Customize Fleet Upgrade

This document covers the following topics:

Build Cisco GISOs

Follow these steps to build a Golden ISO (also known as GISO, golden image or master image) from a IOS XR or XE bootable base ISO, one or more system patches (SMUs), and other optional packages and configuration files.

GISOs are a popular, efficient way to establish a standard baseline system configuration for each category of device you deploy. They help ensure that all new deployments and upgrades include the same base capabilities and mix of fixes. They reduce human error, ensure consistency, and lead to optimized performance and reduced image size.

To build a GISO, you must select one installable Cisco ISO software image to serve as the base. You can then add SMUs and other packages as you choose. The ISO can be any bootable ISO (including mini and K9 ISOs). Both the ISO and the other packages must already be loaded into the local repository.

Before you begin

Image availability: Ensure all required images are present in the local image repository before starting the GISO build to prevent interruptions.

EXR optional packages: For EXR platform Golden ISOs, include optional packages specific to the product series and software version. Collect the necessary RPM files and bundle them into a TAR archive for upload, following the required naming convention.

TAR naming convention: The tar filename format typically follows the pattern: platform-image_type-release.tar. For example, ASR9K-x64-iosxr-25.2.2.tar, NCS540-iosxr-25.2.2.tar, NCS540l-aarch64-iosxr-optional-rpms-25.4.1.tar.

Resource usage during Golden ISO creation: Golden ISO creation may briefly use additional system resources. As a result, some uploads or downloads could be temporarily limited. Normal operations will resume automatically once the process completes.

Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Image repository**.

Crosswork displays the list of images downloaded to the local repository.

Step 2 Click **Build GISO**. Crosswork displays the **Generate GISO** window, with a **Process Overview** listing the steps in the GISO generation workflow.

Step 3 Click **Next** to display the **Select base ISO** window. Crosswork lists all the ISO images in the local repository. Click the selection checkbox next to the base ISO you want to use.

Step 4 Click **Next** to display the **SMU selection** window, listing all the SMU packages in the local repository. Click the selection checkbox next to the **Name** of each SMU or other package you want to include in the GISO.

Note that you will not be able to select any packages that are not already in your local repository. You will need to download these packages first to include them in a GISO.

Step 5 Click **Next** to display the **Refined SMU List** window.

The **Included List** in the upper part of the window lists all the SMUs and other packages you selected that are in the local repository and will be included in the GISO.

Fleet Upgrade will also include any packages required by your selections that are also in your local repository. Fleet Upgrade adds these packages to the **Included List** automatically, and indicates this with the **Added** flag, along with **Details** explaining why they were added.

The refinement process performs the following:

- Adds any dependent SMUs required by your selections that were not initially selected.
- Removes SMUs that are superseded by other selected SMUs.
- Lists whether required images are present in the local image repository. If a required image or component is missing from the local repository, Golden ISO (GISO) creation will be blocked until you upload or download the missing image.

Obsolete or otherwise inappropriate packages that you selected will be shown in the **Excluded List**. Fleet Upgrade excludes these automatically, indicating this with the **Removed** flag, and explaining the reason for their exclusion in the **Details** column. These packages will not be included in the GISO.

Step 6 Click **Next** to display the **Summary** window.

Review your selections. If you are satisfied, click **Generate GISO** to begin building your GISO. Golden ISO creation typically takes 20–180 minutes, depending on the number and size of SMUs and optional packages selected.

After submission, you will be redirected to the **CWMS Systems Task** page, where you can monitor the status of your GISO build task in real time. Your recently initiated GISO build should appear among the **Running** tasks in the task list. Alternatively, select **Workflow Automation** > **CWMS Systems Tasks** to check on the progress of the GISO build. The task details page shows the current status, additional details, and any errors encountered during the build process.

Upon successful completion, the newly created Golden ISO will be added to the local images list and will be available for Fleet Upgrade.

Use parallel upgrades with acceptable failures

Fleet Upgrade provides the **Parallel upgrades** and **Acceptable failures** fields to help you both speed up and control long upgrade runs with many devices.

As explained in Run a Fleet Upgrade job, whenever you create a Fleet Upgrade job, you can select up to 50 devices to be upgraded during that job. Depending on the number and size of each device upgrade, this can result in jobs lasting hours. This would be worse if you had to upgrade each device one at a time, in series. It would be still worse if you couldn't cancel the run if you started experiencing upgrade failures.

