Cisco IOx Local Manager Workflows

This chapter provides step-by-step procedures for many of the workflows and operations that you can perform with Cisco IOx Local Manager.

This chapter includes these sections:

Topic 1

App Lifecycle Workflows

App lifecycle workflows include the operations that you use to add, activate, deactivate, start, stop, upgrade, and delete an app.

There is no limit, other than system resource restrictions, on the number of apps that can simultaneously have the status of DEPLOYED. For PAAS apps, there also is no limit on how many can simultaneously have the status of ACTIVATED, or STARTED. For VM apps, only one can have the status of ACTIVATED or STARTED at a time.

The following sections describe these workflows:

Adding/Deploying an App

Adding an app uploads the app file to the host system. The app can be a tarball or OVA file. After you add the app, it appears on the Cisco IOx Local Manager Applications page and has status DEPLOYED. System CPU and RAM resources are not yet reserved for the app. An app with this status can be activated, upgraded, or deleted.

To add an app, perform the following steps.

Before You Begin

Make sure that the app tarball or OVA file is stored in a local or network location that the system from which you logged in to Cisco IOx Local Manager can access.

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Click the **Add/Deploy** button on the Applications page.
3. In the **Application ID** field in the Deploy application dialog box, enter a unique identifier to be assigned to the app.
4. In the Deploy application dialog box, click the **Choose File** button and follow the on-screen prompts to locate and select the app OVA or tarball file.
5. If you are adding an app OVA file, in the Deploy OVA dialog box, take these actions:
6. In the Deploy application dialog box, click the **OK** button.
7. In the Successfully Deployed dialog box, click the **OK** button.

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Click the **Add/Deploy** button on the Applications page.

The Deploy application dialog box displays.

Step 3 In the **Application ID** field in the Deploy application dialog box, enter a unique identifier to be assigned to the app.

The identifier can contain up to 64 letters, numbers, and underscores (_), in any combination.

Step 4 In the Deploy application dialog box, click the **Choose File** button and follow the on-screen prompts to locate and select the app OVA or tarball file.

If you choose an OVA file, the Deploy OVA dialog box displays. Continue to Step 5.

If you choose a tarball, skip to Step 6.

Step 5 If you are adding an app OVA file, in the Deploy OVA dialog box, take these actions:

a) If the OVA file includes a QEMU guest agent package, check the **OVA includes qemu-guest-agent** check box.
b) From the OS Type drop-down list, choose the operating system in which you will run the app (**Linux** or **Windows**.
c) Click the **OK** button.

Step 6 In the Deploy application dialog box, click the **OK** button.

The file uploads to the host system. This process can take some time. When the upload completes, the Successfully Deployed dialog box displays.

To ensure that the upload completes successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the upload is in process.

Step 7 In the Successfully Deployed dialog box, click the **OK** button.

Activating an App

Activating an app reserves host system CPU and memory (RAM) resources that the app requires to run, designates the network from which the app obtains its IP address, and assigns host system serial ports for use by the app, if requested. After you activate an app, its status on the Cisco IOx Applications page appears as ACTIVATED.

You can activate an app that has a status of DEPLOYED.

As part of the activation process, you designate a *resource profile* or a *resource payload*for the app. A resource profile defines the amount of CPU and memory resources that the app needs to run. You can choose from several preset resource profiles or enter custom values for a profile. A resource payload is a JSON file that defines resource, network, and related information for the app. See the App-ID > Resources Page section for more information.

When an app is activated, the host system reserves the resources that the app needs to run, but the resources are not used until the app starts. You cannot activate an app if the host system does not have sufficient resources available for the app to run.

In addition, for a PAAS app, the appropriate cartridges must be installed before the app can be activated.

To activate an app, follow these steps:

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **DEPLOYED** appears in the **Status** field for the app that you want to activate.
3. Click **activate** in the **Actions** field for the app that you want to activate.
4. Make sure that the **Resources** tab is selected on the *App-ID* page.
5. Take either of these actions:
6. In the Resource Profile area, take these actions to choose a resource profile, which designates the host system CPU and memory resources that the app requires when it runs:
7. In the Advanced Settings area, take the following actions as needed.
8. In the Network Configuration area, take the following actions to designate the logical network from which the app obtains its IP address.
9. (Optional) In the VNC Options area, take the following actions.
10. In the Peripheral Configuration area, take these actions to define peripheral devices that are attached to the host system and that the app controls:
11. If you are activating a Docker type app on a host system that does not support native Docker or are activating a PAAS type app, and if you want to run the app in debug mode, check the **debug mode** check box.
12. Click the **Activate** button top right of the Resources tab.

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **DEPLOYED** appears in the **Status** field for the app that you want to activate.

Step 3 Click **activate** in the **Actions** field for the app that you want to activate.

The *App-ID* page for the app appears.

Step 4 Make sure that the **Resources** tab is selected on the *App-ID* page.

Step 5 Take either of these actions:

a) If you want to activate the app using configuration information that is in a resource payload, click the **Activate using resource payload** link. In the window that pops up, click **Choose File**, navigate to and select the resource payload JSON file, and then click **Activate**.

The activation process executes and no further actions are needed.

b) If you want to activiate the app using resource, network, and related information that you configure on the Resources tab, continue with the next steps in this procedure

Step 6 In the Resource Profile area, take these actions to choose a resource profile, which designates the host system CPU and memory resources that the app requires when it runs:

a) From the **Profile** drop-down list, choose one of the following options, which designates the host system CPU and memory resources that the app requires when it runs on the host system:

- **c1.tiny**, **c1.small**, **c1.medium**, **c1.large**, or **c1.xlarge**—Assigns CPU and memory resources automatically. These values are based on the host system hardware.
- **default**—Assigns CPU and memory resources based on the requirement that is specified in the metadata for the app.
- **custom**—Lets you enter your own CPU and memory values in the CPU and memory fields.
- **exclusive**—Allocates all resources on the host system to the app.

If you choose an option other than **custom**, Cisco Local Manager enters information in the CPU and Memory fields based on the option that you choose, and these fields become read only.

b) If you choose **custom** from the Profile drop-down list, in the CPU field, enter the CPU units that the app requires on the host system when it runs, and in the Memory field, enter the amount of RAM, in MB, that the app requires when it runs. To enter CPU units, either click the **cpu-unit** radio button and enter the number of CPU units required, or click the **%** button and enter the percentage of total host system CPU units required.

Make sure that you do not enter a CPU or memory value that exceeds the available CPU or memory resources that display at the bottom of the Resource Profile area. If you enter a value that exceeds resource availability, the app cannot be activated.

c) In the **Disk** field, enter the disk space, in MB, that the app requires on the host system when it runs.

Make sure that you do not enter disk space value that exceeds the available disk space that displays at the bottom of the Resource Profile area. If you enter a value that exceeds resource availability, the app cannot be activated.

If needed, refer to the app documentation or developer for information regarding resources that an app requires when it runs.

Step 7 In the Advanced Settings area, take the following actions as needed.

This area appears only if the app type is Docker and the host system supports native Docker.

- In the **Docker Options** field, enter one or more Docker run options to be used when you activate the app.

  This field includes the --rm option by default (see the following bullet point).

- Check the **Auto delete container instance** check box to add the --rm run option to the Docker Options field and to use this option when you activate the app.

  When you stop an app that you activated and started with the --rm option, the app container instance is deleted automatically and the app goes to DEPLOYED state (rather than STOPPED state).

  This check box is checked by default.

Step 8 In the Network Configuration area, take the following actions to designate the logical network from which the app obtains its IP address.

The internal interfaces of the app in this area appear as eth*X* , where *X* is a number. The number of internal interfaces depend on the number of network interfaces that the app defines in its metadata. For example, if the app metadata defines one network interface, **eth0** appears in this area. If the app metadata defines two network interfaces, **eth0** and **eith1** appear in this area.

a) Click the **Add App Network Interface** button.
b) In the **Interface Name** field, enter a unique name for the interface. The name can be from 1 to 40 characters in length, and can include alphanumeric characters and underscores characters (_).
c) Click **OK**.
d) From the drop-down list that appears next to the interface name that you entered, choose an option to designate how the app obtains its IP address.

   In each drop-down list option, # is a number that matches the number at the end of the corresponding interface name of the internal Cisco IOx bridge that provides connectivity for an internal network. For example, the logical network iox-bridge0 corresponds to the interface name svcbr_0. Similarly, the logical network iox-nat1 corresponds to the interface name svcbr_1. *Description* is a description of the network interface.

   The options that are available in this list depend on the type of host system. Here are examples of some options that can appear:

   - iox-nat_docker0—App obtains its IP address from an internal native Docker network address translator
   - iox-bridge#—App obtains its IP address from a DHCP pool that is configured in Cisco IOS

   The **Port Mapping** link displays to the right of the drop-down list if you choose a nat type network from the drop-down list for an app whose metadata requests TCP or UDP ports to be open on a network interface and if the interface is connected to a NAT network.

   The **Interface Setting** link displays to the right of the drop-down list if you choose a network other than a nat type.

e) If the **Port Mapping** link displays, take these actions:

   1. Click the **PortMapping** link.

      The Port Mapping dialog box appears. This dialog box lets you configure TCP port mappings and UDP port mappings for the app. It also includes port mapping tables that show the mapping of internal ports to the corresponding external ports that the app requests, as defined in the metadata for the app.

   2. To cause the system to map ports automatically, click the **Auto** radio button, or to enter port mapping information manually, click the **Custom** radio button.

The system takes the auto action by default.

3. Click the **Add TCP port mapping** button, and take these actions:
   - In the **Internal Port(s)** field, enter the port from the app container that is to be mapped to the external port.
   - F you clicked the click the **Custom** radio button, in the **Internal Port(s)** field, enter the ports on the host system to which you want to map the corresponding internal ports.

   You can repeat this sub-step as needed to configure additional TCP port mappings.
4. Click the **Add UDP port mapping** button, and take these actions:
   - In the **Internal Port(s)** field, enter the port from the app container that is to be mapped to the external port.
   - f you clicked the click the **Custom** radio button, in the **Internal Port(s)** field, enter the ports on the host system to which you want to map the corresponding internal ports.

