



Cisco Crosswork Workflow Manager Solutions 2.0 Fleet Upgrade Get Started Guide

First Published: 2024-12-12

Last Modified: 2025-03-19

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 NON-INFRINGEMENT 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 –2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Install Fleet Upgrade 1

- Meeting installation prerequisites 1
- CWM Solutions installation workflow 3
- NSO package pre-installation tasks 3
- Install the Crosswork Workflow Manager SVM Using Docker 6
- Install the CWM CAPP 10
- Install the CWM Solutions CAPP 12
- Use the GUI to create Credential Profiles 16
- Use the GUI to add an NSO Provider 18
- Install the CWM Solutions packages on NSO 20

CHAPTER 2

Get Started With Fleet Upgrade 25

- Onboard Devices 25
- Populate the Image Repository 29
- Create Image Policies 31
- Run a Policy Conformance Report 33
- Monitor Conformance Report Jobs 35
- Run a Fleet Upgrade 37
- Monitor Fleet Upgrade Jobs 39



CHAPTER 1

Install Fleet Upgrade

This document covers the following topics:

- [Meeting installation prerequisites, on page 1](#)
- [CWM Solutions installation workflow, on page 3](#)
- [NSO package pre-installation tasks, on page 3](#)
- [Install the Crosswork Workflow Manager SVM Using Docker, on page 6](#)
- [Install the CWM CAPP, on page 10](#)
- [Install the CWM Solutions CAPP, on page 12](#)
- [Use the GUI to create Credential Profiles, on page 16](#)
- [Use the GUI to add an NSO Provider, on page 18](#)
- [Install the CWM Solutions packages on NSO, on page 20](#)

Meeting installation prerequisites

Cisco Crosswork Workflow Manager (CWM) Solutions is a collection of pre-built use cases that offers customers a convenient and efficient way to manage and upgrade their devices. It provides out-the-box use cases that are easy to deploy and ready to use, allowing users to quickly onboard their devices for management.

CWM Solutions Fleet Upgrade lets users manage, distribute, and commit software image upgrades to multiple devices at the same time, including to third-party devices.

Fleet Upgrade is automated, customizable, extensible, provides strong error checking, and supports devices from Cisco and other vendors.

Installing CWM Solutions Fleet Upgrade requires installation of Cisco Crosswork Workflow Manager (CWM) and Cisco Network Services Orchestrator (NSO). The remaining sections of this topic detail the hardware, software and other requirements to be met for successful installation of this version of Cisco CWM Solutions and Fleet Upgrade.

Server hardware

You must install CWM Solutions on a server equipped with Cisco CWM. CWM Solutions also requires Cisco Network Services Orchestrator (NSO).

As a general guideline, users should select high-specification computing hardware for CWM Solutions installations. Installation of the CWM OVA requires VMware with vCenter 8 and ESXi 8 hosts. Due to their high performance, solid state drives (SSDs) are preferred over traditional hard disk drives (HDDs). If you are

using HDDs, their minimum speed should be over 15000 RPM. The VM data store(s) must have disk-access latency less than 10 ms or greater than 5000 IOPS.

Table 1: Server hardware requirements

Component	Software form	Size	vCPUs	Memory	Disk (SSD)	Swap disk
Cisco CWM SVM	OVA	XLarge profile	24	128GB	1TB	n/a
Cisco NSO 6.4.1	Tar / signed binary	n/a	16	256GB	1TB	256GB

Server software

CWM Solutions Fleet Upgrade runs on the following minimum versions of server software:

- EMS Lite CAPP
- CWM CAPP
- CWM Solutions CAPP
- Cisco NSO Function Pack Packages
- The CWM adapters for NSO and REST: cwm.v2.0.0.cisco.nso.v1.0.3.tar.gz and cwm.v2.0.0.generic.rest.v1.0.3.tar.gz

CWM Solutions Fleet Upgrade runs with Cisco NSO Version 6.4.1, with the following additional requirements:

- The NSO installation must be a System install, **NOT a Local install**. For details on the distinction, see [Ways to Deploy NSO](#).
- Python 3.9 or later
- Python package textfsm.
- Java 17 or later
- Ubuntu 22 or RHEL 8
- Requires ports open on NSO for 8080 or 8888 (HTTP/HTTPS for RESTCONF), 20243 for DLM.

