Cisco Crosswork Workflow Manager Solutions 2.1 Device Migration Guide

First Published: 2026-01-30

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

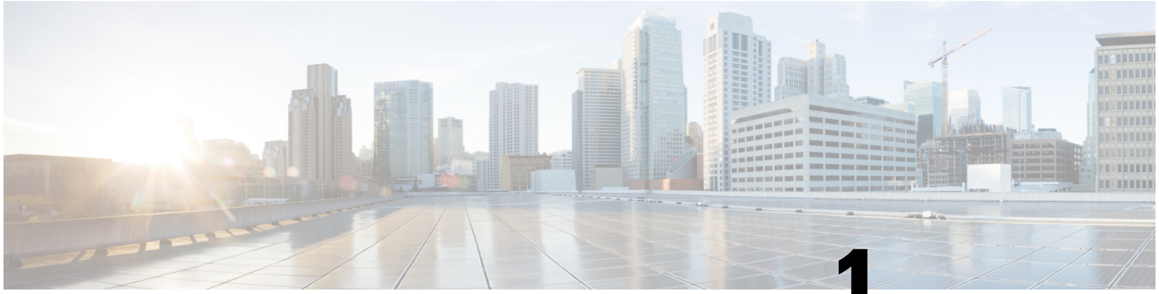
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

CONTENTS



CHAPTER 1

Device Migration Overview

This chapter explains the core concepts and structure of Device Migration.

Device Migration concepts

Device Migration is a framework for enabling a structured approach for transferring services, device configuration, and live network traffic from an existing network device to a new one while preserving operational dependencies and traffic continuity throughout the migration.

How Device Migration works

Device Migration is driven by user-defined migration Methods of Procedure (MOPs). A MOP defines the sequence of actions and validations required for a specific migration scenario, enabling users to design migration logic that fits their network topology and service requirements.

Attention Device Migration is not shipped with a pre-built MOP. Users must create their own MOP to perform specific tasks to facilitate the migration process.

Migration job and device coordination

Each migration runs as a single Device Migration job, which executes the selected MOP instance. All devices involved in the migration—including neighboring devices required for traffic rerouting or validation—operate within the same execution context. This ensures that inter-device dependencies are preserved and that configuration changes and traffic transitions are coordinated consistently.

Migration progression depends on the successful completion of the validations defined in the MOP.

User capabilities

Through the migration workflow application, users:

- Create custom migration MOPs,
- execute MOPs through a guided, pre-defined user flow, and
- tailor migration logic to specific operational and service requirements

Device support

Device Migration supports a heterogeneous device environment and facilitates migrations involving different device types, as long as those devices are supported.

Execution model

Device Migration follows a fleet-wide execution model in which all migration MOP actions run within a shared execution context. Instead of operating as separate per-device tasks, migration actions are evaluated and executed with awareness of every device included in the migration plan.

A migration activity may target:

- a single device, or
- multiple devices simultaneously, depending on its definition.

This model enables coordinated behavior across the migration—for example, validating neighbor state before applying changes, or sequencing configuration updates across dependent devices. By evaluating MOP actions against the full set of participating devices, the system ensures that multi-device operations are executed predictably and in the intended order.

Device roles and labeling

Each device included in a Device Migration job is assigned a role. Device roles define how a device participates in the migration.

Important You can add additional device labels if required. Predefined labels used by Device Migration cannot be removed. Multiple devices can use the same label.

You can add new custom labels by editing the Device Migration application (**Administration** > **Workflow Administration** > **Application Types** > **Device Migration**).

Typical roles include:

- source device, representing the device being replaced
- target device, representing the replacement device
- neighbor device, representing adjacent devices affected by the migration

Roles determine which migration actions apply to each device. Assigning a role does not modify device configuration by itself.

Actions in a migration MOP reference devices through the labels assigned to them, such as *source*, *target*, or *neighbor*. These labels allow the same MOP structure to be reused across different devices or environments. During execution, device-specific details are resolved dynamically through these labels so that each action operates on the correct device.

Migration structure

A Device Migration job follows a predefined structural layout specified by its migration MOP. The MOP organizes the migration into a set of ordered stages, with each stage containing one or more migration MOP actions.

Attention Device Migration is not shipped with a pre-built MOP. You must create your own MOP to perform specific tasks to facilitate the migration process.

