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 Cisco ICFPP licenses, monitoring tasks, and accessing reports and logs.

Configuring Syslog Servers

You can configure Cisco ICFPP so that it forwards log messages to a server instead of recording them in a local file or displaying them.

Procedure

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

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

Step 3 In the **Minimum Severity** drop-down list, choose the minimum severity of the messages that are to be forwarded to the server. For example, if you choose Minor, messages with the severity Minor or Major will be forwarded to the server. If you choose Major, only messages with the severity Major will be forwarded to the server.

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

Field	Description
Server Address	IP address of the syslog server.
Protocol	Protocol to be used for the messages (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 (add) or update an adapter.

Procedure

Step 1 Log in to the Cisco ICFPP GUI.

Step 2 Choose **Install**.

Step 3 In the **Adapters** pane, click **Install**.

Step 4 In the **Install Adapter** dialog box, complete the following fields:

Field	Description
Adapter Type	Choose the adapter type: Cisco or Custom.
Adapter Name	The name of the adapter. If you chose **CISCO** as the adapter type, this field defaults to **CAPI** and cannot be edited.
Adapter Description	The description of the adapter.
Adapter File	The adapter file to use for this adapter. Browse to the required adapter file and click **Open**.

Step 5 Click **Upload**. The file is uploaded to Cisco ICFPP.

Step 6 After the upload is complete, click **Submit**.

Upgrading Cisco ICFPP

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:

- Upgrading a Standalone Node, on page 3
- Upgrading a Multiple-Node Cluster, on page 4

Upgrading a Standalone Node

Cisco ICFPP provides an upgrade mechanism that allows for Cisco bug fixes and upgrading adapters. Upgrading Cisco ICFPP to a newer version is similar to upgrading a custom adapter.

The procedures for upgrading a standalone node and a multiple-node cluster are different. For information on upgrading a multiple-node cluster, see Upgrading a Multiple-Node Cluster, on page 4.

Before You Begin

- Obtain the Cisco ICFPP upgrade file (icfpp-upgrade-2.2.1.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, enter the following information:

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 Click **Upload**.

Step 4 After the unload is complete, click **Submit**.

Step 5 Using SSH, log in to the ShellAdmin console for the virtual appliance.

Step 6 Choose the **Stop Services** option.

Step 7 Choose the **Start Services** option.
Cisco ICFPP is upgraded to the new version, and updated version information is displayed in the **Adapters** tab in the GUI.

Upgrading a Multiple-Node Cluster

This procedure describes how to upgrade a multiple-node cluster for bug fixes and updated adapters. For information on upgrading a standalone (single-node) Cisco ICFPP virtual appliance, see Upgrading a Standalone Node, on page 3.

The high-level tasks involved in upgrading a cluster are:

1. Upgrading the HA primary active node.
2. Stopping the virtual IP services on the upgraded primary active node.
3. Monitoring status as services fail over to the primary standby node.
4. Upgrading the HA primary standby node.
5. Stopping the virtual IP services on the upgraded primary standby node.
6. Starting the virtual IP services on the primary active node.
7. Starting the virtual IP services on the primary secondary node.
8. Upgrading and restarting Infra services for each service node.

The following procedure describes how to perform these tasks.

Before You Begin

- Obtain the Cisco ICFPP upgrade file (icfpp-upgrade-2.2.1.tar.gz) from cisco.com. For assistance, contact your Cisco representative.
- Ensure that the upgrade file is accessible from the Cisco ICFPP appliance.

Procedure

Step 1 Using the node management IP address (instead of the virtual IP address for the HA pair), log in to the Cisco ICFPP GUI for the primary active node in the HA pair.

Step 2 Upgrade the primary active node as follows:

a) Choose **Install** > **Adapters** > **Install**.

b) 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.

c) Click **Upload**.

d) After the upload is complete, click **Submit**.

Note Do NOT restart Infra services after upgrading the primary active node.

Step 3 Log in to the ShellAdmin console for the primary active node that was upgraded in Step 2.

Step 4 In the ShellAdmin console for the primary active node, stop the Virtual IP service as follows:

a) Choose the **Setup HA** option.
b) When asked if you want to reconfigure HA, enter **Y**.
c) Enter **C** to stop the VIP service.
d) Enter **Y** to confirm the action.
e) Press **Enter** to return to the ShellAdmin menu.

Step 5 Log in to the ShellAdmin console for the primary standby node for the HA pair.

Step 6 In the ShellAdmin console for the primary standby node, choose **Display Services Status** to monitor the following events as they occur:

- HA services fail over to the primary standby node in the HA pair.
- Infra services start running on the primary standby node.
- The primary standby GUI becomes available for logging in.
  It can take a few minutes for the services to start and for the GUI of the primary standby node to be accessible from the browser.

Step 7 Using the node management IP address (instead of the virtual IP address for the HA pair), log in to the Cisco ICFPP GUI for the primary standby node.

Step 8 Upgrade the primary standby node by uploading and submitting the upgrade package as described in Step 2 of this procedure.

Note Do NOT restart Infra services after upgrading the primary standby node.

