

RSA SECURID[®] ACCESS

Implementation Guide

Mattermost

Gina Salvazo, RSA Partner Engineering
Last Modified: January 11, 2018

Solution Summary

Mattermost is an open source, private cloud and Slack-alternative used for workplace communication. Mattermost delivers a single sign on experience to the user through SAML. This integration supports both IdP and SP initiated authentication flows.

RSA SecurID Access Features	
Mattermost	
On Premise Methods	
RSA SecurID	<input checked="" type="checkbox"/>
On Demand Authentication	<input checked="" type="checkbox"/>
Risk-Based Authentication (AM)	<input type="checkbox"/>
Cloud Authentication Service Methods	
Authenticate App	<input checked="" type="checkbox"/>
FIDO Token	<input checked="" type="checkbox"/>
SSO	
SAML SSO	<input checked="" type="checkbox"/>
HFED SSO	<input type="checkbox"/>

Identity Assurance	
Collect Device Assurance and User Behavior	<input checked="" type="checkbox"/>

Configuration Summary

All of the supported use cases of RSA SecurID Access with Mattermost require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Mattermost can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

[Cloud Authentication Service – Identity Router IdP Configuration](#)
[Mattermost SAML Configuration](#)

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

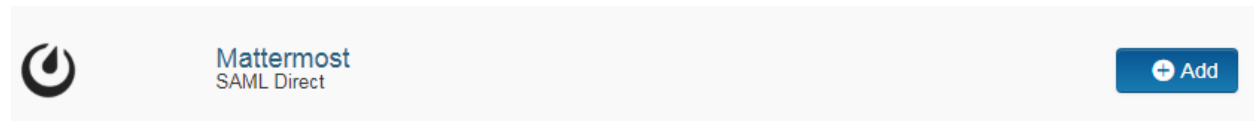
SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Mattermost in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.


Configure RSA Identity Router SAML IdP

Procedure

1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for Mattermost and click **+Add** to add the connector.



2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
 - a. In the **Connection URL** field, keep the field blank as the value is not required.
 - b. Choose **IDP-initiated**.

 **Note:** The following IdP-initiated configuration works for SP-initiated Mattermost connections as well.

Initiate SAML Workflow

Connection URL 


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

4. Scroll down to SAML Identity Provider (Issuer) section.

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

- Default (idp_id): 1x7a2vkz08ti4
- Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

private.key ?

cert.pem

Certificate valid until: Sun Aug
11 10:04:12 UTC 2019

Include Certificate in Outgoing Assertion

- a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
- b. Select **Override** for value for the **Issuer Entity ID**. Replace <IDP_URL> with your Identity provider login URL. For example: <https://portal.sso5.pe-lab.com>
- c. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
- d. Select **Choose File** and upload the private key.
- e. Select **Choose File** to import the public signing certificate.
- f. Select the checkbox for **Include Certificate in Outgoing Assertion**.
- g. Note the value of Issuer Entity ID.

Mattermost

5. Scroll down to the **Service Provider** section.

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<SITE_URL>/login/sso/saml

Audience (Service Provider Entity ID) ?

https://<SITE_URL>

6. In the **Assertion Consumer Service (ACS) URL** field, provide the **value** as per received with service provider metadata. Replace <SITE_URL> with your Mattermost server Site URL.
7. In the **Audience (Service Provider Issuer ID)** field, provide the value as per received with service provider metadata. Replace <SITE_URL> with your Mattermost server Site URL.
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.

User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD20

Property ?

mail






Attribute Hunting ?

NameID Attribute Hunting

8. Click Show Advanced Configuration.
9. Under Attribute Extension verify the settings are correct for your environment. In this example, *Email* will be validated against *mail* and *Username* will be validated against *givenName* from the user store selected.

^ Hide Advanced Configuration

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc	Email	AD20	mail	 
Identity Sc	Username	AD20	givenName	 
 ADD				


Mattermost


10. Click **Next Step**.
12. On the User Access page, select **Allow All Authenticated Users** user policy from the available options.