   You can repeat this sub-step as needed to configure additional TCP port mappings.
5. Click **OK**.

f) If the **Interface Setting** link displays, take these actions:

1. Click the **Interface Mapping** link.

   The Interface Setting dialog box appears. This dialog box lets you configure IPv4 and IPv6 interface settings for the app.
2. In the IPv4 Setting area click one of these radio buttons:
   - **Static**—Select this option to use a static IPv4 address. In the IP/Mask field that displays, enter the static address and subnet mask to use. In the DNS field that displays, optionally enter the IP address of the DNS server that the app uses for external communication. In the Gateway IP field that appears, enter the IP address of the gateway that the app uses for external communication. This field is optional if you do not check the **Default Gateway** check box, and is required otherwise. Check the **Default Gateway** check box if you want to make the gateway that you designate in the **Gateway IP** field the default gateway.
   - **Dynamic**—Select this option if you want to assign IPv4 addresses dynamically.
   - **Disable**—Select this option do not want to use an IPv4 address for the network interface.
3. In the IPv6 Setting area click one of these radio buttons:
   - **Static**—Select this option to use a static IPv6 address. In the IP/Mask field that displays, enter the static address and subnet mask to use. In the DNS field that displays, optionally enter the IP address of the DNS server that the app uses for external communication. In the Gateway IP field that appears, enter the IP address of the gateway that the app uses for external communication. This field is optional if you do not check the **Default Gateway** check box, and is required otherwise. Check the **Default Gateway** check box if you want to make the gateway that you designate in the **GatewayIP** field the default gateway.
   - **Dynamic**—Select this option if you want to assign IPv6 addresses dynamically.
   - **Disable**—Select this option do not want to use an IPv6 address for the network interface.
4. In the **DHCP Client IP** ID field, enter the DHCP client ID that is sent to the DHCP server.

If you enter a value, and if the DHCP server has been configured with a static binding that maps a client ID string to a specific IP address, the DHCP server assigns the mapped IP address to the app when the app boots up.

5. In the **Vlan ID** field, enter the identifier of the VLAN on which this internal network operates. Valid values are 1 through 4000.

   This field displays if your host system supports VLAN.

6. Check the **Mirror Mode Enabled** field, check box to enable port mirroring for the app. Port mirroring is used to monitor network traffic. When this option is enabled, copies of incoming and outgoing packets at the ports of a network device are flooded to the network bridge domain

   This check box displays if mirroring is asked for in the package.yaml file for the app and if the host system supports port mirroring on the selected network interface

7. Click **OK**.

g) Click the **Add** button to add the network interface.

You can repeat this Step 7 as needed to configure additional network interfaces.

Step 9 (Optional) In the VNC Options area, take the following actions.

The area appears only if the host system supports accessing an app via a VNC session.

- In the Password field, enter a password for accessing an app via a VNC session.

  Use this password in the VNC client that you use to access the app.

- In the Port field, enter a port number to be used for accessing the app via a VNC session.

  If you do not enter a port number, the system assigns a value. Valid port numbers are 5900 through 65535.

Step 10 In the Peripheral Configuration area, take these actions to define peripheral devices that are attached to the host system and that the app controls:

a) Click the **Add App Peripheral** button.

b) From the **Device Type** drop-down list, choose one of these options:

- **serial**—Displays if the host device supports serial ports for the app to use
- **USB_storage**—Displays if USB storage devices are available on the host device for the app to use
- **USB_serial**—Displays if USB serial devices are available on the host device for the app to use
- **USB_port**—Displays if the host device supports USB ports for the app to use

c) If you choose **serial** from the **Device Type** drop-down list, from the **Device Name** drop-down list, choose the device that you want. The items that display in this list depend on the serial ports that are available on the host system.

The **Device Name** drop-down list does not display if you choose **USB_storage** or **USB_serial** from the **Device Type** drop-down list.

d) If you choose **USB_storage** or **USB_serial** from the **Device Type** drop-down list, click a radio button to select the device that you want. The radio buttons that display depend on the devices that are connected to the host system.

e) In the **Label** field, type an ID for the app to use to identify the peripheral device.

f) Click **Add**.

You can repeat this Step 9 as needed to define additional peripheral devices.

Before you activate the app, you can click the **edit** link in the App Peripherals table to update configuration settings for the corresponding peripheral device, or click the **delete** link in this table to delete the corresponding device configuration.

Each device in the Peripherals table must be in the Present state for you to be able to activate the app.

Step 11 If you are activating a Docker type app on a host system that does not support native Docker or are activating a PAAS type app, and if you want to run the app in debug mode, check the **debug mode** check box.

If an app that is running in debug mode shuts down unexpectedly, the app does not go to STOPPED state. Instead, the app remains in RUNNING state so that you can use an SSH client to access the app and troubleshoot.

Step 12 Click the **Activate** button top right of the Resources tab.

If sufficient CPU and memory resources are available on the host system, the activation process executes. This process can takes some time.

To ensure that the activation completes successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the activation is in process.

Deactivating an App

Deactivating an app releases the host system CPU and memory (RAM) resources that were reserved for the app and makes these resources available of other uses. After you deactivate an app, its status on the Cisco IOx Applications page appears as DEPLOYED.

You can deactivate an app that has a status of ACTIVATED or STOPPED.

To deactivate an app, perform the following steps. This procedure has the same effect as clicking the **Deactivate** button on the *App-ID* > Resources page.

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **ACTIVATED** or **STOPPED** appears in the **Status** field for the app that you want to deactivate.
3. (Optional) If you want to save the resource, network, and related settings for the app in a resource payload JSON file, Click the **Download activation resource payload** link.
4. Click **deactivate** in the **Actions** field for the app that you want to deactivate.

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **ACTIVATED** or **STOPPED** appears in the **Status** field for the app that you want to deactivate.

Step 3 (Optional) If you want to save the resource, network, and related settings for the app in a resource payload JSON file, Click the **Download activation resource payload** link.

Cisco Local Manager saves the file in the default download directory on your local computer. The file is named *App-Name*_activation_rescources.json, where *App-Name* is the name of th app that you are deactivating. You can rename this file after you download it.

Step 4 Click **deactivate** in the **Actions** field for the app that you want to deactivate.

The deactivation process executes. This process can take some time. A progress bar indicates the status of the deactivation process.

To ensure that process executes successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the app is deactivating.

Starting an App

Starting an app starts the app container for the app on the host system. CPU and memory (RAM) resources that were reserved for the app become in use. After you start an app, its status on the Cisco IOx Applications page appears as RUNNING.

You can start an app that has a status of ACTIVATED or STOPPED.

To start an app, follow these steps:

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **ACTIVATED** or **STOPPED** appears in the **Status** field for the app that you want to start.
3. Click **start** in the **Actions** field for the app that you want to start.

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **ACTIVATED** or **STOPPED** appears in the **Status** field for the app that you want to start.

Step 3 Click **start** in the **Actions** field for the app that you want to start.

The starting process executes. This process can take some time.

To ensure that the app starts successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the app is starting.

Stopping an App

Stopping an app immediately shuts down its app container on the host system. CPU and memory (RAM) resources that were used by the app remain reserved for it but are not in use. After you stop an app, its status on the Cisco IOx Applications page appears as STOPPED.

You can stop an app that has a status of RUNNING.

To stop an app, follow these steps:

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **RUNNING** appears in the **Status** field for the app that you want to stop.
3. On the Applications page, click **stop** in the **Actions** field for the app that you want to stop.

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **RUNNING** appears in the **Status** field for the app that you want to stop.

Step 3 On the Applications page, click **stop** in the **Actions** field for the app that you want to stop.

The stopping process executes. This process can takes some time.

To ensure that the app stops successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the app is stopping.

Upgrading an App

Upgrading an app replaces it with another version. The replacement app must be in a tarball (a file in tar format).

You typically use this operation to replace an app with a newer version or with a version that addresses issues in the existing version. After you upgrade an app, its status on the Cisco IOx Applications page appears as DEPLOYED.

You can upgrade an app that has a status of DEPLOYED.

To upgrade an app, perform the following steps.

Before You Begin

Make sure that upgrade tarball is stored in a local or network location that the system from which you logged in to Cisco IOx Local Manager can access.

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **DEPLOYED** appears in the **Status** field for the app that you want to upgrade.
3. On the Applications page, click **upgrade** in the **Actions** field for the app that you want to upgrade.
4. In the Upgrade application dialog box, take these actions:

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **DEPLOYED** appears in the **Status** field for the app that you want to upgrade.

Step 3 On the Applications page, click **upgrade** in the **Actions** field for the app that you want to upgrade.

The Upgrade application dialog box appears.

Step 4 In the Upgrade application dialog box, take these actions:

a) Make sure that the **Application Id** field shows the identifier of the app that you want to upgrade.

b) Click the **Browse** button and follow the on-screen prompts to locate and select the upgrade tarball.

c) (Optional) Check the **Preserve Application Data** check box if you want the upgrade process to preserve existing app data.

This data includes information written to the app directory, app log files, and app configuration files. If you do not check this check box, the upgrade process deletes this data.

d) Click the **OK** button.

The upgrade process executes. This process can take some time.

To ensure that the upgrade completes successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the upgrade is in process.

Deleting an App

Deleting an app removes it from the host system and releases CPU and memory (RAM) resources that were reserved for the app. After you delete an app, it no longer appears on the Cisco IOx Applications page.

You can delete an app that has a status of DEPLOYED.

To delete an app, follow these steps:

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **DEPLOYED** appears in the **Status** field for the app that you want to delete.
3. Click **delete** in the **Actions** field for the app that you want to delete.

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **DEPLOYED** appears in the **Status** field for the app that you want to delete.

Step 3 Click **delete** in the **Actions** field for the app that you want to delete.

In the dialog box that prompts you to confirm the deletion, click **Yes**.

The delete process executes.

To ensure that the app deletes successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the app deletes.

App Management Workflows

App management workflows include the operations that you use for various app management activities, including updating an app configuration file, accessing an app via a console, and downloading an app log file.

These workflows also include operations that you use to upload files to the /data directory or subdirectory in an app container, download files to your local system, and delete files or subdirectories from the /data directory in an app container. The files can be configuration files or other files that an app needs when it runs.

The following sections describe the app management workflows:

Updating an App Configuration File

When an app starts, it can read its specific configuration information from a configuration file. This file is named package_config.ini. It is a text file that is stored in the /data directory in the app container for the app.

The package_config.ini file is included in the app .tar package. Its contents and format are flexible and are defined by the app developer. It must be a text file, and its name and location cannot be changed.

This section explains how to update the contents of an package_config.ini file from Cisco IOx Local Manager. You also can update this file by accessing the /data directory in the app container through a console and editing package_config.ini.

To update an app configuration file from Cisco IOx Local Manager, follow these steps:

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Click **manage** in the **Actions** field for the app for which you want to update a configuration file.
3. On the *App-ID* page, choose the **App-Config** tab.
4. In the *App-ID* > App-Config page, take these actions:

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Click **manage** in the **Actions** field for the app for which you want to update a configuration file.

The *App-ID* page for the app appears.

