

SafeNet Authentication Service Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Google
Apps

All information herein is either public information or is the property of and owned solely by Gemalto NV. 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.

© 2015 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: 007-013094-001, Rev. B

Release Date: May 2016

Contents

Third-Party Software Acknowledgement	4
Description	4
Applicability	4
Environment.....	4
Audience	5
SAML Authentication using SafeNet Authentication Service Cloud	5
SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE5	5
SAML Authentication Flow using SafeNet Authentication Service	6
SAML Prerequisites	6
Download the SafeNet Identity Provider Certificate	6
Configuring Google Apps.....	7
Configuring SafeNet Authentication Service	10
Synchronizing Users Stores to SafeNet Authentication Service.....	10
Assigning an Authenticator in SafeNet Authentication Service.....	10
Adding Google Apps as a Service Provider (SP) in SafeNet Authentication Service.....	11
Enabling SAML Services in SafeNet Authentication Service.....	14
Running the Solution	19
Support Contacts	20

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:

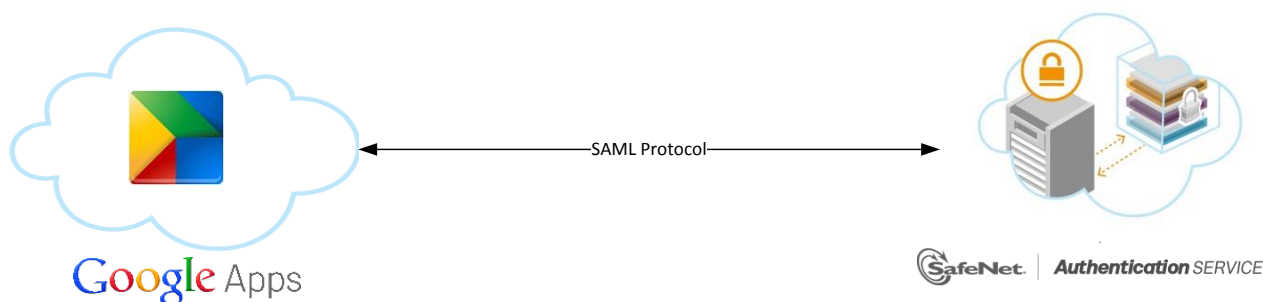
- **SafeNet Authentication Service - Service Provider Edition (SAS-SPE)**
- **Google Apps**

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.

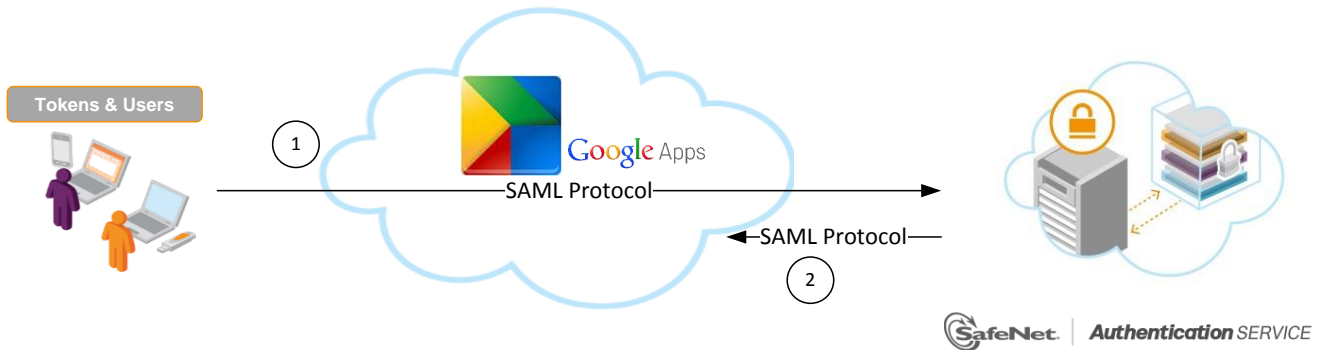
For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

