







Using the Cisco ICFP GUI

- [Cisco ICFP GUI Icons, page 1](#)
- [Common Administrative Tasks, page 3](#)
- [Managing Cloud Instances, page 16](#)
- [Managing Tenants, page 19](#)

Cisco ICFP GUI Icons



Beginning with release 3.1.1, Cisco ICFP introduces a new graphical user interface (GUI). The following icons are used throughout the Cisco ICFP GUI.

Table 1: Common Icons

Icon	Description
	Edit the selected item.
	Refresh the screen.
	Search for an item.
	View details for the selected item.







The following icons are used for working with cloud instances.

Table 2: Cloud Instance Icons

Icon	Description
	Add a cloud instance.
	Delete a cloud instance.



The following icons are used for working with tenant accounts.


Table 3: Tenant Account Icons

Icon	Description
	Add a tenant account.
	Delete or purge a tenant account. Click the icon to see the available options.
	View existing tenant accounts.
	View tenant account faults.
	View tenant account tasks.
	View tenant account VMs.

The following icons are used to install JKS certificate files, update licenses, or update software or adapters.





Table 4: Uploading and Installing Files Icons

Icon	Description
	Install a JKS certificate.
	Update the Cisco ICFP license.

Icon	Description
	Update an adapter or Cisco ICFP software.

The following icons are used to configure syslog and download logs.

Table 5: Logging Icons

Icon	Description
	Configure syslog servers or debug levels for system logs.
	Add log to zip file for download.
	Download the zipped log files.
	Remove log from the download zip file.

Common Administrative Tasks

Cisco ICFP enables you to perform the following common administrative tasks via the GUI:

- Configure admin account options
- Configure syslog servers
- Import JKS certificates
- Install adapters
- Upgrade Cisco ICFP
- Manage licenses
- Check system health
- Monitor tasks
- Specify debug levels
- Download logs

Configuring Admin Account Options

You can reset the admin account password, specify how the Cisco ICFP menu should look when opening the GUI, and configure the amount of time that a session can remain inactive before it times out. For more information, see the following topics:

- [Changing the Admin Account Password](#), on page 4
- [Setting Admin Account Preferences](#), on page 4

Changing the Admin Account Password

Use this procedure to change the password for the Cisco ICFP admin account for standalone and multiple-node clusters as follows:

- To change the password for a standalone node, log in to the Cisco ICFP GUI for that node.
- To change the password for a multiple-node cluster, log in to the Cisco ICFP GUI for the active primary node in the cluster.

Before You Begin

You must have admin account access to perform this task.

Procedure

-
- Step 1** In the Cisco ICFP toolbar, choose **Admin**.
 - Step 2** In the **Admin Log In** dialog box, enter the current credentials for logging in to the Cisco ICFP admin account and click **Login**.
 - Step 3** In the **Admin Panel** dialog box, click the **Password** tab.
 - Step 4** Enter the new password in the **New Password** and **Confirm New Password** fields, and click **Apply**. A success message indicates that the password has been successfully updated.
 - Step 5** Click **Close**.
 - Step 6** Log out of the Cisco ICFP GUI and log in again with the new password.
-

Setting Admin Account Preferences

Cisco ICFP enables you to set the following options for the Cisco ICFP GUI:

- Whether the left menu is expanded or collapsed by default.
- The number of minutes that a session can remain inactive before it times out.

Before You Begin

You must have admin account access to perform this task.

Procedure

- Step 1** In the Cisco ICFP toolbar, choose **Admin**.
 - Step 2** In the **Admin Log In** dialog box, enter the credentials for logging in to the Cisco ICFP admin account and click **Login**.
 - Step 3** In the **Admin Panel** dialog box, click the **Settings** tab.
 - Step 4** In the **Menu state on startup** field, indicate whether the left menu should be expanded or collapsed when you log in to the GUI.
 - Step 5** In the **Session timeout in minutes** field, enter the number of minutes that a session can remain inactive before the session times out.
 - Step 6** Click **Save**.
A success message indicates that the settings have been successfully updated.
 - Step 7** Click **Close**.
 - Step 8** Log out of the Cisco ICFP GUI and log in again for the new settings to take effect.
-

Configuring Syslog Servers

Cisco ICFP enables syslog by default and allows you to specify the severity of messages to be reported. In addition, Cisco ICFP enables you to forward log messages to a remote server instead of recording them in a local file or displaying them.

