Cisco IOx Local Manager Reference Guide

Release 1.4

July 24, 2017

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

CONTENTS

Preface

Overview

This manual 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:

Chapter 1, "Overview"	Provides an introduction to Cisco IOx Local Manager and describes some of the general operations that you perform with it
Chapter 2, "Cisco IOx Local Manager Pages and Options"	Provides detailed reference information about the pages and options that are available in Cisco IOx Local Manager
Chapter 3, "Cisco IOx Local Manager Workflows"	Provides step-by-step procedures for many of the workflows and operations that you can perform with Cisco IOx Local Manager

Obtaining Documentation and Support

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*. This document also lists new and revised Cisco technical documentation. It is available at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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, page 1-1
- Browser Guidelines and Requirements, page 1-1
- Hardware Platform Caveat, page 1-2
- Starting Cisco IOx Local Manager, page 1-2
- Exiting Cisco IOx Local Manager, page 1-3
- Viewing Information about Cisco IOx Local Manager, page 1-3

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:

- 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 configure 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" section on page 1-1.

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

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.
- **Cartridges** tab—Displays the Cartridges page, which 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.
- **System Info** tab—Displays the System Info page, which provides hardware, software, network, and resource information that relates to the host system. This page also provides options for managing and obtaining host system 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 app signature validation
- **Middleware Service** tab—Displays the Middleware Service page, which lists the Cisco Data in Motion services that are available for apps, displays general information about these services, and provides options for starting, stopping, and uploading licenses for them.

- *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 [x].

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. Table 2-1 describes the fields and options that are available on this page.

Start button

Table 2-1   Applications Page Fields and Options

Item	Description
Uploaded App areas	
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
Status of the app	Status of the app:
	• **DEPLOYED**—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.
	• **ACTIVATED**—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.
	• **RUNNING**—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.
	• **STOPPED**—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.
TYPE	Type of the app (**paas**, **kvm**, **lxc**, or **docker**).
VERSION	Version of the app

Table 2-1   Applications Page Fields and Options (continued)

Item	Description
PROFILE	Resources profile that is assigned to the app (**default**, **c1.tiny**, **c1.small**, **c1.medium**, **c1.large**, **c1.xlarge**, or **Custom**)
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 "Starting an App" section on page 3-5.
Stop button	Appears for an app that has a status of RUNNING. Click to stop the app. See the "Stopping an App" section on page 3-6.
Activate button	Appears for an app that has a status of DEPLOYED. Click to activate the app. See the "Activating an App" section on page 3-2.
Deactivate button	Appears for an app that has a status of ACTIVATED or STOPPED. Click to deactivate the app See the "Deactivating an App" section on page 3-5.
Delete button	Appears for an app that has a status of DEPLOYED. Click to remove the app from the host system. See the "Deleting an App" section on page 3-7.
Manage button	Appears when the app that has any status except DEPLOYED. Click to display the *App-ID* page for the app. See the "App-ID Page" section on page 2-9.
Upgrade button	Appears for an app that has a status of DEPLOYED. Click to upgrade the app. See the "Upgrading an App" section on page 3-6.
Visualization 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.

Table 2-1   Applications Page Fields and Options (continued)

Item	Description
General buttons	
The first app that has does not include information for an installed app displays the following buttons:	
Add New button	Uploads the app to the host system and puts the app in DEPLOYED state. See the "Adding/Deploying an App" section on page 3-2.
Refresh button	Click to update the page with current information.

Cartridges Page

The Cartridges 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.

Cartridges are used by PAAS 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" section on page 3-12 for additional information.

Cartridges are not used by KVM, LXC, or Docker apps.

To access the Cartridges page, choose **Cartridges** from the Cisco IOx Local Manager menu bar. Table 2-2 describes the fields and options that are available on this page.

Table 2-2   Cartridges Page Fields and Options

Item	Description
Id field	Unique identifier of the cartridge.
Name field	Name of the cartridge.
Actions field	Provides options that you can click to execute operations for the cartridge: • **Info**—Displays a pop-up window that provides detailed information about the cartridge. See the "Viewing Detailed Information about a Cartridge" section on page 3-13. • **Delete**—Removes the cartridge from the host system. See the "Deleting a Cartridge" section on page 3-13.
Description field	Brief description of the cartridge.
Version field	Version of the cartridge.
Install button	Installs the cartridge on the host system. See the "Installing a Cartridge" section on page 3-12.

