Unit- 2

IICS Sub-organization

Content:

i. IICS Sub-organization
ii. User Management
iii. IICS Runtime Environment

IICS Sub-Organization: Organization Hierarchy

- The IICS Organization is a secure section of the Informatica Cloud repository where you can store data and objects.
- An organization hierarchy is a hierarchy of related organizations.
- It includes a parent organization and one or more sub-organizations.
- To create an organization hierarchy, the parent organization must have the Org hierarchy license. The Administrator of the parent organization can create and manage organizations and the organization hierarchy.
- A user in one Org in the hierarchy cannot log into another Org in the hierarchy without a user account for the other Org. Administrator of the parent organization can create and manage organizations and organization hierarchy.

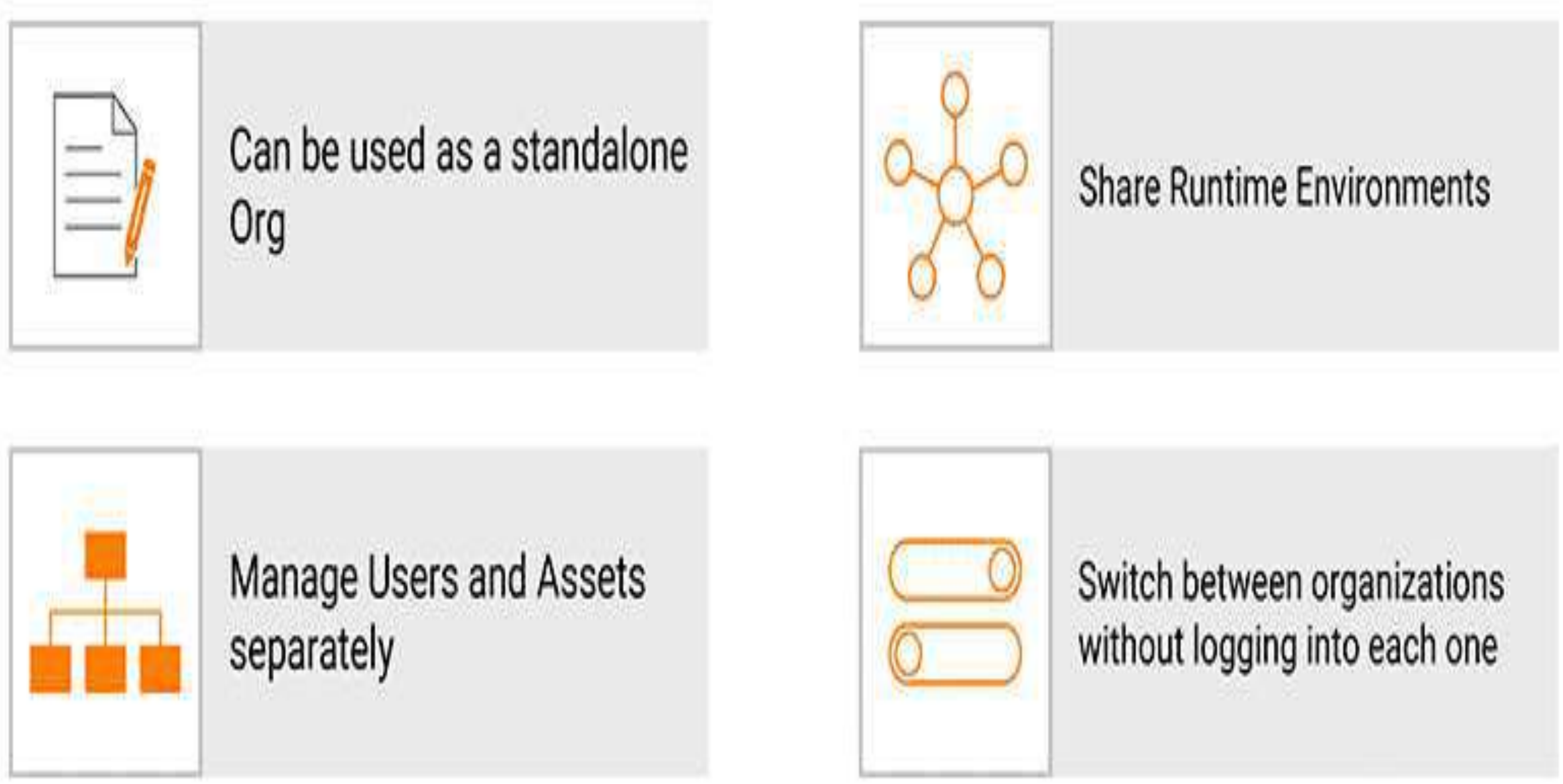
Sub Organizations

- A sub-organization is an Informatica Cloud Org, that is related to the parent organization as part of the organization hierarchy.
- The sub-organization inherits all licenses and subscriptions of the parent organization, except for an Org hierarchy license.
- A sub-organization cannot act as a parent for any other organization or be a part of another organization hierarchy.

Sub Organizations: cont…

- An organization hierarchy can include a limited number of sub-organizations. If you want to increase the number of sub-organizations for the Org, you can contact Informatica Global Support.
- When you create a sub-organization, you must also configure sub-organizations security and create user accounts for the sub-organization. Each sub-organization has its own set of users and assets.
- Note: The Administrator of the parent organization can create a sub-organization.

Advantages of Creating Sub-Organizations



Can be used as a standalone Org

Share Runtime Environments

Manage Users and Assets separately

Switch between organizations without logging into each one

Creating Sub-Organization

Adding a Sub Organization

- To Add a sub-organization, you can create a sub-organization or link existing organizations.
- To create a sub-organization, log in to the organization that you want to be the parent organization and create a sub-organization. The organization you link from becomes the parent organization and the organization that you link to becomes a sub-organization.

Creating a Sub-Organization

1. Log in to the parent IICS organization.
2. From Administrator service home page, select **Organization**.
3. In the Sub-Organizations tab, click **New Sub-Organization**.
4. Enter the properties for the sub-organization such as, Name, Environment Type, Address, and so on.
5. Click **Save**.

Conditions to Link Sub-Organizations

You can link an organization if all the following conditions apply:

i. You have a user account with the organization.

ii. The organization is not the parent of another organization or a sub-organization of another organization.

iii. You are the administrator of the parent organization, and the parent organization has the license to create sub-organizations.

iv. The organization that you want to link as a sub-organization does not have the license to create sub-organizations.

Steps to Link Sub-Organizations:

1. In the Sub-Organizations tab, click **Link Sub-Organization**.
2. In the Link Sub-Organization dialog box, enter the following information:
   - Organization ID
   - User Name
   - Password
3. Click **Link Sub-Organization**.

