RSA SecurID Access SAML Configuration for Jitbit

Last Modified: June 27, 2017

Jitbit Helpdesk ticketing system is ticketing platform for organization. It supports both the cloud-hosted and on premise versions. It also supports auto provisioning for users.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Jitbit.
- Obtain SP metadata details from the Service Provider.

The instructions in this guide use the following SP Login URL, ACS URL and Issuer ID (entity ID) values:

SP Login URL	https://emc.jitbit.com/helpdesk/User/Login
ACS URL	https://emc.jitbit.com/helpdesk/Saml/Consume
Service Provider Issuer ID	http://www.jitbit.com/web-helpdesk/

Procedure

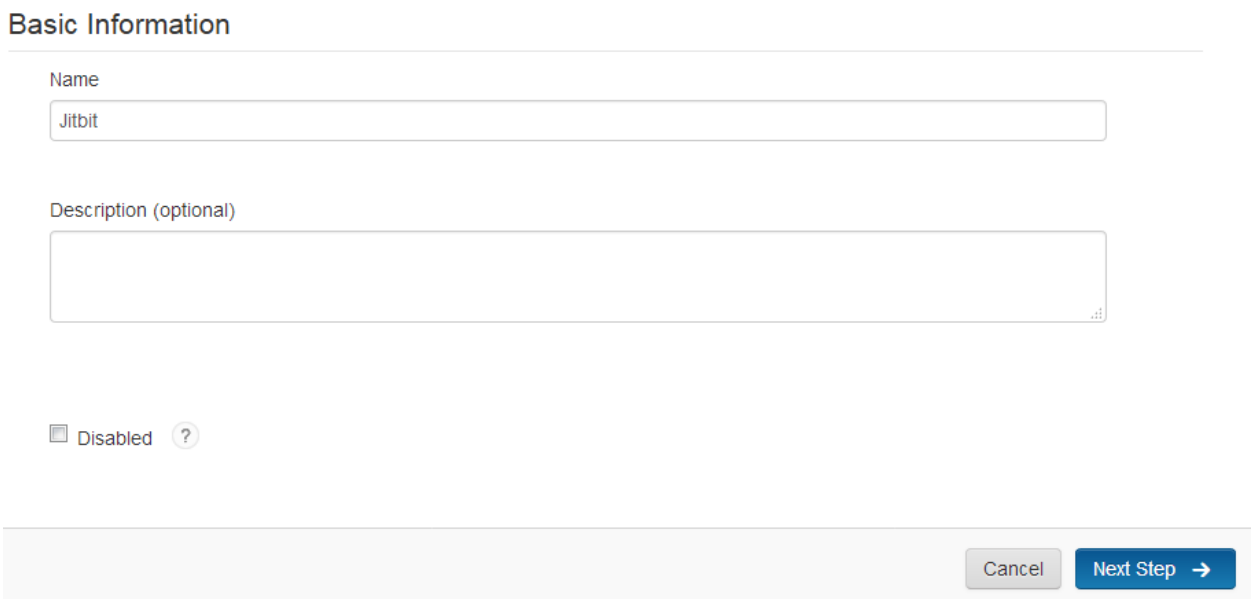
1. Add the Application in RSA SecurID Access
2. Configure Jitbit to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

