

SafeNet Authentication Service Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Zimbra
Webmail Client

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: 007-012926-001, Rev. B

Release Date: June 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	5
SAML Prerequisites	6
Configuring Zimbra Webmail Client	6
Configuring SafeNet Authentication Service	7
Synchronizing Users Stores to SafeNet Authentication Service	7
Assigning an Authenticator in SafeNet Authentication Service.....	8
Adding Zimbra Webmail Client as a Service Provider (SP) in SafeNet Authentication Service	8
Enabling SAML Services in SafeNet Authentication Service.....	12
Running the Solution	16
Support Contacts	17

Third-Party Software Acknowledgement

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

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.

Zimbra Web Client (ZWC) is a full-featured messaging and collaboration application that offers reliable, high-performance email, address books, calendaring, task lists, and web document authoring capabilities.

This document describes how to:

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

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

Zimbra Webmail Client 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:

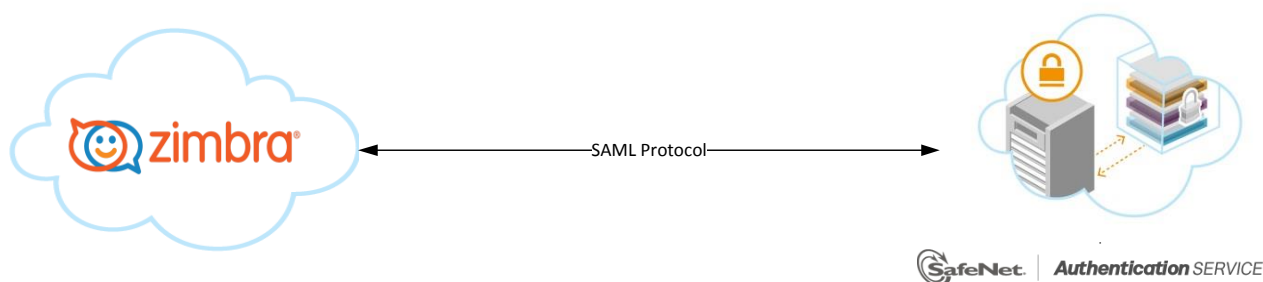
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)** — Mention only if SAS-PCE is relevant. Add version number to the SAS-PCE.
- **Zimbra Network Collaboration Suite** (zcs-NETWORK-8.5.1_GA_3056.RHEL6_64.20141103151728) on CentOS 6.4 64-bit

Audience

This document is targeted to system administrators who are familiar with Zimbra Webmail Client, 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.

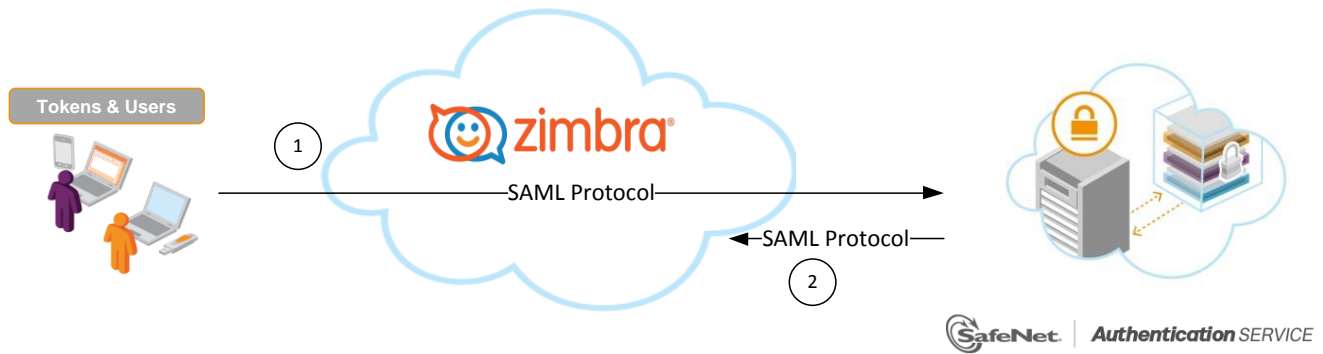
For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

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 Zimbra Webmail Client.



