

# Configure Informatica for Single Sign-On

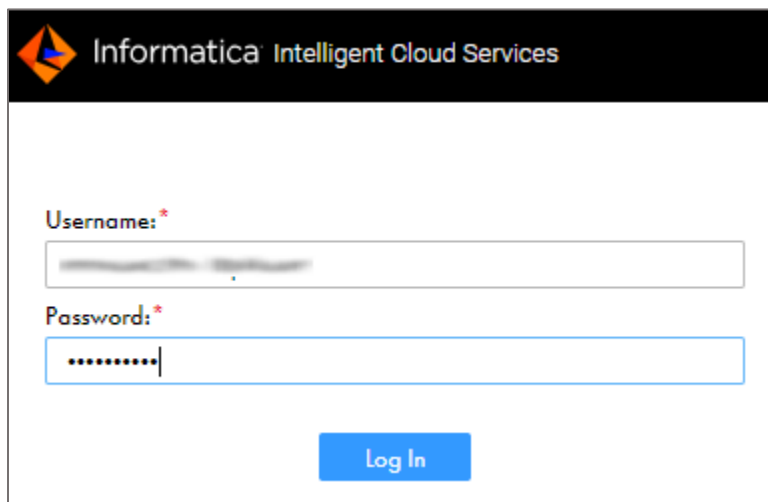
Configuring Informatica for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Informatica by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

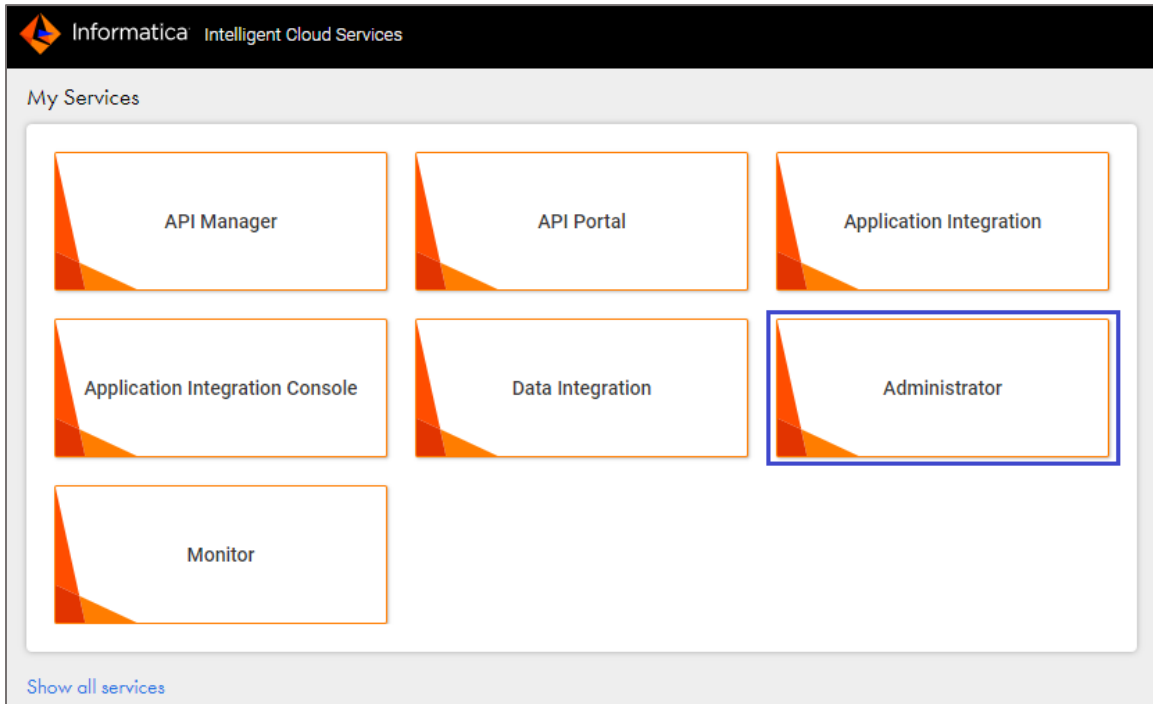
## To configure Informatica for SSO by using SAML:

1. In a browser, type <https://dm-ap.informaticacloud.com/identity-service/home> and press **Enter**.
2. Type your Informatica admin account credentials (**Username** and **Password**) and click **Log In**.