Step 3 On the *App-ID* page, choose the **App-Config** tab.

Step 4 In the *App-ID* > App-Config page, take these actions:

a) In the text field, enter configuration information for the app.

b) Click the **Save** button.

Accessing an App Container or VM from a Console System

If an app is running, you can access its container (for a PAAS app) or VM (for a KVM app) via a console system. After you access the container or VM, you can use Linux console commands to obtain information about the app.

You also can access a terminal shell or a terminal console for an app directly from Cisco Local Manager, as described in the Accessing a Terminal Shell or a Terminal Console for an App from Cisco Local Manager, on page 14 section.

terminal shell or a terminal console

To access an app container of VM from a console system, perform the following steps.

Before You Begin

Use Cisco IOS configuration options to forward an SSH port on the router that you want to use for console access to port 22 on the Cisco IOx host system. For instructions, see your Cisco IOS documentation.

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **RUNNING** appears in the **Status** field for the app that you want to access.
3. Click **manage** in the **Actions** field for the app that you want to access.
4. On the *App-ID* page, choose the **App-Info** tab.
5. On the *App-ID* > App-Info page, take these actions to obtain the private key that you need for console access:
6. On the system from which you logged in to Cisco IOx Local Manager, take these actions:
7. Take these actions to connect to the host system from a console:

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **RUNNING** appears in the **Status** field for the app that you want to access.

Step 3 Click **manage** in the **Actions** field for the app that you want to access.

The *App-ID* page for the app appears.

Step 4 On the *App-ID* page, choose the **App-Info** tab.

Step 5 On the *App-ID* > App-Info page, take these actions to obtain the private key that you need for console access:

a) In the Console Access area, click the *app_id***.pem** link that appears in the sample command, where *app_id* is the identifier of the app.

b) In the dialog box that displays, highlight and copy all text that displays.

Make sure to include the "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----" text.

c) Click the **OK** button to close the dialog box.

Step 6 On the system from which you logged in to Cisco IOx Local Manager, take these actions:

a) Use a text editor to create a text file called *app_id* .pem, where *app_id* is the identifier of the app whose container or VM you want to access.

b) Paste the private key that you copied into this file, and save it locally.

c) Make sure that this file has the Linux permission 700.

Step 7 Take these actions to connect to the host system from a console:

a) From the console system, start an SSH client, and enter the command that appears in the Console Access area on the *App-ID* > App-Info page.

When you enter the command:

- Replace **<SSH_PORT>** with the port number for console access to the host system.
- Replace *app_id***.pem** with the path to the file that you created in Step 6, if the file is not in the current directory.

b) Use the commands in your SSH client to complete the connection process.

Accessing a Terminal Shell or a Terminal Console for an App from Cisco Local Manager

If an app is in the RUNNING state, you can access a terminal shell for a container app or a terminal console for a VM app from Cisco Local Manager. Then you can use Linux console commands to obtain information about the app.

You also can access an app container or VM for an app from a console system, as described in the Accessing an App Container or VM from a Console System, on page 13 section.

To access a terminal shell or terminal console from Cisco Local Manager, perform the following steps.

Before You Begin

- Make sure that the application exec console service is enabled in Local Manager. To do so, click the **Enable Application Exec Console Service** button in the System Setting page. See the System Setting Page section.
- Configure port 8445 must be configured on the router for forwarding traffic. For instructions, see your Cisco IOS documentation.
- A container app must have the /bin/sh, /bin/bash/, or /bin/ash shell in its root filesystem. A VM app must have the getty service configured for serial port access.

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **RUNNING** appears in the **Status** field for the app that you want to access.
3. Click **manage** in the **Actions** field for the app that you want to access.
4. On the *App-ID* page, choose the **App-Console** tab.
5. From the Command drop-down list on the App Console page, choose one of the following commands for connecting to the VM or Console:

- For a container app—**/bin/sh**, **/bin/bash**, or **/bin/ash**
- For a KVM app—**Attach Console**

6. When you are finished, click **Disconnect** to exit the terminal shell or terminal console session.

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **RUNNING** appears in the **Status** field for the app that you want to access.

Step 3 Click **manage** in the **Actions** field for the app that you want to access.

The *App-ID* page for the app appears.

Step 4 On the *App-ID* page, choose the **App-Console** tab.

Step 5 From the Command drop-down list on the App Console page, choose one of the following commands for connecting to the VM or Console:

- For a container app—**/bin/sh**, **/bin/bash**, or **/bin/ash**
- For a KVM app—**Attach Console**

Step 6 When you are finished, click **Disconnect** to exit the terminal shell or terminal console session.

For security, the session also disconnects if you exit the App-Console page, refresh this page, or exit your browser.

Downloading an App Log File

An app writes information about its operation and related activities to app log files that it creates in the /data/logs directory in the app container for the app. You can download an app log file from the host system to the location of your choice.

To download an app log file, follow these steps:

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Click **manage** in the **Actions** field for the app for which you want to download a log file.
3. On the *App-ID* page, choose the **Logs** tab.
4. On the *App-ID* > Log page, click **Download** in the **Download** field for the app log file that you want.
5. Follow the on-screen prompts to save the file in the location of your choice.

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Click **manage** in the **Actions** field for the app for which you want to download a log file.

The *App-ID* page for the app appears.

Step 3 On the *App-ID* page, choose the **Logs** tab.

Step 4 On the *App-ID* > Log page, click **Download** in the **Download** field for the app log file that you want.

Step 5 Follow the on-screen prompts to save the file in the location of your choice.

Uploading a File to an App Data Directory

Uploading a file puts a file into the designated location under the /data directory of the container for an app. The app must be in the ACTIVATED, RUNNING, or STOPPED state. This operation is not available for use when an app is in the DEPLOYED state.

To upload a file to an app /data directory, follow these steps:

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **ACTIVATED**, **RUNNING**, or **STOPPED** appears in the **Status** field for the app for which you want to upload a file.
3. Click **manage** in the **Actions** field for the app for which you want to upload a file.
4. On the *App-ID* page, choose the **App-DataDir** tab.
5. In the *App-ID* > App-DataDir page, click the **Upload** button.
6. In the Upload Configuration dialog box, take these actions:

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **ACTIVATED**, **RUNNING**, or **STOPPED** appears in the **Status** field for the app for which you want to upload a file.

Step 3 Click **manage** in the **Actions** field for the app for which you want to upload a file.

The *App-ID* page for the app appears.

Step 4 On the *App-ID* page, choose the **App-DataDir** tab.

Step 5 In the *App-ID* > App-DataDir page, click the **Upload** button.

The Upload Configuration dialog box displays.

Step 6 In the Upload Configuration dialog box, take these actions:

a) If you want to upload the file to a subdirectory of the /data directory, enter that subdirectory path in the Path field. Do not precede the path with any text, including a slash (/) or **/data**.

If you enter a path that does not exist, the system creates that path under the /data directory.

If you want to upload the file to the top level of the /data directory, do not enter a path in this field.

b) Click the **Browse** button and follow the on-screen prompts to navigate to and select the file to upload.
c) Click the **OK** button.

The upload process executes. This process can take some time. A progress bar indicates the status of the upload process.

To ensure that the file uploads successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the file is uploading.

Downloading a File from an App Data Directory

Downloading a file from an app /data directory file saves a copy of the file to your local PC. The app for which you are downloading a file must be in the ACTIVATED, RUNNING, or STOPPED state. This operation is not available for use when an app is in the DEPLOYED state.

To download a file from an app /data directory, follow these steps:

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **ACTIVATED**, **RUNNING**, or **STOPPED** appears in the **Status** field for the app for which you want to download a file.
3. Click **manage** in the **Actions** field for the app for which you want to download a file.
4. On the *App-ID* page, choose the **App-DataDir** tab.
5. In the *App-ID* > App-DataDir page, take these actions:

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **ACTIVATED**, **RUNNING**, or **STOPPED** appears in the **Status** field for the app for which you want to download a file.

Step 3 Click **manage** in the **Actions** field for the app for which you want to download a file.

The *App-ID* page for the app appears.

Step 4 On the *App-ID* page, choose the **App-DataDir** tab.

Step 5 In the *App-ID* > App-DataDir page, take these actions:

a) In the Name field, navigate to and click the name of the file that you want to download.
b) Follow the on-screen prompts to save the file.

Deleting a File or Directory from an App Data Directory

Deleting a file or directory from an app /data directory permanently removes the item from the directory. The app for which you want to delete a file or directory must be in the ACTIVATED, RUNNING, or STOPPED state. This operation is not available for use when an app is in the DEPLOYED state.

To delete a file or directory from an app /data directory, follow these steps:

SUMMARY STEPS

1. Choose **Applications** from the Cisco IOx Local Manager menu bar.
2. Make sure that **ACTIVATED**, **RUNNING**, or **STOPPED** appears in the **Status** field for the app for which you want to delete a /data directory file or directory.
3. Click **manage** in the **Actions** field for the app for which you want to delete a /data directory file or directory.
4. On the *App-ID* page, choose the **App-DataDir** tab.
5. In the *App-ID* > App-DataDir page, click **delete** in the **Actions** field for the file or directory that you want to delete.
6. In the dialog box that prompts you to confirm the deletion, click **Yes**.

DETAILED STEPS

Step 1 Choose **Applications** from the Cisco IOx Local Manager menu bar.

The Applications page displays.

Step 2 Make sure that **ACTIVATED**, **RUNNING**, or **STOPPED** appears in the **Status** field for the app for which you want to delete a /data directory file or directory.

Step 3 Click **manage** in the **Actions** field for the app for which you want to delete a /data directory file or directory.

The *App-ID* page for the app appears.

Step 4 On the *App-ID* page, choose the **App-DataDir** tab.

Step 5 In the *App-ID* > App-DataDir page, click **delete** in the **Actions** field for the file or directory that you want to delete.

Step 6 In the dialog box that prompts you to confirm the deletion, click **Yes**.

The delete process executes. This process can take some time.

To ensure that the file deletes successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the file is deleting.

App Group Workflows

App group workflows include the operations that you use to add and manage app groups. An app group is a set of apps with different Docker images that is defined in a Docker Compose YAML file.

These workflows include operations that you use to add, manage, and delete app groups, and to perform operations on individual apps in the group.

The following sections describe the app group workflows:

Adding an App Group

Adding an app group uploads an app group spec file, which is a Docker compose YAML file that defines the services (apps) to include in the app group and configuration information such network parameters for the services.

To add an app group, follow these steps:

SUMMARY STEPS

1. Choose **App Groups** from the Cisco IOx Local Manager menu bar.
2. Click the **Add New** button.
3. In the Display App Group dialog box, take these actions:
4. When you see the message Application Group Successfully Imported, click **OK**.

