



## **Cisco IOx Local Manager Reference Guide, Release 1.10**

**First Published:** 2019-11-13

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883





## CONTENTS

---

### PREFACE

#### **Preface** **vii**

Overview **vii**

Organization **vii**

Obtaining Documentation and Submitting a Service Request **vii**

---

### CHAPTER 1

#### **Overview** **1**

About Cisco IOx Local Manager **1**

Browser Guidelines and Requirements **1**

Hardware Platform Caveat **2**

Starting Cisco IOx Local Manager **2**

Exiting Cisco IOx Local Manager **3**

Viewing Information about Cisco IOx Local Manager **3**

---

### CHAPTER 2

#### **Cisco IOx Local Manager Pages and Options** **5**

Cisco IOx Local Manager Tabs **5**

Applications Page **6**

Remote Docker Workflow Page **8**

Docker Layers Page **14**

System Info Page **16**

System Setting Page **17**

System Troubleshoot Page **19**

App-ID Page **21**

App-ID > Resources Page **22**

App-ID > App-info Page **28**

App-ID > App-Config Page **30**

App-ID > App-DataDir Page **31**

App-ID > Logs Page 32

---

**CHAPTER 3****Cisco IOx Local Manager Workflows 33**

App Lifecycle Workflows 33

Adding/Deploying an App 33

Activating an App 34

Deactivating an App 39

Starting an App 40

Stopping an App 40

Upgrading an App 41

Deleting an App 41

App Management Workflows 42

Updating an App Configuration file 42

Accessing an App via a Console 43

Downloading an App Log File 44

Uploading a File to an App Data Directory 44

Downloading a File from an App Data Directory 45

Deleting a File or Directory from an App Data Directory 46

Cartridge Management Workflows 46

Installing a Cartridge 47

Deleting a Cartridge 47

Viewing Detailed Information about a Cartridge 48

Layer Management Workflow 48

Remote Docker App Workflow 49

Internal Network Management Workflows 54

Adding an Internal Network 54

Viewing Information about an Internal Network 55

Editing Information for an Internal Network 55

Deleting an Internal Network 56

Security and App Validation Workflows 57

Configuring an SSL Connection 57

Configuring App Signature Validation 58

Events and Errors Viewing Workflows 59

Viewing Events 59

Viewing Errors	60
Log File Workflows	61
Configuring Log Files	61
Downloading Log Files	62
Diagnostic Information Workflow	63
Tech Support Information Workflows	64
Generating a Snapshot File	64
Downloading a Snapshot File	64
Deleting a Snapshot File	65
Core Dump File Workflows	65
Downloading a Core Dump File	65
Deleting a Core Dump File	66





## Preface

---

This manual explains how to use Cisco IOx Local Manager to manage, administer, monitor, and troubleshoot Cisco IOx apps on a supported device.

- [Overview, on page vii](#)
- [Organization, on page vii](#)
- [Obtaining Documentation and Submitting a Service Request, on page vii](#)

## Overview

This document explains how to use Cisco IOx Local Manager to manage, administer, monitor, and troubleshoot Cisco IOx apps on a supported device.

## Organization

This manual is organized as follows:

<a href="#">Overview, on page 1</a>	Provides an introduction to Cisco IOx Local Manager and describes some of the general operations that you perform with it
<a href="#">Cisco IOx Local Manager Pages and Options, on page 5</a>	Provides detailed reference information about the pages and options that are available in Cisco IOx Local Manager
<a href="#">Cisco IOx Local Manager Workflows, on page 33</a>	Provides step-by-step procedures for many of the workflows and operations that you can perform with Cisco IOx Local Manager

## Obtaining Documentation and Submitting a Service Request







# CHAPTER 1

## Overview

---

This chapter provides an introduction to Cisco IOx Local Manager and describes general operations that you perform with it.

This chapter includes the following sections:

- [About Cisco IOx Local Manager, on page 1](#)
- [Browser Guidelines and Requirements, on page 1](#)
- [Hardware Platform Caveat, on page 2](#)
- [Starting Cisco IOx Local Manager, on page 2](#)
- [Exiting Cisco IOx Local Manager, on page 3](#)
- [Viewing Information about Cisco IOx Local Manager, on page 3](#)

## About Cisco IOx Local Manager

Cisco IOx Local Manager is a platform-specific application that is installed on a host system as part of the installation of the Cisco IOx framework on that device. It provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot apps on the host system, and to perform a variety of related activities. (To manage apps across different devices, you can use Cisco Fog Director. See the Cisco Fog Director documentation for additional information.)

Cisco IOx is an application enablement platform that provides uniform and consistent hosting capabilities for various types of apps across various Cisco platforms. This platform brings together Cisco IOS, the industry-leading networking operating system, and Linux, the leading open source platform. Linux-based applications can run on Cisco devices in the Cisco IOx framework, so using this platform, you can bring custom applications and interfaces to the network.

With Cisco IOx, developers can create a wide variety of IoT apps, such as data aggregation system and control systems.

## Browser Guidelines and Requirements

Review the following guidelines and requirements before you access Cisco IOx Local Manager through a supported browser:

- Supported browsers are Mozilla Firefox version 50 or later and Google Chrome version 55 or later.

- Make sure that the IOx framework is installed on the Cisco host system that you are accessing through Cisco IOx Local Manager.
- Make sure that networking is configured for Cisco IOS and that you can connect to or ping Cisco IOS on the host system.
- Make sure that the following criteria are met on the host system:
  - The Cisco IOx network IP address and gateway are configured
  - The IOS PAT entry allows traffic on port 8443 to be forwarded to the IP address that is configured for configured Cisco IOx
  - VirtualPortGroup0 interface is configured and reachable
  - You are configured in Cisco IOS as a “user” with privilege 15 and you know the corresponding password
  - DHCP and DNS are configured in Cisco IOS
- For increased system security, Cisco IOx Local Manager times out after 30 minutes of no use. When a timeout occurs, you are logged out of Cisco IOx Local Manager. If you want to continue your session, click the **Continue** button. Otherwise, click the **Log out** button or allow the system to log you out automatically.
- Information that Cisco IOx Local Manager displays does not refresh automatically. To make sure that you are viewing current information on a Cisco IOx Local Manager page, click the **Refresh** button if the page provides this button, or click your browser **Refresh** button.
- When you execute a Cisco IOx Local Manager operation for an app, do not refresh your browser or perform another operation until the current operation completes. Otherwise, the current operation may not execute properly.
- Cisco IOx Local Manager supports access from one browser session at a time on the host on which it is running.

## Hardware Platform Caveat

Cisco C800 series devices do not provide dedicated storage for apps. These devices have a single, soldered-on flash storage that is shared between Cisco IOS and apps. The flash storage is not field replaceable.

Flash has a finite number of P/E cycles. It is expected to last for the duration of the device lifecycle if the flash is used only for Cisco IOS configuration. If apps write to the flash frequently, flash wear out becomes a serious concern.

We recommend that developers and users monitor and throttle the frequency of writes to flash. If an app demands frequent writes or a large amount of data storage, we recommend that data be exported for off-device storage.

## Starting Cisco IOx Local Manager

You can access Cisco IOx Local Manager from any supported computer that has IP connectivity to the host system on which it is installed. When you log in to Cisco IOx Local Manager, your user name and password

are authenticated against your Cisco IOS username and password on the host system on which Cisco IOx Local Manager is installed.

To access Cisco IOx Local Manager, perform the following steps.

#### **Before You Begin.**

Review the information in the [Browser Guidelines and Requirements, on page 1](#).

#### **Procedure**

#### **Procedure**

---

**Step 1** Start a supported browser, and in the Address field, enter the following address:

`https://ip_address:port`

where:

- `ip_address` is the IP address of the host system on which Cisco IOx Local Manager is installed.
- `port` is the port number for access to Cisco IOx Local Manager. The default number is 8443.