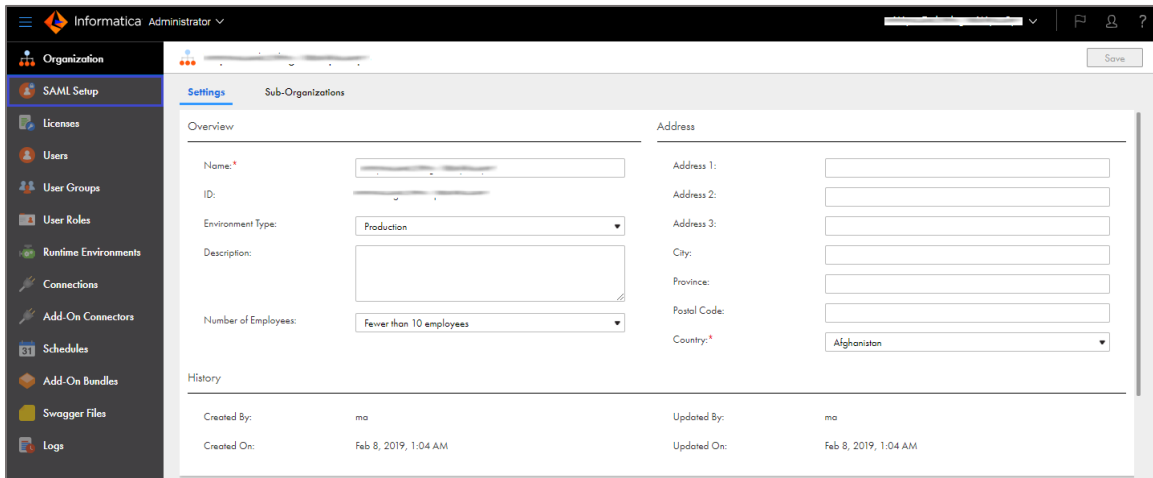


The screenshot shows the Informatica Intelligent Cloud Services login interface. At the top, there is a black header with the Informatica logo (a stylized orange and blue diamond) and the text "Informatica Intelligent Cloud Services". Below the header, the page is white. There are two input fields: "Username:" followed by a text box containing a blurred username, and "Password:" followed by a text box containing a blurred password. Below these fields is a blue button labeled "Log In".

3. In the dashboard page, click the **Administrator** tile.



4. Click **SAML Setup** in the left pane.



- In the **SAML Setup** page, enter the values for the following fields under **Identity Provider Configuration**:

Required Information	Description
Issuer*	Issuer URL
Single Sign-On Service URL*	IdP logon URL
Signing Certificate*	<p>Copy and paste the IdP certificate. The IdP certificate must begin and end with            -----Begin Certificate----- and -----End Certificate-----</p> <p><b>Note:</b> The IdP metadata is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app.  <a href="https://gateway.cloud.com/idp/saml/&lt;citrixcloudcust id&gt;/&lt;app id&gt;/idp_metadata.xml">https://gateway.cloud.com/idp/saml/&lt;citrixcloudcust id&gt;/&lt;app id&gt;/idp_metadata.xml</a></p>

**SAML Setup** [Download Service Provider Metadata] [Save]

Configure Single Sign-On (SSO) using Security Assertion Markup Language

**SSO Configuration**

Use Identity Provider File:

Disable auto provision of users

**Identity Provider Configuration**

Issuer\*:

Single Sign-On Service URL\*:

Single Logout Service URL:

Signing Certificate\*:

Use signing certificate for encryptions

Encryption Certificate:

Name Identifier Format:

Logout Service URL(SOAP BINDING):

Logout Page URL:

**SAML Attribute Mapping**

User friendly SAML attribute names

First Name:

Last Name:

Job Title:

Email Addresses:

Emails Delimiter:

Phone Number:

Time Zone:

User Roles:

Roles Delimiter:

**SAML Role Mapping**

Admin:

Business Manager:

Data Integration Task Executor:

Data Viewer:

- In the **SAML Setup** page, enter the values for the following fields under **SAML Attribute Mapping**:

Required Information	Description
First Name	firstName
Last Name	lastName
Email Addresses	email

The screenshot shows the SAML Setup configuration page with the following sections:

- SSO Configuration:** Includes fields for "Use Identity Provider File" (with a "Drop file here" box and "Choose File..." button), "Disable auto provision of users" (checkbox), "Single Sign-On Service URL", "Single Logout Service URL", "Signing Certificate" (with a certificate viewer), "Use signing certificate for encryptions" (checkbox), "Encryption Certificate", "Name Identifier Format" (set to "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"), "Logout Service URL(SOAP BINDING)", and "Logout Page URL".
- SAML Attribute Mapping:** Includes a "User friendly SAML attribute names" checkbox and input fields for "First Name" (firstName), "Last Name" (lastName), "Job Title" (title), "Email Addresses" (email), "Emails Delimiter" (COMMA), "Phone Number" (telephoneNumber), "Time Zone" (timezone), "User Roles", and "Roles Delimiter" (COMMA).
- SAML Role Mapping:** Includes input fields for "Admin" (role1, role2), "Business Manager" (role3, role4), "Data Integration Task Executor" (role5, role6), and "Data Viewer" (role7, role8).

- Finally, click **Save**.