RSA SecurID Access SAML Configuration for Informatica Cloud

Last Modified: December 13, 2016

Informatica is a software development company founded in 1993. Informatica products are a portfolio focused on data integration: ETL, information lifecycle management, B2B data exchange, cloud data integration, complex event processing, data masking, data quality, data replication, data virtualization, master data management, ultra messaging. These components form a toolset for establishing and maintaining enterprise-wide data warehouses. In 2006, Informatica launched its Informatica Cloud business.

Before You Begin

- Acquire an administrator account for both RSA SecurID Access and Informatica Cloud.
- Obtain SP metadata details from service provider.
- Obtain IdP metadata from IDR portal.

Note: SAML is not by default enabled. Contact Informatica Cloud support@informatica.com OR open support ticket from account to enable SAML.

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

SP Login URL	*https://app.informaticaondemand.com/ma/sso/z6q25o4q*
ACS URL	*https://app.informaticaondemand.com/ma/acs/z6q25o4q*
Service Provider Issuer ID	*https://z6q25o4q.app.informaticaondemand.com/*

Procedure

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

Add the Application in RSA SecurID Access

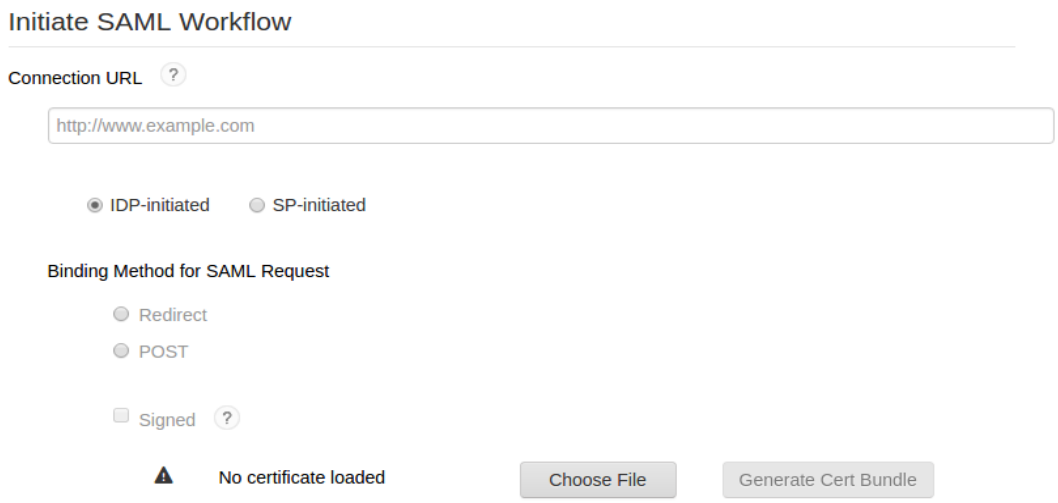
Procedure

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

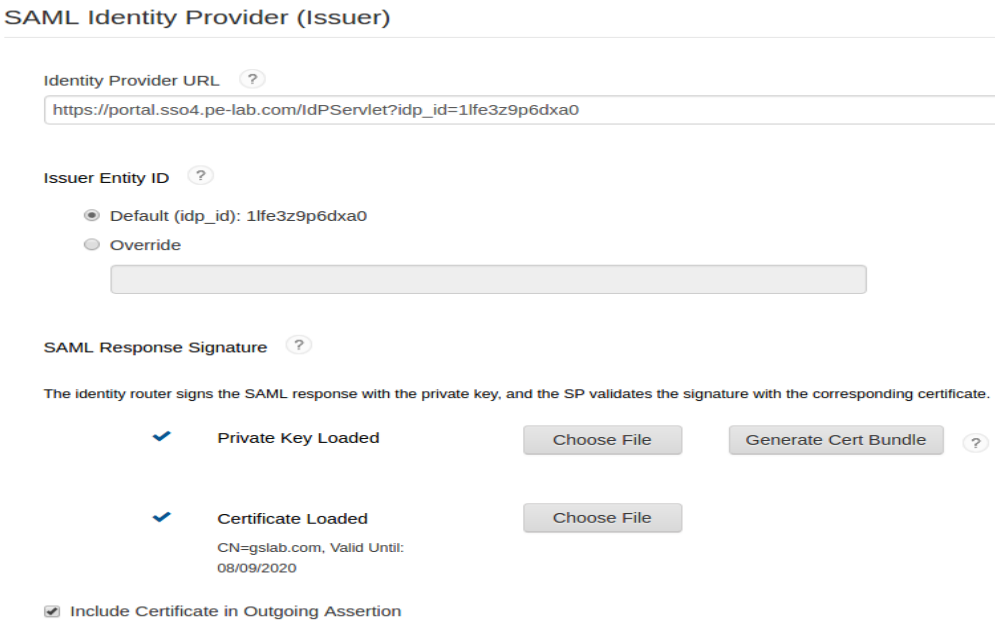
3. On the Basic Information page, specify the application name and click **Next Step**.