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

SAML Prerequisites

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

Configuring Zimbra Webmail Client

Add SAS as an Identity Provider in Zimbra Webmail Client. To get the SAS SAML settings for configuring Zimbra Webmail Client, refer to step 4 of "Adding Zimbra Webmail Client as a Service Provider (SP) in SafeNet Authentication Service", on page 8.

3. Log in to your Zimbra server and run the following commands as a **root** user:

```
mkdir /opt/zimbra/lib/ext/saml
```

```
cp /opt/zimbra/extensions-network-extra/saml/samlextn.jar /opt/zimbra/lib/ext/saml/
```

4. To add the SAML signing certificate (IdP certificate) to the domain, run the following command as the Zimbra user:

```
cat </location/IdP Certificate> |xargs -0 zmprov md <domain > zimbraMyoneloginSamISigningCert
```

where,

- **<domain>** is the Zimbra server host name
- **<IdP Certificate >** is the SAS IdP certificate in base 64 format
- **/location** is the absolute path of the IdP certificate

5. To specify the Identity Provider login and logout URL on the Zimbra server, run the following commands as the Zimbra user:

```
zmprov md <domain> zimbraWebClientLoginURL <IdP login URL>
```

```
zmprov md <domain> zimbraWebclientLogoutURL <IdP logout URL>
```

where, to support SAML 1.1, the SAS login URL for Zimbra will be:

- **IdP login URL:**

`https://< IP of SAS IdP >/idp/profile/SAML2/Unsolicited/SSO?providerId= <Zimbra SAML extension URL> &target=< Zimbra SAML extension URL>`

- **IdP logout URL:**

`https://< IP of SAS IdP >/idp/signout`

where,

- **<Zimbra SAML extension URL>** is `<zimbra_base_url>/service/extension/samlreceiver`
- **<Zimbra_base_url>** is `https://<Zimbra Server Host Name>`

6. To restart the Zimbra services, run the following commands as a Zimbra user:

zmcontrol stop

zmcontrol start

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Zimbra Webmail Client using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 8
- Adding Zimbra Webmail Client as a Service Provider (SP) in SafeNet Authentication Service. page 8
- Enabling SAML Services in SafeNet Authentication Service, page 12

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 Zimbra Webmail Client.

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 Zimbra Webmail Client as a Service Provider (SP) in SafeNet Authentication Service

Add a Service Provider entry in the SAS **SAML Service Providers** module to prepare it to receive SAML authentication requests from Zimbra Webmail Client. You will need the Issuer ID and Assertion Consumer URL location of Zimbra Webmail Client.

Zimbra does not provide any metadata. To support the Zimbra Browser/POST Profile as per the SAML1.1 specification, you need to create a metadata file for Zimbra using the location URL, provider ID, and a flag that specifies not to validate signatures on the SAML request.

To create a metadata file for Zimbra:

Create the Zimbra metadata file (save as **.xml**) and add the following content:

```
<EntityDescriptor entityID="<zimbra_base_url>/service/extension/samlreceiver"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
AuthnRequestsSigned="false">
<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
```



```

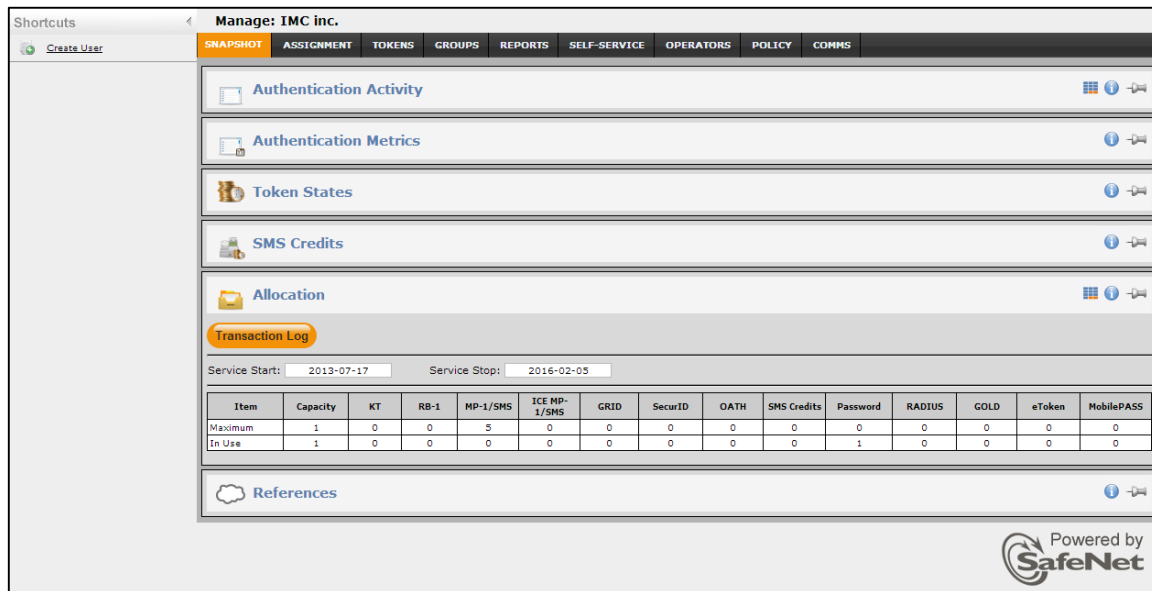
<AssertionConsumerService index="0" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="<zimbra_base_url>/service/extension/samlreceiver"/>
</SPSSODescriptor>
</EntityDescriptor>

```

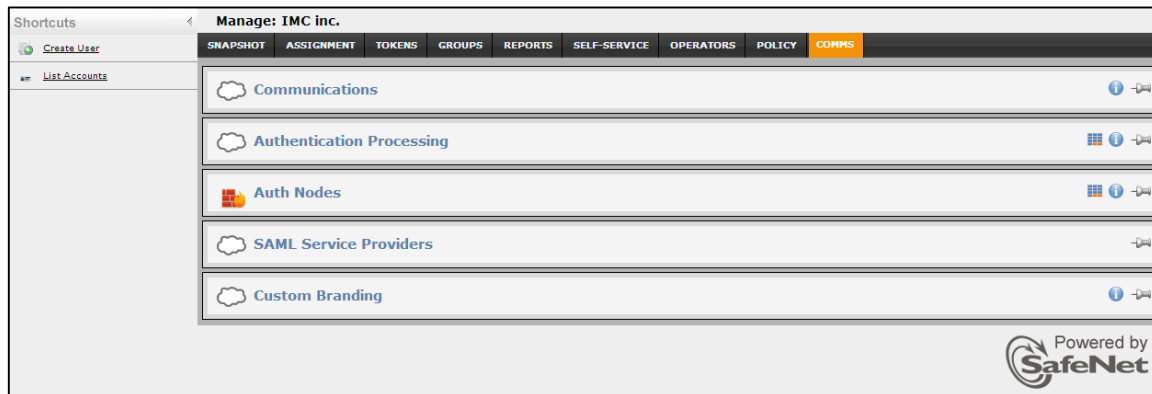
where, <Zimbra_base_url> is https://<Zimbra Server Host Name>.

To add Zimbra Webmail Client as a Service Provider in SafeNet Authentication Service:

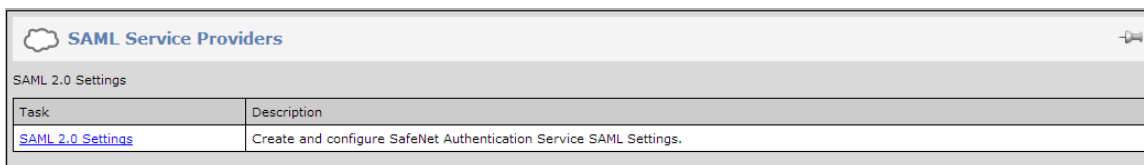
1. Log in to the SafeNet Authentication Service console with an Operator account.