Access Policy

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy 

No Access Allowed 

13. Click **Next Step**.
14. On the **Portal Display** page, select **Display in Portal**.
15. Click **Save and Finish**.
16. Click **Publish Changes**. Your application is now enabled for SSO.

Publish Changes

Status:  Changes Pending

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Mattermost with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

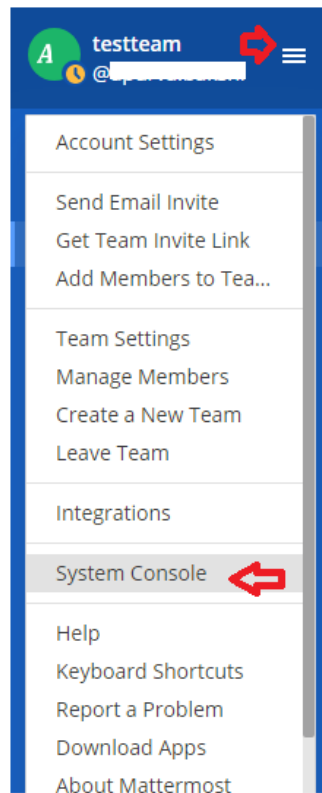
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Mattermost components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Mattermost SAML Configuration

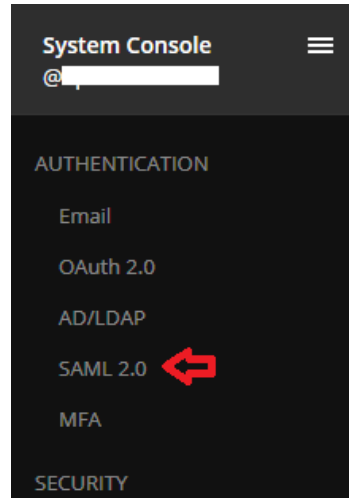
Procedure

1. Login to your Mattermost server as an Administrator.
https://<SITE_URL>
2. On the displayed page, in the left panel, click on the options button to the right of your Username. Click on ***System Console***.



Mattermost

3. On the System Console, scroll down left panel to *Authentication* Section. Click on **SAML 2.0** option.



4. On the displayed page, select **true** for *Enable Login With SAML 2.0*. If you wish to sync your SAML accounts with AD/LDAP select **true** for *Enable Synchronizing SAML Accounts With AD/LDAP*.

SAML 2.0

User attributes in SAML server, including user deactivation or removal, are updated in Mattermost during user login. Learn more at: <https://docs.mattermost.com/deployment/sso-saml.html>

Enable Login With SAML 2.0: true false

When true, Mattermost allows login using SAML 2.0. Please see [documentation](#) to learn more about configuring SAML for Mattermost.

Enable Synchronizing SAML Accounts With AD/LDAP: true false

When true, Mattermost periodically synchronizes SAML user attributes, including user deactivation and removal, from AD/LDAP. Enable and configure synchronization settings at [Authentication > AD/LDAP](#). See [documentation](#) to learn more.

Mattermost

5. Scroll down to the next section.

SAML SSO URL:	<input type="text" value="https://portal.sso5.pe-lab.com/IdPServlet?idp_id=1x7a2vkz08ti4"/>
	The URL where Mattermost sends a SAML request to start login sequence.
Identity Provider Issuer URL:	<input type="text" value="https://portal.sso5.pe-lab.com"/>
	The issuer URL for the Identity Provider you use for SAML requests.
Identity Provider Public Certificate:	<input type="button" value="Choose File"/> <input type="button" value="Upload"/>
	No file uploaded
	The public authentication certificate issued by your Identity Provider.
Verify Signature:	<input checked="" type="radio"/> true <input type="radio"/> false

- In **SAML SSO URL** field, enter your IDP URL.
- In the **Identity Provider Issuer URL** field, enter [IDP URL](#).
- For **Identity Provider Public Certificate** field, click on *Choose File* and select [Public certificate](#) of your IDP.
- In the **Verify Signature** field, select *true* radio button.

