Informatica® Intelligent Cloud Services
November 2024

# User Administration

Informatica Intelligent Cloud Services User Administration
November 2024



Publication Date: 2024-11-05

# 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, on the Informatica Intelligent Cloud Services Status page, click **SUBSCRIBE TO UPDATES**. You can 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 Global Support Center through the Informatica Network or by telephone.

To find online support resources on the Informatica Network, click **Contact Support** in the Informatica Intelligent Cloud Services Help menu to go to the **Cloud Support** page. The **Cloud Support** page includes system status information and community discussions. Log in to Informatica Network and click **Need Help** to find additional resources and to contact Informatica Global Customer Support through email.

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 9. For more information about SAML configuration with a third-party identity provider, see Chapter 3, “SAML single sign-on” on page 11. For more information about configuring user accounts directly, see Chapter 4, “Users” on page 24.

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 34.

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 37.

Each user can configure personal information, including their email, password, and time zone, in their user profile. Users can configure notification preferences and source control credentials in their user settings. For more information, see Chapter 8, “Editing your user profile” on page 79 and Chapter 9, “Editing your user settings” on page 80 .

CHAPTER 2

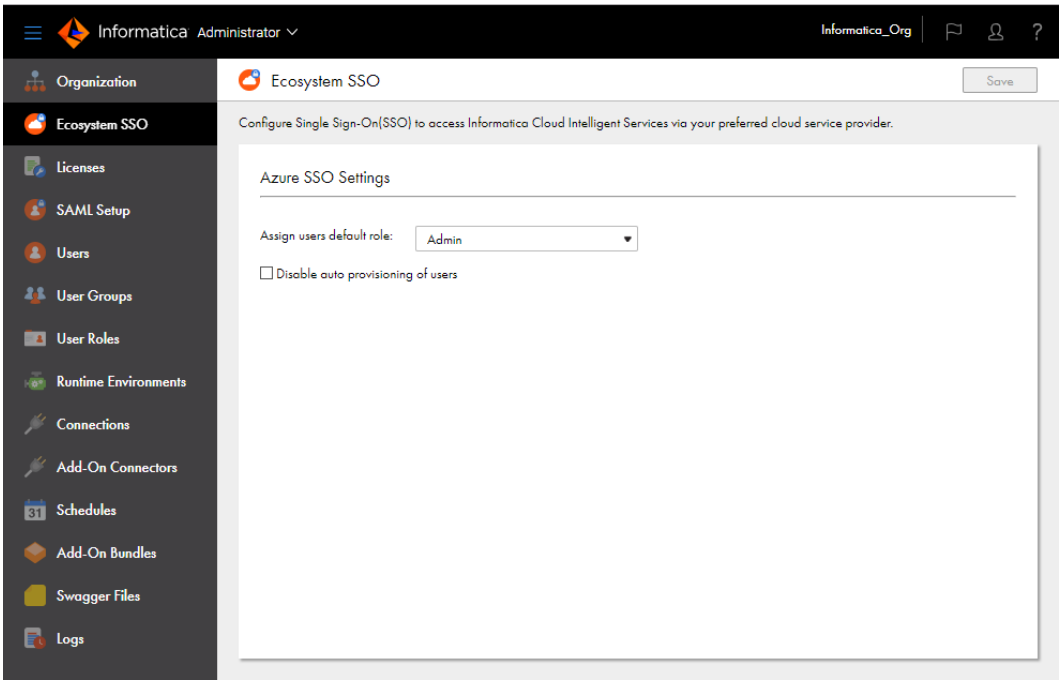
# Ecosystem single sign-on

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 11.

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




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 your organization, 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.

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 a SCIM token which you generate on the **SAML Setup** page.

For information about setting up SCIM 2.0 and creating the provisioning app, see the following 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.

## Managing SCIM tokens

You can create and use up to two SCIM tokens simultaneously. Each token is valid for 180 days from the time of generation. When a token expires, you'll need to generate a new one, even for an existing connection.

As a best practice, create tokens on different days so that they don't expire on the same day. For example, you might want to generate a token on one day and a second token 90 days later. Informatica Intelligent Cloud Services notifies you when a token is about to expire.

**Note:** You can't generate more than two tokens, even if one or both tokens are expired. If your organization uses two tokens and you want to generate a new token, you'll first need to delete one of the existing tokens.

You can also manage SCIM tokens using the scimTokens REST API resource. For more information, see *REST API Reference*.

1. On the **SAML Setup** page in Administrator, click **Manage Token**.

   This option is enabled when you enable the **Enable IdP to push users/groups using SCIM 2.0** option.

   The **SCIM Tokens** dialog box displays the SCIM tokens that have been created for your organization along with the expiration date and status of each token. If two tokens are listed, you'll need to delete one before you can generate a new token.
2. To generate a token, click **Generate Token** and copy the token to the clipboard.

   You'll need this token when you enable SCIM in the provisioning app.
3. To delete a token, click the **Delete** icon for the token you want to delete.

# 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.<br>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.<br>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.<br>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.<br>If you use SCIM 2.0, this option is disabled because users are provisioned by the SCIM client.<br>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.<br>Enable this option to use SAML SSO for both authentication and authorization. Disable this option to use SAML SSO for authentication only.<br>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.<br>When you enable this option, you must generate a bearer token for the identity provider (SCIM client). To generate a token, click **Manage Token**. For more information about generating and managing bearer tokens, see "Managing SCIM tokens" on page 16.<br>**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.<br>When you enable this option, auto-provisioning of users is disabled because users are provisioned through the SCIM client.<br>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.<br>The Issuer value in all messages from the identity provider to Informatica Intelligent Cloud Services must match this value. For example:<br>`<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. |

| Property | Description |
|---|---|
| Signing Certificate | Base64-encoded PEM format identity provider certificate that Informatica Intelligent Cloud Services uses to validate signed SAML messages from the identity provider.<br>**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.<br>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.<br>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.<br>To specify that the name identifier is an email address, the Name Identifier Format is as follows:<br>`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.<br>Informatica Intelligent Cloud Services redirects the logged out user to the landing page in the following ways:<br>- If you specify a logout page URL, Informatica Intelligent Cloud Services redirects the user to this URL after logout.<br>- 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.<br>Default is 180 seconds (3 minutes). |

| Property | Description |
|---|---|
| Name Identifier value represents user's email address | If enabled, Informatica Intelligent Cloud Services uses the name identifier as the email address.<br>Default is enabled. |
| Sign authentication requests | If enabled, Informatica Intelligent Cloud Services signs authentication requests to the identity provider.<br>Default is enabled. |
| Sign logout requests sent using SOAP binding | If enabled, Informatica Intelligent Cloud Services signs logout requests sent to the identity provider.<br>Default is enabled. |
| Encrypt name identifier in logout requests | If enabled, Informatica Intelligent Cloud Services encrypts the name identifier in logout requests.<br>**Note:** Verify that the identity provider supports decryption of name identifiers before you enable this option.<br>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. |
| 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. |

| Property | Description |
|---|---|
| User Roles | SAML attribute used to pass the assigned user roles.<br>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.<br>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.<br>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.<br>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. |
| ID | SCIM attribute used to pass the user id. |
| External ID | SCIM attribute used to pass the user externalId.<br>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.

**Note:** For instruction on how to create a SAML group mapping with Azure Active Directory, see this KB article.

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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.

# OAuth using JSON web tokens

If your organization is configured to use SAML and the organization uses the Informatica Intelligent Cloud Services REST API, users can log in and start a REST API session using a JSON web token (JWT).

Using a JWT access token is similar to using a SAML assertion. However, unlike using SAML assertions, users fetch JWT access tokens from the identity provider and include the tokens in login requests.

Before users can use JWT access tokens, complete the following tasks:

- Configure the organization to use SAML and set up users as SAML users.
- Set up an OAuth identity provider. You can use identity providers such as Azure Active Directory and Okta.
- Set up a method to retrieve JWT access tokens from the identity provider.
- Register the identity provider using the Informatica Intelligent Cloud Services REST API.

To log in, users obtain a JWT access token from the identity provider and include the token in a loginOAuth POST request. The token can be used for one REST API session. If the login request is successful, the response includes a session ID to use in subsequent API calls.

For information about OAuth setup using Azure Active Directory, see the following article:
Set up OAuth with Azure AD

For more information about identity provider configuration, see the identity provider's documentation.

For more information about registering identity providers and logging in using JWT access tokens, see *REST API Reference*.

CHAPTER 4

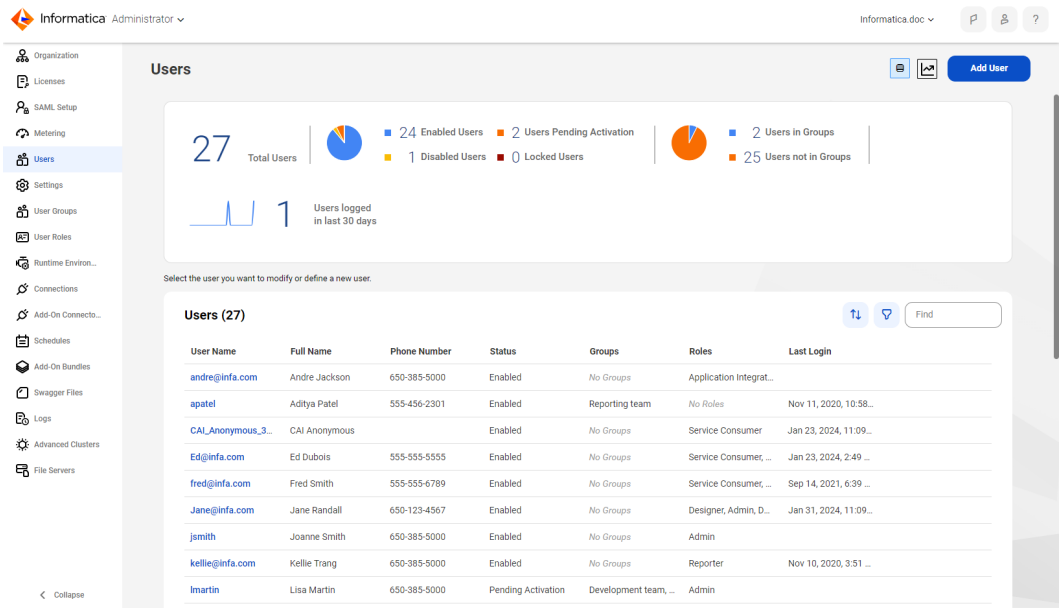
# Users

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:




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 9.

**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 11.

# 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>.

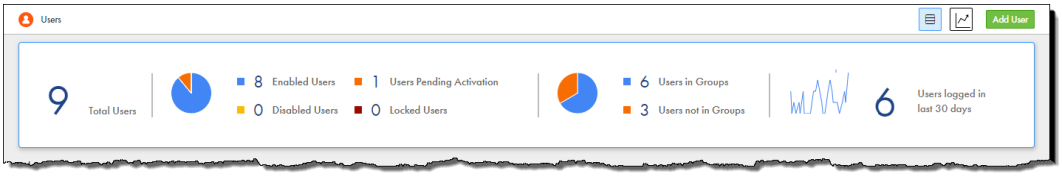
Model Serve needs this user to perform tasks, such as provisioning resources to deploy a machine learning model. Do not edit or delete the Model Serve system user.