Within this structure, the MOP determines:

- the sequence in which migration stages are executed
- the MOP actions associated with each stage
- the order in which MOP actions are evaluated within a stage

This structural definition governs how the migration progresses from initial preparation through final completion. The MOP structure remains fixed for the duration of the migration job and is not modified during execution, ensuring predictable and repeatable behavior.

Important Predefined stages are included in the Device Migration application type. You can add additional stages to support your migration scenarios. Predefined stages cannot be removed.

Migration stages

This topic describes the predefined stages available in Device Migration. These stages act as placeholders for grouping related migration actions. The stages themselves do not trigger any changes on the network; all operational changes occur through the actions you add within each stage.

Important You can add new custom stages by editing the Device Migration application (**Administration** > **Workflow Administration** > **Application Types** > **Device Migration**).

Pre-provision

The **Pre-provision** stage is used to validate the existing network state before the migration starts. You add actions here to confirm that the network is stable and that all prerequisites for migration are satisfied.

Typical actions include checking the health of services on the source device, verifying expected traffic paths, and running reachability tests such as ping or traceroute. No routing or topology changes are performed in this stage.

Pre-migration

The **Pre-migration** stage where you add actions that prepare the target device before any traffic or routing changes occur. This stage is intended for bringing the target device into a ready state.

Typical actions you may add include creating a service instance for the target device, applying baseline configuration such as interfaces or routing parameters, and validating that the service instance deploys successfully. Failures at this point generally indicate configuration or service-definition issues and can be corrected without impacting live traffic.

Migration

The **Migration** stage where you place the actions that perform the actual transition of services and traffic from the source device to the target device. This stage contains the coordinated changes required to complete the migration.

Typical actions include diverting traffic away from the source device (often through neighbor devices), deploying the full configuration on the target device, and updating routing so that traffic moves to the new device. Validation steps confirm that traffic flows correctly after each change. Traffic remains active throughout this stage, and diversion actions ensure continuity.

Post-migration

The **Post-migration** stage contains the actions you add to finalize the migration after traffic has successfully moved to the target device. This stage ensures that the new state is stable and removes configuration that is no longer needed.

Typical actions include validating traffic on the target device, removing the service instance for the source device, and decommissioning the old device configuration.

Supported environments and constraints

Device Migration operates within the limits of the devices, vendors, and services supported by the system. All devices included in a migration must satisfy specific prerequisites to ensure successful execution.

Device requirements

All devices participating in a Device Migration job must:

- Be present in the system inventory
- Be reachable at the time of job execution

Devices that do not meet these criteria cannot participate in the migration.

Environment support

Device Migration supports heterogeneous environments. Devices involved in a migration do not need to be of the same model or vendor, provided they satisfy the requirements of the migration definition. This includes support for multi-vendor environments such as Cisco and Juniper.

MOP customization considerations

Device Migration does not include any pre-built MOPs.

To perform a migration, you must create a migration MOP that reflects your specific scenario. The actions, stages, and validations you include depend on your device models, service implementation, and operational requirements.

Because migration needs differ across deployments, each MOP must be created from scratch and structured according to the steps required in your environment. This includes choosing the appropriate stages, selecting the required actions, and defining the sequence of checks needed to safely transition traffic and configuration to the target device.

Execution notes

- Device-specific details (such as device name, IP address, device type, OS version, etc.) are resolved dynamically at execution time based on the migration definition.
- Migration logic relies on standardized role references established during job configuration, enabling reuse of MOP structures across different environments.

CHAPTER 2

Perform Device Migration

This chapter describes how to run and manage a Device Migration job.

Create a Device Migration job

This topic explains how to create a Device Migration job by selecting devices, selecting a migration MOP, and entering job inputs.

Perform this task when you are ready to start a migration after preparing devices and a migration MOP.

Before you begin

- Ensure the source and target devices are onboarded and reachable.
- Verify that a migration MOP is available.
- Confirm that any required device roles or labels are assigned.
- Ensure you have permission to create and run migration jobs.

Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Device Migration**.

Step 2 The **New Device Migration** window appears, with the first step, **Select Devices**, highlighted. Select all devices that will participate in the migration, including the device being replaced, the device that will receive services and traffic, and any additional devices required for traffic diversion or validation.

