Informatica®

Informatica® Intelligent Cloud Services
May 2023

User Administration

Informatica Intelligent Cloud Services User Administration
May 2023

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2023-05-08

Table of Contents

Preface

Use *User Administration* to learn how to configure Informatica Intelligent Cloud Services℠ user accounts manually or using SAML single-sign on. Learn how to create user groups, assign roles to users, and edit your user profile.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Intelligent Cloud Services web site

You can access the Informatica Intelligent Cloud Services web site at http://www.informatica.com/cloud. This site contains information about Informatica Cloud integration services.

Informatica Intelligent Cloud Services Communities

Use the Informatica Intelligent Cloud Services Community to discuss and resolve technical issues. You can also find technical tips, documentation updates, and answers to frequently asked questions.

Access the Informatica Intelligent Cloud Services Community at:

https://network.informatica.com/community/informatica-network/products/cloud-integration

Developers can learn more and share tips at the Cloud Developer community:

https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers

Informatica Intelligent Cloud Services Marketplace

Visit the Informatica Marketplace to try and buy Data Integration Connectors, templates, and mapplets:

https://marketplace.informatica.com/

Data Integration connector documentation

You can access documentation for Data Integration Connectors at the Documentation Portal. To explore the Documentation Portal, visit https://docs.informatica.com.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Intelligent Cloud Services Trust Center

The Informatica Intelligent Cloud Services Trust Center provides information about Informatica security policies and real-time system availability.

You can access the trust center at https://www.informatica.com/trust-center.html.

Subscribe to the Informatica Intelligent Cloud Services Trust Center to receive upgrade, maintenance, and incident notifications. The Informatica Intelligent Cloud Services Status page displays the production status of all the Informatica cloud products. All maintenance updates are posted to this page, and during an outage, it will have the most current information. To ensure you are notified of updates and outages, you can subscribe to receive updates for a single component or all Informatica Intelligent Cloud Services components. Subscribing to all components is the best way to be certain you never miss an update.

To subscribe, go to https://status.informatica.com/ and click **SUBSCRIBE TO UPDATES**. You can then choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

Informatica Global Customer Support

You can contact a Customer Support Center by telephone or online.

For online support, click **Submit Support Request** in Informatica Intelligent Cloud Services. You can also use Online Support to log a case. Online Support requires a login. You can request a login at https://network.informatica.com/welcome.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at https://www.informatica.com/services-and-training/support-services/contact-us.html.

CHAPTER 1

User administration

Configure users and user groups to allow access to your organization and assets. A user is an individual account in Informatica Intelligent Cloud Services that allows secure access to an organization.

To configure users, you can set up single sign-on through Microsoft Azure or through a SAML third party identity provider. You can also create users directly in Administrator. For more information about SAML configuration with Microsoft Azure, see Chapter 2, “Ecosystem single sign-on” on page 8. For more information about SAML configuration with a third-party identity provider, see Chapter 3, “SAML single sign-on” on page 10. For more information about configuring user accounts directly, see Chapter 4, “Users” on page 22.

A user group is a group of user accounts in which all members of the group can perform the same tasks and have the same access rights for different types of assets. For more information about user groups, see Chapter 5, “User groups” on page 32.

Users and groups can perform tasks and access assets based on the roles that you assign to them. For more information about user roles, see Chapter 6, “User roles” on page 35.

CHAPTER 2

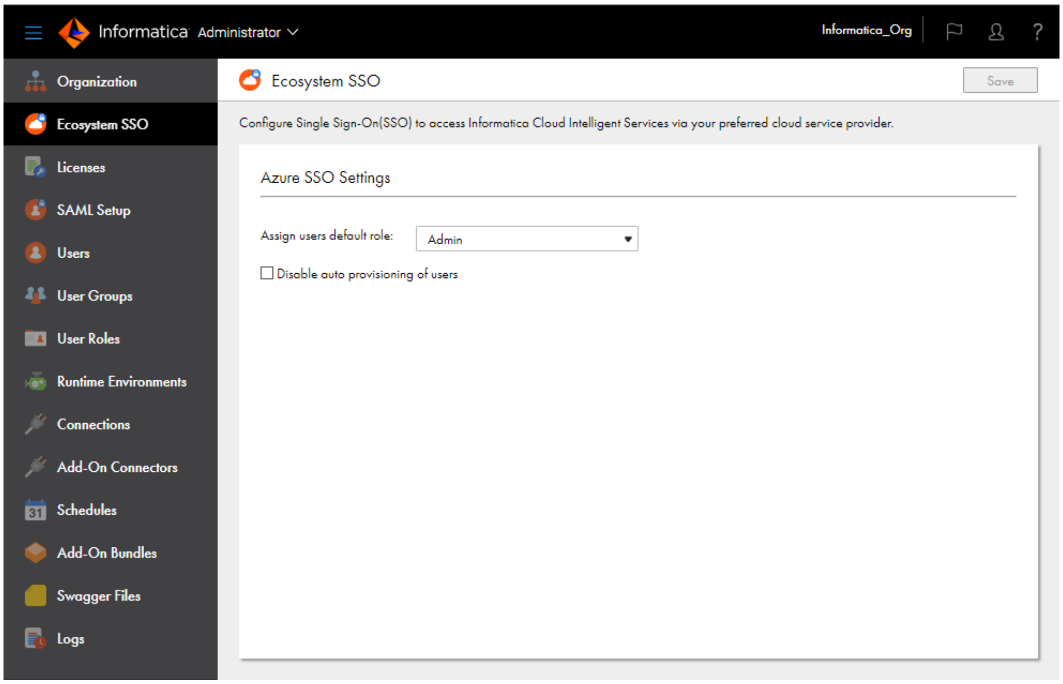
Ecosystem single sign-on

Informatica Intelligent Cloud Services enables single sign-on capability for Microsoft Azure users. This allows Microsoft Azure users to sign in to Informatica Intelligent Cloud Services without having to enter their login information again.

When you create your organization through Microsoft Azure, you can configure some single sign-on properties for Microsoft Azure users on the **Ecosystem SSO** page.

Note: The ecosystem single sign-on properties that you configure for Microsoft Azure are different than the SAML single sign-on properties that you configure to enable single-sign on from a third-party identity provider. To configure SAML single sign-on for your organization, see Chapter 3, "SAML single sign-on" on page 10.

The following image shows the **Ecosystem SSO** page:



Configure Single Sign-On(SSO) to access Informatica Cloud Intelligent Services via your preferred cloud service provider.

Azure SSO Settings

Assign users default role: Admin

□ Disable auto provisioning of users

You can configure the following properties for Microsoft Azure users:

Assign users default role

When a Microsoft Azure user signs in to your organization for the first time, Informatica Intelligent Cloud Services adds the user to your organization and assigns the user a default role. By default, Informatica Intelligent Cloud Services assigns the user the Admin role.

You can change the default role to a different role such as the Designer role. To change the default user role, select a different role in the **Assign users default role** list.

Note: If you want Microsoft Azure users to be able to download, install, and register a Secure Agent, assign them the Admin or Designer role. You can also assign users a custom role that has privileges to create, read, and update Secure Agents.

Disable auto-provisioning of users

By default, the first time a Microsoft Azure user signs in to Data Accelerator for Azure, Informatica Intelligent Cloud Services adds the user to your organization. This process is called auto-provisioning.

You can enable or disable the auto-provisioning of Microsoft Azure users. To do this, enable or disable the **Disable auto provisioning of users** option.

Note: If you disable auto-provisioning, you must create each user on the **Users** page. If you want the user to be able to use single sign-on from Microsoft Azure, you must also set the **Authentication** field on the user details page to **Azure SSO**.

CHAPTER 3

SAML single sign-on

You can enable single sign-on (SSO) capability so that users can access their organization without the need to enter login information. You can use SSO for user authentication or for both authentication and authorization in an organization. You configure SSO capability for an organization on the **SAML Setup** page.

Single sign-on to Informatica Intelligent Cloud Services is based on the Security Assertion Markup Language (SAML) 2.0 web browser single sign-on profile. The SAML web browser single sign-on profile consists of the following entities:

Identity provider

An entity that manages authentication information and provides authentication services through the use of security tokens.

Service provider

An entity that provides web services to principals, for example, an entity that hosts web applications. Informatica Intelligent Cloud Services is a service provider.

Principal

An end user who interacts through an HTTP user agent.

SAML 2.0 is an XML-based protocol that uses security tokens that contain assertions to pass information about a principal between an identity provider and a service provider. An assertion is a package of information that supplies statements made by a SAML authority. You can find more information about SAML on the Oasis web site: https://www.oasis-open.org

The process that occurs when a user enters the Informatica Intelligent Cloud Services URL in a browser or launches Informatica Intelligent Cloud Services through a chicklet differs based on whether the organization uses SAML SSO for authentication only or for both authentication and authorization.

SAML single sign-on for authentication only

When a user signs on to Informatica Intelligent Cloud Services and the organization uses SAML SSO for user authentication only, the following process occurs:

1. Informatica Intelligent Cloud Services sends a SAML authentication request to the organization's identity provider.
2. The identity provider confirms the user's identity and sends a SAML authentication response to Informatica Intelligent Cloud Services. The authentication response includes a SAML token.
3. When Informatica Intelligent Cloud Services receives the SAML authentication response from the identity provider, it completes the following tasks:
    - If the user exists, Informatica Intelligent Cloud Services establishes the user session and logs the user in.

    - If the user does not exist and auto-provisioning of users is enabled, Informatica Intelligent Cloud Services gets the user attributes from the SAML token, creates the user, and assigns the user the default role and the default group, if it is configured. Informatica Intelligent Cloud Services establishes the user session and logs the user in.
    - If the user does not exist and auto-provisioning of users is disabled, Informatica Intelligent Cloud Services fails the login.
4. When a user logs out of Informatica Intelligent Cloud Services or the session times out, Informatica Intelligent Cloud Services sends a SAML logout request to the identity provider.
5. The identity provider terminates the user session on the identity provider side.

SAML single sign-on for authentication and authorization

When a user signs on to Informatica Intelligent Cloud Services and the organization uses SAML SSO for authentication and authorization, the following process occurs:

1. Informatica Intelligent Cloud Services sends a SAML authentication request to the organization's identity provider.
2. The identity provider confirms the user's identity and sends a SAML authentication response to Informatica Intelligent Cloud Services. The authentication response includes a SAML token.
3. When Informatica Intelligent Cloud Services receives the SAML authentication response from the identity provider, it completes the following tasks:
    - If the user exists, Informatica Intelligent Cloud Services gets the user roles, groups, and attributes from the SAML token. It finds the corresponding Informatica Intelligent Cloud Services user roles and groups, and updates the user roles, if necessary. Informatica Intelligent Cloud Services establishes the user session and logs the user in.
    - If the user does not exist and auto-provisioning of users is enabled, Informatica Intelligent Cloud Services gets the user roles, groups, and attributes from the SAML token and creates the user. Informatica Intelligent Cloud Services establishes the user session and logs the user in. If the token contains no SAML role or group information, Informatica Intelligent Cloud Services fails the login.
    - If the user does not exist and auto-provisioning of users is disabled, Informatica Intelligent Cloud Services fails the login.
4. When a user logs out of Informatica Intelligent Cloud Services or the session times out, Informatica Intelligent Cloud Services sends a SAML logout request to the identity provider.
5. The identity provider terminates the user session on the identity provider side.

SAML single sign-on requirements

To set up SAML single sign-on for an Informatica Intelligent Cloud Services organization, the system must use an appropriate identity provider. You must also have the appropriate license.

To set up SAML single sign-on for an organization, ensure that the following requirements are met:

- The system must use a SAML 2.0-based identity provider.

  Common identity providers include Microsoft Active Directory Federation Services (AD FS), Okta, SSOCircle, OpenLDAP, and Shibboleth. The identity provider must be configured to use either the DSA-SHA256 or RSA-SHA256 algorithm to generate the signature.
- The Informatica Intelligent Cloud Services organization must have the SAML based Single Sign-On license.

- You must have access to the organization as an organization administrator to set up single sign-on.

Single sign-on restrictions

There are some restrictions for SAML single sign-on access to Informatica Intelligent Cloud Services.

The following restrictions apply to SAML single sign-on access:

- If your license with the identity provider expires, you cannot access Informatica Intelligent Cloud Services through single sign-on.
- If the identity provider is down or Informatica Intelligent Cloud Services servers cannot reach it, users cannot log in to Informatica Intelligent Cloud Services through single sign-on.
- If the identity provider certificate used for SAML single sign-on to Informatica Intelligent Cloud Services expires, users cannot access Informatica Intelligent Cloud Services through single sign-on.
- If your organization uses trusted IP address ranges, users cannot log in to Informatica Intelligent Cloud Services from an IP address that is not within the trusted IP address ranges.

User management with SAML authentication

When you use SAML SSO for user authentication only, Informatica Intelligent Cloud Services verifies the user credentials each time a user attempts to sign in to Informatica Intelligent Cloud Services. User authorization is managed within Informatica Intelligent Cloud Services through the users' group and role assignments.