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 Informatica Cloud connections as well.

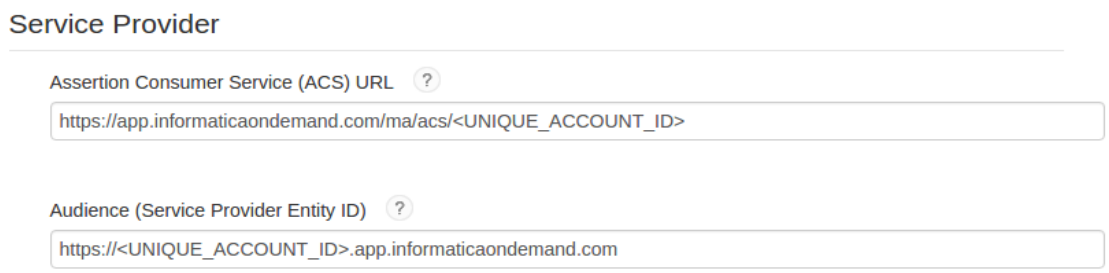


5. Scroll down to **SAML Identity Provider (Issuer)** section.



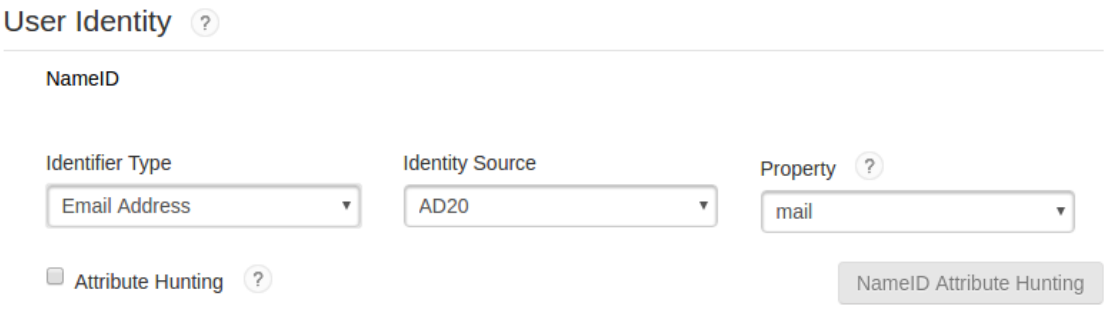
a. Take note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File**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