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. It also provides options for managing and obtaining host system log files and related information for troubleshooting. The information that this page displays is not specific to any particular app.

The Logs area and TechSupport Information area on the System Info page provide options that are useful for troubleshooting the Cisco IOx framework. For related information, see the "Host System Log File Workflows" section on page 3-19, the "Tech Support Information Workflows" section on page 3-21, and the "Core Dump File Workflows" section on page 3-22. (For information about app-specific log files, see the "Downloading an App Log File" section on page 3-9.)

To access the System Info page, choose **System Info** from the Cisco IOx Local Manager menu bar. Table 2-3 describes the fields and options that are available on this page.

Table 2-3   System Info Page Fields and Options

Item	Description
Host Info area	
Information fields	Provides general information about the host system.
Refresh Stats button	Click to update the page with current information.
CPU & Processes area	
Information fields	Provides information about CPU and processes that are used on the host system.
Inspect button	Click to display a pop-up window that provide additional information about processes that are running on the host system.
Memory area	
Information fields	Provides information about memory use on the host system.
Storage area	
Information fields	Provides information about storage devices that host system is using.
Network Information area	
Information fields	Click a link in the Source_Linux_Bridge column to display a pop-up window that provides additional information about the corresponding network.
Serial Interfaces area	
Information fields	Provides information about serial interface devices that are available on the host system.
Interfaces area	
Information fields	Provides information about general interfaces that host system is using.
IP v4 Routing area	
Information fields	Provides IP v4 routing information that relates to the host system.

Table 2-3   System Info Page Fields and Options (continued)

Item	Description
DNS and NTP Settings area	
Information fields	Provides domain information for any DNS and NTP servers that the host system is using.
Logs area	
Logging Management button	Click to configure the type and level of information that the host system captures in its host system log files. See the "Configuring Host System Log Files" section on page 3-20.
Log name field	Name of a host system log file.
Timestamp field	Host system date and time that the host system log file was last updated.
Log Size field	Size of the host system log file, in bytes.
download link	Click to download the corresponding host system log file. See the "Downloading Host System Log Files" section on page 3-21.
TechSupport Information area	
Tech Support snapshot file name field	Lists the names of snapshot files that you have generated. A file name has the format tech_support_*timestamp*, where *timestamp* is the host system date and time that the file was generated. See the "Generating a Snapshot File" section on page 3-21.
File Size field	Size of the snapshot file, in bytes.
Download field	Click **download** to download the corresponding snapshot file to the location of your choice. See the "Downloading a Snapshot File" section on page 3-22.
Delete field	Click the **Delete** icon ✖ to delete the corresponding snapshot file from the host system. See the "Deleting a Snapshot File" section on page 3-22.
Generate snapshot file button	Click to generate a snapshot file. See the "Generating a Snapshot File" section on page 3-21.
Refresh list button	Click to update the list of snapshot files with current information.
Core file name field	Lists the name of core dump files that the system generated.
File Size field	Size of the core dump file, in bytes.
Download field	Click **download** to download the corresponding core dump file to the location of your choice. See the Downloading a Core Dump File, page 3-23.
Delete field	Click the **Delete** icon ✖ to delete the corresponding core dump file from the host system. See the Deleting a Core Dump File, page 3-23.
Refresh list button	Click to update the list of core dump files with current information.

System Setting Page

The System Setting page provides options for managing internal Cisco IOx networks for apps and managing 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. Table 2-4 describes the fields and options that are available on this page.

Table 2-4   System Setting Page Fields and Options

Item	Description
Additional Networks area	
Add Network button	Click to add an internal network on host systems that support adding internal networks. See the "Adding an Internal Network" section on page 3-16.
Interface field	Name of the internal Cisco IOx bridge that provides connectivity for this internal network.
Description field	Brief description of the internal network.
Physical Interface field	Physical interface that the internal network uses for connectivity.
Logical Network 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.
Vlan ID field	Identifier of the VLAN on which this internal network operates, if applicable.
IP Mode field	IP mode of the internal Cisco IOx bridge that provides connectivity for this internal network (**dhcp**, **static**, or **no_ip_address**).
IP Address field	IP address and subnet mask of the internal Cisco IOx bridge that provides connectivity for this internal network.
Actions field	Provides these options: • **edit**—Click to edit information that is configured for the network. See the "Editing Information for an Internal Network" section on page 3-17. • **delete**—Click to remove the network. See the "Deleting an Internal Network" section on page 3-18. • **view**—Click to display information that is configured for the network. See the "Viewing Information about an Internal Network" section on page 3-17.

