# Using the Cisco ICFPP GUI



# Common Administrative Tasks

Cisco ICFPP enables you to perform a number of common administrative tasks via the GUI, such as managing licenses, monitoring tasks, and accessing reports and logs.

## Configuring Syslog Servers

Cisco ICFPP enables syslog by default and allows you to specify the severity of messages to be reported. In addition, Cisco ICFPP 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 are using remote syslog servers, obtain the IP addresses of the primary and secondary syslog servers.

### Procedure

**Step 1** Choose **Administration** > **System**, and click the **Syslog** tab.

**Step 2** Check the **Enable Syslog** check box.

**Step 3** 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 4** Provide the following information for the primary and secondary syslog servers, and then click **Save**:

| Field | Description |
|---|---|
| **Server Address** | IP address of the syslog server. |

| Field | Description |
|---|---|
| **Port** | Port to use. The default port is 514 (read-only). |
| **Protocol** | Protocol to be used for the messages. The default protocol is UDP (read-only). |

# Importing a JKS Certificate File

Cisco ICFPP 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 ICFPP GUI, choose **Administration** > **System** and click the **Certificate Setup** tab.

**Step 2** Click **Upload**.

**Step 3** In the **Upload Certificate in JKS Format** dialog box, in the **Keystore File** field, browse to and choose the JKS file.

**Step 4** Click **Upload**.

**Step 5** After the file has uploaded, enter the password in the **Keystore Password** field and click **Submit**.

# Installing an Adapter

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

### Before You Begin

Confirm that the adapter file is accessible from Cisco ICFPP.

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Install**.

**Step 2** In the **Adapters** pane, click **Install**.

**Step 3** In the **Install Adapter** dialog box, provide the information as described in the following table:

| Field | Description |
|---|---|
| **Adapter Type** | Choose the adapter type: Cisco or Custom. |

| Field | Description |
|---|---|
| **Adapter Name** | The name of the adapter. 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 File** | The file to use for this adapter. Browse to the required adapter file and click **Open**. |

**Step 4** Click **Upload**. The file is uploaded to Cisco ICFPP.

**Step 5** After the file is uploaded, click **Submit**.

**Step 6** Restart services as follows:

a) Using SSH, log in to the ShellAdmin console for the virtual appliance.
b) Choose **Stop Services**.
c) Choose **Start Services**.

# Upgrading Standalone Nodes or Multiple-Node Clusters

Cisco ICFPP 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
- Restarting Services Automatically, on page 3
- Upgrading a Standalone Node, on page 3
- Upgrading a Multiple-Node Cluster, on page 5


## Restarting Services Automatically

Beginning with version 2.3.1, Cisco ICFPP includes a feature that automatically restarts Infra services when you upgrade Cisco ICFPP.

The first time that you upgrade Cisco ICFPP from 2.2.1 or 2.2.1a to 2.3.1 or higher, you must manually restart services. After you restart Infra services, the automatic service restart feature is enabled and you do not need to restart Infra services when you next upgrade Cisco ICFPP.

## Upgrading a Standalone Node

This procedure enables you to apply Cisco bug fixes and upgrade adapters on a standalone node. To upgrade a multiple-node cluster, see Upgrading a Multiple-Node Cluster, on page 5.

### Before You Begin

- Obtain the Cisco ICFPP upgrade file (`icfpp-upgrade-2.3.1.tar.gz`) from cisco.com. For assistance, contact your Cisco representative.
- Confirm that the upgrade file is accessible from the Cisco ICFPP virtual appliance.

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Install** > **Adapters**, and click **Install**.

**Step 2** In the **Install Adapter** dialog box, provide the information as described in the following table and then click **Upload**:

| Field | Description |
|---|---|
| **Adapter Type** | Choose **Cisco**. |
| **Adapter Name** | This field displays CAPI by default. No input is required. |
| **Adapter Description** | Enter the desired description. |
| **Adapter File** | Browse to the Cisco ICFPP upgrade file and click **Open**. |

**Step 3** If you are upgrading from Cisco ICFPP 2.2.1 or 2.2.1a to Cisco ICFPP 2.3.1 or higher, complete the following steps:

a) After the file has been uploaded, click **Submit**.
b) Using SSH, log in to the ShellAdmin console for the virtual appliance.
c) Choose the **Stop Services** option.
d) Choose the **Start Services** option.

**Step 4** If you are upgrading from Cisco ICFPP 2.3.1 to a higher version, a message is displayed stating that the upgrade will start in two minutes. After approximately two minutes, the upgrade is installed, the services automatically restart, and the GUI becomes unresponsive. To finish the upgrade, refresh the browser and log in to the Cisco ICFPP GUI.

