RSA SecurID Access SAML Configuration for 15Five

Last Modified: April 21, 2017

15Five is an inter-company employee feedback system used to elevate the performance and engagement of employees by consistently tracking work related things. 15Five has auto-provisioning of user feature available.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and 15Five.
- Obtain SP metadata details from the Service Provider.
- Obtain IdP metadata from RSA SecurID Access console.

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

SP Login URL	*https://dell.15five.com/account/login*
ACS URL	*https://dell.15five.com/saml2/acs/*
Service Provider Issuer ID	*https://dell.15five.com/saml2/metadata/*

Procedure

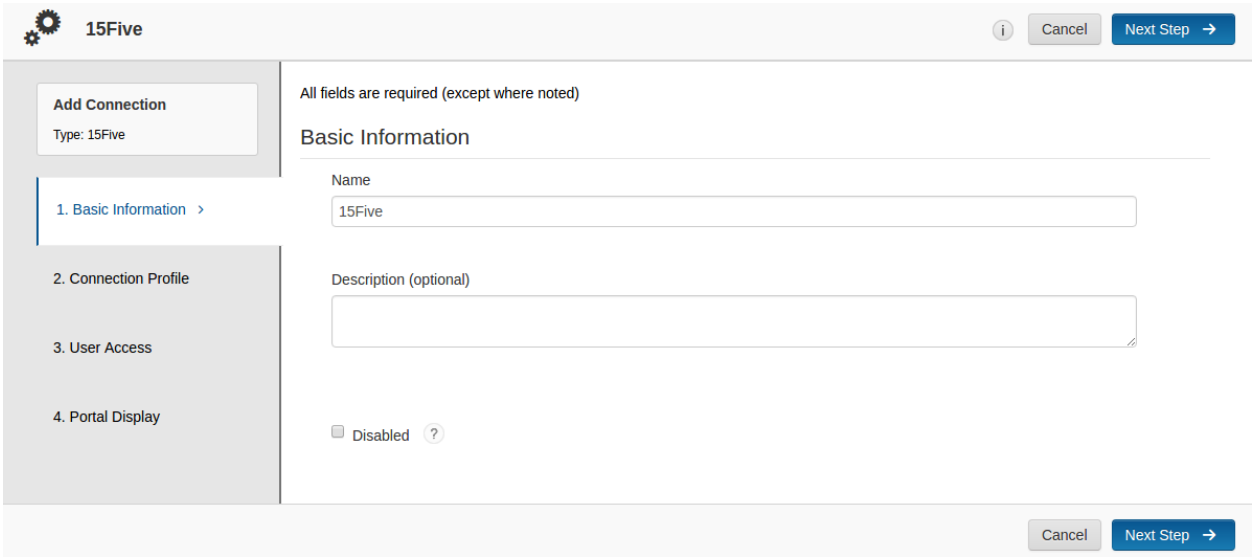
1. Add the Application in RSA SecurID Access
2. Configure 15Five to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