Table 2-4   System Setting Page Fields and Options (continued)

Item	Description
Application Signature Validation area	
Appears only if the host system supports app signing.	
Configuration area	Expand this area to display the following options:
	• Application Signature Validation—Check 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.
	• **Save Configuration**—Click to save changes that you make in the Configuration area.
	See the "App Validation Workflow" section on page 3-19.
Trust Anchor area	Appears if the host system supports managing trust anchors. Expand this area to display the following options:
	• **Import Trust Anchor**—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 **OK**.
	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.
	• **Refresh**—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.
	• See the "App Validation Workflow" section on page 3-19.

Middleware Service Page

The Middleware Service page lists the Cisco Data in Motion middleware service that is available for apps, displays general information about this service, and provides options for starting, stopping, and uploading licenses for it. This service runs on the host system.

To access the Middleware Service page, choose **Middleware Service** from the Cisco IOx Local Manager menu bar. Table 2-5 describes the fields and options that are available on this page.

Table 2-5   Middleware Service Page Fields and Options

Item	Description
Name field	Name of the Cisco Data in Motion service.
Status field	Status of the Cisco Data in Motion service: • **Running**—Service is running on the host system • **Stopped**—Service is not running on the host system
Actions field	Provides options that you can click to execute operations for the Cisco Data in Motion service. Options that appear depend on the status of the service as follows: • **start**—Click to start a service that has a status of Stopped. See the "Starting a Cisco Data in Motion Service" section on page 3-15. • **stop**—Click to stop a service that has a status of Running. See the "Stopping a Cisco Data in Motion Service" section on page 3-15. • **license**—Click to upload a Data in Motion license to the host system. See the "Uploading a Cisco Data in Motion License" section on page 3-14.
Description field	Description of the Cisco Data in Motion service.
Version field	Version of the Cisco Data in Motion service.
Require License field	Indicates whether a license is required for the Cisco Data in Motion service to operate on the host system.
Refresh button	Click to update the page 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" section on page 2-10.

• **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" section on page 2-12.

• **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" section on page 2-14.

• **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" section on page 2-14.

• **Logs** tab—Displays the Logs page, from which you can view information about and download app log files. See the "App-ID > Logs Page" section on page 2-15.

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**. Table 2-6 describes the fields and options that are available on this page.

Table 2-6   App-ID > Resources Page Fields and Options

Item	Description
Resources title	Click to expand or collapse this page.
Resource Profile area	
Profile drop-down list	Provides options for designating the *resource profile* 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. • **default**—Assigns CPU and memory resources based on the requirement that is specified in the metadata for the app. • **c1.tiny**, **c1.small**, **c1.medium**, **c1.large**, or **c1.xlarge**—Assigns the CPU and memory resources that the options display. These values are based on the host system hardware. • **Custom**—Lets you enter your own CPU and RAM values in the CPU and Memory field See the "Activating an App" section on page 3-2 for more information.
CPU field	Number of CPU units that the app requires on the host system. If you choose **Custom** from the **Profile** drop-down list, enter a value in this field. If you choose another option, the system enters a value in this field for you.
Memory field	Amount of RAM, in MB, that the app requires on the host system. If you choose **Custom** from the **Profile** drop-down list, enter a value in this field. If you choose another option, the system enters a value in this field for you.

Table 2-6   App-ID > Resources Page Fields and Options (continued)