Before You Begin

If you use remote syslog servers, obtain the IP addresses of the primary and secondary syslog servers.

Procedure

- Step 1** Choose **Logs > Configure Syslog**.
 - Step 2** Click the **Configure** icon.
 - Step 3** In the **Syslog Configuration** dialog box, check the **Enable Syslog** check box.
 - Step 4** From the **Log Level** drop-down list, choose the minimum severity of the messages to display or forward. For example, if you choose **Minor**, messages with the severity **Minor** or **Major** are displayed or forwarded. If you choose **Major**, only messages with the severity **Major** are displayed or forwarded.
 - Step 5** Enter the IP addresses for the primary and secondary syslog servers and click **Apply**.
Cisco ICFP uses UDP and port 514 for syslog messages by default.
-

Importing a JKS Certificate File

Cisco ICFP enables you to import a Java KeyStore (JKS) file, which is a repository of certification authority (CA) security certificates used in SSL encryption.

Procedure

-
- Step 1** In the Cisco ICFP GUI, choose **Certificate** and click the **Install Certificate** icon.
- Step 2** In the **Install Certificate** dialog box, in the **Keystore Password** field, enter the KeyStore password.
Tip Click in the field to choose an existing password.
- Step 3** Click **Browse** to choose the JKS file.
- Step 4** Click **Upload**.
- Step 5** When prompted, click **Yes** to confirm the upload.
-

Installing an Adapter

You can use the Cisco ICFP GUI to install or upgrade an adapter.

Before You Begin

Confirm that the adapter file is accessible from Cisco ICFP.

Procedure

-
- Step 1** In the Cisco ICFP GUI, choose **Upgrade Software** and click the **Upgrade Adapter** icon.
- Step 2** In the **Upgrade Adapter** dialog box, provide the following information:

Field	Description
Adapter Type	Choose the adapter type: Cisco or Custom.
Adapter Name	The adapter name. If you choose Cisco in the Adapter Type field, this field defaults to CAPI and cannot be modified.
Adapter Description	The description of the adapter.
Adapter Version	The adapter version.
Select File to Upload	Browse to the required adapter file and click Open .

- Step 3** Click **Upload**.
- Step 4** When prompted, click **Yes** to upload the adapter.
- Step 5** Restart services as follows:
- Using SSH, log in to the ShellAdmin console for the virtual appliance.
 - Choose **Stop Services**.
 - Choose **Start Services**.

For information about the ShellAdmin console, see [Using Cisco ICFP ShellAdmin Commands](#).

Upgrading Standalone Nodes or Multiple-Node Clusters

Cisco ICFP enables you to upgrade standalone appliances and multiple-node clusters for bug fixes and updated adapters. For more information, see the following topics:

- [Supported Upgrade Paths](#), on page 7
- [Upgrading a Standalone Node](#), on page 7
- [Upgrading a Multiple-Node Cluster](#), on page 8

Supported Upgrade Paths

Cisco ICFP 3.1.1 supports the following upgrade paths:

- OpenStack—Cisco ICFP 2.3.1 to 3.1.1.
- VMware—Cisco ICFP 2.3.1 to 3.1.1.

Upgrading a Standalone Node

This procedure enables you to upgrade Cisco ICFP to a newer version and apply Cisco bug fixes on a standalone node. To upgrade a multiple-node cluster, see [Upgrading a Multiple-Node Cluster](#), on page 8.

Upgrading from Cisco ICFP version 2.3.1 to 3.1.1 automatically resets the admin account password to **changeme**. For information on changing the admin account password to another password, see [Changing the Admin Account Password](#), on page 4.

Before You Begin

- Obtain the Cisco ICFP upgrade file (`icfp-upgrade-3.1.1.tar.gz`) from [Cisco.com](#). For assistance, contact your Cisco representative.
- Confirm that the upgrade file is accessible from the Cisco ICFP virtual appliance.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Upgrade Software**, and click the **Upgrade Adapter** icon.