The Log In page displays.

On some browsers, you can see information about supported browsers by hovering your mouse over the Down-arrow icon next to “For best results use a supported browser” near the top of the Log In page.

**Step 2** In the **Username** and **PASSWORD** fields, enter the user name and password that you use to log in to Cisco IOS on the host system that you identified in Step 1.

Your password is case-sensitive, so make sure to enter it exactly as it is configured.

**Step 3** Click **Login**.

---

## Exiting Cisco IOx Local Manager

To exit Cisco IOx Local Manager, click **Log Out** from any Cisco IOx Local Manager page.

## Viewing Information about Cisco IOx Local Manager

To view information about Cisco IOx Local Manager, including its version number and the name of this host on which it is running, click **About** from any Cisco IOx Local Manager page.





## CHAPTER 2

# Cisco IOx Local Manager Pages and Options

This chapter provides detailed reference information about the pages and options that are available in Cisco IOx Local Manager.

This chapter includes these sections:

- [Cisco IOx Local Manager Tabs, on page 5](#)
- [Applications Page, on page 6](#)
- [Remote Docker Workflow Page, on page 8](#)
- [Docker Layers Page, on page 14](#)
- [System Info Page, on page 16](#)
- [System Setting Page, on page 17](#)
- [System Troubleshoot Page, on page 19](#)
- [App-ID Page, on page 21](#)

## Cisco IOx Local Manager Tabs

Cisco IOx Local Manager includes the following main tabs in its menu bar. You use these tabs to access the Cisco IOx Local Manager pages:

- **Applications** tab—Displays the Applications page, displays general information about the Cisco IOx apps that have been uploaded to the host system, provides options for managing and administering them, and provides an option for adding a new app.
- **Remote Docker Workflow** tab—Displays the Remote Docker Workflow page. This page provides access from your local PC to Docker apps on the host system so that you can develop, test and troubleshooting these apps. It also lets you create Docker app profiles and perform related activities.
- **Docker Layers** tab—Displays the Docker Layers page. For host systems that are running Cisco IOx 1.x, this page lists the Cisco cartridges that have been installed on the host system, displays general information about these cartridges, and provides options for installing, deleting, and obtaining additional information about them. For host systems that support Docker type apps, this page also displays information about the Docker layers that are used by all applications that are installed on the host system, and provides an option for deleting unused layers.
- **System Info** tab—Displays the System Info page, which provides hardware, software, network, and resource information that relates to the host system.

- **System Troubleshoot** tab—Displays the System Troubleshoot page, which provides options for reviewing events, errors, and diagnostic information on the host system, and managing and obtaining log files and related information for troubleshooting.
- **System Setting** tab—Displays the System Settings page, which provides information about the range of NAT IP addresses that are reserved for app, and provides options for managing SSL connections and app signature validation.
- **App-ID** tab—When you click the **manage** option on the Applications tab for an app, a tab with the ID of that app is added to the menu bar. The *App-ID* tab displays the *App-ID* page, which provides access to pages for viewing information and performing other activities that relate to a specific app.

To remove an *App-ID* tab from the menu bar, hover your mouse over the tab and click its Close button, which appears as an X in the tab.

On Cisco IOx Local Manager pages:

- You can click any field title in a table that displays rows of information to toggle the information in that table in ascending or descending alphabetical order by that field.
- On most pages that display information in multiple areas, you can click an area title to expand or collapse the information in that area.

## Applications Page

The Applications page lists the Cisco IOx apps that have been uploaded to the host system, displays general information about these apps, and provides options for managing and administering them.

It also provides buttons for adding an app and refreshing the page

To access the Applications page, choose **Applications** from the Cisco IOx Local Manager menu bar. The following table describes the fields and options that are available on this page.

**Table 1: Applications Page Fields and Options**

Item	Description
<b>Uploaded App areas</b>	Each app that has been uploaded to the host system displays in an area that includes the following items:
Name of the app	Displays at the top left of an app area
Description of the app	Displays under the name of the app

Item	Description
Status of the app	<p>Status of the app:</p> <ul style="list-style-type: none"> <li>• <b>DEPLOYED</b>—App is uploaded to the host system. System CPU and RAM resources are not committed to the app. An app with this status can be activated, upgraded, or deleted.</li> <li>• <b>ACTIVATED</b>—App is on the host system and ready to run. System CPU and RAM resources have been reserved for the app but are not yet in use. An app with this status can be started or deactivated.</li> <li>• <b>RUNNING</b>—App is operating on the host system. System CPU and RAM resources are in use for the app. An app with this status can be stopped.</li> <li>• <b>STOPPED</b>—App has been running on the host system but its operation has been stopped. System CPU and RAM resources remain reserved for the app. An app with this state can be started or deactivated.</li> </ul>
TYPE	Type of the app ( <b>paas, kvm, lxc, or docker</b> ).
VERSION	Version of the app
PROFILE	Resources profile that is assigned to the app ( <b>default, c1.tiny, c1.small, c1.medium, c1.large, c1.xlarge, custom, or exclusive</b> ).
Memory bar	For an app that is in DEPLOYED state, blue shading indicates the relative amount of total memory (RAM) resources on a host system that the app requests. For an app that is in ACTIVATED, RUNNING, or STOPPED, state, green shading indicates the relative amount of total memory resources on a host system that is allocated to the app. The percentage value at the right of the bar indicates the percentage of total memory on the host system that is requested by or allocated to the app.
CPU bar	For an app that is in DEPLOYED state, blue shading indicates the relative amount of CPU resources on a host system that the app requests. For an app that is in ACTIVATED, RUNNING, or STOPPED, state, green shading indicates the relative amount of CPU resources on a host system that is allocated to the app. The percentage value at the right of the bar indicates the percentage of total CPU resources on the host system that is requested by or allocated to the app.
Start button	Appears for an app that has a status of ACTIVATED or STOPPED. Click to start the app. See the <a href="#">Starting an App, on page 40</a> section.
Stop button	Appears for an app that has a status of RUNNING. Click to stop the app. See the <a href="#">Stopping an App, on page 40</a> section.
Activate button	Appears for an app that has a status of DEPLOYED. Click to activate the app. See the <a href="#">Activating an App, on page 34</a> section.
Deactivate button	Appears for an app that has a status of ACTIVATED or STOPPED. Click to deactivate the app. See the <a href="#">Deactivating an App, on page 39</a> section.
Delete button	Appears for an app that has a status of DEPLOYED. Click to remove the app from the host system. See the <a href="#">Deleting an App, on page 41</a> section.

Item	Description
<b>Manage</b> button	Appears when the app that has any status except DEPLOYED. Click to display the <i>App-ID</i> page for the app. See the <a href="#">App-ID Page, on page 21</a> section.
<b>Upgrade</b> button	Appears for an app that has a status of DEPLOYED. Click to upgrade the app. See the <a href="#">Upgrading an App, on page 41</a> section.
<b>Visualization</b> button	Appears for an app is in running state if its descriptor file (package.yaml) file asks for visualization. Click to open a new tab that can show graphs and tables of data that relates to the app. The information that displays depends on what visualization information the app asks for.
<b>General buttons</b>	The first app that has does not include information for an installed app displays the following buttons:
<b>Add New</b> button	Uploads the app to the host system and puts the app in DEPLOYED state. See the <a href="#">Adding/Deploying an App, on page 33</a> section.
<b>Refresh</b> button	Click to update the page with current information.

## Remote Docker Workflow Page

The Remote Docker Workflow page provides access from your local PC to Docker apps on the host system so that you can develop, test, and troubleshooting these apps. If an app is deployed, you can enable access to the app from this page. If an app is not deployed, you can create a Docker app profile from this page. You also can generate and download a package.yaml file for an app from this page.