Restrict Access to Sub-Organization

- You can use the **Deny parent organization access to this sub-organization** option to restrict users in the parent Org from switching to the sub-organization.
- Parent Org users with relevant privileges can make the changes such as enabling and disabling the sub-organization, updating the sub-organization licenses, and editing the sub-organization properties such as the organization description and CLAIRE recommendation preferences.

Switching between Sub-Organizations

- A user with privileges to view sub-organizations or an Administrator in parent Org can switch among organizations.
- To switch between the different organization, select the sub-organization to navigate to from the Organization drop-down.
- When you switch to a sub-organization, the following operations cannot be performed:
  - Create or import data transfer tasks
  - Create or import dynamic mapping tasks
  - Validate or run taskflows

Sub-Organization Licenses

Managing License

- A sub-organization has licenses that are maintained by the parent organization.
- When you create a sub-organization, each sub-organization inherits licenses from the parent organization as custom licenses.
- An Administrator of the parent organization can edit sub-organization licenses. You can manage the licenses of Sub-Organization in one of the following ways:
- The administrator of the parent organization can edit the sub-organization's licenses manually.
- Sub-organization licenses can be synchronized with the parent's organization automatically.

Sub-Organization Licenses: cont…

- If a sub-organization requires a license that does not belong to the parent organization, contact Informatica Global Customer Support to obtain the license for the parent organization.
- The sub-organization inherits all licenses except for the following licenses:
- The license to create sub-organizations.
- Bundle licenses. To use a bundle in the sub-organization, a user in the sub-organization must install the bundle.

Editing Sub-Organization Licenses

From Parent Organization

Follow the below steps to edit licenses from within the parent organization:

1. In the Sub-Organization tab, select the Sub-org for which you edit the license
2. Click **Licenses** tab.
3. Select licenses to enable features, and clear licenses to disable features.
4. Optionally, you can modify expiration dates.
   a. All licenses must have expiration dates. You cannot extend a license past its original expiration date.

Editing Sub-Organization Licenses

From within the Sub-Org

Follow the below steps to edit licenses from within the sub-organization:

1. From the Organization menu, navigate to the sub-org.
2. In the Administrator service, select the **Licenses** tab.
3. Select licenses to enable features, and clear licenses to disable features.
4. Optionally, modify expiration dates.

Synchronizing Licenses with the Parent Organization

- Synchronizes the new or modified licenses in the parent organization, with all the sub-organizations. The parent organization administrator does not have to take any action to synchronize the licenses.
- When the synchronizing license feature is enabled and then you disable a sub-organization, the sub-organization loses its license settings. When you re-enable the sub-organization, the sub-organization inherits all license settings from the parent organization.
- You need to contact Informatica Global Customer Support to enable the license synchronization feature for your IICS account.
- When the license for this feature is enabled, you cannot edit sub-organization licenses individually.

Working with Sub-Organizations

- **Actions on Sub-Organization**

After the sub-organization is created, you can perform the following actions on it:

- Unlink
- Delete
- Disable

Unlink Sub-Organization

- You can unlink a sub-organization if all the following conditions apply:

i. You have an administrator account in the sub-organization you want to unlink

ii. You must be the Administrator of the parent organization and the parent organization must have the Org hierarchy license

iii. No asset in the sub-organization uses a shared Secure Agent group as the runtime environment

Delete Sub-Organization

- When you delete a sub-organization, you delete all the associated data.
- You can delete a sub-organization, if you are the administrator of the parent organization.

Enable/Disable Sub-Organization

When the sub-organization is disabled:

- The organization remains active.
- Sub-organization users cannot log in to Org.
- Jobs scheduled in the Sub-organization cannot run.

When the sub-organization is enabled:

- The sub-organization users can log into it.
- Users can access assets and perform tasks based on their user roles.
- Jobs scheduled in the Sub-organization run successfully.

User Management

- You can create a combination of user, roles, and user groups, to assign access to assets in your IDMC organization. The IICS Administrator service allows you to create users, user groups, and user roles.

- A user is an individual account in IDMC, 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.
- A role defines the general tasks that the user can perform within the organization. For example, users with Admin role can create and manage users.

- A user group defines the objects that the user can work with and the tasks the user can perform on objects. For example, a user can only read and use connections in a task but cannot create new connections.

User Authentication

IDMC uses the following types of user authentication:

1. **Native:**
   - Native users log in to IDMC through the login page using user names and passwords.
   - They are authenticated through Informatica Intelligent Cloud Services.
2. **Salesforce:**
   - Salesforce users sign in to IDMC through Salesforce or a Salesforce app.
   - They are authenticated through Salesforce.
3. **SAML:**
   - SAML users sign in to IDMC through their identity provider.
   - They are authenticated through their identity provider.

Creating Users

Administrators can create and configure user accounts on the Users page of the Administrator service.

To create a user in IICS, perform the following steps:

1. In the **Administrator** service, navigate to the **Users** tab, and click **Add User**.
2. In the New User window, enter user details and set the authentication type, and value for max login attempts. In IICS, the following user types are supported to authenticate the user:
   1. Native
   2. Salesforce
   3. SAML (Security Assertion Markup Language)
3. Assign role to the user. You can assign system-defined and custom roles to a user.
4. Optionally, you can assign a user group to the user. If you assign a group, the user inherits all roles that are associated with the group.
5. Save the configuration. You will need to confirm the user account using the email sent to the registered email Id. While confirming the account, you will be prompted to set the user password to log in to IICS.

Creating Users: cont…

After the user creation, its status is set to one of the following based on the authentication method:

- Native Authentication:
  - Set to Pending Activation.
  - The user receives a confirmation email to set user credentials.
  - After confirmation, the status changes to Enabled.
- Salesforce Authentication:
  - Set to Pending Activation.
  - To activate using the verification code, the user needs to enter the verification code in Salesforce.
  - To activate using Salesforce Oauth, the user needs to click on confirm account link and login to Salesforce.
- SAML Authentication
  - Set to Enabled.
  - The user can sign in through the user's identity provider.