To use SAML SSO for authentication only, disable the **Map SAML Groups and Roles** option on the **SAML Setup** page. This option is disabled by default. When this option is disabled, you must configure a default user role for new users on this page. You can also configure a default user group.

When you use SAML for authentication only, users are managed in the following ways:

New users with auto-provisioning

When a new user signs on to Informatica Intelligent Cloud Services for the first time and auto-provisioning is enabled, Informatica Intelligent Cloud Services gets the user attributes such as first name, last name, and email address from the SAML token and stores them in the repository. It creates the user and assigns the user the default role and the default group, if it is configured.

If you want to refine the user's level of access to assets, update the user's group and role assignments on the user details page.

New users without auto-provisioning

If auto-provisioning is disabled, users are not automatically added to the organization when they attempt to sign on to Informatica Intelligent Cloud Services for the first time. You must create the user in Administrator.

Existing users

When an existing user signs on, Informatica Intelligent Cloud Services authenticates the user but does not get the SAML roles, groups, or user attributes from the SAML token. If this information changes, you can update the user's groups and roles on the user details page.

You can also create a native user account with credentials in Administrator, and the user credentials are saved in the Informatica Intelligent Cloud Services repository. If you do this, the user must log in to Informatica Intelligent Cloud Services directly instead of using single sign-on.

If you delete a user from Informatica Intelligent Cloud Services, the user is deleted from the Informatica Intelligent Cloud Services repository but not from the identity provider.

For all SAML users, the information in the user profile is read-only except for the time zone. The password and security question do not appear in the user profile.

Switching from SAML authentication and authorization

If your organization uses SAML for authentication and authorization and you want to use SAML for authentication only, you can disable the **Map SAML Groups and Roles** option.

If you disable this option after it was previously enabled, the group and role mapping information on the **SAML Setup** page becomes read-only but is not deleted. All SAML groups become regular Informatica Intelligent Cloud Services groups. You can edit the groups, delete them, and add and remove group members.

When you disable this option, users' Informatica Intelligent Cloud Services roles do not change, so scheduled jobs are unaffected.

User management with SAML authentication and authorization

When you use SAML SSO for user authentication and authorization, Informatica Intelligent Cloud Services verifies the user credentials each time a user attempts to sign on. It also gets the user's SAML groups and roles and assigns the user the corresponding Informatica Intelligent Cloud Services roles.

To use SAML SSO for authentication and authorization, enable the **Map SAML Groups and Roles** option on the **SAML Setup** page. For some identity providers, you can also choose to push user and group information to Informatica Intelligent Cloud Services using SCIM 2.0.

When you enable the **Map SAML Groups and Roles** option, you must map Informatica Intelligent Cloud Services roles to SAML groups and roles on the **SAML Setup** page. Mapping roles and groups ensures that users have the appropriate levels of access to Informatica Intelligent Cloud Services assets. You cannot configure user roles or groups for these users individually in Administrator.

If the SAML groups that you map on the **SAML Setup** page do not exist in Informatica Intelligent Cloud Services, Informatica Intelligent Cloud Services creates user groups for them. You can view these groups on the **User Groups** page, but you cannot edit the group information or change the group members.

Informatica Intelligent Cloud Services ignores any SAML groups and roles that are returned in the SAML token but are not mapped on the **SAML Setup** page.

When you use SAML for authentication and authorization, users are managed in the following ways:

New users with auto-provisioning

When a new user signs on to Informatica Intelligent Cloud Services for the first time and auto-provisioning is enabled, Informatica Intelligent Cloud Services gets the SAML roles, groups, and user attributes from the SAML token and stores them in the repository. It creates and authenticates the user and assigns the user the Informatica Intelligent Cloud Services roles that are mapped on the **SAML Setup** page.

If there are no roles or groups in the SAML token, Informatica Intelligent Cloud Services fails the login.

New users without auto-provisioning

If auto-provisioning is disabled, users are not automatically added to the organization when they attempt to sign on to Informatica Intelligent Cloud Services for the first time. You must create the user in Administrator.

Existing users

When an existing user signs on, Informatica Intelligent Cloud Services authenticates the user and gets the SAML roles, groups, and user attributes from the SAML token. If this information has changed since the last login, Informatica Intelligent Cloud Services updates the user attributes and roles.

You can also create a native user account with credentials in Administrator, and the user credentials are saved in the Informatica Intelligent Cloud Services repository. If you do this, the user must log in to Informatica Intelligent Cloud Services directly instead of using single sign-on. You can delete these user accounts in Administrator.

For all SAML users, the information in the user profile is read-only except for the time zone. The password and security question do not appear in the user profile.

Switching from SAML authentication only

If your organization uses SAML authentication only and you want to use SAML for authentication and authorization, you can enable the **Map SAML Groups and Roles** option.

If you enable this option after it was previously disabled, the group and role mapping information on the **SAML Setup** page becomes editable. If any group or role mapping was configured previously, it is retained.

When you enable this option, users' authorization information is updated when they are authenticated in Informatica Intelligent Cloud Services with a new SAML token. This can affect a user's scheduled jobs if the user's privileges change.

Pushing user and group information using SCIM 2.0

When you use SAML SSO for authentication and authorization and the identity provider is Okta or Azure Active Directory, you can choose to push user and group information to Informatica Intelligent Cloud Services using SCIM 2.0. To do this, enable the **Enable IdP to push users/groups using SCIM 2.0** option on the **SAML Setup** page.

Enabling this option allows the identity provider to push user and group information at regular intervals to provision new users, delete users, and keep each user's SAML groups and roles in sync with their Informatica Intelligent Cloud Services user roles. In this case, auto-provisioning of users is disabled because users are provisioned through SCIM. You can also create users manually in Administrator.

Informatica Intelligent Cloud Services hosts SCIM endpoints that the identity provider can use to perform certain operations in Informatica Intelligent Cloud Services. These operations include creating and deactivating users, creating and deleting user groups, adding and removing users from groups, and updating user attributes.

To access the SCIM endpoints, you must create a provisioning app as a SCIM client in Azure Active Directory or Okta. No special privileges are needed to access the SCIM endpoints. When you create the app, you must provide the token that you generate on the **SAML Setup** page. The SCIM token is valid for six months from the time of generation.

For information about setting up SCIM 2.0 and creating the provisioning app, see the following H2L articles on Informatica Network:

- Setting up SCIM with Azure Active Directory
- Setting up SCIM with Okta

When you enable SCIM provisioning, additional user attributes such as Display Name, Employee Number, Organization, Division, and Department are also pushed to Informatica Intelligent Cloud Services. You must map these attributes on the **SAML Setup** page. You can view these attributes for each user on the user details page.

User and group information for individual users is also passed in the SAML token during single sign-on. As a result, if a user's SAML roles, groups, or attributes change, Informatica Intelligent Cloud Services updates the user information when the user signs on.

SAML single sign-on configuration for Informatica Intelligent Cloud Services

Informatica Intelligent Cloud Services and your identity provider exchange configuration information when you set up single sign-on.

Informatica Intelligent Cloud Services requires identity provider metadata to send authentication and authorization requests to the identity provider. The identity provider requires service provider metadata from Informatica Intelligent Cloud Services to send responses to Informatica Intelligent Cloud Services.

SAML and Informatica Intelligent Cloud Services attributes need to be mapped so that Informatica Intelligent Cloud Services can consume the data passed in authentication responses. After you configure single sign-on settings in Informatica Intelligent Cloud Services, pass the Informatica Intelligent Cloud Services service provider metadata to your identity provider.

To configure single sign-on for Informatica Intelligent Cloud Services, complete the following tasks:

1. Configure the SAML identity provider and service provider settings, and map SAML attributes to Informatica Intelligent Cloud Services attributes in Informatica Intelligent Cloud Services.
2. Download the Informatica Intelligent Cloud Services service provider metadata from Informatica Intelligent Cloud Services, and deliver the metadata and the Informatica Intelligent Cloud Services single sign-on URL for your organization to your SAML identity provider administrator.

Configuring provider settings and mapping attributes

Configure SAML single sign-on settings and map SAML attributes on the **SAML Setup** page.

1. Log in to Informatica Intelligent Cloud Services as an organization administrator.
2. In Administrator, select **SAML Setup**.
3. On the **SAML Setup** page, configure the following properties:
    - SSO configuration properties
    - Identity provider configuration properties

- Service provider settings
- SAML attribute mapping properties
- SAML role and group mapping properties (if you use SAML SSO for authentication and authorization)

4. Click **Save**.

   Informatica Intelligent Cloud Services generates the service provider metadata file. Informatica Intelligent Cloud Services also generates a unique token for your organization and saves the token to the Informatica Intelligent Cloud Services repository. The single sign-on URL for your organization includes the token. For example:

   ```
   https://dm-us.informaticacloud.com/ma/sso/<organization token>
   ```

After you save your changes on the **SAML Setup** page, download the service provider metadata, and send it to your identity provider along with the Informatica Intelligent Cloud Services single sign-on URL.

SSO configuration properties

Define single sign-on configuration properties on the **SAML Setup** page.

If you have an identity provider XML file, you can upload the file to populate some of the properties. Informatica Intelligent Cloud Services can parse and extract most of the data from the XML file. However, you might need to enter certain fields manually such as the name identifier format.

The following table describes the SSO configuration properties:

Property	Description
Use Identity Provider File	The identity provider XML file that populates many of the properties on the **SAML Setup** page. To use an identity provider XML file to define identity provider properties, click **Browse**, and navigate to the identity provider XML file.
Disable auto provisioning of users	Disables auto-provisioning of SAML users. When you enable this option, users are not automatically added to the organization when they attempt to sign on to Informatica Intelligent Cloud Services for the first time. If you disable auto-provisioning and you don't use SCIM 2.0 to push user and group information from the identity provider, you must create the users manually in Administrator. If you use SCIM 2.0, this option is disabled because users are provisioned by the SCIM client. Default is disabled.
Map SAML Groups and Roles	Maps groups and roles from the SAML token each time a user signs on to Informatica Intelligent Cloud Services. Enable this option to use SAML SSO for both authentication and authorization. Disable this option to use SAML SSO for authentication only. Default is disabled.
Enable IdP to push users/groups using SCIM 2.0	Allows your identity provider to push user and group information to Informatica Intelligent Cloud Services using SCIM 2.0 in addition to passing these attributes in the SAML token. When you enable this option, you must generate a bearer token for the identity provider (SCIM client). To generate the token, click **Generate Token**. **Warning:** If you provide the identity provider with a token and then generate a new token, the previous token is overwritten, and you must provide the identity provider with the new token. When you enable this option, auto-provisioning of users is disabled because users are provisioned through the SCIM client. Default is disabled.

Identity provider configuration properties

Define identity provider configuration properties on the **SAML Setup** page.

The following table describes the identity provider configuration properties:

Property	Description
Issuer	The entity ID of the identity provider, which is the unique identifier of the identity provider. The Issuer value in all messages from the identity provider to Informatica Intelligent Cloud Services must match this value. For example: `<saml:Issuer>http://idp.example.com</saml:Issuer>`
Single Sign-On Service URL	The identity provider's HTTP-POST SAML binding URL for the SingleSignOnService, which is the SingleSignOnService element's location attribute. Informatica Intelligent Cloud Services sends login requests to this URL.
Single Logout Service URL	The identity provider's HTTP-POST SAML binding URL for the SingleLogoutService, which is the SingleLogoutService element's location attribute. Informatica Intelligent Cloud Services sends logout requests to this URL.
Signing Certificate	Base64-encoded PEM format identity provider certificate that Informatica Intelligent Cloud Services uses to validate signed SAML messages from the identity provider. **Note:** The identity provider signing algorithm must be either DSA-SHA1 or RSA-SHA1.
Use signing certificate for encryption	Uses the public key in your signing certificate to encrypt logout requests sent to your identity provider when a user logs out from Informatica Intelligent Cloud Services.
Encryption Certificate	Base64-encoded PEM format identity provider certificate that Informatica Intelligent Cloud Services uses to encrypt SAML messages sent to the identity provider. Applicable if you do not enable use of the signing certificate for encryption.
Name Identifier Format	The format of the name identifier in the authentication request that the identity provider returns to Informatica Intelligent Cloud Services. Informatica Intelligent Cloud Services uses the name identifier value as the Informatica Intelligent Cloud Services user name. The name identifier cannot be a transient value that can be different for each login. For a particular user, each single sign-on login to Informatica Intelligent Cloud Services must contain the same name identifier value. To specify that the name identifier is an email address, the Name Identifier Format is as follows: `urn:oasis:names:tc:SAML:1.1:nameidformat:emailAddress`
Logout Service URL (SOAP Binding)	The identity provider's SAML SOAP binding URL for the single logout service. Informatica Intelligent Cloud Services sends logout requests to this URL.
Logout Page URL	The landing page to which a user is redirected after the user logs out of Informatica Intelligent Cloud Services. Informatica Intelligent Cloud Services redirects the logged out user to the landing page in the following ways: - If you specify a logout page URL, Informatica Intelligent Cloud Services redirects the user to this URL after logout. - If you do not specify a logout page URL, Informatica Intelligent Cloud Services redirects the user to a default logout page.