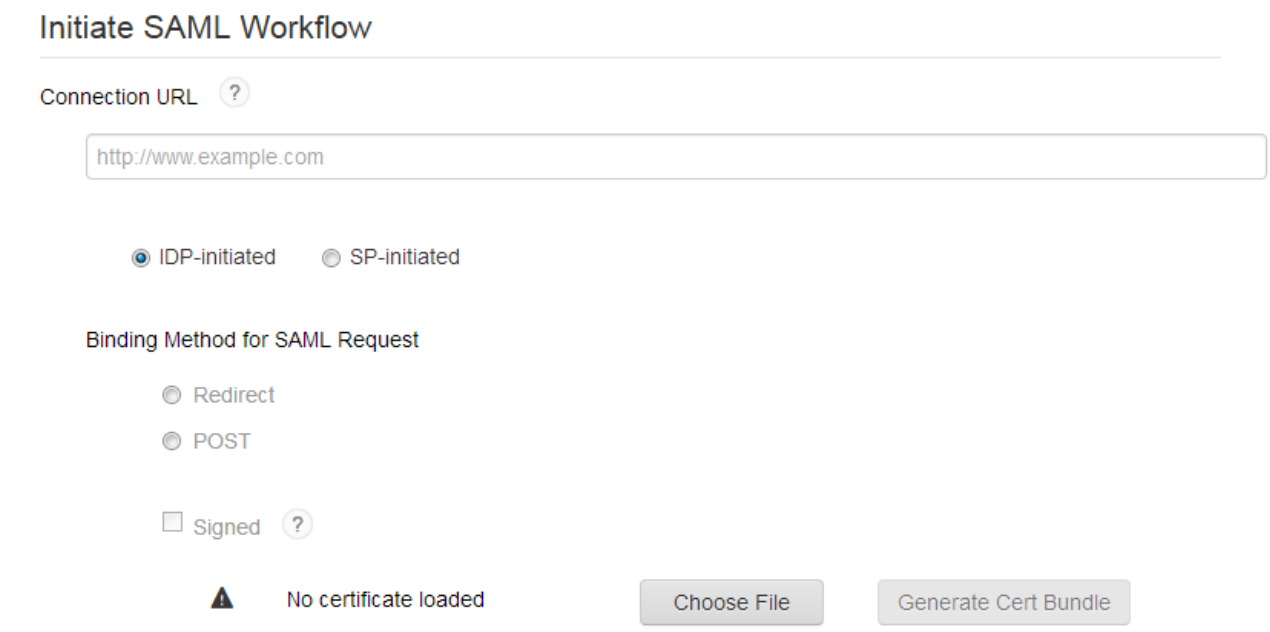
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Jitbit.