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

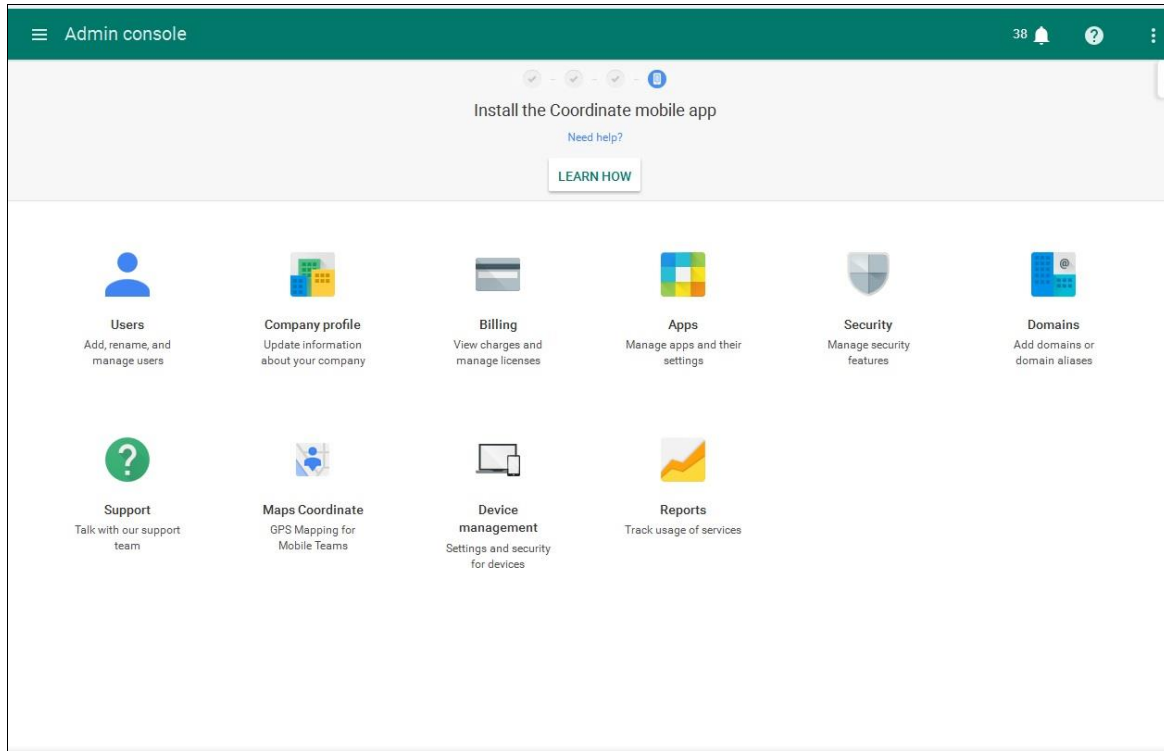
Browse to the <https://cloud.safenet-inc.com/console/cert/idp.crt> URL. The SafeNet identity provider certificate will automatically download. Save it locally on your machine.