Service provider settings

Define the Informatica Intelligent Cloud Services service provider settings on the **SAML Setup** page.

The following table describes service provider settings:

Property	Description
Informatica Cloud Platform SSO	Displays the single sign-on URL for your organization. This URL is automatically generated by Informatica Intelligent Cloud Services.
Clock Skew	Specifies the maximum permitted time, in seconds, between the time stamps in the SAML response from the identity provider and the Informatica Intelligent Cloud Services clock. Default is 180 seconds (3 minutes).
Name Identifier value represents user's email address	If enabled, Informatica Intelligent Cloud Services uses the name identifier as the email address. Default is enabled.
Sign authentication requests	If enabled, Informatica Intelligent Cloud Services signs authentication requests to the identity provider. Default is enabled.
Sign logout requests sent using SOAP binding	If enabled, Informatica Intelligent Cloud Services signs logout requests sent to the identity provider. Default is enabled.
Encrypt name identifier in logout requests	If enabled, Informatica Intelligent Cloud Services encrypts the name identifier in logout requests. **Note:** Verify that the identity provider supports decryption of name identifiers before you enable this option. Default is disabled.

SAML attribute mapping properties

User login attributes such as name, email address, and user role are included in the authentication response from the identity provider to Informatica Intelligent Cloud Services. If the identity provider passes user and group information using SCIM 2.0, the authentication response includes additional SCIM attributes such as Display Name, Employee Number, and Organization.

Map the Informatica Intelligent Cloud Services user fields to corresponding SAML attributes on the **SAML Setup** page.

Note: The attribute format differs based on your identity provider. Refer to the provider documentation for more information.

The following table describes the SAML attribute mapping properties:

Property	Description
Use friendly SAML attribute names	If selected, uses the human-readable form of the SAML attribute name which might be useful in cases in which the attribute name is complex or opaque, such as an OID or a UUID.
First Name	SAML attribute used to pass the user first name.

Property	Description
Last Name	SAML attribute used to pass the user last name.
Job Title	SAML attribute used to pass the user job title.
Email Addresses	SAML attribute used to pass the user email addresses. This property must be mapped.
Emails Delimiter	Delimiter to separate the email addresses if multiple email addresses are passed.
Phone Number	SAML attribute used to pass the user phone number.
Time Zone	SAML attribute used to pass the user time zone.
User Roles	SAML attribute used to pass the assigned user roles. This field is enabled when the **Map SAML Groups and Roles** option is enabled.
Roles Delimiter	Delimiter to separate the roles if multiple roles are passed. This field is enabled when the **Map SAML Groups and Roles** option is enabled.
User Groups	SAML attribute used to pass the assigned user groups. This field is enabled when the **Map SAML Groups and Roles** option is enabled.
Groups Delimiter	Delimiter to separate the groups if multiple groups are passed. This field is enabled when the **Map SAML Groups and Roles** option is enabled.

The following table describes the additional attributes. These attributes are visible when the **Enable IdP to push users/groups using SCIM 2.0** option is enabled:

Property	Description
Display Name	SCIM attribute used to pass the user displayName.
Employee Number	SCIM attribute used to pass the enterprise user employeeNumber.
Organization	SCIM attribute used to pass the enterprise user organization.
Department	SCIM attribute used to pass the enterprise user department.
Street Address	SCIM attribute used to pass the user streetAddress.
Locality	SCIM attribute used to pass the user locality.
Region	SCIM attribute used to pass the user region.
Post Code	SCIM attribute used to pass the user postalCode.
Country	SCIM attribute used to pass the user country.
Locale	SCIM attribute used to pass the user locale.
Preferred Language	SCIM attribute used to pass the user preferredLanguage.

Property	Description
ID	SCIM attribute used to pass the user id.
External ID	SCIM attribute used to pass the user externalId. For Azure Active Directory, this is the objectID. For Okta, it is the id.

SAML role and group mapping properties

When you use SAML for authentication only, define a default role and optional default user group for new users. When you use SAML for authentication and authorization, map SAML role and group names to Informatica Intelligent Cloud Services role names. You can map multiple SAML roles and groups to a single Informatica Intelligent Cloud Services role.

Define the SAML role and group mapping properties on the **SAML Setup** page.

The following table describes SAML role mapping properties:

Property	Description
Informatica Intelligent Cloud Services role	The SAML role equivalent for the Informatica Intelligent Cloud Services role. If you need to enter more than one role, use a comma to separate the roles. The role mapping fields are enabled when the **Map SAML Groups and Roles** option is enabled.
Default Role	Default user role for single sign-on users. When auto-provisioning is enabled, new users are assigned this role the first time they sign on to Informatica Intelligent Cloud Services. This field is visible when the **Map SAML Groups and Roles** option is disabled.
Default User Group	Optional, default user group for single sign-on users. When auto-provisioning is enabled, new users are assigned to this user group the first time they sign on to Informatica Intelligent Cloud Services. This field is visible when the **Map SAML Groups and Roles** option is disabled.

The following table describes SAML group mapping properties:

Property	Description
Informatica Intelligent Cloud Services role	The SAML group equivalent for the Informatica Intelligent Cloud Services role. If you need to enter more than one group, use a comma to separate the groups. You can enter up to 4000 characters. The role mapping fields are enabled when the **Map SAML Groups and Roles** option is enabled.
Default Role	Default user role for single sign-on users. When auto-provisioning is enabled, new users are assigned this role the first time they sign on to Informatica Intelligent Cloud Services. This field is visible when the **Map SAML Groups and Roles** option is disabled.
Default User Group	Optional, default user group for single sign-on users. When auto-provisioning is enabled, new users are assigned to this user group the first time they sign on to Informatica Intelligent Cloud Services. This field is visible when the **Map SAML Groups and Roles** option is disabled.

Downloading the service provider metadata

The identity provider requires the SAML service provider metadata and Informatica Intelligent Cloud Services URL to complete the SAML single sign-on setup process. After Informatica Intelligent Cloud Services generates the service provider metadata file, deliver the file and the Informatica Intelligent Cloud Services URL to the identity provider.

1. On the **SAML Setup** page, click **Download Service Provider Metadata**.

   The service provider metadata file is downloaded to your machine.
2. In the **Information** dialog box, note the URL for single sign-on access to your Informatica Intelligent Cloud Services organization.
3. Click **OK** to close the **Information** dialog box.
4. Send the metadata file and the Informatica Intelligent Cloud Services single sign-on URL to your identity provider administrator.

CHAPTER 4

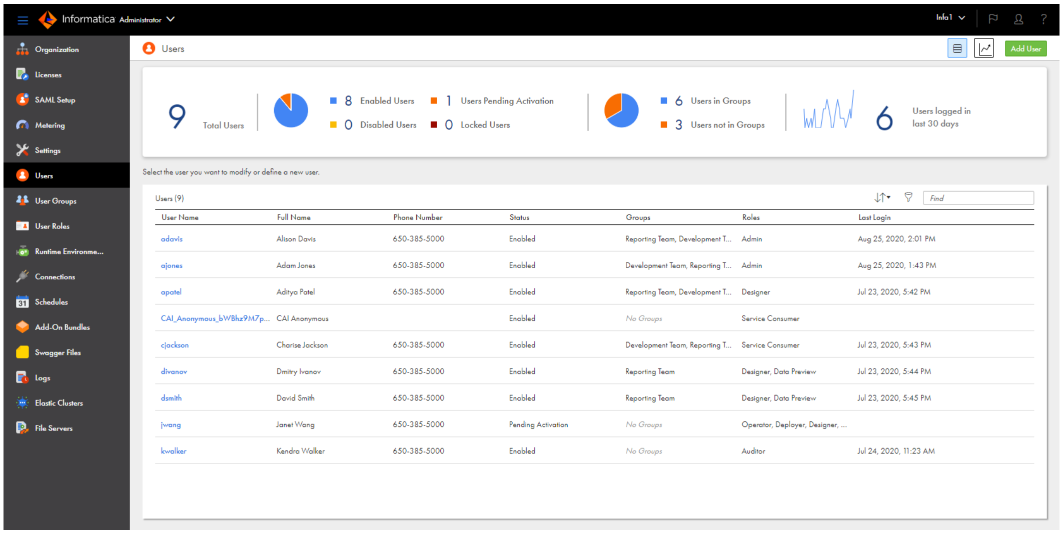
Users

A user is an individual Informatica Intelligent Cloud Services account that allows secure access to an organization. A user can perform tasks and access assets based on the roles that are assigned to the user. You can assign roles directly to the user or to a group that the user is a member of.

Administrators can create and configure user accounts for the organization.

The **Users** page lists the users in your organization. To access the **Users** page, in Administrator, select **Users**.

The following image shows the **Users** page:



Select the user you want to modify or define a new user.

Users (9)

User Name	Full Name	Phone Number	Status	Groups	Roles	Last Login
adavis	Alison Davis	650-385-5000	Enabled	Reporting Team, Development T...	Admin	Aug 25, 2020, 2:01 PM
ajones	Adam Jones	650-385-5000	Enabled	Development Team, Reporting T...	Admin	Aug 25, 2020, 1:43 PM
apatel	Aditya Patel	650-385-5000	Enabled	Reporting Team, Development T...	Designer	Jul 23, 2020, 5:42 PM
CAI_Anonymous_bWBhz9M7p...	CAI Anonymous		Enabled	No Groups	Service Consumer	
cjackson	Charise Jackson	650-385-5000	Enabled	Development Team, Reporting T...	Service Consumer	Jul 23, 2020, 5:43 PM
divanov	Dmitry Ivanov	650-385-5000	Enabled	Reporting Team	Designer, Data Preview	Jul 23, 2020, 5:44 PM
dsmith	David Smith	650-385-5000	Enabled	Reporting Team	Designer, Data Preview	Jul 23, 2020, 5:45 PM
jwang	Janet Wang	650-385-5000	Pending Activation	No Groups	Operator, Deployer, Designer, ...	
kwalker	Kendra Walker	650-385-5000	Enabled	No Groups	Auditor	Jul 24, 2020, 11:23 AM

The **Users** page displays user statistics for the organization and lists each user.

The statistics area displays the total number of users, number of users with each status, number of users in groups, and the number of users that have logged in during the last 30 days. The number of users logged in during the last 30 days is calculated using the organization's time zone and excludes the current day.

The Users area lists each user. If you use Application Integration, the list includes the Application Integration anonymous user and its status. To view detailed information about a user, click the user name.

You can perform the following tasks for a user:

- View and edit user details.
- Create a user.
- Assign and unassign services.
- Disable a user.
- Reset a user.

- Reassign a user's scheduled jobs to a different user.
- Delete a user.

User authentication

Informatica Intelligent Cloud Services uses different types of user authentication. Native users are authenticated through Informatica Intelligent Cloud Services. Salesforce, Microsoft Azure, and SAML users are authenticated through their identity providers.

Informatica Intelligent Cloud Services can use the following types of user authentication:

Native

Native users log in to Informatica Intelligent Cloud Services through the Informatica Intelligent Cloud Services login page using their user names and passwords. They are authenticated through Informatica Intelligent Cloud Services.

Salesforce

Salesforce users sign in to Informatica Intelligent Cloud Services through Salesforce or a Salesforce app. They are authenticated through Salesforce.

For more information about Salesforce authentication, see the help for the Salesforce connector in the Data Integration help.

Microsoft Azure

Microsoft Azure users sign in to Informatica Intelligent Cloud Services through Microsoft Azure. They are authenticated through Microsoft Azure.

For more information about Microsoft Azure authentication, see Chapter 2, “Ecosystem single sign-on” on page 8.

SAML

SAML users sign in to Informatica Intelligent Cloud Services through their identity provider. They are authenticated through their identity provider.

For more information about configuring SAML single sign-on, see Chapter 3, “SAML single sign-on” on page 10.

Application Integration anonymous user

Informatica Intelligent Cloud Services creates a system user called `CAI_Anonymous_<Organization_ID>`. Application Integration needs this user when you invoke an anonymous process that calls a Data Integration task.

Important: Do not edit or delete the Application Integration anonymous user if you need to invoke an anonymous process that calls a Data Integration task.

If you assign custom permissions to a Data Integration task and invoke the Data Integration task through an Application Integration process or a guide, you must complete either of the following tasks:

- Give the Application Integration anonymous user permission to run the associated Data Integration asset.

- Add the Application Integration anonymous user to a user group that has permission to run the associated Data Integration asset.

Model Serve system user

Informatica Intelligent Cloud Services creates a system user called ModelServe_System_<Organization_ID>.

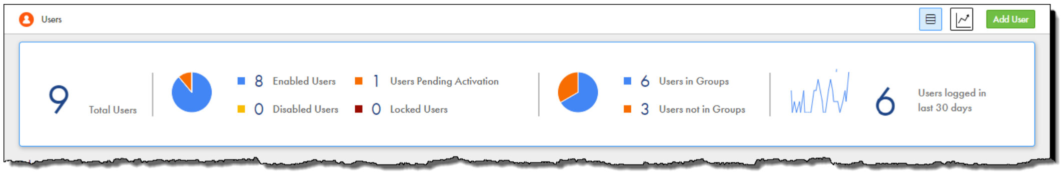
Model Serve needs this user to perform tasks, such as provisioning resources to deploy a machine learning model. Do not edit or delete the Model Serve system user.

