RSA SECURID® ACCESS
Implementation Guide

Mattermost

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

RSA READY

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	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	✓
SSO	
SAML SSO	✓
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	✓

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

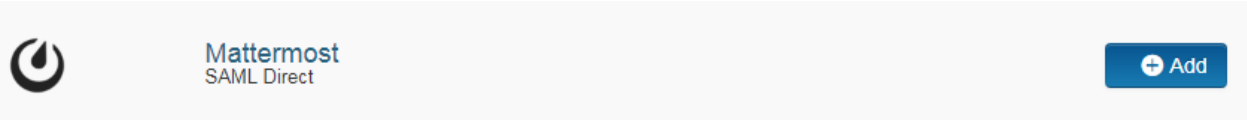
SAML via RSA Identity Router (IdP)

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

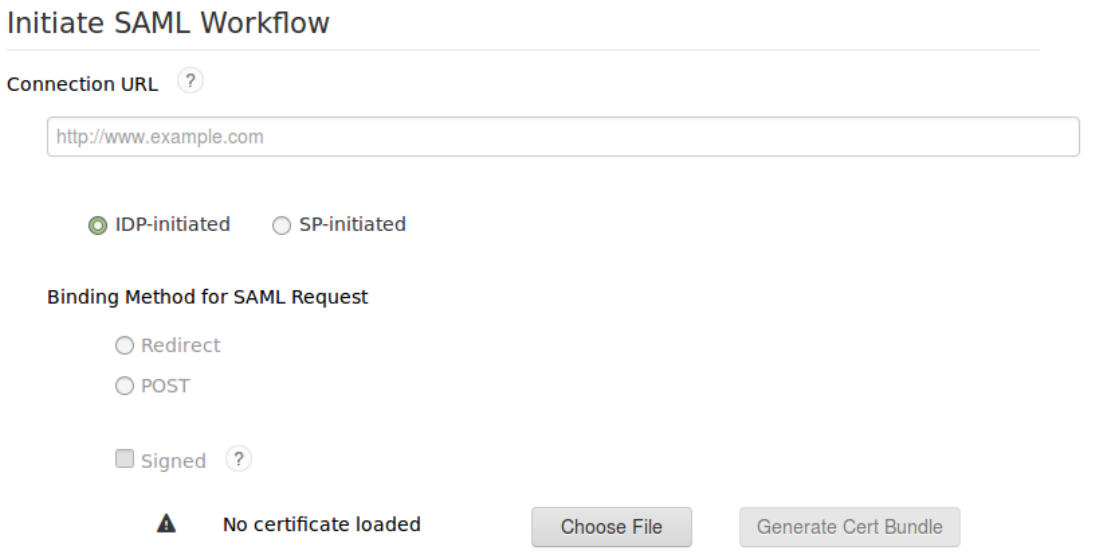
Procedure

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

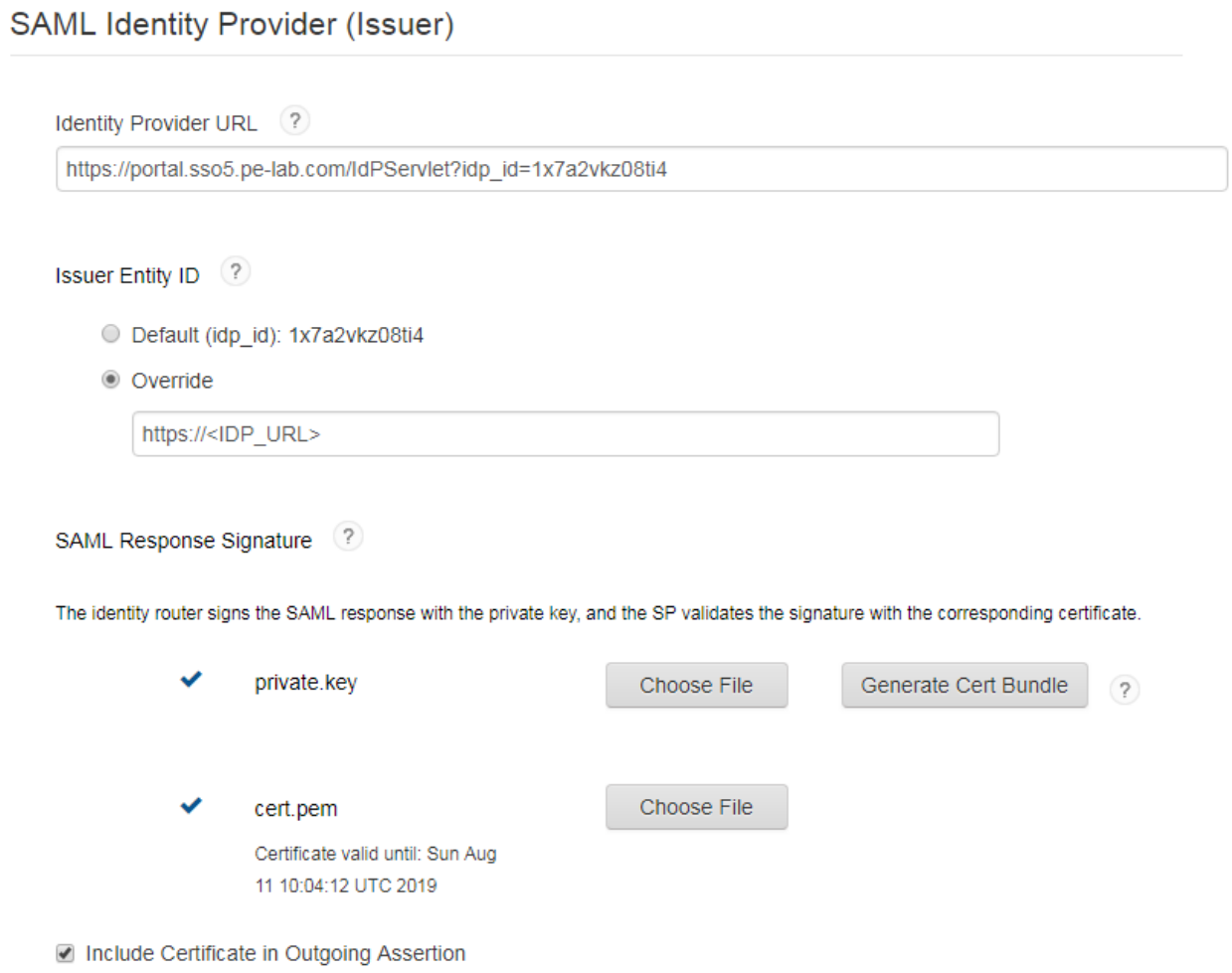


2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
    a. In the **Connection URL** field, keep the field blank as the value is not required.
    b. Choose **IDP-initiated.**

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



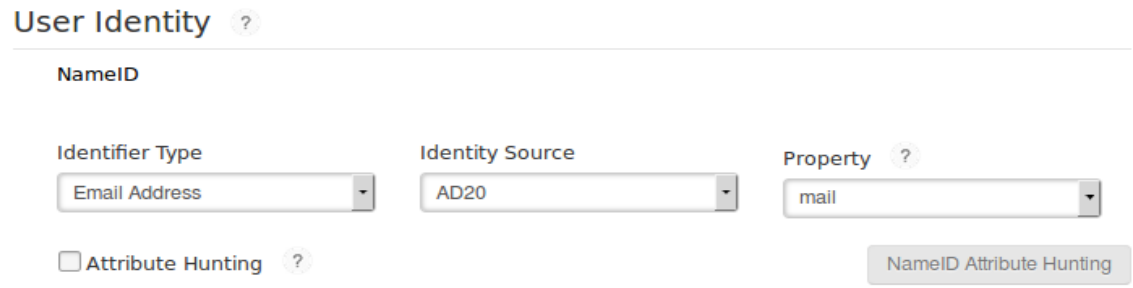
4. Scroll down to SAML Identity Provider (Issuer) section.



