Cisco IOx Local Manager Workflows

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

This chapter includes these sections:

App Lifecycle Workflows

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

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

The following sections describe these workflows:

Adding/Deploying an App

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

To add an app, perform the following steps.

Before You Begin

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

Procedure

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

The Applications page displays.

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

The Deploy application dialog box displays.

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

a. In the **Application ID** field enter, a unique identifier to be assigned to the app.

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

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

c. Click the **OK** button.

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

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

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

Activating an App

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

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

As part of the activation process, you designate a *resource profile* for the app. A resource profile designates the amount of CPU and memory resources that the app needs to run. You can choose from several preset resource profiles or enter custom values for a profile. See the "App-ID > Resources Page" section on page 2-8 for more information.

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

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

To activate an app, follow these steps:

Procedure

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

The Applications page displays.

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

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

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

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

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

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

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

- To enter your own values for a resource profile, choose **Custom** from the **Profile** drop-down list. Then, in the **CPU** field, enter the number of CPU units that the app requires when it runs, and in the **Memory** field, enter the amount of RAM, in MB, that the app requires when it runs.

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

Step 6 In the Network Configuration area, choose one of the following values from the **Network Name** drop-down list to designate the network from which the app obtains its IP address:

- **iox-bridge0**—App obtains its IP address from a DCHP pool that is configured in Cisco IOS
- **ioxnat0**—App obtains its IP address from an internal network address translator

Step 7 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 8 Click the **Activate** button at the bottom of the Resources tab.

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

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

Deactivating an App

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

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

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

Procedure

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

The Applications page displays.

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

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

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

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

Starting an App

Starting an app initiates its operation 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 operation 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 appears, take these actions:

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

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

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

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

d. Click the **OK** button.

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

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

Deleting an App

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

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

To delete an app, follow these steps:

Procedure

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

The Applications page displays.

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

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

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

The delete process executes.

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

App Management Workflows

App management workflows include the operations that you use for various app management activities. The following sections describe these workflows:

- Updating an App Configuration file, page 3-6
- Accessing an App via a Console, page 3-7
- Downloading an App Log File, page 3-8

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. The only restrictions are that it must be a text file, and its name and location cannot be changed.

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

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

Procedure

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

The Applications page displays.

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

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

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

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

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

b. Click the **Save** button.

Accessing an App via a Console

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

To access an app via a console, perform the following steps.

Before You Begin

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

Procedure

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

The Applications page displays.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

When you enter the command:

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

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

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

Downloading an App Log File

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

To download an app log file, follow these steps:

Procedure

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

The Applications page displays.

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

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

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

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

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

Cartridge Management Workflows

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

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

If an app requires cartridges but the cartridges are not yet installed, you can still add the app in Cisco IOx Local Manager. However, you must install the required cartridges before you can activate the app. To determine whether an app requires cartridges, you can look at the **Cartridge Required** field on the *App-ID* > App-Info page. See the "App-ID > App-info Page" section on page 2-10 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** from the Cisco IOx Local Manager menu bar.

The Cartridges page displays.

Step 2 Click the **Install** button on the Cartridges page.

The Deploy Cartridge dialog box displays.

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

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

b. Click the **OK** button.

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

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

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

Deleting a Cartridge

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

To delete cartridge, perform the following steps.

Before You Begin

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

Procedure

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

The Cartridges page displays.

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

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

Viewing Detailed Information about a Cartridge

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

Procedure

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

The Cartridges page displays.

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

The Cartridge Information window displays.

Middleware Management Workflows

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

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

- Uploading a Cisco Data in Motion License, page 3-11

Uploading a Cisco Data in Motion License

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

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

Before You Begin

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

Procedure

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

The Middleware Service page displays.

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

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

The Upload License File dialog box displays.

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

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

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

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

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

d. Click the **OK** button.

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

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

Starting a Cisco Data in Motion Service

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

Before You Begin

You must upload the license before the service becomes fully functional. See the “Uploading a Cisco Data in Motion License” section on page 3-11.

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.

Syslog Server Workflows

You can set up Cisco IOx to send logging information to a Syslog server.