User statistics

If you have the Admin role or the Read User and Audit Log - View privileges, you can view user statistics for your organization.

The statistics area on the **Users** page displays statistics such as the number of users in the organization, the number of users with each status, and the number of users that logged in during a certain time period.

The following image shows the statistics area:



Users

Add User

9 Total Users

8 Enabled Users

1 Users Pending Activation

0 Disabled Users

0 Locked Users

6 Users in Groups

3 Users not in Groups

6 Users logged in last 30 days

You can use the statistics area to filter the users on the **Users** page. For example, to display only users with the status Pending Activation, click **Users Pending Activation**. To list all users, click **Total Users**.

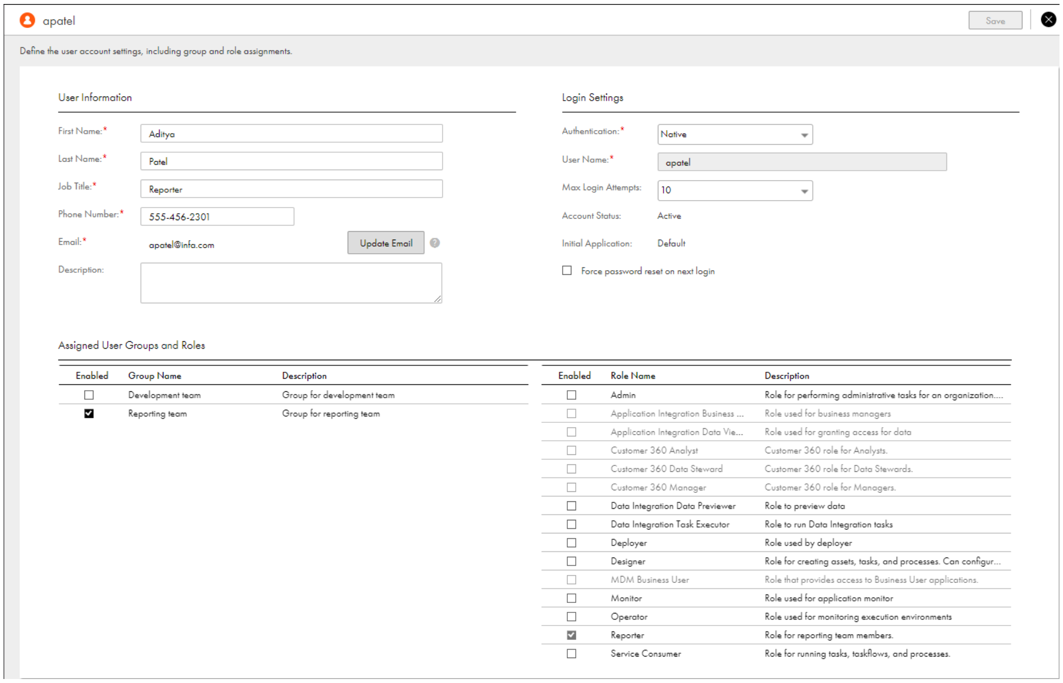
If you have the Admin role or the Create User and Audit Log - View privileges, you can view a graph of the numbers of users that logged in per day during the last 7, 30, or 90 days. To view the graph, click **Chart View** and select the appropriate time period. You can also download a report that lists the login date and time for each user during the time period.

To return to the list view of the **Users** page, click **List View**.

User details

You can configure user details such as user name, email, login settings, and assigned user groups and roles on the user details page. To display the user details page, in Administrator, select **Users**, and then click the user name.

The following image shows the user details page:



apatel

Define the user account settings, including group and role assignments.

User Information

First Name:* Aditya

Last Name:* Patel

Job Title:* Reporter

Phone Number:* 555-456-2301

Email:* apatel@infa.com

Description:

Login Settings

Authentication:* Native

User Name:* apatel

Max Login Attempts: 10

Account Status: Active

Initial Application: Default

□ Force password reset on next login

Assigned User Groups and Roles

Enabled	Group Name	Description
□	Development team	Group for development team
☑	Reporting team	Group for reporting team

Enabled	Role Name	Description
□	Admin	Role for performing administrative tasks for an organization....
□	Application Integration Business ...	Role used for business managers
□	Application Integration Data Vie...	Role used for granting access for data
□	Customer 360 Analyst	Customer 360 role for Analysts.
□	Customer 360 Data Steward	Customer 360 role for Data Stewards.
□	Customer 360 Manager	Customer 360 role for Managers.
□	Data Integration Data Previewer	Role to preview data
□	Data Integration Task Executor	Role to run Data Integration tasks
□	Deployer	Role used by deployer
□	Designer	Role for creating assets, tasks, and processes. Can configur...
□	MDM Business User	Role that provides access to Business User applications.
□	Monitor	Role used for application monitor
□	Operator	Role used for monitoring execution environments
☑	Reporter	Role for reporting team members.
□	Service Consumer	Role for running tasks, taskflows, and processes.

You can configure the following details for a user:

User information

The following table describes the user information:

Property	Description
First name	First or given name of the user.
Last name	Last or family name of the user.
Job title	User job title.
Phone number	Telephone number for the user.

Property	Description
Email	Email address of the user. Must be a valid email address in the format: `<local_part>@<domain>`. For example, jsmith@mycompany.com. To update the email address, click **Update Email**. Informatica Intelligent Cloud Services sends a verification email to the new email address. The email contains a link that is valid for 24 hours. When the user clicks the link in the verification email, the new email address is verified, and it appears on the user details page and in the user's profile. If the link expires, you can resend the verification email. You cannot update the email address for a SAML user in Administrator. To update a SAML user's email address, update the email address in the identity provider.
Description	Optional user description.

Extended user attributes

If your organization uses SAML single sign-on for authentication and authorization and the identity provider pushes user and group information to IICS using SCIM 2.0, this tab displays SCIM attributes such as the display name, employee number, organization, and department.

This tab does not appear for non-SAML users.

Login settings

The following table describes the login settings:

Property	Description
Authentication	Authentication method. Can be one of the following values: - Native. The user is authenticated through Informatica Intelligent Cloud Services. The user logs in through the Informatica Intelligent Cloud Services URL. - Salesforce. The user is authenticated through Salesforce and signs in through Salesforce or a Salesforce app. - Azure SSO. The user is authenticated and signs in through Microsoft Azure. - IDP with SAML. The user is authenticated and signs in through a SAML identity provider.
Activate using verification code / Activate using Salesforce OAuth	Account activation method for Salesforce users. Select one of the following options: - Activate using verification code. Select this option when the user signs in to Informatica Intelligent Cloud Services through a Salesforce app. When you select this option, the user receives an email with a verification code. The user account is activated when the user logs in to Salesforce, opens the Salesforce app, and enters the verification code. - Activate using Salesforce OAuth. Select this option to activate the user account using Salesforce OAuth. When you select this option, the user receives an email with a **Confirm Account** link. The user account is activated when the user clicks the **Confirm Account** link and enters the Salesforce user name and password. These options are displayed when the authentication method is Salesforce.
Environment	Salesforce organization environment, either production or sandbox. This option displayed when the user activation method is Salesforce OAuth.

Property	Description
User name	Informatica Intelligent Cloud Services user name. Must be unique within the Informatica Intelligent Cloud Services organization. You cannot change the name after you save the user. This property is displayed when the authentication method is Native.
Salesforce user name	Salesforce user name. Must be unique within the Informatica Intelligent Cloud Services organization. You cannot change the name after you save the user. For Salesforce users, the Informatica Intelligent Cloud Services user name is the same as the Salesforce user name unless that name is already used in the Informatica Intelligent Cloud Services organization. If the name is already used, then Informatica Intelligent Cloud Services appends the string ".Salesforce," ".Salesforce1," ".Salesforce2," etc. to the end of the Salesforce user name to form a unique Informatica Intelligent Cloud Services user name. This property is displayed when the authentication method is Salesforce.
Azure user name	Microsoft Azure user name. Must be unique within the Informatica Intelligent Cloud Services organization. You cannot change the name after you save the user. For Microsoft Azure users, the Informatica Intelligent Cloud Services user name is the same as the Azure user name unless that name is already used in the Informatica Intelligent Cloud Services organization. If the name is already used, then Informatica Intelligent Cloud Services appends the string ".Azure," ".Azure1," ".Azure2," etc. to the end of the Azure user name to form a unique Informatica Intelligent Cloud Services user name. This property is displayed when the authentication method is Azure SSO.
SAML user name	SAML user name. Must be unique within the Informatica Intelligent Cloud Services organization. You cannot change the name after you save the user. For SAML users, the Informatica Intelligent Cloud Services user name is the same as the SAML name identifier unless that name is already used in the Informatica Intelligent Cloud Services organization. If the name is already used, then Informatica Intelligent Cloud Services appends the string ".SAML," ".SAML1," ".SAML2," etc. to the end of the SAML name identifier to form a unique Informatica Intelligent Cloud Services user name. This property is displayed when the authentication method is IDP with SAML.
Max login attempts	Maximum number of login attempts that the user can make before the user is locked out. Select a number or "No Limit." If locked out, the user can click the **Forgot your password** link on the Login page, or the organization administrator can reset the user on the **Users** page. This property is displayed when the authentication method is Native.
Account status	Account status. Can be one of the following statuses: - Pending Activation. The user account has been created or reset, but the user has not yet activated the account. - Enabled. The user account has been created and validated, and the user can log in to Informatica Intelligent Cloud Services. - Locked. Applies to native user accounts. The account is locked because the user has exceeded the maximum number of login attempts. To unlock the user, the user can click the **Forgot your password** link on the Login page, or you can reset the user on the **Users** page. - Disabled. The user account has been disabled by an administrator. The user cannot log in to Informatica Intelligent Cloud Services.

Property	Description
Initial application	This field is reserved for future use.
Force password reset on next login	Forces the user to reset the password the next time the user tries to log in. This property is displayed when the authentication method is Native.

Assigned user groups and roles

You must assign at least one user group or role to each user. To assign or remove a user group or role, enable or disable the group or role, and then click **Save**.

When you assign a group to a user, all roles that are associated with the group become enabled. You cannot remove these roles individually. To remove the roles, you must remove the group.

Note: If your organization uses SAML for authentication and authorization, you cannot edit user details for a SAML user. User details are mapped automatically according to the mapped attributes, roles, and groups on the **SAML Setup** page.

Creating a user

Create a user on the **Users** page. When you create a user, the user status is set to Pending Activation or to Enabled based on the authentication method.

1. In Administrator, select **Users**.
2. Click **Add User**.
3. Enter the user information.
4. Enter the login settings:
    a. Select the authentication method.
    b. For Salesforce users, specify whether to activate the user account using a verification code or Salesforce OAuth.
    c. Enter the Informatica Intelligent Cloud Services user name or the user name in the third-party identity provider's system.

       For native users, enter the Informatica Intelligent Cloud Services user name. For Salesforce, Microsoft Azure, or SAML users, enter the user name in the third-party identity provider's system.

       The user name must be unique within the Informatica Intelligent Cloud Services organization. You cannot change the user name after you create a user.
    d. For native users, select the maximum number of login attempts.
5. In the Assigned User Groups and Roles section, select the user groups and roles that you want to assign to the user.

   You can assign system-defined and custom roles to a user. If you assign a group, the user inherits all roles that are associated with the group.
6. Click **Save**.

After you create a user, the user status is set as follows based on the authentication method:

- Native users are set to Pending Activation. The user receives an email to confirm the account. When the user clicks the **Confirm Account** link in the email, the user is prompted to set up a password and security question. When the user does this, the status changes to Enabled, and the user can log in to Informatica Intelligent Cloud Services.
- Salesforce users are set to Pending Activation.

  If you activate the user using a verification code, the user receives an email with a verification code. The user account is activated when the user logs in to Salesforce, opens the Salesforce app, and enters the verification code.

  If you activate the user using Salesforce OAuth, the user receives an email with a **Confirm Account** link. The user account is activated when the user clicks the **Confirm Account** link and enters the Salesforce user name and password.
- Microsoft Azure and SAML users are set to Enabled. The user can sign in through the user's identity provider.

Assigning and unassigning services

When you create a user, the user can access services based on the organization's licenses and the user's role. You can restrict the user's access to these services.

To allow or prevent a user from accessing certain services, you assign or unassign the services to the user. Assign and unassign services to a user on the **Users** page.

When you assign a service to a user, the service is visible on the **My Services** page. The user can access and use the service as long as the user's role allows this.

When you unassign a service, the user cannot see the service on the **My Services** page. The user cannot access or use the service regardless of the user's role.

For example, you want to allow an application developer with the Service Consumer role to use API Portal but not Data Integration or Application Integration. Assign the API Portal service to the user and unassign the Data Integration and Application Integration services. When you do this, the application developer can no longer see the Data Integration and Application Integration services on the **My Services** page. The application developer cannot use these services even though the Service Consumer role has privileges related to them.

