



Cisco IOx Local Manager Reference Guide, Release 1.8

First Published: 2019-03-28

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 vii

Organization vii

Obtaining Documentation and Support 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

Cartridges/Layers Page 8

System Info Page 9

System Setting Page 11

System Troubleshoot Page 13

Middleware Service Page 15

App-ID Page 16

App-ID > Resources Page 17

App-ID > App-info Page 20

App-ID > App-Config Page 23

App-ID > App-DataDir Page 23

App-ID > Logs Page 24

CHAPTER 3	Cisco IOx Local Manager Workflows	27
	App Lifecycle Workflows	27
	Adding/Deploying an App	27
	Activating an App	28
	Deactivating an App	32
	Starting an App	33
	Stopping an App	33
	Upgrading an App	34
	Deleting an App	34
	App Management Workflows	35
	Updating an App Configuration file	35
	Accessing an App via a Console	36
	Downloading an App Log File	37
	Uploading a File to an App Data Directory	37
	Downloading a File from an App Data Directory	38
	Deleting a File or Directory from an App Data Directory	39
	Cartridge Management Workflows	39
	Installing a Cartridge	40
	Deleting a Cartridge	40
	Viewing Detailed Information about a Cartridge	41
	Layer Management Workflow	41
	Middleware Management Workflows	42
	Uploading a Cisco Data in Motion License	42
	Starting a Cisco Data in Motion Service	42
	Stopping a Cisco Data in Motion Service	43
	Internal Network Management Workflows	43
	Adding an Internal Network	44
	Viewing Information about an Internal Network	45
	Editing Information for an Internal Network	45
	Deleting an Internal Network	46
	Security and App Validation Workflows	46
	Configuring an SSL Connection	47
	Configuring App Signature Validation	47

Events and Errors Viewing Workflows	48
Viewing Events	49
Viewing Errors	50
Log File Workflows	51
Configuring Log Files	51
Downloading Log Files	52
Diagnostic Information Workflow	53
Tech Support Information Workflows	54
Generating a Snapshot File	54
Downloading a Snapshot File	54
Deleting a Snapshot File	55
Core Dump File Workflows	55
Downloading a Core Dump File	55
Deleting a Core Dump File	56

Preface

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:

Overview, on page 1	Provides an introduction to Cisco IOx Local Manager and describes some of the general operations that you perform with it
Cisco IOx Local Manager Pages and Options, on page 5	Provides detailed reference information about the pages and options that are available in Cisco IOx Local Manager
Cisco IOx Local Manager Workflows, on page 27	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.



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](#)
- [Cartridges/Layers Page, on page 8](#)
- [System Info Page, on page 9](#)
- [System Setting Page, on page 11](#)
- [System Troubleshoot Page, on page 13](#)
- [Middleware Service Page, on page 15](#)
- [App-ID Page, on page 16](#)

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/Layers** tab—Displays the Cartridges/Layers page. 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. It 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
- **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



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
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

Item	Description
Status of the app	<p>Status of the app:</p> <ul style="list-style-type: none"> • 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
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, on page 33 section.
Stop button	Appears for an app that has a status of RUNNING. Click to stop the app. See the Stopping an App, on page 33 section.
Activate button	Appears for an app that has a status of DEPLOYED. Click to activate the app. See the Activating an App, on page 28 section.
Deactivate button	Appears for an app that has a status of ACTIVATED or STOPPED. Click to deactivate the app. See the Deactivating an App, on page 32 section.
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, on page 34 section.

Item	Description
Manage 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 App-ID Page, on page 16 section.
Upgrade button	Appears for an app that has a status of DEPLOYED. Click to upgrade the app. See the Upgrading an App, on page 34 section.
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.
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, on page 27 section.
Refresh button	Click to update the page with current information.

Cartridges/Layers Page

The Cartridges/layers 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. 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 39](#) section for additional information.

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

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

Table 2: Cartridges/Layers Page Fields and Options

Item	Description
Cartridges Area	Click the area name to expand or hide the information in this area
Total field	Total number of megabytes that cartridges consume on the disk of the host system.
Id field	Unique identifier of the cartridge.
Name field	Name of the cartridge.

Item	Description
Actions field	Provides options that you can click to execute operations for the cartridge: <ul style="list-style-type: none"> • Info—Displays a pop-up window that provides detailed information about the cartridge. See the Viewing Detailed Information about a Cartridge, on page 41 section. • Delete—Removes the cartridge from the host system. See the Deleting a Cartridge, on page 40 section.
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, on page 40 section.
Docker Layers Area	Click the area name to expand or hid the information in this area
Total field	Total number of megabytes that layers consume on the disk of the host system.
Layer Id field	Unique identifier of the layer.
Size field	Number of megabytes that layer consumes on the disk of the host system
Used By field	Name of the app that uses the layer.
Delete Unused Layer button	Deletes layers that are not used by installed apps on the host system. See the Layer Management Workflow, on page 41 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 3: System Info Page Fields and Options

Item	Description
Refresh Stats button	Click to update the page with current information.
Host Info area	
Information fields	Provides general information about the host system.
Memory area	
Information fields	Provides information about memory use on the host system.