User Actions

You can perform the following actions on a user in IICS:

- View and edit user details
- Assign and unassign services to a user
- Disable a user
- Reset a user
- Reassign scheduled jobs
- Delete a user

View and Edit User

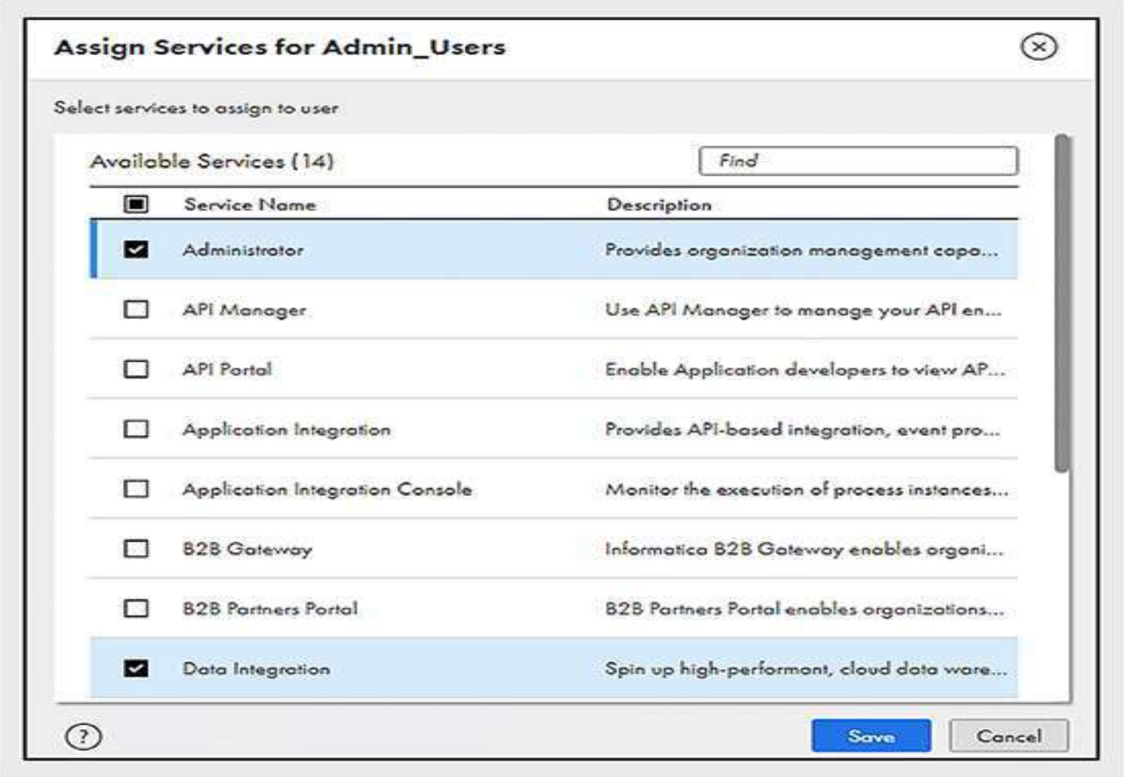
You can view and edit user details by clicking on the user’s user name, which opens the user configuration page.

- In the user configuration page, you can perform the following actions:
- To update the email associated with the user, click the **Update Email** option. After the email is updated, IICS sends a verification email to the new email address with a verification link that is valid for 24 hours.
- Change the value of Max login attempts for the user. It indicates the maximum number of login attempts that the user can make before the user is locked out. If the user gets locked out, click the **Forgot your password link** on the Login page, or the organization administrator can reset the user.
- Enable **Force password reset on the next login** to ensure the user resets the password the next time the user tries to log in.
- Assign new role or user group to a user.
- Unassigned exiting role or user group to a user.

Assign and Unassign Services

To allow or prevent a user from accessing certain services, you can assign or unassign the services to the user.

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



Assign Services for Admin_Users

Select services to assign to user

Available Services (14)

■	Service Name	Description
☑	Administrator	Provides organization management capa...
□	API Manager	Use API Manager to manage your API en...
□	API Portal	Enable Application developers to view AP...
□	Application Integration	Provides API-based integration, event pro...
□	Application Integration Console	Monitor the execution of process instances...
□	B2B Gateway	Informatica B2B Gateway enables organi...
□	B2B Partners Portal	B2B Partners Portal enables organizations...
☑	Data Integration	Spin up high-performant, cloud data ware...

Assign and Unassign Services

- When you unassign a service, the user cannot see the service on the **My Services page**. The user cannot access or use the service regardless of the user's role.
- To assign/unassign services to a user, perform the following steps:

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

Disable User

- You can disable a user on the Users page. When you disable a user, the user can no longer log in to IICS.
- If the disabled user has any scheduled tasks assigned to it, the scheduled job fails. So, the administrator must reassign the scheduled job to another user before disabling a user.
- When you disable a user, you can still view the user details but cannot edit them.
- To disable a user perform the2 following steps:
  1. In Administrator, select **Users**.
  2. In the row that contains the user whom you want to disable, click **Actions** and select **Disable**.

Reset User

- When you reset a user, its status is set to Pending Activation or Enabled based on the authentication method.
- To reset a user, select the user, and from the **Actions** menu, select **Reset**.

Reassign Jobs

You can reassign a user’s job in the following scenarios:

- When the owner of assets leave the organization
- The user needs to be disabled
- Change in user’s responsibilities

To reassign the scheduled job, perform the following steps:

- Select the user for which you want to reassign the job and select **Reassign Scheduled Jobs**.
- Select the user to reassign the scheduled jobs. The selected user must be an enabled user.
- Click **Reassign**.

Delete User

- When a user is deleted, it is removed from the organization and from the IICS repository.
- To delete a user, select the user you want to delete, click **Actions** and select **Delete**.
- If your organization uses SAML for authentication and authorization, you cannot delete a SAML user that is not created in Administrator.

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

Managing User Profile

- The **Profile** page is used to update the details of the user currently logged into IICS.
- You can access the Profile page by clicking on the User icon in the top right corner of the IICS interface.

You can update the following information in the Profile page:

i. First and last name
ii. Job title
iii. Email address
iv. Phone number
v. Time zone (used in the job execution time stamp)
vi. Password
vii. Security question and answer

User Statistics

- **List View**
  - To view user statistics for your organization, you must have the Admin role, or the Read User and Audit log - view privileges.
  - 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 active users in a certain time period.