Fleet Upgrade supported NOS and devices

The Fleet Upgrade workflow has been tested with and is known to work with the network operating systems and devices shown in the following table.

Table 2: Fleet Upgrade network OS and device support

Network OS	Device
Cisco IOS-XR Versions: 7.8.2, 7.9.2, 7.10.1, 7.11.1, 24.1.1, 24.2.2	Cisco NCS 540, Cisco C8000 (VXR), ASR9903, NCS 5501, XR LNDT and eXR platforms
Cisco IOS-XE Versions: IOS-XE 17.09, IOS-XE 17.12	ASR 1000 series, Catalyst 9000 series

Juniper JunOS versions 18.1R1.9, 21.1R3.11	Juniper MX960
--	---------------

Additional requirements

Supported browsers: Google Chrome (Version 131.0.x) and Mozilla Firefox (134.0.1) . For full functionality, browsers must have JavaScript and cookies enabled.

Site preparation: The user network environment must include the following:

- All network devices need access to the data network. The data network is the portion of the network dedicated to the transmission of user data, as opposed to the management network, which is optimized for IT management and control traffic.
- IPv4 address reservation and distribution: 4 total, 2 for the management network, 2 for the data network.
- IPv6 address reservation and distribution: 4 total, 2 for the management network, 2 for the data network.
- The Cisco Software Download feature requires access to the Internet from the server, and a Cisco customer username and password with authorization to download images from software.cisco.com.
- Active DNS and NTP servers.
- Active FTP and SFTP servers on ports TCP Ports 30621 and 30622, respectively.

CWM Solutions installation workflow

When you have reviewed the requirements listed in [Meeting installation prerequisites, on page 1](#), complete the following tasks in this order to install CWM Solutions and Fleet Upgrade:

1. [NSO package pre-installation tasks, on page 3](#)
2. [Install the Crosswork Workflow Manager SVM Using Docker, on page 6.](#)
3. [Install the CWM CAPP, on page 10.](#)
4. [Install the CWM Solutions CAPP, on page 12.](#)
5. [Use the GUI to create Credential Profiles, on page 16](#)
6. [Use the GUI to add an NSO Provider, on page 18](#)
7. [Install the CWM Solutions packages on NSO, on page 20](#)

With Fleet Upgrade fully installed, continue by following the steps in [Get Started With Fleet Upgrade, on page 25](#).

NSO package pre-installation tasks

Before installing the CWM Solutions packages for NSO, you must ensure that additional Python packages are installed and that NSO supports REST. CWM Solutions can use both HTTP and HTTPS, so you can choose to enable SSL/HTTPS in the REST configuration if needed. You will need to install SSL certificate files and specify their location in the RESTCONF configuration if you want to enable SSL.

Before you begin

Ensure that you have met the basic software requirements for the NSO installation, as explained in [Server software, on page 2](#). If you plan to enable HTTPS/SSL as part of the REST configuration, Cisco recommends that you create and install SSL certificate and key files in the NCS configuration directory before completing this task.

Procedure

Step 1 Install the following Python packages:

```
~$ sudo pip install textfsm
~$ sudo pip install jinja2
~$ sudo pip install pyyaml
~$ sudo pip install pycryptodome
```

Step 2 Edit the NSO `ncs.conf` file as shown below to enable REST support. The `<ssl>` block is optional and shown below in *italics* to distinguish it from REST and other commands. For example:

```
sudo vi /etc/ncs/ncs.conf

<webui>
  <enabled>true</enabled>
  <transport>
<tcp>
  <enabled>true</enabled>
  <ip>0.0.0.0</ip>
  <port>8080</port>
  <extra-listen>
    <ip>::</ip>
    <port>8080</port>
  </extra-listen>
</tcp>
<ssl>
  <enabled>true</enabled>
  <ip>0.0.0.0</ip>
  <port>8888</port>
  <key-file>${NCS_CONFIG_DIR}/ssl/cert/host.key</key-file>
  <cert-file>${NCS_CONFIG_DIR}/ssl/cert/host.cert</cert-file>
  <extra-listen>
    <ip>::</ip>
    <port>8888</port>
  </extra-listen>
</ssl>
</transport>

<cgi>
  <enabled>true</enabled>
  <php>
    <enabled>>false</enabled>
  </php>
</cgi>
</webui>

<restconf>
  <enabled>true</enabled>
</restconf>
```