Item	Description
Disk field	Amount of disk space, in MB, that the app requires on the host system.
	If you choose **Custom** from the **Profile** drop-down list, enter a value in this field. If you choose another option, the system enters a value in this field for you.
Vcpu field	Appears only for VM-based apps. Enter the number of virtual CPUs that the app requires on the system.
	If you choose **Custom** from the **Profile** drop-down list, enter a value in this field. If you choose another option, the system enters a value in this field for you.
Avail. CPU field	Number of available CPU units on the host system.
	The system does not allow you to activate an app if the value in the **CPU** field exceeds this available CPU value.
Avail. Memory field	Amount of available RAM, in MB, on the host system.
	The system does not allow you to activate an app if the value in the **Memory** field exceeds this available memory value.
Max VCPU/App field	Appears only for VM-based apps. Number of virtual CPUs that are available on the host system.
Network Configuration area	
Network Name drop-down list	Designates the network from which the app obtains its IP address or addresses:
	• **iox-bridge0**—App obtains its IP address from a DCHP pool that is configured in Cisco IOS
	• **ioxnat0**—App obtains its IP address from an internal network address translator
Port Mapping link	Click to configure mapping of external ports to internal ports for an app. See Step 8 in the "Activating an App" section on page 3-2.
Serial Access Configuration area	
Appears only if the app metadata requests that a serial port on the host system be assigned for use by the app.	
Port_description radio button	Identifies one or more serial ports on the host system that the app metadata requests for use by the app. *Port_description* is a description of the port usage that comes from the app metadata.
	Click the radio button for each port that you want to assign for use by the app.
Activate / Deactivate toggle button	Click to activate or deactivate an app. See the "Activating an App" section on page 3-2 and the "Deactivating an App" section on page 3-5.

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**. Table 2-7 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 2-7   App-ID > App-info Page Fields and Options

Item	Description
Application Information area	
ID field	ID of the app
State field	Current state of the app (for example, DEPLOYED).
Name field	Name of the app.
Cartridge Required field	For PAAS applications, the name of each cartridge that the app requires. See the "Cartridge Management Workflows" section on page 3-12.
Version field	Version of the app.
Author field	Author of the app (for example, the company that provided the app).
Author link field	Link to an external page for the author (for example, the website of the author).
Application Type field	Type of the app (PAAS or MV).
Description field	Brief description of the app.
Toolkit service field	Not used.
App Access area	
Console Access	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 "Accessing an App via a Console" section on page 3-8.
Requested Resource area	
CPU field	Number of CPU units that the app consumes on the host system.
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 "Activating an App" section on page 3-2.
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.

Table 2-7   App-ID > App-info Page Fields and Options (continued)

Item	Description
Network Information area	
interface-name field	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:
	• interface-name—Name of the network interface that the app uses for network access.
	• 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 **info** appears in this field, click **info** to display a dialog box that provides port mapping information for this network interface.
	• 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 **info** appears in this field, click **info** to display a dialog box that provides port mapping information for this network interface.
	• mac_address—MAC address of the network interface that the app uses for network access.
	• network_name—Name of the network on which the app is activated.
	• ipv4—PV4 address that is assigned to the internal interface of the app.
Device Information area	
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.
type field	Indicates the type of device (**serial** or **usbport**).
label field	ID used by the app to identify the USB or serial device that the app uses on the host system.
Resource Usage area	
CPU field	Percentage of total CPU units on the host system that the app is currently consuming.
Memory field	Memory, in KB, that the app is currently consuming on the host system.
Disk field	Disk space, in MB, that the app is currently consuming on the host system.
Network field	Data, in bytes, that the app has received from and transferred to the host system.
Refresh 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**. Table 2-9 describes the fields and options that are available on this page.

Table 2-8   App-ID > App-Config Page Fields and Options

Item	Description
Text field	Lets you enter configuration information for the app. See the "Updating an App Configuration file" section on page 3-8.
Save button	Click to save the updates that you made in the **Text** 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**. Table 2-9 describes the fields and options that are available on this page.

Table 2-9   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: • If you are viewing a subdirectory, click **../** to display the contents of the directory that is one level up from the directory that you are viewing. • Click the **Home** button to the contents of the top level of the /data directory. • Click a subdirectory name to see its contents. • Click a file name to download the file to your local PC. See the "Downloading a File from an App Data Directory" section on page 3-11.

Table 2-9   App-ID > App-DataDir Page Fields and Options (continued)

Item	Description
Type field	Indicates the type of the corresponding item: • **file**—Item is a file in the /data directory or a subdirectory • **dir**—Item is a subdirectory in the /data directory
Size field	Size of a file, in bytes. For directories, the size displays as 0.
Actions field	Provides the **delete** option for deleting a file or directory. See the "Deleting a File or Directory from an App Data Directory" section on page 3-11.
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**. Table 2-10 describes the fields and options that are available on this page.

Table 2-10   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.
download button	Lets you download a log file. See the "Downloading an App Log File" section on page 3-9.

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

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:

   a.   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.

   b.   Click the **Choose File** button and follow the on-screen prompts to locate and select the app tarball.

   c.   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" section on page 2-10 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   Makes sure that the **Resources** tab is selected on the *App-ID* page.