DETAILED STEPS

Step 1 Choose **App Groups** from the Cisco IOx Local Manager menu bar.

The App Groups page displays.

Step 2 Click the **Add New** button.

The Display App Group dialog box displays.

Step 3 In the Display App Group dialog box, take these actions:

a) In the App Group ID field, enter a unique identifier for the app group.

The identifier can contain up to 64 letters, numbers, and underscores (_), in any combination.

b) Click the **Select App Group spec** field and use the dialog box that appears to locate and select the Docker compose file that you want to add.

c) Click **OK**.

The system uploads the app group. A progress bar and messages indicate the status of the process.

Step 4 When you see the message Application Group Successfully Imported, click **OK**.

Uploading an App in an App Group

Use the upload feature to upload an app in an app group for the first time or to upgrade an app that has already been uploaded. The upload feature is available for apps that are in the following states in the Apps Group page:

- IMAGE UNAVAILABLE—When an app is in this state, the upload feature uploads the app image to the device for the first
- DEPLOYED—When an app is in this state, the upload feature upgrades the version of the app on the device to the version that you upload

To upload an image for an app in an app group, follow these steps:

SUMMARY STEPS

1. Choose **App Groups** from the Cisco IOx Local Manager menu bar.
2. Click the **Upload** button in the Action column for the app that you want to upload.
3. In the Upload/Upgrade Application dialog box, take these actions:
4. 4When you see the message that the upload is successful, click **OK**.

DETAILED STEPS

Step 1 Choose **App Groups** from the Cisco IOx Local Manager menu bar.

The App Groups page displays.

Step 2 Click the **Upload** button in the Action column for the app that you want to upload.

The Upload/Upgrade Application dialog box displays.

Step 3 In the Upload/Upgrade Application dialog box, take these actions:

a) Click the **Choose File** button and use the dialog box that appears to locate and select the app image that you want to upload.
b) Click **OK**.

Step 4 4When you see the message that the upload is successful, click **OK**.

Managing an App in an App Group

You can access pages for managing individual apps in an app group. These pages provide options for viewing information about an app, updating the configuration file for the app, managing the contents of the /data directory in the app container, and view information about the app log files that the app creates.

To manage an app in an app group, follow these steps:

SUMMARY STEPS

1. Choose **App Groups** from the Cisco IOx Local Manager menu bar.
2. Click the **Manage** button in the Action column for that app that you want to manage.

DETAILED STEPS

Step 1 Choose **App Groups** from the Cisco IOx Local Manager menu bar.

The App Groups page displays.

Step 2 Click the **Manage** button in the Action column for that app that you want to manage.

The Manage page for the app displays. This page includes these tabs:

- App-Info—Displays system, resource, and network information that relates to an app. It also provides information that you can use to access an app via a console.

  For a description of the fields and options on this page, see the App-ID > App-info Page section.

- App-Config—Lets you update the configuration file for the app.

  For a description of the fields and options on this page, see the App-ID > App-Config Page section.

- App-DataDir—Lets you see the contents of the /data directory in the app container of the app, upload files to the /data directory or subdirectory, download files to your local system, and delete files or subdirectories from the /data directory.

  For a description of the fields and options on this page, see the App-ID > App-DataDir Page section.

- Logs—Provides information about the app log files that the app creates in the /data/logs directory in the app container for the app, and lets you download these log files.

  For a description of the fields and options on this page, see the App-ID > Logs Page section.

Bringing Up and Starting an App Group

You can bring up, or bring up and start, an app group that is in the DEPLOYED, ACTIVATED, or STOPPED state.

Bringing up an app group moves the app group to the ACTIVATED state, activates the apps in the app group, and moves the apps in the app group to the ACTIVATED state.

Bringing up and starting an app group moves the app group to the RUNNING state, activates and starts the apps in the app group, and moves the apps in the app group to the RUNNING state.

To bring up or bring up and start an app group, follow these steps:

SUMMARY STEPS

1. Choose **App Groups** from the Cisco IOx Local Manager menu bar.
2. Click the **Up** button in the App Group Area for the app group that you want to bring up or bring up and start.
3. Click one of these options:
4. When you see the message that the operation was successful, click **OK**.

DETAILED STEPS

Step 1 Choose **App Groups** from the Cisco IOx Local Manager menu bar.

The App Groups page displays.

Step 2 Click the **Up** button in the App Group Area for the app group that you want to bring up or bring up and start.

Step 3 Click one of these options:

- **Up with App Start**—Moves the app group to the RUNNING state
- **Up without App Start**—Moves the app group to the ACTIVATED state

The system performs the operation that you choose. This process can take some time. A progress bar and messages indicate the status of the process.

To ensure that the operation is successful, do not refresh your browser or attempt another Cisco IOx Local Manager operation until the conversion completes.

Step 4 When you see the message that the operation was successful, click **OK**.

Bringing Down and Destroying an App Group

You can bring down, or bring down and destroy (stop), an app group that is in the ACTIVATED, RUNNING, or STOPPED state.

Bringing down an app group moves it to the STOPPED state, deactivates the apps in the app group, and moves the apps in the app group to the DEPLOYED state.

Bringing down and destroying an app group moves to the DEPLOYED state, stops and deactivates the apps in the app group, and moves the apps in the app group to the DEPLOYED state. This operation releases CPU and memory (RAM) resources that were reserved for each app in the app group.

To bring down or bring down and destroy an app group, follow these steps:

SUMMARY STEPS

1. Choose **App Groups** from the Cisco IOx Local Manager menu bar.
2. Click the **Down** button in the App Group Area for the app group that you want to bring down or bring down and destroy.
3. Click one of these options:
4. When you see the message that the operation was successful, click **OK**.

DETAILED STEPS

Step 1 Choose **App Groups** from the Cisco IOx Local Manager menu bar.

The App Groups page displays.

Step 2 Click the **Down** button in the App Group Area for the app group that you want to bring down or bring down and destroy.

Step 3 Click one of these options:

- **Down with App Destroy**—Moves the app group to the DEPLOYED state, stops and deactivates the apps in the app group, and moves the apps in the app group to the DEPLOYED state
- **Down without App Destroy**—Moves the app group to the STOPPED state, deactivates the apps in the app group, and moves the apps in the app group to the DEPLOYED state

The system performs the operation that you choose. This process can take some time. A progress bar and messages indicate the status of the process.

To ensure that the operation is successful, do not refresh your browser or attempt another Cisco IOx Local Manager operation until the conversion completes.

Step 4 When you see the message that the operation was successful, click **OK**.

Managing an App Group

You can access pages for managing an app group. These pages provide options for displaying and optionally editing the contents of the Docker compose YAML file for the app group, and for viewing information about the group and its apps.

To manage an app group, follow these steps:

SUMMARY STEPS

1. Choose **App Groups** from the Cisco IOx Local Manager menu bar.
2. Click the **Manage** button in the App Group Area for the app group that you want to manage.
3. In the Manage App Group page, take the following actions as needed

DETAILED STEPS

Step 1 Choose **App Groups** from the Cisco IOx Local Manager menu bar.

The App Groups page displays.

Step 2 Click the **Manage** button in the App Group Area for the app group that you want to manage.

The Manage App Group page for the app group displays.

Step 3 In the Manage App Group page, take the following actions as needed

- Click the **App Group Spec** tab to display and optionally edit the contents of the Docker compose YAML file for the app group. This file is the Select App Group spec file that you selected when you added the app group.

  When the app group is in the DEPLOYED state, you can click the **Edit** button to edit this file in this tab. After you edit the file, click the Save button. The tab closes and the app group information updates automatically according to the updates that you made.

- Click the **App Group Info** tab to display the following information for the app group:

Field	Description
AppGroup Info Displays the following general information for the app group:	

Field	Description
App Group ID	The state of the app group displays at the top left of an app group box. The state can be one of the following: • **DEPLOYED**—The app group has been added but some or all apps in the app group have not been uploaded. • **ACTIVATED**—Each app in the group is on the host system and ready to run. System CPU and RAM resources have been reserved for the apps but are not yet in use. • **RUNNING**—Each app in the group is operating on the host system. System CPU and RAM resources are in use for the apps. • **STOPPED**—Each the app group has been running on the host system but its operation has been stopped. System CPU and RAM resources remain reserved for the group.
Version	Name of the Docker compose YAML file for the app group.
Start Order	Order in which the system starts the apps in the group when you bring up and start the apps.
Services Displays the following set of information for each app in the app group:	
App State	Status of the app, which can be DEPLOYED, ACTIVATED, RUNNING, STOPPED, or IMAGE UNAVAILABLE.
Image	Name of the app image.
Restart	Docker restart policy, which decides the condition in which the app automatically restarts.
Networks	Network used by the app.
Dependencies	List of other apps on which the app is dependent.
Volumes	Docker volumes that the app uses.

Deleting an App Group

Deleting an app group removes it from the host system. This process also removes from the host system the Docker Compose YAML file for the app group. This process does not remove the images of the apps in the app group.

To delete an app group, follow these steps:

SUMMARY STEPS

1. Choose **App Groups** from the Cisco IOx Local Manager menu bar.
2. Click the **Delete** button in the App Group Area for the app group that you want to delete.
3. In the dialog box that prompts you to confirm the deletion, click **Yes**.

DETAILED STEPS

Step 1 Choose **App Groups** from the Cisco IOx Local Manager menu bar.

The App Groups page displays.

Step 2 Click the **Delete** button in the App Group Area for the app group that you want to delete.

Step 3 In the dialog box that prompts you to confirm the deletion, click **Yes**.

The delete process executes. This process can take some time.

To ensure that the app group deletes successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the app group is deleting.

Cartridge Management Workflows

A Cisco IOx app can be a PAAS type, a KVM type, LXC app, or a Docker type. Unlike a KVM, Docker, or LXC, a PAAS app, which typically is created with a higher-level language such as Java or Python, is in a package that contains only files for the app logic. The package does not include Linux operating system files or the root file system that the app requires.

To activate, a PAAS app requires cartridges, which are Cisco-provided files that you install on the host system.

If an app requires cartridges but the cartridges are not yet installed, you can still add the app in Cisco IOx Local Manager. However, you must install the required cartridges before you can activate the app. To determine whether an app requires cartridges, you can look at the **Cartridge Required** field on the *App-ID* > App-Info page. See the App-ID > App-info Page section for more information.

Cartridge management workflows include the operations that you use to install, delete, and view information about cartridges. The following sections describe these workflows:

Installing a Cartridge

Installing a cartridge uploads it to the host system and makes it available to the apps that require it.