Remote Docker access is intended for use by developers. Operators do not need to use this feature.

To access the Remote Docker Workflow page, choose **Remote Docker Workflow** from the Cisco IOx Local Manager menu bar. If the options on this page are hidden, click **Remote Docker Workflow** at the top of the page.

The following table describes the fields and options that are available on this page. If Remote Docker Access is disabled on this page, only the **Remote Docker Access** field and the **Enable Remote Docker Access** buttons are available. The options that display on this page depend on the procedure you are performing. For example, the Docker Runtime options and the Usage options do not display when you are adding a Docker app profile.

Using the options on this page requires that the host support the native Docker engine.

For more detailed information about how to use the options on this page, see the [Remote Docker App Workflow, on page 49](#) section.

**Table 2: Remote Docker Workflow Page Fields and Options**

Item	Description
<b>Step 1: Enable Remote Docker Access area</b>	
Click the area name to expand or hide the information in this area.	



Item	Description
<b>Enable Remote Docker Access / Disable Remote Docker Access</b> toggle button	<p>Click to enable or disable remote Docker access.</p> <p>Enable this feature to access the other options on the Remote Docker Workflow page.</p> <p>When you enable this feature, the host system generates TLS certificates.</p> <p>Enabling remote Docker access opens the Docker web server port on the host system for external access. For the security of that system, we recommend that you disable this feature when you are not using it.</p>
<b>Download</b> button	<p>Click to download the TLS certificates package that the host system created to your local machine.</p> <p>The package is a file named tlscerts.tar. After you download and extract this file and set environment as described in the <a href="#">Remote Docker App Workflow, on page 49</a> section, you can access Docker from your local machine.</p>
<p><b>Step 2: Setup Docker App Profiles area</b></p> <p>Click the area name to expand or hide the information in this area. Click the area name of an options set to expand or hide the information in the set.</p>	
<b>Refresh</b> button	<p>Click to update information in the Step 2: Enable Remote Docker Access area with current information.</p>
<b>App Profile</b> options	<ul style="list-style-type: none"> <li>• <b>Docker App Profiles</b> drop-down list—Choose an existing Docker app profile to use with the app.</li> <li>• <b>Add New</b> button—Click to add a Docker app profile.</li> <li>• <b>Delete</b> button—Click to delete a Docker app profile. This button does not display if you are adding a new Docker app profile.</li> <li>• <b>Profile Name</b> field—If you are adding a Docker app profile, you can enter the name of the profile in this field. Otherwise, this field displays the name of the current Docker app profile.</li> </ul>

Item	Description
<b>App Resource options</b>	<p>The options in this area are display-only unless you are adding a Docker app profile. If you are adding a Docker app profile, options become available for data entry as appropriate for the type of resource profile you choose.</p> <ul style="list-style-type: none"><li>• <b>Profile</b> drop-down list—Choose a profile for the app (<b>default</b>, <b>c1.tiny</b>, <b>c1.small</b>, <b>c1.medium</b>, <b>c1.large</b>, <b>c1.xlarge</b>, <b>custom</b>, or <b>exclusive</b>)</li><li>• <b>CPU</b> field—Number of CPU units that the app requires on the host system when the app runs</li><li>• <b>Memory</b> field—RAM, in MB, that the app requires on the host system when the app runs</li><li>• <b>Disk</b> field—Disk space, in MB, that the app requires on the host system when the app runs</li><li>• <b>Resource display</b>—Shows the number of CPU units, memory (in MB), and disk space (in MB) that is available on the host system</li></ul>

Item	Description
<p><b>App Network Interfaces</b> options</p>	<ul style="list-style-type: none"> <li>• <b>Interface table</b>—Displays the following for each app network interface that has been configured for the app: <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of the interface.</li> <li>• <b>Network Config</b>—Name of the network.</li> <li>• <b>Description</b>—Description of the interface.</li> <li>• <b>Action</b>—The following links can appear in this field: <ul style="list-style-type: none"> <li>• <b>Details</b>—Displays when you are not performing an add Docker app profile procedure. Click to display detailed information about the interface.</li> <li>• <b>Edit</b>—Displays after you have added an app network interface but have not yet clicked the <b>Submit</b> button to save the new Docker app profile. Click to update information that you have configured for the interface.</li> <li>• <b>Delete</b>—Displays after you have added an app network interface but have not yet clicked the <b>Submit</b> button to save the new Docker app profile. Click to delete the interface.</li> </ul> </li> </ul> </li> <li>• <b>Add App Network Interface</b> button—Displays when you are performing an add Docker app profile procedure. Click to access options for adding and configuring an interface for the app.</li> </ul> <p>The following options display after you click the <b>Add App Network Interface</b> button:</p> <ul style="list-style-type: none"> <li>• <b>Interface Name</b> field—Enter a name for the interface.</li> <li>• <b>OK</b> button—Click to save the interface name that you entered.</li> <li>• <b>Network name</b> drop-down list—Networks that are available for the corresponding interface.</li> <li>• <b>Port Mapping</b> or <b>Interface Setting</b> link—Link name depends on the interface type that you choose. Click to access options for mapping ports or configuring interface settings.</li> <li>• <b>Description</b> field—Displays after you click the <b>Add App Network Interface</b> button. Optionally enter a description for the interface.</li> <li>• <b>Add</b> button—Click to save the interface that you are configuring.</li> <li>• <b>Cancel</b> button—Click to discard the interface that you are configuring.</li> </ul>

Item	Description
Add Peripherals options	

Item	Description
	<ul style="list-style-type: none"> <li>• <b>Peripherals table</b>—Displays the following for each peripheral device that the app requires: <ul style="list-style-type: none"> <li>• <b>Device Type</b>—Type of the peripheral device.</li> <li>• <b>Name</b>—Name of the peripheral device.</li> <li>• <b>Label</b>—ID that the app uses to identify the peripheral device.</li> <li>• <b>Status</b>—Displays one of the one of the following strings to indicate the state of the peripheral device. If the state of a peripheral device changes, this field updates only when you refresh the Remote Docker Workflow page. <ul style="list-style-type: none"> <li>• <b>Present</b>—The peripheral device is plugged in to the host device and available for use. Each device in Peripherals table must be in this state for you to be able to create the Docker app profile.</li> <li>• <b>Not Present</b>—The peripheral device is not plugged in to the host device.</li> <li>• <b>Used by name</b>—The peripheral device is being used by the app that <i>name</i> indicates. While a device is in this state, it is unavailable for use by any other app.</li> </ul> </li> </ul> </li> <li>• <b>Action</b>—The following links can appear in this field: <ul style="list-style-type: none"> <li>• <b>details</b>—Displays when you are not performing an add Docker app profile procedure. Click to display detailed information about the peripheral device.</li> <li>• <b>edit</b>—Displays after you have added a peripheral device interface but have not yet clicked the <b>Submit</b> button to save the new Docker app profile. Click to update information that you have configured for the device.</li> <li>• <b>delete</b>—Displays after you have added a peripheral device interface but have not yet clicked the <b>Submit</b> button to save the new Docker app profile. Click to delete the information that you have configured for the device.</li> </ul> </li> <li>• <b>Add Peripheral button</b>—Displays when you are performing an add Docker app profile procedure. Click to access options for adding and configuring a peripheral device.</li> </ul> <p>The following options display after you click the <b>Add Peripheral</b> button:</p> <ul style="list-style-type: none"> <li>• <b>Device Type</b> drop-down list—Choose the type of peripheral device you are adding (<b>serial</b>, <b>USB-storage</b>, or <b>USB-serial</b>). Options that display depend on ports or devices that are available on the host system for the app to use.</li> <li>• <b>Device Name</b> drop-down list—Displays only if you choose <b>serial</b> from</li> </ul>