# 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:




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**.

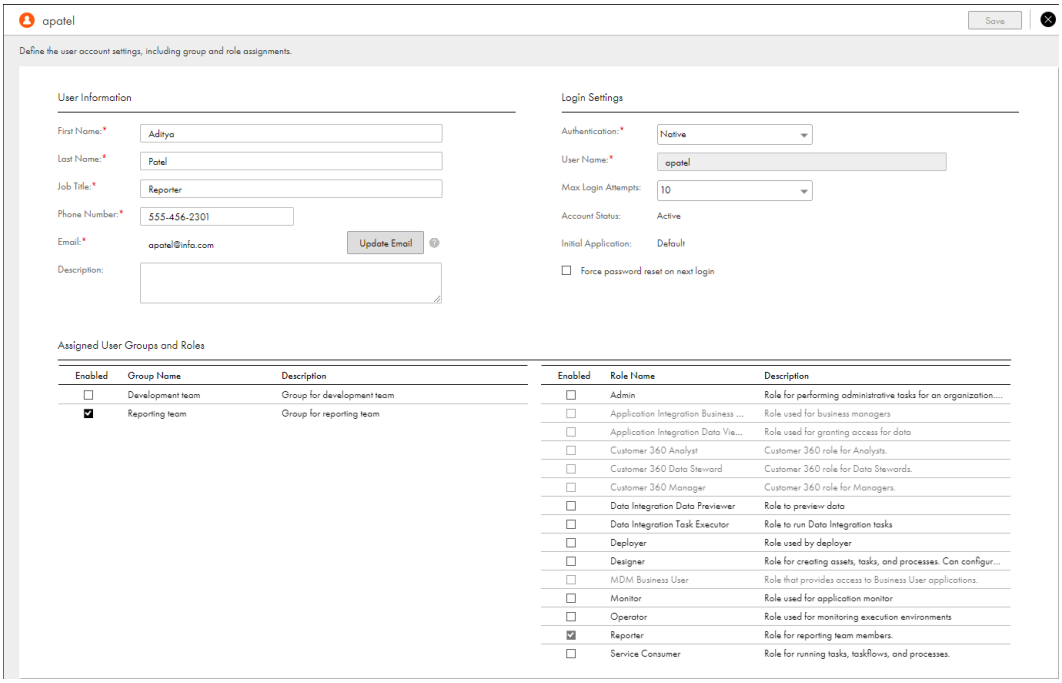
If you have the Admin role or the Create User and Audit Log - View privileges, you can view a graph of the numbers of users that logged in per day during the last 7, 30, or 90 days. To view the graph, click **Chart View** and select the appropriate time period. You can also download a report that lists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




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.<br>Must be a valid email address in the format: <local_part>@<domain>. For example, jsmith@mycompany.com.<br>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.<br>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:<br>- Native. The user is authenticated through Informatica Intelligent Cloud Services. The user logs in through the Informatica Intelligent Cloud Services URL.<br>- Salesforce. The user is authenticated through Salesforce and signs in through Salesforce or a Salesforce app.<br>- Azure SSO. The user is authenticated and signs in through Microsoft Azure.<br>- 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:<br>- Activate using verification code. Select this option when the user signs in to Informatica Intelligent Cloud Services through a Salesforce app.<br>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.<br>- Activate using Salesforce OAuth. Select this option to activate the user account using Salesforce OAuth.<br>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.<br>These options are displayed when the authentication method is Salesforce. |
| Environment | Salesforce organization environment, either production or sandbox.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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."<br>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.<br>This property is displayed when the authentication method is Native. |
| Account status | Account status. Can be one of the following statuses:<br>- Pending Activation. The user account has been created or reset, but the user has not yet activated the account.<br>- Enabled. The user account has been created and validated, and the user can log in to Informatica Intelligent Cloud Services.<br>- 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.<br>- 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.<br>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, the user's roles, and the groups to which the user belong.

Users normally inherit the services assigned to their user groups. However, you can specifically allow or deny access to services on the **Users** page.

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. Explicitly allow the API Portal service for the user and deny 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 even though the Service Consumer role has privileges related to them.

When a user has access to a service, the service is visible on the **My Services** page. The user can access and use the service as long as access is allowed.

When a user loses access to a service, the user can no longer see the service on the **My Services** page.

**Important:** Allowing or denying a service only reveals or hides the service from the user interface. The user retains all privileges associated with their assigned roles, even if you explictly deny a service. This means that the user might be able to perform an action through the API even if access is denied. As a best practice, only assign privileges that align with services assigned to a user.

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, perform one of the following tasks for each service:
   - To let the user's group memberships define whether the user can access the service, leave both the **Allow** and **Deny** options deselected. If the group's services change, the user's access to services changes automatically.
   - To allow access to the service regardless of what's defined in the user's group, select the **Allow** option.

**Tip:** If you don't see the service you wish to assign, that means the service isn't present in the organization's license.

- To deny access to the service, regardless of whether the user's group allows it, select the **Deny** option.

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), you must reassign the ownership of the file listener association from one user to another using the REST API before you disable a user. For more information, see *REST API Reference*.

# 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), you must reassign the ownership of the file listener association from one user to another using the REST API before you delete a user. For more information, see *REST API Reference*.

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

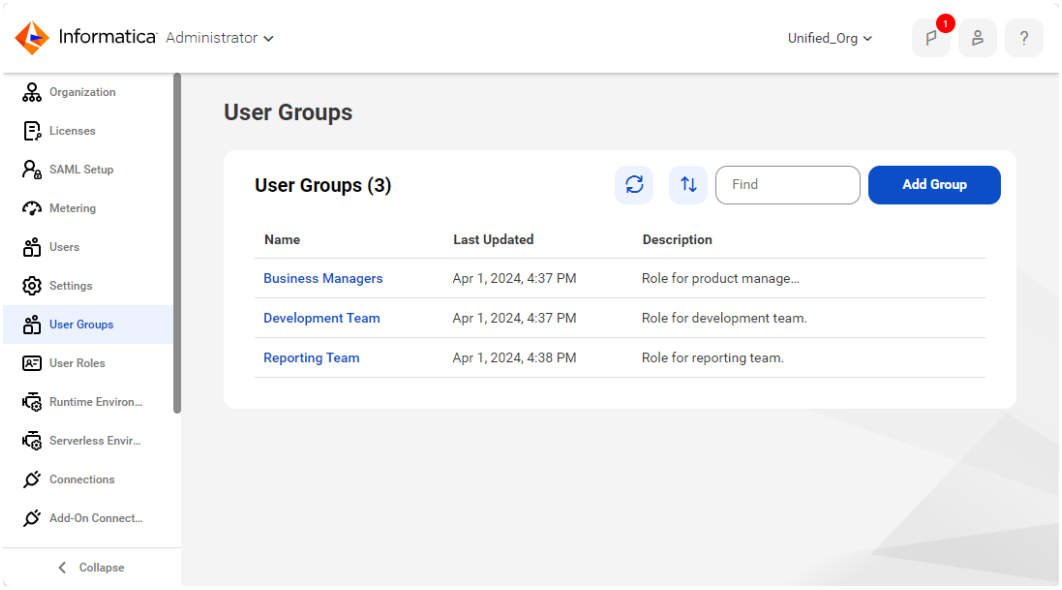
# User groups

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:



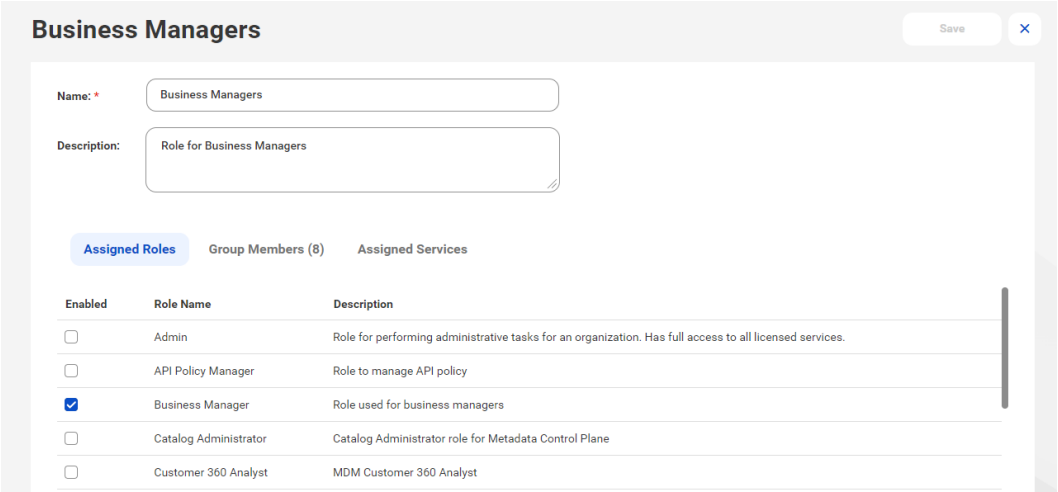

You can perform the following tasks for a user group:

- 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, group members, and assigned services. 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:




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.<br>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. |
| Group Members | Users who are assigned to the group.<br>Use the **Manage Users** button to add or remove users from the list.<br>When you assign a user to a group, the user is automatically assigned all roles and services that are assigned to the group. |
| Assigned Services | Services to which the group has access. These are all the services in the organization's license.<br>By default, a user group is assigned all the services the organization is licensed to use.<br>When you add a user to a group, that user gains access to all of the group's services provided that all the following conditions are met:<br>- At least one of the user's roles allow access to the service.<br>- The user is not explicitly "denied" access to the service.<br>For more information about a user's role, see "User details" on page 27.<br>For more information about explicitly allowing or denying access to services for a user, see "Assigning and unassigning services " on page 31.<br>**Note:** By explicitly allowing access, it is possible for a user to have access to a service that is not included in the user's group membership. |

**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, or if they need access to the same services. 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, click **Add Users** and select the user from the 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. In the Assigned Services section, select the services that are enabled for the group.

   You can override service access at the user level, so that members of this user group can have access to services that differ from the user group.
7. 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.

Organization administrators can configure and assign roles for the organization.

