

SafeNet Authentication Service Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Wrike

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.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto 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: 007-013639-001, Rev. A

Release Date: November 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-PCE	5
SAML Authentication Flow using SafeNet Authentication Service	6
SAML Prerequisites	6
Configuring Wrike	6
Downloading the SafeNet Authentication Service Metadata	6
Downloading the SafeNet Identity Provider Certificate	6
Configuring SafeNet Authentication Service	7
Synchronizing Users Stores to SafeNet Authentication Service.....	7
Assigning an Authenticator in SafeNet Authentication Service.....	7
Adding Wrike as a Service Provider (SP) in SafeNet Authentication Service	8
Enabling SAML Services in SafeNet Authentication Service	11
Running the Solution	16
Support Contacts	19

Third-Party Software Acknowledgement

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

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 (SAS) provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Wrike combines project management with a real time work space for collaboration, discussion, and document sharing. Wrike is a real-time workspace, where teams collaborate to get the job done. Enterprise user can access Wrike with corporate credentials if SAML-based SSO (SSO/SAML integration) is enabled for their subscription. Wrike supports SAML2.0 as a service provider.

This document describes how to:

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

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

Wrike 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:

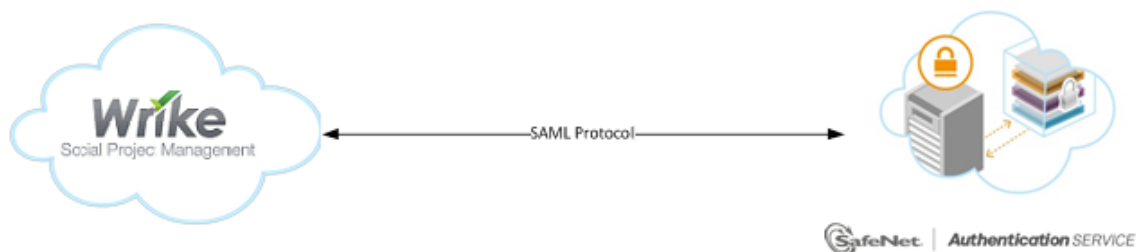
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)** — Mention only if SAS-PCE is relevant. Add version number to the SAS-PCE.
- **Wrike**

Audience

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



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

SAML Prerequisites

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

Configuring Wrike

You cannot access the IDP configuration console of Wrike. To configure SAS cloud as IDP in Wrike, please contact to the Wrike support team (email ID: support@team.wrike.com) and provide the SAS metadata. The Wrike support team will configure the IDP settings for you.

Downloading the SafeNet Authentication Service Metadata

Browse to the <https://idp1.cryptocard.com/idp/shibboleth> URL. The SafeNet Authentication Service (SAS) metadata will be downloaded automatically. Save it locally on your machine.

Downloading the SafeNet Identity Provider Certificate

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

Configuring SafeNet Authentication Service

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

- Synchronizing Users Stores to SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 7
- Adding Wrike as a Service Provider (SP) in SafeNet Authentication Service. page 8
- Enabling SAML Services in SafeNet Authentication Service, page 11

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*:

https://safenet.gemalto.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 Wrike.

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.

https://safenet.gemalto.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Account_Operator_Guide/

Adding Wrike 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 Wrike. You will need the Wrike metadata. Open the <https://www.wrike.com/saml/metadata> link in a web browser to download the Wrike metadata file.

To add Wrike as a Service Provider in SafeNet Authentication Service (SAS):