Item	Description
	<p>the <b>Device Type</b> drop-down list and contains options based on the device.</p> <ul style="list-style-type: none"> <li>• <b>Device radio buttons</b>—Display if you choose <b>USB-storage</b> or <b>USB-serial</b> from the <b>Device Type</b> drop-down list and vary depend on the device.</li> <li>• <b>pid</b> and <b>vid</b> fields—Display if you choose <b>USB-storage</b> or <b>USB-serial</b> from the <b>Device Type</b> drop-down list and show the Product ID and the Vendor ID, respectively, of the device.</li> <li>• <b>fs-uuid</b> field—Displays only if you choose <b>USB-storage</b> from the <b>Device Type</b> drop-down list and shows the universally unique ID of the device.</li> <li>• <b>Label</b> field—Enter a unique ID that the app uses to identify the peripheral device.</li> <li>• <b>Add</b> button—Click to save the peripheral device that you are configuring.</li> <li>• <b>Cancel</b> button—Click to discard the peripheral configuring information that you entered for the device.</li> </ul>
<b>App Persistent Data</b> option	<b>Upload File</b> button—Click 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.
<b>Submit</b> option	Displays when you are adding an app resource profile. Click to save the new profile.
<b>Cancel</b> option	Displays when you are adding an app resource profile. Click to exit the add profile operation without saving configuration updates or the profile.
<b>Docker Runtime Options</b> option	<ul style="list-style-type: none"> <li>• <b>Options</b> field—Display only. Shows runtime options that the system generates for the app based on the Docker app profile configuration information that you entered.</li> <li>• <b>General IOx pkg descriptor (package.yaml)</b> button—Click to generate a package.yaml file for the app based on the Docker app profile information that you entered.</li> </ul>
<b>Usage</b> option	<b>Usage</b> —Display only. Shows the command that you enter on your local machine to run the app Docker container.

## Docker Layers Page

The Docker Layers page displays information about the layers that have been installed on the host system, displays general information about these cartridges, and provides options for installing, deleting, and obtaining additional information about them. This page also displays information about the layers that are used by all applications that are installed on the host system, and provides an option for deleting unused layers.

Cartridges are used by PAAS apps, but not for KVM, LXC, or Docker apps. The packages for these apps include only the app logic (such as Python or Java files), but not the Linux operating system files or the root

file system that the app requires. Cartridges provide the root file system and Python or Java files that an app requires to run. See the [Cartridge Management Workflows, on page 46](#) section for additional information.

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

To access the Docker Layers page, choose **Docker Layers** from the Cisco IOx Local Manager menu bar. The following table describes the fields and options that are available on this page.

**Table 3: Docker Layers Page Fields and Options**

Item	Description
<b>Cartridges Area</b>	
This area is available only for host systems that are running Cisco IOx 1.x. Click the area name to expand or hide the information in this area.	
<b>Total</b> field	Total number of megabytes that cartridges consume on the disk of the host system.
<b>Name</b> field	Name of the cartridge.
<b>Actions</b> field	Provides options that you can click to execute operations for the cartridge: <ul style="list-style-type: none"> <li>• <b>Info</b>—Displays a pop-up window that provides detailed information about the cartridge. See the <a href="#">Viewing Detailed Information about a Cartridge, on page 48</a> section.</li> <li>• <b>Delete</b>—Removes the cartridge from the host system. See the <a href="#">Deleting a Cartridge, on page 47</a> section.</li> </ul>
<b>Description</b> field	Brief description of the cartridge.
<b>Version</b> field	Version of the cartridge.
<b>Size</b> field	Number of megabytes that the cartridge consumes on the disk of the host system.
<b>Install</b> button	Installs the cartridge on the host system. See the <a href="#">Installing a Cartridge, on page 47</a> section.
<b>DockerLayers Area</b>	
This area is available only for host systems that support Docker type apps. Click the area name to expand or hide the information in this area.	
<b>Total Id</b> field	Total number of megabytes that layers consume on the disk of the host system.
<b>Layer Id</b> field	Unique identifier of the layer.
<b>Size</b> field	Number of megabytes that layer consumes on the disk of the host system
<b>Used By</b> field	Name of the app that uses the layer.

Item	Description
<b>Delete Unused Layer</b> button	Deletes layers that are not used by installed apps on the host system. See the <a href="#">Layer Management Workflow, on page 48</a> section.

## System Info Page

The System Info page provides hardware, software, network, and resource information that relates to the host system and to the Cisco IOx infrastructure and framework. The information that this page displays is not specific to any particular app.

To access the System Info page, choose **System Info** from the Cisco IOx Local Manager menu bar. The following table describes the fields and options that are available on this page.

**Table 4: System Info Page Fields and Options**

Item	Description
<b>Refresh Stats</b> button	Click to update the page with current information.
<b>Host Info</b> area	
Information fields	Provides general information about the host system.
<b>Memory</b> area	
Information fields	Provides information about memory use on the host system.
<b>CPU &amp; Processes</b> area	
Information fields	Provides information about CPU and processes that are used on the host system.
<b>Inspect Process</b> button	Click to display a pop-up window that provide additional information about processes that are running on the host system.
<b>Monitoring</b> area	
Corrupted Apps field	If any apps are corrupted on the host system, this field shows the name of each app.
Disk Status field	Displays the status of the hard disk on the host system, if the host system provides this information.  This information can indicate that disk status is not available, that the last file system consistency check identified errors, or that the file system consistency check cannot recover from disk errors.
<b>IP v4 Routing</b> area	
Information fields	Provides IP v4 routing information that relates to the host system.
<b>DNS and NTP Settings</b> area	



Item	Description
Information fields	Provides domain information for any DNS and NTP servers that the host system is using.
<b>Storage area</b>	
SSD Lifetime Information	Displays the expected remaining lifetime of the SSD on the host system, as a percentage of the total expected lifetime, if the host system provides this information.  If Cisco Local Manager cannot display this information, a message in this field explains why the information is not available.  SSD lifetime information is supported only on Cisco 829 Industrial Integrated Services Routers.
Information fields	Provides information about storage devices that host system is using.
<b>Serial Interfaces area</b>	
Information fields	Provides information about serial interface devices that are available on the host system.
<b>Interfaces area</b>	
Information fields	Provides information about general interfaces that host system is using.

## System Setting Page

The System Setting page provides options for managing internal Cisco IOx networks for apps and managing SSL connections and app signature validation.

Internal Cisco IOx networks allow apps on host systems to communicate with other systems. The network named svcbr\_0 is provided by default, and cannot be deleted. Some host systems allow other 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 access the System Setting page, choose **System Setting** from the Cisco IOx Local Manager menu bar. The following table describes the fields and options that are available on this page.

**Table 5: System Setting Page Fields and Options**

Item	Description
<b>Additional Networks area</b>	
<b>Add Network</b> button	Click to add an internal network on host systems that support adding internal networks. See the <a href="#">Adding an Internal Network, on page 54</a> section.
<b>Interface</b> field	Name of the internal Cisco IOx bridge that provides connectivity for this internal network.