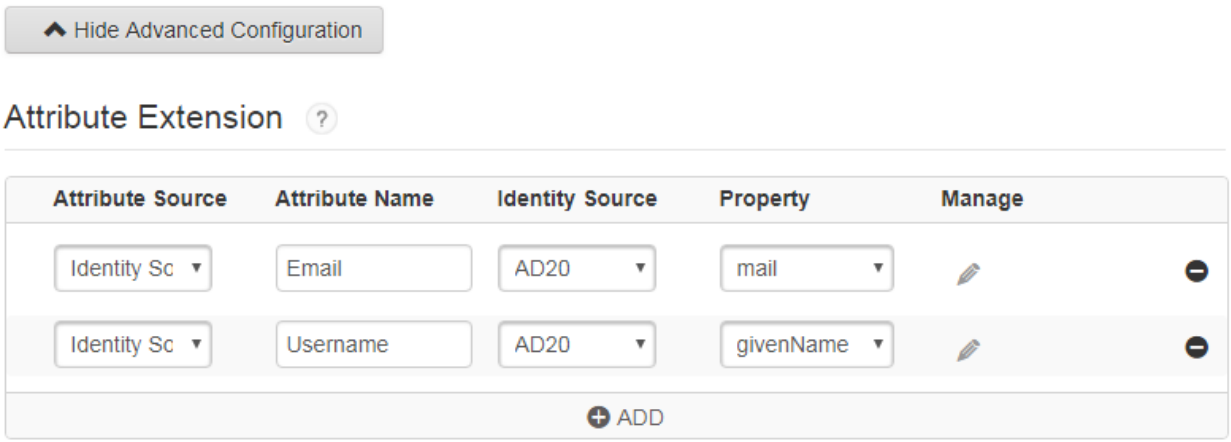
a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Override** for value for the **Issuer Entity ID**. Replace <IDP_URL> with your Identity provider login URL. For example: **https://portal.sso5.pe-lab.com**
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.

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

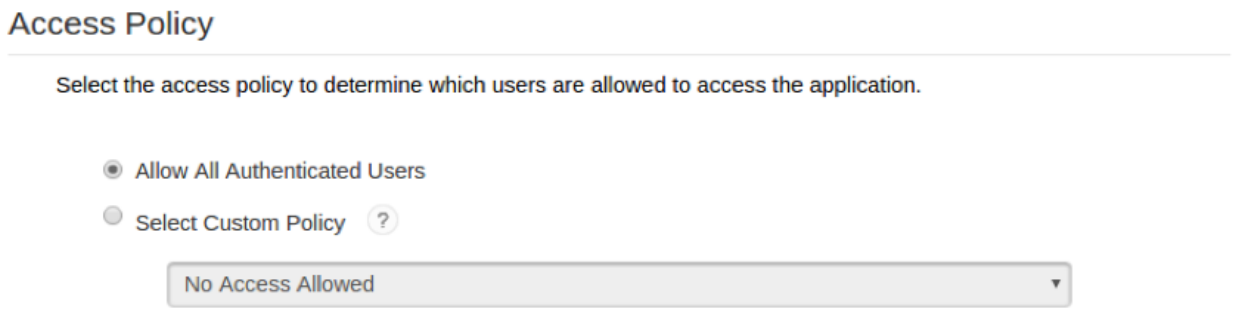
6. In the **Assertion Consumer Service (ACS) URL** field, provide the **value** as per received with service provider metadata. Replace <SITE_URL> with your Mattermost server Site URL.
7. In the **Audience (Service Provider Issuer ID)** field, provide the value as per received with service provider metadata. 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.



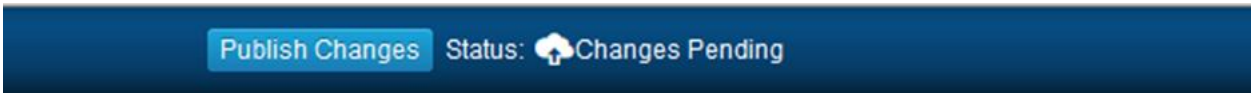
8. Click Show Advanced Configuration.
9. Under Attribute Extension verify the settings are correct for your environment. In this example, *Email* will be validated against *mail* and *Username* will be validated against *givenName* from the user store selected.



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



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.



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.

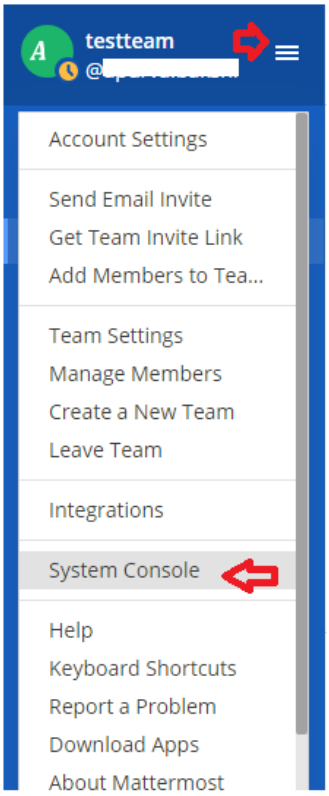
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