Step 2 In the **Upgrade Adapter** dialog box, provide the following information:

Field	Description
Adapter Type	Choose Cisco .
Adapter Name	<i>Display only.</i> This field displays CAPI by default.
Adapter Description	Enter the desired description.

Field	Description
Adapter Version	Enter the new version.
Select File to Upload	Browse to the Cisco ICFP upgrade file and click Upload .

- Step 3** When prompted, click **Yes** to confirm the upload.
When upgrading from Cisco ICFP 2.3.1 to 3.1.1 or higher, a message is displayed stating that the upgrade will start in 2 minutes. After approximately 2 minutes, the upgrade is installed, the services automatically restart, and the GUI becomes unresponsive.
- Step 4** Finish the upgrade by refreshing the browser and logging in to the Cisco ICFP GUI.
- Step 5** To verify that the upgrade was successful, click **About** in the GUI toolbar and confirm that the correct version is displayed.
Cisco ICFP displays the version, build number, build date, the last modification date, and the version hash value.

What to Do Next

If required, change the admin account password as described in [Changing the Admin Account Password, on page 4](#).

Upgrading a Multiple-Node Cluster

Use this procedure to upgrade a multiple-node cluster for bug fixes and updated adapters. To upgrade a standalone Cisco ICFP virtual appliance, see [Upgrading a Standalone Node, on page 7](#).

Upgrading from Cisco ICFP version 2.3.1 to 3.1.1 automatically resets the admin account password to **changeme**. For information on changing the admin account password to another password, see [Changing the Admin Account Password, on page 4](#).

This procedure applies to multiple-node clusters with the following components and configuration:

- An HA pair that:
 - Consists of two Cisco ICFP virtual appliances configured with the Primary Node role.
 - Is configured with one active node and one standby node.
- Additional Cisco ICFP virtual appliances that are configured as service nodes.

The workflow for upgrading a cluster includes the following high-level tasks:

- 1 Stop the virtual IP (VIP) service on the HA active node.
- 2 Monitor status while services fail over to the HA standby node.
- 3 Upgrade the current HA active node (originally the standby node).
- 4 Start the VIP service on the current HA standby node (originally the active node).
- 5 Stop the VIP service on the upgraded HA active node.

- 6 Monitor status while services fail over to the current HA standby node, making it the active node again.
- 7 Upgrade the current HA active node.
- 8 Start the VIP service on the current HA standby node.
- 9 Upgrade each service node.
- 10 If required, change the admin account password.

The following procedure describes how to perform these tasks.

Before You Begin

- Obtain the Cisco ICFP upgrade file (`icfp-upgrade-3.1.1.tar.gz`) from Cisco.com. For assistance, contact your Cisco representative.
- Confirm that the upgrade file is accessible from the Cisco ICFP virtual appliance.
- Confirm that HA has been configured on two Cisco ICFP virtual appliances that are configured with the Primary Node role.

Procedure

-
- Step 1** Stop the VIP service on the HA active node as follows:
- a) Log in to the ShellAdmin console for the HA active node.
 - b) Choose **Setup HA**.
 - c) When asked if you want to reconfigure HA, enter **Y**.
 - d) Enter **C** to stop the VIP service.
 - e) Enter **Y** to confirm the action.
 - f) Press **Enter** to return to the ShellAdmin menu.
- Step 2** Log in to the ShellAdmin console for the HA standby node.
- Step 3** In the ShellAdmin console for the standby node, choose **Display Services Status** to monitor the following events as they occur:
- HA services fail over to the standby node in the HA pair.
 - Infra services start running on the standby node.
 - The GUI for the standby node becomes available for logging in.
- It can take a few minutes for the services to start and for the GUI of the standby node to be accessible from the browser.
- Note** The node that was originally the HA standby node becomes the HA active node.
- Step 4** Upgrade the currently active node of the HA pair as follows:
- a) Log in to the Cisco ICFP GUI for the active node of the HA pair by using the management IP address of the node.
 - b) In the GUI, choose **Upgrade Software** and click the **Upgrade Adapter** icon.
 - c) In the **Upgrade Adapter** dialog box, provide the required information.
For information about the fields in this dialog box, see [Upgrading a Standalone Node](#), on page 7.