Item	Description
<b>Description</b> field	Brief description of the internal network.
<b>Physical Interface</b> field	Physical interface that the internal network uses for connectivity.
<b>Logical Network</b> field	Logical networks that provide bridge and NAT networking modes for the internal network.  Click a logical network name to display a dialog box that provides detailed information about that logical network.
<b>Vlan ID</b> field	Identifier of the VLAN on which this internal network operates, if applicable.
<b>IP Mode</b> field	IP mode of the internal Cisco IOx bridge that provides connectivity for this internal network ( <b>dhcp</b> , <b>static</b> , or <b>no_ip_address</b> ).
<b>IP Address</b> field	IP address and subnet mask of the internal Cisco IOx bridge that provides connectivity for this internal network.
<b>Actions</b> field	Provides these options: <ul style="list-style-type: none"> <li>• <b>edit</b>—Click to edit information that is configured for the network. See the <a href="#">Editing Information for an Internal Network, on page 55</a> section.</li> <li>• <b>delete</b>—Click to remove the network. See the <a href="#">Deleting an Internal Network, on page 56</a> section.</li> <li>• <b>view</b>—Click to display information that is configured for the network. See the <a href="#">Viewing Information about an Internal Network, on page 55</a> section.</li> </ul>
<b>SSL/TLS area</b>	
<b>Import Certificates</b> button	Click to import a externally signed SSL certificate to the host system.  See the <a href="#">Configuring an SSL Connection, on page 57</a> section.
<b>Application Signature Validation area</b>	Appears only if the host system supports app signing.
<b>Enable Application Signature / Disable Application Signature</b> toggle button	Click the <b>Enable Application Signature</b> button to enable App Package Signature Verification on the host system. When this option is enabled, the Cisco application-hosting framework verifies the signature of an app when the app is installed on the host system. If the app signature is not verified, the installation fails.  Click the <b>Disable Application Signature</b> button to disable App Package Signature Verification on the host system. When this option is disabled, the Cisco application-hosting framework does not verify the signature of an app when the app is installed on the host system.  See the <a href="#">Configuring App Signature Validation, on page 58</a> section.
<b>Trust Anchor area</b>	Appears if the host system supports managing trust anchors.

Item	Description
<b>Import Trust Anchor</b> button	Click to import a trust anchor (a .tar or .tar.gz certificate file) to the host system. Use the Import Trust Anchor dialog box that displays to locate and select the trust anchor that you want, and then click <b>OK</b> .  If you enabled application signature verification, apps are validated against this certificate when they are added to the host system. If the validation fails, an app does not install.  See the <a href="#">Configuring App Signature Validation, on page 58</a> section.
<b>Refresh</b> button	If a certificate already exists on the host system, click to display the certificate. If this certificate is the one that you want to use, you do not need to import a certificate. If you import a certificate, it replaces the one that exists on the host system.
List of trust anchors	Displays the checksum value and metadata for each certificate that you imported.

## System Troubleshoot Page

The System Troubleshoot page provides options for reviewing events, errors, and diagnostic information on the host system, and managing and obtaining log files and related information for troubleshooting.



The options on this page are useful for troubleshooting the Cisco IOx framework. For related information, see the following sections.

To access the System Troubleshoot page, choose **System Troubleshoot** from the Cisco IOx Local Manager menu bar. The following table describes the fields and options that are available on this page.

**Table 6: System Troubleshoot Page Fields and Options**

Item	Description
<b>Events area</b>	
<b>Refresh</b> button	Click to update the fields in the Events area with current information.  The information in these fields does not update automatically while the System Troubleshoot page is displayed.
<b>Device Uptime</b> field	The amount of time that has passed since the host system last started, shown as days, hours, minutes, and seconds.
<b>CAF Uptime</b> field	The amount of time that has passed since the Cisco application-hosting framework last started on the host system, shown as days, hours, minutes, and seconds.
<b>System Time</b> field	The current date and time on the host system.

Item	Description
<b>Current CAF Stats</b> fields	The following fields provide information about the number of items that have been written to the Cisco application-hosting framework log files since the Cisco application-hosting framework last started on the host system: <ul style="list-style-type: none"> <li>• <b>Warning</b> field—Number of warnings.</li> <li>• <b>Error</b> field—Number of errors.</li> <li>• <b>Critical</b> field—Number of errors that have a severity of critical.</li> <li>• <b>Events</b> field—Number of events. An event typically relates to a successful Cisco application-hosting framework operation.</li> </ul>
<b>Search</b> field and button	Lets you display specific Events or Errors in the Events list or Errors list. See the <a href="#">Viewing Events, on page 59</a> section or the <a href="#">Viewing Errors, on page 60</a> section.
<b>Events</b> button	Click to display the Events list. See the <a href="#">Viewing Events, on page 59</a> section.
<b>Errors</b> button	Click to display the Errors list. See the <a href="#">Viewing Errors, on page 60</a> section.
Events list	Appears when you click the <b>Events</b> button. Displays information about events that have occurred on the host system. An event typically relates to a successful Cisco application-hosting framework operation.  See the <a href="#">Viewing Events, on page 59</a> section.
Errors list	Appears by default or when you click the <b>Errors</b> button. Displays information about errors that have occurred on the host system and lets you view detailed information about an error.  See the <a href="#">Viewing Errors, on page 60</a> section.
Pagination controls	Let you navigate the Events list or Errors list. See the <a href="#">Viewing Events, on page 59</a> section or the <a href="#">Viewing Errors, on page 60</a> section.
<b>Logs area</b>	
<b>Refresh</b> button	Click to update the fields in the Logs area with current information.  The information in these fields does not update automatically while the System Troubleshoot page is displayed.
<b>Logging Management</b> button	Click to configure the type and level of information that the host system captures in its log files. See the <a href="#">Configuring Log Files, on page 61</a> section.
<b>Select Log Type</b> drop-down list	Choose the type of log files that appear in the Log File list. See the <a href="#">Downloading Log Files, on page 62</a> section.
Log File list	Displays information for each log file, according to the log type option that you choose. See the <a href="#">Downloading Log Files, on page 62</a> section.  You can drag a border between column headings to resize a column.
<b>Diagnostics area</b>	

Item	Description
<b>Diagnostic Type</b> field	Choose the type of diagnostic information to obtain and display. See the <a href="#">Diagnostic Information Workflow, on page 63</a> section.
<b>Detailed Information</b> check box	Check this check box to display detailed diagnostic information in the Display field. See the <a href="#">Diagnostic Information Workflow, on page 63</a> section.
Display field	Displays diagnostic information according to the Diagnostic Type option that you chose. See the <a href="#">Diagnostic Information Workflow, on page 63</a> section.
<b>TechSupport Information area</b>	
<b>Tech Support snapshot file name</b> field	Lists the names of snapshot files that you have generated. A file name has the format <code>tech_support_timestamp</code> , where <i>timestamp</i> is the host system date and time that the file was generated. See the .
<b>File Size</b> field	Size of the snapshot file, in bytes.
<b>Download</b> field	Click <b>download</b> to download the corresponding snapshot file to the location of your choice. See the <a href="#">Downloading a Snapshot File, on page 64</a> section.
<b>Delete</b> field	Click the <b>Delete</b> icon  to delete the corresponding snapshot file from the host system. See the <a href="#">Deleting a Snapshot File, on page 65</a> section.
<b>Generate snapshot file</b> button	Click to generate a snapshot file. See the <a href="#">Generating a Snapshot File, on page 64</a> section.
<b>Refresh</b> button	Click to update the list of snapshot files with current information.
<b>Core file name</b> field	Lists the name of core dump files that the system generated.
<b>File Size</b> field	Size of the core dump file, in bytes.
<b>Download</b> field	Click <b>download</b> to download the corresponding core dump file to the location of your choice. See the <a href="#">Downloading a Core Dump File, on page 65</a> section.
<b>Delete</b> field	Click the <b>Delete</b> icon  to delete the corresponding core dump file from the host system. See the <a href="#">Deleting a Core Dump File, on page 66</a> section.
<b>Refresh</b> button	Click to update the list of core dump files with current information.

## App-ID Page

The *App-ID* page, where *App-ID* is the ID of an app, includes the following tabs. These tabs provide access to pages for viewing information and performing other activities that relate to a specific app.