To help with these issues, you can use the **Parallel upgrades** field to specify how many upgrades you want performed at the same time, in parallel. If you enter a **Parallel upgrades** value equal to the total number of devices to be upgraded (up to the maximum of `50`), all the upgrades will take place at the same time. If you leave **Parallel upgrades** set to the default value of `1`, Fleet Upgrade performs each of them one at a time.

Most users specify a lower **Parallel upgrades** value, such as `5` or `10`. Doing so helps conserve processing resources and ensures that only a few of the network devices in a 50-device job set will be offline at one time.

With a lower **Parallel upgrades** value, Fleet Upgrade performs the upgrades in batches. For a 50-device upgrade group with a **Parallel upgrades** value of `5`, this means 10 batches of five upgrades each. In this case, Fleet Upgrade performs all five of the upgrades in batch #1 at the same time, in parallel, and doesn't initiate any of the upgrades in batch #2 until all of the upgrades in batch #1 are finished.

How can you cancel a job that's failing too often? Fleet Upgrade will automatically cancel the remaining upgrades in a job depending on the number of **Acceptable failures** you set. The value you specify in this field acts as a failure "budget" that, when exceeded, triggers automatic cancellation of all of the remaining upgrades in the run. If you want to avoid automatic cancellation entirely, specify an **Acceptable failures** value equal to the total number of devices to be upgraded (up to the maximum of `50`). Set it to the default value of `1` if you want the system to cancel remaining upgrades after the very first failure.

Bear in mind that a batch will run to completion once started. The error budget defined in **Acceptable failures** will block additional batches from starting if it has been exceeded. Sometimes, this means the total number of actual failures will exceed the failure budget, and it will take longer for cancellation to kick in than you might expect.

For example: Let's assume that our job set is 50 devices. Our **Parallel upgrades** setting is 5 and our **Acceptable failures** setting is 5. That means we have 10 batches of 5 devices for Fleet Upgrade to perform. Let's further suppose that, during execution of batch #1, we encounter 4 failures. The 5-failures budget is not yet exceeded, so Fleet Upgrade will begin to execute all the upgrades in batch #2 in parallel. We then encounter 4 more failures in batch #2. The 5-failure budget is now exceeded, so Fleet Upgrade will automatically cancel execution of batch #3 and the remaining 7 other batches. However, we've actually encountered 8 failures, not 5. Similarly, we might encounter only 1 failure each in batches #1, #2, #3, and #4, then encounter 1 more failure in batch #5. We now have a total of 5 failures, but this does not *exceed* the failure budget, only *equals* it. So Fleet Upgrade then goes on to the next batch. Then, in batch #6, every upgrade fails, exceeding the failure budget and triggering cancellation of the run. In this case, we've actually encountered 10 failures, twice the number we specified. Also, cancellation wasn't triggered until batch #7 and device #35, some 70 percent of the way through the entire run.

Download software upgrades using a proxy server

You can download Cisco SMUs to your local image repository using a proxy server, but you must configure the proxy first, using the following steps.

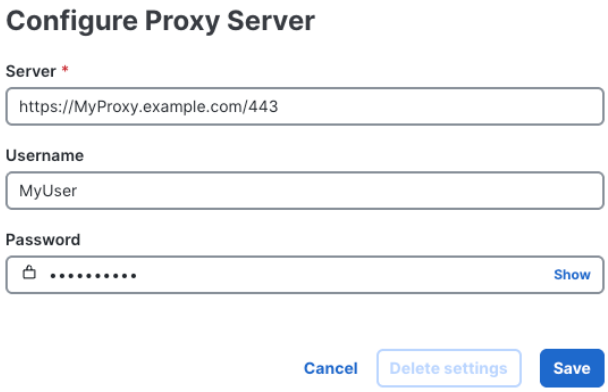
Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Image repository**.

Step 2 With the contents of the **Image repository** displayed, click the **Cisco.com** tab to display the Cisco.com image catalog.

Step 3 Click **Configure proxy server** tab to display a popup like the one shown below.

Figure 1: Configure proxy server



Step 4 Complete the proxy server fields as needed. When you are finished, click **Save**.