- d) Click **Upload**.
- e) When prompted, click **Yes** to confirm that you want to upload the selected file.

When upgrading from Cisco ICFP 2.3.1 to 3.1.1 or higher, the Infra services restart automatically and you can log in to Cisco ICFP after approximately 2 minutes.

Step 5 Verify that the HA active node was successfully upgraded as follows:

- a) Log in to the Cisco ICFP GUI of the active node by using the management IP address of the node.
- b) Click **About** in the Cisco ICFP toolbar.
- c) Confirm that the correct version is displayed.

Step 6 Restart the VIP service on the current HA standby node as follows:

- a) Log in to the ShellAdmin console for the current HA standby node.
- b) Choose **Setup HA**.
- c) When asked if you want to reconfigure HA, enter **Y**.
- d) Enter **D** to start the VIP service.
- e) Press **Enter** to return to the ShellAdmin menu.

Step 7 Stop the VIP service on the currently active node that was upgraded in Step 4 as follows:

- a) Log in to the Shell Admin console for the currently active node in the HA pair.
- b) Choose **Setup HA**.
- c) When asked if you want to reconfigure HA, enter **Y**.
- d) Enter **C** to stop the VIP service.
- e) Enter **Y** to confirm the action.
- f) Press **Enter** to return to the ShellAdmin menu.

Step 8 Log in to the ShellAdmin console for the standby node in the HA pair.

Step 9 In the ShellAdmin console for the standby node, choose **Display Services Status** to monitor the following events as they occur:

- HA services fail over to the standby node in the HA pair.
- Infra services start running on the standby node.
- The GUI for the standby node becomes available for logging in.

It can take a few minutes for the services to start and for the GUI of the standby node to be accessible from the browser.

Note The node that was previously the HA standby node becomes the HA active node.

Step 10 Upgrade the HA active node as follows:

- a) Using the management IP address instead of the virtual IP address for the HA pair, log in to the Cisco ICFP GUI for the HA active node.
- b) Upgrade the node as described in Step 4.
- c) Verify that the upgrade was successful as described in Step 5.

Step 11 Restart the VIP service on the HA standby node as follows:

- a) Log in to the ShellAdmin console for the HA standby node.
- b) Choose **Setup HA**.
- c) When asked if you want to reconfigure HA, enter **Y**.
- d) Enter **D** to start the VIP service.

e) Press **Enter** to return to the ShellAdmin menu.

Step 12 Upgrade each service node in the cluster as follows:

- a) Log in to the Cisco ICFP GUI for the service node.
- b) Upgrade the service node by uploading the upgrade package as described in Step 4.
When upgrading from Cisco ICFP 2.3.1 to 3.1.1 or higher, the Infra services restart automatically and you can log in to the upgraded service node after approximately 2 minutes.

Step 13 Verify that each service node upgraded successfully as follows:

- a) For each service node, refresh the browser and log in to the Cisco ICFP GUI for the service node.
- b) Click **About** in the Cisco ICFP toolbar and confirm that the correct version is displayed.

Step 14 (Optional) If required, change the admin account password as described in [Changing the Admin Account Password](#), on page 4.

Managing Licenses

Cisco ICFP is automatically installed with a 60-day evaluation license that supports 20 hybrid cloud units (HCUs). The topics in this section describe how to obtain a permanent license by using a Product Authorization Key (PAK), install a license file, update a license, and view license details.

Cisco ICFP Licensing

A Cisco ICFP license is based on hybrid cloud units (HCUs). One or more HCUs are used for each VM running in the public cloud. A powered-off VM does not use any HCUs.

For Amazon Web Services and Microsoft Azure, two HCUs are used for each VM. For example, if the HCU count is ten, five VMs can run in the public cloud. For Cisco-powered providers, one HCU is used for each VM. For example, if the HCU count is ten, ten VMs can run in the public cloud.

Cisco ICFP includes the following types of licenses:

- Evaluation License (ICFP-EVAL-EBD)—Cisco ICFP includes a 60-day, 20-HCU evaluation license that lets you try the software before you purchase permanent licenses. The evaluation period begins when you install the software and expires within 60 days of installation.
- Permanent License (ICFP-CPC)—Permanent licenses have an expiration date. The license file specifies the number of licenses that you purchased. Contact your Cisco representative to purchase permanent licenses.
- Partner License (ICFP-NFR-EBDS)—Partner (not for resale) licenses are available only to Cisco partners for demonstration and lab purposes. Partner licenses have an expiration date. The license file specifies the number of licenses that you purchased. Contact your Cisco representative to purchase partner licenses.