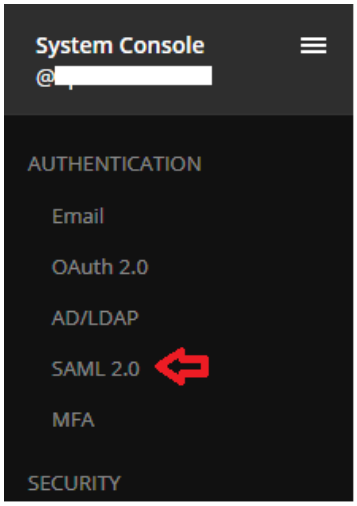
Mattermost SAML Configuration

Procedure

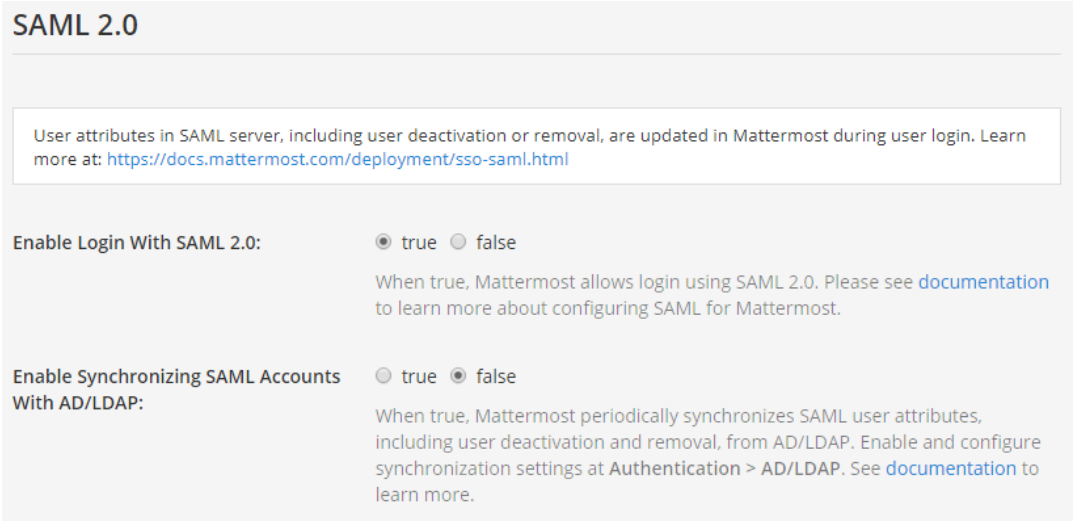
1. Login to your Mattermost server as an Administrator.
   https://<SITE_URL>
2. On the displayed page, in the left panel, click on the options button to the right of your Username. Click on ***System Console***.



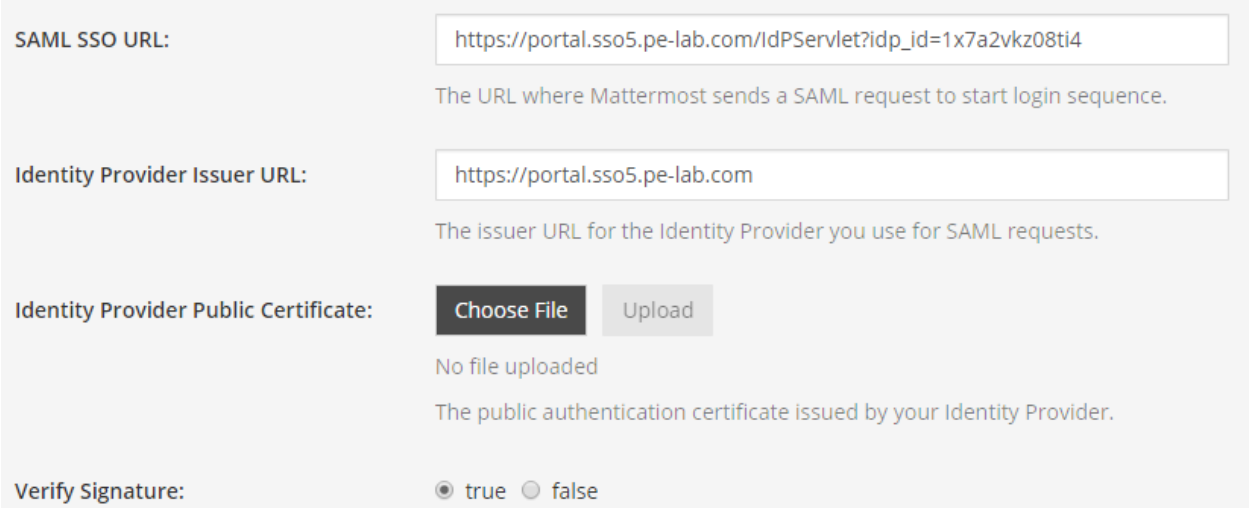
3. On the System Console, scroll down left panel to *Authentication* Section. Click on **SAML 2.0** option.