**Step 5** To verify that the upgrade was successful, click **About** in the GUI toolbar and confirm that the correct version is displayed.
The Product Version field displays the version using the format *version-build-patch* where:

- *version* is the product version, such as 2.3.1.
- *build* is the build number, such as 204.
- *patch* is the patch applied to the version and build, such as p208.

For example, you might see the version 2.3.1-204-p208.

## 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 ICFPP virtual appliance, see Upgrading a Standalone Node, on page 3.

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

- An HA pair consisting of two Cisco ICFPP virtual appliances that are configured as primary nodes.
- The HA pair is configured with one active node and one standby node.
- Additional Cisco ICFPP virtual appliances 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.

The following procedure describes how to perform these tasks.

### Before You Begin

- Obtain the Cisco ICFPP upgrade file (`icfpp-upgrade-2.3.1.tar.gz`) from Cisco.com. For assistance, contact your Cisco representative.
- Ensure that the upgrade file is accessible from the Cisco ICFPP virtual appliance.
- Confirm that HA has been configured on two Cisco ICFPP 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 ICFPP GUI for the active node of the HA pair by using the management IP address of the node.
b) In the GUI, choose **Install** > **Adapters** > **Install**.
c) In the **Install Adapter** dialog box, provide the required information.
For more information about the fields in this dialog box, see Upgrading a Standalone Node, on page 3.
d) Click **Upload**.
e) After the upload is complete, click **Submit**.

**Step 5** Do one of the following, depending on the Cisco ICFPP version:

- If you are upgrading from Cisco ICFPP 2.2.1 or 2.2.1a to 2.3.1, restart Infra services from the ShellAdmin console by first choosing **Stop Services** and then choosing **Start Services**.
- If you are upgrading from Cisco ICFPP 2.3.1 to a higher version, the Infra services are restarted automatically and you can log in to Cisco ICFPP after approximately two minutes.

**Step 6** Verify that the HA active node was successfully upgraded as follows:

a) Log in to the Cisco ICFPP GUI of the active node by using the management IP address of the node.
b) In GUI toolbar, click **About**.
c) Confirm that the correct version is displayed.
The version uses the format *version-build-patch*, such as 2.3.1-204-p208.

**Step 7** 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 8** 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 9** Log in to the ShellAdmin console for the standby node in the HA pair.

**Step 10** 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 11** 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 ICFPP GUI for the HA active node.
b) Upgrade the node as described in Step 4.
c) If needed, restart services as described in Step 5.
d) Verify that the upgrade was successful as described in Step 6.

**Step 12** 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 13** Upgrade each service node in the cluster as follows:
a) Log in to the Cisco ICFPP GUI for the service node.
b) Upgrade the service node by uploading and submitting the upgrade package as described in Step 4.
c) Do one of the following, depending on the Cisco ICFPP version:

- If you are upgrading from Cisco ICFPP 2.2.1 or 2.2.1a to 2.3.1, restart Infra services from the ShellAdmin console by first choosing **Stop Services** and then choosing **Start Services**.
- If you are upgrading from Cisco ICFPP 2.3.1 to a higher version, the Infra services are restarted automatically and you can log in to the service nodes after approximately two minutes.

**Step 14** Verify that each service node upgraded successfully as follows:
a) For each service node, refresh the browser and log in to the Cisco ICFPP GUI for the service node.
b) Click **About** in the GUI toolbar and confirm that the correct version is displayed.
The version uses the format *version-build-patch*, such as 2.3.1-204-p208.

# Managing Licenses

Cisco ICFPP is installed with an evaluation license and support for 20 VMs. The topics in this section describe how to update a license and view license details.

## Updating a License

To ensure continuous operation, update the Cisco ICFPP license before the current license expires.

### Before You Begin

Confirm that the license file is accessible from Cisco ICFPP.

### Procedure

**Step 1** Choose **Administration** > **License**.

**Step 2** In the **License Keys** tab, click **Update License**.

**Step 3** In the **Update License** dialog box, do one of the following:

- Select a license file to upload:
  1. Browse to and choose the license file.
  2. Click **Open**.
  3. Click **Upload**.
- Enter the license text:
  1. Check the **Enter License Text** check box.
  2. Copy the text of the license file and paste it into the **License Text** field.

**Step 4** Click **Submit**.

## Viewing License Details

After you install Cisco ICFPP, you can view license details at any time to confirm the term of the license, view the number of VMs supported, and obtain the license identifier.

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Administration** > **License**.

**Step 2** In the **License Keys** table, expand the required entry.
The license details are displayed, including the expiration date, license identifier, and the number of supported VMs.