Configuring Google Apps

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

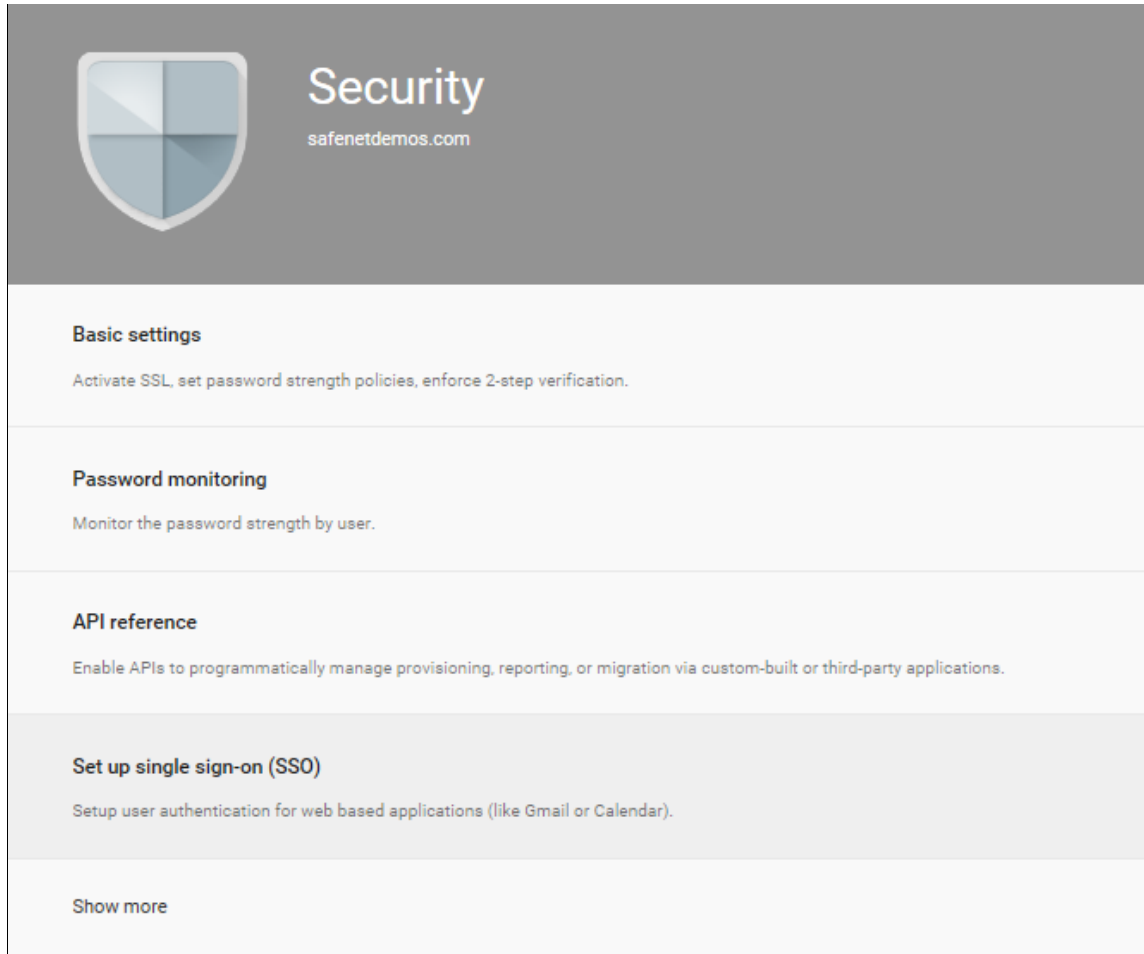
Add SafeNet Authentication Service as an Identity Provider in Google Apps.

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.

^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL
URL for signing in to your system and Google Apps

Sign-out page URL
URL for redirecting users to when they sign out

Change password URL
URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate No file chosen

The certificate file must contain the public key for Google to verify sign-in requests. ?

Use a domain specific issuer ?

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

[DISCARD CHANGES](#) [SAVE CHANGES](#)

(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, page 10
- Assigning an Authenticator in SafeNet Authentication Service, page 10
- Adding Google Apps as a Service Provider (SP) in SafeNet Authentication Service. page 11
- 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 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

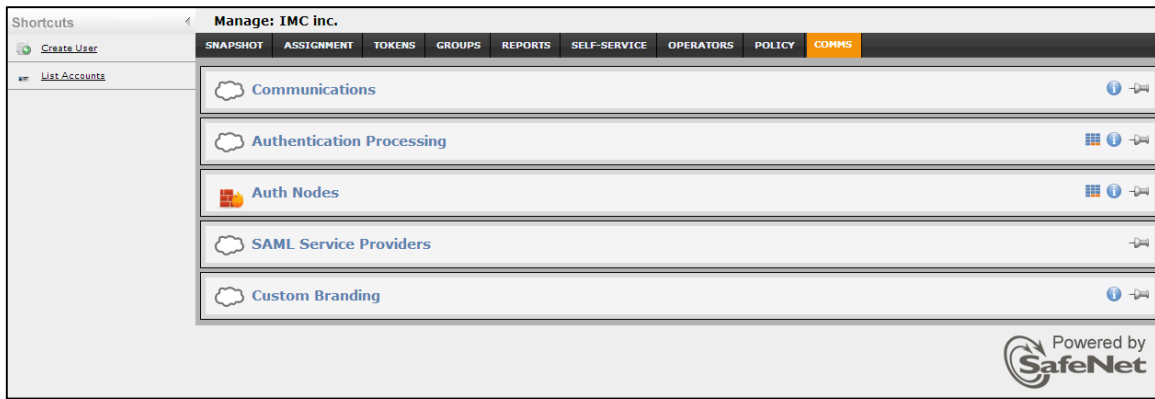
Add a service provider entry in the SafeNet Authentication Service (SAS) **SAML Service Providers** module to prepare it to receive SAML authentication requests from Google Apps. You will need the Issuer ID and assertion consumer URL location of Google Apps.