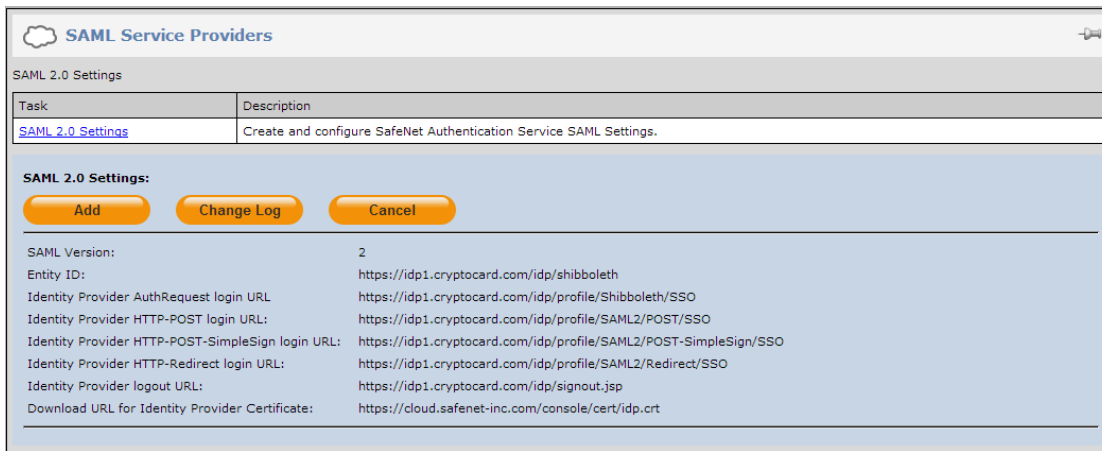
2. Click the **COMMS** tab, and then click **SAML Service Providers**.



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 Zimbra Webmail Client name.
SAML 2.0 Metadata	Select Upload Existing Metadata File . Click Choose File , select the Service Provider's metadata file created previously, and then click Open .



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/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](#)

Zimbra Webmail Client is added as a service provider in the system.

SAML Service Providers

SAML 2.0 Settings

Task	Description
SAML 2.0 Settings	Create and configure SafeNet Authentication Service SAML Settings.

SAML 2.0 Settings:

SAML Version: 2
Entity ID: https://10.164.44.236/ldap/shibboleth
Identity Provider AuthRequest login URL: https://10.164.44.236/ldap/profile/Shibboleth/SSO
Identity Provider HTTP-POST login URL: https://10.164.44.236/ldap/profile/SAML2/POST/SSO
Identity Provider HTTP-POST-SimpleSign login URL: https://10.164.44.236/ldap/profile/SAML2/POST-SimpleSign/SSO
Identity Provider HTTP-Redirect login URL: https://10.164.44.236/ldap/profile/SAML2/Redirect/SSO
Identity Provider logout URL: https://10.164.44.236/ldap/signout
Download URL for Identity Provider Certificate: http://10.164.44.195/console/cert/ldap.crt

Service Provider	Entity ID			
Zimbra	https://10.164.44.110/service/extension/samlreceiver	Edit	Remove	Resync

Enabling SAML Services in SafeNet Authentication Service

After Zimbra Webmail Client 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.