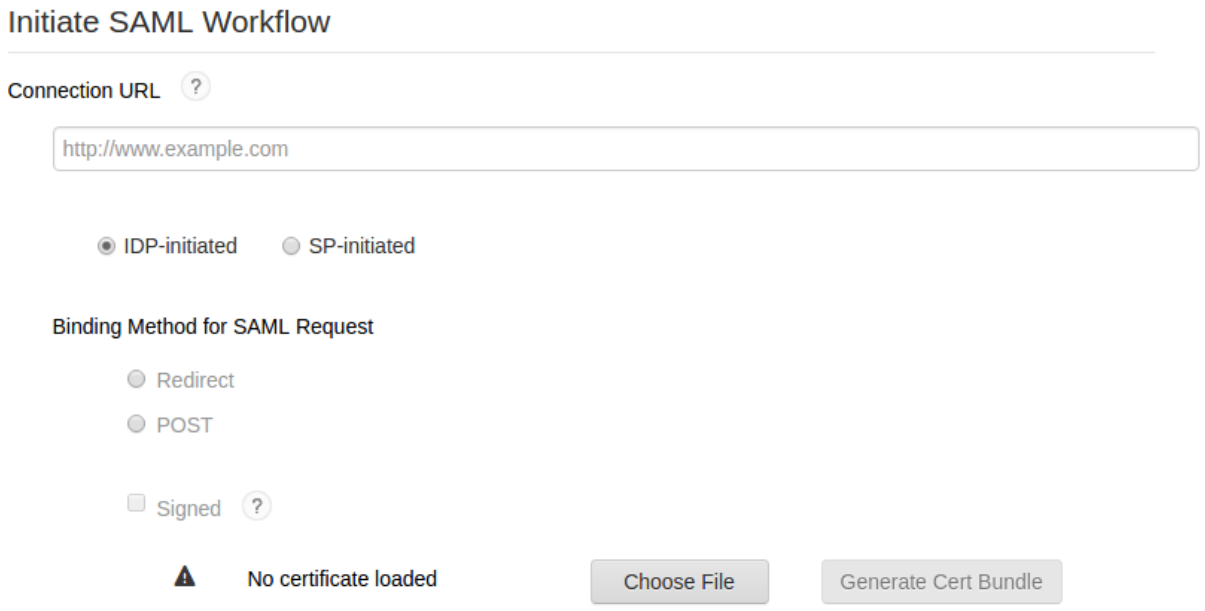
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** 15Five.