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

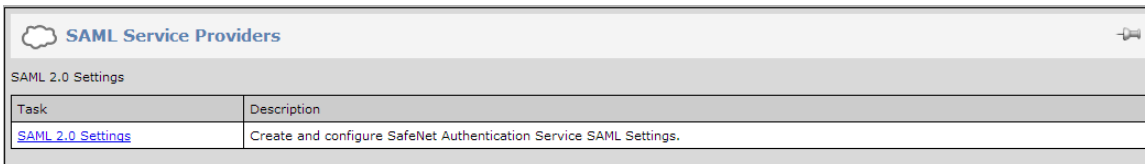
1. Log in to the SafeNet Authentication Service console with an Operator account.

Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	0

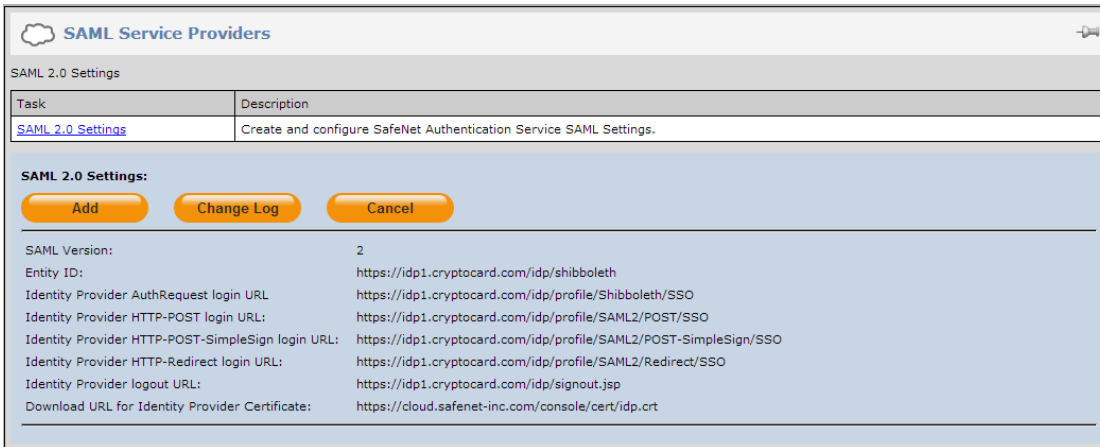
2. Click the **COMMS** tab, and then click **SAML Service Providers**.



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	<p>a. Select Create New Metadata File.</p> <p>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).</p> <p>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).</p>