Step 3 When you have finished the edit, save the `ncs.conf` file and restart NSO. For example:

```
sudo systemctl restart ncs
```

Step 4 Using an admin user ID, verify that REST is working correctly on your NSO installation. For example:

```
admin1@ncs% run show ncs-state rest
ncs-state rest listen tcp
ip    ::
port  8080
ncs-state rest listen tcp
ip    0.0.0.0
port  8080
ncs-state rest listen ssl
ip    ::
port  8888
ncs-state rest listen ssl
ip    0.0.0.0
port  8888
```

Step 5 Specify the following NSO global configuration settings:

```
admin1@ncs% show devices global-settings
connect-timeout 600;
read-timeout    600;
write-timeout   600;
ssh-algorithms {
  public-key [ ssh-rsa ];
}
trace           pretty;
ned-settings {
  cisco-iosxr {
    read {
      admin-show-running-config false;
    }
  }
}
```

Step 6 Ensure that the NETCONF Access Control Model (NACM) rule list grants the ncsadmin and Linux users permissions to perform functions on NSO. For example:

```
admin1@ncs% show nacm
read-default    deny;
write-default   deny;
exec-default    deny;
groups {
  group ncsadmin {
    user-name [ admin1 private ];
  }
  group ncsoper {
    user-name [ public ];
  }
}
```

For help adding more users, including adding them to auth groups, see the NSO topic [Adding a User](#).

What to do next

Follow the steps in [Install the CWM Solutions packages on NSO, on page 20](#).

Install the Crosswork Workflow Manager SVM Using Docker

The standalone version of CWM Solutions Fleet Upgrade runs on the SVM (single virtual machine) version of Crosswork Workflow Manager, also known as CWM SVM .

The following instructions explain how to install CWM SVM using a Docker container installed on VMWare vCenter.

Before you begin

When following the instructions in this section:

- Make sure that your VMware environment meets all the vCenter requirements specified in the *Crosswork Network Controller 7.1 Installation Guide* section [Installation Requirements](#).
- The edited template in the /data directory contains sensitive information (VM passwords and the vCenter password). The operator needs to manage access to this content. Store the templates used for your install in a secure environment or edit them to remove the passwords.
- The install.log, install_tf.log, and .tfstate files will be created during the install and stored in the /data directory. If you encounter any trouble with the installation, provide these files to the Cisco Customer Experience team when opening a case.
- The install script is safe to run multiple times. Upon error, input parameters can be corrected and re-run. You must remove the install.log, install_tf.log, and tfstate files before each re-run. Running the installer tool multiple times may result in the deletion and re-creation of VMs.
- In case you are using the same installer tool for multiple Crosswork installations, it is important to run the tool from different local directories, allowing for the deployment state files to be independent. The simplest way for doing so is to create a local directory for each deployment on the host machine and map each one to the container accordingly.
- Docker version 19 or higher is required while using the installer tool. For more information on Docker, see <https://docs.docker.com/get-docker/>.
- In order to change install parameters or to correct parameters following installation errors, it is important to distinguish whether the installation has managed to deploy the VM or not. Deployed VM is evidenced by the output of the installer similar to:

```
vsphere_virtual_machine.crosswork-IPv4-vm["1"]: Creation complete after 2m50s
[id=4214a520-c53f-f29c-80b3-25916e6c297f]
```