# Monitoring Tasks

You can use the Cisco ICFPP GUI to monitor the tasks of the tenants.

In the Cisco ICFPP GUI, choose **Tenants** and then click the **Tasks** tab.

The **Tasks** pane displays the details and status of all tasks for the tenants.

# Obtaining Logs

You can use Cisco ICFPP logs to debug issues, collect system information, and review detailed information related to HA or cluster environments. For more information, see the following topics:


- Obtaining System Information, on page 9
- Downloading Logs for HA and Cluster Environments, on page 10


## Obtaining System Information

Cisco ICFPP can provide general or detailed system information, and can assist in troubleshooting issues. This information is also helpful if you need to contact Cisco for technical support.

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Administration** > **Support Information**.

**Step 2** From the **Support Information** drop-down list, choose the required option as described in the following table:

| Option | Description |
|---|---|
| System Information (Basic) | Displays status for system services, the Cisco ICFPP license, and accounts and resource usage. |
| System Information (Advanced) | Displays detailed system information including system configuration, running processes, memory usage, processor details, and task status. |
| Show Log | Displays the log that you select:<br>• Infra Manager<br>• Web Context Cloud Manager<br>• Tomcat Log<br>• Authenticator Log<br>• Mail Delivery Log<br>• Patch Log |

| Option | Description |
|---|---|
| Download All Logs | Downloads a zipped file of all logs. |
| Debug Logging | Enables debug logging and records up to 30 minutes of activity. |

## Downloading Logs for HA and Cluster Environments

Cisco ICFPP enables you to download the following logs associated with HA and cluster environments:

- Infra Manager log
- MySQL log
- Apache Catalina log
- OpenAPI log
- Scalability log
- HA log
- Install log
- Cisco ICFPP syslog messages log
- System messages log

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

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Administration** > **System**, and click the **Logs** tab.

**Step 2** Check the check box for each log that you want to download, and click **Download**.
A zipped file containing all requested logs is downloaded to your system.

# Generating Reports

Cisco ICFPP reports are available from the GUI in three formats: Tabular, Historical, and Snapshot. Cisco ICFPP dynamically updates the lists of the reports that are available to you and provides graphic renderings of each type of report. For each context, a different set of reports (each identified by a reportId) is available.

The available reports are:

- Tenant report

- Cloud instance report
- Virtual machine report
- Adapters report
- Faults report
- System tasks report

To generate a report:

**Procedure**

**Step 1** In the Cisco ICFPP GUI, navigate to the required object type. For example, to generate a VM report, you would choose **Tenants** > **All Tenants**, and click the **VM** tab.

**Step 2** In the toolbar, click **Export Report**.

**Step 3** In the **Export Report** dialog box, choose the required report format (PDF, CSV, or XLS) and click **Generate Report**.

**Step 4** After the report has been generated, click **Download**.

# 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 ICFPP GUI.

## Adding a Cloud Instance

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

**Procedure**

**Step 1** In the Cisco ICFPP GUI, choose **Cloud Instances**.

**Step 2** In the **Cloud Instances** pane, click **Add**.

**Step 3** In the **Add Cloud Instance** dialog box, provide the following information, and then click **Add**:

| Field | Description |
|---|---|
| **Cloud Instance Name** | The name of the cloud instance. |
| **Type** | The cloud instance type: Cisco or Custom. |

| Field | Description |
|---|---|
| **Module Name** | For a Cisco cloud instance type, choose the module name, such as OSP for OpenStack Platform.<br>For a custom cloud instance type, enter the custom module name. |
| **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. |
| **FTP Server Name** | For Cisco Intercloud Services — V modules, the name of the FTP server. |
| **Endpoint URI** | The endpoint URI for the cloud instance. |

# Viewing a Cloud Instance's Details

You can use the Cisco ICFPP GUI to view a cloud instance's details.

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Cloud Instances**.

**Step 2** In the **Cloud Instances** pane, choose a cloud instance and click **View**.
The **Cloud Instance Details** dialog box is displayed with the details of the cloud instance.

# Editing a Cloud Instance

You can use the Cisco ICFPP GUI to edit a cloud instance.

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Cloud Instances**.

**Step 2** In the **Cloud Instances** pane, choose a cloud instance and click **Edit**.

**Step 3** In the **Edit Cloud Instance** dialog box, update the following information as needed and click **Save**:

| Field | Description |
|---|---|
| **Cloud Instance Name** | The name of the cloud instance (read-only). |
| **Type** | The cloud instance type (read-only). |
| **Image Conversion Support on Cloud** | Displayed for custom cloud instance types only.<br>Indicate whether or not image conversion on the cloud is required. |
| **Module Name** | The module name (read-only). |
| **FTP Server Name** | For Dimension Data modules only, the FTP server name. |
| **Endpoint URI** | The URI for the cloud instance. |

## Deleting a Cloud Instance

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

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Cloud Instances**.