Cisco ICFP Licensing Workflow

This workflow applies to all Cisco ICFP licenses except for the Cisco ICFP evaluation license. This workflow is not required for the 60-day evaluation license that is included with Cisco ICFP.

- 1 Before installing Cisco ICFP, locate your Cisco ICFP license and Product Authorization Key (PAK).

- To purchase a license, contact your Cisco representative.
- 2 Register the PAK on the Cisco software license site.
For more information, see [Generating a License Using a PAK](#), on page 12.
 - 3 Install Cisco ICFP.
For more information, see the *Cisco Intercloud Fabric for Provider Installation Guide*.
 - 4 Upload the license in Cisco ICFP.
For more information, see [Uploading a License](#), on page 12.
 - 5 Check license status.
For more information, see [Viewing License Details](#), on page 13.
 - 6 Update the license.
To update an existing license, use the procedure for uploading a license.

Generating a License Using a PAK

This procedure describes how to generate a Cisco ICFP license by using a PAK.

Before You Begin

Obtain the Cisco ICFP PAK.

Procedure

- Step 1** In a browser, go to the [Cisco Product License Registration](#) page.
This page offers training on assigning PAKs or tokens, and a link to the Cisco Product License Registration tool.
 - Step 2** Click **Continue to Product License Registration**.
 - Step 3** In the **Product License Registration** screen, enter the PAK number in the **Get New Licenses** field, and click **Fulfill**.
 - Step 4** In the **Get New Licenses** dialog box, provide the required information and click **Submit**.
The status of your request is displayed, and a digital license agreement and a zipped license file are sent to the email address that you specified.
-

What to Do Next

Upload the license file in Cisco ICFP. For more information, see [Uploading a License](#), on page 12.

Uploading a License

Use this procedure to upload a new license in Cisco ICFP or to update an existing license. To ensure continuous operation, be sure to update the license before the current license expires.

Before You Begin

- Obtain the Cisco ICFP license file. For more information, see [Generating a License Using a PAK, on page 12](#).
- If you received a zipped license file by email, extract and save the `.lic` file to your local machine.

Procedure

-
- Step 1** In the Cisco ICFP GUI, choose **License** and click the **Upload License** icon.
- Step 2** In the dialog box, select the Cisco ICFP `.lic` file and click **Upload**.
- Step 3** When prompted, click **Yes** to confirm the upload.
After the license file is successfully processed, a success message is displayed.
-

Viewing License Details

To view license details in the Cisco ICFP GUI, choose **License**.

The license details are displayed, including the license type, the license status, the number of HCUs supported, and the term of the license.

Monitoring System Health

Cisco ICFP enables you to monitor the system health of standalone, primary, and service nodes as described in the following topics:

- [Checking System Status, on page 13](#)
- [Monitoring Tasks, on page 14](#)
- [Configuring Logs for Debugging, on page 15](#)
- [Downloading Logs, on page 15](#)

Checking System Status

This procedure enables you to view the following information for Cisco ICFP nodes:

- Node information, including the node type (such as standalone, primary, or service), status (active or inactive), name, IP address, and length of uptime.
- Cisco ICFP version, build number, and build date.
- JVM name and version.
- Database status.
- System memory capacity, amount used, and amount free.
- System disk capacity, amount used, and amount free.

- CPU load, number of CPUs, architecture, and operating system version.
- Applications and their status.

The scope of the information that is displayed depends on the node that you use to check status:

- If you log in to a standalone node, you can view system status for the standalone node only.
- If you log in to a primary node in a multiple-node cluster, you can view system status for the primary node and each service node in the cluster.
- If you log in to a service node in a multiple-node cluster, you can view the system status for that service node only.

Procedure

Step 1 In the Cisco ICFP GUI, choose **System Health**.

Step 2 Click **Node Info** for the required node.