You can assign the following types of roles:

**System-defined**

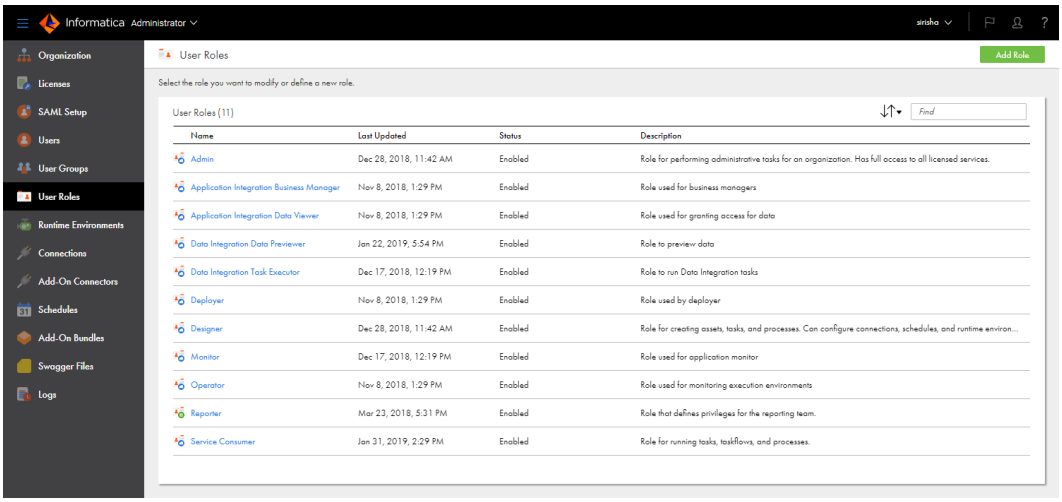
System-defined roles are pre-defined roles that define access privileges for the services that your organization uses. The system-defined roles that you can assign to users and user groups vary based on your organization's licenses. You can't edit, rename, or delete system-defined roles. You can clone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



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

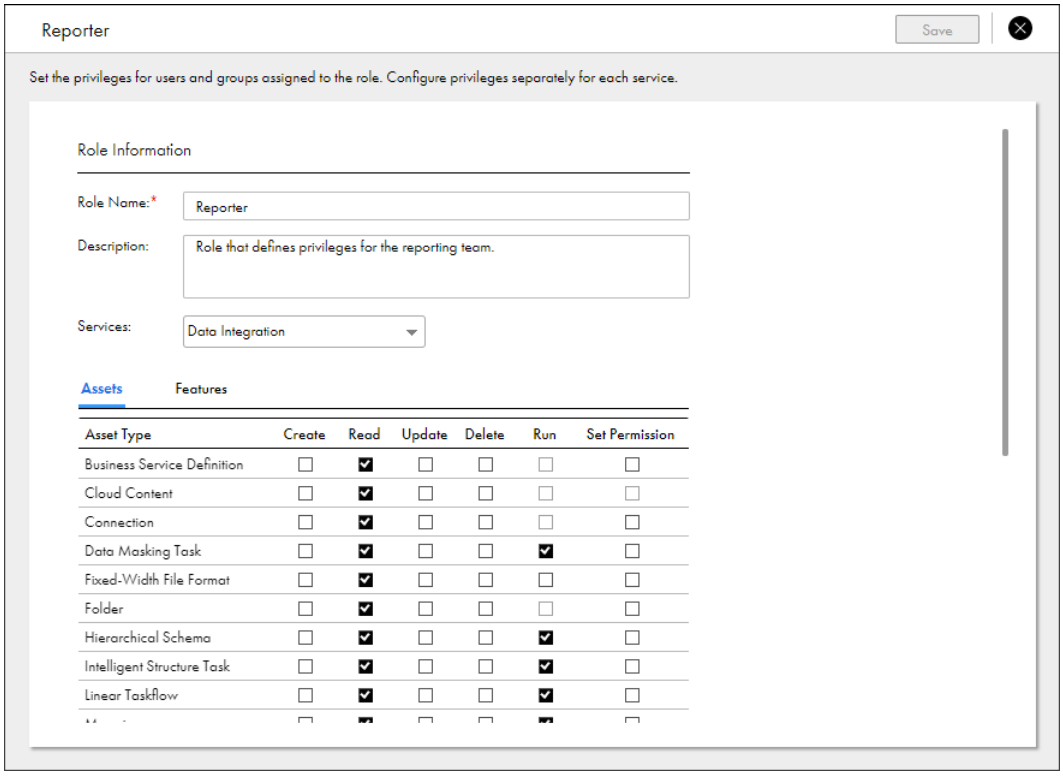
You can assign multiple roles to a user or user group. When you assign multiple roles, the user or group inherits the access privileges associated with all of the roles.

# 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:




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 can't create, update, delete, or set permissions on mappings.

If a privilege doesn't 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.

For more information about asset and feature privileges, see "Role asset and feature privileges" on page 60.

# System-defined roles

Informatica Intelligent Cloud Services provides system-defined roles that you can assign to users or user groups. You can't 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, you can't assign the Application Integration Business Manager or Application Integration Data Viewer role to any user or group in your organization.

There are two types of system-defined roles:

**Cross-service roles**

Cross-service roles define access privileges across multiple services. For example, users with the Deployer role can access some features in API Center, API Manager, Application Integration, Application Integration Console, Data Quality, and Data Ingestion and Replication.

**Service-specific roles**

Service-specific roles define access privileges for one service or for a group of closely related services. For example, users with the Governance User role can access Data Governance and Catalog but have no access to other services unless you assign additional roles.

**Note:** Don't assign the system-defined role "Dataloader admin" to any users. This role is used with Informatica Data Loader only.

## Cross-service roles

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

The following table describes the cross-service roles:

| Cross-service role | Provides access to... | Description |
|---|---|---|
| Admin | All services | Role for organization administrators. Provides full access to all licensed services with the following exceptions:<br>- Doesn't provide privileges to enable or disable the use of customer managed encryption keys for the organization. To provide these privileges, assign the user both the Admin and Key Admin roles.<br>- Doesn't provide full access to all MDM services. For example, doesn't allow the user to access the workflow inbox or create hierarchies in MDM business services. To provide full access to MDM services, assign the user an appropriate MDM service-specific role.<br>**Tip:** 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 | - Data Integration<br>- Data Profiling<br>- Data Quality<br>- Data Validation | Supplemental role that allows designers to preview data while creating mappings, tasks, profiles, and test cases. Allows users to perform the following tasks:<br>- Preview data in a mapping or task in Data Integration.<br>- Preview data on a data quality transformation in a mapping in Data Integration.<br>- View source object data for profiles and profile results in Data Profiling.<br>- Preview data while creating test cases in Data Validation.<br>**Note:** This is a supplemental role. Assign this role with another role, such as the Designer role, to ensure that users can access Data Integration, Data Profiling, and Data Validation. |
| Data Integration Task Executor | - Data Integration<br>- Data Access Management | Role for running tasks and taskflows and executing data access policies. Allows users to perform the following tasks:<br>- View assets and asset details in Data Integration.<br>- Run tasks and taskflows and test-run mappings in Data Integration.<br>- View user's own data integration jobs and job details in Data Integration.<br>- Start and stop user's own jobs in Data Integration.<br>- Download session logs in Data Integration.<br>- Execute data access policies in Data Integration.<br>- Access Data Access Management.<br>- View data access policies in Data Access Management. |
| Deployer | - API Center<br>- Application Integration<br>- Application Integration Console<br>- Data Quality<br>- Data Ingestion and Replication<br>- Data Validation | Role for users that deploy assets and processes. Allows users to perform the following tasks:<br>- View and deploy assets, assign policies, manage organization settings, and add OAuth 2.0 clients in API Center when assigned with the Service Consumer role.<br>- View asset details in Application Integration.<br>- Deploy assets, view settings, and upload and deploy Process Developer-generated orchestration artifacts (BPRs) in Application Integration Console.<br>- View asset details except dictionary data in Data Quality.<br>- View application ingestion, database ingestion, and streaming ingestion tasks in Data Ingestion and Replication.<br>- View test cases, test suites, and reports in Data Validation.<br>- Run test cases and test suites in Data Validation. |

| Cross-service role | Provides access to... | Description |
|---|---|---|
| Designer | - Administrator<br>- API Center<br>- Application Integration<br>- Application Integration Console<br>- B2B Gateway<br>- Data Integration<br>- Data Profiling<br>- Data Quality<br>- Integration Hub<br>- Data Ingestion and Replication<br>- Model Serve<br>- Monitor<br>- Data Validation | Role for users that create assets, tasks, and processes. Allows users to perform the following tasks:<br>- Create assets, tasks, and processes.<br>- Configure connections, schedules, and runtime environments.<br>- Monitor jobs and advanced clusters, except in Mass Ingestion.<br>- View, create, and edit test cases and test suites in Data Validation.<br>Provides full access to Application Integration, B2B Gateway, Data Integration, Data Profiling, Data Quality, and Monitor.<br>Provides full access to API Center when the Service Consumer role is also assigned.<br>Provides partial access to Administrator, API Center, Application Integration Console, Integration Hub, Data Ingestion and Replication, Model Serve, and Data Validation. |
| Monitor | - Administrator<br>- API Center<br>- Application Integration<br>- Application Integration Console<br>- B2B Gateway<br>- Data Integration<br>- Data Profiling<br>- Data Quality<br>- Integration Hub<br>- Data Ingestion and Replication<br>- Model Serve<br>- Monitor | Role for users that monitor jobs. Allows users to perform the following tasks:<br>- Monitor API Center assets, Data Integration jobs, Data Quality assets, Integration Hub assets, Data Ingestion and Replication jobs, Model Serve assets, and Application Integration process instances.<br>- View schedules and upgrade settings for Secure Agent services in Administrator.<br>- Start and stop file servers, configure proxy servers, and view file server settings in Administrator.<br>- View asset details in Application Integration, B2B Gateway, Data Integration, Data Profiling, Integration Hub, and Model Serve.<br>- View settings in Application Integration Console.<br>- View asset details except dictionary data in Data Quality.<br>- View API invocation logs in API Center.<br>- View application ingestion, database ingestion, and streaming ingestion jobs and job details in Data Ingestion and Replication.<br>- View data integration and job details in Monitor. |

| Cross-service role | Provides access to... | Description |
|---|---|---|
| Operator | - Application Integration<br>- Application Integration Console<br>- Data Profiling<br>- Data Quality<br>- Model Serve<br>- Operational Insights | Role for users that manage processes. Allows users to perform the following tasks:<br>- View asset details in Application Integration, Data Profiling, and Model Serve.<br>- Manage process instances and modify some operational server parameters in Application Integration.<br>- View and edit Process Server settings and some Cloud Server settings in Application Integration Console.<br>- View asset details except dictionary data in Data Quality.<br>- View cloud and domain infrastructure and Secure Agent alert settings in Operational Insights. |
| Service Consumer | - Administrator<br>- API Portal<br>- Application Integration<br>- Data Integration<br>- Data Quality | Role for users that run tasks and processes. Allows users to perform the following tasks:<br>- View schedules, Swagger files, and upgrade settings for Secure Agent services, start and stop file servers, configure proxy servers, and view other file server settings in Administrator.<br>- Open API Portal.<br>- Invoke processes in Application Integration.<br>- View tasks, run tasks, test-run mappings, run taskflows, and download workflow XML in Data Integration.<br>- View asset details except dictionary data in Data Quality.<br>Provides full access to API Portal. |

## Administrator roles

To provide access to the Administrator service, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Administrator:

| Role | Description |
|---|---|
| Admin* | Provides full access to Administrator except for privileges to enable or disable the use of customer managed encryption keys for the organization. To allow this ability, assign the user both the Admin and Key Admin roles. |
| Designer* | Allows users to perform the following tasks in Administrator:<br>- Configure connections, runtime environments, schedules, Swagger files, and advanced configurations.<br>- Install add-on connectors and install and uninstall add-on bundles.<br>- View upgrade settings for Secure Agent services.<br>- Start and stop file servers, configure proxy servers, and view other file server settings. |
| Key Admin | Allows users to enable and disable the use of customer managed encryption keys for their organization on the **Security** tab of the **Settings** page. Assign this role to a user who also has the Admin role. If the user doesn't have both roles, they can't see the **Security** tab.<br>For more information about customer managed encryption keys, see *Organization Administration*. |
| Monitor* | Allows users to perform the following tasks in Administrator:<br>- View schedules and upgrade settings for Secure Agent services.<br>- Start and stop file servers, configure proxy servers, and view other file server settings. |

| Role | Description |
|---|---|
| Service Consumer* | Allows users to perform the following tasks in Administrator:<br>- View schedules, Swagger files, and upgrade settings for Secure Agent services.<br>- Start and stop file servers, configure proxy servers, and view other file server settings. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

## API Center roles

To provide access to API Center, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to API Center:

| Role | Description |
|---|---|
| Admin* | Provides full access to API Center. |
| API Policy Manager | Allows users to define policies. Allows users to access the following pages in API Center:<br>- Explore (read-only)<br>- Policies |
| Deployer* | When assigned with the Service Consumer role, allows users to view and deploy assets, assign policies, manage organization settings, and add OAuth 2.0 clients in API Center. Allows users to access the following pages:<br>- Explore (read-only)<br>- API Console<br>- Configuration<br>**Note:** To provide these privileges, you must assign both the Deployer and Service Consumer roles. |
| Designer* | When assigned with the Service Consumer role, provides full access to all asset privileges and allows users to assign policies in API Center. Allows users to access the following pages:<br>- New Asset<br>- Explore<br>**Note:** To provide these privileges, you must assign both the Designer and Service Consumer roles. |
| Monitor* | Allows users to monitor API Center assets. Allows users to access the following pages:<br>- Explore (read-only)<br>- API Monitor |
| Service Consumer* | Allows users to access API Center when the Designer or Deployer role is also assigned. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

For more information about API Center roles, see the API Center help.