**Step 2** In the **Cloud Instances** pane, choose the required cloud instance and click **Delete**.

# Managing Tenants

The following topics describe how to add, edit, delete, and view tenants by using the Cisco ICFPP GUI.

## Adding a Tenant

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

For a CloudStack cloud instance, you must obtain the API Key and Secret Key for the tenant before adding the tenant. After the tenant is created, Cisco ICFPP generates a Pass Key, which is available in the **View Tenant** dialog box (**Tenants** > **All Tenants** > ***tenant*** > **View**). This Pass Key is required by Cisco Intercloud Fabric Director when configuring a cloud. For more information, see the *Cisco Intercloud Fabric User Guide*.

### Before You Begin

Confirm the following:

- A cloud has been created to which the tenant can be assigned.
- For a VMware vCloud Director cloud instance, you have the name of the organization for the tenant. For more information, see the VMware vCloud Director documentation.
- For a CloudStack cloud instance, you have the API Key and Secret Key for the tenant. For more information, see the Apache CloudStack documentation.

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Tenants** and click the **Accounts** tab.

**Step 2** Click **Add**.

**Step 3** In the **Add Tenant** dialog box, provide the information as described in the following table, and then click **Add**:

| Field | Description |
|---|---|
| **Tenant Name** | Enter the tenant name.<br>You cannot change the name after adding the tenant. |
| **Cloud Instance Name** | Choose the name of the cloud instance.<br>You cannot change the cloud instance name after adding the tenant. |
| **Enable Tenant Account** | |
| **Enabled** | (Read-only) Indicates whether or not the tenant account is enabled. The account is enabled by default. |
| **Org Name** | For VMware vCloud Director clouds, enter the name of the organization to which the tenant belongs. |
| **Resource Limits** | |
| **Max Servers** | Enter the maximum number of servers provisioned for the tenant, including stopped VMs. |
| **User Account** | |
| **Username** | Enter the account username. |
| **Email** | Enter the account email address. |
| **API Key** | For CloudStack clouds, enter the API key for the tenant. |
| **Secret Key** | For CloudStack clouds, enter the Secret key for the tenant. |

# Editing a Tenant

You can edit existing tenants by using the Cisco ICFPP GUI.

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Tenants** and click the **Accounts** tab.

**Step 2** In the **Accounts** pane, choose a tenant and click **Edit**.

**Step 3** In the **Edit Tenant** dialog box, update the information as needed and then click **Save**:

| Field | Description |
|---|---|
| **Tenant Name** | The name of the tenant (read-only). |
| **Cloud Instance Name** | The name of the cloud instance (read-only). |
| **Enable Tenant Account** | |
| **Enable** | Check the check box to enable the tenant account, or uncheck the check box to disable the tenant account. |
| **Org Name** | For VMware vCloud Director clouds only, the name of the organization to which the tenant belongs (read-only). |
| **Resource Limits** | |
| **Max Servers** | The maximum number of servers provisioned for the tenant, including stopped VMs. |
| **User Account** | |
| **Username** | The account username (read-only). |
| **Email** | The account email address. |
| **API Key** | For CloudStack clouds only, the API Key for the tenant. |
| **Secret Key** | For CloudStack clouds only, the Secret Key for the tenant. |

# Deleting a Tenant

You can use the Cisco ICFPP GUI to delete a tenant.

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Tenants**.

**Step 2** In the **Accounts** tab, choose the tenant that you want to delete, and then click **Delete**.

**Step 3** In the **Delete Tenant** dialog box:

1. Do one of the following:
   - Check the **Purge** check box to remove all tenant resources from the database. If you choose this option, the tenant is removed from the database and the GUI.
   - Uncheck the **Purge** check box to retain the tenant resources in the database. If you choose this option, the tenant is displayed in the GUI with a state of Deleted and the tenant's resources remain in the database.
2. Click **Delete**.

# Viewing a Tenant's Details

You can use the Cisco ICFPP GUI to view a tenant's details.

### Procedure

**Step 1** In the Cisco ICFPP GUI, choose **Tenants**.

**Step 2** Click the **Accounts** tab.

**Step 3** In the **Accounts**, choose the required tenant and click **View**.
The **Tenant Details** dialog box is displayed with the tenant details.

# Monitoring Tenants

You can use the Cisco ICFPP GUI to monitor tenant VMs.

In the Cisco ICFPP GUI, choose **Tenants** and then click the **VM** tab.

The **VM** pane displays the details and status of all tenant VMs.