1. In Administrator, select **Users**.
2. In the row that contains the user, click **Actions** and select **Assign Services**.
3. In the **Assign Services** dialog box, select the services that you want to assign to the user and deselect the services that you want to unassign.
4. Click **Save**.

Disabling a user

Disable a user on the **Users** page. When you disable a user, the user can no longer log in to Informatica Intelligent Cloud Services.

Before you disable a user, verify that the user did not schedule any tasks or taskflows. If you disable a user who has scheduled tasks or taskflows, the scheduled jobs fail.

When you disable a user, the user remains in the organization and in the Informatica Intelligent Cloud Services repository. You can view the user details, but you cannot edit them. Assets that the user created or updated also remain in the organization. On the Explore page, the Created by and Updated by columns indicate that the user is disabled.

1. In Administrator, select **Users**.
2. In the row that contains the user whom you want to disable, click **Actions** and select **Disable**.

   Note: When you use a file listener in Mass Ingestion Files (as a trigger or as a source) and in taskflow (as a trigger or as a file watch) you must reassign the ownership of the file listener association from one user to another using REST API before you delete a user. For more information, see *REST API Reference* guide.

Resetting a user

Reset a user on the **Users** page. You can reset a user whose account is disabled or locked. When you reset a user, the user status is set to Pending Activation or to Enabled based on the authentication method.

1. In Administrator, select **Users**.
2. In the row that contains the user, click **Actions** and select **Reset**.

After you reset a user, the user status is reset differently based on the authentication method:

- Native users are set to Pending Activation. The user receives an email to confirm the account. When the user clicks the **Confirm Account** link in the email, the user is prompted to reset the password and security question. The user can then log in to Informatica Intelligent Cloud Services.
- Salesforce users are set to Pending Activation.

  If you activated the user using a verification code, the user receives an email with a verification code. The user account is activated when the user logs in to Salesforce, opens the Salesforce app, and enters the verification code.

  If you activated the user using Salesforce OAuth, the user receives an email with a **Confirm Account** link. The user account is activated when the user clicks the **Confirm Account** link and enters the Salesforce user name and password.
- Microsoft Azure and SAML users are set to Enabled. The user can sign in through the user's identity provider.

Reassigning a user's scheduled jobs

Reassign a user's scheduled jobs on the **Users** page. You might want to reassign scheduled jobs when a user that has scheduled tasks or taskflows leaves the organization. You must reassign the user's scheduled jobs before you can delete the user.

The owner of a scheduled job is the last person that saves the scheduled task or taskflow. For example, in your organization, user Arun creates a schedule, user Beth creates a mapping task and assigns the schedule to the task, and then user Chandra updates and saves the task. Chandra becomes the owner of the scheduled job. If Chandra leaves the organization, you must reassign her scheduled jobs to another user before you can delete her user account.

1. In Administrator, select **Users**.
2. In the row that contains the user, click **Actions** and select **Reassign Scheduled Jobs**.
3. Select a user to whom to reassign the scheduled jobs.

   The user you select must be an enabled user.
4. Click **Reassign**.

You can reassign the ownership of a file listener association from one user to an another using REST API. For more information, see *REST API Reference*.

Deleting a user

Delete a user on the **Users** page. When you delete a user, the user is removed from the organization and from the Informatica Intelligent Cloud Services repository. If your organization uses SAML for authentication and authorization, you cannot delete a SAML user that you did not create in Administrator.

Before you can delete a user, you must reassign the user's scheduled jobs to a different user.

Note: You cannot reset a deleted user. If you think you might need to reactivate the user account, disable the user instead of deleting the user.

1. In Administrator, select **Users**.
2. In the row that contains the user whom you want to delete, click **Actions** and select **Delete**.
3. If the user is the owner of any scheduled tasks or taskflows, Administrator prompts you to reassign the jobs to a different user. Select the user to whom you want to reassign the jobs and click **Reassign and Delete**.

   Note: When you use a file listener in Mass Ingestion Files (as a trigger or as a source) and in taskflow (as a trigger or as a file watch) you must reassign the ownership of the file listener association from one user to another using REST API before you delete a user. For more information, see *REST API Reference* guide.

If the user did not own scheduled tasks or taskflows, Administrator deletes the user. If the user was the owner of any scheduled tasks or taskflows, Administrator reassigns the jobs and then deletes the user.

CHAPTER 5

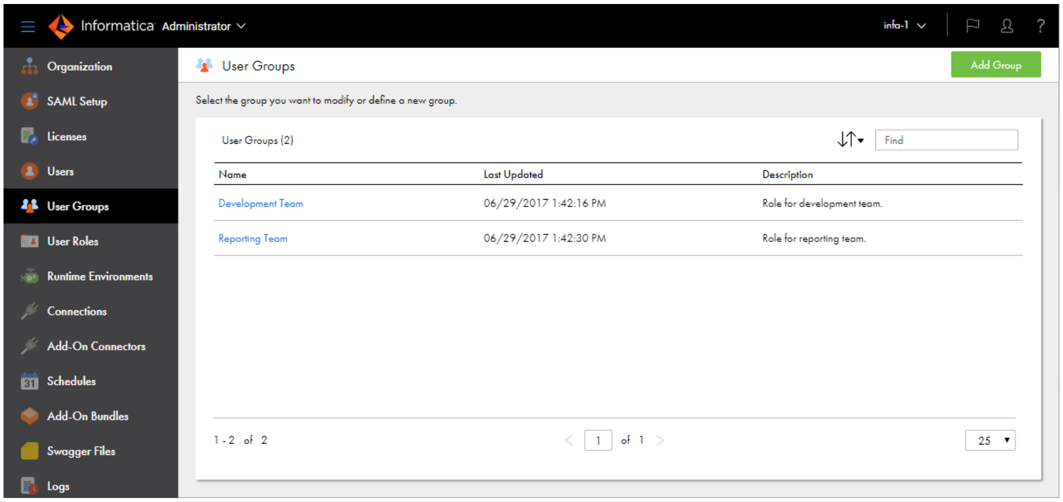
User groups

A user group is a group of users in which all members can perform the same tasks and have the same access rights for different types of assets. Members of a group can perform tasks and access assets based on the roles that you assign to the group.

Administrators can configure user groups for the organization.

The **User Groups** page displays a list of all user groups in the organization. To access the **User Groups** page, in Administrator, select **User Groups**.

The following image shows the **User Groups** page:



User Groups

Select the group you want to modify or define a new group.

User Groups (2)

Name	Last Updated	Description
Development Team	06/29/2017 1:42:16 PM	Role for development team.
Reporting Team	06/29/2017 1:42:30 PM	Role for reporting team.

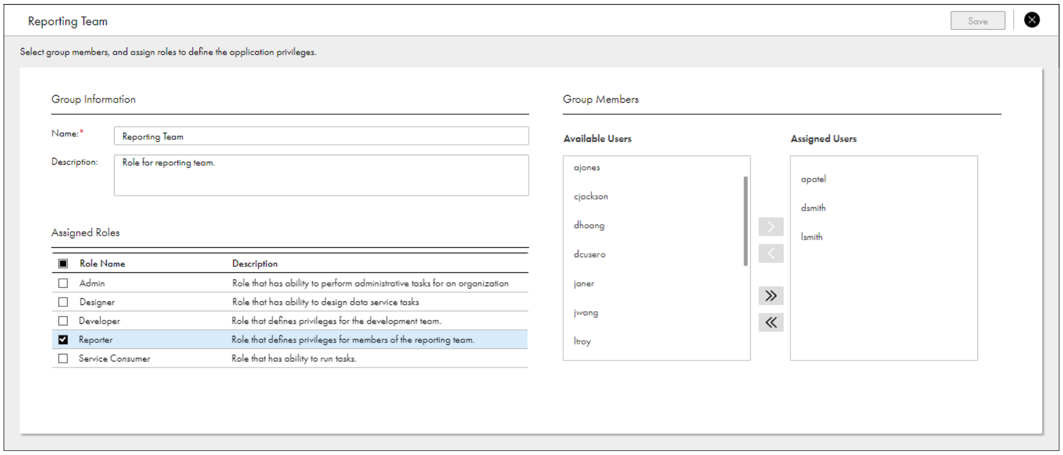
You can perform the following tasks for a user group:

- View and edit group details.
- Create a group.
- Rename a group.
- Delete a group.

User group details

You can configure details about a user group that include the group information, assigned roles, and group members on the group details page. To display the group details page, in Administrator, click **User Groups**, and then click the group name.

The following image shows the group details page:



Reporting Team

Select group members, and assign roles to define the application privileges.

Group Information

Name:* Reporting Team

Description: Role for reporting team.

Assigned Roles

■	Role Name	Description
□	Admin	Role that has ability to perform administrative tasks for an organization
□	Designer	Role that has ability to design data service tasks
□	Developer	Role that defines privileges for the development team.
☑	Reporter	Role that defines privileges for members of the reporting team.
□	Service Consumer	Role that has ability to run tasks.

Group Members

Available Users	Assigned Users
ajones	apatel
cjackson	dsmith
dhoang	lsmith
dcusero	
joner	
jwang	
ltroy	

You can configure the following details for a user group:

Property	Description
Name	Required. Name of the user group. Must be unique within an organization. You can change the group name after you create it.
Description	Optional description for the user group.
Assigned roles	Roles that are assigned to all members of the group. You must assign at least one role to each group. To assign or remove a role, enable or disable the role, and then click **Save**.
Group members	Users who are assigned to the group. To assign a user to the group, move the user from the **Available Users** list to the **Assigned Users** list, and then click **Save**. To remove a user from the group, move the user from the **Assigned Users** list to the **Available Users** list, and then click **Save**. When you assign a user to a group, the user is automatically assigned all roles that are assigned to the group.

Note: You cannot edit group details for a SAML group. SAML groups are identified with the label **Mirrors the SAML group: <group name>** in the Group Information area.

Creating a user group

Create a user group when multiple users in your organization need to perform the same tasks and need the same access rights for different types of assets. Group members can perform tasks and access assets based on the roles that you assign to the group. Create a user group on the **User Groups** page.

1. In Administrator, select **User Groups**.
2. Click **Add Group**.
3. Enter a group name and optional description.

   The group name must be unique within an organization.
4. In the Assigned Roles section, select the roles that you want to assign to the group.

   You can assign system-defined and custom roles to a group. The roles apply to all members of the group.
5. Optionally, assign users to the group.

   To assign a user to the group, move the user from the **Available Users** list to the **Assigned Users** list. The list of available users does not include SAML users because you cannot assign SAML users to a group.

   You can also assign a user to a group when you create or edit a user.
6. Click **Save**.

Renaming a user group

Rename a user group on the **User Groups** page. You can also edit the user group and change the group name on the Group Details page. You cannot rename a SAML group.

1. In Administrator, select **User Groups**.
2. In the row that contains the user group, click **Actions** and select **Rename**.
3. Enter the new name and click **Save**.

Deleting a user group

Delete a user group on the **User Groups** page. You cannot delete a SAML group if your organization uses SAML SSO for authentication and authorization.

Tip: Before you delete a user group, verify that all group members have appropriate roles or are assigned to other groups so that they can continue to use Informatica Intelligent Cloud Services without interruption.

1. In Administrator, select **User Groups**.
2. In the row that contains the user group, click **Actions** and select **Delete**.

CHAPTER 6

User roles

A role is a collection of privileges that you can assign to users and groups. To ensure that every user can access assets and perform tasks in your organization, assign at least one role to each user or user group.

A role defines the privileges for different types of assets and service features. For example, users with the Designer role can create, read, update, delete, and set permissions on most types of data integration assets. However, they have no access to certain Administrator service features such as sub-organizations and audit logs.

Administrators can configure and assign roles for the organization.

You can assign the following types of roles:

System-defined

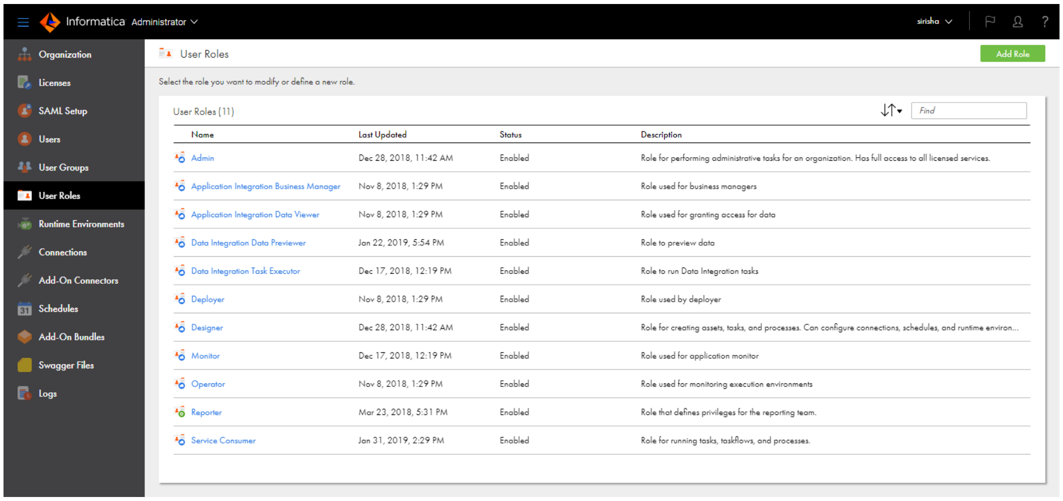
System-defined roles are pre-defined roles that define access privileges for the services that your organization uses. The system-defined roles that you can assign to users and groups vary based on your organization's licenses. You cannot edit, rename, or delete system-defined roles. You can clone system-defined roles except for the Admin role.