## API Manager roles

To provide access to API Manager, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to API Manager:

| Role | Description |
|---|---|
| Admin* | Provides full access to API Manager. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

To provide different levels of access to API Manager, create custom roles. For more information, see the API Manager help.

## API Portal roles

To provide access to API Portal, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to API Portal:

| Role | Description |
|---|---|
| Admin* | Provides full access to API Portal. |
| Service Consumer* | Allows users to open API Portal. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

## Application Integration and Application Integration Console roles

To provide access to Application Integration and Application Integration Console, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Application Integration and Application Integration Console:

| Role | Description |
|---|---|
| Admin* | Provides full access to Application Integration and Application Integration Console. Has the execution privileges. |
| Application Integration Business Manager | Role for monitoring business activity. Users with this role can view information about assets and process instances, but they can't change them.<br>Allows users to perform the following tasks:<br>- View folder and asset lists and asset details in Application Integration.<br>- Access the Processes, APIs, and Connections pages in Application Integration Console. |

| Role | Description |
|---|---|
| Application Integration Data Viewer | Supplemental role that allows users to view detailed logs in Application Integration Console. 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.<br>**Note:** Users can view detailed logs for an artifact when the logging level is set to verbose. |
| Deployer* | Allows users to perform the following tasks in Application Integration and Application Integration Console:<br>- View asset details in Application Integration.<br>- Deploy assets and view settings on the Processes, Logs, Server Configuration, Deployed Assets, and Resources pages in Application Integration Console.<br>- Upload and deploy Process Developer-generated orchestration artifacts (BPRs) in Application Integration Console.<br>Assign this role in a production environment where deployment access is typically restricted. |
| Designer* | Provides full access to Application Integration.<br>Allows users to view and edit all settings except server configuration properties in Application Integration Console. |
| Monitor* | Allows users to perform the following tasks in Application Integration and Application Integration Console:<br>- View asset details in Application Integration.<br>- View settings in Application Integration Console. |
| Operator* | Allows users to perform the following tasks in Application Integration and Application Integration Console:<br>- View asset details in Application Integration.<br>- View and edit Process Server settings and some Cloud Server settings in Application Integration Console. For example, a user with the Operator role can create an alert service but can't view tenant details. |
| Service Consumer* | Allows users to execute Application Integration processes through APIs. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

## B2B Gateway roles

To provide access to B2B Gateway, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to B2B Gateway:

| Role | Description |
|---|---|
| Admin* | Provides full access to B2B Gateway. |
| Designer* | Provides full access to B2B Gateway. |
| Monitor* | Allows users to view asset details. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

## B2B Partners Portal 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.

**Note:** There is no system-defined role for B2B Partners Portal external trading partners. Therefore, you'll need to create a custom role for them.

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 59.

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.

## Business 360 Console roles

To provide access to Business 360 Console, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Business 360 Console:

| Role | Description |
|---|---|
| Admin* | Provides full access to Business 360 Console. Allows users to perform solution upgrades.<br>**Note:** To provide full access to Business 360 Console, assign users the Admin, Designer, and MDM Designer user roles. To allow users to perform only the configuration tasks in Business 360 Console, you can assign users the Admin role or both the Designer and MDM Designer roles. |
| Business 360 Process Executor | Required role for users with custom user roles to perform tasks in Business 360 Console and business applications. Allows users to update business entities in Business 360 Console.<br>Allows users to perform the following tasks in business applications:<br>- Save records and custom reports.<br>- View, create, update, and delete hierarchies.<br>- Import records, related records, and hierarchy data.<br>- Access the **Workflow Inbox** page. |
| Designer* | Allows users to perform tasks in Business 360 Console that require integration with other services such as Data Integration and Data Quality.<br>Allows users to perform the following tasks in Business 360 Console:<br>- Create MDM SaaS assets except reference data assets.<br>- Define a data model and source systems.<br>- Define and monitor jobs, such as ingress and egress.<br>- Configure data quality, match and merge, survivorship, business events, and global settings.<br>Doesn't allow users to define reference data assets. |
| Job Executor | Allows users to run ingress and egress jobs in Business 360 Console.<br>**Note:** This role is not required to run jobs that business applications run when users perform tasks, such as file import. |

| Role | Description |
|---|---|
| MDM Designer | Allows users to perform the following tasks in Business 360 Console:<br>- Create MDM SaaS assets.<br>- Define a data model and source systems.<br>- Define and monitor jobs, such as ingress and egress.<br>- Configure data quality, match and merge, survivorship, business events, and global settings.<br>- Export and import assets when the user also has the Designer role. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

For more information about Business 360 Console roles, see the Business 360 Console help.

## CLAIRE GPT roles

To provide access to CLAIRE GPT, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined user role that provides access to CLAIRE GPT:

| Role | Description |
|---|---|
| CLAIRE GPT User | Provides full access to all the capabilities of CLAIRE GPT. |

For more information about CLAIRE GPT user roles, see the CLAIRE GPT help.

## Cloud Data Integration for PowerCenter (CDI-PC) roles

To provide access to the CDI-PC service, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to CDI-PC:

| Role | Description |
|---|---|
| Domain Management | Provides full access to CDI-PC. |

## Customer 360 SaaS roles

To provide access to MDM - Customer 360 SaaS, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to MDM - Customer 360 SaaS:

| Role | Description |
|---|---|
| Customer 360 Analyst | Role for creating records. Allows users to create, edit, and delete records in MDM - Customer 360 SaaS.<br>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 Data Steward | Role for creating records and hierarchies. Allows users to perform any task in Customer 360 SaaS, including the following tasks:<br>- Create, edit, and delete records without approval.<br>- Run jobs.<br>- Review and approve customer records. |
| Customer 360 Manager | Role for managing records. Allows users to perform the following tasks:<br>- Review and approve or reject customer records.<br>- Create, edit, and delete records without approval. |
| MDM Business User | Allows users to view records in Customer 360 SaaS but not create or edit them. |

For more information about Customer 360 SaaS roles, see the MDM - Customer 360 SaaS help.

## Data Access Management roles

To provide access to Data Access Management, assign users the appropriate roles. You can assign a system-defined role to or create custom roles for users.

The following table describes the system-defined roles that provide access to Data Access Management:

| Role | Description |
|---|---|
| Admin* | Role for performing administrative tasks. Provides full access to Data Access Management, but cannot execute data access policies. |
| Data Integration Task Executor* | Role for executing data access policies. Allows users to perform the following tasks:<br>- Access Data Access Management.<br>- View data access policies in Data Access Management.<br>- Execute data access policies in Data Integration. |
| Data Marketplace Administrator** | Role for performing administrative tasks. Provides full access to Data Access Management, but cannot execute data access policies. |
| Data Marketplace Technical Administrator** | Role for performing technical administrative tasks. Provides full access to Data Access Management, but cannot execute data access policies. |
| Data Marketplace User** | Role for reading data access policies. Allows users to perform the following tasks in Data Access Management:<br>- Access Data Access Management.<br>- View data access policies. |

| Role | Description |
|---|---|
| Governance Administrator*** | Role for performing administrative tasks. Provides full access to Data Access Management, but cannot execute data access policies. |
| Governance User*** | Role for viewing data access policies. Allows users to perform the following tasks in Data Access Management:<br>- Access Data Access Management.<br>- View data access policies. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40.<br>** Also provides access to Data Marketplace. For more information, see "Data Marketplace roles" on page 51.<br>*** Also provides access to Data Governance and Catalog. For more information, see "Data Governance and Catalog roles" on page 49. | |

For more information about Data Access Management roles, see the Data Access Management help.

## Data Governance and Catalog roles

To provide access to Data Governance and Catalog, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Data Governance and Catalog:

| Role | Description |
|---|---|
| Governance Administrator* | Role for administering assets and operations in Data Governance and Catalog and Metadata Command Center. Allows users to perform the following tasks in Data Governance and Catalog:<br>- View business assets, data classifications, profiled stats, sensitive data, technical assets, and unpublished content.<br>- Curate automatic glossary associations and data classifications.<br>- Assign stakeholders for technical assets.<br>- Participate in change approvals.<br>- Export and import assets. |
| Governance User* | Role for viewing and exporting assets in Data Governance and Catalog. Allows users to perform the following tasks in Data Governance and Catalog:<br>- View business assets, data classifications, profiled stats, and technical assets.<br>- Export assets. |
| * Also provides access to Data Access Management, Data Marketplace and Metadata Command Center. For more information, see "Data Access Management roles" on page 48, "Data Marketplace roles" on page 51 and "Metadata Command Center roles" on page 55. | |

For more information about Data Governance and Catalog roles, see the Data Governance and Catalog help.

## Data Ingestion and Replication roles

To provide access to Data Ingestion and Replication, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Data Ingestion and Replication:

| Role | Description |
|---|---|
| Admin* | Provides full access to Data Ingestion and Replication. |
| Deployer* | Allows users to view application ingestion, database ingestion, and streaming ingestion tasks. |
| Designer* | Allows users to create, view, edit, delete, run, and set permissions on application ingestion, database ingestion, and streaming ingestion tasks. |
| Monitor* | Allows users to view application ingestion, database ingestion, and streaming ingestion jobs and job details. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

## Data Integration roles

To provide access to Data Integration, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Data Integration:

| Role | Description |
|---|---|
| Admin* | Provides full access to Data Integration. |
| Data Integration Data Previewer* | Supplemental role that allows users to perform the following tasks in Data Integration:<br>- Preview data when they select a source, target, or lookup object for use in a mapping or task.<br>- Preview data when on a data quality transformation that they select in a mapping.<br>Assign this role with another role, such as the Designer role, to ensure that users can access Data Integration. |
| Data Integration Task Executor* | Role for running tasks and taskflows. Allows users to perform the following tasks in Data Integration:<br>- View assets and asset details.<br>- Run tasks and taskflows and test-run mappings.<br>- View user's own data integration jobs and job details.<br>- Start and stop user's own jobs.<br>- Download session logs. |
| Designer* | Provides full access to Data Integration. |
| Monitor* | Allows users to view asset details in Data Integration. |
| Service Consumer* | Allows users to view tasks, run tasks, test-run mappings, run taskflows, and download workflow XML in Data Integration. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

# Data Marketplace roles

To provide access to Data Marketplace, assign users the appropriate roles. You can assign a system-defined role to Data Marketplace users.