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

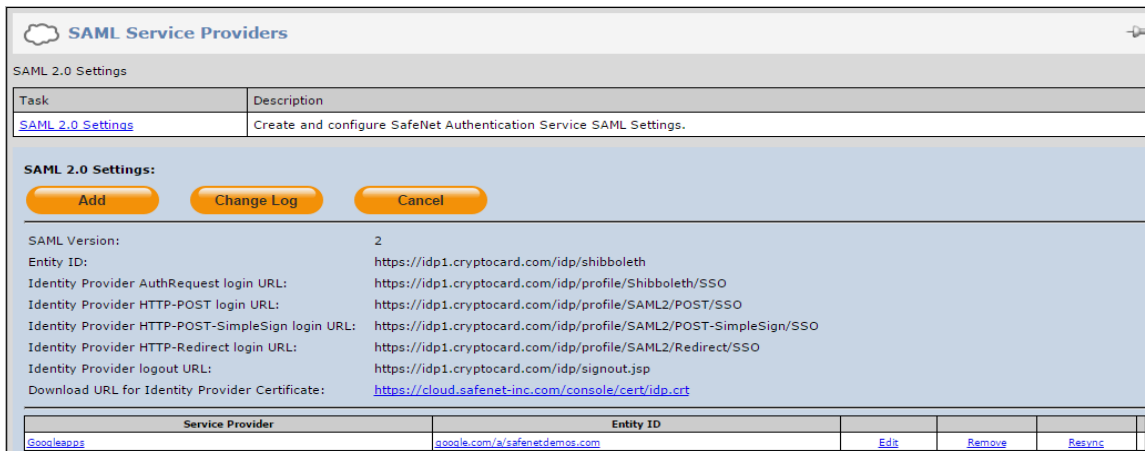
Name	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/uid	According to ThirdParty Product Requirements
http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount name	According to ThirdParty Product Requirements
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	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

Return Attributes

Name	Value
X <input type="text" value="http://schemas.microsoft.com/ws/2008/06/identity/claims/uid"/>	UID
X <input type="text" value="http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"/>	SAML Login ID
X <input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"/>	Email address
X <input type="text" value="http://schemas.xmlsoap.org/claims/EmailAddress"/>	Email address
X <input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"/>	Name
X <input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"/>	Given name
X <input type="text" value="http://schemas.xmlsoap.org/claims/CommonName"/>	Name
X <input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"/>	Name
X <input type="text" value="principal"/>	Custom... <input type="text" value="principal"/>

[Add attribute](#)

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.

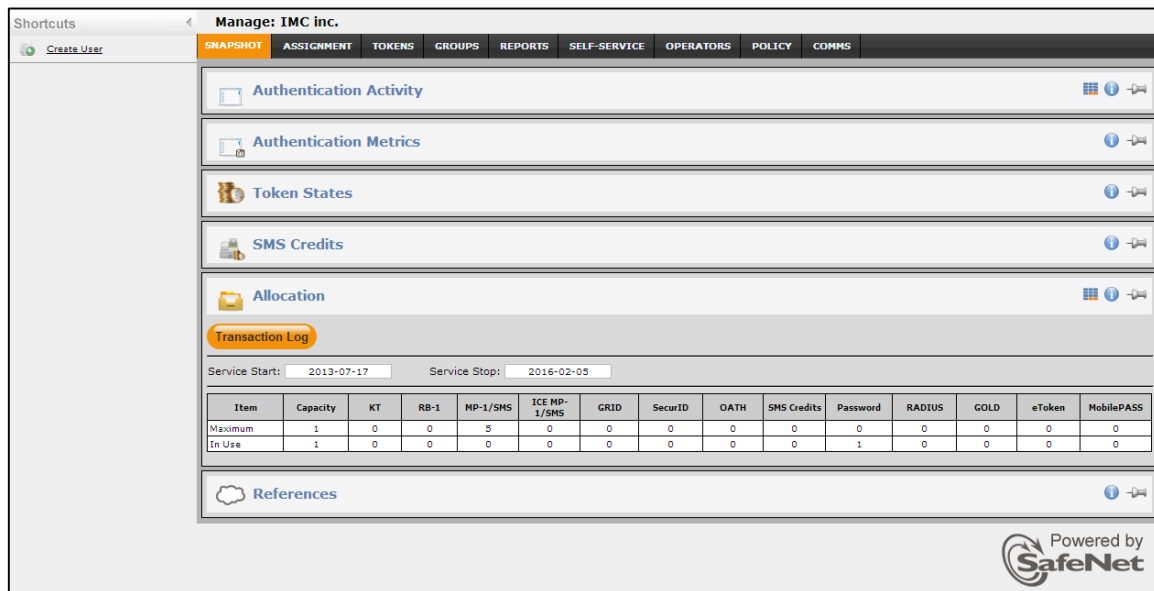
There are two methods to enable the user to use the service provider:

- 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.