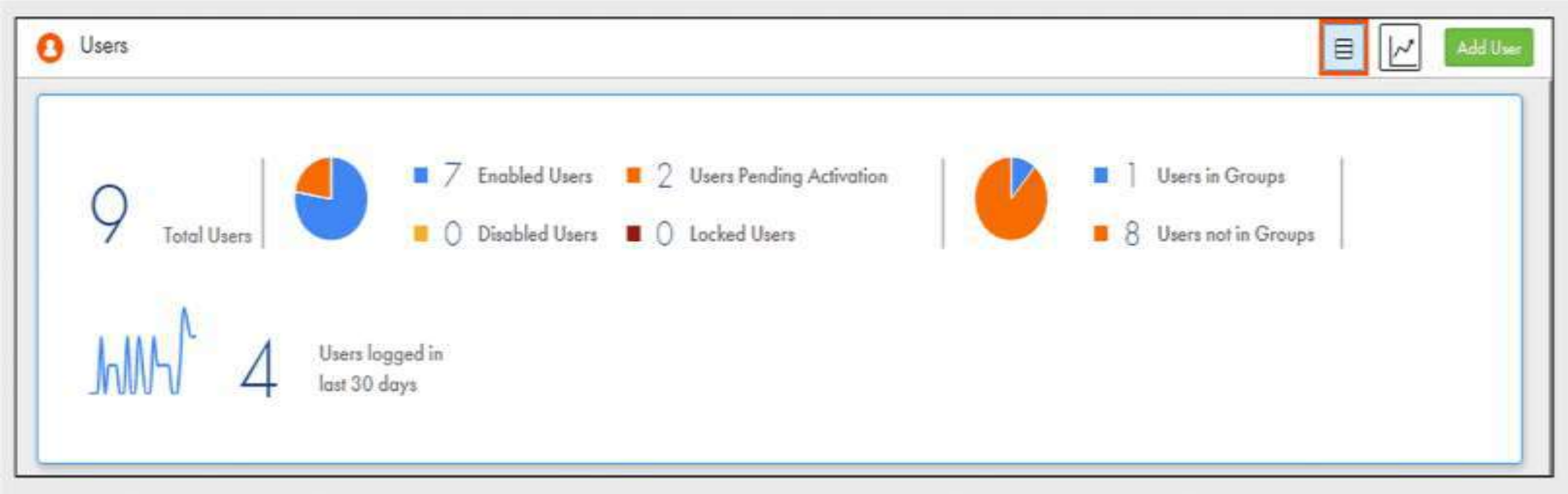
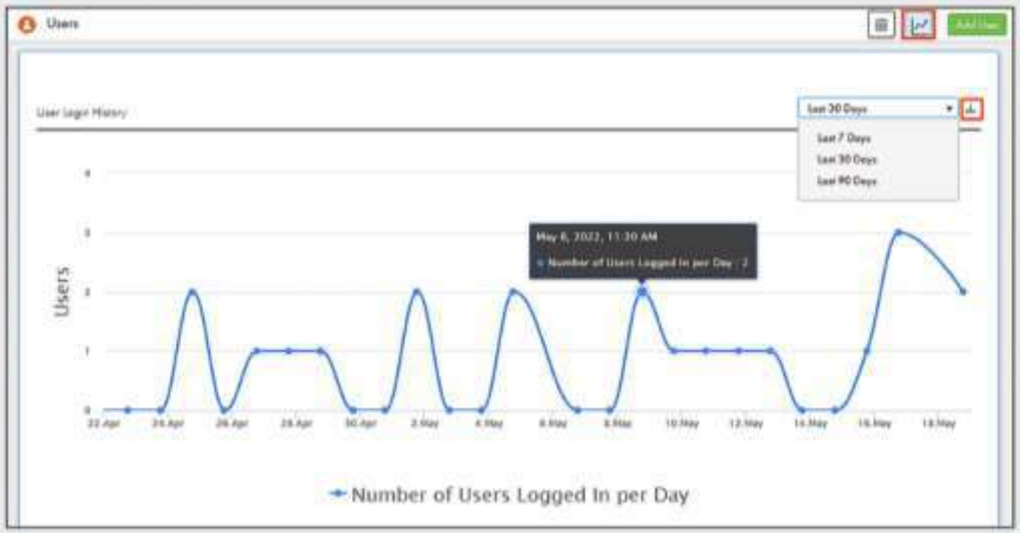
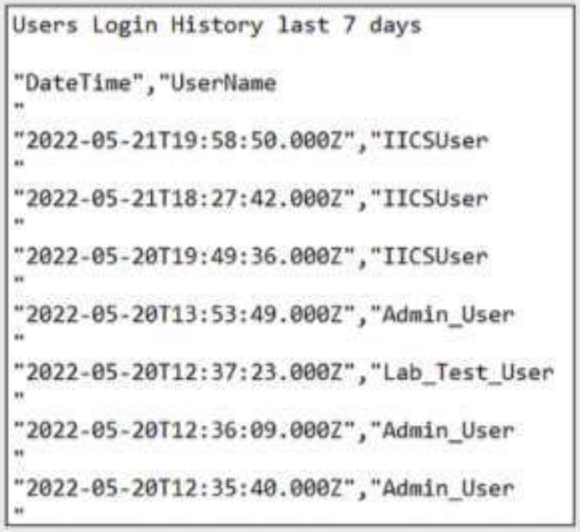


Chart View

- You can also view the user statistics in graphical form. To view the graph, click on **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 specified time period using the download icon next to the time period selector drop-down.