Item	Description
CPU & Processes area	
Information fields	Provides information about CPU and processes that are used on the host system.
Inspect Process button	Click to display a pop-up window that provide additional information about processes that are running on the host system.
Monitoring 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.
IP v4 Routing area	
Information fields	Provides IP v4 routing information that relates to the host system.
DNS and NTP Settings area	
Information fields	Provides domain information for any DNS and NTP servers that the host system is using.
Storage area	
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.
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.

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 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, on page 44 section.
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.

Item	Description
Actions field	Provides these options: <ul style="list-style-type: none"> • edit—Click to edit information that is configured for the network. See the Editing Information for an Internal Network, on page 45 section. • delete—Click to remove the network. See the Deleting an Internal Network, on page 46 section. • view—Click to display information that is configured for the network. See the Viewing Information about an Internal Network, on page 45 section.
SSL/TLS area	
Import Certificates button	Click to import a externally signed SSL certificate to the host system. See the Configuring an SSL Connection, on page 47 section.
Application Signature Validation area	Appears only if the host system supports app signing.
Enable Application Signature / Disable Application Signature toggle button	Click the Enable Application Signature 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 Disable Application Signature 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 Configuring App Signature Validation, on page 47 section.
Trust Anchor area	Appears if the host system supports managing trust anchors.
Import Trust Anchor 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 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. See the Configuring App Signature Validation, on page 47 section.
Refresh 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 5: System Troubleshoot Page Fields and Options

Item	Description
Events area	
Refresh 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.
Device Uptime field	The amount of time that has passed since the host system last started, shown as days, hours, minutes, and seconds.
CAF Uptime 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.
System Time field	The current date and time on the host system.
Current CAF Stats 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"> • Warning field—Number of warnings. • Error field—Number of errors. • Critical field—Number of errors that have a severity of critical. • Events field—Number of events. An event typically relates to a successful Cisco application-hosting framework operation.
Search field and button	Lets you display specific Events or Errors in the Events list or Errors list. See the Viewing Events, on page 49 section or the Viewing Errors, on page 50 section.
Events button	Click to display the Events list. See the Viewing Events, on page 49 section.
Errors button	Click to display the Errors list. See the Viewing Errors, on page 50 section.

Item	Description
Events list	Appears when you click the Events 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 Viewing Events, on page 49 section.
Errors list	Appears by default or when you click the Errors button. Displays information about errors that have occurred on the host system and lets you view detailed information about an error. See the Viewing Errors, on page 50 section.
Pagination controls	Let you navigate the Events list or Errors list. See the Viewing Events, on page 49 section or the Viewing Errors, on page 50 section.
Logs area	
Refresh 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.
Logging Management button	Click to configure the type and level of information that the host system captures in its log files. See the Configuring Log Files, on page 51 section.
Select Log Type drop-down list	Choose the type of log files that appear in the Log File list. See the Downloading Log Files, on page 52 section.
Log File list	Displays information for each log file, according to the log type option that you choose. See the Downloading Log Files, on page 52 section. You can drag a border between column headings to resize a column.
Diagnostics area	
Diagnostic Type field	Choose the type of diagnostic information to obtain and display. See the Diagnostic Information Workflow, on page 53 section.
Detailed Information check box	Check this check box to display detailed diagnostic information in the Display field. See the Diagnostic Information Workflow, on page 53 section.
Display field	Displays diagnostic information according to the Diagnostic Type option that you chose. See the Diagnostic Information Workflow, on page 53 section.
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 <code>tech_support_timestamp</code> , where <i>timestamp</i> is the host system date and time that the file was generated. See the .
File Size field	Size of the snapshot file, in bytes.

Item	Description
Download field	Click download to download the corresponding snapshot file to the location of your choice. See the Downloading a Snapshot File, on page 54 section.
Delete field	Click the Delete icon  to delete the corresponding snapshot file from the host system. See the Deleting a Snapshot File, on page 55 section.
Generate snapshot file button	Click to generate a snapshot file. See the Generating a Snapshot File, on page 54 section.
Refresh 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, on page 55 section.
Delete field	Click the Delete icon  to delete the corresponding core dump file from the host system. See the Deleting a Core Dump File, on page 56 section.
Refresh button	Click to update the list of core dump files with current information.

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. The following table describes the fields and options that are available on this page.