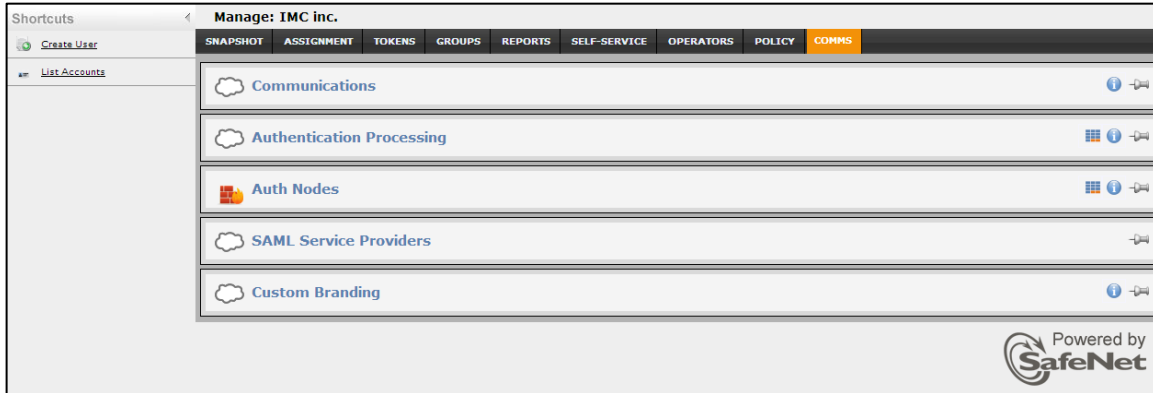
1. Log in to the SafeNet Authentication Service console with an Operator account.

The screenshot shows the SafeNet Authentication Service console interface. The top navigation bar includes tabs for SNAPSHOT, ASSIGNMENT, TOKENS, GROUPS, REPORTS, SELF-SERVICE, OPERATORS, POLICY, and COMMS. The main content area is titled "Allocation" and features a "Transaction Log" button. Below this, there are date pickers for "Service Start" (2013-07-17) and "Service Stop" (2016-02-05). A table displays the following data:

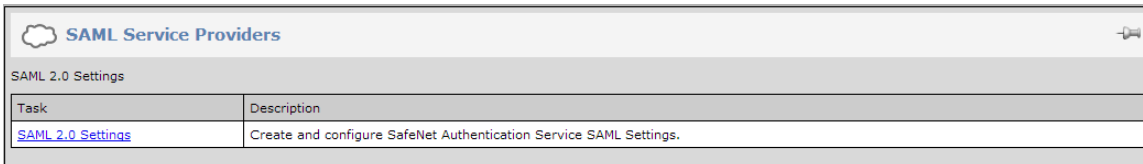
Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	0

At the bottom right of the console, it says "Powered by SafeNet".

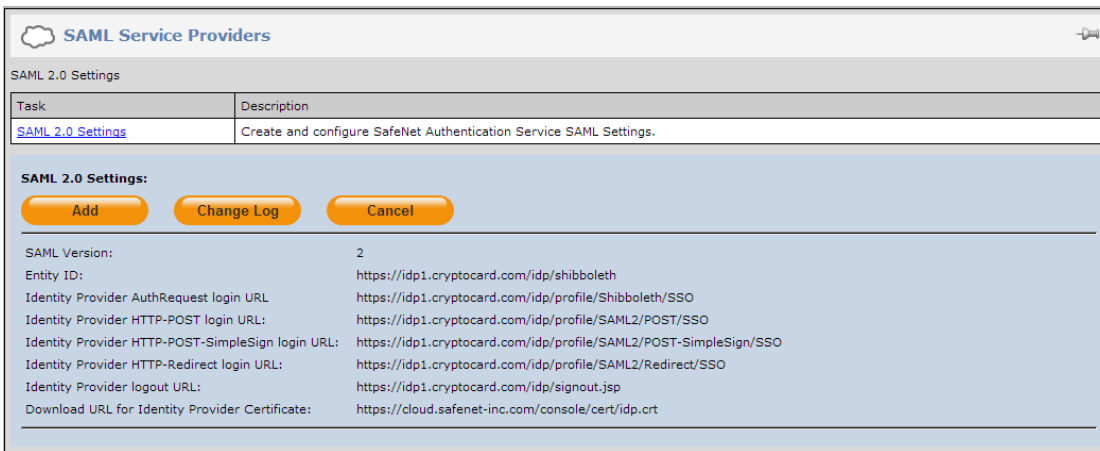
- Click the **COMMS** tab, and then click **SAML Service Providers**.