Procedure

-
- Step 1** In your Docker-capable Virtual Machine, create a directory where you will store everything you will use during this installation. For purposes of these instructions, we will call this directory `myinstall`. If you are using a Mac, make sure the directory name is in lower case.
- Step 2** In `myinstall`, use the file editor of your choice to create a VMWare deployment template manifest (or "tfvars") file like the sample shown below. The tfvars file contains parameters for deploying a CWM SVM OVA in a VM environment, including assigning four IP addresses on vCenter. Before using the tfvar file, customize the parameter values *shown in italics* to fit your environment. Name the file `deployment.tfvars`.

```

Cw_VM_Image = ""      # Line added automatically by installer.
ClusterIPStack       = "IPv4"
DNS                  = "171.70.168.183"
DomainName           = "cisco.com"
CWPASSWORD           = "Cisco123#"
NTP                  = "ntp.esl.cisco.com"
VMSIZE               = "XLarge"
ThinProvisioned      = "false"
IgnoreDiagnosticsCheckFailure = "False"
Timezone             = "America/Los_Angeles"
EnableSkipAutoInstallFeature = "True"
ManagementVIP        = "172.22.140.180"
ManagementIPNetmask  = "255.255.255.0"
ManagementIPGateway  = "172.22.140.1"
DataVIP              = "14.14.14.12"
DataIPNetmask        = "255.255.255.0"
DataIPGateway        = "14.14.14.1"
CwVMs = {
  "0" = {
    VMName              = "svm-180",
    ManagementIPAddress = "172.22.140.182",
    DataIPAddress       = "14.14.14.13",
    NodeType            = "Hybrid"
  }
}
VCenterDC = {
  VCenterAddress = "<vcenterAddress>",
  VCenterUser    = "administrator@vsphere.local",
  VCenterPassword = "<vcenterPassword>",
  DCName         = "SVM-Datacenter",
  MgmtNetworkName = "VM Network",
  DataNetworkName = "Network2"
  VMs = [{
    HostedCwVMs = ["0"],
    Host         = "172.22.140.210",
    Datastore    = "datastore1",
    HSDatastore  = "datastore1"
  }]
}
SchemaVersion = "7.1.0"

```

- Step 3** Download the CWM SVM installer bundle (.tar.gz file) and the OVA file from software.cisco.com to myinstall. For the purpose of these instructions, we will use the file name **signed-cw-na-unifiedems-installer-7.1.0-85-release710-240823.tar.gz** and **signed-cw-na-unifiedems-7.1.0-85-release700-240823.ova**

The file names mentioned in this topic are sample names. They may differ from the actual file names in software.cisco.com

- Step 4** Use the following command to extract the installer bundle:

```
tar -xvf signed-cw-na-unifiedems-installer-7.1.0-85-release700-240823.tar.gz
```

The contents of the installer bundle is extracted (e.g. signed-cw-na-unifiedems-installer-7.1.0-85-release700-240823-release). The extracted files will contain the installer image (**cw-na-unifiedems-installer-7.1.0-85-release710-240823.tar.gz**) and files necessary to validate the image.

- Step 5** Review the contents of the README file to understand everything that is in the package and how it will be validated in the following steps.

Step 6 Use the `python --version` command to learn the version of Python on your machine. Then use one of the following commands to verify the signature of the installer image:

If you are using Python 2.x: `python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file> -v dgst -sha512`

If you are using Python 3.x: `python3 cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file> -v dgst -sha512`

If you do not have Python installed, go to python.org and download the version of Python that is appropriate for your machine.

Step 7 Use the following command to load the installer image file into your Docker environment.

```
docker load -i <.tar.gz file>
```

For example: `docker load -i cw-na-unifiedems-installer-7.1.0-85-release710-240823.tar.gz`

Step 8 Run the `docker image list` or `docker images` command to get the IMAGE ID value you will need in the next step.

For example: `docker images`

The output of this command will be similar to the following example. The IMAGE ID value you will need in the next step is underlined for clarity in the example below:

```
My Machine% docker images
REPOSITORY                                TAG                                IMAGE ID                                CREATED
SIZE
dockerhub.cisco.com/cw-installer cw-na-unifiedems-7.1.0-85-release710-240823 a4570324fad30 7 days
ago 276MB
```

Pay attention to the `CREATED` time stamp in the table presented when you run `docker images`, as you may have other images present from the installation of prior releases. If you wish to remove these, you can use the `docker image rm {image id}` command.

Step 9 Launch the Docker container using the following command:

```
docker run --rm -it -v `pwd`::/data {image id of the installer container}
```

To run the image with the IMAGE ID from our example in the previous step, you would use the following command:

```
docker run --rm -it -v `pwd`::/data a4570324fad30
```

Note

- You do not have to enter the full IMAGE ID value. In this case, `docker run --rm -it -v `pwd`::/data a45` would also work. Docker requires enough of the IMAGE ID value to uniquely identify the image you want to use for the installation.
- We are using the backtick (`). This is recommended. Do not use the single quote or apostrophe (') for this purpose, as the meaning to the shell is very different. By using the backtick, the template file and the OVA will be stored in the current directory (that is, where you are on your local disk) when you run the commands, instead of inside the container.
- When deploying an IPv6 setup, the installer needs to run on an IPv6-enabled container/VM. This requires additionally configuring the Docker daemon before running the installer, using the following method:

- **Linux hosts (ONLY):** Run the Docker container in host networking mode by adding the `-network host` flag to the `docker run` command. For example:

```
docker run --network host <remainder of docker run options>
```


- Centos/RHEL hosts, by default, enforce a strict SELinux policy which does not allow the installer container to read from or write to the mounted data volume. On such hosts, run the Docker volume command with the Z option:

```
docker run --rm -it -v `pwd`:data:Z <remainder of docker options>
```

Note

The Docker command provided will use the current directory to read the template and the ova files, and to write the log files used during the install.

If you encounter either of the following errors, you should move the files to a directory where the path is in all lowercase, with no spaces or other special characters. Then navigate to that directory and rerun the installer.

- Error 1: % docker run --rm -it -v `pwd`:data a45 docker: invalid reference format: repository name must be lowercase. See 'docker run --help'
- Error 2: docker: Error response from daemon: Mounts denied: approving /Users/Desktop: file does not exist ERRO[0000] error waiting for container: context canceled

Step 10 From the /opt/installer directory, run the installer:

```
./cw-installer.sh install -m /data/<template file name> -o /data/<.ova file>
```

For example:

```
./cw-installer.sh install -m /data/deployment.tfvars -o  
/data/signed-cw-na-unifiedems-7.1.0-85-release710-240823.ova
```

Step 11 Enter Yes to accept the End User License Agreement (EULA).

Step 12 Enter "yes" when prompted to confirm the operation.

It is not uncommon to see some warnings like the following during the install:

```
Warning: Line 119: No space left for device '8' on parent controller '3'.  
Warning: Line 114: Unable to parse 'enableMPTSupport' for attribute 'key' on element 'Config'.
```

You can ignore these warnings if the install script shows output like the sample below, which indicates that the installation is proceeding to a successful conclusion:

Sample output:

```
cw_vms = <sensitive>  
INFO: Copying day 0 state inventory to CW  
INFO: Waiting for deployment status server to startup on 10.90.147.66.  
Elapsed time 0s, retrying in 30s
```

If the install script fails, open a case with Cisco and provide the .log files that were created in the /data directory (and the local directory where you launched the installer Docker container), to Cisco for review. The most common reasons for the install to fail are a password that is not adequately complex, and errors in the template file. If the installer fails for any errors in the template (for example, mistyped IP address), correct the error and rerun the install script.

Step 13 When the install script concludes successfully, it starts to deploy a new VM onto the vCenter specified in the tfvars file and returns output like the following sample:

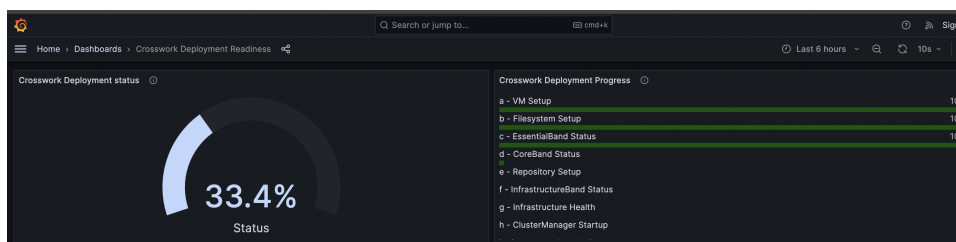
```
Crosswork deployment status available at  
http://172.22.140.180:30602/d/NK1bwVxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark
```

Once deployment is complete login to Crosswork via: <https://172.22.140.180:30603/#/logincontroller>