3. On the Basic Information page, specify the application name and click **Next Step**.

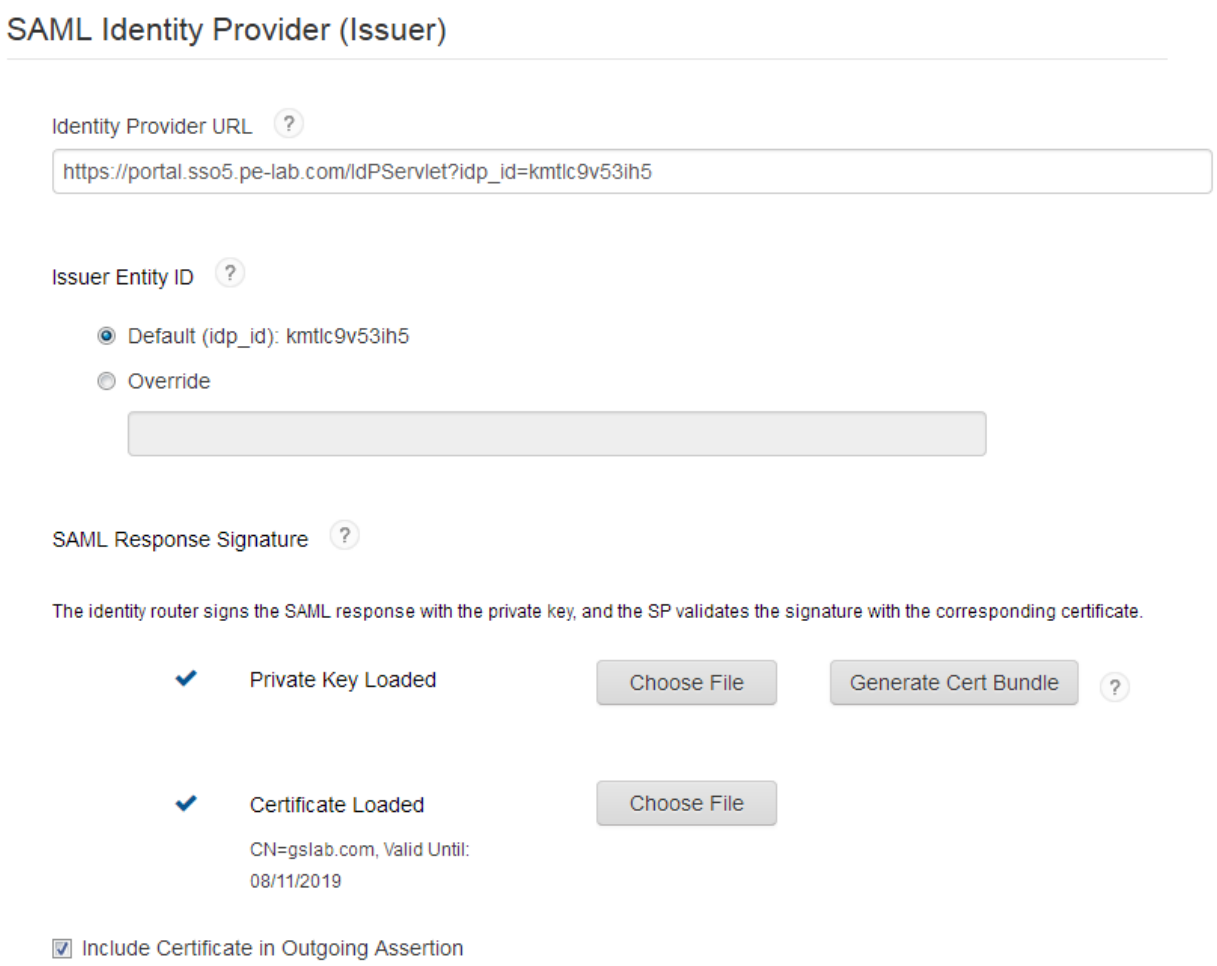


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

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

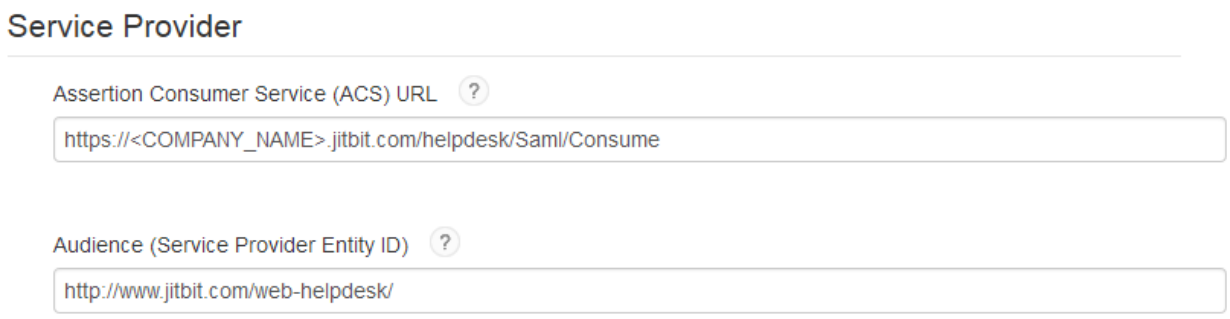


5. Scroll down to **SAML Identity Provider (Issuer)** section.



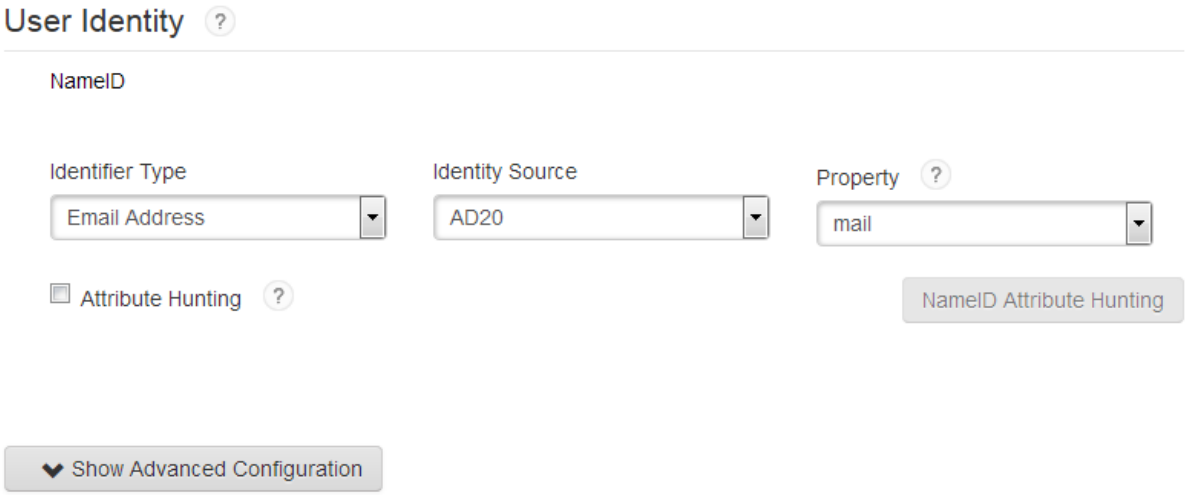
a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