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

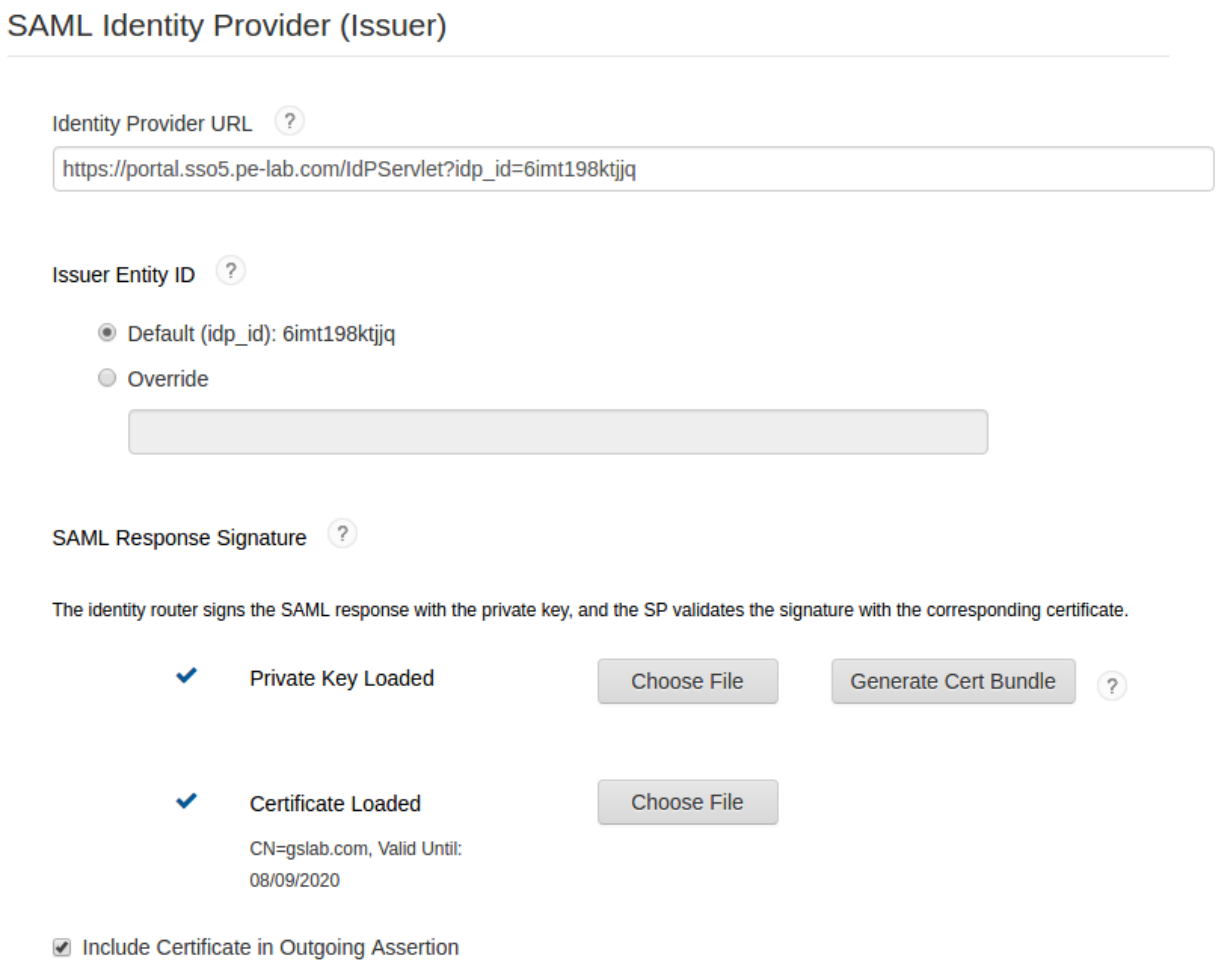


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

Note: The following IdP-initiated configuration works for SP-initiated 15Five connections as well.

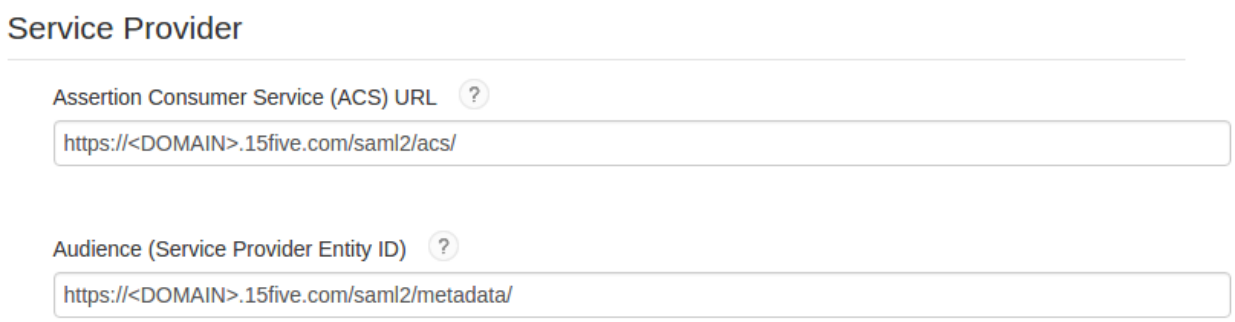


5. Scroll down to **SAML Identity Provider (Issuer)** section.



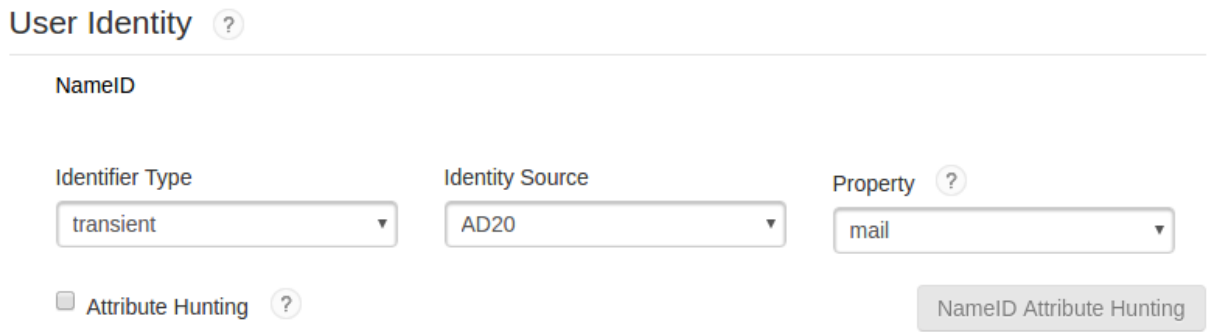
a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** 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.