The information that is displayed depends on the node you choose:

- If you choose a standalone node, node-specific and system resource information is displayed.
- If you choose a primary node or an active service node, node-specific and system resource information is displayed.
- If you choose an inactive service node, a high-level summary is displayed. To view the status and more detailed information about an inactive service node, log in to the Cisco ICFP ShellAdmin console for that service node.
- If you log in to the GUI using the virtual IP address for an HA pair, detailed information for the active node is displayed.

Step 3 (Optional) Click **Refresh** to view updated information.

Monitoring Tasks

You can use the Cisco ICFP GUI to monitor the tasks of each tenant.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenants Accounts**.

Step 2 In the **Tenant Accounts** table, click the **Accounts** icon for the required tenant.

Step 3 In the **User Statistics** area, click the **Tasks** icon.
All tasks for the tenant account are listed.

Configuring Logs for Debugging

In addition to specifying the level for syslog reporting (see [Configuring Syslog Servers, on page 5](#)), you can specify the level of messages to be reported in Tomcat and Infra Manager logs.

Procedure

- Step 1** In the Cisco ICFP GUI, choose **Logs > Configure Debug**.
- Step 2** Click the **Configure** icon.
- Step 3** In the **Debug Configuration** dialog box, choose the level of messages to be reported in Tomcat and Infra Manager logs:
- **Debug**—Displays messages of all levels.
 - **Error**—Displays messages with the level Error.
 - **Info**—Displays messages with the level Error or Information.
 - **Warn**—Displays messages with the level Warning or Error.
- Step 4** Click **Apply**.
-

Downloading Logs

Cisco ICFP enables you download the following logs:

- CAPI Controller Log
- CAPI Tomcat Log
- Catalina Log
- Database Log
- HA Log
- Install Log
- MultiNode Log
- Syslog Messages Log
- System Messages Log

If you choose a log that does not apply to your environment (for example, if you choose the HA Log but HA is not configured in your environment), Cisco ICFP generates and downloads all logs except the log that does not apply.

Procedure

-
- Step 1** In the Cisco ICFP GUI, choose **Logs > Download Logs**.
- Step 2** Click the **Add** icon for each log that you want to download and click **Download**.
A zipped file containing all requested logs that apply to your environment is downloaded to your system.
-

Managing Cloud Instances

A cloud instance has a unique identifier that binds the back-end cloud URI to a southbound adapter that is installed by the service provider. Multiple back-end URIs can have multiple cloud instances. A tenant is a part of a single cloud instance. The following topics describe how to manage cloud instances by using the Cisco ICFP GUI.

Creating a Cloud Instance

You can use the Cisco ICFP GUI to add, or *provision*, a cloud instance.

Before You Begin

Obtain the endpoint URI for the cloud instance.

Procedure

-
- Step 1** In the Cisco ICFP GUI, choose **Cloud Instances** and click the **Add Cloud Instance** icon.
- Step 2** In the **New Cloud Instance** dialog box, provide the following information and click **Create**:

Field	Description
Cloud Instance Name	Name of the cloud instance.
Select Cloud	The cloud instance type: Cisco or Custom.
Select Module	For a Cisco cloud instance type, choose the module type: <ul style="list-style-type: none"> • CSP—Apache CloudStack Platform • DiData—Cisco Intercloud Services – V • OSP—OpenStack Platform • VCDP—VMware vCloud Director Platform For a custom cloud instance type, enter the custom module name.
Endpoint URI	The endpoint hostname or IP address of the cloud instance.

Field	Description
Parameters The parameters that are displayed depend on the selected module.	
Image Conversion Support on Cloud	For OSP modules, indicate whether or not image conversion on the cloud is required.
First Boot Image Conversion Support	For OSP modules, indicate whether or not image conversion during VM boot on the cloud is required.
Enable Group-Based Policy Support	For OSP modules, indicate whether or not the provider OpenStack cloud uses a group-based policy framework.
Enable Keystone V3 API Support	For OSP modules, indicate whether or not OpenStack Keystone V3 Identity Service is used for authentication in the provider OpenStack cloud.
Enable Boot from Volume Support	For OSP modules, indicate whether or not the cloud instance is to be booted from a Cinder volume.
FTP Server Name	For Cisco Intercloud Services — V modules, enter the FTP server name.