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



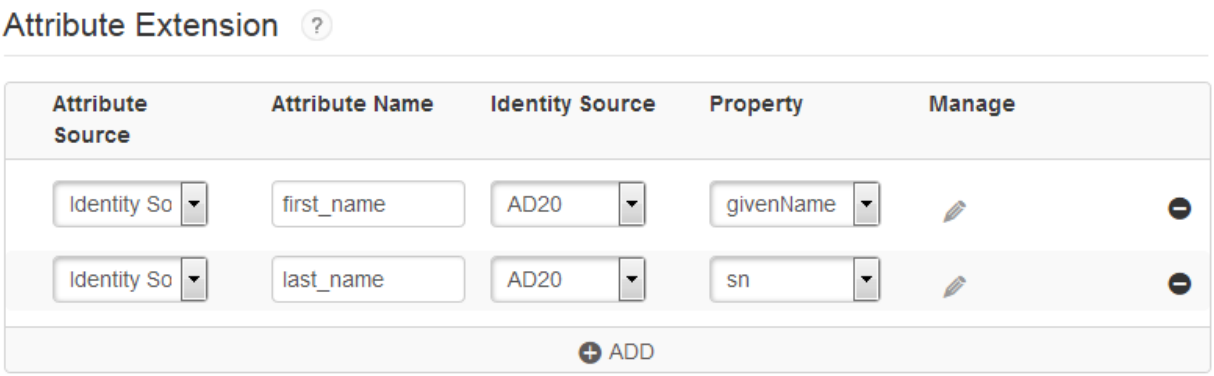
   a. In the **Assertion Consumer Service (ACS) URL** field, replace <COMPANY_NAME> value with your organization name value.
   b. In the **Audience (Service Provider Issuer ID)** field, provide value as per received from service provider.

7. 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.



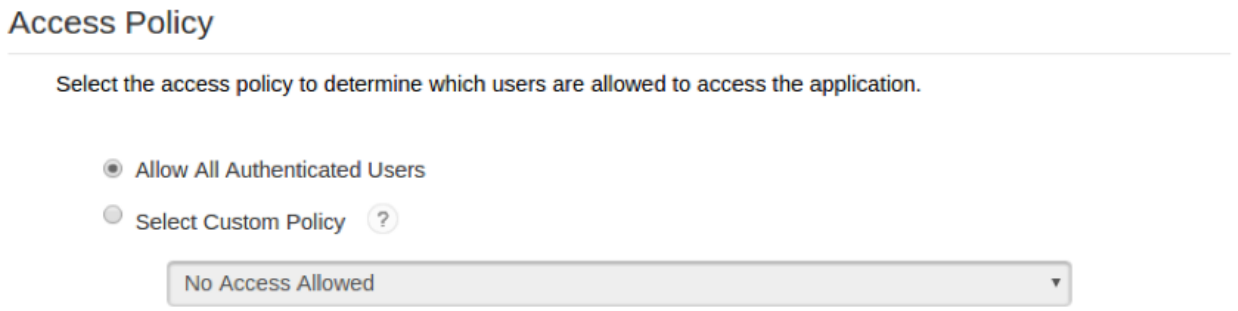
8. Click on **Show Advanced Configuration** button.

9. In the **Attribute Extension** section,

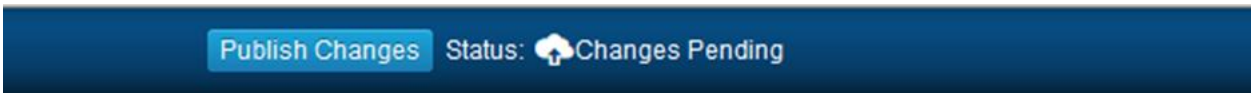


   a. Select Attribute source as **Identity Source**.
   b. In Attribute name column, add two attribute names first_name, last_name respectively.
   c. Select Identity source against which values of first_name and last_name will be validated, enter respective property names.