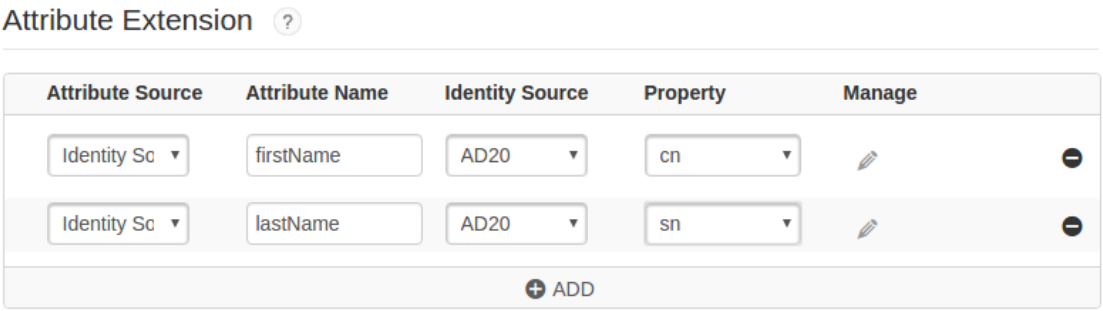
a. In the **Assertion Consumer Service (ACS) URL** field, replace <UNIQUE_ACCOUNT_ID> with the ID assigned to your account.
b. In the **Audience (Service Provider Entity ID)** field, replace <UNIQUE_ACCOUNT_ID> with the ID assigned to your account.

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.

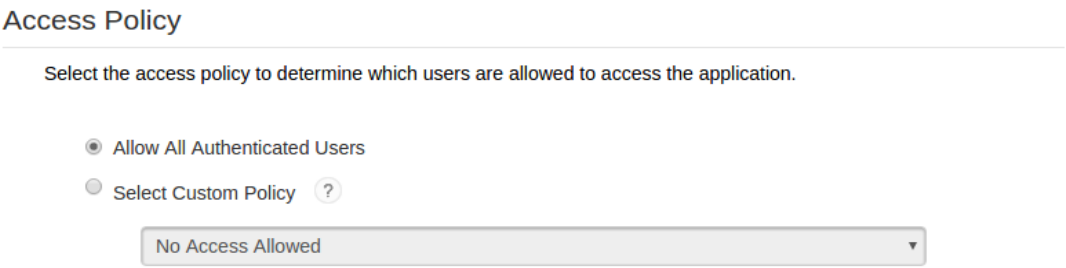


8. Select **Show Advanced Configuration.**

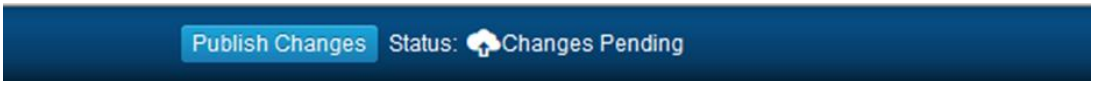
9. In the **Attribute Extension** section, add **firstName**, **lastname**. These are mandatory provisioning attributes needs to be forwarded at the time of SSO.



10. Click **Next Step**.
11. On the **User Access page,** select **Allow All Authenticated Users** option from drop down list.



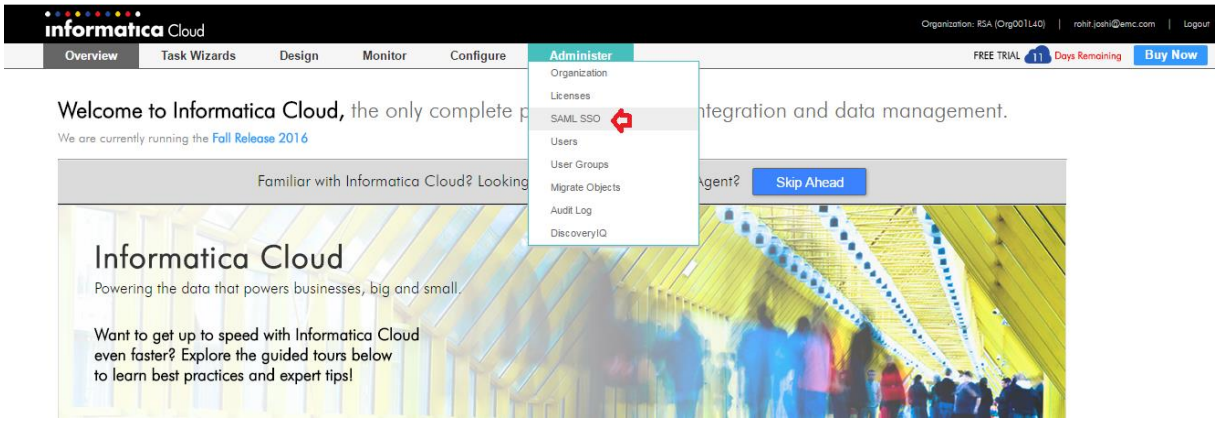
12. Click **Next Step**.
13. On the **Portal Display** page, select **Display in Portal**.
14. Click **Save and Finish**.
15. Click **Publish Changes**. Your application is now enabled for SSO.