6. Scroll down to the next section.

Service Provider Login URL:	<input type="text" value="https://mmost.dyn.pontus.lab.emc.com/login/sso/saml"/>
	This field is also known as the Assertion Consumer Service URL.
Enable Encryption:	<input type="radio"/> true <input checked="" type="radio"/> false
	When false, Mattermost will not decrypt SAML Assertions encrypted with your Service Provider Public Certificate. Not recommended for production environments. For testing only.
Service Provider Private Key:	<input type="button" value="Choose File"/> <input type="button" value="Upload"/>
	No file uploaded
	The private key used to decrypt SAML Assertions from the Identity Provider.
Service Provider Public Certificate:	<input type="button" value="Choose File"/> <input type="button" value="Upload"/>

- Note the value of **Service Provider Login URL**. This is the ACS URL value.
- Select *false* for **Enable Encryption** radio button.
The *Service Provider Private Key* and *Service Provider Public Certificate* fields will get disabled.

Mattermost

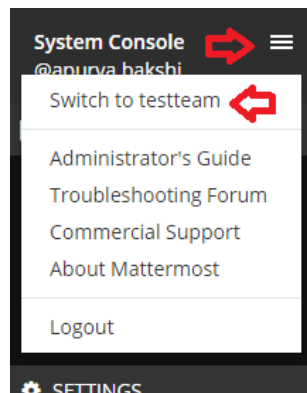
7. In the next section,

Email Attribute:	<input type="text" value="Email"/>
	The attribute in the SAML Assertion that will be used to populate the email addresses of users in Mattermost.
Username Attribute:	<input type="text" value="Username"/>
	The attribute in the SAML Assertion that will be used to populate the username field in Mattermost.

- In **Email Attribute** section, enter *Email* as the value.
 - In **Username Attribute** section, enter *Username* as the value.
 - Fields below it are optional, leave them blank.
8. Scroll down to the end of the page, in the **Login Button Text** field enter a name for the button, such as *RSA SecurID Access*. Click on **Save**.

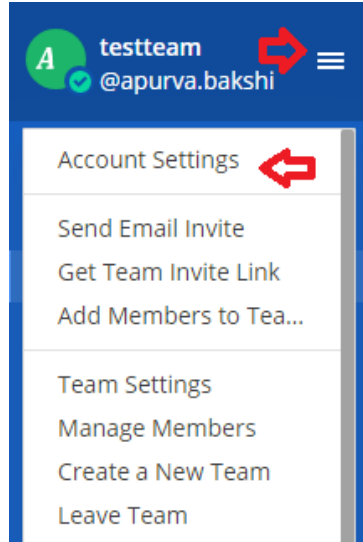
Login Button Text:	<input type="text" value="RSA SecurID Access"/>
	(Optional) The text that appears in the login button on the login page. Defaults to "With SAML".

