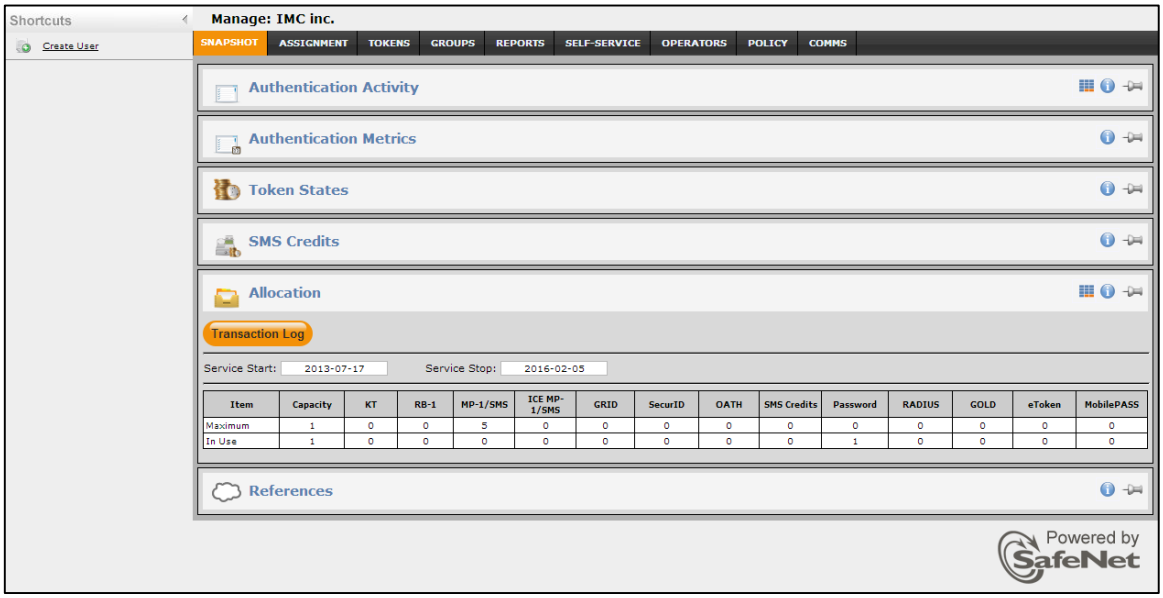
There are two methods to enable the user to use the service provider:

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

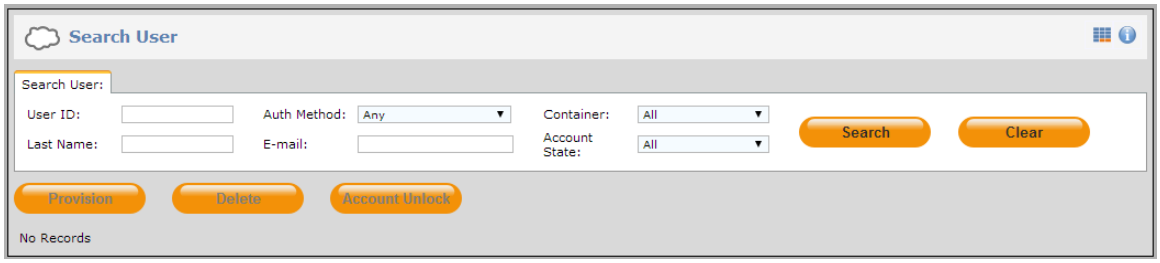
Using the SAML Services Module

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

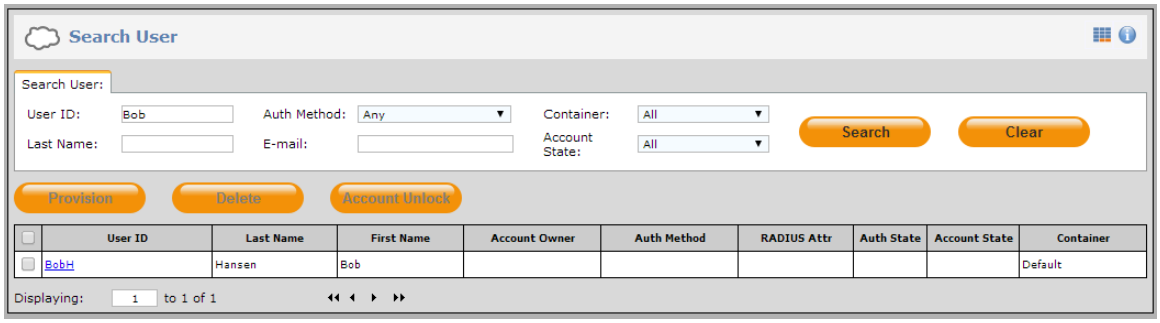
1. Log in to the SafeNet Authentication Service console with an Operator account.