- **Resources** tab—Displays the Resources page, from which you can assign various resources to an app, activate an app, and deactivate an app. See the [App-ID > Resources Page, on page 22](#) section.

- **App-info** tab—Displays the App-info page, from which you can view system and network information that relates to an app. See the [App-ID > App-info Page, on page 28](#) section.
- **App-Config** tab—Displays the App-Config page, from which you can update configuration information for an app. See the [App-ID > App-Config Page, on page 30](#) section.
- **App-DataDir** tab—Displays the App-DataDir page, from which you can see the contents of the /data directory in an app container, upload files to the /data directory or subdirectory, download files to your local system, and delete files or subdirectories from the /data directory. The files can be configuration files or other files that the app needs when it runs. See the [App-ID > App-DataDir Page, on page 31](#) section.
- **Logs** tab—Displays the Logs page, from which you can view information about and download app log files. See the [App-ID > Logs Page, on page 32](#) section.

To access the *App-ID* page, choose the *App-ID* tab for the app from the Cisco IOx Local Manager menu bar.

If you do not see the tab for an app, choose the **Applications** tab, and then click the **manage** option for the app that you want.

To remove an App-ID tab from the menu bar by, hover your mouse over the tab and click its **Close** button



## App-ID > Resources Page

The *App-ID > Resources* page lets you assign a resource profile (host system CPU and memory resources) to an app, designate the network from which the app obtains its IP address, and activate or deactivate an app. This page also shows CPU and memory resources that are available on the host system.

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

To access the *App-ID > Resources* page, choose an *App-ID* tab from the Cisco IOx Local Manager menu bar, and then choose **Resources**. The following table describes the fields and options that are available on this page.

**Table 7: App-ID > Resources Page Fields and Options**

Item	Description
<b>Resources</b> title	Click to expand or collapse this page.
<b>ActivateApp / DeactivateApp</b> toggle button	Click to activate or deactivate an app. See the <a href="#">Activating an App, on page 34</a> section and the <a href="#">Deactivating an App, on page 39</a> section.

Item	Description
<b>debug mode</b> check box	<p>Available before you click the <b>Activate App</b> button and only for Docker type apps when the host system does not support native Docker, and for PAAS type apps. Check this check box to activate the app in debug mode.</p> <p>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.</p> <p>If you want to enable or disable the debug mode of an app that has been activated, you must first deactivate the app.</p>
<b>Resource Profile area</b>	
<b>Profile</b> drop-down list	<p>Provides options for designating the <i>resource profile</i> for an app. A resource profile designates the amount of host system CPU and memory (RAM) resources that the app requires to run, as follows.</p> <ul style="list-style-type: none"> <li>• <b>c1.tiny, c1.small, c1.medium, c1.large, or c1.xlarge</b>—Assigns the CPU and memory resources that the options display. These values are based on the host system hardware.</li> <li>• <b>default</b>—Assigns CPU and memory resources based on the requirement that is specified in the metadata for the app.</li> <li>• <b>Custom</b>—Lets you enter your own CPU, RAM, and disk space values in the CPU, Memory, and Disk fields.</li> <li>• <b>Exclusive</b>—Allocates all resources on the host system to the apps.</li> </ul> <p>See the <a href="#">Activating an App, on page 34</a> section for more information.</p>
<b>CPU</b> field	<p>Number of CPU units that the app requires on the host system.</p> <p>If you choose <b>Custom</b> from the <b>Profile</b> drop-down list, enter a value in this field. If you choose another option, the system enters a value in this field for you.</p>
<b>Memory</b> field	<p>Amount of RAM, in MB, that the app requires on the host system.</p> <p>If you choose <b>Custom</b> from the <b>Profile</b> drop-down list, enter a value in this field. If you choose another option, the system enters a value in this field for you.</p>
<b>Disk</b> field	<p>Amount of disk space, in MB, that the app requires on the host system.</p> <p>You can enter a value in this field for any option that you choose from the <b>Profile</b> drop-down list. The value that you enter must be greater than the existing value; you cannot decrease the disk space value.</p>

Item	Description
Vcpu field	<p>Appears only for VM-based apps. Enter the number of virtual CPUs that the app requires on the system.</p> <p>If you choose <b>Custom</b> from the <b>Profile</b> drop-down list, enter a value in this field. If you choose another option, the system enters a value in this field for you.</p>
Avail. CPU field	<p>Number of available CPU units on the host system.</p> <p>The system does not allow you to activate an app if the value in the <b>CPU</b> field exceeds this available CPU value.</p>
Avail. Memory field	<p>Amount of available RAM, in MB, on the host system.</p> <p>The system does not allow you to activate an app if the value in the <b>Memory</b> field exceeds this available memory value.</p>
Max VCPU/App field	<p>Appears only for VM-based apps. Number of virtual CPUs that are available on the host system.</p>
<p><b>Advanced Settings area</b></p> <p>Appears only if the app type is Docker and the host system supports native Docker.</p>	
Docker options	<p>Enter one or more Docker run options to be used when you activate the app.</p> <p>This field includes the <code>--rm</code> option by default. For related information, see the following row in this table.</p>
Auto delete container instance	<p>Check this check box to add the <code>--rm</code> run option to the Docker Options field and to use this option when you activate the app.</p> <p>When you stop an app that you activated and started with the <code>--rm</code> option, the app container instance is deleted automatically and the app goes to DEPLOYED state (rather than STOPPED state).</p> <p>This check box is checked by default.</p>
<p><b>Network Configuration area</b></p>	



Item	Description
Network Configuration table	<p>Displays the following for each app network interface that has been configured for the app:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of the interface</li> <li>• <b>Network Config</b>—Name of the network</li> <li>• <b>Description</b>—Description of the interface</li> <li>• <b>Action</b>—The following links can appear in this field: <ul style="list-style-type: none"> <li>• <b>details</b>—Displays after you click the <b>Activate App</b> button for an app. Click to display detailed information about the interface.</li> <li>• <b>edit</b>—Displays before you click the <b>Activate App</b> button for an app. Click to update information that you have configured for the interface.</li> <li>• <b>delete</b>—Displays before you click the <b>Activate App</b> button for an app. Click to delete the interface.</li> </ul> </li> </ul>
<b>Add App Network Interface</b> button	<p>Click to access options for adding and configuring an interface for the app. See the <a href="#">Activating an App, on page 34</a> section.</p> <p>The following options display after you click the <b>Add App Network Interface</b> button:</p> <ul style="list-style-type: none"> <li>• <b>Interface name</b> field—Enter a name for the interface.</li> <li>• <b>OK</b> button—Click to save the interface name that you entered.</li> </ul> <p>The following options display after enter a name in the Interface Name field and click <b>OK</b>:</p> <ul style="list-style-type: none"> <li>• Network name drop-down list—Networks the are available for the corresponding interface..</li> <li>• <b>Port Mapping</b> link or <b>Interface Setting</b> link—Link name depends on the interface type that you choose. Click to access options for mapping ports or configuring interface settings.</li> <li>• <b>Description</b> field—Displays after you click the <b>Add App Network Interface</b> button. Optionally enter a description for the interface.</li> <li>• <b>Add</b> button—Click to save the interface that you are configuring.</li> <li>• <b>Cancel</b> button—Click to discard the interface that you are configuring.</li> </ul>
<p><b>Peripheral Configuration area</b></p> <p>Appears only if the host system can provide this information and if the app metadata requests that a serial port, USB device, or USB port on the host system be assigned for use by the app.</p>	