Custom roles

Custom roles are roles that you create to set privileges individually. To create custom roles, you need the appropriate license. You can edit, clone, rename, and delete custom roles.

You can view both system-defined and custom roles on the **User Roles** page. The **User Roles** page displays a list of all roles in the organization. To access the **User Roles** page, in Administrator, select **User Roles**.

The following image shows the **User Roles** page:



Select the role you want to modify or define a new role.

User Roles (11)

Name	Last Updated	Status	Description
Admin	Dec 28, 2018, 11:42 AM	Enabled	Role for performing administrative tasks for an organization. Has full access to all licensed services.
Application Integration Business Manager	Nov 8, 2018, 1:29 PM	Enabled	Role used for business managers
Application Integration Data Viewer	Nov 8, 2018, 1:29 PM	Enabled	Role used for granting access for data
Data Integration Data Previewer	Jan 22, 2019, 5:54 PM	Enabled	Role to preview data
Data Integration Task Executor	Dec 17, 2018, 12:19 PM	Enabled	Role to run Data Integration tasks
Deployer	Nov 8, 2018, 1:29 PM	Enabled	Role used by deployer
Designer	Dec 28, 2018, 11:42 AM	Enabled	Role for creating assets, tasks, and processes. Can configure connections, schedules, and runtime environ...
Monitor	Dec 17, 2018, 12:19 PM	Enabled	Role used for application monitor
Operator	Nov 8, 2018, 1:29 PM	Enabled	Role used for monitoring execution environments
Reporter	Mar 23, 2018, 5:31 PM	Enabled	Role that defines privileges for the reporting team.
Service Consumer	Jan 31, 2019, 2:29 PM	Enabled	Role for running tasks, taskflows, and processes.

The Status column indicates whether the role is enabled or disabled for your organization. A role is disabled when the license expires.

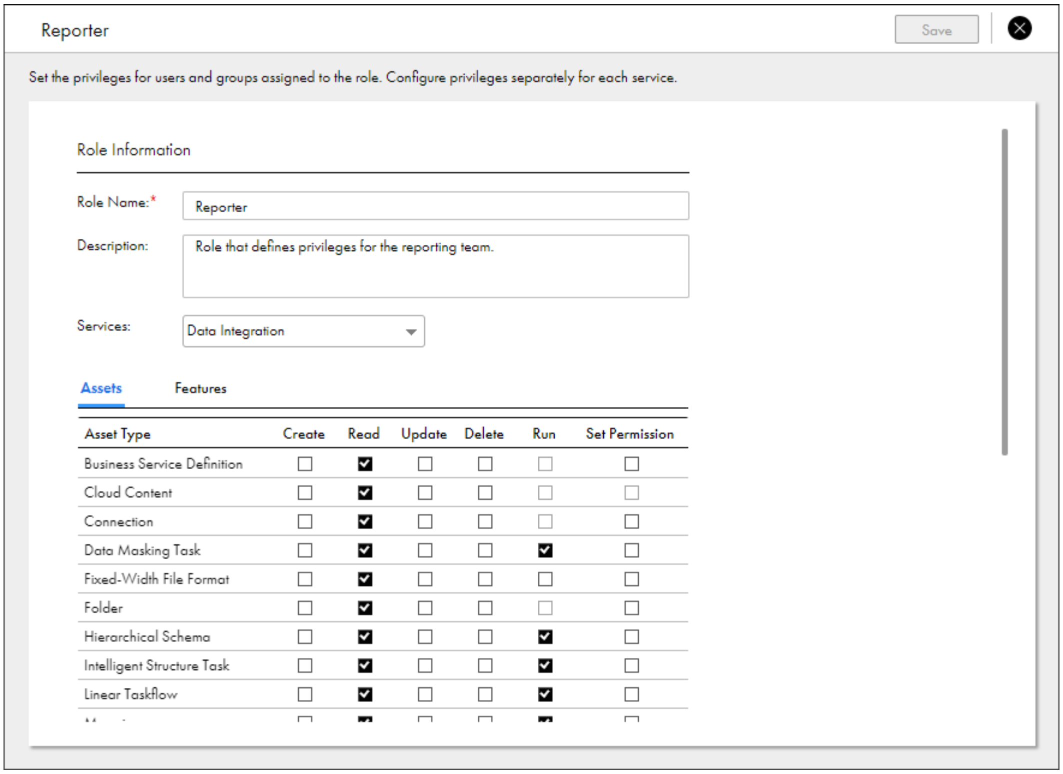
You can assign multiple roles to a user or user group. When you assign multiple roles, the user or group inherits the access privileges associated with all of the roles.

Role details

The role details page displays information about a role, including the asset and feature privileges that are associated with the role. For system-defined roles, you can view the role information and privileges. For custom roles, you can view and change the role information and the assigned asset and feature privileges.

To display the role details page, in Administrator, select **User Roles**, and then click the role name.

The following image shows the role details page:



Set the privileges for users and groups assigned to the role. Configure privileges separately for each service.

Role Information

Role Name:* Reporter

Description: Role that defines privileges for the reporting team.

Services: Data Integration

Asset Type	Create	Read	Update	Delete	Run	Set Permission
Business Service Definition	□	☑	□	□	□	□
Cloud Content	□	☑	□	□	□	□
Connection	□	☑	□	□	□	□
Data Masking Task	□	☑	□	□	☑	□
Fixed-Width File Format	□	☑	□	□	□	□
Folder	□	☑	□	□	□	□
Hierarchical Schema	□	☑	□	□	☑	□
Intelligent Structure Task	□	☑	□	□	☑	□
Linear Taskflow	□	☑	□	□	☑	□

Each role has the following properties:

Role name

Name of the role. For custom roles, you can change the role name.

Description

Role description. For custom roles, you can change the role description.

Services

Name of the service for which privileges are enabled or disabled. Select a service to view the asset and feature privileges that are associated with the service.

If the license for a service expires, the service is marked as disabled. You can view the asset and feature privileges that are associated with a disabled service.

Assets

Asset privileges for the selected service. Asset privileges control access to different types of assets. For example, users with the Service Consumer role can view and run mappings in Data Integration, but they cannot create, update, delete, or set permissions on mappings.

The following table describes the asset privileges:

Privilege	Description
Create	Create assets of the selected type. For Secure Agents, this privilege allows users to download and install the Secure Agent. Requires the Read and Update privileges, which are automatically granted.
Read	Open assets of the selected type. For tasks, this privilege also allows users to use a connection or schedule in the task.
Update	Edit assets of the selected type. Requires the Read privilege, which is automatically granted.
Delete	Delete assets of the selected type.
Run	Run assets of the selected type. For the Data Integration service, users can run mappings, tasks, or taskflows. Users can also monitor, stop, and restart instances of the mapping, task, or taskflow. For the Hub Integration service, users can run publications or subscriptions.
Set permission	Configure permissions for assets of the selected type. For example, if you grant this privilege for projects, users with the role can select a project and enable other users and groups to read, update, delete, or change permissions for the selected project. To configure this privilege, your organization must have the appropriate license.

If a privilege does not apply to an asset type, the privilege is disabled. For example, the run privilege is disabled for folders.

For custom roles, you can enable and disable the asset privileges for a service as long as the service is not disabled.

Features

Feature privileges for the selected service. Feature privileges are general privileges that control the ability to use the features of a service. For example, users with the Designer role have the ability to perform data catalog discovery in Data Integration but not to preview data.

For custom roles, you can enable and disable feature privileges for a service as long as the service is not disabled.

Application Integration feature privileges

Use Application Integration feature privileges to create custom roles.

Important: You must assign the Folder and Project asset privileges to the user's role. To do this, select the Data Integration service and then select the CRUD options for the folder and project assets.

You can enable the following Application Integration feature privileges when you create a custom role:

Administration

Assign the Administration privilege to a role when you want the user to have complete design-time and run-time administrative access to the Application Integration and Application Integration Console.

Users with the Administration privilege can perform the following tasks:

- View, create, update, and delete all Application Integration assets.
- Manage and invoke services.
- Stop running processes.
- View instances and logs for deployed process.
- Deploy Process Developer BPR files to the Application Integration Console.
- Manage deployed catalogs.
- View WSDL files deployed across multiple systems.
- View Process Server metrics.
- Activate and deactivate process APIs.
- View, start, and stop event sources in listener-based connections.

Note: The Application Integration Administration privilege does not give the user Informatica Intelligent Cloud Services-wide administrator privileges. For example, a user with the only the Application Integration Administration privilege will be unable to create sub-organizations.

Console Administration

Assign the Console Administration privilege to a role when you want the user to have near-complete access to the Application Integration Console.

Users with the Console Administration privilege can perform the following tasks:

- View instances for deployed process.
- Stop running processes.
- View deployed Process Developer BPRs and catalogs.
- View WSDL files deployed across multiple systems.
- View Process Server metrics.
- Activate and deactivate process APIs.
- View, start, and stop event sources in listener-based connections.

Users with the Console Administration privilege cannot deploy BPR files.

Data Viewer

Assign the Data Viewer privilege to a user who needs to access detailed logs in the Application Integration Console.

For example, you could assign this privilege to a someone who needs to see all logs across the organization. You would not normally assign this role to a developer.

Note: The process logging level must be set to verbose to get detailed logs.

Development

Assign the Development privilege to developers who will occasionally need to debug processes.

Users with the Development privilege can perform the following tasks:

- View, create, update, and delete all Application Integration assets.
- Invoke services.

- View the Detailed Process Instance page on the Application Integration Console.
- Manage processes instances.
- Activate and deactivate process APIs.
- View, start, and stop event sources in listener-based connections.

Monitoring

Assign the Monitoring privilege to a user who needs to view all parts of the Application Integration Console except for detailed logs.

Users with the Monitoring privilege can perform the following tasks:

- Activate and deactivate process APIs.
- View, start, and stop event sources in listener-based connections.

Publish Application Integration Assets

Assign the Publish Application Integration Assets privilege to a user that needs to be able to publish Application Integration processes, guides, connections, or service connectors.

View Application Integration Console

Assign the View Application Integration Console privilege to a user who needs access to the Application Integration Console service. You must assign this privilege to any role that has privileges that include working on the Application Integration Console.

For example, you need to assign this privilege along with the Development privilege.

View Application Integration Designer

Assign the View Application Integration Designer privilege to a user who needs access to the Application Integration service. You must assign this privilege to any role that has privileges that include working on the Application Integration Console.

For example, you need to assign this privilege along with the Publish Application Integration Assets privilege.

Data Quality feature privileges

Use Data Quality feature privileges to grant users access to the preview functionality in data quality assets. You can enable the feature privileges when you create a custom role.

You can enable the following feature privileges for Data Quality:

Data Preview - Dictionaries

Enable the Data Preview - Dictionaries privilege on a role to enable a user to view the contents of a dictionary in the following cases:

- The user opens the dictionary from the Explore page.
- The user selects the dictionary in a Data Quality asset.

Data Preview - Test Panel

Enable the Data Preview - Test panel privilege on a role to enable a user to view data in the Test panel in a Data Quality asset.

Exceptions Data - Delete

Enable the Exceptions Data - Delete privilege on a role to enable a user to delete the exception data associated with an exception management job from the exception data store. Find the exception management job on the **My Jobs** page in Data Quality, Data Profiling, or Data Integration.

Exceptions Data - View

Enable the Exceptions Data - View privilege on a role to enable a user to download the exception records that an exception management job identifies. Find the exception management job on the **My Jobs** page in Data Quality, Data Profiling, or Data Integration.

The Data Quality feature privileges are enabled by default on the Administrator and Designer roles.

Note: The Data Preview - Dictionaries feature privilege and the Read privilege for dictionary assets work independently of each other. The Read privilege allows you to open the dictionary from the Explore page. The Data Preview - Dictionaries privilege allows you to view the dictionary data.

If you open a dictionary without the Data Preview - Dictionaries privilege, Data Quality displays a message to notify you that you do not have sufficient permissions to view the data.

Mass Ingestion Databases asset and feature privileges

To create, view, or edit database ingestion tasks, assign a user role that includes the following minimum required asset privileges:

- For Mass Ingestion service, select the Create, Read, and Update privileges for the Database Ingestion Task asset.
- For Administrator service, select the Read privilege for the following asset types:
  - Connection
  - Secure Agent Group

  Also, enable the Connectors - view feature.

You can use a system-defined role such as Admin or Designer that includes these privileges, or you can define a custom role that includes them.

Human Task asset privileges

Use the human task asset feature privileges to allow users access to specific functionality while working with human task assets. You can enable the feature privileges when you create a custom role.