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

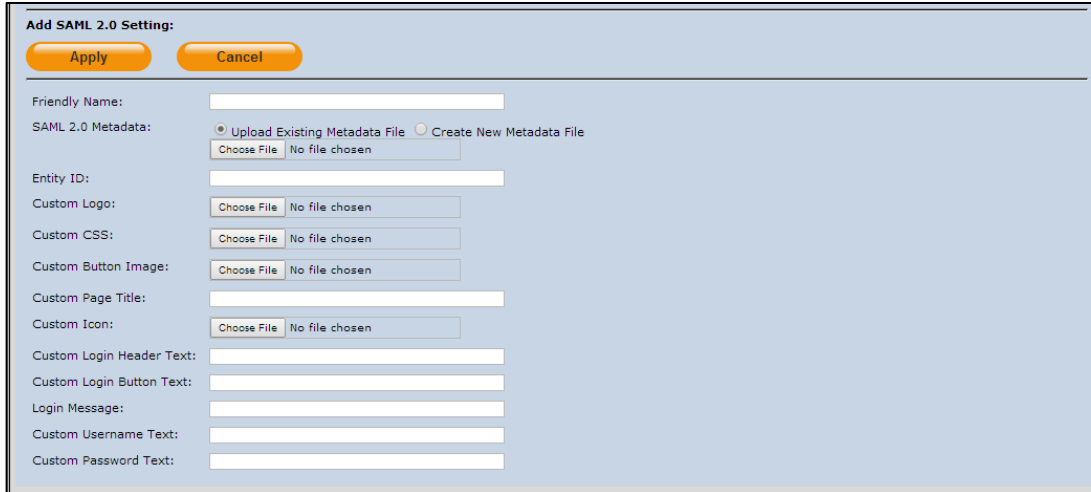


- Click **Add**.



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

Friendly Name	Enter the Wrike name.
SAML 2.0 Metadata	Select Upload Existing Metadata File . Click Choose File to search for and select the Service Provider's metadata file, and then click Open .




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

https://safenet.gemalto.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__SAML_Authentication_Quick_Start_Guide/

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](#)

Wrike is added as a service provider in the system.

SAML 2.0 Settings:

SAML Version: 2

Entity ID: <https://idp1.cryptocard.com/idp/shibboleth>

Identity Provider AuthRequest login URL: <https://idp1.cryptocard.com/idp/profile/Shibboleth/SSO>

Identity Provider HTTP-POST login URL: <https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO>

Identity Provider HTTP-POST-SimpleSign login URL: <https://idp1.cryptocard.com/idp/profile/SAML2/POST-SimpleSign/SSO>

Identity Provider HTTP-Redirect login URL: <https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO>

Identity Provider logout URL: <https://idp1.cryptocard.com/idp/signout.jsp>

Download URL for Identity Provider Certificate: <https://cloud.safenet-inc.com/console/cert/idp.crt>

Service Provider	Entity ID			
PingOne	http://pingone.com/safenet/a6899c34-2458-437f-b41f-9a983	Edit	Remove	Resync
BlueCoat	https://10.9.89.11:4433/saml/SAM_SAML	Edit	Remove	Resync
MobileIron	bvodportal-ssg	Edit	Remove	Resync
Wrike	https://www.wrike.com	Edit	Remove	Resync

Enabling SAML Services in SafeNet Authentication Service

After Wrike 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.

Shortcuts Manage: IMC inc.

Create User

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

Search User

Search User:

User ID: Auth Method: Any Container: All

Last Name: E-mail: Account State: All

Search Clear

Provision Delete Account Unlock

No Records

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

Search User

Search User:

User ID: Bob Auth Method: Any Container: All

Last Name: Hansen E-mail: Account State: All

Search Clear

Provision Delete Account Unlock

User ID	Last Name	First Name	Account Owner	Auth Method	RADIUS Attr	Auth State	Account State	Container
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

Edit Delete Change Log Return

First Name: Bob Address: Phone: Alias #1:
Last Name: Hansen Extension: Alias #2:
User ID: BobH City: Emergency:
E-mail: Bob@safenet-inc.com State Account Owner:
Mobile/SMS: Country: Custom #2:
Container: Default Postal/Zip: Custom #3:

Tokens

Authentication Metrics

Authentication Activity

Access Restrictions

Group Membership

RADIUS Attributes (user)

SAML Services

5. Click **Add**.

SAML Services

Add Change Log

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

- From the **Service** menu, select the Wrike service provider.
- In **SAML Login ID** field, select the type of login ID (User ID, E-mail, or Custom) to be sent as **Email** to Wrike in the response.
- Click **Add**.