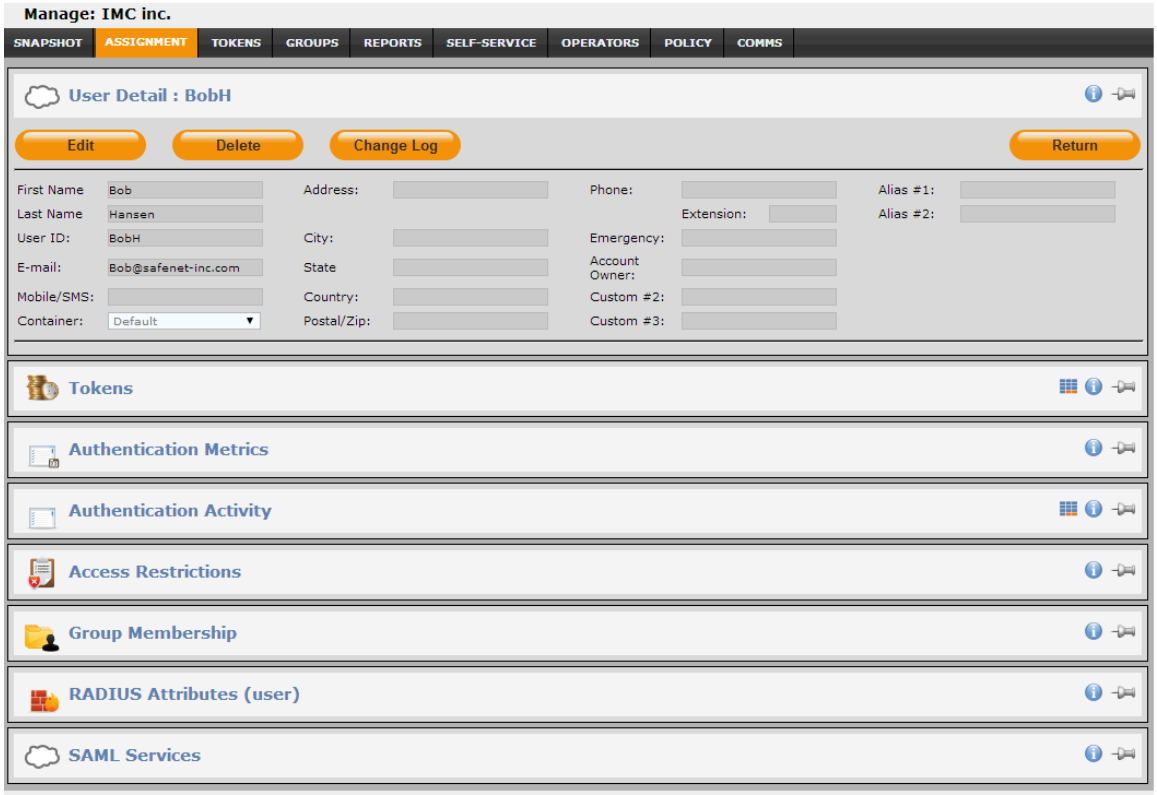
2. Click the **ASSIGNMENT** tab, and then search for the required user.



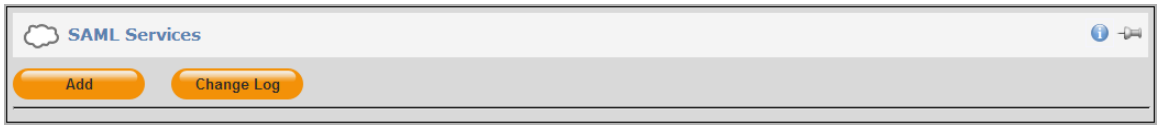
3. Click the appropriate user in the **User ID** column.