To access human task assets, you can assign a user role that includes the following asset privileges on the **New Role** > **Role Information** > **Asset** tab:

- **Create**. To create a human task asset. When you select the **Create** option, the **Read** and **Update** options are set to enabled automatically.
- **Read**. To view human tasks on the **Explore** page of Application Integration.
- **Update**. To edit a human task asset. When you select the **Update** option, the **Read** option is set to enabled automatically.
- **Delete**. To delete a human task asset.
- **Run**. To run a process that contains a Human Task step which in turn generates the human task.
- **Set Permissions.**To assign permissions to other user roles to access human task assets.

On the **New Role** > **Role Information** > **Features** tab, select the **View Human Task Application** option to allow a user role to view and access tasks in the Human Task Inbox.

System-defined roles

Informatica Intelligent Cloud Services provides system-defined roles that you can assign to users or user groups. You cannot change or delete the system-defined roles.

The system-defined roles that you can assign to users and groups vary based on your organization's licenses. For example, if your organization has no access to Application Integration or API Manager, you cannot assign the Deployer, Application Integration Business Manager, Application Integration Data Viewer, or Operator role to any user or group in your organization.

Assign system-defined roles to users and groups based on the tasks that they need to perform.

There are two types of system-defined roles:

- Cross-service roles define access privileges across multiple services.
- Service-specific roles define access privileges for one service or for a group of closely related services.

Cross-service roles

Cross-service roles are system-defined roles that define access privileges across multiple services.

For example, users with the Designer role can create assets and tasks in Data Integration, create assets in Cloud Integration Hub, create processes in Application Integration, and can also access the Application Integration Console. Users with the Monitor role can monitor Data Integration jobs, Cloud Integration Hub assets, and Application Integration process instances.

The following roles are cross-service roles:

- Admin
- Data Integration Data Previewer
- Deployer
- Designer
- Monitor
- Operator
- Service Consumer

Note: The Data Integration Data Previewer role is a supplemental role that allows users to preview data in Data Integration and Data Profiling. It provides no access to services. Assign this role with another role that allows users to access Data Integration or Data Profiling.

The following table shows the services that each cross-service role can access:

Service	Roles
Administrator	- Admin - Designer - Monitor - Service Consumer
API Manager	- Admin - Designer - Service Consumer
API Portal	- Admin - Service Consumer

Service	Roles
Application Integration	- Admin - Deployer - Designer - Monitor - Operator - Service Consumer
Application Integration Console	- Admin - Deployer - Designer - Monitor - Operator - Service Consumer
B2B Gateway	- Admin - Designer - Monitor
B2B Partners Portal	- Admin
Business 360 Console	- Admin - Designer
Data Integration	- Admin - Designer - Monitor - Service Consumer
Data Quality	- Admin - Deployer - Designer - Monitor - Operator - Service Consumer
Data Profiling	- Admin - Designer - Monitor - Operator
Integration Hub	- Admin - Designer - Monitor
Mass Ingestion	- Admin - Deployer - Designer - Monitor
Model Serve	- Admin - Designer - Monitor - Operator

Service	Roles
Monitor	- Admin - Designer - Monitor
Operational Insights	- Admin - Operator

Access privileges for cross-service roles

Assign cross-service roles to users who need access privileges for different services across Informatica Intelligent Cloud Services. Each cross-service role provides different access privileges.

Cross-service roles have the following access privileges:

Admin

Users with the Admin role have full access to all licensed services except for the following privileges:

- Admin users do not have privileges for OAuth 2.0 client management in API Manager. To provide full access to the API Manager service, including full privileges for OAuth 2.0 client management, assign the user both the Admin and Service Consumer roles.
- Admin users cannot enable and disable the use of customer managed encryption keys for the organization. To allow this, assign the user both the Admin and Key Admin roles.

The best practice is to assign the Admin role to one or two trusted users and assign the users to an administrative user group that has full permissions on all asset types. These users can act as alternative organization administrators and can help troubleshoot access control and other organization security issues.

Data Integration Data Previewer

Users with the Data Integration Data Previewer role can preview data when they select a source, target, or lookup object for use in a mapping or task in Data Integration. They can also view source object data when creating a profile or viewing profile results in Data Profiling.

The Data Integration Data Previewer role is a supplemental role. Assign this role with another role, such as the Designer role, to ensure that users can access Data Integration and Data Profiling.

Mass Ingestion service does not use the Data Integration Data Previewer role.

Deployer

Users with the Deployer role can deploy Application Integration assets and manage APIs through API Manager. Assign this role in a production environment where deployment access is typically restricted.

Note: To provide full access to the API Manager service, including full privileges for OAuth 2.0 client management, assign the user both the Deployer and Service Consumer roles.

In Data Quality, users with the Deployer privilege can view assets.

In Mass Ingestion service, users with the Deployer role can view application ingestion, database ingestion, and streaming ingestion tasks.

The following table lists the services that users with the Deployer role can access and the access privileges associated with each service:

Service	Access Privileges
API Manager	Has full access to this service, including OAuth 2.0 client management privileges, when the Service Consumer role is also assigned.
Application Integration	Can view asset details.
Application Integration Console	Can deploy assets and view settings on the Processes, Logs, Server Configuration, Deployed Assets, and Resources pages. Can upload and deploy Process Developer-generated orchestration artifacts (BPRs).
Data Quality	Can view asset details.
Mass Ingestion	Can view application ingestion, database ingestion, and streaming ingestion tasks.

Designer

Users with the Designer role can create assets, tasks, and processes. They can configure connections, schedules, and runtime environments. They can also monitor jobs and advanced clusters for the organization.

Note: Mass Ingestion users with the Designer role cannot monitor advanced clusters.

The following table lists the services that users with the Designer role can access and the access privileges associated with each service:

Service	Access Privileges
Administrator	Can configure connections, runtime environments, schedules, swagger files, and advanced configurations. Can install add-on connectors and install and uninstall add-on bundles. Can view upgrade settings for Secure Agent services. Can start and stop file servers, configure proxy servers, and view other file server settings.
Application Integration	Has full access to this service.
Application Integration Console	Can view and edit all settings except for server configuration properties.
B2B Gateway	Has full access to this service.
Data Integration	Has full access to this service.
Data Quality	Has full access to this service.
Data Profiling	Has full access to this service.
Integration Hub	Has full access to this service.
Mass Ingestion	Can create, view, edit, delete, run, and set permissions on application ingestion, database ingestion, and streaming ingestion tasks.

Service	Access Privileges
Model Serve	Can create, view, edit, and delete machine learning models. Can create, view, edit, delete, and run model deployments.
Monitor	Has full access to this service.

Monitor

Users with the Monitor role can monitor Data Integration jobs, Mass Ingestion jobs, Cloud Integration Hub assets, Data Quality assets, Model Serve assets, and Application Integration process instances for the organization.

The following table lists the services that users with the Monitor role can access and the access privileges associated with each service:

Service	Access Privileges
Administrator	Can view schedules and upgrade settings for Secure Agent services. Can start and stop file servers, configure proxy servers, and view other file server settings.
Application Integration	Can view asset details.
Application Integration Console	Can view settings.
B2B Gateway	Can view asset details.
Data Integration	Can view asset details.
Data Quality	Can view asset details.
Data Profiling	Can view asset details.
Integration Hub	Can view asset details.
Mass Ingestion	Can view application ingestion, database ingestion, and streaming ingestion jobs and job details.
Model Serve	Can view asset details.
Monitor	Can view data integration jobs and job details. Cannot view export or import jobs.

Operator

An Operator is responsible for process execution management and Process Server configuration updates. Users with the Operator role can view asset details but cannot modify them. They can manage process instances and modify some operational server parameters.

The following table lists the services that users with the Operator role can access and the access privileges associated with each service:

Service	Access Privileges
Application Integration	Can view asset details.
Application Integration Console	Can view and edit Process Server settings and some Cloud Server settings. For example, a user with the Operator role can create an alert service, but cannot view tenant details.
Data Profiling	Can view asset details.
Data Quality	Can view asset details.
Model Serve	Can view asset details.
Operational Insights	Can view cloud and domain infrastructure. Can edit domain and infrastructure Secure Agent alert settings. Can edit domain infrastructure, including registering domains.

Mass Ingestion service does not use the Operator role.

Service Consumer

Users with the Service Consumer role can run tasks, taskflows, and processes but they cannot create or edit assets. Assign this role to users who need to execute Data Integration jobs and Application Integration processes through APIs.

Note: To provide full access to the API Manager service, assign the user both the Service Consumer and Deployer roles, or assign the user both the Service Consumer and Admin roles.

The following table lists the services that users with the Service Consumer role can access and the access privileges associated with each service:

Service	Access Privileges
Administrator	Can view schedules, swagger files, and upgrade settings for Secure Agent services. Can start and stop file servers, configure proxy servers, and view other file server settings.
API Manager	Has full access to this service when the Deployer or the Admin role is also assigned.
API Portal	Has full access to this service.
Application Integration	Can invoke Application Integration processes.
Data Integration	Can view tasks, run tasks, test-run mappings, run taskflows, and download workflow XML.
Data Quality	Can view asset details.

Mass Ingestion service does not use the Service Consumer role.

Service-specific roles

Service-specific roles are system-defined roles that define access privileges for one service or for a group of closely related services. For example, the service-specific roles for Application Integration provide access to both Application Integration and Application Integration Console.

Assign service-specific roles to users who do not need access across multiple services. Service-specific roles have different access privileges based on the services to which they apply.

The following table lists the service-specific roles for each service that uses them:

Service	Service-Specific Roles
Administrator	Key Admin
Application Integration	Application Integration Business Manager Application Integration Data Viewer
Business 360 Console	MDM Designer
Customer 360	Customer 360 Analyst Customer 360 Manager Customer 360 Data Steward MDM Business User
Data Integration	Data Integration Task Executor
Model Serve	Model Serve Admin Model Serve Predictions User Model Serve System Role
Product 360	Product 360 Read-Only Product 360 Manager
MDM - Reference 360	Reference 360 Administrator Reference 360 Business Analyst Reference 360 Business Steward Reference 360 Planner Reference 360 Primary Owner Reference 360 Stakeholder
Supplier 360	Supplier 360 Read Only Supplier 360 Analyst Supplier 360 Data Steward Supplier 360 Task Admin Supplier 360 Risk Manager Supplier 360 Contract Manager Supplier 360 Credit Manager Supplier 360 Commodity Manager

Access privileges for Administrator roles

Users with the Key Admin role can enable and disable the use of customer managed encryption keys for their organization in Administrator.

Note: The Key Admin role is a supplemental role that allows users to enable and disable the use of customer managed encryption keys. It provides no access to services.

Assign the Key Admin role to a user that also has the Admin role. When a user has both roles, they can enable and disable the use of customer managed keys on the **Security** tab of the **Settings** page. If they don't have both roles, they can't see the **Security** tab.

For more information about customer managed encryption keys, see *Organization Administration*.

Access privileges for Application Integration roles

Assign Application Integration roles to users who need access privileges for Application Integration and Application Integration Console. Each role provides different access privileges.

The following service-specific roles define access privileges for Application Integration and Application Integration Console:

Application Integration Business Manager

An Application Integration Business Manager monitors business activity. Users with the Application Integration Business Manager role can view information about assets and process instances, but they cannot change them.

The following table lists the services that users with the Application Integration Business Manager role can access and the access privileges associated with each service:

Service	Access Privileges
Application Integration	Can view folder and asset lists and asset details.
Application Integration Console	Can access the following page: - Processes - APIs - Connections

Application Integration Data Viewer

Users with the Application Integration Data Viewer role can view detailed logs in the Application Integration Console service.

Note: The logging level of an artifact must be set to verbose for a user to view detailed logs.

The Application Integration Data Viewer role is a supplemental role. Assign this role along with at least one other role. For example, if you want a user with the Designer role to view detailed Process Server logs, assign the user the Application Integration Data Viewer and the Designer roles, and set the Process Server logging level to verbose.

Access privileges for Business 360 Console roles

Assign Business 360 Console roles to the users who need access privileges for Business 360 Console.

The following service-specific role defines access privileges for Business 360 Console:

MDM Designer

Users with the MDM Designer role can define reference data in Business 360 Console.

Access privileges for Customer 360 roles

Assign Customer 360 roles to the users who need access privileges for Customer 360. Each role provides different access privileges.

The following service-specific roles define access privileges for Customer 360:

Customer 360 Analyst

Users with the Customer 360 Analyst role can create and edit records in Customer 360. When a Customer 360 Analyst creates or edits a record, the changes trigger a review process that requires approval from a Customer 360 Manager.

Customer 360 Manager

Users with the Customer 360 Manager role can review and approve customer records or update customer records. They can also create or edit records without approval. Managers can also create and update hierarchies.

Customer 360 Data Steward

Users with the Customer 360 Data Steward role can perform any task in Customer 360. They can create and edit records without approval, run jobs, and review and approve customer records.Data Stewards can also create and update hierarchies.

MDM Business User

Users with the MDM Business User role can view records in Customer 360. They cannot create or edit records in Customer 360.