Search User

Search User:

User ID: Auth Method: Container:

Last Name: E-mail: Account State:

No Records

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

Search User

Search User:

User ID: Auth Method: Container:

Last Name: E-mail: Account State:

<input type="checkbox"/>	User ID	Last Name	First Name	Account Owner	Auth Method	RADIUS Attr	Auth State	Account State	Container
<input checked="" type="checkbox"/>	BobH	Hansen	Bob						Default

Displaying: 1 to 1 of 1

4. Click **SAML Services**.

Manage: IMC inc.

SNAPSHOT **ASSIGNMENT** TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS

User Detail : BobH

First Name: Address: Phone: Alias #1:

Last Name: Extension: Alias #2:

User ID: City: Emergency:

E-mail: State: Account Owner:

Mobile/SMS: Country: Custom #2:

Container: Postal/Zip: Custom #3:

Tokens

Authentication Metrics

Authentication Activity

Access Restrictions

Group Membership

RADIUS Attributes (user)

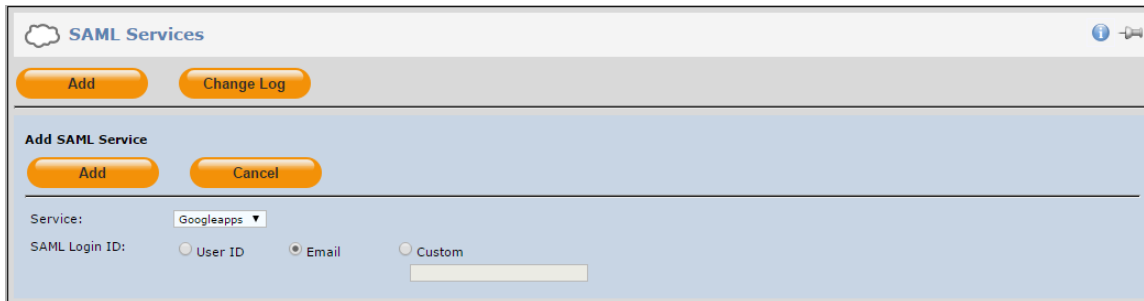
SAML Services

5. Click **Add**.

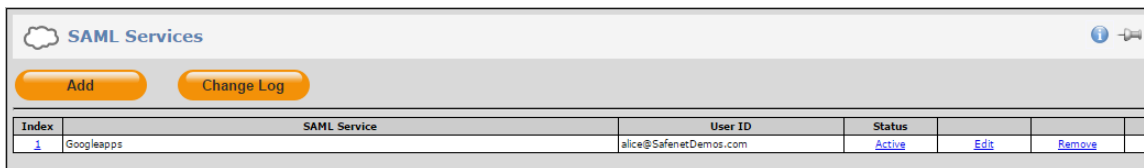
SAML Services

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**.