16. Navigate to **Applications > My Applications**.
17. Locate Informatica Cloud in the list and from the **Edit** pulldown select **Export Metadata**.

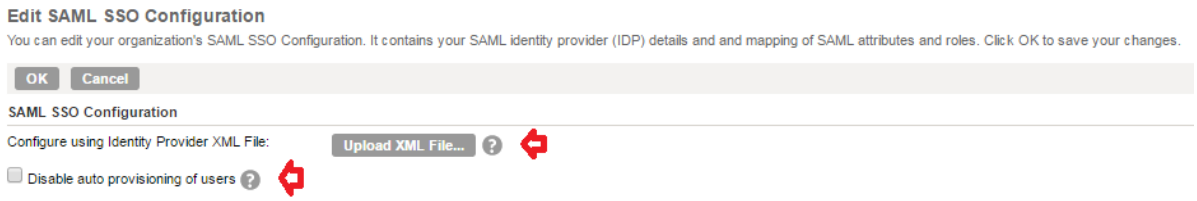
Configure Informatica Cloud to Use RSA SecurID Access as an Identity Provider

1. Login to your Informatica Cloud account. (https://app.informaticaondemand.com/ma/login)
2. Following page will be displayed. Select **SAML SSO** option available under **Administer** tab.

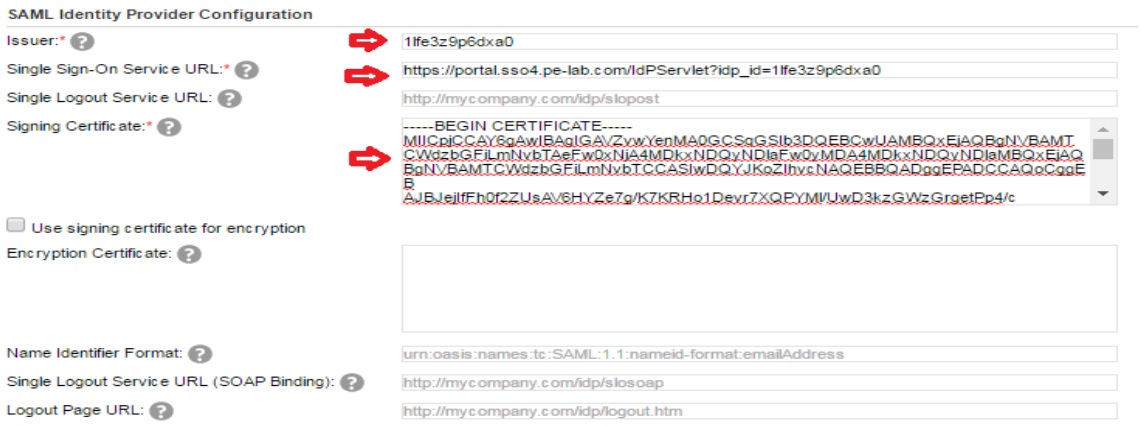


3. Following page will be displayed to **Edit SAML SSO Configuration.** You can simply import IdP metadata you have downloaded in step-17 directly by clicking on **Upload XML File** button. If chosen to configure manually, then only follow below steps.

   Keep the **Disable auto provisioning of users** option **unchecked**.