The following table describes the system-defined roles that provide access to Data Marketplace:

| Role | Description |
|---|---|
| Data Marketplace Administrator* | Role for performing administrative tasks. Provides full access to access to Data Marketplace. |
| Data Marketplace Category Owner | Role for users that have the rights to a category. Allows users to perform the following tasks:<br>- Create and bulk create data collections within the user's category.<br>- Add and remove data assets inside data collections within the user's category.<br>- Approve and reject data orders for data collections.<br>- Approve and reject data collection requests on categories that the user is responsible for.<br>- Add and edit delivery targets inside data to collections within the user's category.<br>- Link and remove variants to data collections within the user's category.<br>- Delete data collections within the user's category.<br>- Rate data collections that the user has access to against the context the user has access with.<br>- Search for published data collections.<br>- Compare collections.<br>- Add and bulk add data assets to data collections.<br>- Create an order and raise data collection requests.<br>- Create, bulk create, modify, and delete categories.<br>- Add and remove terms of use inside data collections within the user's category.<br>- Participate in public discussion channels.<br>- Comment on private channels that the user has access to. |
| Data Marketplace Data Collection Owner | Role for users that have rights to a data collection. Allows users to perform the following tasks:<br>- Create, bulk create, modify, and delete data collections.<br>- View data collections that the user owns.<br>- Add and bulk add terms of use and data assets to data collections that the user owns.<br>- Remove terms of use and data assets from data collections that the user owns.<br>- Search for published data collections.<br>- Compare collections.<br>- Add and edit delivery targets inside the data collections that the user owns.<br>- Rate data collections that the user has access to against the context the user has access with.<br>- Create an order for collections and raise data collection requests against collections or categories.<br>- Complete and reject data collection requests raised on data collections that the user owns.<br>- Approve and reject data collection access requests.<br>- Link variants.<br>- Participate in public discussion channels.<br>- Comment on private channels that the user has access to. |

| Role | Description |
| --- | --- |
| Data Marketplace Data Collection Technical Owner | Role for users that have technical rights to a data collection. Allows users to perform the following tasks:<br>- View orders for data collections.<br>- Add and edit delivery targets to data collections.<br>- Request withdrawal and withdraw access to data collections.<br>- Add and remove data assets and terms of use inside data collections.<br>- Rate data collections that the user has access to against the context the user has access with.<br>- Search for published data collections.<br>- Compare collections.<br>- Create an order on collections and raise data collection requests against collections and categories.<br>- Bulk create "terms of use - data collection" relationships and "delivery target - data collection" relationships.<br>- Deliver data that is ordered by a data user.<br>- Participate in public discussion channels.<br>- Comment on private channels that the user has access to. |
| Data Marketplace Delivery Owner | Role for managing the delivery option for delivering data collections. Allows users to perform the following tasks:<br>- Search and compare data collections.<br>- Rate data collections that user has access to.<br>- Create delivery options and delivery targets.<br>- Bulk create delivery formats, delivery methods, delivery templates, and "delivery target - data collection" relationships.<br>- Request withdrawal of consumer access, withdraw consumer access, and fulfill data orders for data collections that have a delivery option that the user is responsible for.<br>- Participate in public and private discussion channels that the user has access to. |
| Data Marketplace Technical Administrator* | Role for performing technical administrative tasks. Allows users to perform the following tasks:<br>- View data orders for and add delivery targets to data collections.<br>- Deliver requested data collections to data users.<br>- Search and compare data collections.<br>- Rate data collections that the user has access to.<br>- Add data assets, delivery targets, and terms of use to data collections.<br>- Bulk create data elements, data assets, and consumer accesses.<br>- Delete data elements and data assets.<br>- Modify object labels.<br>- Configure data delivery formats and methods.<br>- Configure default delivery targets to deliver data.<br>- Import assets from Data Governance and Catalog.<br>- Configure the general "terms of use" message and create new terms of use.<br>- Create cost centers.<br>- Request withdrawal and withdraw consumer accesses.<br>- Bulk create cost centers, delivery formats, delivery methods, delivery templates, "terms of use - data collection" relationships, and "delivery target - data collection" relationships.<br>- Configure star owners.<br>- Participate in public and private discussion channels that the user has access to.<br>- Customize the Data Marketplace user interface. |
| Data Marketplace User* | Role for using data collections. Allows users to perform the following tasks:<br>- Order, and compare data collections.<br>- Search for published data collections.<br>- View requested and delivered data collections.<br>- View data collection details.<br>- Rate data collections that the user has access to.<br>- Create and cancel data collection requests on collections and categories.<br>- Participate in public and private discussion channels. |

| Role | Description |
|---|---|
| Governance Administrator* | Role for using data collections. Allows users to perform the following tasks:<br>- Order, and compare data collections.<br>- Search for published data collections.<br>- View requested and delivered data collections.<br>- View data collection details.<br>- Rate data collections that the user has access to.<br>- Create and cancel data collection requests on collections and categories.<br>- Participate in public and private discussion channels. |
| Governance User* | Role for using data collections. Allows users to perform the following tasks:<br>- Order, and compare data collections.<br>- Search for published data collections.<br>- View requested and delivered data collections.<br>- View data collection details.<br>- Rate data collections that the user has access to.<br>- Create and cancel data collection requests on collections and categories.<br>- Participate in public and private discussion channels. |
| * Also provides access to Data Access Management. For more information, see "Data Access Management roles" on page 48. | |

For more information about Data Marketplace roles, see the Data Marketplace help.

## Data Profiling roles

To provide access to Data Profiling, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Data Profiling:

| Role | Description |
|---|---|
| Admin* | Provides full access to Data Profiling. |
| Data Integration Data Previewer* | Supplemental role that allows users to preview source object data when they create a profile or view profile results.<br>Assign this role with another role, such as the Designer role, to ensure that users can access Data Profiling. |
| Designer* | Provides full access to Data Profiling. |
| Monitor* | Allows users to view asset details in Data Profiling. |
| Operator* | Allows users to view asset details in Data Profiling. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

## Data Quality roles

To provide access to Data Quality, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Data Quality:

| Role | Description |
|---|---|
| Admin* | Provides full access to Data Quality. |
| Deployer* | Allows users to view asset details except dictionary data in Data Quality. |
| Designer* | Provides full access to Data Quality. |
| Monitor* | Allows users to view asset details except dictionary data in Data Quality. |
| Operator* | Allows users to view asset details except dictionary data in Data Quality. |
| Service Consumer* | Allows users to view asset details except dictionary data in Data Quality. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

## Integration Hub roles

To provide access to Cloud Integration Hub, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Cloud Integration Hub:

| Role | Description |
|---|---|
| Admin* | Provides full access to Cloud Integration Hub. |
| Designer* | Allows users to create, view, edit, delete and run Cloud Integration Hub assets.<br>Doesn't provide privileges to perform provisioning, set system properties, or set permissions for Cloud Integration Hub assets. |
| Monitor* | Allows users to view asset details in Cloud Integration Hub. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

For more information about Cloud Integration Hub roles, see the Cloud Integration Hub help.

## Metadata Command Center roles

To provide access to Metadata Command Center, assign users the appropriate roles. You can assign a system-defined role or custom roles for users.

The following table describes the system-defined roles that provide access to Metadata Command Center:

| Role | Description |
|---|---|
| Admin* | Role for performing upgrades. In addition, this role can perform all tasks that a Governance Administrator can perform in Metadata Command Center. |
| Governance Administrator** | Role for administering assets and operations in Data Governance and Catalog and Metadata Command Center. Allows users to perform the following tasks in Metadata Command Center:<br>- Create, read, update and delete AI models, business reports, business terms, catalog source configurations, catalog source types, custom models, data quality, data sets, glossary domains and subdomains, metrics, policies, processes, and systems.<br>- Run and set permissions on catalog source configurations.<br>- Read and update technical assets.<br>- Manage access control, connection assignments, custom attributes, data classifications, reference data, system settings, and workflow settings.<br>- Monitor jobs.<br>- View custom attributes, data classifications, and reference data. |
| Governance User** | Role for viewing and exporting assets in Data Governance and Catalog. Allows users to view AI models, business reports, business terms, custom catalog source types, custom models, data quality, data sets, glossary domains and subdomains, metrics, policies, processes, systems, and technical assets in Metadata Command Center. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40.<br>** Also provides access to Data Governance and Catalog. For more information, see "Data Governance and Catalog roles" on page 49. | |

For more information about Metadata Command Center roles, see the Metadata Command Center help.

## Model Serve roles

To provide access to Model Serve, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Model Serve:

| Role | Description |
|---|---|
| Admin* | Provides full access to Model Serve. |
| Designer* | Allows users to perform the following tasks in Model Serve:<br>- Create, view, edit, and delete machine learning models.<br>- Create, view, edit, delete, and run model deployments.<br>- Generate predictions from a deployed machine learning model. |
| Model Serve Admin | Role for Model Serve administration. Allows users to perform the following tasks:<br>- Assign permissions for other Model Serve users.<br>- Register and deploy machine learning models.<br>- Generate predictions from a deployed machine learning model. |

| Role | Description |
|---|---|
| Model Serve Predictions User | Role for generating predictions. Allows users to perform the following tasks:<br>- Generate predictions from a deployed machine learning model.<br>- View, but not change, model deployment assets. |
| Model Serve System Role | Role for the Model Serve system user. Assigns necessary permissions so that the system user can perform tasks such as provisioning resources for model deployments.<br>Do not assign this role to users.<br>For more information about the Model Serve system user, see "Model Serve system user" on page 26. |
| Monitor* | Allows users to view asset details in Model Serve. |
| Operator* | Allows users to view asset details in Model Serve. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

## Monitor roles

To provide access to Monitor, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Monitor:

| Role | Description |
|---|---|
| Admin* | Provides full access to Monitor. |
| Designer* | Provides full access to Monitor. |
| Monitor* | Allows users to view data integration jobs and job details in Monitor.<br>Doesn't allow users to view export or import jobs. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

## Operational Insights roles

To provide access to Operational Insights, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to Operational Insights:

| Role | Description |
|---|---|
| Admin* | Provides full access to Operational Insights. |
| Operator* | Allows users to perform the following tasks in Operational Insights:<br>- View cloud and domain infrastructure.<br>- View Secure Agent alert settings. |
| * Provides access to multiple services. For more information, see "Cross-service roles" on page 40. | |

## Product 360 SaaS roles

To provide access to MDM - Product 360 SaaS, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to MDM - Product 360 SaaS:

| Role | Description |
|---|---|
| Product 360 Manager | Role for managing records. Allows users to perform the following tasks:<br>- Review and approve records.<br>- Create, edit, and delete records without approval. |
| Product 360 Read-Only | Role for viewing records. Allows users to view records in Product 360 SaaS but not edit them. |

For more information about Product 360 SaaS roles, see the MDM - Product 360 SaaS help.