4. Click **SAML Services**.



5. Click **Add**.

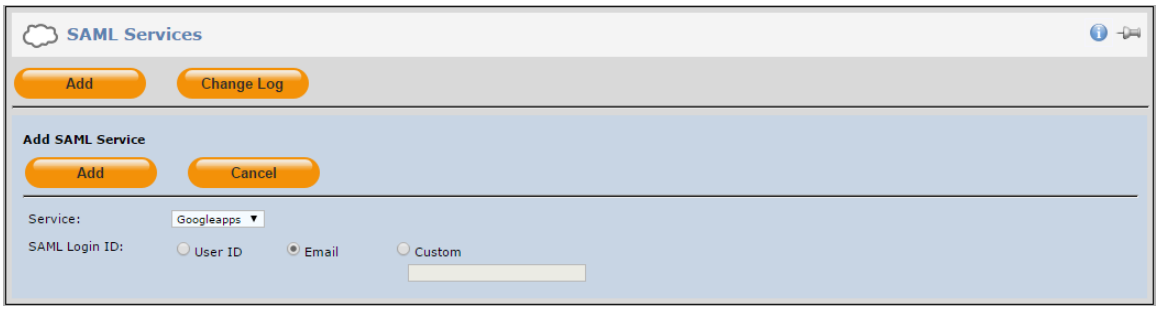


6. Under **Add SAML Service**, do the following:

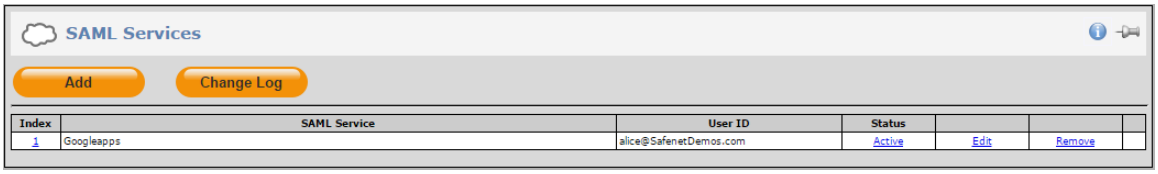
a. From the **Service** menu, select the Google Apps service provider.

b. In the **SAML Login ID** field, select **E-mail** to be sent as a UserID to Google Apps in the response.

c. Click **Add**.



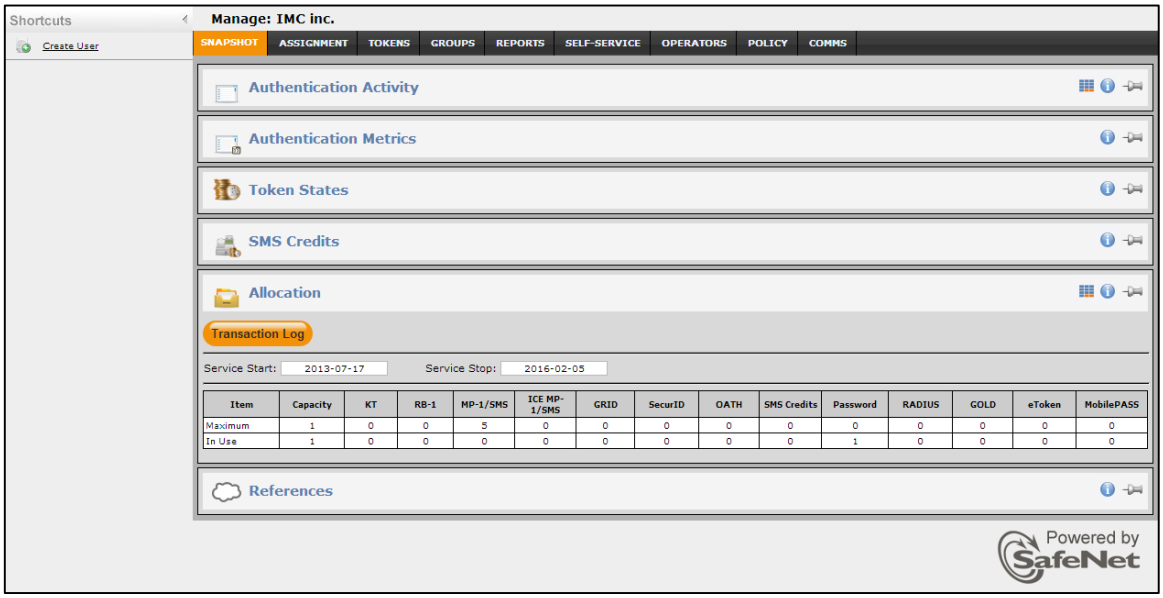
The user can now authenticate to Google Apps using SAML authentication.