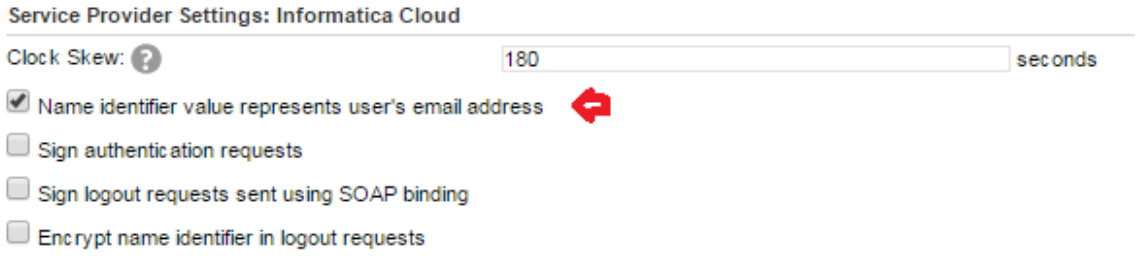
4. Next on the same page is **SAML Identity Provider Configuration**.



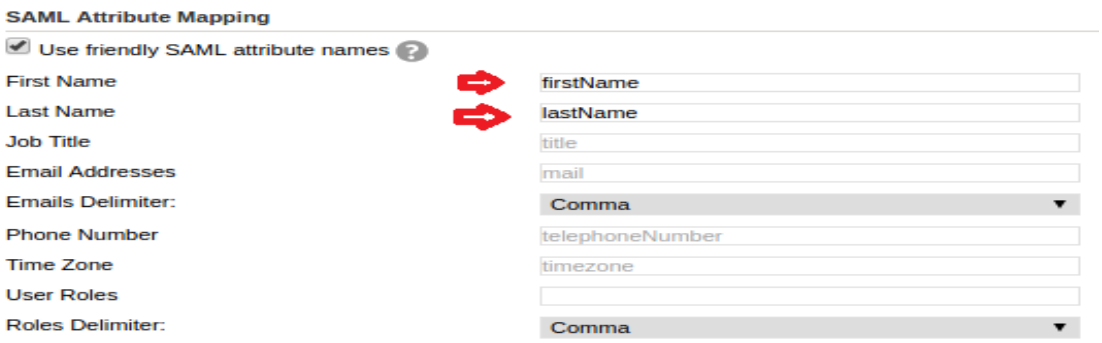
Provide here below details:

a. **Issuer:** Provide IdP issuer value in the textfield.
b. **Single Sign-On Service URL:** Enter the Identity Provider URL found on page 2 step-5 with the following format – https://<Your_Portal_URL>?idp_id=<Unique_IdP_ID>
c. Keep the **Single Logout Service URL** field blank.
d. **Signing Certificate:** Paste the RSA SecurID Access IdP public certificate here.
e. Keep the rest of the fields to their defaults.

5. Moving next is **Service Provider Settings** as shown below. Click on checkbox which tells – **Name identifier value represents user's email address**. Keep rest of the fields to their defaults.



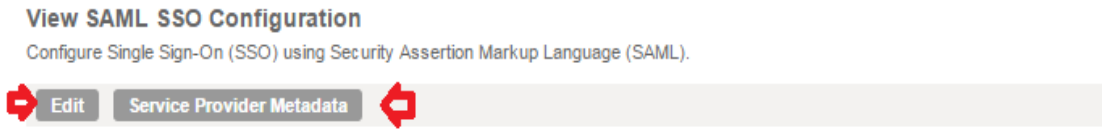
6. On the same page, next will appear is **SAML Attribute Mapping**. Provide values here of your choice for **First Name**, **Last Name**.



Note: User Roles can't be provided with assertions while doing SSO as Informatica admin can only set those.

7. Once sure of all the settings, click on **OK** button to save all configurations.

8. Once completed, there will be option available for you to download **Service Provider Metadata** and **Edit** SAML SSO configurations as shown below –



9. Your Informatica Cloud account is now enabled for SAML SSO authentication.