## Reference 360 roles

To provide access to MDM - Reference 360, assign users the appropriate roles. You can assign a system-defined role to Reference 360 users.

The following table describes the system-defined roles that provide access to MDM - Reference 360:

| Role | Description |
|---|---|
| Reference 360 Administrator | Administrative role for Reference 360. Allows users to configure the Reference 360 environment. |
| Reference 360 Business Analyst | Role for analyzing assets. Allows users to view and analyze assets, but not propose changes to them. |
| Reference 360 Business Steward | Role for the subject matter experts for reference data. Allows users to perform the following tasks:<br>- Create and manage code values in code lists and value mappings in crosswalks.<br>- Approve changes proposed by other users.<br>- Send their own changes for approval or directly publish their changes without approval. |
| Reference 360 Planner | Role for creating and managing hierarchies. Allows users to perform the following tasks:<br>- Create hierarchy assets, define hierarchy models, and import hierarchy relationships.<br>- Delete hierarchies that are no longer needed.<br>- Assign the Planner stakeholder role to other users for a hierarchy. |
| Reference 360 Primary Owner | Role for creating and defining reference data structures. Allows users to perform the following tasks:<br>- Create and define reference data structures, such as reference data sets and code lists.<br>- Delete code lists.<br>- Propose changes to code values in code lists. The changes must be approved by Business Stewards.<br>- Assign users access to code lists and reference data sets using Stakeholder roles. |

| Role | Description |
|---|---|
| Reference 360 Stakeholder | Role for proposing changes to code values. Allows users to propose changes, but the proposed changes must be approved by Business Stewards. |
| Reference 360 User | Restricted access role. By default, users with this role can't access any assets. To allow users to access a specific asset, such as a code list or crosswalk, assign this role along with the stakeholder role for the asset. |

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

## Supplier 360 SaaS roles

To provide access to MDM - Supplier 360 SaaS, assign users the appropriate roles. You can assign a system-defined role or create custom roles for users.

The following table describes the system-defined roles that provide access to MDM - Supplier 360 SaaS:

| Role | Description |
|---|---|
| Supplier 360 Analyst | Role for analyzing records. Allows users to create, read, edit, and delete records in Supplier 360 SaaS. 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 Commodity Manager | Role for managing commodity evaluation tasks. Has the originator and approver privileges. Allows users to perform the following tasks:<br>- Claim and disclaim commodity evaluation tasks.<br>- Act on the commodity evaluation tasks in the approval workflow.<br>- Create, read, edit, and delete records. |
| Supplier 360 Contract Manager | Role for managing contract evaluation tasks. Has the originator and approver privileges. Allows users to perform the following tasks:<br>- Claim and disclaim contract evaluation tasks.<br>- Act on the contract evaluation tasks in the approval workflow.<br>- Create, read, edit, and delete records. |
| Supplier 360 Credit Manager | Role for managing credit evaluation tasks. Has the originator and approver privileges. Allows users to perform the following tasks:<br>- Claim and disclaim credit evaluation tasks.<br>- Act on the credit evaluation tasks in the approval workflow.<br>- Create, read, edit, and delete records. |
| Supplier 360 Data Steward | Role for managing records. Allows users to perform the following tasks:<br>- Create, read, edit, and delete records with or without approval.<br>- Run jobs.<br>- Review and approve records.<br>- Match, merge, and unmerge records. |
| Supplier 360 Read Only | Role for viewing records in Supplier 360 SaaS. Allows users to view records but not create or edit them. |

| Role | Description |
|---|---|
| Supplier 360 Risk Manager | Role for managing risk evaluation tasks. Has the originator and approver privileges. Allows users to perform the following tasks:<br>- Claim and disclaim risk evaluation tasks.<br>- Act on the risk evaluation tasks in the approval workflow.<br>- Create, read, edit, and delete records. |
| Supplier 360 Task Admin | Role for administering evaluation tasks. Has the originator and approver privileges. Allows users to view all unclaimed evaluation tasks. |

For more information about Supplier 360 SaaS roles, see the MDM - Supplier 360 SaaS help.

# 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 can't create, edit, or run data integration tasks.

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 doesn't grant additional privileges to custom roles when your organization gets a new license.

**Note:** Custom roles can't 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**.

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 can't 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 can't delete a custom role if it is assigned to any user or user group. You can't 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**.

# Role asset and feature privileges

Every role is associated with a set of asset or feature privileges. These privileges allow users to perform specific functions while working with assets and service features. Assign asset and feature privileges when you create a custom role.

Asset privileges provide CRUD, Run, and Set Permission privileges for different types of assets. For example, if you assign the Create privilege for mappings to a role, users with the role can create, view, and update 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.<br>Automatically grants the Read and Update privileges. |
| Read | Open assets of the selected type. For tasks, this privilege also allows users to use a connection or schedule in the task. |

| Privilege | Description |
|---|---|
| Update | Edit assets of the selected type.<br>Automatically grants the Read privilege. |
| Delete | Delete assets of the selected type. |
| Run | Run assets of the selected type.<br>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.<br>For the Cloud Integration Hub 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.<br>To configure this privilege, your organization must have the appropriate license. |

Feature privileges control the ability to use certain features of a service. For example, the Data Quality "Data Preview - Dictionaries" privilege allows users to view the contents of a dictionary.

Assign asset and feature privileges on the role details page when you create a custom role. For more information about the role details page, see "Role details" on page 38.

You can't change the asset and feature privileges associated with a system-defined role.

# Administrator asset and feature privileges

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

## Administrator asset privileges

The following table describes the Administrator asset privileges:

| Asset privilege | Description |
|---|---|
| Connection | Allows users to create, read, update, delete, or set permissions on connections. |
| Elastic Configuration | Allows users to create, read, update, delete, or run advanced configurations. |
| Folder | Allows users to create, read, update, delete, or set permissions on project folders. |
| Group | Allows users to create, read, update, or delete user groups. |
| OAuth Client | Allows users to create, read, update, or delete OAuth 2.0 clients.<br>For more information about creating and managing OAuth 2.0 clients, see the help for API Center. |
| Organization | Allows users to read and update organization information. |
| Privilege | Allows users to view the asset and feature privileges associated with each role. |
| Project | Allows users to create, read, update, delete, or set permissions on projects. |

| Asset privilege | Description |
|---|---|
| Role | Allows users to view users' roles and the **User Roles** page in Administrator. |
| Schedule | Allows users to create, read, update, delete, or set permissions on project schedules. |
| Scheduler Blackout | Allows users to create, read, update, or delete schedule blackout periods. |
| Scheduler Job | Allows users to run assets on a schedule, view schedule information for assets, update the schedule for an asset, or delete a schedule from an asset. |
| Secure Agent | Allows users to create, read, update, delete, or set permissions on Secure Agents. |
| Secure Agent Group | Allows users to create, read, update, delete, or set permissions on Secure Agent groups. |
| User | Allows users to create, read, update, and delete user accounts. |

## Administrator feature privileges

The following table describes the Administrator feature privileges:

| Feature privilege | Description |
|---|---|
| AdditionalOrg creation privilege | Allows users to create additional production and sandbox organizations when the AdditionalOrg view privilege is also granted. |
| AdditionalOrg view privilege | Allows users to view additional production and sandbox organizations from the production organization.<br>This privilege is required to create additional production and sandbox organizations. |
| Asset - check in/out | Allows users to check in and check out assets from the source control repository. |
| Asset - export | Allows users to export assets from the organization. |
| Asset - import | Allows users to import assets into the organization. |
| Asset - pull version | Allows users to pull assets from the source control repository. |
| Asset - Source Control Logs | Allows users to view the source control logs. |
| Audit Log - view | Allows users to view the audit log. |
| Bundle - create | Allows users to create bundles when the "Bundle - view" privilege is also granted. |
| Bundle - delete | Allows users to delete bundles when the "Bundle - view" privilege is also granted. |
| Bundle - install | Allows users to install bundles so that they are available to your organization when the "Bundle - view" privilege is also granted. |
| Bundle - publish | Allows users to publish bundles when the "Bundle - view" privilege is also granted. |
| Bundle - update | Allows users to update bundles when the "Bundle - view" privilege is also granted. |

| Feature privilege | Description |
|---|---|
| Bundle - view | Allows users to view bundles.<br>This privilege is required to create, delete, install, publish, and update bundles. |
| Configure Custom Repository Source Control | Allows users to configure a project-specific repository URL and branch name for project-level source control repositories when the Configure Source Control privilege is also granted. |
| Configure Source Control | Allows users to configure source control to enable version management for projects, folders, and assets. |
| Connectors - view | Allows users to view the connectors available to their organization and to view the **Add-On Connectors** page in Administrator. |
| Force Undo Checkout | Allows users to undo the checkout of an object that has been checked out by another user. |
| KMS View managed Key | Allows users to view the **Customer Managed Keys** area on the **Security** tab of the **Settings** page. |
| Manage Billing | Allows users of Data Integration-PayGo to manage their payment information.<br>For more information about Data Integration-Free and PayGo, see "Introducing Informatica Cloud Data Integration-Free and PayGo." |
| Manage key rotation settings | Allows customers to manage key rotation for their organization through the platform REST API version 3 key resource.<br>For more information about the v3 key resource, see *REST API Reference*. |
| ratecard.view | Allows users to view the current rate card for their organization on the Metering page. |
| SMS Manage Connection | Allows users to enable and disable the use of a secrets manager for the organization and to configure and update the secrets manager settings. |
| SMS View Connection | Allows users to view the **Secret Vault** area on the **Security** tab of the **Settings** page. |
| Suborg - create | Allows users to create sub-organizations when the "Suborgs - view" privilege is also granted. |
| Suborg - delete | Allows users to delete sub-organizations when the "Suborgs - view" privilege is also granted. |
| Suborg - update | Allows users to edit sub-organization settings when the "Suborgs - view" privilege is also granted. |
| Suborgs - link | Allows users to link sub-organizations when the "Suborgs - view" privilege is also granted. |
| Suborgs - manage licenses | Allows users to manage licenses for the organization's sub-organizations when the "Suborgs - view" privilege is also granted. |
| Suborgs - unlink | Allows users to unlink sub-organizations from the parent organization when the "Suborgs - view" privilege is also granted. |

| Feature privilege | Description |
|---|---|
| Suborgs - view | Allows users to view sub-organizations and switch into sub-organizations from the parent organization.<br>This privilege is required to create, delete, update, link, manage the licenses of, and unlink sub-organizations. |
| Upgrade SDI | Allows users to upgrade Data Integration-Free organizations to PayGo organizations.<br>For more information about Data Integration-Free and PayGo, see "Introducing Informatica Cloud Data Integration-Free and PayGo." |

## Application Integration feature privileges

Assign Application Integration feature privileges when you create custom roles for Application Integration and Application Integration Console.