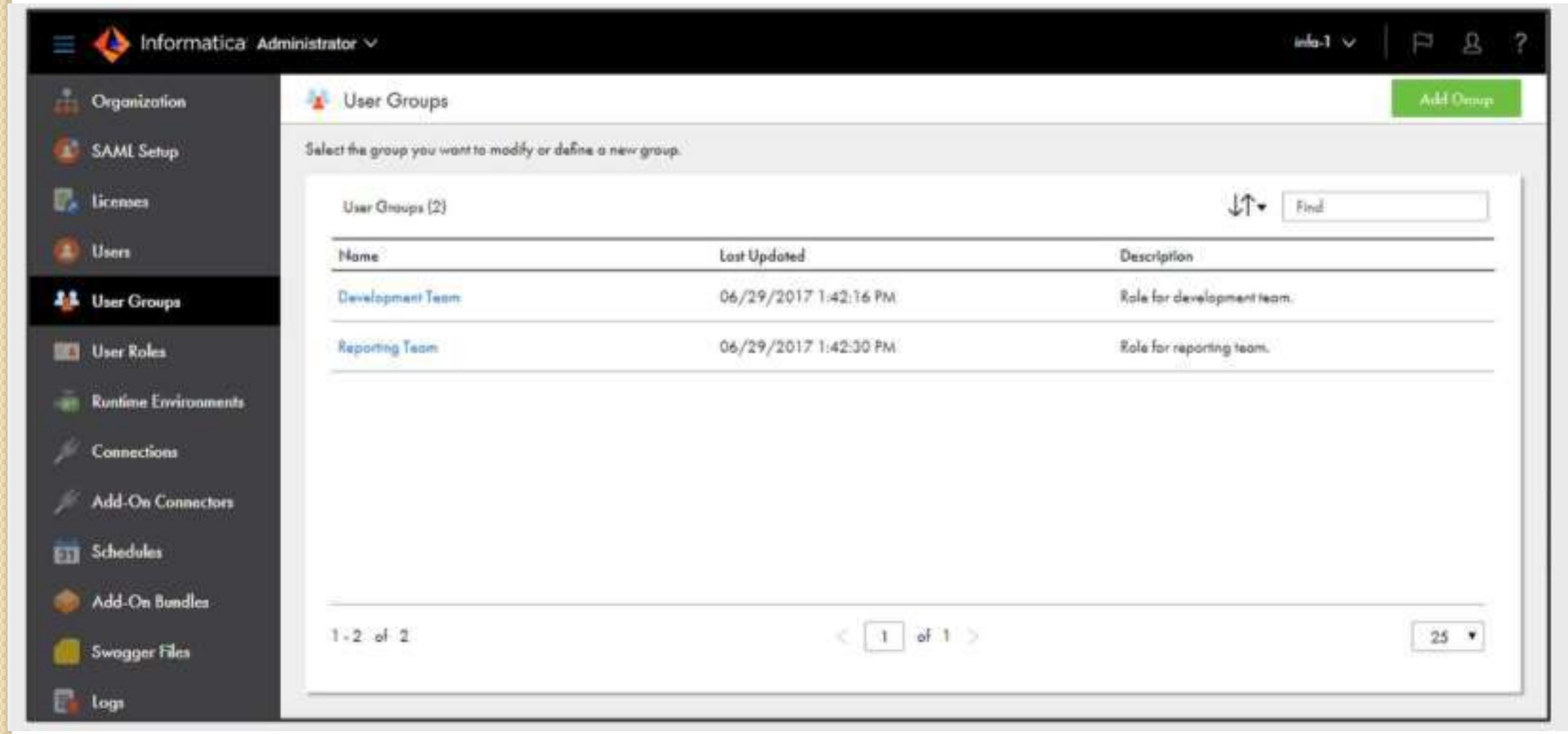
```
Users Login History last 7 days

"DateTime","UserName
"
"2022-05-21T19:58:50.000Z","IICSUser
"
"2022-05-21T18:27:42.000Z","IICSUser
"
"2022-05-20T19:49:36.000Z","IICSUser
"
"2022-05-20T13:53:49.000Z","Admin_User
"
"2022-05-20T12:37:23.000Z","Lab_Test_User
"
"2022-05-20T12:36:09.000Z","Admin_User
"
"2022-05-20T12:35:40.000Z","Admin_User
"
```

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 the Administrator assigns to the group.
- The Administrator can view and edit user group details, create a group, rename a group, and delete a group.
- To view the User Groups page, in the Administrator Service, select **User Groups**.

User Groups

- The Administrator can view and edit user group details, create a group, rename a group, and delete a group.
- To view the User Groups page, in the Administrator Service, select **User Groups**.



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

User Groups (2)

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

Creating User Group

Find below the steps to create a User group:

1. In the Administrator service, navigate to the **User Groups** tab.
2. From the User Groups page, select **Add Group**.
3. Here, enter a group name. It must be unique within an organization.
4. Select the roles to assign to the group.
   - Optionally, assign users to the group.
   - If the available users list does not include SAML users. You cannot assign SAML users to a group.
5. Save the group.

Actions on User Group

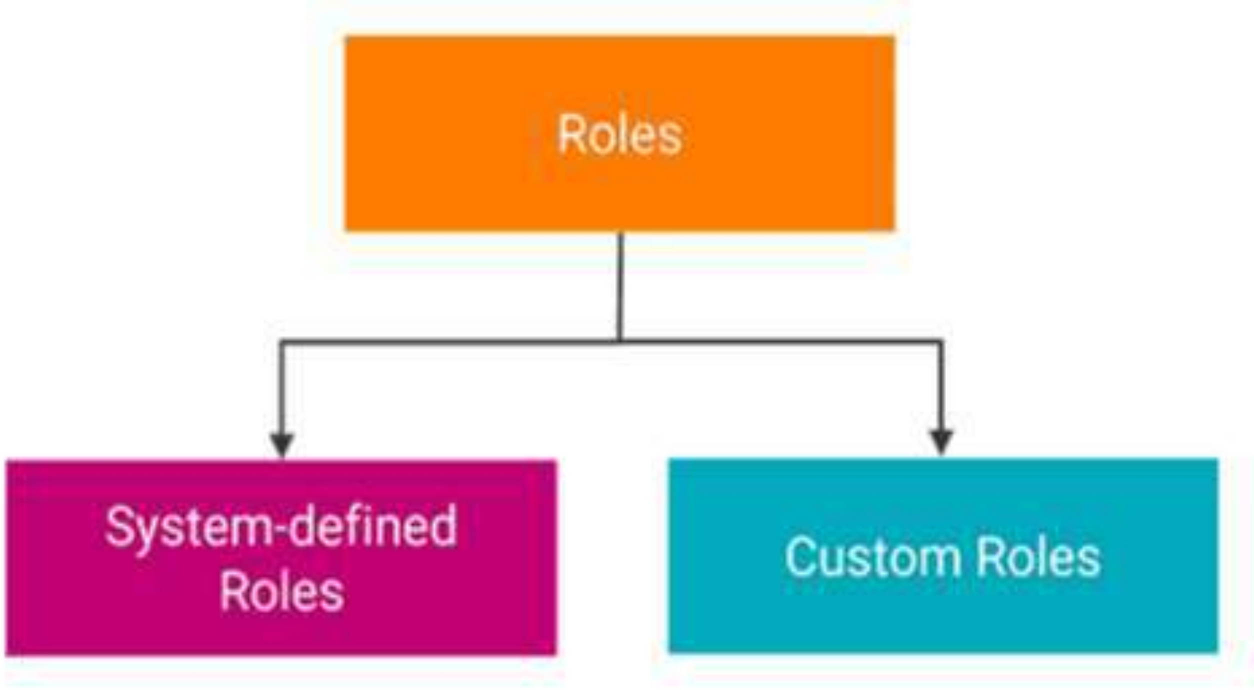
- To rename a group, in the row that contains the user group, click **Actions** and select **Rename.**
- To delete a group, in the row that contains the user group, click **Actions** and select **Delete**.
- Note: You cannot rename or delete a SAML user group.

User Roles

What is a Role?

- A role is a set of privileges that allows a user to perform tasks in the organization. Roles determine the functionalities available to a user. For example, to perform Administrative tasks, the user must have the Admin role.
- You must assign each user in the Org at least one role. While there is no technical limitation on assigning multiple roles to a single user, the best practice is to assign only one role to each user.
- In IICS, you can assign a system-defined role or a custom role to a user.
- You can view existing roles, or create a new role on the User Roles page of the Administrator service.

Types of Role:



System-defined Roles

- System-defined roles are pre-defined roles that define access privileges for the services your organization uses. You cannot edit, rename, or delete system-defined roles. You can clone system-defined roles except for the Admin role.