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*.

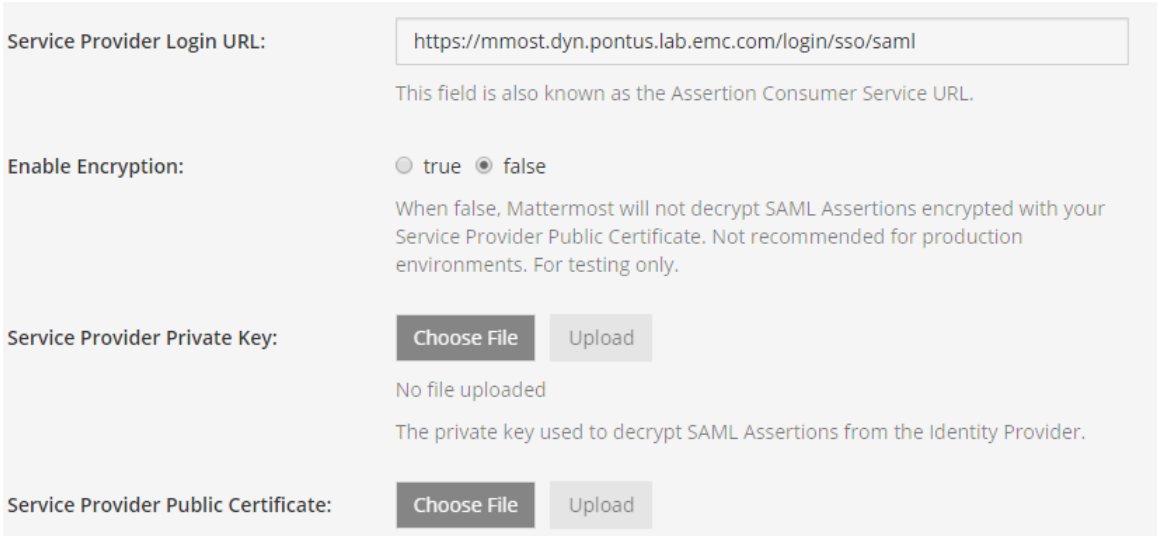


5. Scroll down to the next section.



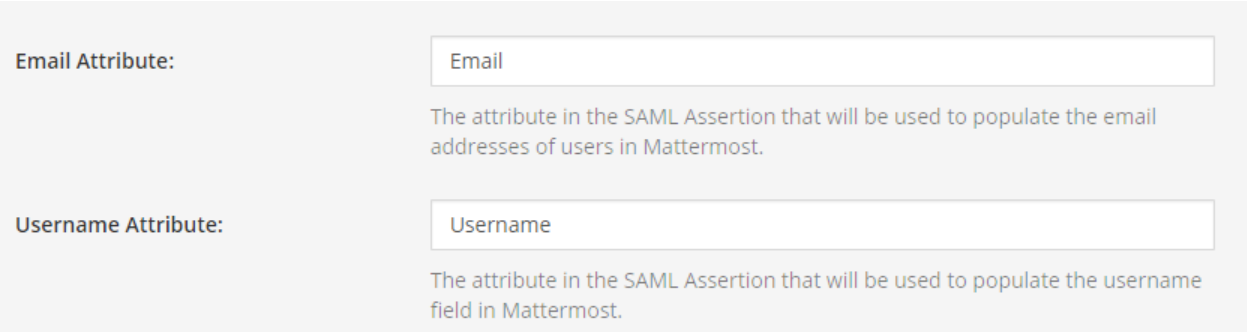
a) In **SAML SSO URL** field, enter your IDP URL.
b) In the **Identity Provider Issuer URL** field, enter **IDP URL**.
c) For **Identity Provider Public Certificate** field, click on *Choose File* and select **Public certificate** of your IDP.
d) In the **Verify Signature** field, select *true* radio button.