Step 5   In the Resource Profile area, take either of these actions to choose a resource profile, which designates the host system CPU and memory resources that the app requires when it runs:

- To use a preset or default resource profile, choose the option that you want from the **Profile** drop-down list.

  The system enters information in the **CPU** and **Memory** fields based on the option that you choose. In this case, these fields become read only.

- To enter your own values for a resource profile, choose **Custom** from the **Profile** drop-down list. Then, in the **CPU** field, enter the number of CPU units that the app requires 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 are displayed 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 Network Configuration area, choose an option from each drop-down to designate the logical network from which the app obtains its IP address for the corresponding the port.

The ports in this area appear as eth*X*, where *X* is a number. The number of ports 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 **eith1** appear in this area.

The options that appear in the drop-down list include either of the following terms in their descriptions:

- **bridge**—Indicates that an app obtains its IP address from a DCHP pool that is configured in Cisco IOS

- **nat**—Indicates that an app obtains its IP address from an internal network address translator.

- *#* 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. See the "System Setting Page" section on page 2-7 for related information.

- *description* is the description of the network as defined on the System Setting page.

Step 7 (Optional) If the app metadata requests TCP or UDP ports to be open on a network interface and if the interface is connected to a NAT network, take these actions to configure how TCP and UDP ports on the host system are mapped to internal ports of the app:

    a. Click the **Port Mapping** link that corresponds to the network interface for which you want to configure port mapping. (This link appear only if the app metadata requests TCP or UDP ports to be open on a network interface and if the interface is connected to a NAT network.)

    b. Take either of these actions in the Port Mapping dialog box that appears:

        – To cause the system to map ports automatically, click the **Auto** radio button. The system takes this action by default.

        – To enter port mapping information manually, click the **Custom** radio button. The Port Mapping table provides a description of each internal port and the corresponding internal ports that the app requests, as defined in the metadata for the app. In each the External Port(s) field, enter the ports on the host system to which you want to map the corresponding internal ports.

    c. Click the **OK** button.

Step 8 (Optional) To manually configure eth*X* TCP and UDP port mappings for a NAT network, take the following actions.

If you skip this step, the system configures these port mappings automatically based on a range of ports that is defined in the Cisco IOx configuration.

    a. In the Network Configuration area, click the **Port Mapping** link that corresponds to the logical NAT network for which you want to configure port mappings.

    The Port Mapping dialog box appears. This dialog box lists the TCP and UDP internal ports that are defined by the metadata for the app. It also lists the external ports to which each internal port is mapped. An external port value of **auto** indicates that the system assigns external ports for NAT automatically.

    b. In the Port Mapping dialog box that displays, click the **custom** radio button.

    If you click the **Auto** radio button, the system assigns external ports for NAT automatically, and the other options in this dialog box are not available for editing.

    c. In each External Port(s) field, enter the port or port range to which the corresponding internal port should be mapped. To enter a port range, separate the first and last port in the range with a hyphen (-).

    d. Click the **OK** button.

Step 9 In the Serial Access Configuration area, click the radio button or buttons that correspond to the host system serial port or ports that you want to assign for use by the app.

This area appears only if the app metadata requests that a serial port on the host system be assigned for use by the app.

Step 10 Click the **Activate** button at the bottom 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:

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

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

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

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

d. Click the **OK** button.

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

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

Deleting an App

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

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

To delete an app, follow these steps:

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:

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

b.   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:

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

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

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

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

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

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

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

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

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

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

When you enter the command:

–   Replace **<SSH_PORT>** with the port number for console access to the host system.

–   Replace *app_id***.pem** with the path to the file that you created in Step 6, if the file is not in the current directory.

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

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" section on page 2-12 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, page 3-12
- Deleting a Cartridge, page 3-13
- Viewing Detailed Information about a Cartridge, page 3-13

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 **Cartridges** from the Cisco IOx Local Manager menu bar.

The Cartridges page displays.

Step 2   Click the **Install** button on the Cartridges 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 cartridge, perform the following steps.

Before You Begin

Deactivate all apps that use the cartridge, as described in the "Deactivating an App" section on page 3-5.

Procedure

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

The Cartridges page displays.

Step 2   On the Cartridges 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 **Cartridges** from the Cisco IOx Local Manager menu bar.

The Cartridges page displays.

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

The Cartridge Information window displays.