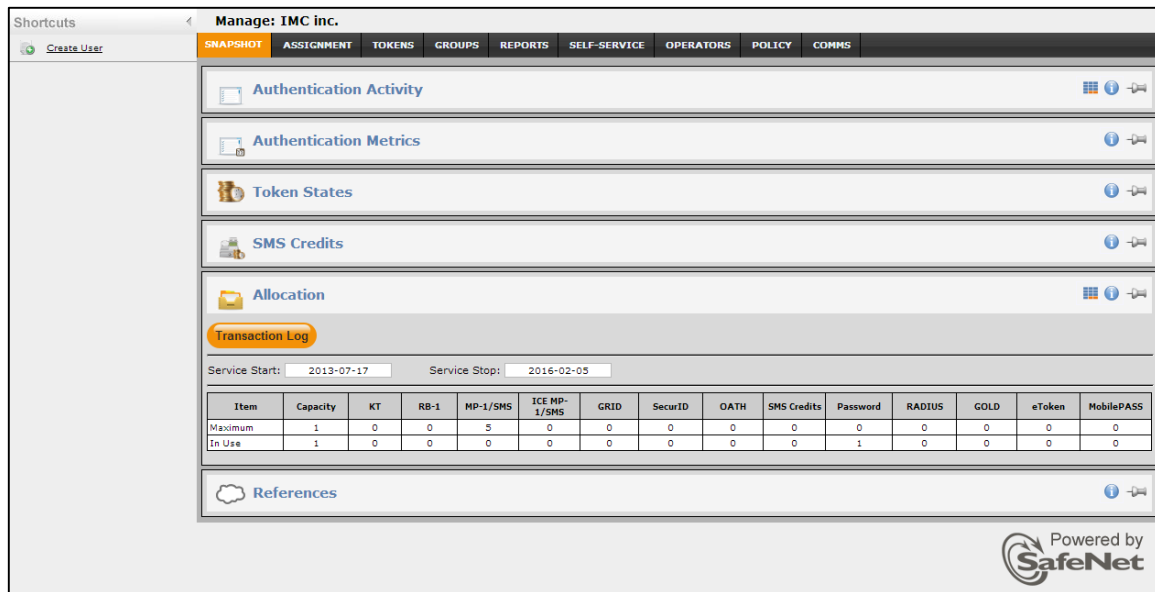
There are two methods to enable the user to use the service provider:

- 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.

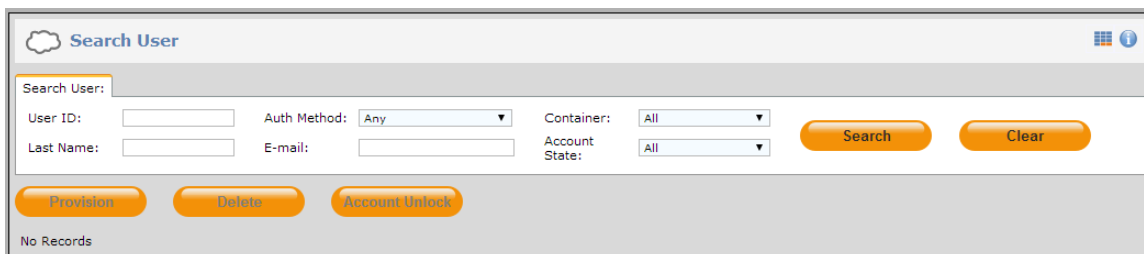
1. Log in to the SafeNet Authentication Service console with an Operator account.



The screenshot shows the 'Manage: IMC inc.' console interface. The 'ASSIGNMENT' tab is selected. The 'Allocation' section is expanded, showing a 'Transaction Log' table. The table has columns for Item, Capacity, KT, RB-1, MP-1/SMS, ICE MP-1/SMS, GRID, SecurID, OATH, SMS Credits, Password, RADIUS, GOLD, eToken, and MobilePASS. The 'In Use' row shows 1 user in use for Password authentication.

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



The screenshot shows the 'Search User' interface. It includes search fields for User ID, Last Name, Auth Method, Container, Account State, and E-mail. There are 'Search' and 'Clear' buttons, and 'Provision', 'Delete', and 'Account Unlock' buttons below. The status 'No Records' is displayed at the bottom.

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: 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 Zimbra Webmail Client 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 Zimbra Webmail Client in the response.
- c. Click **Add**.

Add SAML Service

Service:

SAML Login ID: User ID E-mail Custom

The user can now authenticate to Zimbra Webmail Client using SAML authentication.

SAML Services

Index	SAML Service	User ID	Status		
i	Zimbra	bob	Active	Edit	Remove

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.

Shortcuts **Manage: IMC inc.**

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

Authentication Activity

Authentication Metrics

Token States

SMS Credits

Allocation

Transaction Log

Service Start: 2013-07-17 Service Stop: 2016-02-05

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

References

Powered by **SafeNet**

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

- 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

- 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

- 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

To verify this solution, you need to log on to Zimbra Webmail Client, which uses SAML authentication with SafeNet Authentication Service.