To install a cartridge, perform the following steps.

Before You Begin

Make sure that the cartridge file is stored in a local or network location that the system from which you logged in to Cisco IOx Local Manager can access.

SUMMARY STEPS

1. Choose **Docker Layers** from the Cisco IOx Local Manager menu bar.
2. Click the **Install** button in the Cartridges area on the Docker Layers page.
3. In the Deploy Cartridge dialog box, take these actions:
4. In the Successfully Deployed dialog box, click **OK**.

DETAILED STEPS

Step 1 Choose **Docker Layers** from the Cisco IOx Local Manager menu bar.

The Docker Layers page displays.

Step 2 Click the **Install** button in the Cartridges area on the Docker Layers page.

The Deploy Cartridge dialog box displays.

Step 3 In the Deploy Cartridge dialog box, take these actions:

a) Click the **Browse** button and follow the on-screen prompts to locate and select the cartridge file.
b) Click the **OK** button.

The cartridge file installs on the host system. This process can take some time. When the upload completes, the Successfully Deployed dialog box displays.

To ensure that the cartridge deploys successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the deployment is in process.

Step 4 In the Successfully Deployed dialog box, click **OK**.

Deleting a Cartridge

Deleting a cartridge removes it from the host system. Apps that require this cartridge cannot be activated until the cartridge is installed again.

To delete a cartridge, perform the following steps.

Before You Begin

Deactivate all apps that use the cartridge, as described in the Deactivating an App, on page 8 section.

SUMMARY STEPS

1. Choose **Docker Layers** from the Cisco IOx Local Manager menu bar.
2. On the Docker Layers page, click **Delete** in the **Actions** field for the cartridge that you want to delete.
3. In the dialog box that prompts you to confirm the deletion, click **Yes**.

DETAILED STEPS

Step 1 Choose **Docker Layers** from the Cisco IOx Local Manager menu bar.

The Docker Layers page displays.

Step 2 On the Docker Layers page, click **Delete** in the **Actions** field for the cartridge that you want to delete.

Step 3 In the dialog box that prompts you to confirm the deletion, click **Yes**.

The delete process executes. This process can take some time.

To ensure that the cartridge deletes successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the cartridge is deleting.

Viewing Detailed Information about a Cartridge

You can view detailed information about any cartridge that is installed on the host system. To do so, follow these steps:

SUMMARY STEPS

1. Choose **Docker ayers** from the Cisco IOx Local Manager menu bar.
2. On the Docker Layers page, click **Info** in the **Actions** field for the cartridge for which you want to view detailed information.

DETAILED STEPS

Step 1 Choose **Docker ayers** from the Cisco IOx Local Manager menu bar.

The Docker Layers page displays.

Step 2 On the Docker Layers page, click **Info** in the **Actions** field for the cartridge for which you want to view detailed information.

The Cartridge Information window displays.

Layer Management Workflow

A layer is a component of a Docker image from which an app package has been created.

When Local Manager installs an app, the Cisco application-hosting framework identifies the layers that the app requires and installs the required layers.

When you delete an app, the system does not automatically remove from the host system the layers that relate to that app. Similarly, when you upgrade an app and the new version no longer needs some layers that were used by the older version, the system does not automatically remove from the host system the layers that are no longer used. In both cases, if you want to remove unused layers from the device, you must remove them manually. This process is useful if you need to free up disk space on this host system.

You can delete any layer that is not in use by an installed app. To do so, follow these steps:

SUMMARY STEPS

1. Choose **Docker Layers** from the Cisco IOx Local Manager menu bar.
2. On the Cartridges page, click **Delete Unused Layers** at the bottom of the Layers area.

DETAILED STEPS

Step 1 Choose **Docker Layers** from the Cisco IOx Local Manager menu bar.

The Docker Layers page displays.

Step 2 On the Cartridges page, click **Delete Unused Layers** at the bottom of the Layers area.

Remote Docker App Workflow

Cisco Local Manager provides access from your local PC to Docker apps on the host system so that you can test and troubleshooting these apps. After you enable this remote Docker access, you download to your local PC a TLS certificate file, which allows communication with the Docker engine on the host system. You then can create a Docker app profile, which sets up app network interfaces, peripheral devices, and a persistent data file on the platform.

As part of this profile creation, Cisco IOx provides associated Docker runtime options for you to use when you run the app.

After your local PC is set up for remote Docker access, you can run the Docker app on the host system. When you have validated that the app runs as it should, you can generate and download an IOx package descriptor (package.yaml) file for the app. You can use this package.yaml file and the ioxclient tool to create the IOx application package, which you should verify again by deploying the app.

To enable remote Docker access, create a Docker app profile, and test the app, follow these steps:

SUMMARY STEPS

1. Choose **Remote Docker Workflow** from the Cisco IOx Local Manager menu bar.
2. In the Step 1, Enable Remote Docker Access area, take these actions:
3. Copy the TLS certs.tar file to one of these directories:
4. Set the following environment variables as shown on your local system to provide access from your local machine to the Docker engine:
5. In the App Profile area, take one of the following actions.
6. If you are creating a new Docker app profile, take the following actions in the App Resource area:
7. If you are creating a new Docker app profile, in the App Network Interfaces area, take these actions to configure the interfaces that the app uses for network access:
8. If you are creating a new Docker app profile, in the App Peripherals area, take these actions to define peripheral devices that are attached to the host system and that the app controls:
9. (Optional) In the App Persistent Data area, take the following actions to upload a data file to the profile.
10. Click the **Submit** button to save the information that you configured for the Docker app profile.

11. To test the app by running it on a local machine, enter the following command on the remote machine.
12. When you are satisfied with the operation of the app, take these actions in the Docker Runtime Options area to generate a package.yamls file for the app:

DETAILED STEPS

Step 1 Choose **Remote Docker Workflow** from the Cisco IOx Local Manager menu bar.

The Remote Docker Workflow page displays.

Step 2 In the Step 1, Enable Remote Docker Access area, take these actions:

a) If the **Enable Remote Docker Access** button displays, click this button to enable remote Docker access.

This button displays as **Disable Remote Docker Access** if Remote Docker Access is enabled already.

b) Click the **Download** button and follow the on screen prompts to download the tlscerts.tar file to your local machine.

Step 3 Copy the TLS certs.tar file to one of these directories:

- On Linux or macOS systems: $HOME/.docker
- On Microsoft Windows systems: %USERPROFILE%/.docker

Step 4 Set the following environment variables as shown on your local system to provide access from your local machine to the Docker engine:

- DOCKER_HOST=tcp://*Externally_Reacheable_Host_Sytem_IP_Address*:2376
- DOCKER_TLS=1
- DOCKER_API_VERSION=1.37

Step 5 In the App Profile area, take one of the following actions.

A Docker app profile defines host system resources that the app requires, network interfaces for the app, peripheral devices that the app controls, and a persistent data file for the app.

- To use an existing Docker app profile, choose the profile from the **Docker App Profiles** drop-down list. Skip to Step 9.
- To create a new Docker app profile, click the **Add New** button, enter a unique name for the profile in the Profile Name field, and then click the **OK** button. The name can be from 1 to 40 characters in length, and can include alphanumeric characters and underscores (_). Continue to Step 6.
- To delete an existing Docker app profile, choose the profile from **Docker App Profiles** drop-down list, click the **Delete** button, and then click **Yes** in the confirmation dialog box that pop up.

Step 6 If you are creating a new Docker app profile, take the following actions in the App Resource area:

a) From the Profile drop-down list, choose a resource profile, which designates the host system CPU and memory resources that the app requires when it runs on the host system.

Cisco Local Manager provides these resource profiles:

- **c1.tiny**, **c1.small**, **c1.medium**, **c1.large**, or **c1.xlarge**—Assigns CPU and memory resources automatically. These values are based on the host system hardware.

- **default**—Assigns CPU and memory resources based on the requirement that is specified in the metadata for the app.
- **custom**—Lets you enter your own CPU and memory values in the CPU and memory fields.
- **exclusive**—Allocates all resources on the host system to the app.

If you choose an option other than **custom**, Cisco Local Manager enters information in the CPU and Memory fields based on the option that you choose, and these fields become read only.

b) If you choose **custom** from the Profile drop-down list, in the CPU field, enter the number of CPU units that the app requires on the host system when it runs, and in the Memory field, enter the amount of RAM, in MB, that the app requires when it runs.
c) In the Disk field, enter the disk space, in MB, that the app requires on the host system when it runs.

Make sure that you do not enter a CPU, memory, or disk value that exceeds the available CPU, memory, or disk resources that display at the bottom of the App Resource area. If you enter a value that exceeds resource availability, the Docker app profile cannot be created.

If needed, see the app documentation or developer for information regarding resources that an app requires when it runs.

Step 7 If you are creating a new Docker app profile, in the App Network Interfaces area, take these actions to configure the interfaces that the app uses for network access:

a) Click the **Add App Network Interface** button.
b) In the Interface Name field, enter a unique name for the interface. The name can be from 1 to 40 characters in length, and can include alphanumeric characters and underscores characters (_).
c) Click **OK**.
d) From the drop-down list that appears next to the interface name that you entered, choose an option to designate how the app obtains its IP address.

The options that are available in this list depend on the type of host system. Here are examples of some options that can appear:

- iox-nat_docker0—App obtains its IP address from an internal native Docker network address translator
- iox-bridge#—App obtains its IP address from a DHCP pool that is configured in Cisco IOS

The **Port Mapping** link displays to the right of the drop-down list if you choose a nat type network from the drop-down list for an app whose metadata requests TCP or UDP ports to be open on a network interface and if the interface is connected to a NAT network.

The **Interface Setting** link displays to the right of the drop-down list if you choose a network other than a nat type.

e) If the **Port Mapping** link displays, take these actions:

1. Click the **Port Mapping** link.

   The Port Mapping dialog box appears. This dialog box lets you configure TCP port mappings and UDP port mappings for the app. It also includes port mapping tables that show the mapping of internal ports to the corresponding external ports that the app requests, as defined in the metadata for the app.

2. To cause the system to map ports automatically, click the **Auto** radio button, or to enter port mapping information manually, click the **Custom** radio button.

   The system takes the auto action by default.

3. Click the **Add TCP port mapping** button, and take these actions:
   - In the Internal Port(s) field, enter the port from the app container that is to be mapped to the external port.
   - If you clicked the click the **Custom** radio button, in the External Port(s) field, enter the ports on the host system to which you want to map the corresponding internal ports.

   You can repeat this sub-step as needed to configure additional TCP port mappings.
4. Click the **Add UDP port mapping** button, and take these actions:
   - In the Internal Port(s) field, enter the port from the app container that is to be mapped to the external port.
   - If you clicked the click the **Custom** radio button, in the External Port(s) field, enter the ports on the host system to which you want to map the corresponding internal ports.