Middleware Management Workflows

Cisco Data in Motion runs on a Cisco IOx host system and provides a middleware service to Cisco IOx apps. Cisco Data in Motion also can be used as a standalone service. The Cisco Data in Motion middleware service must be started before an app can use it. This service requires you to upload a license before starting it.

The following sections describe the workflows that relate to middleware management:

- Uploading a Cisco Data in Motion License, page 3-14
- Starting a Cisco Data in Motion Service, page 3-15
- Stopping a Cisco Data in Motion Service, page 3-15

Uploading a Cisco Data in Motion License

Uploading a Cisco Data in Motion license puts the license on the host system so that the Cisco Data in Motion service can run.

To upload a Cisco Data in Motion license, perform the following steps.

Before You Begin

Make sure that the Cisco Data in Motion license 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 **Middleware Service** from the Cisco IOx Local Manager menu bar.

The Middleware Service page displays.

Step 2   If the Status field for the service for which you want to upload the license shows **Stopped**, click **start** in the **Actions** field for the service.

Step 3   Click **license** in the **Actions** field for the service for which you want to upload the license.

The Upload License File dialog box displays.

Step 4   In the Upload License File dialog box, take these actions:

  a.   In the **Login name** field, enter the user name that you use to log in to Cisco IOS.

   This name must be configured in Cisco IOS as a "user" with privilege 15.

  b.   In the **Login password** field, enter the user name that you use to log in to Cisco IOS.

  c.   Click the **Browse** button and follow the on-screen prompts to locate and select the file that you want.

  d.   Click the **OK** button.

The upload process begins. This process can take some time.

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.

Starting a Cisco Data in Motion Service

Starting the Cisco Data in Motion service makes the service available to apps that require it.

Before You Begin

You must upload the license before the service becomes fully functional. See the "Uploading a Cisco Data in Motion License" section on page 3-14.

To start the Cisco Data in Motion service, follow these steps:

Procedure

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

The Middleware Service page displays.

Step 2   On the Middleware Service page, click **start** in the **Actions** field for the service that you want to start.

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

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

Stopping a Cisco Data in Motion Service

Stopping the Cisco Data in Motion service makes the service unavailable on the host system.

To stop the Cisco Data in Motion service, follow these steps:

Procedure

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

The Middleware Service page displays.

Step 2   On the Middleware Service page, click **stop** in the **Actions** field for the service that you want to stop.

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

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

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:

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

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

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

    c. In the **Vlan ID** field, enter the identifier of the VLAN on which this internal network operates, if applicable.

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

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

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

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

f. Click one of these Bridge IP radio buttons:

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

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

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. 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:

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

b.   In the **NAT Subnet** field, update the address range for the NAT subnet.

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

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

Information for the network is updated.

Deleting an Internal Network

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

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

In addition, an internal network cannot be deleted if an app that uses is 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.

App Validation Workflow

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, take these actions:

a.   Check the **Enabled** check box next to "Application Signature Verification."

b.   Click the **Save Configuration** 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.

Host System Log File Workflows

The host system can capture information about a variety of operations and store this information in host system 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 host system log files:

Configuring Host System Log Files

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

To configure host system 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 Info** from the Cisco IOx Local Manager menu bar.

The System Info page displays.

Step 2 Click the **Logging Management** button in the Logs area on the System Info 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. Categories include:

   – **API Services**— REST API communication between the Cisco IOx host system and Cisco IOx Local Manager (or Cisco Fog Director)

   – **APP Management**—App lifecycle management

   – **System Information**—System health info for the host system

   – **Other**—Other system components

   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.

Downloading Host System Log Files

You can download a host system 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 host system log file, follow these steps:

Procedure

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

The System Info page displays.

Step 2   In the Logs area on the System Info page, click **download** in the **View** field for the host system log 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.

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 Info** from the Cisco IOx Local Manager menu bar.

The System Info page displays.

Step 2   Click the **Generate snapshot file** button in the TechSupport Information area on the System Info 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 Info** from the Cisco IOx Local Manager menu bar.

The System Info 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 Info** from the Cisco IOx Local Manager menu bar.

The System Info page displays.

Step 2   In the TechSupport Information area on the System Info 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 Snapshot File, page 3-22

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 Info** from the Cisco IOx Local Manager menu bar.

The System Info page displays.

Step 2   In the TechSupport Information area on the System Info 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 Info** from the Cisco IOx Local Manager menu bar.

The System Info page displays.

Step 2   In the TechSupport Information area on the System Info 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.

A

T

U

V