Access privileges for Data Integration roles

The Data Integration Task Executor role defines access privileges for Data Integration. Users with the Data Integration Task Executor role can run tasks and taskflows and test-run mappings in Data Integration. They can also monitor data integration jobs.

The following table lists the services that users with the Data Integration Task Executor role can access and the access privileges associated with each service:

Service	Access Privileges
Administrator	Can view schedules and upgrade settings for Secure Agent services. Can start and stop file servers, configure proxy servers, and view other file server settings.
Data Integration	Can view assets and asset details, run tasks and taskflows, and test-run mappings. Can view user's own data integration jobs and job details, start and stop user's own jobs, and download session logs. Cannot view export or import jobs.
Monitor	Can view data integration jobs and job details, start and stop data integration jobs, and download session logs. Cannot view export or import jobs.

Access privileges for Model Serve roles

Assign Model Serve roles to users who need access privileges for Model Serve. Each role provides different access privileges.

The following service-specific roles define access privileges for Model Serve:

Model Serve Admin

Users with the Model Serve Admin role can assign permissions for other Model Serve users, and they can register and deploy machine learning models.

Model Serve Predictions User

Users with the Model Serve Predictions User role can generate predictions from a deployed machine learning model. They can view model deployment assets, but they cannot make changes to the assets.

Model Serve System Role

This role assigns necessary permissions to the Model Serve system user, so the system user can perform tasks such as provisioning resources for model deployments. For more information about the Model Serve system user, see Chapter 4, “Users” on page 22.

Access privileges for Product 360 roles

Assign Product 360 roles to the users who need access privileges for Product 360 SaaS. Each role provides different access privileges.

The following service-specific roles define access privileges for Product 360:

Product 360 Read-Only

Users with the Product 360 Read-Only role can view records in Product 360. They can't create or edit records in Product 360.

Product 360 Manager

Users with the Product 360 Manager role can review and approve records. They can also create, edit, or delete records without approval.

Access privileges for Reference 360 roles

Assign Reference 360 roles to users who need access privileges for MDM - Reference 360. Each role provides different access privileges.

The following service-specific roles define access privileges for Reference 360:

Reference 360 Administrator

Users with the Reference 360 Administrator role configure the Reference 360 environment.

Reference 360 Business Analyst

Users with the Reference 360 Business Analyst role view and analyze Reference 360 assets. They cannot propose changes to assets.

Reference 360 Business Steward

Users with the Reference 360 Business Steward role are subject matter experts for reference data. They create and manage code values in code lists and value mappings in crosswalks. They are responsible for approving changes proposed by other users. They can send their own changes for approval or directly publish their changes without approval. They can assign users access to crosswalks.

Reference 360 Planner

Users with the Reference 360 Planner role create and manage hierarchies. They assign users access to hierarchies.

Reference 360 Primary Owner

Users with the Reference 360 Primary Owner role create and define reference data structures, such as reference data sets and code lists. They can delete code lists and propose changes to code values in code lists. The user with the Business Steward role must approve the proposed changes. Primary owners can also assign users access to code lists and reference data sets.

Reference 360 Stakeholder

Users with the Reference 360 Stakeholder role propose changes to code values. The user with the Business Steward role must approve the proposed changes.

For more information about these roles, see the MDM - Reference 360 help.

Access privileges for Supplier 360 roles

Assign Supplier 360 roles to the users who need access privileges for Supplier 360 SaaS. Each role provides different access privileges.

The following service-specific roles define access privileges for Supplier 360:

Supplier 360 Read Only

Users with the Supplier 360 Read Only role can view records in Supplier 360. They can't create or edit records in Supplier 360.

Supplier 360 Analyst

Users with the Supplier 360 Analyst role can create, read, edit, and delete records in Supplier 360. When a Supplier 360 Analyst creates or edits a record, the changes trigger a review process that requires approval from a Supplier 360 manager.

Supplier 360 Data Steward

Users with the Supplier 360 Data Steward role can create, edit, and delete records without approval, run jobs, review and approve records, and match, merge, and unmerge records.

Supplier 360 Task Admin

Users with the Supplier 360 Task Admin role can view all unclaimed evaluation tasks and assign or release evaluation tasks. They also have the originator and approver privileges.

Supplier 360 Risk Manager

Users with the Supplier 360 Risk Manager role can claim and disclaim risk evaluation tasks and act on the risk evaluation tasks. They can create, read, edit, and delete records. They also have the originator and approver privileges.

Supplier 360 Contract Manager

Users with the Supplier 360 Contract Manager role can claim and disclaim contract evaluation tasks and act on the contract evaluation tasks in the approval workflow. They can create, read, edit, and delete records. They also have the originator and approver privileges.

Supplier 360 Credit Manager

Users with the Supplier 360 Credit Manager role can claim and disclaim credit evaluation tasks and act on the credit evaluation tasks in the approval workflow. They can create, read, edit, and delete records. They also have the originator and approver privileges.

Supplier 360 Commodity Manager

Users with the Supplier 360 Commodity Manager role can claim and disclaim commodity evaluation tasks and act on the commodity evaluation tasks in the approval workflow. They can create, read, edit, and delete records. They also have the originator and approver privileges.

Custom roles

A custom role is a role that you create based on the needs of your organization. For example, you might want to create a custom administrative role that can configure roles, user groups, and access control, but cannot create, edit, or run data integration tasks.

To create custom roles, your organization must have the appropriate license. You can edit, rename, and delete custom roles after you create them.

You might want to edit custom roles when your organization gets a new license. Edit the roles to grant access to new asset types and features. Informatica Intelligent Cloud Services does not grant additional privileges to custom roles when your organization gets a new license.

Note: Custom roles cannot be assigned privileges to create, update, or delete roles. If you need to modify roles, log in to Informatica Intelligent Cloud Services as a user with the system-defined Admin role.

Creating a custom role

Create a custom role on the **User Roles** page. When you create a role, you must configure the privileges that are associated with the role. You configure privileges separately for each service.

To create a custom role, you can create a new role or clone an existing role. A new role has no privileges until you configure them. A cloned role has the same privileges as the role that you clone, but you can change the privileges.

1. In Administrator, select **User Roles**.
2. Perform either of the following actions:
   - To create a new role, click **Add Role**.
   - To clone an existing role, in the row that contains the role that you want to clone, click **Actions** and select **Clone**. You can clone any role except for the Admin role.
3. Enter a role name and optional description.
4. In the **Services** field, select the service for which you want to configure privileges.

   For example, to configure privileges for Data Integration, select **Data Integration**. To configure administrative privileges, select **Administrator**.
5. To configure the asset privileges, select **Assets**, and enable or disable the appropriate privileges for each asset type.

   For example, to enable users with the role to create folders, enable **Create** next to **Folder**.
6. To configure the feature privileges, select **Features**, and enable or disable the appropriate privileges.

   For example, to prevent users with the role from importing assets, disable **Asset - import**.
7. Repeat steps 4 through 6 for each service.
8. Click **Save**.

Note: If you want to create a user role that can only view, save, or edit a connection, select **Administrator** in the **Services** field, then select the **Features** tab and enable Connectors-view.

After you create a role, you can assign it to a user or user group. To assign the role to a user or group, edit the user or group.

Renaming a role

Rename a role on the **User Roles** page. You can rename a custom role. You cannot rename a system-defined role.

1. In Administrator, select **User Roles**.
2. In the row that contains the role that you want to rename, click **Actions** and select **Rename**.
3. Enter a new name for the role.
4. Click **Save**.

Deleting a role

Delete a role on the **User Roles** page. You cannot delete a custom role if it is assigned to any user or user group. You cannot delete a system-defined role.

1. In Administrator, select **User Roles**.
2. In the row that contains the role that you want to delete, click **Actions** and select **Delete**.

B2B Partners Portal user roles

If your organization uses B2B Gateway, you might want to enable access to B2B Partners Portal for your external trading partners. To give your trading partners access to B2B Partners Portal, create a custom role and assign it to partner users.

When you create a custom role for partner users, name the role so that you know it is for B2B Partners Portal users. For example, you might name the role "B2B Partners Portal User."

Optionally, you can give the role a description. Clearly describe the role so that you know it is for users from partner companies. For example, you might describe the role as "Role for users from partner companies to access the B2B Partners Portal service."

When you create a custom role for B2B Partners Portal users, enable the Partners Portal feature privilege for the B2B Partners Portal service. For more information about creating custom roles, see “Creating a custom role” on page 52.

Assign the custom role to users from your partner companies. You only need to create one role for B2B Partners Portal users. Assign the same role to all external B2B Partners Portal users.

CHAPTER 7

User configuration examples

The following examples illustrate ways in which you can configure users, user groups, and roles to control access to Informatica Intelligent Cloud Services according to your business needs.

You want your development team to create tasks and taskflows in Data Integration. The development team needs to view sample data in development, but you want to restrict access to production data.

1. Create a Developer role for the development team. Configure the role with all privileges for tasks and related assets, but only the Read privilege for connections.
2. Create a Development Team user group and add all members of the development team to the group.
3. Assign the Developer role to the Development Team group.
4. If possible, create development connections to sample data. If you have both development and production connections, configure the production connections so that the Development Team group does not have read permission for these connections. This prevents users in the Development Team group from using production connections in tasks.
5. After testing is complete and tasks are ready to move into production, have an administrator or other qualified user configure the tasks to use production connections.
6. Edit the Developer role and remove the privilege to run tasks. If development is complete for a task type, you can also remove the privileges to read and update the tasks. By removing the read privilege, you prevent users with the Developer role from accessing information about production tasks.

You have a reporting team that needs to run tasks in Data Integration, but does not have the technical knowledge to configure tasks safely.

1. Create a Reporter role for the reporting team. Configure the role with privileges to read and run tasks and taskflows, and privileges to read, create, and update schedules. Do not enable privileges to create, update, delete or set permissions on assets in the organization.
2. Create a Reporting Team user group and add all members of the reporting team to the group.
3. Assign the Reporter role to the Reporting Team group.

You want a security administrator who can assign roles and user groups and configure access control, but cannot create, edit, or run tasks.

1. Create a custom role called Security Administrator.
2. Edit the Security Administrator role and grant all privileges except the privileges to create, update, delete, and run tasks, connections, and schedules.
3. Assign the Security Administrator role to the security administrator.

You want to easily keep track of your organization administrators.

Create a user group called "Organization Administrators" and assign the Admin role to the group. Add all of your organization administrators to the group.

Your organization uses an OrderProcessing API to manage orders to a large supplier. This API consists of processes in Application Integration that include CreateOrder, ApproveOrder, and GetOrder. As an Admin, you want to restrict access to the ApproveOrder process to a few people.

1. Create a custom role called Approver. Configure the Run privilege for Application Integration Assets for the Approver role.
2. Create a user group called Order Approvers.
3. Assign the Approver role to the Order Approvers group.
4. Assign the Service Consumer role to the Order Approvers group. You must do this as the Service Consumer role can access and invoke processes.
5. Assign the users who need to be able to invoke the ApproveOrder process to the Order Approvers group.
6. In the ApproveOrder process, you must configure one of the following fields:
    - To assign access to a group of users, enter the Order Approvers group in the **Allowed Groups** field.
    - To assign access to a specific user, enter the user in the **Allowed Users** field. You can enter more than one user in the field.

Only members of the Order Approvers group or the users specified in the **Allowed Users** field will be able to invoke the ApproveOrder process.

You want an Application Integration developer to be able to perform all functions in the Application Integration Console except for viewing detailed process logs.

1. Create a role called Custom_Dev and configure the role with the following privileges:
    a. Select the Application Integration service, go to the **Assets** tab, and enable all CRUD privileges for **Application Integration Assets**.
    b. Go to the **Features** tab and add the Development, Console Administration, Publish Application Integration Assets, View Application Integration Console, and View Application Integration Designer privileges to the role.
    c. Select the Data Integration service, go to the **Assets** tab, and enable all CRUD privileges for the **Project** and **Folder** assets.
2. Assign the Custom_Dev role to the developer.

CHAPTER 8

Editing your user profile

Your user profile contains the details of your Informatica Intelligent Cloud Services user account.

You can update the following information in your profile:

- First and last name
- Job title
- Email address
- Phone number
- Time zone (used in the job execution time stamps on the **All Jobs**, **Running Jobs**, **My Jobs**, **Import/Export Logs**, and **My Import/Export Logs** pages)
- Password
- Security question and answer

Note: If you use SAML to sign on to Informatica Intelligent Cloud Services and your organization administrator has enabled SAML group and role mapping on the **SAML Setup** page in Administrator, you can only update the time zone. The other attributes are updated directly from your enterprise directory each time you log into Informatica Intelligent Cloud Services.

1. Click the **User** icon in the top right corner of the Informatica Intelligent Cloud Services window and then select **Profile**.
2. On the **Profile** page, add or edit personal information such as your name, job title, phone number, and time zone.
3. To update your email address, click **Update Email**.

   Informatica Intelligent Cloud Services sends a verification email to your new email address. The email contains a link that is valid for 24 hours. When you click the link in the email, the new address is verified, and it appears in your profile. If the link expires, you can resend the verification email.
4. Optionally, change your password or security question.
5. Click **Save**.

INDEX