SAML Services

Add Change Log

Add SAML Service

Add Cancel

Service: Wrike

SAML Login ID: User ID Email Custom

The user can now authenticate to Wrike using SAML authentication.

Index	SAML Service	User ID	Status		
1	Wrike	Yateendra.Jaiman@safenet-inc.com	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.

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

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	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 E-mail . The E-mail will be returned to the service provider in the SAML assertion.

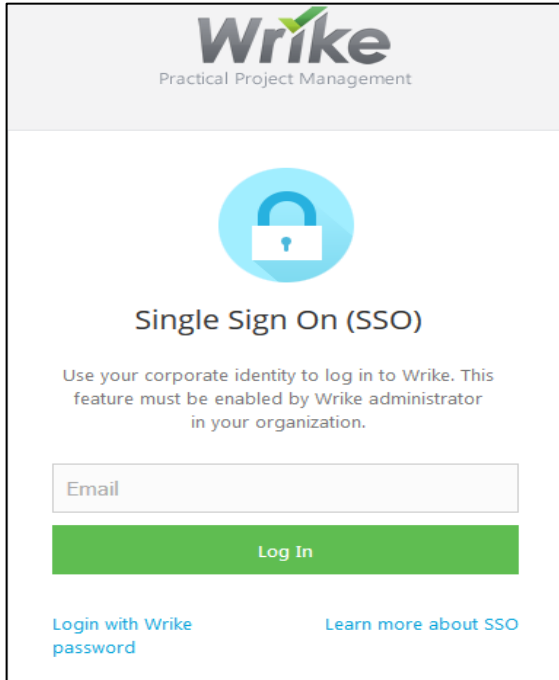
Running the Solution

Before running this section, user should be subscribed with Wrike enterprise account. User is enrolled with Grid sure token on SafeNet Authentication Service (SAS).

1. In a web browser, open the following URL:

wrike.com/sso

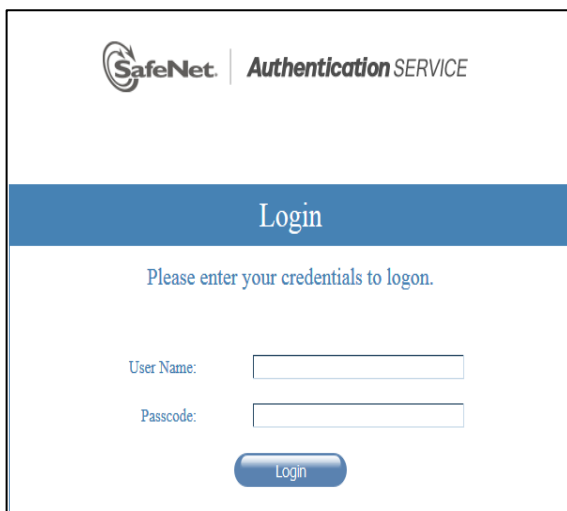
2. On the Wrike **Single Sign On (SSO)** window, enter your company's (SSO) E-mail ID, and then click **Log In**.



The screenshot shows the Wrike Single Sign On (SSO) login interface. At the top, the Wrike logo is displayed with the tagline "Practical Project Management". Below the logo is a blue circular icon containing a white padlock. The heading "Single Sign On (SSO)" is centered. A message states: "Use your corporate identity to log in to Wrike. This feature must be enabled by Wrike administrator in your organization." Below this is a text input field labeled "Email". A prominent green button labeled "Log In" is positioned below the email field. At the bottom left, there is a link "Login with Wrike password" and at the bottom right, a link "Learn more about SSO".