There are two types of system-defined roles:

- **Cross service roles:**
  Defines access privileges across multiple services. In IICS, the following roles are cross-service roles:
  - Admin
  - Data Integration Data Previewer
  - Deployer
  - Designer
  - Monitor
  - Operator
  - Service Consumer
- **EXAMPLE:** A user with the Designer role can create assets and tasks in Data Integration, Cloud Integration Hub, and Application Integration, and can also access the Application Integration Console.

System-defined Roles: cont…

- **Service specific roles:**
  Defines access privileges for one service, or for a group of closely related services.
- **EXAMPLE:** The service-specific roles for Application Integration provide access to both Application Integration and Application Integration Console.
- It is recommended to assign service-specific roles to users who do not need access across multiple services.

Custom Roles

- You can create a custom role based on the business requirements of your organization. For example, you can create a custom administrator role that can configure roles, user groups, and access control, but cannot create, edit, or run Data Integration tasks.
- You can edit, rename, and delete custom roles after you create them.
- To create custom roles, your organization must have the **Custom Roles** license.
- Custom roles cannot be assigned privileges to create, update, or delete roles. If you need to modify roles, log in to IICS as a user with the system-defined Admin role.

Creating a Custom Role

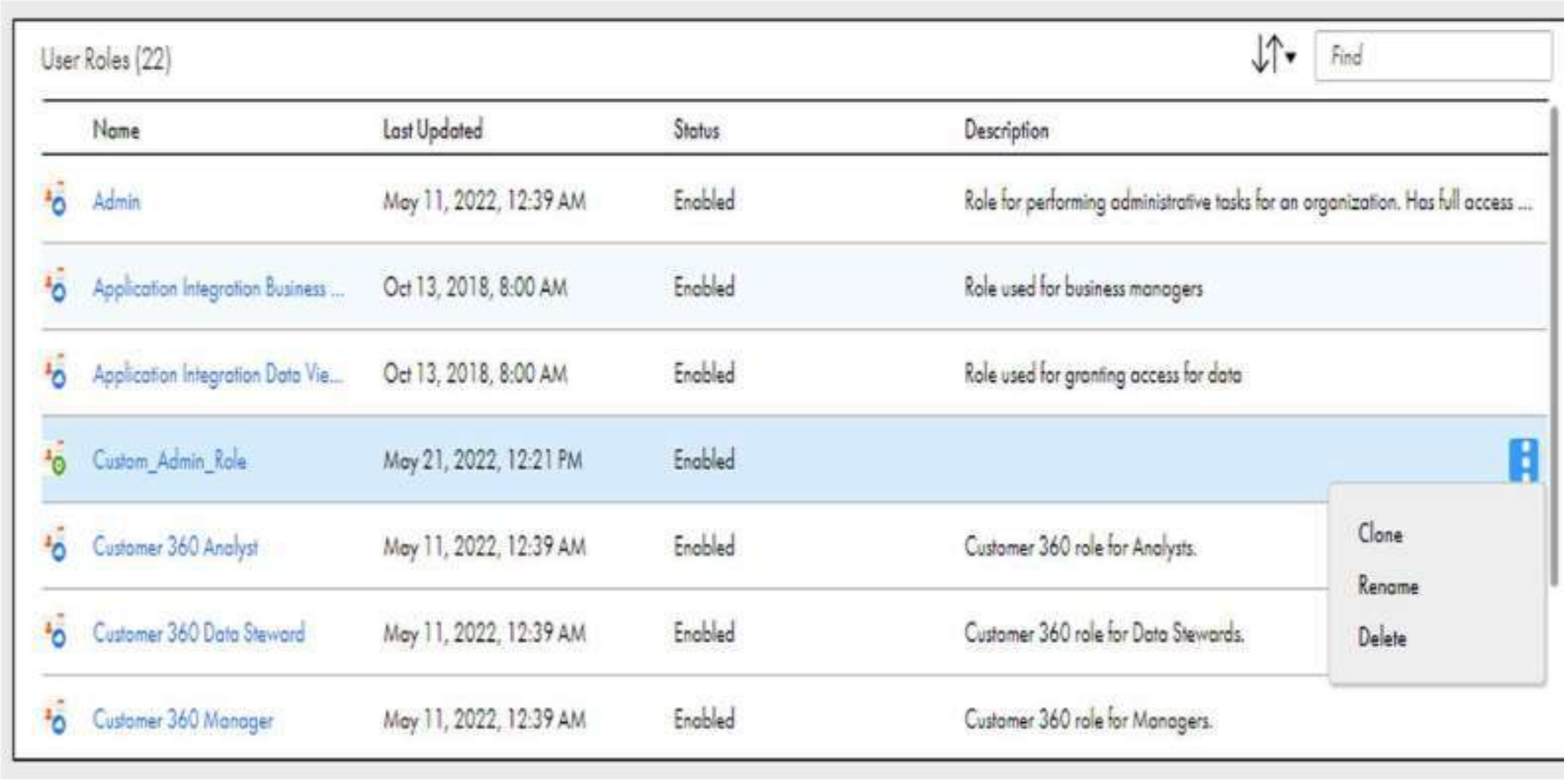
- You can create custom roles on the **User Roles** page.
- To create a custom role, perform the following steps:

1. On the User Roles page, click **Add Role** to create a new role.
2. To copy properties of an existing role, select the role, and click **Clone**3.
3. Enter a name for the role.
4. From the Services drop-down, select the service for which you want to configure privileges. You configure privileges separately for each service.
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 connections, enable Create next to Connection.
6. To configure the feature privileges, select **Features**, and enable or disable the appropriate privileges. For example, to enable users to import and export assets, enable **Asset – import** and **Asset - export** as shown in the image.
7. Save the role.

Notes: After the role is created, you can assign it to users or user groups.