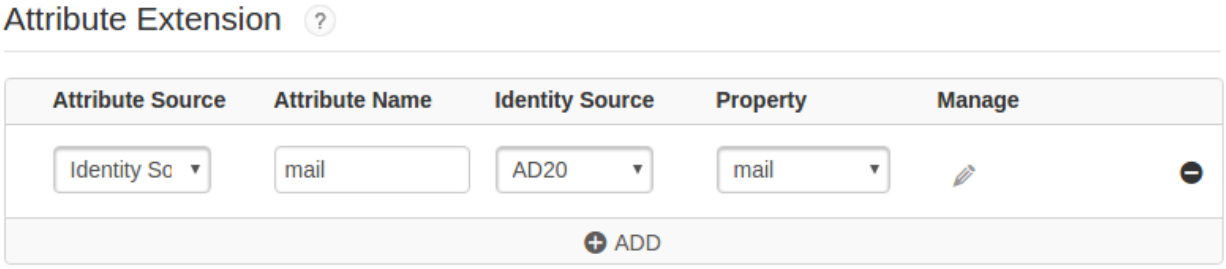


   a. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> value with your organization account value.
   b. In the **Audience (Service Provider Issuer ID)** field, replace <DOMAIN> value with your organization account value.

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.

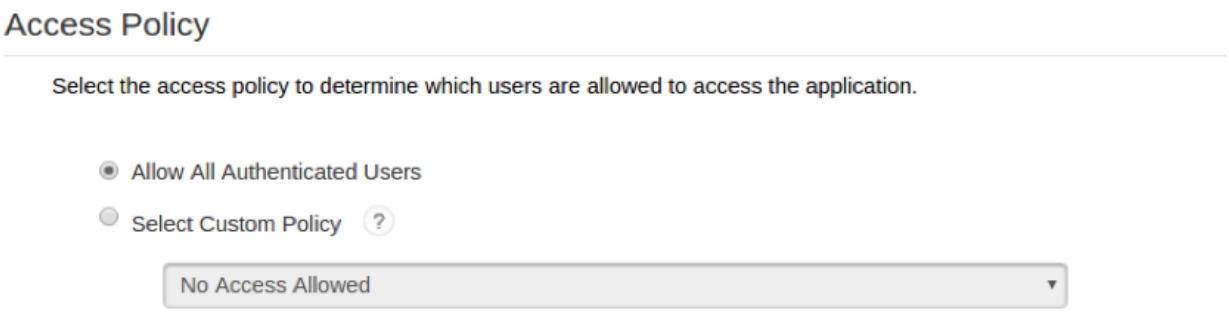


8. Select **Show Advanced Configuration**. In the **Attribute Extension** section, add **mail**. This is mandatory provisioning attribute needs to be forwarded at the time of SSO.

