

**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:

|                                   |   |
|-----------------------------------|---|
| <b>SP Login URL</b>               | <a href="https://emc.jitbit.com/helpdesk/User/Login">https://emc.jitbit.com/helpdesk/User/Login</a>     |
| <b>ACS URL</b>                    | <a href="https://emc.jitbit.com/helpdesk/Saml/Consume">https://emc.jitbit.com/helpdesk/Saml/Consume</a> |
| <b>Service Provider Issuer ID</b> | <a href="http://www.jitbit.com/web-helpdesk/">http://www.jitbit.com/web-helpdesk/</a>                   |

## 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.



Jitbit  
SAML Direct



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

### Basic Information

Name

Jitbit


Description (optional)

Disabled ?

Cancel

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.

### Initiate SAML Workflow

Connection URL ?

http://www.example.com

IDP-initiated  SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed ?



No certificate loaded

Choose File

Generate Cert Bundle

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

## SAML Identity Provider (Issuer)

---

Identity Provider URL ?

Issuer Entity ID ?

Default (idp\_id): kmtlc9v53ih5

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 Loaded

?

Certificate Loaded

CN=gslab.com, Valid Until:

08/11/2019

Include Certificate in Outgoing Assertion

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

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

## Service Provider

Assertion Consumer Service (ACS) URL ?

https://<COMPANY\_NAME>.jitbit.com/helpdesk/Saml/Consume

Audience (Service Provider Entity ID) ?

http://www.jitbit.com/web-helpdesk/

- 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.

## User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD20

Property ?

mail

Attribute Hunting ?



NameID Attribute Hunting

▼ Show Advanced Configuration

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

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

### Attribute Extension ?

| Attribute Source           | Attribute Name | Identity Source     | Property                 | Manage   |
|----------------------------|----------------|---------------------|--------------------------|--|
| Identity So <span>▼</span> | first_name     | AD20 <span>▼</span> | givenName <span>▼</span> |  <span>⊖</span> |
| Identity So <span>▼</span> | last_name      | AD20 <span>▼</span> | sn <span>▼</span>        |  <span>⊖</span> |
| <span>+</span> ADD         |                |                     |                          |  |

- Select Attribute source as **Identity Source**.
- In Attribute name column, add two attribute names first\_name, last\_name respectively.
- 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.

### 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 ▼

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.