6. Scroll down to the next section.



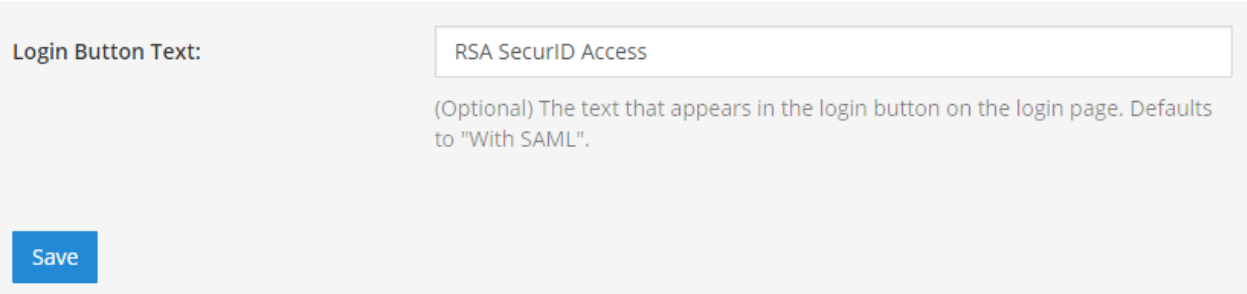
a) Note the value of **Service Provider Login URL**. This is the ACS URL value.
b) Select *false* for **Enable Encryption** radio button.
The *Service Provider Private Key* and *Service Provider Public Certificate* fields will get disabled.

7. In the next section,

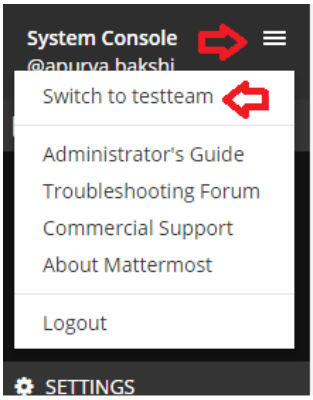


a) In **Email Attribute** section, enter *Email* as the value.
b) In **Username Attribute** section, enter *Username* as the value.
c) Fields below it are optional, leave them blank.

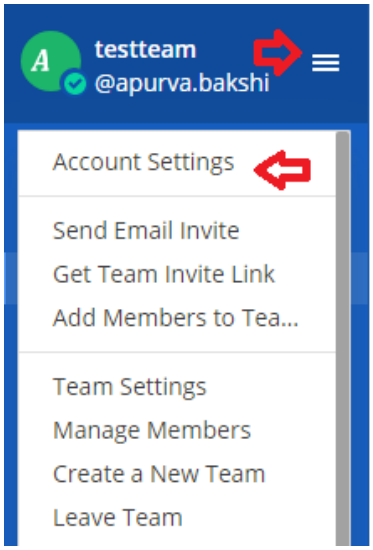
8. Scroll down to the end of the page, in the **Login Button Text** field enter a name for the button, such as *RSA SecurID Access*. Click on **Save**.