Actions on a Role

- You can perform actions on a role such as View details, Rename role (only for the custom role), and Delete role (only for the custom role)



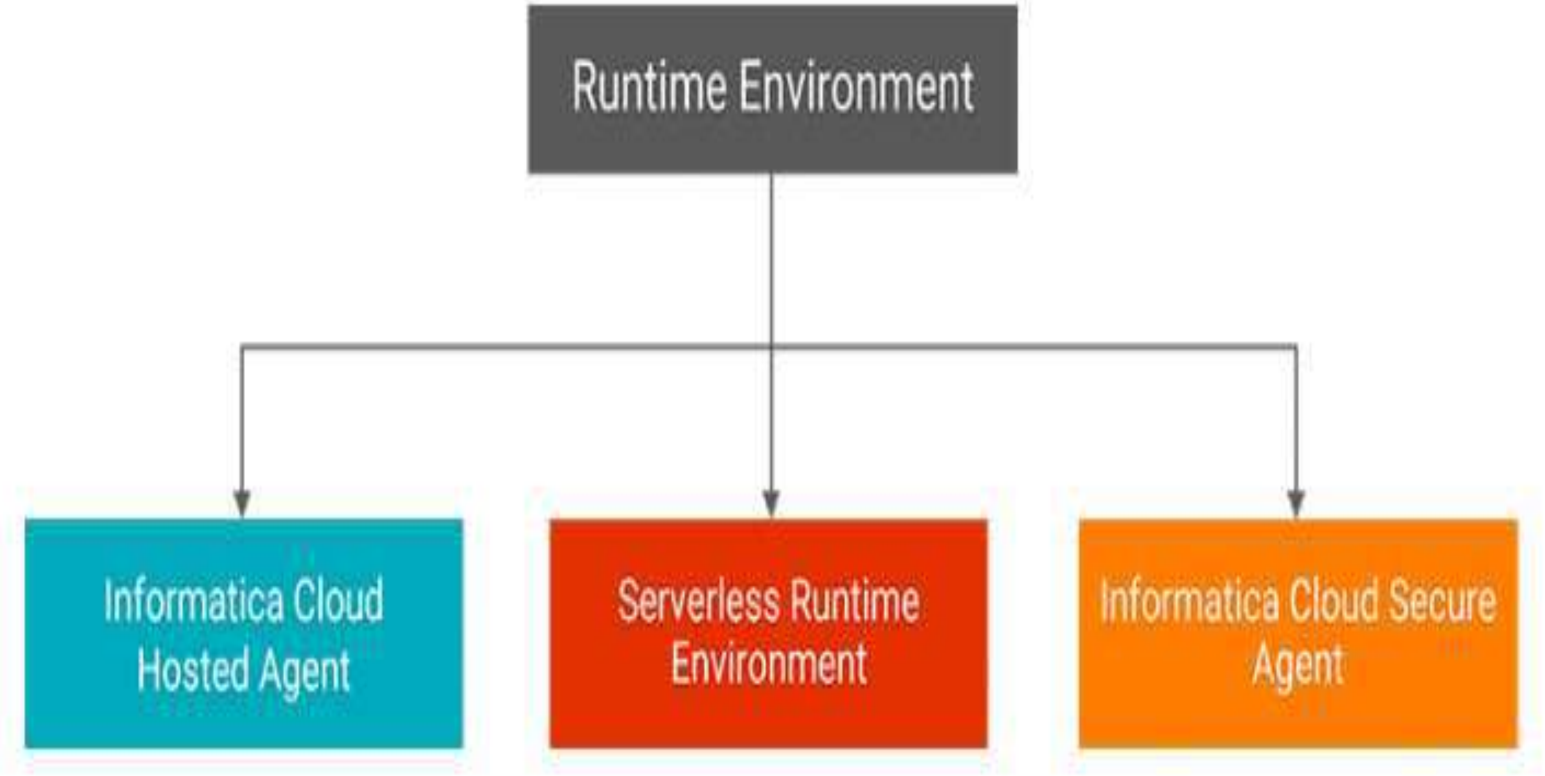
User Roles (22)

Name	Last Updated	Status	Description
Admin	May 11, 2022, 12:39 AM	Enabled	Role for performing administrative tasks for an organization. Has full access ...
Application Integration Business ...	Oct 13, 2018, 8:00 AM	Enabled	Role used for business managers
Application Integration Data Vie...	Oct 13, 2018, 8:00 AM	Enabled	Role used for granting access for data
Custom_Admin_Role	May 21, 2022, 12:21 PM	Enabled	
Customer 360 Analyst	May 11, 2022, 12:39 AM	Enabled	Customer 360 role for Analysts.
Customer 360 Data Steward	May 11, 2022, 12:39 AM	Enabled	Customer 360 role for Data Stewards.
Customer 360 Manager	May 11, 2022, 12:39 AM	Enabled	Customer 360 role for Managers.

Informatica Cloud Secure Agent Overview:

- **Runtime Environments:-**
  - A runtime environment is the execution platform that is required to run any task in IICS. The tasks can include any data integration or application integration tasks.
  - To run tasks in your organization, you must have at least one runtime environment set-up in your organization.

Informatica Runtime Environment types:


Runtime Environment
Informatica Cloud Hosted Agent
Serverless Runtime Environment
Informatica Cloud Secure Agent