Table 6: 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: <ul style="list-style-type: none"> • Running—Service is running on the host system • Stopped—Service is not running on the host system

Item	Description
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: <ul style="list-style-type: none"> • start—Click to start a service that has a status of Stopped. See the Starting a Cisco Data in Motion Service section. • stop—Click to stop a service that has a status of Running. See the Stopping a Cisco Data in Motion Service, on page 43 section. • license—Click to upload a Data in Motion license to the host system. See the Uploading a Cisco Data in Motion License, on page 42 section.
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, on page 17](#) 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 20](#) 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 23](#) 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 23](#) 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 24](#) 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
Resources title	Click to expand or collapse this page.
Resource Profile area	
Profile 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"> • 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, RAM, and disk space values in the CPU, Memory, and Disk fields <p>See the Activating an App, on page 28 section for more information.</p>
CPU field	<p>Number of CPU units that the app requires on the host system.</p> <p>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.</p>
Memory field	<p>Amount of RAM, in MB, that the app requires on the host system.</p> <p>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.</p>
Disk 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 Profile 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 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.</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 CPU 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 Memory 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>
Advanced Settings area	<p>This area 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 --rm 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 --rm 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 --rm 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>
Network Configuration area	

Item	Description
Network Name drop-down list	<p>Provides options for designating the network from which the app obtains its IP address or addresses. The options that are available in this list depend on the type of host system. Here are examples of some options that can appear:</p> <ul style="list-style-type: none"> • iox-bridge0—App obtains its IP address from a DHCP pool that is configured in Cisco IOS. • ioxnat0—App obtains its IP address from an internal network address translator. • iox-nat_docker0—App obtains its IP address from an internal native Docker network address translator. (Applicable only to host systems that support native Docker.) <p>The default network that the Cisco Application Framework returns is selected by default, but you can chose another network.</p>
Port Mapping link Available when the Network Name option is set to a nat type network	<p>Click to configure mapping of external ports to internal ports for an app. See Step 11 in the Activating an App, on page 28 section.</p>
Interface Setting link Available when the Network Name option is set to a bridge type network	<p>Click to configure mapping of external ports to internal ports for an app. See the Activating an App, on page 28 section.</p>
Serial Access Configuration area	<p>Appears only if the app metadata requests that a serial port on the host system be assigned for use by the app.</p>
<i>Port description</i> radio button	<p>Identifies one or more serial ports on the host system that the app metadata requests for use by the app. <i>Port description</i> is a description of the port usage that comes from the app metadata.</p> <p>Click the radio button for each port that you want to assign for use by the app.</p>
Activate / Deactivate toggle button	<p>Click to activate or deactivate an app. See the Activating an App, on page 28 section and the Deactivating an App, on page 32 section.</p>
debug mode check box	<p>Appears only for Docker and 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>
USB Configuration area	<p>Appears only if the host system can provide this information and if the app metadata requests that a USB port on the host system be assigned for use by the app.</p>

Item	Description
<i>Port_description</i> radio button	Identifies one or more USB ports on the host system that the app metadata requests for use by the app. <i>Port_description</i> 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.
VNC Options area	Appears only if the host system supports this functionality.
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.
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.

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
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, on page 39 section.
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.

Item	Description
Toolkit service field	Not used.
Debug mode field	If the app was activated in debug mode, this field shows true . Otherwise, this field shows false .
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, on page 36 section.
VNC Access field	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</i> > Resources page. You use this password and port number when you access an app via a VNC session.
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, on page 28 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.
Network Information area	

Item	Description
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"> • 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—IPv4 address that is assigned to the internal interface of the app. • ipv6—IPv6 address that is assigned to the internal interface of the app.
Device Information area	
SI.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.
App Health area	
App Health 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.
Reconcile Attempted field	If Cisco IOx determined that the app was corrupted and tried to recover the app, this field shows true . Otherwise, this field shows false .

Item	Description
Reconcile Failure field	If Cisco IOx tried to recover the app but was not able to, this field shows true . Otherwise, this field shows false . If this field shows true , the app must be recovered manually.
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**. 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 Updating an App Configuration file section.
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**. 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"> • 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, on page 38 section.
Type field	Indicates the type of the corresponding item: <ul style="list-style-type: none"> • 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, on page 39 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.

Item	Description
download button	Lets you download a log file. See the Downloading an App Log File, on page 37 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 27](#)
- [App Management Workflows, on page 35](#)
- [Cartridge Management Workflows, on page 39](#)
- [Layer Management Workflow, on page 41](#)
- [Middleware Management Workflows, on page 42](#)
- [Internal Network Management Workflows, on page 43](#)
- [Security and App Validation Workflows, on page 46](#)
- [Events and Errors Viewing Workflows, on page 48](#)
- [Log File Workflows, on page 51](#)
- [Diagnostic Information Workflow, on page 53](#)
- [Tech Support Information Workflows, on page 54](#)
- [Core Dump File Workflows, on page 55](#)

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 17](#) 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 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, in the **Memory** field, enter the amount of RAM, in MB, that the app requires when it runs, and in the **Disk** field, enter the amount of disk space, in MB, that the app requires when it runs.
- A value that you enter in the **Disk** field must be greater than the existing value. You cannot decrease the disk space value.
- 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 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** From the drop-down list in the Network Configuration area, choose an option 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.