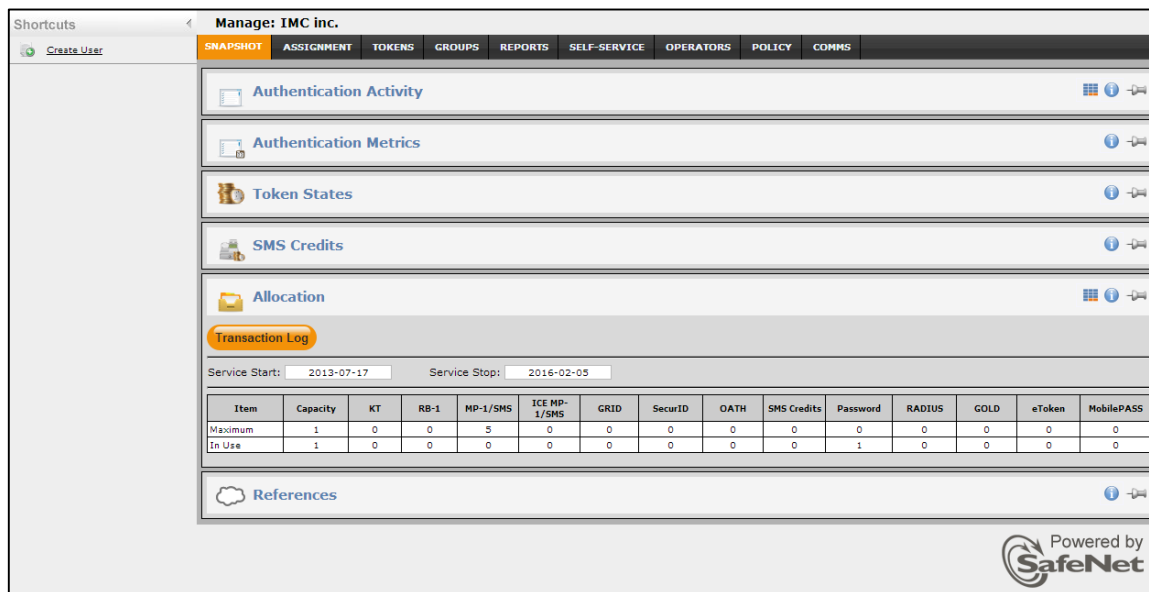
The user can now authenticate to Google Apps using SAML authentication.



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**.

Manage: IMC inc.

SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS **POLICY** COMMS

User Policies

Token Policies

Role Management

Automation Policies

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

Manage: IMC inc.

SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS **POLICY** COMMS

User Policies

Token Policies

Role Management

Automation Policies

Use these policies to set rules for provisioning tokens, set a URL and options for self-enrollment.

Task	Description
Time Zone Offset	Set the number of hours relative to UTC to be applied to reports
Provisioning Rules	Create and edit provisioning rules.
Self-enrollment Policy	Set the URL and options for self-enrollment.
SAML Provisioning Rules	User account SAML creation.
Role Provisioning Rules	Create and edit role provisioning rules.
Auto Remove	Configure automatic removal of old reports

4. Click **New Rule**.

Automation Policies

Use these policies to set rules for provisioning tokens, set a URL and options for self-enrollment.

Task	Description
Time Zone Offset	Set the number of hours relative to UTC to be applied to reports
Provisioning Rules	Create and edit provisioning rules.
Self-enrollment Policy	Set the URL and options for self-enrollment.
SAML Provisioning Rules	User account SAML creation.
Role Provisioning Rules	Create and edit role provisioning rules.
Auto Remove	Configure automatic removal of old reports