Step 9 In the ShellAdmin console for the primary standby node that was upgraded in Step 8, stop the Virtual IP service as described in Step 4 of this procedure.

Step 10 In the ShellAdmin console for the primary active node that was upgraded in Step 2, start the Virtual IP service as follows:

a) Choose the **Setup HA** option.
b) When asked if you want to reconfigure HA, enter **Y**.
c) Enter **D** to start the VIP service.
d) Press **Enter** to return to the ShellAdmin menu.

Step 11 In the ShellAdmin console for the primary standby node that was upgraded in Step 8, start the Virtual IP service as described in Step 10.

Step 12 For each service node in the cluster:

a) Log in to the Cisco ICFPP GUI for the service node.
b) Upgrade each service node by uploading and submitting the upgrade package as described in Step 2.
c) Using the ShellAdmin console, restart Infra services by first choosing the **Stop Services** option and then choosing the **Start Services** option.

Managing Licenses

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

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 either 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.

Procedure

Step 1 Log in to the Cisco ICFPP GUI.

Step 2 Choose **Tenants** and then click the **Tasks** tab.
The **Tasks** pane displays the details and status of all of the 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 7
- Downloading Logs for HA and Cluster Environments, on page 8

Obtaining System Information

Cisco ICFPP can provide general or detailed system information, and can assist in troubleshooting issues. This information can also be 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.

Option	Description
Show Log	Displays the log that you select: • Infra Manager • Web Context Cloud Manager • Tomcat Log • Authenticator Log • Mail Delivery Log • Patch Log
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
- 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 will generate and download 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, or 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 ties the back-end cloud URI with a southbound adapter that is installed by the service provider. Multiple back-end URIs should have multiple cloud instances. A tenant is part of only one cloud instance. You can manage cloud instances by using the Cisco ICFPP GUI.

Adding a Cloud Instance

You can use the Cisco ICFPP GUI to add (provision) a cloud instance.

Procedure

Step 1 In the Cisco ICFPP, 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.
Module Name	For a **CISCO** cloud instance type, choose the module name, such as OSP for OpenStack. For a **CUSTOM** cloud instance type, enter the custom module name.
Image Conversion Support on Cloud	Displayed for OSP modules only. Indicate whether or not image conversion on the cloud is required.
FTP Server Name	For Dimension Data (DiData) modules only, 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 Intercloud Fabric Provider Platform (ICFPP) GUI to view a cloud instance's details.

Procedure

Step 1 Log in to the ICFPP.

Step 2 Choose **Cloud Instances**.

Step 3 In the **Cloud Instances** pane, choose a cloud instance.

Step 4 Click **View**.
The **Cloud Instance Details** dialog box appears, which contains the details of the cloud instance.

Step 5 Click **Close**.

Editing a Cloud Instance

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

To edit a cloud instance using the APIs, see Update Cloud Instance.

Procedure

Step 1 In the 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 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. 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 endpoint uniform resource identifier (URI) for the cloud instance.

Deleting a Cloud Instance

You can use the Cisco Intercloud Fabric Provider Platform (ICFPP) GUI to delete a cloud instance.

To delete a cloud instance using the APIs, see Delete Cloud Instance.

Procedure

Step 1 Log in to the ICFPP.

Step 2 Choose **Cloud Instances**.

Step 3 In the **Cloud Instances** pane, choose a cloud instance.

Step 4 Click **Delete**.

Step 5 In the **Delete Cloud Instance** dialog box, click **Delete**.

Managing Tenants

You can manage tenants by using the Cisco Intercloud Fabric Provider Platform (ICFPP) GUI.

Adding a Tenant

After you create a cloud instance, you can add (provision) 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. **Note** You cannot change this entry after the tenant is added.

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

Viewing a Tenant's Details

You can use the Cisco Intercloud Fabric Provider Platform (ICFPP) GUI to view a tenant's details.

To view a tenant's details using the APIs, see Get Tenant Details.

Procedure

Step 1 Log in to the ICFPP.

Step 2 Choose **Tenants**.

Step 3 Click the **Accounts** tab.

Step 4 In the **Accounts** pane, choose a tenant.

Step 5 Click **View**.
The **Tenant Details** dialog box appears, which contains the details of the tenant.

Step 6 Click **Close**.

Editing a Tenant

You can edit existing tenants as needed 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 account, or uncheck the check box to disable the 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.

To delete a tenant using the APIs, see Delete Tenant.

Procedure

Step 1 Log in to the Cisco ICFPP GUI.

Step 2 Choose **Tenants** and then click the **Accounts** tab.

Step 3 Choose the tenant that you want to delete, and then click **Delete**.

Step 4 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 will be 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 will be visible in the GUI with a state of Deleted and the tenant's resources will remain in the database.
2. Click **Delete**.

Monitoring Tenants

You can use the Cisco ICFPP GUI to monitor tenants' VMs.

Procedure

Step 1 Log in to the Cisco ICFPP GUI.

Step 2 Choose **Tenants** and then click the **VM** tab.
The **VM** pane displays the details and status of all VMs for the tenants.