Item	Description
Peripheral table	<p>Displays the following for each peripheral device that the app requires:</p> <ul style="list-style-type: none"> <li>• <b>Device Type</b>—Type of the peripheral device.</li> <li>• <b>Name</b>—Name of the peripheral device.</li> <li>• <b>Label</b>—ID that the app uses to identify the peripheral device</li> <li>• <b>Status</b>—Displays one of the one of the following strings to indicate the state of the peripheral device. If the state of a peripheral device changes, this field updates only if you close and then reopen the App Resources page. <ul style="list-style-type: none"> <li>• <b>Present</b>—The peripheral device is plugged in to the host device and available for use. Each device in Peripherals table must be in this state for you to be able to activate the app.</li> <li>• <b>Not Present</b>—The peripheral device is not plugged in to the host device.</li> <li>• <b>Used by name</b>—The peripheral device is being used by the app that <i>name</i> indicates. While a device is in this state, it is unavailable for use by any other app.</li> </ul> </li> <li>• <b>Action</b>—The following links can appear in this field: <ul style="list-style-type: none"> <li>• <b>details</b>—Displays after you click the <b>Activate App</b> button for an app. Click to display detailed information about the peripheral device.</li> <li>• <b>edit</b>—Displays before you click the <b>Activate App</b> button for an app. Click to update information that you have configured for the device.</li> <li>• <b>delete</b>—Displays before you click the <b>Activate App</b> button for an app. Click to delete device.</li> </ul> </li> </ul>

Item	Description
<b>Add Peripherals</b> button	<p>Click to access options for adding and configuring a peripheral device.</p> <p>The following options display after you click the <b>Add Peripherals</b> button, depending on what the host system supports:</p> <ul style="list-style-type: none"> <li>• <b>Device Type</b> drop-down list—Choose the type of peripheral device you are adding (<b>serial</b>, <b>USB_storage</b>, <b>USB_serial</b> or <b>USB_port</b>). Options that display depend on ports or devices that are available on the host system for the app to use.</li> <li>• <b>Device Name</b> drop-down list—Displays only if you choose <b>serial</b> from the <b>Device Type</b> drop-down list and contains options based on the device</li> <li>• <b>Device</b> radio buttons—Display if you choose <b>USB_storage</b>, <b>USB_serial</b>, or <b>USB_port</b> from the <b>Device Type</b> drop-down list and vary depend on the device</li> <li>• <b>pid</b> and <b>vid</b> fields—Display if you choose <b>USB_storage</b>, <b>USB_serial</b>, or <b>USB_port</b> from the <b>Device Type</b> drop-down list and show the Product ID and the Vendor ID, respectively, of the device</li> <li>• <b>fs-uuid</b> field—Displays if you choose <b>USB_storage</b> from the <b>Device Type</b> drop-down list and shows the Universally unique ID of the device</li> <li>• <b>label</b> field—Enter a unique ID that the app uses to identify the peripheral device</li> <li>• <b>Add</b> button—Click to save the peripheral device that you are configuring</li> <li>• <b>cancel</b> button—Click to discard the peripheral configuring information that you entered for the device</li> </ul>
<p><b>VNC Options area</b></p> <p>Appears only if the host system supports this functionality.</p>	
<b>Password</b> field	<p>Enter a password for accessing an app via a VNC session.</p> <p>Use this password in the VNC client that you use to access the app.</p>
<b>Port</b> field	<p>Enter a port number to be used for accessing the app via a VNC session.</p> <p>If you do not enter a port number, the system assigns a value.</p> <p>Valid port numbers are 5900 through 65535.</p>

## App-ID > App-info Page

The *App-ID > App-info* page 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. Much of the information on this page comes from the app metadata.

To access the *App-ID > App-info* page, choose an *App-ID* tab from the Cisco IOx Local Manager menu bar, and then choose **App-info**. The following table describes the fields and options that are available on this page. Some of the fields on this page appear only when an app is in a specific state or has a specific configuration.

**Table 8: App-ID > App-info Page Fields and Options**

Item	Description
<b>Application Information area</b>	
<b>ID field</b>	ID of the app
<b>State field</b>	Current state of the app (for example, DEPLOYED).
<b>Name field</b>	Name of the app.
<b>Cartridge Required field</b>	For PAAS applications, the name of each cartridge that the app requires. See the <a href="#">Cartridge Management Workflows, on page 46</a> section.
<b>Version field</b>	Version of the app.
<b>Author field</b>	Author of the app (for example, the company that provided the app).
<b>Author link field</b>	Link to an external page for the author (for example, the website of the author).
<b>Application Type field</b>	Type of the app (PAAS or MV).
<b>Description field</b>	Brief description of the app.
<b>Toolkit service field</b>	Not used.
<b>Debug mode field</b>	If the app was activated in debug mode, this field shows <b>true</b> . Otherwise, this field shows <b>false</b> .
<b>App Access area</b>	
<b>Console Access</b>	For an app that has a status of RUNNING, displays the command that you can use to access the app via a console. See the <a href="#">Accessing an App via a Console, on page 43</a> section.
<b>VNC Access field</b>	For a VM-based app that has a status of RUNNING, displays the password and port number that you entered in the VNC Options area in the <i>App-id &gt; Resources</i> page. You use this password and port number when you access an app via a VNC session.
<b>Requested Resource area</b>	
<b>CPU field</b>	Number of CPU units that the app consumes on the host system.

Item	Description
Memory field	RAM, in MB, that the app consumes on the host system.
Profile field	Resource profile that you assigned to the app. See the <a href="#">Activating an App, on page 34</a> section.
Disk field	Disk space, in MB, that the app consumes on the host system.
Vcpu field	Number of virtual CPUs that are available on the host system for a VM-based app.
<b>Network Information area</b>	
interface-name field	<p>Name of the network interfaces that the app uses for network access. Click an interface name to display a dialog box that shows the following information, as available:</p> <ul style="list-style-type: none"> <li>interface-name—Name of the network interface that the app uses for network access.</li> <li>TCP—If the app metadata requests that TCP ports be open on the host system, displays the TCP port number or numbers that the app requests be open for its use. If <b>info</b> appears in this field, click <b>info</b> to display a dialog box that provides port mapping information for this network interface.</li> <li>UDP—If the app metadata requests that UDP ports be open on the host system, displays the TCP port number or numbers that the app requests be open for its use. If <b>info</b> appears in this field, click <b>info</b> to display a dialog box that provides port mapping information for this network interface.</li> <li>mac_address—MAC address of the network interface that the app uses for network access.</li> <li>network_name—Name of the network on which the app is activated.</li> <li>ipv4—IPv4 address that is assigned to the internal interface of the app.</li> <li>ipv6—IPv6 address that is assigned to the internal interface of the app.</li> <li>mirroring—This field displays with a value of <b>true</b> if port mirroring is enabled for the app. You can enable port mirroring for an app that supports this feature when you activate the app. See the <a href="#">Activating an App, on page 34</a> section.</li> </ul>
<b>Device Information area</b>	
Sl.No field	Row number in this area number for the corresponding information.
usage field	Description of the USB or serial device that the app uses on the host system.
device-id field	Unique ID used by the host system to identify the USB or serial device that the app uses.

Item	Description
<b>type</b> field	Indicates the type of device ( <b>serial</b> or <b>usbport</b> ).
<b>label</b> field	ID used by the app to identify the USB or serial device that the app uses on the host system.
<b>App Health area</b>	
<b>App Health</b> field	Description of the health of the app. “Healthy” means that the app has no errors and is operating normally. “Unhealthy” means that the app has errors. Click a description to see more detailed information, if available.
<b>Reconcile Attempted</b> field	If Cisco IOx determined that the app was corrupted and tried to recover the app, this field shows <b>true</b> . Otherwise, this field shows <b>false</b> .
<b>Reconcile Failure</b> field	If Cisco IOx tried to recover the app but was not able to, this field shows <b>true</b> . Otherwise, this field shows <b>false</b> .  If this field shows <b>true</b> , the app must be recovered manually.
<b>Resource Usage area</b>	
<b>CPU</b> field	Percentage of total CPU units on the host system that the app is currently consuming.
<b>Memory</b> field	Memory, in KB, that the app is currently consuming on the host system.
<b>Disk</b> field	Disk space, in MB, that the app is currently consuming on the host system.
<b>Network</b> field	Data, in bytes, that the app has received from and transferred to the host system.
<b>Refresh</b> button	Click to update the page with current information.