   You can repeat this sub-step as needed to configure additional UDP port mappings.
5. Click **OK**.

f) If the **Interface Setting** link displays, take these actions:

1. Click the **Interface Setting** link.

   The Interface Setting dialog box appears. This dialog box lets you configure IPv4 and IPv6 interface settings for the app.
2. In the IPv4 Setting area click one of these radio buttons:
   - **Static**—Select this option to use a static IPv4 address. In the IP/Mask field that displays, enter the static address and subnet mask to use. In the DNS field that displays, optionally enter the IP address of the DNS server that the app uses for external communication. In the Gateway IP field that appears, enter the IP address of the gateway that the app uses for external communication. This field is optional if you do not check the **Default Gateway** check box, and is required otherwise. Check the **Default Gateway** check box if you want to make the gateway that you designate in the Gateway IP field the default gateway
   - **Dynamic**—Select this option if you want to assign IPv4 addresses dynamically.
   - **Disable**—Select this option do not want to use an IPv4 address for the network interface.
3. In the IPv6 Setting area click one of these radio buttons:
   - **Static**—Select this option to use a static IPv6 address. In the IP/Mask field that displays, enter the static address and subnet mask to use. In the DNS field that displays, optionally enter the IP address of the DNS server that the app uses for external communication. In the Gateway IP field that appears, enter the IP address of the gateway that the app uses for external communication. This field is optional if you do not check the **Default Gateway** check box, and is required otherwise. Check the **Default Gateway** check box if you want to make the gateway that you designate in the Gateway IP field the default gateway
   - **Dynamic**—Select this option if you want to assign IPv6 addresses dynamically.
   - **Disable**—Select this option do not want to use an IPv6 address for the network interface.
4. In the DHCP Client ID field, enter the DCHP client ID that is sent to the DHCP server.

   If you enter a value, and if the DHCP server has been configured with a static binding that maps a client ID string to a specific IP address, the DHCP server assigns the mapped IP address to the app when the app boots up.

5. In the Vlan ID field, enter the identifier of the VLAN on which this internal network operates.

   This field displays only if the network and the device support VLAN hosting.

6. Click the **OK**.

g) Click the **Add** button to add the network interface.

You can repeat this Step 7 as needed to configure additional network interfaces..

Before you submit the Docker app profile that you are creating, you can click the **edit** link in the App Network Interfaces table to update configuration settings for the corresponding interface, or click the **delete** link in this table to delete the corresponding interface.

Step 8 If you are creating a new Docker app profile, in the App Peripherals area, take these actions to define peripheral devices that are attached to the host system and that the app controls:

a) Click the **Add App Peripheral** button.
b) From the Device Type drop-down list, choose one of these options:

- **serial**—Displays if the host device supports serial ports for the app to use
- **USB-storage**—Displays if USB storage devices are available on the host device for the app to use
- **USB-serial**—Displays if USB serial devices are available on the host device for the app to use

c) If you choose **serial** from the Device Type drop-down list, from the Device Name drop-down list, choose the device that you want. The items that display in this list depend on the devices that are connected to the host system.

The Device Name drop-down list does not display if you choose **USB-storage** or **USB-serial** from the Device Type drop-down list.

d) If you choose **USB-storage** or **USB-serial** from the Device Type drop-down list, click a radio button to select the device that you want. The radio buttons that display depend on the devices that are connected to the host system.
e) In the Label field, type an ID for the app to use to identify the peripheral device.
f) Click **Add**, and then click **OK** in the Add Peripheral dialog box that pops-up.

You can repeat this Step 8 as needed to define additional peripheral devices.

Before you submit the Docker app profile that you are creating, you can click the **edit** link in the App Peripherals table to update configuration settings for the corresponding peripheral device, or click the **delete** link in this table to delete the corresponding device configuration.

Each device in Peripherals table must be in the Present state for you to be able to create the Docker app profile.

Step 9 (Optional) In the App Persistent Data area, take the following actions to upload a data file to the profile.

This file contains data that you can access from the app when the app is running and that is used when the Docker container runs.

a) Click the **Upload File** button.
b) In the Upload Path dialog box that displays, click **Choose File**, navigate to and select the file that you want, and then click **OK**.
c) n the Successfully Uploaded pop-up window, click **OK**.

Step 10 Click the **Submit** button to save the information that you configured for the Docker app profile.

If you do not want to save this information, click the **Cancel** button.

Step 11 To test the app by running it on a local machine, enter the following command on the remote machine.

This syntax displays in the Usage area on the Remote Docker Workflow page.

$ **docker run** *generated_runtime_options user_options image_name*

where:

- *generated_runtime_options*—Docker runtime options shown in the Options field in the Remote Docker Options area
- *user_options*—Additional runtime options that you'd like to add
- *image_name*—Name of the Docker image name that you want

Step 12 When you are satisfied with the operation of the app, take these actions in the Docker Runtime Options area to generate a package.yamls file for the app:

a) Click the **Generate IOx pkg descriptor (package.yaml)** button.

b) In the Generate package.yaml dialog box that displays, take these actions:

1. In the entrypoint field, enter the entry point for the app.
2. In the cmd field, enter the cmd argument for the entry point.
3. Click **OK**. The system generates the package.yaml file and downloads it to your local machine.

OVA File Conversion Workflow

Cisco Local Manager lets you convert apps that are in OVA file format to Cisco IOx packages that can be deployed on a device via Cisco Local Manager.

This process converts an OVA file that is on a USB storage device to a Cisco IOx package, puts the package on the same USB storage device, and optionally deploys the package on the host system.

To convert an OVA file to a Cisco IOx package, perform the following steps.

Before You Begin

- Put the OVA file that you want to convert onto a USB storage device that has been formatted to Ext2, Ext3, Ext4, FAT16, or FAT32.
- Make sure that the USB storage device has enough free space to store the Cisco IOx package that the OVA file is converted to. This package typically is at least have the size of the OVA file.

SUMMARY STEPS

1. Plug a USB storage device that contains the OVA file to convert into port 2 on the device on which you are running Cisco Local Manager.
2. Choose **IOx Tools** from the Cisco IOx Local Manager menu bar.
3. In the **OVA file location in System USB** field, enter the path and base name of the OVA file on the USB device.

4. In the **IOx Package Name** field, enter the base name to be given to the IOx package tar file that you are creating.
5. If the OVA file that you are converting includes a QEMU guest agent package, check the **OVA includes qemu-guest-agent package** check box.
6. If you want Cisco Local Manager to deploy the IOx package automatically after it is created, click the**Deploy IOx Package app on this device** check box.
7. From the OS Type drop-down list, choose the operating system in which you will run the IOx package on the device (**Linux** or **Windows**).
8. Click **Convert**.

DETAILED STEPS

Step 1 Plug a USB storage device that contains the OVA file to convert into port 2 on the device on which you are running Cisco Local Manager.

Step 2 Choose **IOx Tools** from the Cisco IOx Local Manager menu bar.

The IOx Tools page displays.

Step 3 In the **OVA file location in System USB** field, enter the path and base name of the OVA file on the USB device.

Do not include the file extension. Local Manager adds the extension automatically.

Step 4 In the **IOx Package Name** field, enter the base name to be given to the IOx package tar file that you are creating.

Do not include the file extension. Local Manager adds the extension automatically.

Step 5 If the OVA file that you are converting includes a QEMU guest agent package, check the **OVA includes qemu-guest-agent package** check box.

Step 6 If you want Cisco Local Manager to deploy the IOx package automatically after it is created, click the**Deploy IOx Package app on this device** check box.

Step 7 From the OS Type drop-down list, choose the operating system in which you will run the IOx package on the device (**Linux** or **Windows**).

Step 8 Click **Convert**.

The system creates an IOx package from the OVA file, puts it on the USB storage device.

To ensure that the conversion is successful, do not refresh your browser or attempt another Cisco IOx Local Manager operation until the conversion completes.

Internal Network Management Workflows

Internal network management workflows include the operations that you use to add, view information about, edit information for, or delete a Cisco IOx internal network. These networks allow apps on host systems to communicate with other systems.

The workflows for adding and deleting an internal network can be performed only for host systems that allow internal networks to be added.

The following sections describe the internal network management workflows:

Adding an Internal Network

Adding an internal network lets you add a Cisco IOx internal network for an app that requires the network for external connectivity. This operation is available only on host systems that allow internal networks to be added.

If needed, refer to the app documentation or developer for information network configuration that an app requires when it runs.

To add an internal network, follow these steps:

SUMMARY STEPS

1. Choose **System Setting** from the Cisco IOx Local Manager menu bar.
2. Click the **Add Network** button in the System Logs area on the System Setting page.
3. In the Add Network dialog box, take these actions:

DETAILED STEPS

Step 1 Choose **System Setting** from the Cisco IOx Local Manager menu bar.

The System Setting page displays.

Step 2 Click the **Add Network** button in the System Logs area on the System Setting page.

The Add Network dialog box displays.

If you do not see the **Add** button, click **Additional Networks** to expand this area.

Step 3 In the Add Network dialog box, take these actions:

a) In the **Network Description** field, enter a brief description of the internal network.

b) From the **Physical Interface** drop-down list, choose the physical interface that the internal network should use for connectivity.

The options that are available depend on your host system platform. See your host system documentation for information about these options.

c) In the **Vlan ID** field, enter the identifier of the VLAN on which this internal network operates, if applicable. Valid values are 1 through 4000

d) Check the **Nat Enabled** check box if you want to enable NAT networking mode on this network, otherwise skip to Step 3.

If you check **Nat Enabled**, the Nat Subnet fields and Bridge IP radio buttons appear. The Nat Subnet fields include a system-provided address range for the NAT subnet.

e) If you want to change the system-provided address range for the NAT subnet, in the Nat Subnet fields, enter the range that you want.

The system does not allow you to define an address range that includes addresses that are in use by another internal NAT network that is configured on the host system.

f) Click one of these Bridge IP radio buttons:

- **Static**—Click to configure a static IP address for the Cisco IOx bridge. The **IP Address** / **Mask**, **Gateway IP**, **DNS**, and **Domain** fields appear.