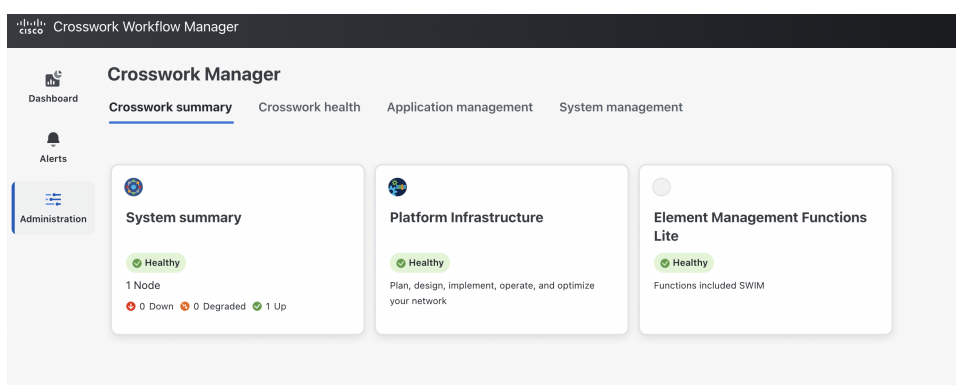
```
Tue Mar 25 17:07:00 UTC 2099:  
INFO: Cw Installer operation complete.
```

Step 14

Use the first link from the script completion message ("Crosswork deployment status available...") to display a Crosswork Deployment Readiness dashboard like the one shown below. Use the dashboard to monitor the continuing deployment of the new CWM SVM installation. When the Crosswork Deployment Status displays 100%, the CWM SVM is ready.

**Step 15**

Use the second link from the script completion message ("Once deployment is complete login...") to access the CWM SVM interface. Use the default username and password **admin** to log in and set up a new password. Log in with the new credentials and select **Administration > Crosswork Manager** to verify that the system is healthy.

**What to do next**

Follow the steps in [Install the CWM CAPP, on page 10](#).

Install the CWM CAPP

Once you have installed CWM SVM, you can install the Crosswork Workflow Manager application, which is distributed as a Crosswork CAPP file.

Procedure

- Step 1** Get the URL of the CWM CAPP file from your Cisco sales team. You can either download it directly from the Cisco server to CWM, or download it to a storage directory on your local VM or another storage resource in your network and then upload it to CWM.
- Step 2** Log in to CWM using an admin ID and select **Administration > Crosswork Manager > Application Management**.
- Step 3** Click **Add new file** and select **Upload CAPP file (.tar.gz)**.
- Step 4** Using the **Add File (.Tar.Gz)** page, first select the **Protocol** you want to use to add the CWM Solutions CAPP file to the system. Then:

- a) If you selected **URL**: Enter the **URL** where the CAPP file is stored, and ensure the **Basic Auth** checkbox is selected. Then enter the **Username** and **Password** needed to access the URL.
- b) If you selected **SCP**: Enter the file's **Server path/Location**, the server's **Host name/IP address**, **Port**, and the login **Username** and **Password**, as shown in the following figure.

Add Application Bundle (.tar.gz)

Protocol ☒ URL ☐ SCP

URL *

Example: <http/https>://foo.com/temp.tar.gz

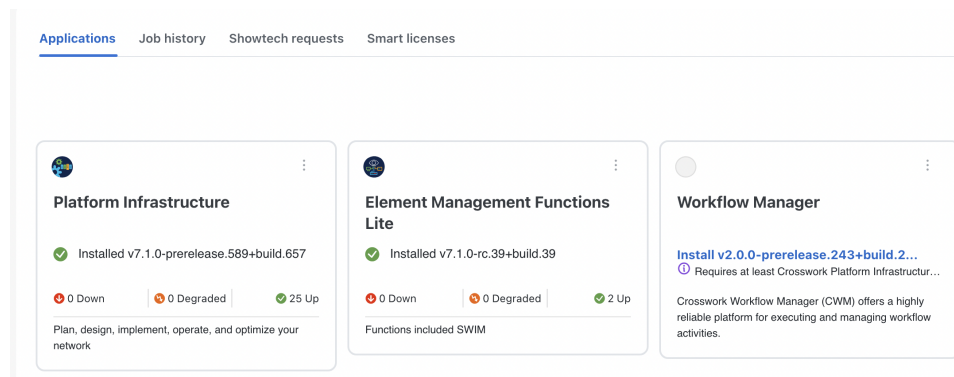
☐ Basic auth

☐ Automatically clean all repository files before adding a new file

Cancel Add

Step 5 Click **Add**. You can select the **Job History** option to monitor the download while it proceeds.

Step 6 When the addition completes, the **CWM Solutions** tile appears on the **Applications** page, indicating that the application is ready to install.



Step 7 Click the **More** icon (three dots) on the **Workflow Manager** tile to display the **Workflow Manager** installation pop up.