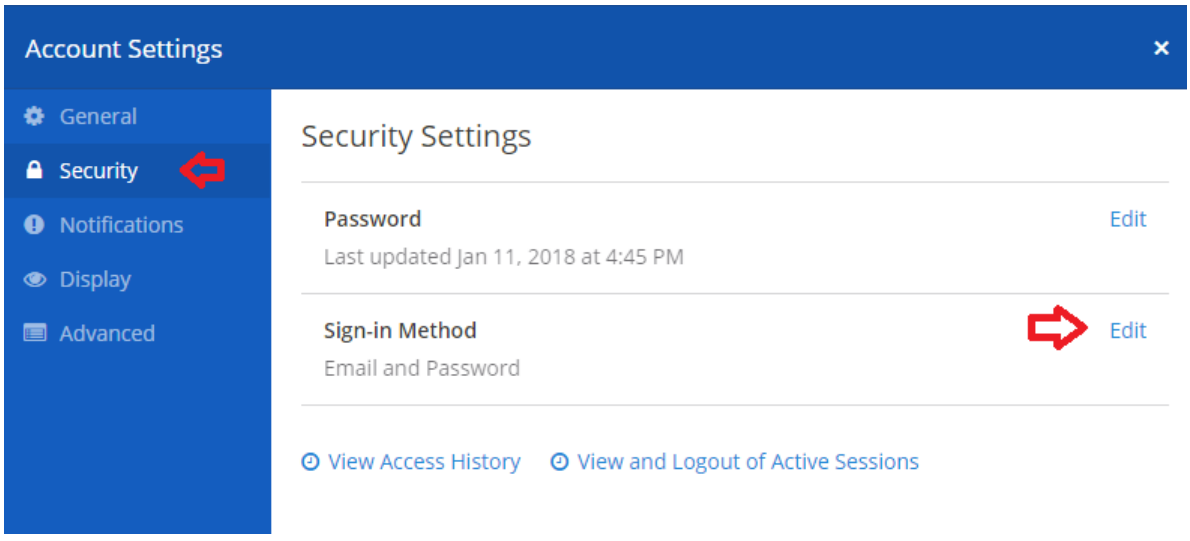
9. In the left panel, click on *options* and select *Switch to <TEAM_NAME>* as shown below.



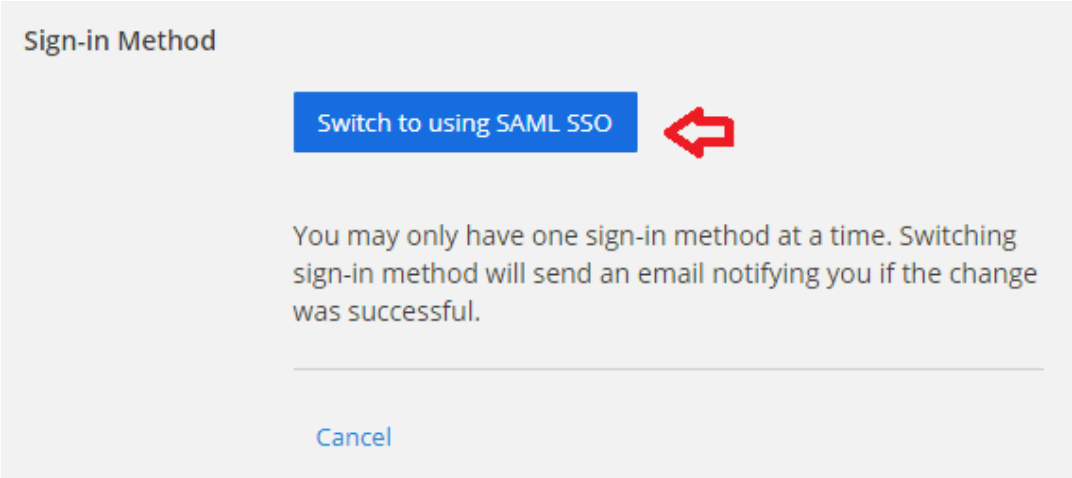
10. On the displayed page, click on *options* and select ***Account Settings*** as shown below.



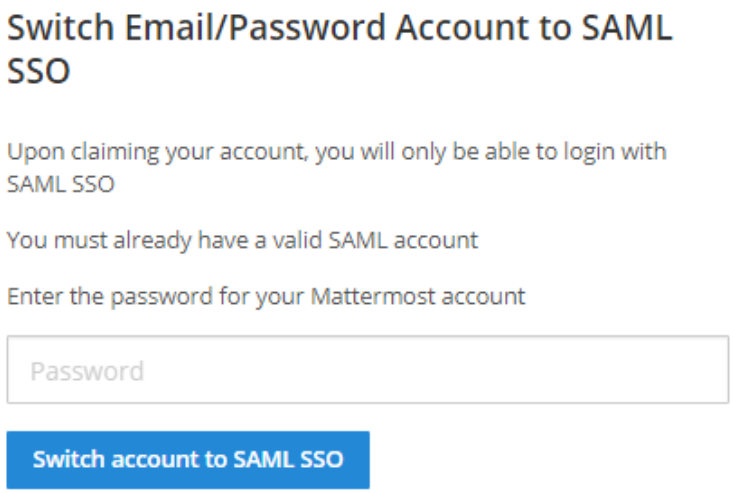
11. A pop up will be displayed. Go to Security tab and click on *Edit* in the **Sign-in Method** section.



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



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



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