You must enter the **Server** URL or IP address and port number. You must also enter a valid **Username** and **Password** if the proxy server requires a login.

Troubleshoot Fleet Upgrade failures

The following table summarizes common Fleet Upgrade issues and their remedies.

Table 1: Common Fleet Upgrade Issues and Remedies

Issue	Description	Remedy
Upgrade fails; unable to transition state	Upgrade fails due to inability to transition state during image distribution	Increase timeouts to at least 3600 seconds for Action, Event, State, and Workflow. System Activity timeout should be at least 10 seconds.

Issue	Description	Remedy
FPD causes activation failure	The failure message will include a recommendation that you "Please reconfigure your settings and create a new job." Upgrade fails during "Activate" stage, with the following message: "Performing FPDs upgrade on the device. FPDs upgrade success except for the following FPDs: PO-PrimMCU, PO-PrimMCU". This occurs on VXR devices.	Add the following to the `Activate` Action configuration input: `"fpd": "false","isISSUUpgrade": "false" }`
Fleet Upgrade GUI drop downs are not working	The Vendor, Product series and other GUI drop down selection lists don't appear when clicked on.	The issue occurs when NSO packages are not updated. Please install the correct packages when installing Fleet Upgrade.
Software Image Policy has no Vendor or Device drop down	The Vendor and Product series drop down selection lists don't appear when clicked on.	Check that at least one software image has been downloaded to the local image repository. Fleet Upgrade is designed to display Vendor and Product series selections only when software images are available in the local repository.
Upgrade fails due to failure to find FTP services	Upgrade fails with a message indicating that a `Distribute` action failed due to the FTP server not being found.	From the main menu, select **Administration** > **File servers** and ensure that **Enable FTP** and **Enable SFTP server upload** are both checked. Also ensure that your organization's FTP and SFTP servers are active on TCP Ports 30621 and 30622, respectively.

Use the default MOPs

Fleet Upgrade comes installed with default (or "pre-built") MOPs. These MOPs are provided by Cisco, cannot be modified directly (although they can be copied and the copies modified), and are intended for use in performing upgrades for specific supported vendors and device families:

- **Default Juniper Upgrade**: For upgrading Juniper MX960 series devices running JunOS
- **Default XE Upgrade**: For upgrading Cisco Systems ASR 900 series devices running Cisco IOS-XE
- **Default XR Upgrade**: For upgrading Cisco Systems 8000 series devices running Cisco IOS-XR

In most cases, you will want to select one of these default MOPs when a conformance report indicates that it is time to upgrade a suppported device in the series. They are usually your safest choice when upgrading devices from these manufacturers. Each of the default MOPs is customized for the supported vendor and

product series, and the customizations are extensive. Each MOP varies significantly in the number of action types it makes available, the selected actions it performs during an upgrade, and the stages it goes through as it performs these actions. For example:

- **Default Juniper Upgrade**: Offers 17 action types. The majority of these Actions are Juniper-specific. It performs 19 Actions during an upgrade: nine during the Pre check stage, three during the Distribute stage, one during the Activate stage, and six during the Post stage.
- **Default XE Upgrade**: Offers 15 Action Types. It performs 17 Actions during an upgrade: seven during the Pre check stage, two during the Distribute stage, one during the Activate stage, and seven during the Post stage.
- **Default XR Upgrade**: Offers 22 Action Types. It performs 25 Actions during an upgrade: 11 during the Pre check stage, three during the Distribute stage, three during the Activate stage, one during its unique Commit stage, and seven during the Post stage.

However, running a default MOP may not always be your best choice for an efficient, targeted upgrade. You may find it useful to view each default MOP as a comprehensive library of all the Fleet Upgrade Actions relevant to a particular vendor and product series, arranged as a useful workflow.

You don't have to stick with the default MOP. You can copy a default MOP, and then manipulate and customize the copy to suit your needs. For example, you may decide that a MOP step that checks existing disk space is not necessary when you are upgrading software on a set of devices that are all factory-fresh. Similarly, you may that find running sanity checks against devices that you know are up and running is a waste of time and don't belong in the MOP you want to run. For more information about creating custom MOPs, see the *Cisco Crosswork Network Controller Solutions 7.2 MOP User Guide*