9. In the left panel, click on *options* and select *Switch to <TEAM_NAME>* as shown below.

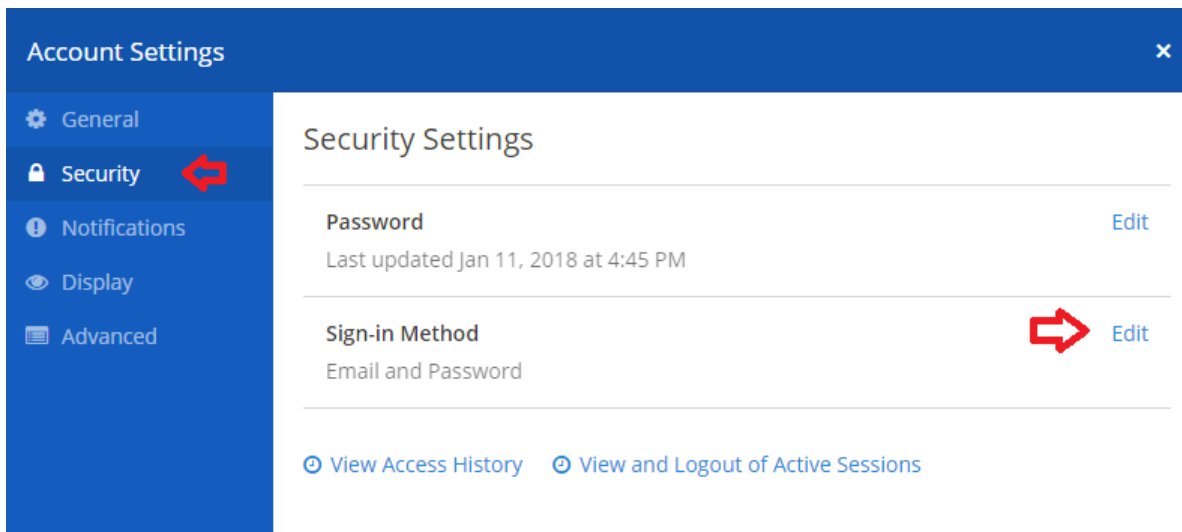


Mattermost

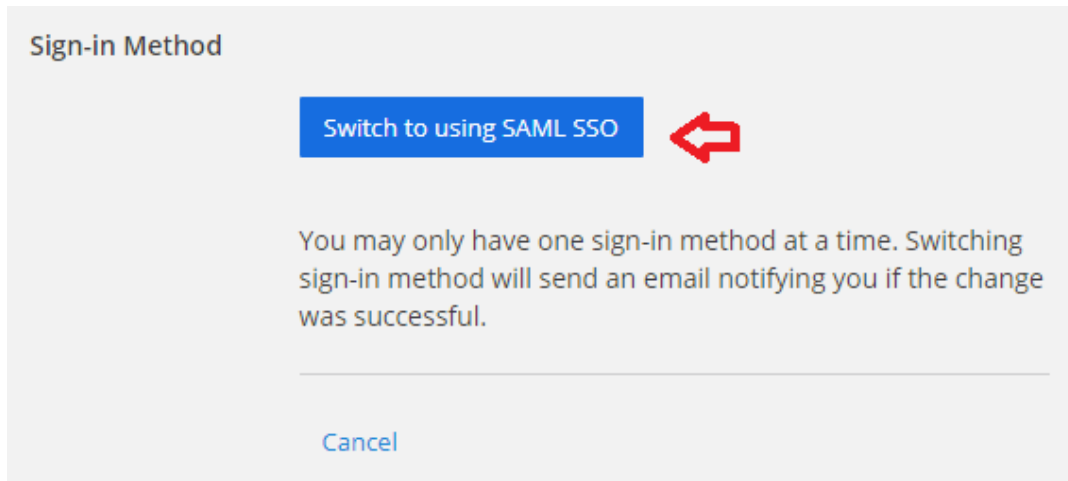
10. On the displayed page, click on *options* and select **Account Settings** as shown below.



11. A pop up will be displayed. Go to Security tab and click on *Edit* in the **Sign-in Method** section.



12. Click on **Switch to using SAML SSO** button.



Sign-in Method

[Switch to using SAML SSO](#)

You may only have one sign-in method at a time. Switching sign-in method will send an email notifying you if the change was successful.

[Cancel](#)

13. You will get prompt for account password. Submit your password and it will redirect you to IDR to test SAML flow.

Switch Email/Password Account to SAML SSO

Upon claiming your account, you will only be able to login with SAML SSO

You must already have a valid SAML account

Enter the password for your Mattermost account

[Switch account to SAML SSO](#)

14. Your Mattermost account is now enabled for SAML Single Sign on.