Step 3 Click Next. The **New Device Migration** window is refreshed, with the next step, **Assign Device Roles**, highlighted. Assign a role to each selected device.

- *Source* for the device being migrated

- *Target* for the device receiving configuration and traffic
- *Neighbor* for devices used during traffic diversion or validation

Note

- You can assign the same role to multiple devices. This is useful when several devices share the same function in the migration—for example, when multiple neighboring devices participate in validating or diverting traffic during the migration.
- Assigning a device role does not modify the device configuration. Roles are used only to control how actions reference devices during execution.

Step 4 Click **Next**. The **New Device Migration** window is refreshed, with the next step, **Select MOP**, highlighted. Select a custom migration MOP that defines the stages, actions, and validation logic for the migration.

The selected MOP must already exist and must be designed to operate using the assigned device roles.

Note

All inputs required by the actions must be defined in the migration MOP. These typically include references to existing services, parameters used to create or update services, and values required for validation checks. All inputs must be explicitly provided.

Step 5 Click **Next**. The **New Device Migration** window is refreshed, with the next step, **Execution Settings**, highlighted. Provide an appropriate *Job name* and select the *Execution sequence*. Specify whether the migration job should execute immediately or be scheduled to run at a later time. The execution timing applies to the job as a whole.

- Provide an appropriate *Job name*
- Select the *Execution sequence*: Choose whether the migration job should start immediately or be scheduled for a later time. The execution timing applies to the job as a whole.
- (Optional) Enter *Job tags* to help identify the job later.

Important

You can run the stages in a migration MOP back-to-back—either immediately or at a scheduled time—or you can run each stage at different times. This page allows you to define the stage schedule, including setting individual execution times and adding delays or gaps between stages if needed.

Step 6 Click **Next**. The **New Device Migration** window is refreshed, with the final step, **Summary**, highlighted. Review the device migration settings you selected. Click **Run Job** to submit the job.

The migration job is created and appears on the **CWM Solutions Jobs** page.

Monitor a Device Migration job

After submission, the migration job is queued for execution based on the selected timing. The job executes each stage defined in the migration MOP in order. All actions in a stage complete before the next stage begins. If an action fails, execution stops at that point, and the job enters a failed state.

Use this procedure to monitor the progress and outcome of a Device Migration job.

Procedure

Step 1 From the main menu, choose **Operate** > **CWM Solution Jobs**.

Step 2 Identify the migration job using its name or status.

Step 3 Observe how the job progresses through the defined migration stages.

Step 4 Select individual actions to view execution status, inputs, outputs, and validation results.

Step 5 Use action-level messages to determine where issues occurred and whether corrective action is required.

Retry a Device Migration job

Retry allows a failed migration job to be executed again. When a job is retried, you can execute the entire job or resume execution from a specific stage.

Use this procedure to retry a migration job.

Procedure

Step 1 From the main menu, choose **Operate** > **CWM Solution Jobs**.

Step 2 Locate the job that failed and review the action where the failure occurred.

Step 3 Choose ⋯ and select **Retry**. You can choose to retry the entire job or a specific stage.

Note
If you choose to retry a specific stage, the previously completed stages are not re-executed.

Click **Retry** to confirm.

Step 4 The job is retried as per your selection.

Step 5 Observe job execution to confirm successful completion.

Rerun a migration stage

Use this procedure to rerun a stage of the Device Migration job.

Note Rerun operation is useful when earlier assumptions need to be revalidated or when migration inputs have changed.

Procedure

Step 1 From the main menu, choose **Operate** > **CWM Solution Jobs**.

Step 2 Identify the job that must be re-executed.

Step 3 Choose ⋯ and select **Rerun**.

The **Rerun Stage** window appears.

Step 4 Select the migration stage. Click **Rerun** to confirm.

Step 5 Track progress as the job reruns the selected migration stage.

Failure handling and validation

Action evaluation

Each action evaluates its outcome based on defined success conditions. Optional warning or failure conditions may also be configured. If the success condition is not met, the action is marked as failed by default.

Failure visibility

Failure information is available at multiple levels:

- Action-level details in the Jobs page show inputs, outputs, and evaluation results.
- Workflow execution details provide additional diagnostic information about where and why a failure occurred.