Viewing Cloud Instance Details

You can use the Cisco ICFP GUI to view cloud instance details.

Procedure

- Step 1** In the Cisco ICFP GUI, choose **Cloud Instances**.
Cisco ICFP displays the cloud instance name, type, module, and endpoint URI for each cloud instance.
- Step 2** To view parameter details, click **Edit** for the required cloud instance.
The **Edit Cloud Instance** dialog box is displayed with the configured parameters.

Editing a Cloud Instance

You can use the Cisco ICFP GUI to edit the cloud instance endpoint URI and parameters. The cloud instance name, type, and module cannot be changed.

Procedure

- Step 1** In the Cisco ICFP GUI, choose **Cloud Instances**.
- Step 2** Choose the required cloud instance and click **Edit**.
- Step 3** In the **Edit Cloud Instance** dialog box, update the following information as needed and click **Update**:

Field	Description
Cloud Instance Name	<i>Display only.</i> The name of the cloud instance.
Select Cloud	<i>Display only.</i> The cloud instance type.
Select Module	<i>Display only.</i> The module name.
Endpoint URI	The endpoint URI for the cloud instance.
Parameters The parameters that are displayed depend on the selected module.	
Image Conversion Support on Cloud	For OpenStack cloud instances, indicate whether or not image conversion on the cloud is required.
First Boot Image Conversion Support	For OpenStack cloud instances, indicate whether or not image conversion during VM boot on the cloud is required.
Enable Group-Based Policy Support	For OpenStack cloud instances, indicate whether or not the OpenStack cloud uses a group-based policy framework.
Enable Keystone V3 API Support	For OpenStack cloud instances, indicate whether or not OpenStack Keystone V3 Identity Service is used for authentication in the cloud.
Enable Boot from Volume Support	For OpenStack cloud instances, indicate whether or not the cloud instance is to be booted from a Cinder volume.
FTP Server Name	For Cisco Intercloud Services — V modules, enter the FTP server name.

Deleting a Cloud Instance

You can use the Cisco ICFP GUI to delete a cloud instance.

Procedure

-
- Step 1** In the Cisco ICFP GUI, choose **Cloud Instances**.
- Step 2** Choose the required cloud instance and click **Delete**.
After the cloud instance is deleted, a success message is displayed.
-

Managing Tenants

The following topics describe how to add, edit, and delete tenant accounts, and view tenant account details by using the Cisco ICFP GUI.

Creating a Tenant Account

After you create a cloud instance, you can create a tenant account on the cloud.

For a CloudStack cloud instance, you must obtain the API Key and Secret Key for the tenant account before adding the account. After the tenant account is created, Cisco ICFP generates a Pass Key, which is available in the tenant **Account Information** screen (**Tenant Accounts > *tenant* > Accounts**). This Pass Key is required by Cisco Intercloud Fabric when configuring a cloud. For more information, see the Cisco Intercloud Fabric documentation on [Cisco.com](https://www.cisco.com).

For an OpenStack cloud instance, you need additional information depending on the support enabled in the cloud:

- Group-based policies:
 - The external segment name in OpenStack.
 - The name of the external group that is used to connect internal groups to the Internet.
- Keystone V3 Identity Service—The domain name.

Before You Begin

- Confirm that the required cloud instance has been created.
- Depending on the type of cloud instance, obtain the following information:

Cloud Instance Type	Requirement
CloudStack	The API Key and Secret Key for the tenant. For more information, see the Apache CloudStack documentation.

Cloud Instance Type	Requirement
OpenStack	<ul style="list-style-type: none"> • If Keystone V3 Identity Service is enabled on the cloud instance, the authentication domain. • If group-based policies are enabled on the cloud instance: <ul style="list-style-type: none"> ◦ The external segment name. ◦ The name of the external group that is used to connect internal groups to the Internet. <p>For more information, see the OpenStack documentation.</p>
VMware vCloud Director	The name of the organization for the tenant. For more information, see the VMware vCloud Director documentation.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenant Accounts** and click the **Add Tenant Account** icon.