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



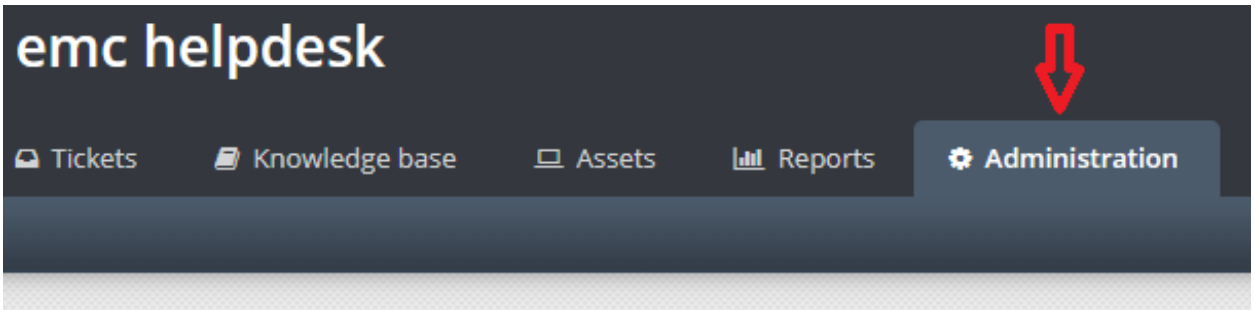
12. Click **Next Step**.
13. On the **Portal Display** page, select **Display in Portal**.
14. Click **Save and Finish**.
15. Click **Publish Changes**. Your application is now enabled for SSO.



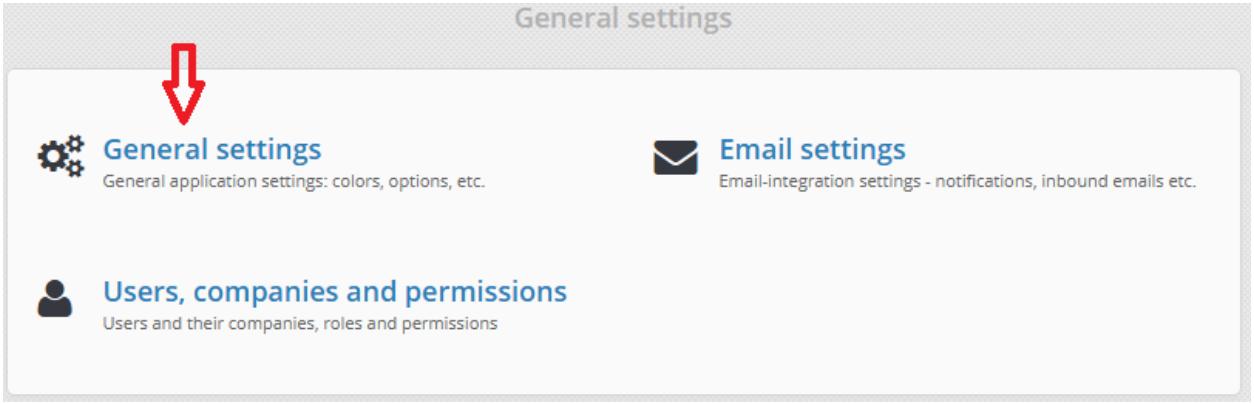
Configure Jitbit to Use RSA SecurID Access as an Identity Provider