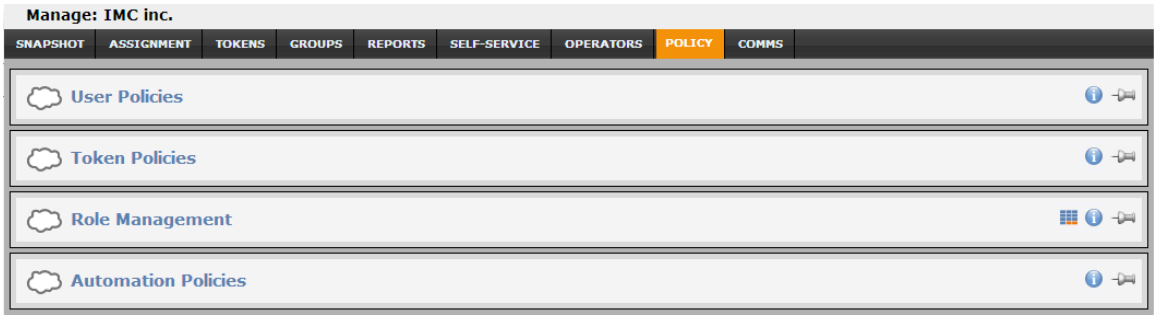
Using SAML Provisioning Rules

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

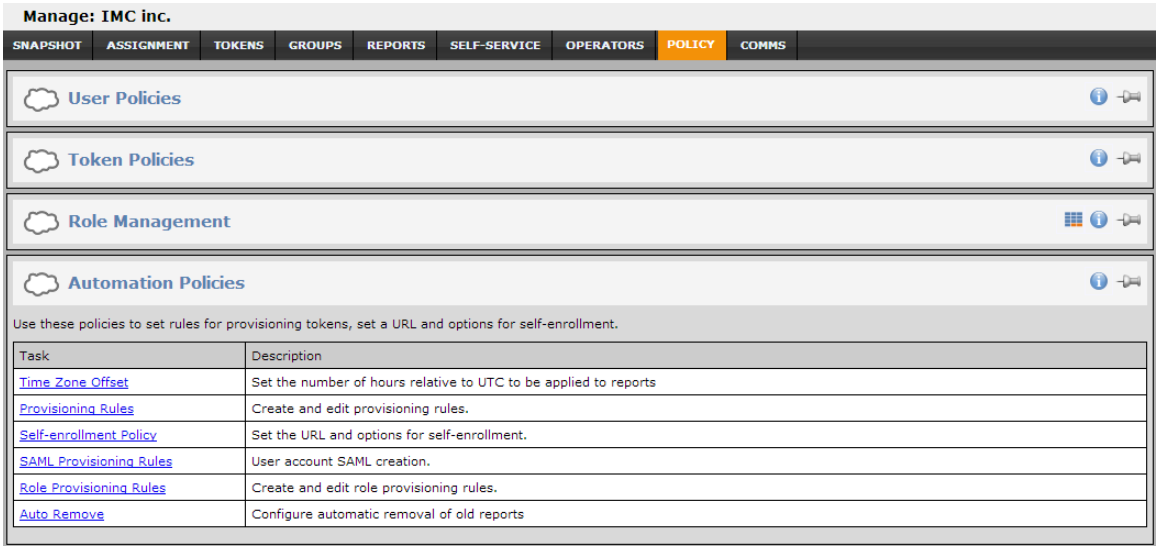
1. Log in to the SafeNet Authentication Service console with an Operator account.