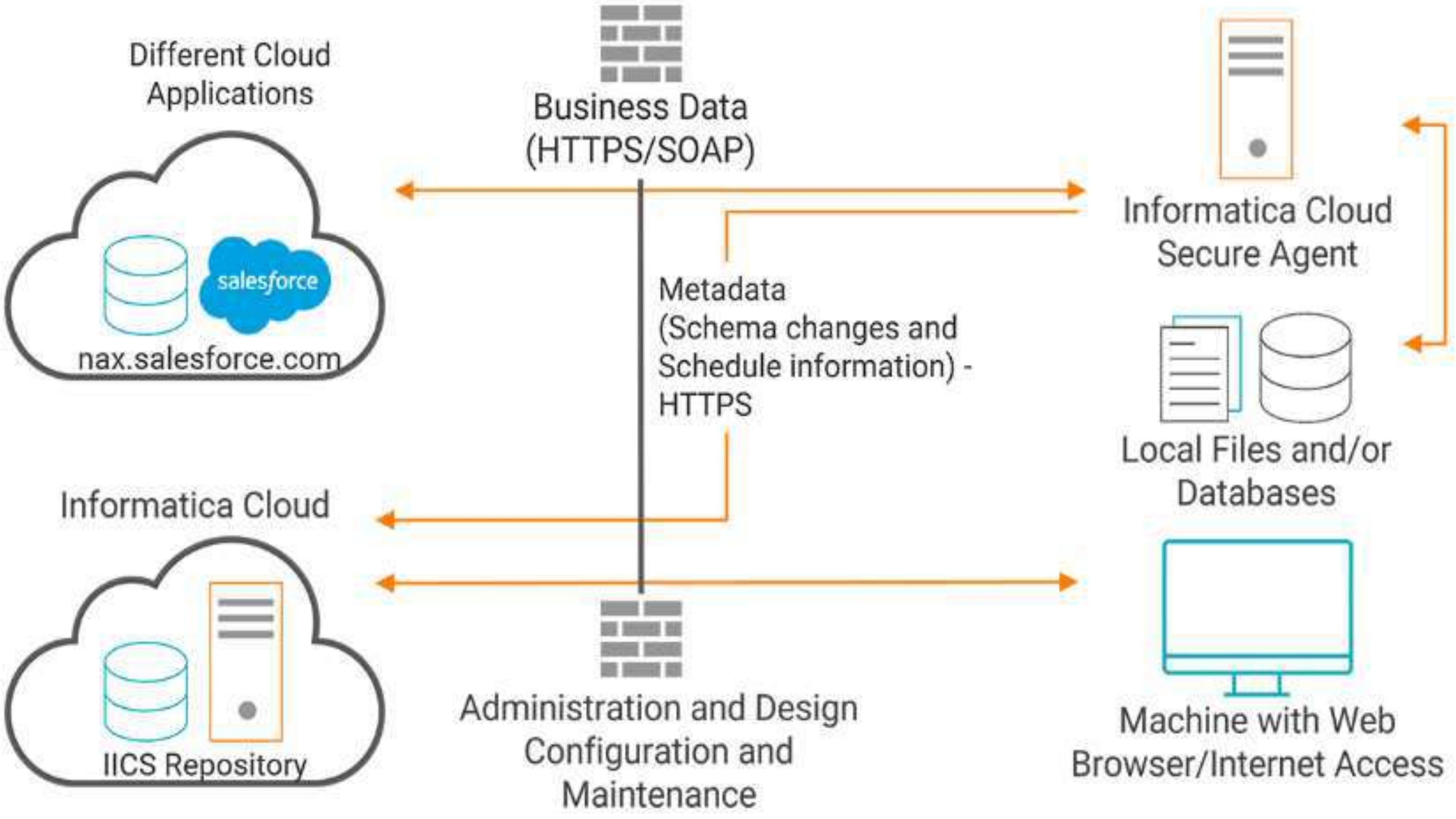
Informatica Cloud Hosted Agent

- The Hosted Agent runs synchronization, mapping, and replication tasks in IICS that uses certain connectors as source or target.
- As the Hosted Agent runtime environment is managed by Informatica Cloud Data Integration, so, you cannot add, delete, or configure a Hosted Agent.
- To use a hosted agent for a connection, you must check the list of connectors supported by the hosted agent from the IICS help section.

Informatica Cloud Secure Agent

- The Secure Agent is a lightweight, self-upgrading program that runs tasks in IICS. It is responsible for moving data directly from the source to the target to access all your local resources
- The Secure Agent is the local agent that runs on a physical or virtual machine running on Windows or Linux. Therefore, your application data never gets staged or run through the Informatica Cloud servers, and remains completely secure and stays behind the firewall
- To run any task, the Secure Agent uses pluggable microservices for data processing.

Secure Agent Architecture


Different Cloud Applications
salesforce
nax.salesforce.com
Business Data (HTTPS/SOAP)
Metadata (Schema changes and Schedule information) - HTTPS
Informatica Cloud Secure Agent
Local Files and/or Databases
Informatica Cloud
IICS Repository
Administration and Design Configuration and Maintenance
Machine with Web Browser/Internet Access

Secure Agent Architecture

- If you include the Secure Agent in the IICS architecture, you can see the agent running behind the firewall. The agent gives you access to any local files or on-premise databases or applications.
- Once the task is initiated, the Secure Agent connects to the IICS Repository and downloads all metadata, including scheduling information, mappings, and so on. IICS performs the design and administration of tasks through a web browser.
- When the agent wants to connect to a SaaS application, in this case Salesforce, it connects through the Business API.

Minimum Requirements for Secure Agent

- If your organization uses a protective firewall, you must include the Informatica Intelligent Cloud Services domain name or IP address ranges in the list of approved domain names or IP addresses and enable the secure agent's port. This ensures that the Secure Agent can perform all necessary tasks through the firewall. The Secure Agent uses port 443 (HTTPS) to connect to the internet.
- The first few characters of the URL string identify the POD. For example, if the URL starts with usw3.dm-us.informaticacloud.com, your POD is **USW3**.

Secure Agent Manager

- To install the Secure Agent on windows, you must use the Secure Agent Manager.
- After the agent is installed, the Secure Agent runs as a Windows service.
- You can launch the Secure Agent Manager from the Windows Start menu or the desktop icon.

Secure Agent Manager perform the following tasks:

- View the status of the Secure Agent and the services that the Secure Agent runs. It shows the services that the Secure Agent runs. If one or more services are not running, you can click on the alert link to view service details.
- Stop or Restart the Secure Agent. You must stop the agent before you uninstall the agent.
- If your Org uses proxy services to connect to a network, you must configure the proxy settings on the Proxy tab of Secure Agent Manager.

Secure Agent Service Startup

- To ensure there is only one instance of agentcore process, it obtains a lock on **agentcore.lock** file. This file is located in <Agent_Install_Dir>\apps\agentcore\data\ directory. This directory also contains appspec for all the services.
- Once the lock is obtained, agentcore reads the agent proxy properties file, infaagent.ini, agentcore.cfg files, and loads the agent configuration. Then, it reads the agent ID from infaagent.ini file.
- If the agent ID value returns null, it sets the initialState state as NOT_CONFIGURED, or else sets the initial State to CONFIGURED.

Secure Agent Service Startup

- If the initial state is set to **configured**, it reads the MasterURL from infaagent.ini file and establishes a session with IICS. After which, the authentication goes through, you see the runtime Environment in RUNNING state in your Org's Administrative service.
- Then, the agent core gets the list of registered/licensed services and starts the service orchestration.

Agentcore:

- The AgentCore is the first process to start when agent startup is invoked. It is responsible for the agent's configuration and associating it with the IICS Org.
- It is also used for the following actions on the Secure Agent:
  - To establish a secure connection with IICS
  - Managing upgrades
  - Maintaining application specification (appspec) for every application
  - Downloading and deploying packages based on the appspec
  - Syncs with IICS on application statuses by monitoring services through status scripts

Service startup routine:

1. All applications are governed by a specific component called LCM (Log Collection Manager) within Agentcore.
   - As a first step, LCM reads appspec for all the services.
2. Then, it downloads all the dependent packages from IICS. This contains jars, libraries, and executable files.
3. Once the download is complete, it deploys all these packages and creates a specific version under **<Agent_home>/apps/<service_name>** locati on in secure agent installation directory.
4. Then, it creates soft links to the downloaded binaries present in the dependent package.
5. Once the links are created, it invokes the start script for services and waits for success return status for each service.
6. When a service status changes to success, it updates IICS of the current status.

Running Secure Agent as Local/Network User

- If you are a user who runs the agent on a Windows system, the agent inherits the access privileges of the Windows user. This happens automatically when you install the agent.
- The agent needs permission to access the directories on Windows. Therefore, you may have to reconfigure the Windows service

Lab Activity:

- Installing Secure Agent on Windows