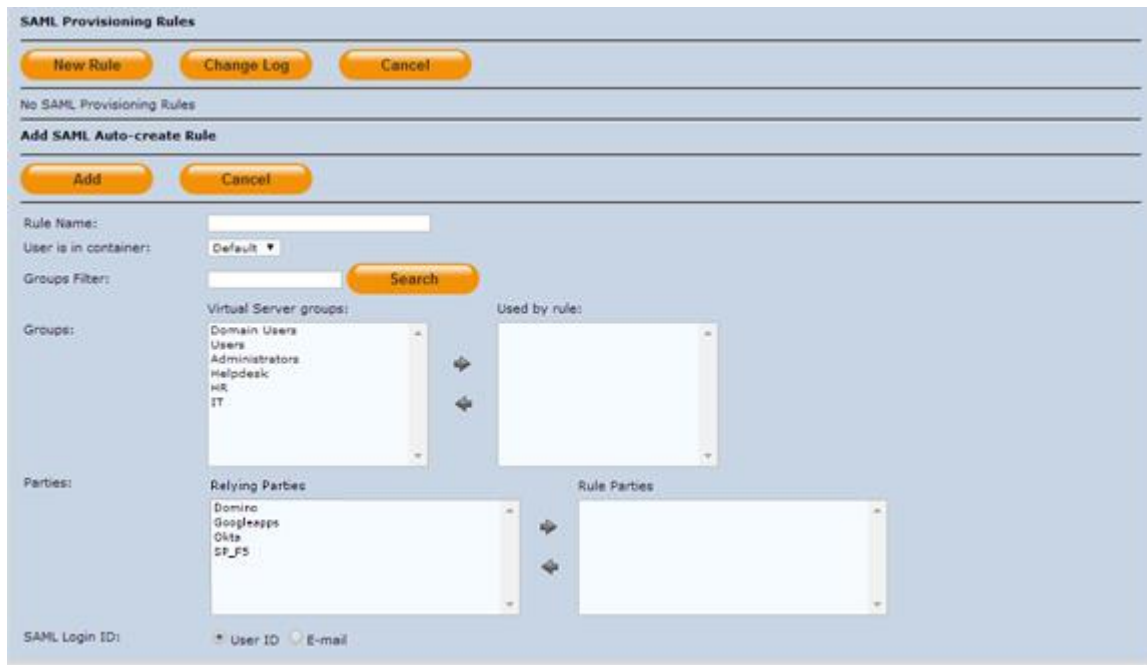
SAML Provisioning Rules

[New Rule](#) [Change Log](#) [Cancel](#)

No SAML Provisioning Rules

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 .

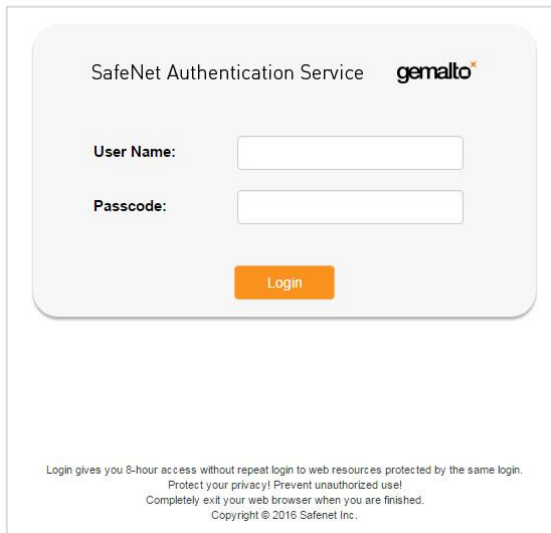


Running the Solution

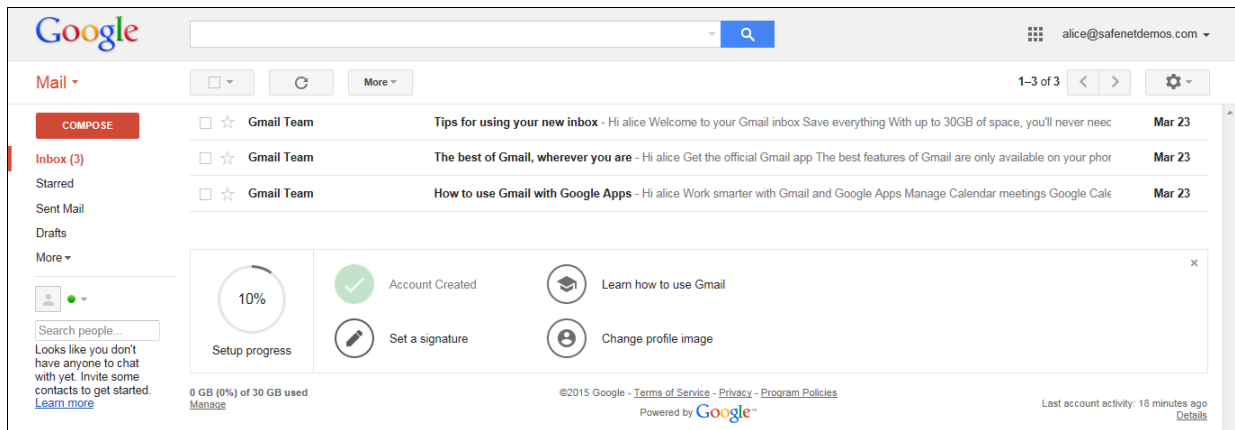
To access Google Mail, the user will browse to the Google Apps URL provided. After successful authentication, the user will be allowed to access Google Mail.

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.	