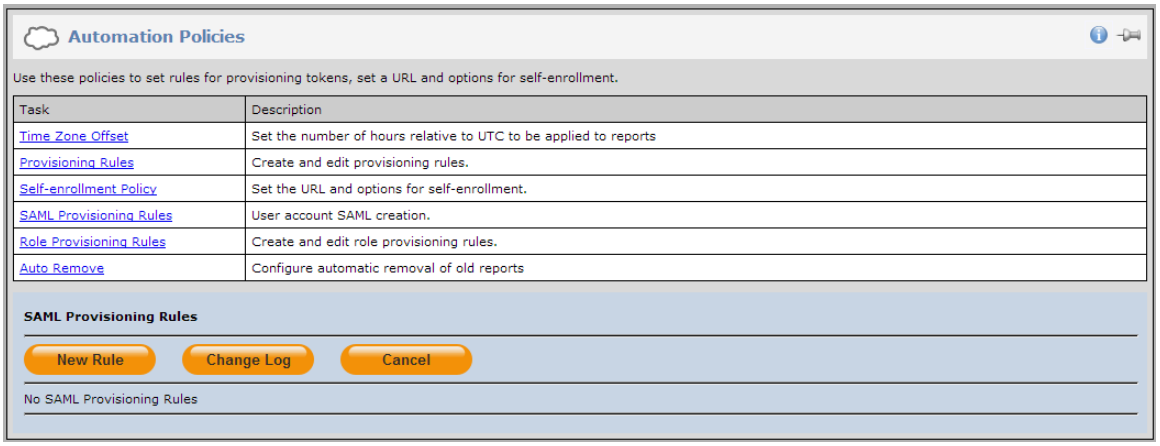
2. Click the **POLICY** tab, and then click **Automation Policies**.