**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 privileges for the folder and project assets.

The following table describes the Application Integration feature privileges:

| Feature privilege | Description |
|---|---|
| Administration | Gives users complete design-time and run-time administrative access to the Application Integration and Application Integration Console. Allows users to perform the following tasks:<br>- View, create, update, and delete all Application Integration assets.<br>- Manage and invoke services.<br>- Stop running processes.<br>- View instances and logs for deployed process.<br>- Deploy Process Developer BPR files to the Application Integration Console.<br>- Manage deployed catalogs.<br>- View WSDL files deployed across multiple systems.<br>- View Process Server metrics.<br>- Activate and deactivate process APIs.<br>- View, start, and stop event sources in listener-based connections.<br>**Note:** This privilege doesn't give users organization administration privileges. For example, a user with the only the Application Integration Administration privilege can't create sub-organizations. |
| Console Administration | Gives users near-complete access to the Application Integration Console. Allows users to perform the following tasks:<br>- View instances for deployed process.<br>- Stop running processes.<br>- View deployed Process Developer BPRs and catalogs.<br>- View WSDL files deployed across multiple systems.<br>- View Process Server metrics.<br>- Activate and deactivate process APIs.<br>- View, start, and stop event sources in listener-based connections.<br>This privilege doesn't allow users to deploy BPR files. |
| Data Viewer | Gives users access to detailed logs in the Application Integration Console.<br>For example, you might 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.<br>**Note:** The process logging level must be set to verbose to get detailed logs. |

| Feature privilege | Description |
|---|---|
| Development | Gives users the ability to debug processes. Allows users to perform the following tasks:<br>- View, create, update, and delete all Application Integration assets.<br>- Invoke services.<br>- View the **Detailed Process Instance** page on the Application Integration Console.<br>- Manage processes instances.<br>- Activate and deactivate process APIs.<br>- View, start, and stop event sources in listener-based connections. |
| Monitoring | Gives users the ability to view all parts of the Application Integration Console except for detailed logs. Allows users to perform the following tasks:<br>- Activate and deactivate process APIs.<br>- View, start, and stop event sources in listener-based connections. |
| Publish Application Integration Assets | Gives users the ability to publish Application Integration processes, guides, connections, and service connectors. |
| View Application Integration Console | Gives users access to the Application Integration Console.<br>You must assign this privilege to any role that has privileges that include working on the Application Integration Console. For example, assign this privilege with the Development privilege. |
| View Application Integration Designer | Gives users access to Application Integration.<br>You must assign this privilege to any role that has privileges that include working on the Application Integration Console. For example, assign this privilege with the Publish Application Integration Assets privilege. |

## Data Access Management feature privileges

Use the Data Access Management feature privileges to allow users access to specific functionality while working with Data Access Management. You can enable feature privileges when you create a custom role.

The following table describes the Data Access Management feature privileges:

| Feature | Description |
|---|---|
| Access Data Access Management | Allows users to see Data Access Management on the **My Services** page. |
| Approve data access policies | Allows users to read the following assets:<br>- Audit events<br>- Data classes<br>- Policies<br>- Rules<br>- Terms<br>- Transformations<br>Allows users to read, approve, and decline policy tasks. |

| Feature | Description |
|---|---|
| Curate data access policies | Allows users to create, read, edit, and delete the following assets:<br>- Policies<br>- Rules<br>- Transformations<br>Allows users to read and edit data classes.<br>Allows users to view audit events and terms. |
| Execute data access policies | Allows a user to run a mapping that includes a data access policy in Data Integration. |
| View data access policies | Allows users to read the following assets:<br>- Data classes<br>- Policies<br>- Rules<br>- Terms<br>- Transformations |
| Manage system settings | Allows users to change access control policy behavior, configure the data proxy, and view audit events. |

## Data Governance and Catalog feature privileges

Use the Data Governance and Catalog feature privileges to allow users access to specific functionality while working with Data Governance and Catalog. You can enable feature privileges when you create a custom role.

The following table describes the Data Governance and Catalog feature privileges:

| Feature | Description |
|---|---|
| Access Data Governance and Catalog application | Enable this feature to grant access to Data Governance and Catalog. If disabled, you cannot access Data Governance and Catalog to perform any governance tasks. |
| Curate Automatic Glossary Associations | Give users the ability to curate Glossary terms that appear as intelligent suggestions in Data Governance and Catalog. |
| Curate Data Classifications | Give users the ability to curate data classifications that appear as intelligent suggestions in Data Governance and Catalog. |
| Execute Data Access Management | Give users the ability to execute a mapping that includes an Access Policy transformation in Data Integration.<br>**Note:** This feature is for a future release. |
| Export | Give users the ability to export assets from Data Governance and Catalog in the Microsoft Excel format. |
| Import | Give users the ability to download predefined templates and import business assets into Data Governance and Catalog. If you enable this privilege, you must additionally grant users the following asset privileges to import assets:<br>- Business assets. Create and update privilege<br>- Technical assets. Update privilege |

| Feature | Description |
|---|---|
| Participate in Change Approvals | Allow users the following privileges:<br>- Participate in workflow approvals in Data Governance and Catalog.<br>The role for which you grant this privilege appears in the **Role** in Metadata Command Center when a user creates or modifies a workflow task.<br>- Add stakeholders to assets in Data Governance and Catalog.<br>- Configure workflows in Metadata Command Center. |
| Stakeholdership | Allow users the following privileges in Data Governance and Catalog:<br>- Be assigned as stakeholders for assets on the **Stakeholders** tab.<br>- Create or modify assets |
| Super Admin | Allows users access to unique administrator capabilities beyond the Governance Administrator role. |
| View Business Assets | Give users the ability to view business assets in Data Governance and Catalog. |
| View Data Access Audit | Give users the ability to view Data Access Management audit logs in Data Governance and Catalog.<br>**Note:** This feature is for a future release. |
| View Data Access Management | Give users the ability to view Data Access Management in Data Governance and Catalog. If you enable this privilege, you must additionally grant users any of the following asset privileges:<br>- Data Access Control assets<br>- Data De-Identification assets<br>- Data De-Identification technique assets<br>- Data De-Identification tier assets<br>- Data Filter assets<br>**Note:** This feature is for a future release. |
| View Data Classifications | Give users the ability to view data classification for technical assets in Data Governance and Catalog. |
| View Profiled Stats | Give users the ability to view profiling statistics for technical assets in Data Governance and Catalog. |
| View Sensitive Data | Give users the ability to view asset details that are classified as sensitive in Data Governance and Catalog. |
| View Technical Assets | Give users the ability to view technical assets in Data Governance and Catalog. |
| View Unpublished Content | Give users the ability to view assets that are in the unpublished state during an approval workflow process in Data Governance and Catalog. |

## Data Ingestion and Replication minimum asset and feature privileges

Assign Data Ingestion and Replication Database asset and feature privileges when you create custom roles for Data Ingestion and Replication Database.

To create, view, or edit database ingestion and replication tasks, assign a user role that includes the minimum required privileges. 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.

### Minimum asset privileges

The following table describes the minimum required asset privileges:

| Service | Asset type | Asset privileges |
|---|---|---|
| Data Ingestion and Replication | Database Ingestion Task | Create, Read, Update |
| Administrator | Connection | Read |
| Administrator | Secure Agent Group | Read |

### Minimum feature privileges

The following table describes the minimum required feature privileges:

| Service | Feature privileges |
|---|---|
| Administrator | Connectors - view |

## Data Integration asset and feature privileges

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

### Data Integration asset privileges

The following table describes the Data Integration asset privileges:

| Asset privilege | Description |
|---|---|
| API Collection | Allows users to create, read, update, delete, run, and set permissions on API collections. |
| Azure Data Sync Task | This privilege is not used. |
| Business Service Definition | Allows users to create, read, update, delete, and set permissions on business services. |
| Data Loader Task | Allows users to create, read, update, delete, run, and set permissions on data loader tasks. |
| Data Masking Task | Allows users to create, read, update, delete, run, and set permissions on data masking tasks. |
| Data Transfer Task | Allows users to create, read, update, delete, run, and set permissions on data transfer tasks. |
| Dynamic Mapping Task | Allows users to create, read, update, delete, run, and set permissions on dynamic mapping tasks. |
| File Listener | Allows users to create, read, update, delete, run, and set permissions on file listeners. |
| Fixed-Width File Format | Allows users to create, read, update, delete, run, and set permissions on fixed-width file formats. |

| Asset privilege | Description |
|---|---|
| Hierarchical Schema | Allows users to create, read, update, delete, run, and set permissions on hierarchical schemas. |
| Industry Data Services | Allows users to create, read, update, delete, run, and set permissions on industry data service customizers. |
| Intelligent Structure Task | Allows users to create, read, update, delete, run, and set permissions on intelligent structure models. |
| Linear Taskflow | Allows users to create, read, update, delete, run, and set permissions on linear taskflows. |
| Mapping | Allows users to create, read, update, delete, run, and set permissions on mappings.<br>To run a mapping, users must have Run permission on both mappings and mapping tasks. |
| Mapping Task | Allows users to create, read, update, delete, run, and set permissions on mapping tasks.<br>To run a mapping task, users must have Run permission on both mappings and mapping tasks. |
| Mapplet | Allows users to create, read, update, delete, run, and set permissions on mapplets. |
| PowerCenter task | Allows users to create, read, update, delete, run, and set permissions on PowerCenter tasks. |
| Replication Task | Allows users to create, read, update, delete, run, and set permissions on replication tasks. |
| Saved Query | Allows users to create, read, update, delete, run, and set permissions on saved queries. |
| Sequence Generator | Allows users to create, read, update, delete, and set permissions on shared sequences. |
| Swagger | Allows users to create, read, update, and delete Swagger files. |
| Synchronization Task | Allows users to create, read, update, delete, run, and set permissions on synchronization tasks. |
| Taskflow | Allows users to create, read, update, delete, run, and set permissions on taskflows. |
| User-Defined Function | Allows users to create, read, update, delete, run, and set permissions on user-defined functions. |
| Visio Template | Allows users to create, read, update, delete, run, and set permissions on Visio templates. |

### Data Integration feature privileges

The following table describes the Data Integration feature privileges:

| Feature privilege | Description |
|---|---|
| Access CDI error logs | Allows users to preview error rows files from the **All Jobs**, **Running Jobs**, and **My Jobs** pages, and from the job details. |
| Data - preview | Allows users to preview data in mappings and when they run SQL ELT optimization data preview jobs. |
| EDC for IICS Discovery | Allows users to use data catalog discovery to find objects from Enterprise Data Catalog and use them in mappings and some types of tasks.<br>**Note:** Before users can perform data catalog discovery, you must configure the Enterprise Data Catalog integration properties on the **Organization** page. |

## Data Marketplace feature privileges

View the features privileges in Informatica Intelligent Cloud Services Administrator that are available to a user role for the Data Marketplace service.

The following table describes the Data Marketplace feature privileges:

| Feature | Description |
|---|---|
| Access Data Marketplace application | Display Data Marketplace in the Informatica Intelligent Cloud Services **My Services** page. |
| Approve data collection order | Approve a Data User's request to gain access to a Data Marketplace. |
| Bulk import data categories | Create multiple new categories at once in Data Marketplace. |
| Bulk import data collections | Create multiple new data collections at once in Data Marketplace. |
| Curate consumer access | Curate consumer accesses in Data Marketplace. |
| Curate data categories | Curate categories in Data Marketplace. |
| Curate data collections | Curate data collections in Data Marketplace. |
| Curate delivery targets | Curate the delivery targets of a data collection. |
| Curate delivery templates | Curate the delivery templates in Data Marketplace. |
| Fulfill data collection order | Grant data collection access to a Data User that ordered the data collection. |
| Manage application options | Configure the various settings of Data Marketplace. |
| Order data collection | Request access to a data collection. |
| View data categories | View categories in Data Marketplace. |
| View data collections | View data collections in Data Marketplace. |

# Data Profiling feature privileges

Use the Data Profiling feature privileges to allow users access to specific functionality while working with Data Profilingassets. You can enable asset and feature privileges when you create a custom role.