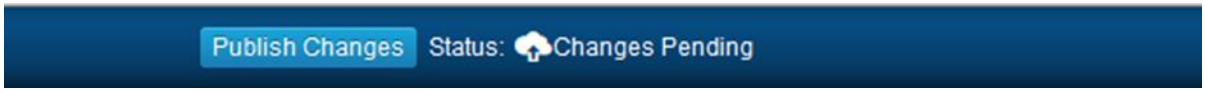


9. Click **Next Step**.

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



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

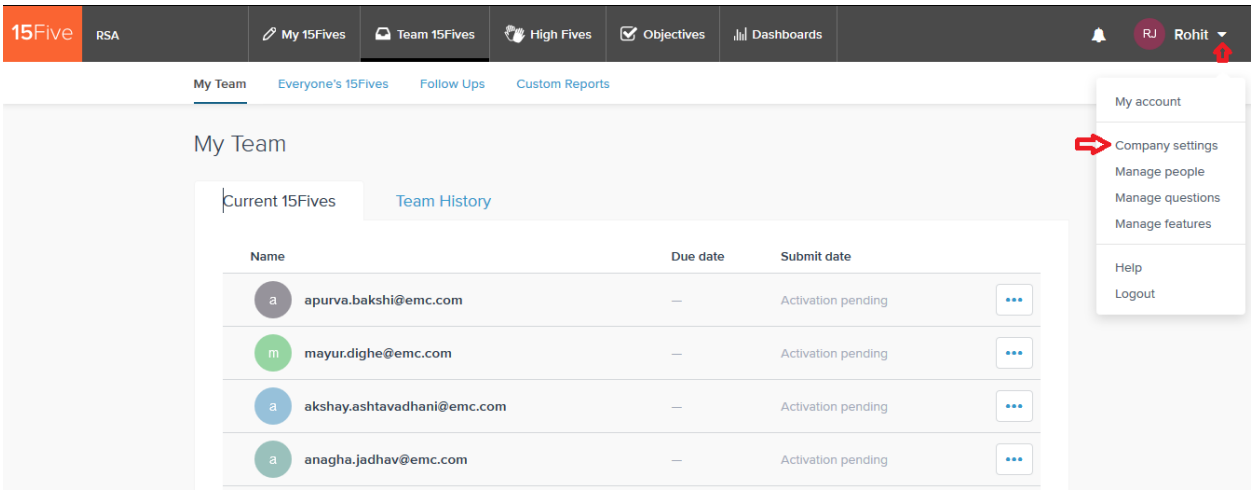


15. Navigate to **Applications > My Applications**.
16. Locate 15Five in the list and from the **Edit** option, select **Export Metadata**.

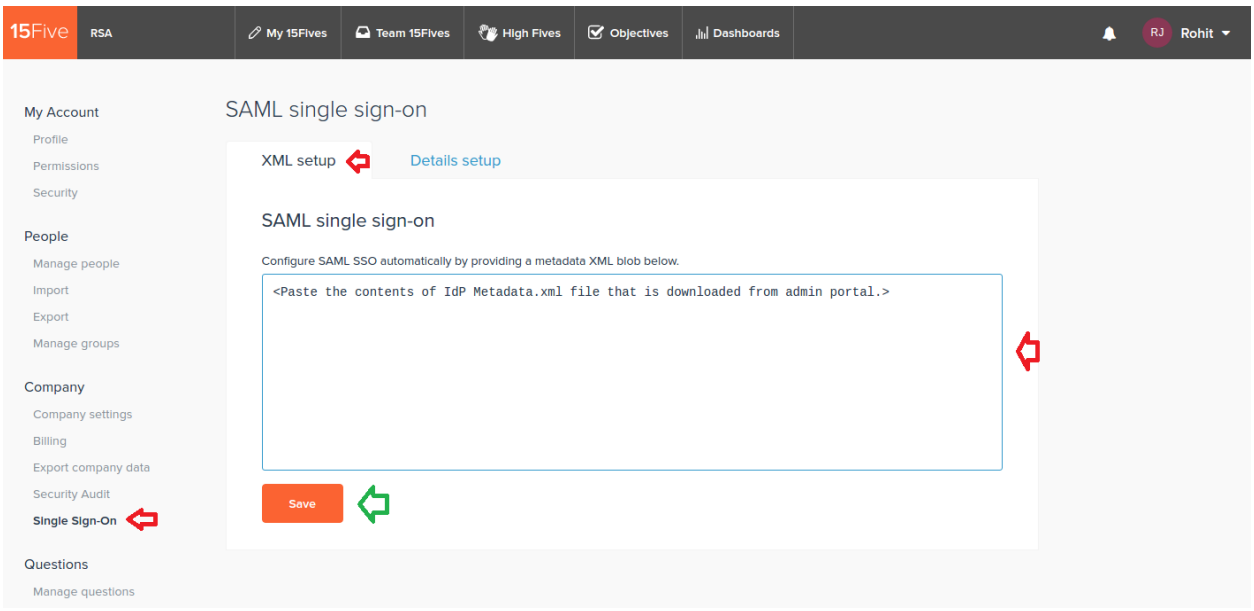
Configure 15Five to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login to your 15Five application web account. (https://dell.15five.com/account/login)
2. Following UI will be displayed. Click on **Arrow** symbol followed by *Company settings* option.



3. Following UI will be displayed. Go to *Company → Single Sign-On.*



   a. Under **XML setup** option, provide xml contents of 15Five IdP Metadata file that is downloaded in step – 16) on page 5.
   b. Once sure of settings, click on **Save** button to complete configuration changes.

4. Your 15Five account is now enabled for the SAML authentication.

RJ