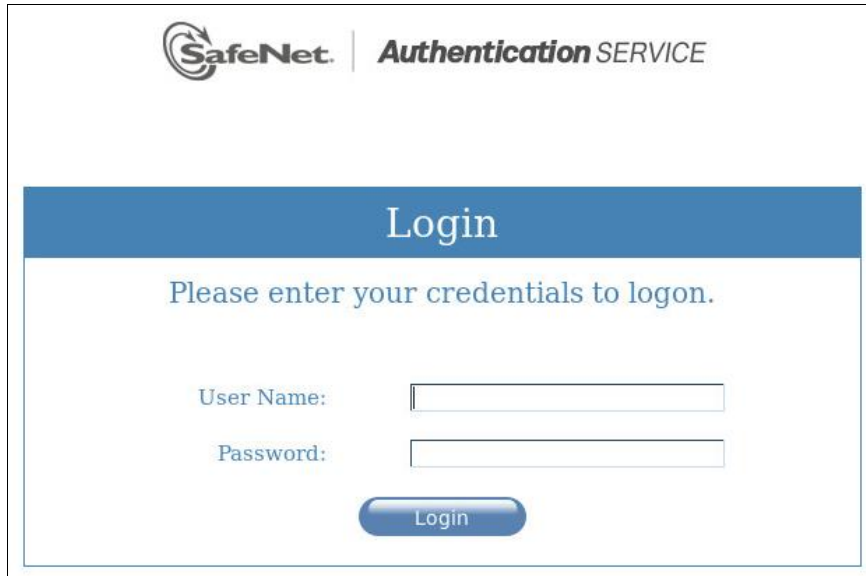
For this integration, SafeNet eToken PASS is configured for authentication with the SAS solution.

1. Open a web browser and enter the Zimbra Webmail Client login URL:

https://<Zimbra Server Host Name>

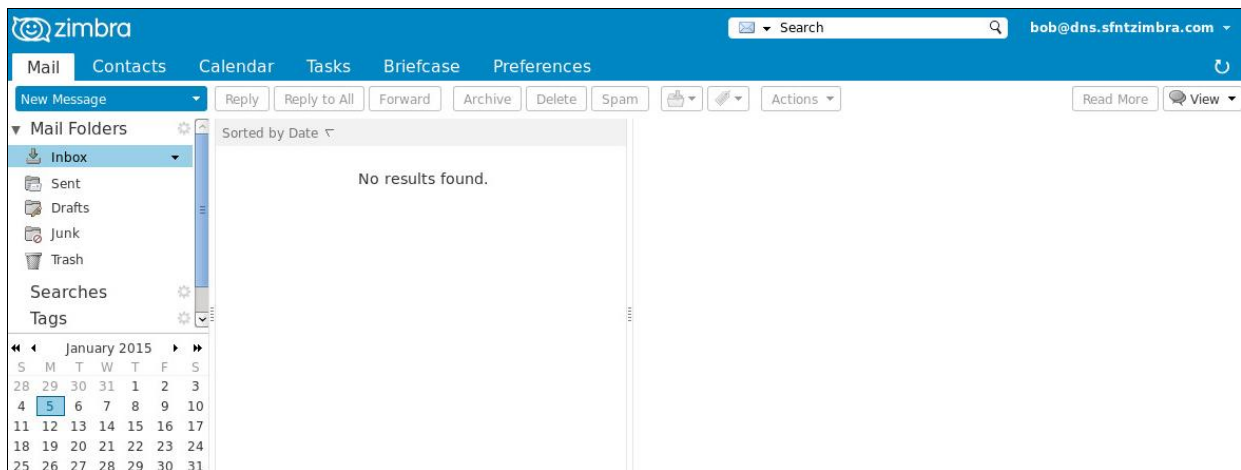
You are redirected to the SAS login page.

2. In **User Name** field, enter your user name.



3. Generate an OTP using SafeNet eToken PASS and enter it in the **Password** field. Click **Login**.

After successful authentication, the browser is redirected to the default Zimbra mail URL.



(The screen image above is from Zimbra®. 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.	