

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.




15Five
SAML Direct




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

The screenshot shows a configuration page for a connection named '15Five'. The page has a sidebar on the left with a navigation menu containing four items: '1. Basic Information >', '2. Connection Profile', '3. User Access', and '4. Portal Display'. The main content area is titled 'Basic Information' and includes a header 'All fields are required (except where noted)'. Below this, there are three input fields: 'Name' (containing '15Five'), 'Description (optional)' (empty), and a 'Disabled' checkbox (unchecked). At the bottom right, there are 'Cancel' and 'Next Step →' buttons.

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.

Initiate SAML Workflow

Connection URL 


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): 6imt198ktjjq

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:
08/09/2020

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://<DOMAIN>.15five.com/saml2/acs/

Audience (Service Provider Entity ID) 

https://<DOMAIN>.15five.com/saml2/metadata/

- 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.

User Identity


NameID

Identifier Type

transient

Identity Source

AD20

Property 




mail

Attribute Hunting 

NameID Attribute Hunting

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.

Attribute Extension

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc ▾	mail	AD20 ▾	mail ▾	 
 ADD				

9. Click **Next Step**.

10. 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

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.

Publish Changes Status:  Changes Pending

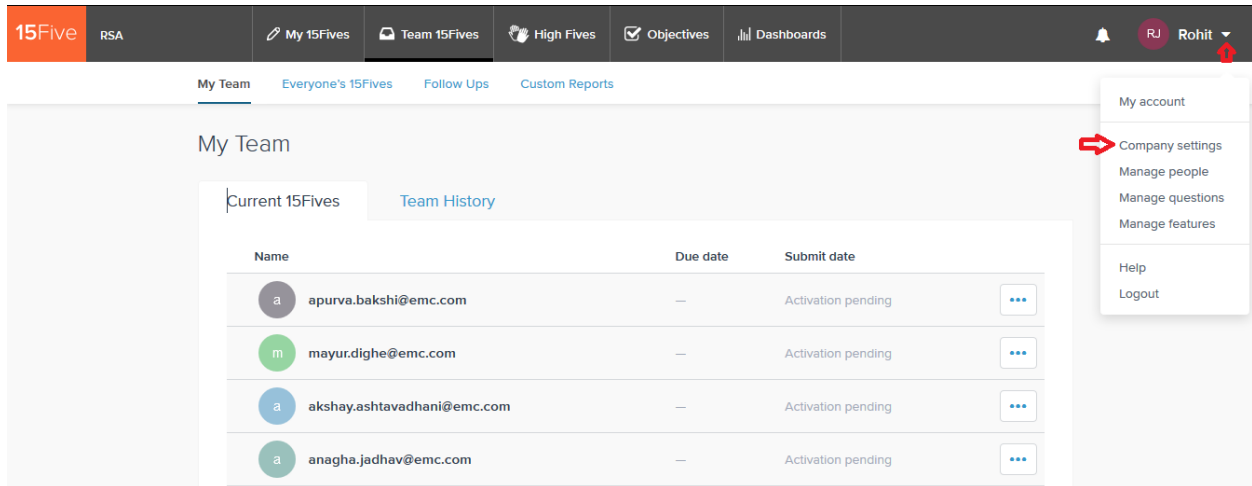
15. Navigate to **Applications > My Applications**.
16. Locate 15Five in the list and from the **Edit** option, select **Export Metadata**.

	15Five Created From: 15Five SAML Direct	Edit 
		 Edit
		 Export Metadata
		 Delete

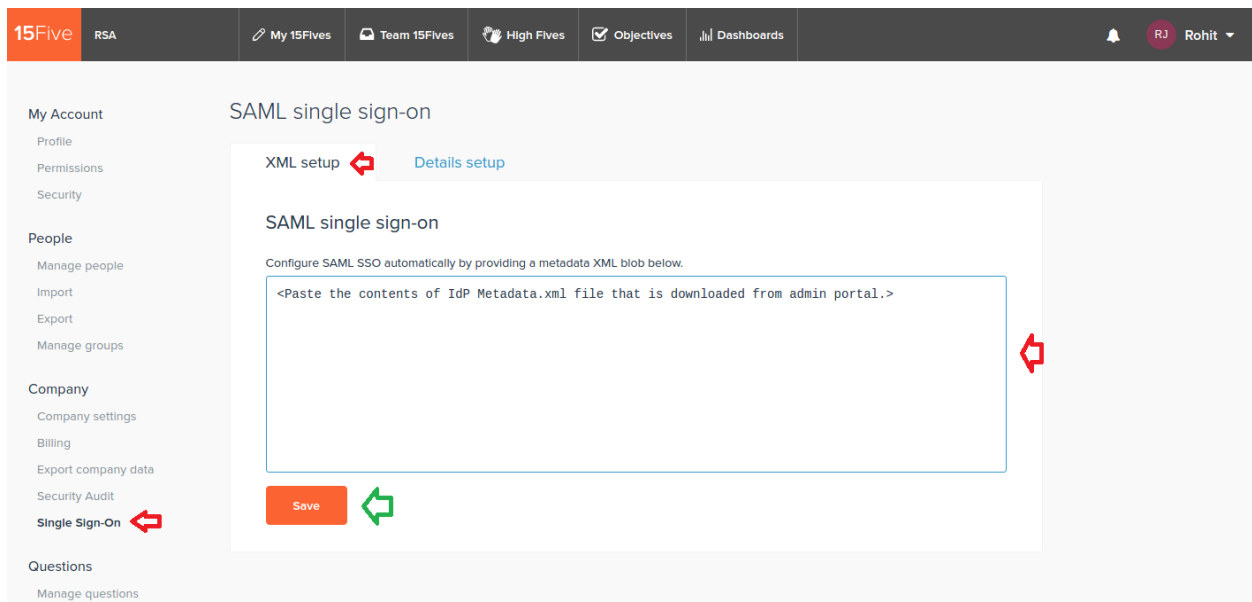
Configure 15Five to Use RSA SecurID Access as an Identity Provider

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.