## App-ID > App-Config Page

The *App-ID > App-Config* page from lets you update the configuration file for an app.

An app configuration file is a text file named `package_config.ini`, which is stored in the `/data` directory in the app container for the app. When an app starts, it obtains configuration parameters from this file, if the file exists. The contents and use of this file by its app are defined by the app developer.

To access the *App-ID > App-Config* page, choose an *App-ID* tab from the Cisco IOx Local Manager menu bar, and then choose **App-Config**. The following table describes the fields and options that are available on this page.

**Table 9: App-ID > App-Config Page Fields and Options**

Item	Description
Text field	Lets you enter configuration information for the app. See the <a href="#">Updating an App Configuration file</a> section.

Item	Description
Save button	Click to save the updates that you made in the <b>Text</b> field.

## App-ID > App-DataDir Page

The *App-ID > App-DataDir* page lets you see the contents of the /data directory in an app container, upload files to the /data directory or subdirectory, download files to your local system, and delete files or subdirectories from the /data directory. The files can be configuration files or other files that the app needs when it runs. log files, and other files that are created while app is running.

To access this page, the app must be in the ACTIVATED, RUNNING, or STOPPED state. This page is not available for use when an app is in the DEPLOYED state.

To access the *App-ID > App-DataDir* page, choose an *App-ID* tab from the Cisco IOx Local Manager menu bar, and then choose **App-DataDir**. The following table describes the fields and options that are available on this page.

**Table 10: App-ID > App-DataDir Page Fields and Options**

Item	Description
Current Location	Location in the app container /data directory of a folder that you clicked in the Name field.
Name field	Displays the files and subdirectories in the app container /data directory. In this field, you can take the following actions: <ul style="list-style-type: none"> <li>• If you are viewing a subdirectory, click <b>../</b> to display the contents of the directory that is one level up from the directory that you are viewing.</li> <li>• Click the <b>Home</b> button to the contents of the top level of the /data directory.</li> <li>• Click a subdirectory name to see its contents.</li> <li>• Click a file name to download the file to your local PC. See the <a href="#">Downloading a File from an App Data Directory, on page 45</a> section.</li> </ul>
Type field	Indicates the type of the corresponding item: <ul style="list-style-type: none"> <li>• <b>file</b>—Item is a file in the /data directory or a subdirectory</li> <li>• <b>dir</b>—Item is a subdirectory in the /data directory</li> </ul>
Size field	Size of a file, in bytes. For directories, the size displays as 0.
Actions field	Provides the <b>delete</b> option for deleting a file or directory. See the <a href="#">Deleting a File or Directory from an App Data Directory, on page 46</a> section.
Home button	Click to display in the Name field the contents of the top level of the /data directory.

## App-ID > Logs Page

The *App-ID* > Logs page 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.

To access the *App-ID* > Logs page, choose an *App-ID* tab from the Cisco IOx Local Manager menu bar, and then choose **Logs**. The following table describes the fields and options that are available on this page.

**Table 11: App-ID > Logs Page Fields and Options**

Item	Description
Log name field	Name of the log file.
Timestamp field	Host system date and time that the log file was last updated.
Log Size field	Size of the log file, in bytes.
<b>download</b> button	Lets you download a log file. See the <a href="#">Downloading an App Log File, on page 44</a> section.





## CHAPTER 3

# 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:

- [App Lifecycle Workflows, on page 33](#)
- [App Management Workflows, on page 42](#)
- [Cartridge Management Workflows, on page 46](#)
- [Layer Management Workflow, on page 48](#)
- [Remote Docker App Workflow, on page 49](#)
- [Internal Network Management Workflows, on page 54](#)
- [Security and App Validation Workflows, on page 57](#)
- [Events and Errors Viewing Workflows, on page 59](#)
- [Log File Workflows, on page 61](#)
- [Diagnostic Information Workflow, on page 63](#)
- [Tech Support Information Workflows, on page 64](#)
- [Core Dump File Workflows, on page 65](#)

## 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 tarball (a file in tar format) to the host system. 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 is stored in a local or network location that the system from which you logged in to Cisco IOx Local Manager can access.

### Procedure

---

- 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 Deploy application dialog box, take these actions:
- In the **Application ID** field enter, a unique identifier to be assigned to the app.  
The identifier can contain up to 64 letters, numbers, and underscores (\_), in any combination.
  - Click the **Choose File** button and follow the on-screen prompts to locate and select the app tarball.
  - 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 4** In the Successfully Deployed dialog box, click **OK**.
- 

## 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* for the app. A resource profile designates 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. See the [App-ID > Resources Page, on page 22](#) 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:

## Procedure

---

- 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** 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:
- 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.
  - 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.
- 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.
- 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 6** 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 7

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 ethX, 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 the this area. If the app metadata defines two network interfaces, **eth0** and **eth1** appear in this area.

- Click the **Add App Network Interface** button.
- 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 (\_).
- Click **OK**.
- 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.

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

- 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.

- 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.

- 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 **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.
- If you clicked 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 if you 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 if you 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 8

(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 9

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 10** 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 11** 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.

### Procedure

---

**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** 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 initiates 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:

### Procedure

---

- 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:

### Procedure

---

- 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.

### Procedure

---

- 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:
- Make sure that the **Application Id** field shows the identifier of the app that you want to upgrade.
  - Click the **Browse** button and follow the on-screen prompts to locate and select the upgrade tarball.
  - (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.
- 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:

### Procedure

---

- 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:

### Procedure

---

- 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:
- In the text field, enter configuration information for the app.
  - Click the **Save** button.

---

## Accessing an App via a Console

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

To access an app via a console, 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.

### Procedure

---

- 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:
- 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.
  - 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.
- 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:
- 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.
  - Paste the private key that you copied into this file, and save it locally.
  - Make sure that this file has the Linux permission 700.
- Step 7** Take these actions to connect to the host system from a console:
- 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.

---

## 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:

### Procedure

---

- 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:

### Procedure

---

- 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:

### Procedure

---

**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:

### Procedure

- 
- 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.
- 

## 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, on page 28](#) 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 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.

### Procedure

---

**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 39](#) section.

### Procedure

---

**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:

### Procedure

---

- 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 **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:

### Procedure

---

- 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:

## Procedure

- 
- 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:
- 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.
  - 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 you 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 characters (\_). 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. 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) In 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.ymls 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.

# 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, perform the following steps.

### Procedure

---

- 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:
- In the **Network Description** field, enter a brief description of the internal network.
  - 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.
  - 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
  - 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.
  - 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 DHCP 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:

### Procedure

---

- 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:

### Procedure

---

- 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:
- In the **Network Description** field, update the description of the internal network.
  - 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:

### Procedure

---

- 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 57](#) section
- Signature validation of apps that you install on the host system—See the [Configuring App Signature Validation, on page 58](#) 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:

#### Procedure

- 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 supports 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:

### Procedure

---

**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:

### Procedure

---

- 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:

### Procedure

- 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 [Downloading Log Files, on page 62](#).
- 

## 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.

#### Procedure

---

- 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 quickly check 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:

### Procedure

**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 devices 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

### Procedure

---

**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 for assistance.
- 

## 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:

#### Procedure

---

- 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:

#### Procedure

---

- 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:

### Procedure

---

**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:

### Procedure

---

**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:

### Procedure

---

- 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.
-