Syslog server workflows include the operations that you use to add, edit information for, or delete a Syslog server. The following sections describe these workflows:

- Adding a Syslog Server, page 3-13
- Editing Information for a Syslog Server, page 3-13
- Deleting a Syslog Server, page 3-14

Adding a Syslog Server

Adding a Syslog server causes the host system to send Syslog system messages to that server for logging. Cisco IOx Local Manager supports the deployment of one Syslog server at a time.

To add a Syslog server, perform the following steps.

Before You Begin

Make sure that the Syslog server is operating, accessible by the host system, and properly configured.

Procedure

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

The System Setting page displays.

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

The Add dialog box displays.

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

If the **Add** button is dimmed, a Syslog server has been added already. In this case, you can either edit the existing Syslog server to provide information for the new server, or delete the existing Syslog server and then add a new one. See the "Editing Information for a Syslog Server" section on page 3-13 or the "Deleting a Syslog Server" section on page 3-14.

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

a. In the **Hostname or IP address** field, enter the host name or the IP address of the Syslog server that you want to use.

b. From the **Protocol** drop-down list, choose the protocol that the host system uses to communicate with the Syslog server.

   Options are **UDP** and **TCP**.

c. In the Port Number field, enter the port number on which the host communicates with the Syslog server.

d. From the **Log Level** drop-down list, choose the level of logging information that the host system sends to the Syslog server.

   Options, in order of least messages to most messages sent, are **emergency**, **alert**, **critical**, **error**, **warning**, **notice**, **info**, and **debug**.

e. Click the **Save** button.

The Syslog server is added and starts collecting logging information.

Editing Information for a Syslog Server

You can edit any information that you entered for a Syslog server when you added that server in Cisco IOx Local Manager.

To edit a Syslog server, 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 **edit** in the **Actions** field in the System Logs area on the System Setting page.

The Add dialog box displays.

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

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

a. In the **Hostname or IP address** field, enter the host name or the IP address of the Syslog server that you want to use.

b. From the **Protocol** drop-down list, choose the protocol that the host system uses to communicate with the Syslog server.

   Options are **UDP** and **TCP**.

c. In the Port Number field, enter the port number on which the host communicates with the Syslog server.

d. From the **Log Level** drop-down list, choose the level of logging information that the host system sends to the Syslog server.

   Options, in order of least messages to most messages sent, are **emergency**, **alert**, **critical**, **error**, **warning**, **notice**, **info**, and **debug**.

e. Click the **Save** button.

Information for the Syslog server is updated.

Deleting a Syslog Server

Deleting a Syslog server removes the access and log level information that you configured when you added or edited that server and causes the host system to stop sending Syslog system messages to that server

To delete a Syslog server, 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 **delete** in the **Actions** field in the System Logs area on the System Setting page.

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

Host System Log File Workflows

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

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

- Configuring Host System Log Files, page 3-15
- Downloading Host System Log Files, page 3-16

Configuring Host System Log Files

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

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

Procedure

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

The System Info page displays.

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

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

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

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

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

- **API Services**— REST API communication between the Cisco IOx host system and Cisco IOx Local Manager (or Cisco Fog-Director)
- **APP Management**—App lifecycle management
- **System Information**—System health info for the host system
- **Other**—Other system components

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

b. Take either of these actions:

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

c. Click the **Save** button.

The host system starts collecting logging information.

Downloading Host System Log Files

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

To download a host system log file, follow these steps:

Procedure

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

The System Info page displays.

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

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

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

Tech Support Information Workflows

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

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

- Generating a Snapshot File, page 3-16
- Downloading a Snapshot File, page 3-17
- Deleting a Snapshot File, page 3-17

Generating a Snapshot File

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

To generate a snapshot file, follow these steps:

Procedure

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

The System Info page displays.

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

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

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

Downloading a Snapshot File

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

To download a snapshot file, follow these steps:

Procedure

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

The System Info page displays.

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

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

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

Deleting a Snapshot File

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

To delete a snapshot file, follow these steps:

Procedure

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

The System Info page displays.

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

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

Core Dump File Workflows

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

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

- Downloading a Snapshot File, page 3-17
- Deleting a Snapshot File, page 3-17

Downloading a Core Dump File

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

To download a core dump file, follow these steps:

Procedure

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

The System Info page displays.

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

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

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

Deleting a Core Dump File

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

To delete a core dump file, follow these steps:

Procedure

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

The System Info page displays.

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

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