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 as defined on the System Setting page. See the [System Setting Page, on page 11](#) section for related information.

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-bridge# Description** —App obtains its IP address from a DHCP pool that is configured in Cisco IOS.
- **iox-nat# Description** —App obtains its IP address from an internal network address translator
- **iox-nat_docker# Description**—App obtains its IP address from an internal native Docker network address translator. (Applicable only to host systems that support native Docker.)

Step 8

If you choose a bridge type network from the drop-down list in the Network Configuration area and you want to assign IP addresses to the network interface dynamically, take these actions.

- a) Click the **Interface Setting** link that corresponds to the network interface for which you want to configure how an IP address is assigned.
- b) Make sure that the **Dynamic** radio button in the IPv4 Setting area or in the IPv6 setting area is selected, depending on the type of IP addresses that your network uses.

The **Dynamic** radio buttons are selected by default.

- c) (Optional) In the **DHCP Client ID** field, enter a DHCP client ID that is sent to the DHCP server when the app is activated.

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.

- d) Click the **OK** button.

Step 9

If you choose a bridge type network from the drop-down list in the Network Configuration area and you want to assign a static IP address to the network interface, take these actions.

- a) Click the **Interface Setting** link that corresponds to the network interface for which you want to configure how an IP address is assigned.
- b) Click the **Static** radio button the IPv4 Setting area or the IPv6 setting area, depending on the type of IP addresses that your network uses.

If you want to assign IP addresses dynamically, click the **Dynamic** radio button in the appropriate area instead.

- c) Configure the following options that appear:

Enter the static address and subnet mask to use. You can enter an IPv4 or an IPv6 address. If the `IPv6required` field is set to “true” in the app descriptor file (`package.yaml`) for an app, you must enter an IPv6 address.

- **IP/Mask** field (for IPv4 Setting only)—Enter the static address and subnet mask to use

- **IP/Prefix** field (for IPv6 Setting only)—Enter the static address and prefix to use
- **DNS** field —(Optional) Enter the IP address of the DNS server that the app uses for external communication
- **Gateway IP** field—(Optional if you do not check the **Default Gateway** check box, required otherwise) Enter the IP address of the gateway that the app uses for external communication.
- **Default Gateway** check box— Check this check box to make the gateway that you designate in the **Gateway IP** field the default gateway.

d) Click the **OK** button.

Step 10 If you choose a bridge type network from the drop-down list in the Network Configuration area and you do not want to use an IP address for the network interface, click the Disable radio button in the IPv4 Setting area or the IPv6 setting area.

Step 11 If you choose a nat type network from the drop-down list in the Network Configuration area 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, 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 12 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 13 (Optional) In the USB Configuration area, click the radio button for each port that you want to assign for use by the app.

This area appears only if the host system can provide this information and if the app metadata requests that a USB port on the host system be assigned for use by the app.

This area identifies one or more USB 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.

Step 14 (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 15 If you are activating a Docker or PAAS type app and 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 16 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 take 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 for 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 20](#) 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 **Cartridges/Layers** from the Cisco IOx Local Manager menu bar.

The Cartridges/Layers page displays.

Step 2 Click the **Install** button in the Cartridges area 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, on page 32](#) section.

Procedure

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

The Cartridges/Layers 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/Layers** from the Cisco IOx Local Manager menu bar.
The Cartridges/Layers 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.
-

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 **Cartridges/Layers** from the Cisco IOx Local Manager menu bar.
The Cartridges/Layers page displays.
- Step 2** On the Cartridges page, click **Delete Unused Layers** in the at the bottom of the Layers area.
-

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

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:
- 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.
 - In the **Login password** field, enter the user name that you use to log in to Cisco IOS.
 - Click the **Browse** button and follow the on-screen prompts to locate and select the file that you want.
 - 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, on page 42](#) section.

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 3.

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

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

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

- f) Click one of these Bridge IP radio buttons:

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

- **DHCP**—Click to cause the Cisco IOx bridge to obtain its IP address from an available 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 47](#) section
- Signature validation of apps that you install on the host system—See the [Configuring App Signature Validation, on page 47](#) 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:

 Secure ://192.11

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:
- Click the **Import Trust Anchor** button. The Import Trust Anchor dialog box appears.
 - 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.
 - 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 52](#).

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.
-