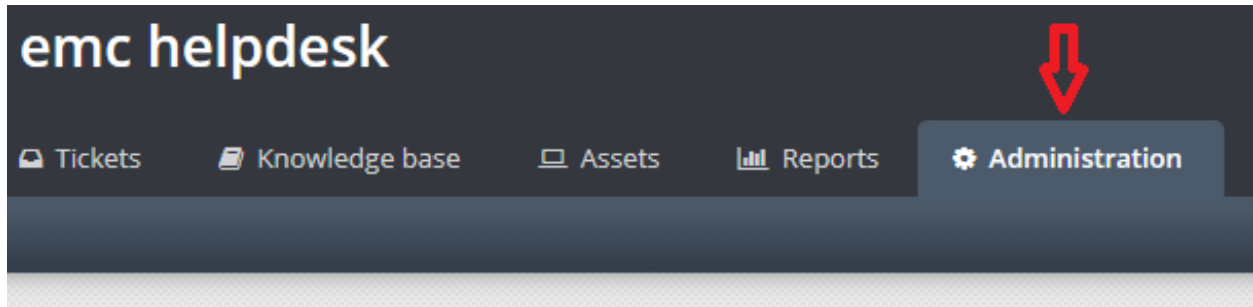
**Publish Changes**

Status:  Changes Pending

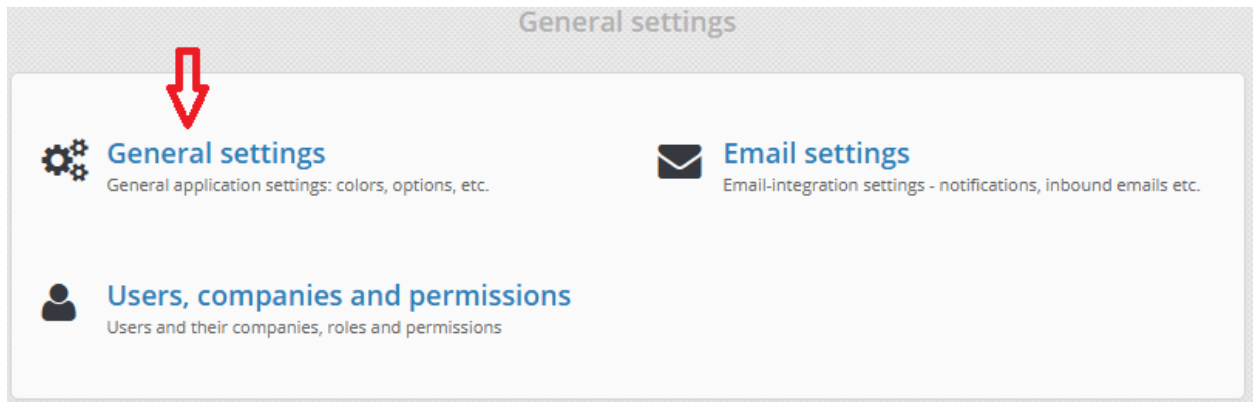
# Configure Jitbit to Use RSA SecurID Access as an Identity Provider

## Procedure

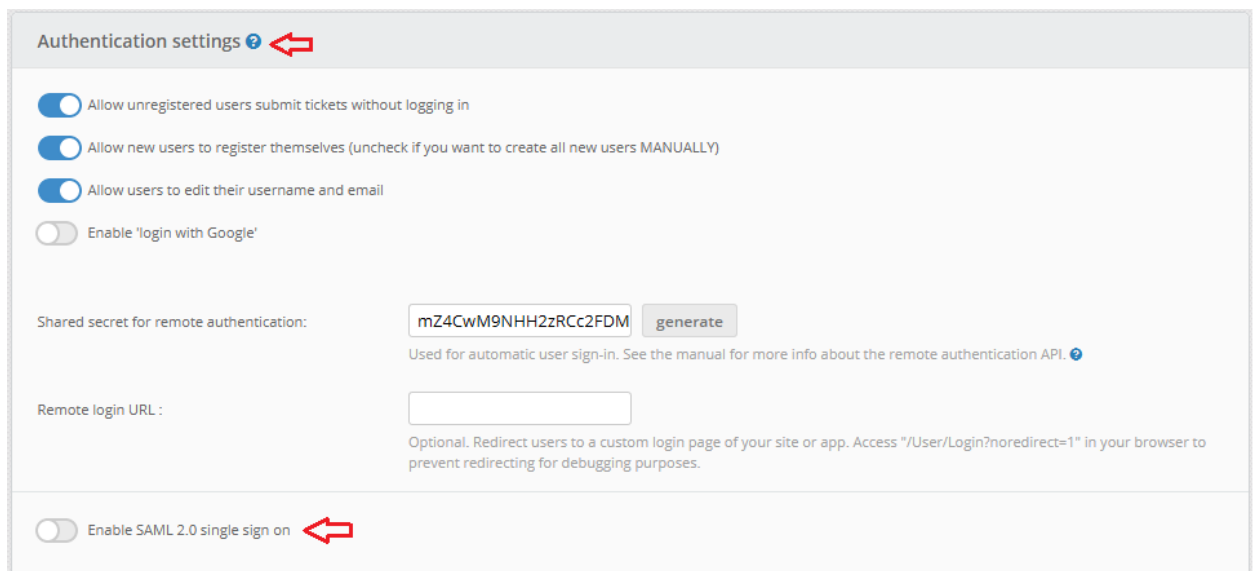
1. Login to your Jitbit application web account. (<https://emc.jitbit.com/helpdesk/User/Login>)
2. On the homepage, click on **Administration** tab.



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.

Enable SAML 2.0 single sign on

EndPoint URL:

x509 certificate:

Hide regular 'login' controls from the form when SAML enabled

Active Directory: *If you want to remotely-authenticate users via your Active Directory - download the AD-authentication integration script [here](#), you'll find the IIS-installation instructions inside.*

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

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