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

3. You will be redirected to the SAS login page. In the **User Name** field, enter your SAS User ID, and then click on **Login**.



The screenshot displays the SafeNet Authentication Service login page. At the top left, the SafeNet logo is shown next to the text "Authentication SERVICE". A blue horizontal bar with the word "Login" in white is centered. Below this bar, the instruction "Please enter your credentials to logon." is displayed. There are two input fields: "User Name:" followed by a text box, and "Passcode:" followed by a text box. A blue button labeled "Login" is located below the passcode field.

4. In the **Passcode** field, enter your Personal Identification Pattern (PIP), and then click **Login**.

SafeNet Authentication SERVICE

Login

Please enter your credentials to logon.

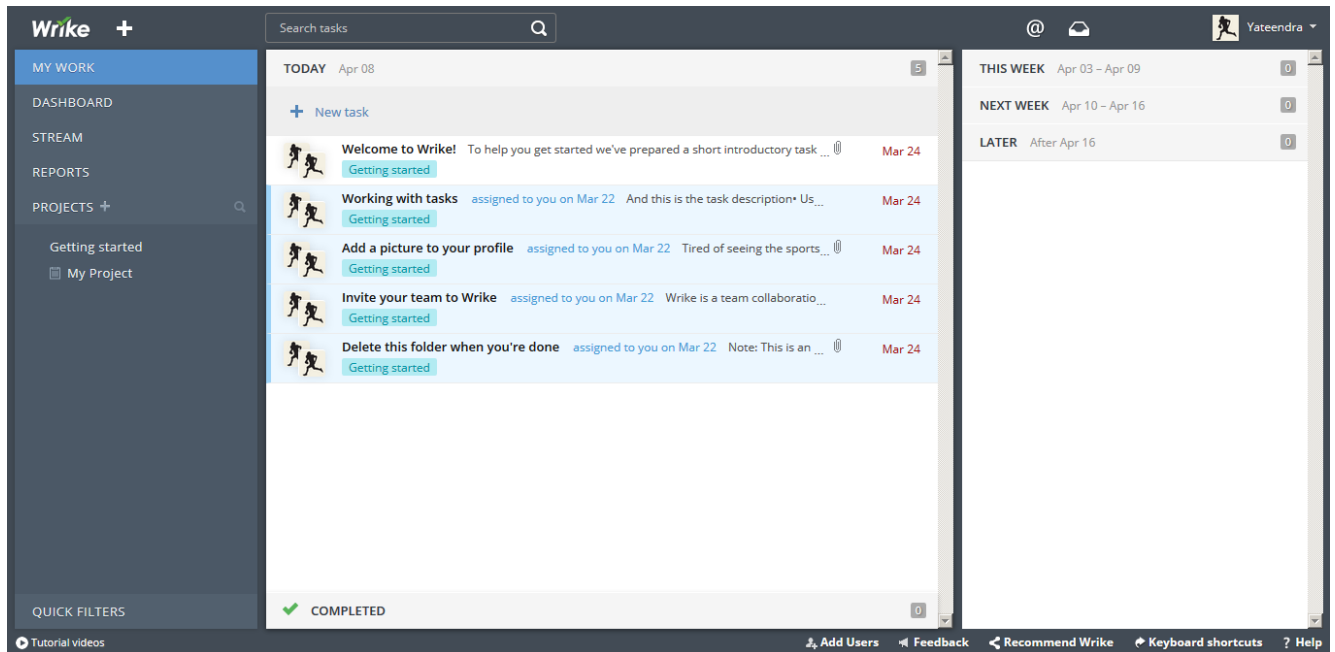
Please enter characters in sequence corresponding to your chosen pattern.

2	4	6	6	1
8	5	1	6	8
2	9	9	7	2
0	7	5	9	4
3	8	7	0	3

Passcode:

Login

After successful authentication, you will be able to access the Wrike workspace.



(The screen image above is from Wrike 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 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 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.	