- **DHCP**—Click to cause the Cisco IOx bridge to obtain its IP address from an available DCHP server. Skip to Step 3.

g) If you clicked the **Static** radio button for Bridge IP, take these actions:

- In the **IP Address / Mask** field, enter the IP address and subnet mask for the Cisco IOx bridge
- In the **Gateway IP** field, enter the IP address of the gateway server for the Cisco IOx bridge
- In the **DNS** field, enter the IP address of the DNS server for the Cisco IOx bridge
- In the **Domain** field, enter the domain for the static bridge IP address.

h) Check the **Bridge Enabled** check box if you want to enable bridge networking mode on this network.
i) Check the **Mirror Mode** check box if you want to enable an app to monitor network traffic that flows through the physical interface of the host system.
j) Click the **OK** button.

The network is added.

Viewing Information about an Internal Network

You can view information about any internal network that is configured in Cisco IOx Local Manager.

To view information about an internal network, follow these steps:

SUMMARY STEPS

1. Choose **System Setting** from the Cisco IOx Local Manager menu bar.
2. In the Additional Networks area on the System Setting page, click **view** in the **Actions** field for the network about which you want to view information.

DETAILED STEPS

Step 1 Choose **System Setting** from the Cisco IOx Local Manager menu bar.

The System Setting page displays.

Step 2 In the Additional Networks area on the System Setting page, click **view** in the **Actions** field for the network about which you want to view information.

The Additional Information window displays, which provide detailed information about the internal network.

Editing Information for an Internal Network

You can edit the description of any internal network that is configured in Cisco IOx Local Manager. You also can edit the address range for the NAT subnet, if NAT is enabled for the internal network.

To edit information for an internal network, follow these steps:

SUMMARY STEPS

1. Choose **System Setting** from the Cisco IOx Local Manager menu bar.
2. In the Additional Networks area on the System Setting page, click **edit** in the **Actions** field for the network for which you want to edit information.
3. In the Edit Network dialog box, take these actions as needed:
4. In the Edit Network dialog box, click the **OK** button.

DETAILED STEPS

Step 1 Choose **System Setting** from the Cisco IOx Local Manager menu bar.

The System Setting page displays.

Step 2 In the Additional Networks area on the System Setting page, click **edit** in the **Actions** field for the network for which you want to edit information.

The Edit Network dialog box displays.

Step 3 In the Edit Network dialog box, take these actions as needed:

a) In the **Network Description** field, update the description of the internal network.
b) In the **NAT Subnet** field, update the address range for the NAT subnet.

The system does not allow you to define an address range that includes addresses that are in use by another internal network that is configured on the host system.

Step 4 In the Edit Network dialog box, click the **OK** button.

Information for the network is updated.

Deleting an Internal Network

Deleting an internal network removes its configuration from the host system.

The internal network named svcbr_0 is provided by default. This network cannot be deleted because it provides minimum outside connectivity for Cisco IOx hosting.

In addition, an internal network cannot be deleted if an app that uses it is in the ACTIVATED, RUNNING, or STOPPED state.

To delete an internal network, perform the following steps:

SUMMARY STEPS

1. Choose **System Setting** from the Cisco IOx Local Manager menu bar.
2. In the Additional Networks area on the System Setting page, click **delete** in the **Actions** field for the network that you want to delete.
3. In the dialog box that prompts you to confirm the deletion, click **Yes**.

DETAILED STEPS

Step 1 Choose **System Setting** from the Cisco IOx Local Manager menu bar.

The System Setting page displays.

Step 2 In the Additional Networks area on the System Setting page, click **delete** in the **Actions** field for the network that you want to delete.

Step 3 In the dialog box that prompts you to confirm the deletion, click **Yes**.

The delete process executes. This process can take some time.

To ensure that the network deletes successfully, do not refresh your browser or attempt another Cisco IOx Local Manager operation while the network is deleting.

Security and App Validation Workflows

You can configure Cisco IOx Local manager for the following security features:

- SSL connection between Cisco IOx Local Manager and the Cisco application-hosting framework (CAF)—See the Configuring an SSL Connection, on page 38 section
- Signature validation of apps that you install on the host system—See the Configuring App Signature Validation, on page 39 section

Configuring an SSL Connection

By default, Cisco IOx Local Manager uses a self-signed certificate for communication with the CAF. You can configure Cisco IOx Local Manager to use an SSL certificate, signed by a private or commercial CA, that you provided. When you configure an SSL connection, a green lock icon and "Secure" indication appear next to the Cisco IOx Local Manager IP address in the address field in your browser, as shown here:

To configure SSL connections for Cisco IOx Local Manager, follow these steps:

SUMMARY STEPS

1. Choose **System Setting** from the Cisco IOx Local Manager menu bar.
2. Click **Import Certificates** in the **SSL/TLS** area on the System Setting page.
3. In the pop-up window that informs you that CAF will restart after the certificate is uploaded, click **Yes**.
4. In the Import SSL dialog box, take these actions:
5. When you see the pop-up window with the message "Successfully Deployed," click **OK**.
6. When you see the pop-up window with the message "Please reopen LM in new tab once CAF is up" click **OK**.
7. Open Cisco IOx Local Manager in a new browser tab

DETAILED STEPS

Step 1 Choose **System Setting** from the Cisco IOx Local Manager menu bar.

The System Setting page displays.

Step 2 Click **Import Certificates** in the **SSL/TLS** area on the System Setting page.

Step 3 In the pop-up window that informs you that CAF will restart after the certificate is uploaded, click **Yes**.

The Import SSL dialog box displays.

Step 4 In the Import SSL dialog box, take these actions:

a) Click **Choose File** next to Certificate and then navigate to and select the signed SSL certificate that you want to use.
b) Click **Choose File** next to Key and then navigate to and select the encryption key for the signed SSL certificate.
c) Click **OK**.

Step 5 When you see the pop-up window with the message "Successfully Deployed," click **OK**.

Step 6 When you see the pop-up window with the message "Please reopen LM in new tab once CAF is up" click **OK**.

The CAF server, which is the server that hosts Cisco IOx Local Manager, restarts so that the CAF updates with the certificate that you uploaded.

Step 7 Open Cisco IOx Local Manager in a new browser tab

Configuring App Signature Validation

The app signature validation feature causes Cisco IOx Local Manager to validate each app that you add by comparing a certificate on the host system with a certificate in the app. This feature ensures that an app that you add meets the following criteria:

- The app image is consistent. It has not been corrupted or improperly sent to the host system.
- The app image has not been tampered with and contains no malware or code injection.
- The app image comes from a trusted source.

When you enable the app signature validation feature, you can only add apps that are signed. If you try to add an app that is not signed, the message "Application Deployment Failed" displays.

You can enable the app signature validation feature only on host systems that support app signing. The Application Signature Validation configuration options do not appear on host systems that do not support app signing.

Configuring the app signature validation feature involves enabling the feature and uploading to the host system the trust anchor (certificate) that matches the certificate in the apps that you will add.

To configure app signature validation, follow these steps:

SUMMARY STEPS

1. Choose **System Setting** from the Cisco IOx Local Manager menu bar.
2. In the Configuration area under the Application Signature Validation area, click the **Enable Application Signature** button, and then click **OK** in the Successfully Saved dialog box that appears.

3. In the Trust Anchor area under the Application Signature Validation area, take these actions to upload the certificate to the host system:

DETAILED STEPS

Step 1 Choose **System Setting** from the Cisco IOx Local Manager menu bar.

The System Setting page displays.

Step 2 In the Configuration area under the Application Signature Validation area, click the **Enable Application Signature** button, and then click **OK** in the Successfully Saved dialog box that appears.

The button changes to **Disable Application Signature**. If you later want to disable this feature, click the **Disable Application Signature** button.

Step 3 In the Trust Anchor area under the Application Signature Validation area, take these actions to upload the certificate to the host system:

a) Click the **Import Trust Anchor** button. The Import Trust Anchor dialog box appears.
b) In the Import Trust Anchor dialog box, click Choose File, and then navigate to and select the certificate file (a .tar or .tar.gz file) that you want to use.
c) In the Import Trust Anchor dialog box, click **Choose File**.

The certificate uploads to the host system and the Trust Anchor area displays the checksum value and metadata of the certificate. If this certificate is not the one that you want, you can upload another one, which replaces the one that is displayed.

Events and Errors Viewing Workflows

The host system captures information about events and errors that have been written to the Cisco application-hosting framework log files since the Cisco application-hosting framework last started on the host system. You can view this information as needed.

The following sections describe the workflows that relate to log files:

Viewing Events

An event is an activity that occurred on the host system. An event typically relates to a successful Cisco application-hosting framework operation. The system captures information about events and you can view this information to help monitor your system or for troubleshooting.

To view events, follow these steps:

SUMMARY STEPS

1. Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.
2. Click the **Events** button in the Events area on the System Troubleshoot page.

3. (Optional) To display in the Events list only events with text in the corresponding App_id, Event_type, or Message fields that starts with a specific case-sensitive character string, enter the string in the Search field and then click the **Search** button  .
4. (Optional) Use the following controls to navigate the Events list:

DETAILED STEPS

Step 1 Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

The System Troubleshoot page displays.

Step 2 Click the **Events** button in the Events area on the System Troubleshoot page.

If you do not see the **Events** button, click **Events** to expand this area.

The Events list near the bottom of this area displays a list of events that have occurred on the host system and the following information for each event:

- Timestamp—Date and time that the event occurred
- #Record—Unique system-assigned record identifier of the event
- App_id—Identifier of the app to which the event relates
- Event_type—Descriptive term that indicates the type of event
- Message—Text that briefly describes the event

Step 3 (Optional) To display in the Events list only events with text in the corresponding App_id, Event_type, or Message fields that starts with a specific case-sensitive character string, enter the string in the Search field and then click the **Search** button  .

To redisplay all events after performing a search, delete all characters in the Search field and then click the **Search** button  .

Step 4 (Optional) Use the following controls to navigate the Events list:

- Page size drop-down list—Choose the number of events that appear on each page of list. Options are **5**, **10**, **15**, **20**, and **25**.
- First page button  —Click to display the first page of a list.
- Previous page button  —Click to display the previous page of a list.
- Next page button —Click to display the next page of a list.
- Last page button  —Click to display the first last of a list.

- Record field and Go to #Record button—To display at the top of the list an event with a specific record identifier, enter that record identifier in the Record field and then click the **Go to #Record** button. You can type a record identifier in the field or click the Up-Arrow or Down-Arrow buttons in the field to enter a value.

Viewing Errors

An error is an issue that occurred on the host system. The system captures information about errors and you can view this information to help monitor your system or for troubleshooting.

To view errors, follow these steps:

SUMMARY STEPS

1. Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.
2. Click the **Errors** button in the Events area on the System Troubleshoot page.
3. (Optional) To display in the Errors list only errors with text in the Type or Message fields that starts with a specific character string, enter the case-sensitive string in the Search field and then click the **Search** button  .
4. (Optional) Use the following controls to navigate the Errors list:
5. (Optional) To see additional information that relates to an error, click **details** in the Details field for the error.