Step 2 In the **New Tenant Account** dialog box, provide the following information and then click **Create**:

Field	Description
Tenant Name	Enter the tenant name. You cannot change the name after adding the tenant.
Select Cloud	Choose the cloud instance. You cannot change the cloud instance after adding the tenant.
Org Name	For a VMware vCloud Director cloud, enter the name of the organization to which the tenant belongs. You cannot change the organization name after adding the tenant.
Max Servers	Enter the maximum number of servers provisioned for the tenant, including stopped VMs.
Username	Enter the tenant account username.
Email	Enter the tenant account email address.
API Key	For a CloudStack cloud, enter the API Key for the tenant.
Secret Key	For a CloudStack cloud, enter the Secret Key for the tenant.

Field	Description
Parameters The parameters that are displayed depend on the selected cloud.	
External Segment Name	For an OpenStack cloud that uses a group-based policy framework, enter the external segment name.
Domain Name	For an OpenStack cloud with Keystone V3 Identity Service enabled, enter the domain name.
External Group Name	For an OpenStack cloud that uses a group-based policy framework, enter the name of the external group that is used to connect internal groups to the Internet.

Editing a Tenant Account

You can edit an existing tenant account by using the Cisco ICFP GUI.

You can edit the maximum number of servers, the tenant account email address, and parameters. For tenants using a CloudStack cloud, you can also edit the API Key and Secret Key. The other fields are display-only.

Procedure

- Step 1** In the Cisco ICFP GUI, choose **Tenants Accounts**.
- Step 2** Choose the required tenant and click **Edit**.
- Step 3** In the **Edit Tenant Account** dialog box, update the information as needed and then click **Update**:

Field	Description
Tenant Name	<i>Display only.</i> The name of the tenant.
Select Cloud	<i>Display only.</i> The name of the cloud instance.
Org Name	<i>Display only.</i> For VMware vCloud Director clouds, the name of the organization to which the tenant belongs.
Max Servers	The maximum number of servers provisioned for the tenant, including stopped VMs.
Username	<i>Display only.</i> The tenant account username.
Email	The tenant account email address.
API Key	For CloudStack clouds, the API Key for the tenant.

Field	Description
Secret Key	For CloudStack clouds, the Secret Key for the tenant.
Parameters The parameters that are displayed depend on the selected cloud.	
External Segment Name	For OpenStack clouds using group-based policies, the name of the external segment for external connectivity.
Domain Name	For OpenStack clouds, the domain name for Keystone V3 Identity authentication.
External Group Name	For OpenStack clouds using group-based policies, the name of the external group that is used to connect internal users to the Internet.

Deleting or Purging a Tenant Account

You can use the Cisco ICFP GUI to delete or purge a tenant account:

- If you delete a tenant account:
 - The tenant account remains in the GUI with the state Deleted.
 - The tenant account resources remain in the Cisco ICFP database.
- If you purge a tenant account:
 - The tenant account is removed from the GUI.
 - All tenant account resources are removed from the Cisco ICFP database.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenant Accounts**.

Step 2 Choose the tenant account that you want to delete or purge, and then do one of the following:

- Click the **More** icon and choose **Delete** to retain the tenant account resources in the database and to change the tenant account to Deleted in the GUI.
- Click the **More** icon and choose **Purge** to remove the tenant account from the GUI and all tenant account resources from the database.

Viewing Tenant Account Details

You can use the Cisco ICFP GUI to view tenant account details.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenants Accounts**.

Step 2 Choose the required tenant and click **Accounts**.

The following information is displayed:

- Account information, including account username and email. Tenant accounts using a CloudStack-based cloud also display the account API Key, Secret Key, and Pass Key.
 - VM summary information in a graph format, including the number of active and inactive VMs, and the number of VMs by type.
 - User statistics, including the total number of VMs, the number of tasks, and the number of faults. Click the **VMs**, **Tasks**, or **Faults** icon to view additional detailed information for that item.
-

Monitoring Tenant Accounts

You can use the Cisco ICFP GUI to monitor tenant accounts.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenant Accounts**.

Step 2 Click the **Accounts** icon for the required tenant account.

The row expands to display information about the account, VMs, and user statistics.

Step 3 Under **User Statistics**, click **VMs**, **Tasks**, or **Faults** to view detailed information about each of these items.