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

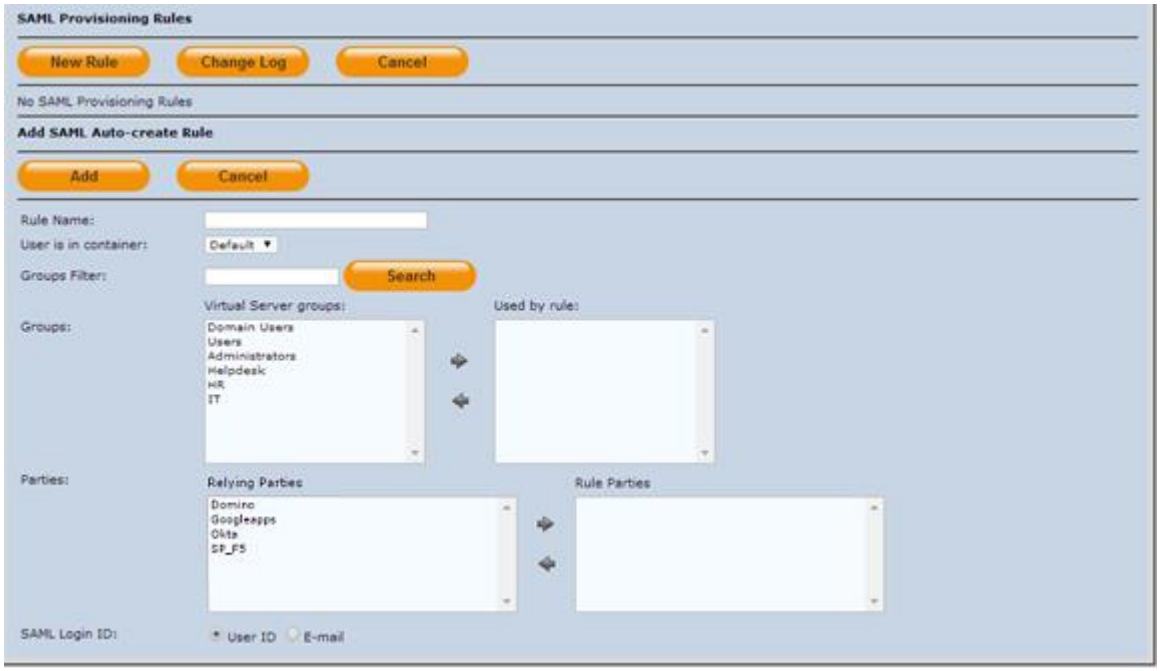


4. Click **New Rule**.



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

Rule Name	Enter a name for the rule.
User is in container	Select a container. Users affected by this rule must be in the selected container.
Groups	The **Virtual Server groups** list contains all groups. Click to select the user group(s) that will be affected by the rule, and then click the right arrow to move them to the **Used by rule** list.
Parties	The **Relying Parties** list contains all service providers. Click to select the service providers that the group of users will authenticate to and then click the right arrow to move them to **Rule Parties** list.
SAML Login ID	This is the User ID that will be returned to the service provider in the SAML assertion. Select **E-mail**.

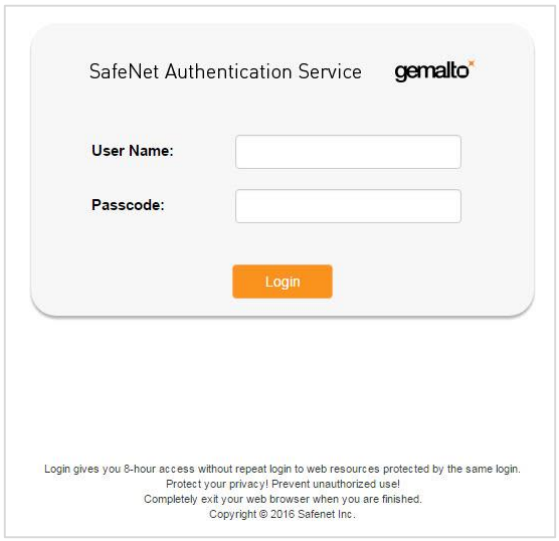


Running the Solution

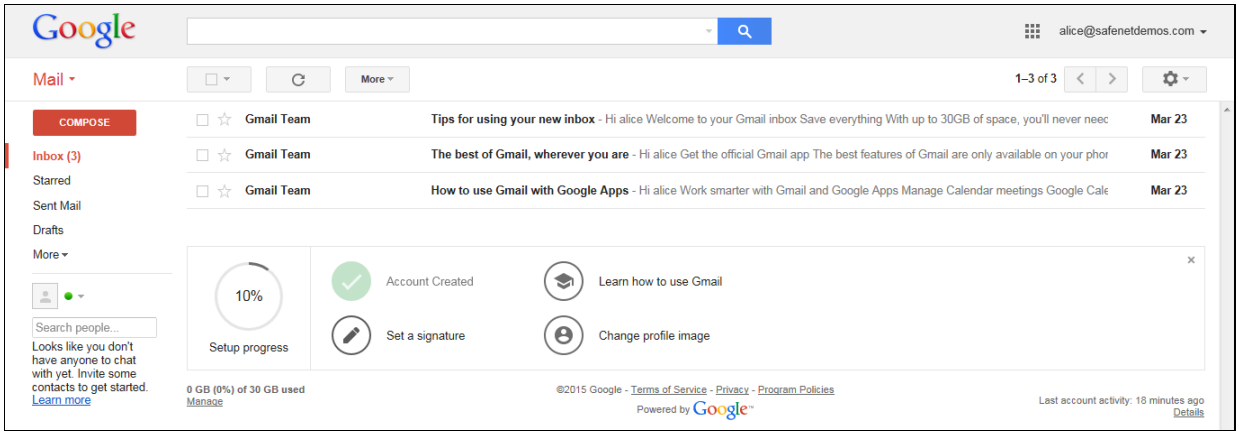
To access Google Mail, the user will browse to the Google Apps URL provided. After successful authentication, the user will be allowed to access Google Mail.

For this integration, the SafeNet GrIDsure token is configured for authentication with the SAS solution.

1. Open the web browser, and enter the Google Apps URL (for example, **https://mail.google.com/a/safenetdemos.com**). You are redirected to the SAS **Login** page.
2. In the **User Name** field, enter the username, and in the **Password** field, enter the OTP for your enrolled token.



3. If authentication is successful, the user is logged in and will be allowed to access Google Mail.



(The screen image above is from Google®. 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 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.	