Procedure

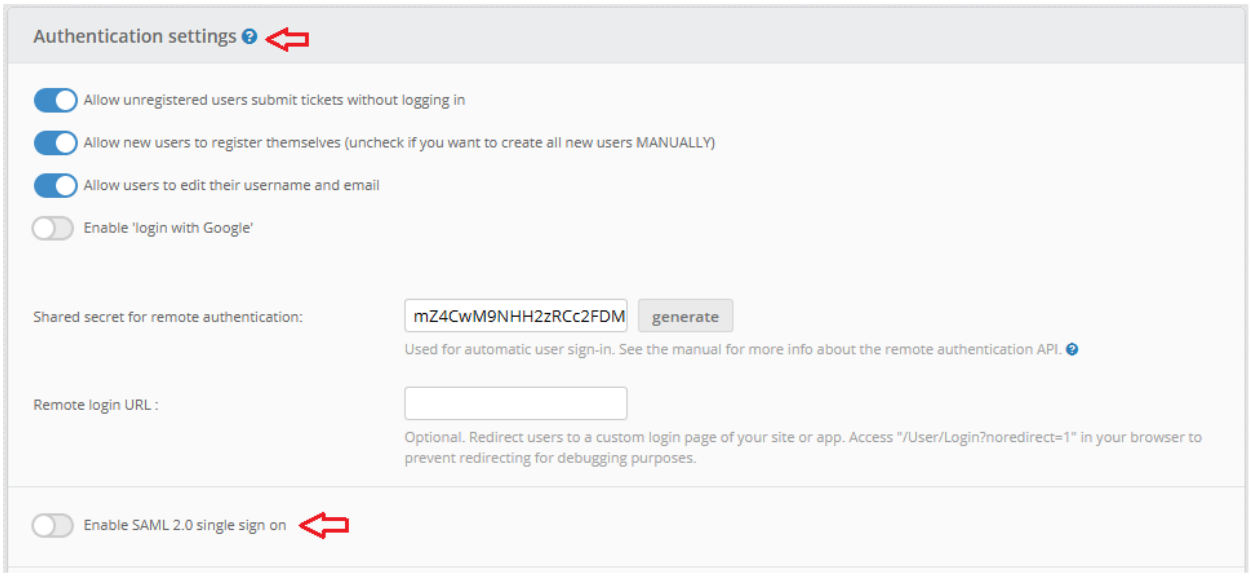
1. Login to your Jitbit application web account. (https://emc.jitbit.com/helpdesk/User/Login)
2. On the homepage, click on **Administration** tab.



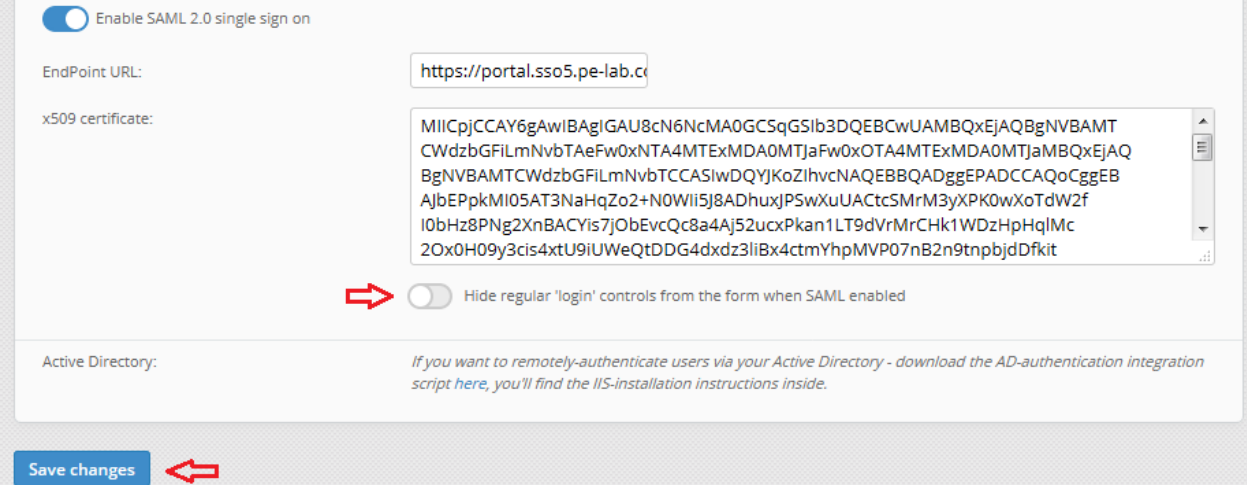
3. On the displayed page, click on **General settings**.



4. Scroll down to **Authentication settings** section. Select **Enable SAML 2.0 single sign on** to enable SAML.



5. New settings will get displayed.



   a. In the **EndPoint URL** section, enter IDP URL you got from IDR.
   b. In the x509 certificate section, enter public signing certificate contents which you have imported in IDR.
   c. Enable button below x509 certificate section, if you want users to login using only single sign on option.
   d. Click on **Save changes** button.

6. Your Jitbit account is now enabled for SAML SSO.

AB