The following table describes the Data Profiling feature privileges:

| Privilege | Description |
|---|---|
| Data Profiling | Create, read, update, delete, run, and set permissions for a data profiling task. |
| Data Profiling - Compare Columns | Compare columns in a profile run. |
| Data Profiling - Compare Data Profiling Runs | Compare multiple profile runs. |
| Data Profiling - Data Profiling Results - View* | - View the profiling results for a data profiling task for any user including the user who created the data profiling task.<br>- View the valid and invalid rows in the Data Governance and Catalog scorecard using the **Preview of Successful Rows** and **Preview of Unsuccessful Rows**. |
| Data Profiling - Drill down* | View and select the drill-down option when you create a data profiling task. |
| Data Profiling - Export Data Profiling Results | Export the profiling results to a Microsoft Excel file. |
| Data Profiling - Manage Rules | Add or delete rules for a data profiling task. |
| Data Profiling - Query - Create | Create a query. |
| Data Profiling - Query - Submit | Run a query and view query results. |
| Data Integration - Data Preview | View source object data in the **Data Preview** area. |
| Data Profiling<br>Sensitive Data - view | Hide sensitive information for a particular user role. When the **Sensitive Data - view** privilege is configured, you cannot view the minimum value, maximum value, and most frequent values information in the **compare column** tab. |
| Data Profiling<br>Disable Data Value Storage | Does not store minimum, maximum, and most frequent values in the profiling warehouse. When you configure the **Disable Data Value Storage** feature, the sensitive information is not stored in the profile results and the source system. The values are not stored even if you have permissions to view the sensitive data, or if you configure a profiling task with the **Maximum Number of Value Frequency Pairs** option. By default, this feature is disabled. When the feature is disabled, the values are stored as expected. |
| * To perform drill down, and to view the **Preview of Successful Rows** and **Preview of Unsuccessful Rows** in a Data Governance and Catalog scorecard, you need the following privileges:<br>- Data Profiling - Query - Create<br>- Data Profiling - Query - Submit<br>- Data Profiling - Data Profiling Results - View<br>- Data Profiling Sensitive Data - view | |

The following table describes how the **Disable Data Value Storage** and **Sensitive Data- view** features function when you configure for different user roles:

| Features | Custom role | Administrator or Designer | Result |
|---|---|---|---|
| Disable Data Value Storage | Inactive | Active | Sensitive information is not stored. |
| | Active | Inactive | Sensitive information is not stored. |
| Sensitive Data- view | Inactive | Active | Sensitive information is displayed. |
| | Active | Inactive | Sensitive information is displayed. |

**Note:** When you activate the **Disable Data Value Storage** feature, Data Profiling or the source system does not store the sensitive information.

## Data Quality feature privileges

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

The Data Quality feature privileges are enabled by default for the Admin and Designer roles.

The following table describes the Data Quality feature privileges:

| Feature privilege | Description |
|---|---|
| Data Preview - Dictionaries | Allows users to view the contents of a dictionary in the following cases:<br>- The user opens the dictionary from the **Explore** page.<br>- The user selects the dictionary in a Data Quality asset. |
| Data Preview - Test Panel | Allows users to view data in the Test panel in a Data Quality asset.<br>**Note:** To run a test in a Data Quality asset, your role must also have the **Run** privilege for mappings in Data Integration. |
| Exceptions Data - Delete | Enables users 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 | Enables users 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. |

**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.

# Domain Management Service asset and feature privileges

Use the Domain Management Service asset and feature privileges to allow users access to specific functionality while working with CDI-PC. You can enable asset and feature privileges when you create a custom role.

**Important:** You must assign Read access on the Secure Agent and Secure Agent Group assets to the user's role. To do this, select the Administrator service and assign Read privilege for the assets.

## Domain Registration asset privileges

The following table describes the Domain Registration asset privileges:

| Asset privilege | Description |
|---|---|
| Read | Allows users to view registered domains and domain details. |
| Create | Allows users to perform the following tasks:<br>- View registered domains and domain details.<br>- Register a domain.<br>- Deregister a domain.<br>- Retry registration.<br>- Edit domain details.<br>- Reconcile a domain.<br>Create includes the Read and Update privileges. |
| Update | Allows users to perform the following tasks:<br>- View registered domains and domain details.<br>- Deregister a domain.<br>- Retry registration.<br>- Edit domain details.<br>- Reconcile a domain.<br>Update includes the Read privilege. |
| Delete | Allows users to perform the following tasks:<br>- View registered domains and domain details.<br>- Delete a deregistered domain.<br>Delete includes the Read privilege. |

## Domain Registration feature privileges

The following table describes the Domain Registration feature privileges:

| Domain Registration feature privilege | Description |
|---|---|
| Domain Update | Allows users to update a domain. |

# Human Task asset and feature privileges

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

## Human Task asset privileges

The following table describes the Human Task asset privileges:

| Asset privilege | Description |
|---|---|
| Human Task Assets | Allows users to perform the following actions:<br>- Create, read, update, or delete human task assets.<br>- Run processes that contain Human Task steps, which generate human tasks.<br>- Assign permissions to other user roles so that they can access human task assets. |

## Human Task feature privileges

The following table describes the Human Task feature privileges:

| Feature privilege | Description |
|---|---|
| Development | Allows users to create and edit human task assets and use Human Task steps in Application Integration processes. |
| View Human Task Application | Allows users to view and access the Human Task service. |
| View Tasks | Allows users to access the Human Task Inbox in the Human Task service. |

# Metadata Command Center feature privileges

Use Metadata Command Center feature privileges to allow users access to specific functionality while working with Metadata Command Center. You can enable feature privileges when you create a custom role.

The following table describes the Metadata Command Center feature privileges:

| Feature | Description |
|---|---|
| Access Metadata Command Center application | Grants access to Metadata Command Center. If disabled, users can't access Metadata Command Center. |
| Asset Page Customization | Allows users to modify the layout of pages and preview panes of assets. Allow users to assign default layouts to other users based on their roles, user groups, or to all users in the organization. |
| Manage Access Control | Allows users to assign asset privileges and feature privileges to other users. |
| Manage IDMC Metadata Settings | Allows users to synchronize metadata from Data Integration tasks and Application Integration objects with the catalog. |

| Feature | Description |
|---|---|
| Manage Connection Assignments | Allows users to perform the following tasks:<br>- Assign or unassign connections to one or more catalog sources in Metadata Command Center.<br>- Link catalog sources to generate lineage in Metadata Command Center. |
| Manage Custom Attributes | Allows users to manage asset relationships, predefined attributes, and custom attributes for asset types that appear in Data Governance and Catalog. |
| Manage Data Classifications | Allows users to create and manage data classification inclusion rules in Metadata Command Center. |
| Manage Reference Data | Allows users to import and publish lookup tables that you can use in data classification in Metadata Command Center. |
| Manage System Settings | Allows users to modify system settings in Metadata Command Center. |
| Manage Upgrade | Allows users to initiate upgrades to the latest version of Data Governance and Catalog. |
| Manage Workflow Settings | Allows users to create or modify workflows in Metadata Command Center. |
| Monitor Jobs | Allows users to monitor jobs in Metadata Command Center. |
| Super Admin | Allows users access to unique administrator capabilities beyond the Governance Administrator role. |
| View Custom Attributes | Allows users to view attributes for asset types in Data Governance and Catalog. |
| View Data Classifications | Allows users to view data classifications in Data Governance and Catalog after you enable the capability and run the catalog source job in Metadata Command Center. |
| View Reference Data | Allows users to view reference data in Data Governance and Catalog. |

# Model Serve asset and feature privileges

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

## Model Serve asset privileges

The following table describes the Model Serve asset privileges:

| Asset privilege | Description |
|---|---|
| Machine Learning Model | Allows users to create, read, update, delete, run, and set permissions on machine learning models. |
| Model Deployment | Allows users to create, read, update, delete, run, and set permissions on model deployments.<br>To run a model deployment, users must have Run permission on both machine learning models and model deployments. |

### Model Serve feature privileges

The following table describes the Model Serve feature privileges:

| Feature privilege | Description |
|---|---|
| Predictions | Allows users to access the URL endpoint that generates predictions from a machine learning model. |

## Monitor feature privileges

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

The following table describes the Monitor feature privileges:

| Feature privilege | Description |
|---|---|
| Job Results - view | Allows users to view job results on the **All Jobs**, **Running Jobs**, and **My Jobs** pages. |
| Logs - View and Download | Allows users to view and download job log files. |

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**.

CHAPTER 9

# Editing your user settings

In your user settings, configure the types of notifications you receive and set your source code credentials.

To access user settings, click the **User** icon on the toolbar and then select **Settings**.

The user settings page includes the following sections:

**Notification settings**

The **Notification Settings** section lists categories of notifications that you're eligible to receive. You can configure which notifications you receive by email each time an event occurs, which notifications you receive in a summary email, and how often you receive a summary email.

**Source Code Control Credentials**

In the **Source Code Control Credentials** section, you can configure your repository credentials that allow you to work with source controlled object.

CHAPTER 10

# Inviting users to join your organization

If you have an appropriate role, you can invite users to join your organization when you configure a runtime environment or primary cloud data warehouse. Invite users to join your organization so they can help you set up a runtime environment or connect to your cloud data warehouse.

To invite users to join your organization, click **Invite a friend or colleague to help you**. To invite users, you must have the Admin role, or you must have the Designer role and a custom role that has the "read role" and "create user" Administrator asset privileges. You must assign the user you invite the Admin or Designer role.

If you don't see the **Invite a friend or colleague to help you** option or you want to assign the user a different role, you can add a user on the **Users** page in Administrator.

1. Click **Invite a friend or colleague to help you**.
2. Enter the first name, last name, email address, user name, and role for the person you want to invite.

   The user name must be unique within the organization. You cannot change the user name after you invite the user.
3. Click **OK**.

   The user you invite receives an email with a link to join your organization.

CHAPTER 11

# Notifications

You receive notifications in Informatica Intelligent Cloud Services for certain events, including job status updates, license expiration, and workflow progress. You can view notifications in the notifications tray, manage them on the **Notifications** page, and receive alerts by email.

The Notifications icon on the toolbar displays the number of unread notifications. You can click the icon to view the latest unread notifications in the notifications tray. In Data Governance and Catalog, you can filter the tray to display only Data Governance and Catalog notifications. In other services, filtering the tray doesn't change the display.

You can view and manage all of your notifications on the **Notifications** page. To access the **Notifications** page, select **View All Unread** from the action menu in the notifications tray.

To receive notification alerts by email, configure the options in your user settings. For more information, see Chapter 9, “Editing your user settings” on page 80.

# INDEX

## S



## T



## U



## W