DETAILED STEPS

Step 1 Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

The System Troubleshoot page displays.

Step 2 Click the **Errors** button in the Events area on the System Troubleshoot page.

If you do not see the **Errors** button, click **Events** to expand this area.

The Errors list near the bottom of this area displays error lines from the CAF log file and the following information for each error:

- Timestamp—Date and time that the error occurred.
- #Record—Unique system-assigned record identifier of the error
- Type—Type of error: **INFO**, **ERROR**, **CRITICAL**, or **WARNING**.
- Message—Text that briefly describes the error.

Step 3 (Optional) To display in the Errors list only errors with text in the Type or Message fields that starts with a specific character string, enter the case-sensitive string in the Search field and then click the **Search** button  .

To redisplay all errors after performing a search, delete all characters in the Search field and then click the **Search** button  .

Step 4 (Optional) Use the following controls to navigate the Errors list:

- Page size drop-down list—Choose the number of errors that appear on each page of list. Options are **5**, **10**, **15**, **20**, and **25**.
- First page button —Click to display the first page of a list.
- Previous page button —Click to display the previous page of a list.
- Next page button —Click to display the next page of a list.
- Last page button —Click to display the first last of a list.
- Record field and Go to #Record button—To display at the top of the list error with a specific record identifier, enter that record identifier in the Record field and then click the **Go to #Record** button. You can type a record identifier in the field or click the Up-Arrow or Down-Arrow buttons in the field to enter a value.

Step 5 (Optional) To see additional information that relates to an error, click **details** in the Details field for the error.

A window displays that shows the error in red type, and the few lines in the CAF log file that come before and after the error.

If needed, you can download the CAF log file that contains the error. You can then locate the error in the log file by searching the file for the timestamp that matches the timestamp corresponds to the error in the Errors list. To download a CAF log file, see the Downloading Log Files, on page 44 section.

Log File Workflows

The host system can capture information about a variety of operations and store this information in log files. You can configure the type and level of information that the system logs, and you can download and provide host log files to Cisco for troubleshooting, if needed.

The following sections describe the workflows that relate to log files:

Configuring Log Files

Configuring log files lets you set the categories for which the host system logs information and the level at which it logs information.

To configure log files, perform the following steps. This procedure sets the same log level for each category that you choose. If you want to set different log levels for different categories, repeat this procedure as needed.

SUMMARY STEPS

1. Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.
2. Click the **Logging Management** button in the Logs area on the System Troubleshoot page.
3. In the Logging Management dialog box, take these actions:

DETAILED STEPS

Step 1 Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

The System Troubleshoot page displays.

Step 2 Click the **Logging Management** button in the Logs area on the System Troubleshoot page.

The Logging Management dialog box displays. This dialog box lists each category for which the system collects logging information, and shows the log level that is configured for each category. It also lets you configure options that relate to host system logs.

If you do not see the **Logging Management** button, click **Logs** to expand this area.

Step 3 In the Logging Management dialog box, take these actions:

a) Check the check box for each category for which you want the system to collect logging information.

You can click the check box in the title row of the table to check the boxes for all categories.

b) Take either of these actions:

- From the **Log Level** drop-down list, choose the level of logging messages that the system collects. Options, in order of least messages to most messages collected, are **critical**, **error**, **warning**, **info**, and **debug**.
- Click the **Load Defaults** button to set the log level for each category to the default value of **info**.

c) Click the **Save** button.

The host system starts collecting logging information according to the options that you configured.

Downloading Log Files

You can download a log file from the host system to the location of your choice. You can then review the file or provide it to Cisco for assistance with troubleshooting, if needed.

To download a log file, follow these steps:

SUMMARY STEPS

1. Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.
2. (Optional) From the **Select Log Type** drop-down list in the Logs area, choose the type of log files that appear in the Log File list.
3. In the Log File list, click **download** in the **View** field for the log file that you want to download.
4. Follow the on-screen prompts to save the file in the location of your choice.

DETAILED STEPS

Step 1 Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

The System Troubleshoot page displays. The Logs area on this page includes the Log File list, which displays the following information for each log file, according to the log type that you select:

- Log name—Name of the log file
- Timestamp—Host system date and time that the log file was last updated
- Log Size—Size of the log file, in bytes
- Error—Number of errors in the log file

Step 2 (Optional) From the **Select Log Type** drop-down list in the Logs area, choose the type of log files that appear in the Log File list.

Options are:

- **All Logs**—All log files that the host device generates
- **CAF logs**—Log files that the Cisco application-hosting framework generates on the host device
- **Common platform logs**— Log files that Linux and services such as Syslog generate on the host device
- **Other logs**—Log files other than CAF logs and common platform logs that are generated on the host device

Step 3 In the Log File list, click **download** in the **View** field for the log file that you want to download.

Step 4 Follow the on-screen prompts to save the file in the location of your choice.

Diagnostic Information Workflow

Diagnostic information can help you evaluate or troubleshoot the operation of the host system or its components.

When reviewing diagnostic information, we recommend that you generate and review summary diagnostics first. If the summary information does not indicate any issues, there is no need to review other diagnostic information. If the summary information indicates that issues exist, you can generate and review specific information that relates to the issues that are indicated.

To generate and view diagnostic information, follow these steps:

Procedure

SUMMARY STEPS

1. Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.
2. From the **Diagnostic Type** drop-down list in the Diagnostic area on the System Troubleshoot page, choose the type of diagnostic information to obtain and display.
3. (Optional) Check the **Detailed Information** check box to display detailed diagnostic information in the Display field.
4. (Optional) If you need assistance with an issue that the display field indicates, copy the text in this field, paste it in a document or message, and provide the document or message to Cisco.

DETAILED STEPS

Step 1 Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

The System Troubleshoot page displays.

Step 2 From the **Diagnostic Type** drop-down list in the Diagnostic area on the System Troubleshoot page, choose the type of diagnostic information to obtain and display.

If you do not see this drop-down list, click **Diagnostics** to expand this area.

Options in the **Diagnostic Type** drop-down list are:

- **summary**—General diagnostic information for the host system
- **memory**—Diagnostic information that relates to memory on the host system
- **disk**—Diagnostic information that relates to the hard disk on the host system
- **process**—Diagnostic information that relates to processes that are running on the host system
- **networking**—Diagnostic information that relates to networking on the host system
- **application**—Diagnostic information that relates to apps that are installed on the host system

The Display field in the Diagnostics area Displays diagnostic information according to the Diagnostic Type option that you chose

Step 3 (Optional) Check the **Detailed Information** check box to display detailed diagnostic information in the Display field.

By default, this field displays high-level information.

Step 4 (Optional) If you need assistance with an issue that the display field indicates, copy the text in this field, paste it in a document or message, and provide the document or message to Cisco.

Tech Support Information Workflows

A snapshot file is a tar file that contains hardware and app file information that relates to the IOx framework. It includes information from log files and specific system health and debugging information that can be useful for troubleshooting complex issues. If you experience issues with Cisco IOx Local Manager, you can generate and then download a snapshot file, which you can provide to Cisco for assistance.

The following sections describe the workflows that relate to snapshot files:

Generating a Snapshot File

Generating a snapshot files collects information in a tar file that is stored on the host system. You can generate a snapshot file whenever needed.

To generate a snapshot file, follow these steps:

SUMMARY STEPS

1. Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.
2. Click the **Generate snapshot file** button in the TechSupport Information area on the System Troubleshoot page.

DETAILED STEPS

Step 1 Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

The System Troubleshoot page displays.

Step 2 Click the **Generate snapshot file** button in the TechSupport Information area on the System Troubleshoot page.

If you do not see **Generate snapshot file** button, click **Logs** to expand this area.

The snapshot file is generated and its name appears in the Tech Support snapshot file name field. The filename is tech_support_*timestamp* , where *timestamp* is the host system date and time that the file was generated.

Downloading a Snapshot File

Downloading a snapshot file downloads it from the host system to the location of your choice.

To download a snapshot file, follow these steps:

SUMMARY STEPS

1. Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.
2. In the TechSupport Information area on the System Info page, click **download** in the **Download** field for the snapshot file that you want to download.
3. Follow the on-screen prompts to save the file in the location of your choice.

DETAILED STEPS

Step 1 Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

The System Troubleshoot page displays.

Step 2 In the TechSupport Information area on the System Info page, click **download** in the **Download** field for the snapshot file that you want to download.

If you do not see the **download** option, click **Logs** to expand this area.

Step 3 Follow the on-screen prompts to save the file in the location of your choice.

Deleting a Snapshot File

Deleting a snapshot file removes it from the host system. You can delete any snapshot file when it is no longer needed.

To delete a snapshot file, follow these steps:

SUMMARY STEPS

1. Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

2. In the TechSupport Information area on the System Troubleshoot page, click the **Delete** icon  in the Delete field for the snapshot file that you want to delete.

DETAILED STEPS

Step 1 Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

The System Troubleshoot page displays.

Step 2 In the TechSupport Information area on the System Troubleshoot page, click the **Delete** icon  in the Delete field for the snapshot file that you want to delete.

If you do not see the **Delete** icon, click **Logs** to expand this area.

Core Dump File Workflows

The host system can create a core dump file if a process crashes. A core dump file contains information that can be useful for troubleshooting.

The following sections describe the workflows that relate to core dump files:

Downloading a Core Dump File

Downloading a core dump file downloads it from the host system to the location of your choice.

To download a core dump file, follow these steps:

SUMMARY STEPS

1. Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.
2. In the TechSupport Information area on the System Troubleshoot page, click **download** in the **Download** field for the core file that you want to download.
3. Follow the on-screen prompts to save the file in the location of your choice.

DETAILED STEPS

Step 1 Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

The System Troubleshoot page displays.

Step 2 In the TechSupport Information area on the System Troubleshoot page, click **download** in the **Download** field for the core file that you want to download.

If you do not see the **download** option, click **Logs** to expand this area.

Step 3 Follow the on-screen prompts to save the file in the location of your choice.

Deleting a Core Dump File

Deleting a core dump file removes it from the host system. You can delete any core dump file when it is no longer needed.

To delete a core dump file, follow these steps:

SUMMARY STEPS

1. Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.
2. In the TechSupport Information area on the System Troubleshoot page, click the **Delete** icon  in the Delete field for the core dump file that you want to delete.

DETAILED STEPS

Step 1 Choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar.

The System Troubleshoot page displays.

Step 2 In the TechSupport Information area on the System Troubleshoot page, click the **Delete** icon  in the Delete field for the core dump file that you want to delete.

If you do not see the **Delete** icon, click **Logs** to expand this area.