Step 8 When installation is complete, the **Applications Management > Job History** tab should display an "Activation Successful" message. You can also verify successful installation by choosing **Administration > Crosswork Manager > Crosswork Health > Workflow Manager**. The **Microservices** tab should show the 10 microservices in the following figure, all with a **Healthy** status.

Crosswork Manager

Crosswork summary **Crosswork health** Application management System management

Workflow Manager Healthy Microservices(10) 10 0 0 0 Recommendation None

Description: Crosswork Workflow Manager (CWM) offers a highly reliable platform for executing and managing workflow activities.

Microservices Alarms

Filtered 0 / Total

Status	Type	Name	Current version	Up time	Recommendation	Description
Healthy	Static	cwm-engine-history-service	2.0.0-prerelease.178	21m 14s	None	
Healthy	Static	cwm-engine-matching-service	2.0.0-prerelease.178	21m 7s	None	
Healthy	Static	cwm-engine-worker-service	2.0.0-prerelease.178	21m 1s	None	
Healthy	Static	cwm-event-worker-service	2.0.0-prerelease.178	19m 54s	None	
Healthy	Static	cwm-worker-manager-service	2.0.0-prerelease.178	17m 23s	None	
Healthy	Static	cwm-adapter-manager-service	2.0.0-prerelease.178	22m 31s	None	
Healthy	Static	cwm-dsl-service	2.0.0-prerelease.178	20m 31s	None	
Healthy	Static	cwm-event-service	2.0.0-prerelease.178	19m 46s	None	
Healthy	Static	cwm-api-service	2.0.0-prerelease.178	19m 16s	None	
Healthy	Static	cwm-engine-frontend-service	2.0.0-prerelease.178	21m 48s	None	

What to do next

[Install the CWM Solutions CAPP, on page 12](#)

Install the CWM Solutions CAPP

Once you have installed Crosswork Workflow Manager, you can install the Crosswork Workflow Manager Solutions application, which is also distributed as a Crosswork CAPP file.

Procedure

- Step 1** As with the CWM CAPP file, get the URL of the CWM Solutions CAPP file from your Cisco sales team. You can either download it directly from the Cisco server to CWM, or download it to a storage directory on your local VM or another storage resource in your network and then upload it to CWM.
- Step 2** Log in to CWM using an admin ID and select **Administration > Crosswork Manager > Application Management**.
- Step 3** Click **Add new file** and select **Upload CAPP file (.tar.gz)**.
- Step 4** Using the **Add File (.Tar.Gz)** page, first select the **Protocol** you want to use to add the CWM Solutions CAPP file to the system. Then:
- If you selected **URL**: Enter the **URL** where the CAPP file is stored, and ensure the **Basic Auth** checkbox is selected. Then enter the **Username** and **Password** needed to access the URL.
 - If you selected **SCP**: Enter the file's **Server path/Location**, the server's **Host name/IP address**, **Port**, and the login **Username** and **Password**, as shown in the following figure.

Add Application Bundle (.tar.gz)

Protocol ☒ URL ☐ SCP

URL * Example: <http/https>://foo.com/temp.tar.gz

☐ Basic auth

☐ Automatically clean all repository files before adding a new file

[Cancel](#) [Add](#)

Step 5

Click **Add**. You can select the **Job History** option to monitor the download while it proceeds.

Step 6

When the addition completes, the **Workflow Manager Solutions** tile appears on the **Applications** page at the far right, indicating that the application is ready to install.

Crosswork Manager

Crosswork summary Crosswork health **Application management** System management

[Applications](#) [Job history](#) [Showtech requests](#) [Smart licenses](#)

[Add new](#)

Platform Infrastructure

Installed v7.1.0-prerelease.589+build.657

0 Down 0 Degraded 26 Up

Plan, design, implement, operate, and optimize your network

Element Management Functions Lite

Installed v7.1.0-rc.39+build.39

0 Down 0 Degraded 2 Up

Functions included SWIM

Workflow Manager

Installed v2.0.0-prerelease.243+build.2

0 Down 0 Degraded 10 Up

Crosswork Workflow Manager (CWM) offers a highly reliable platform for executing and managing workflow activities.

Workflow Manager Solutions

Install v2.0.0-RC.3+1

Requires at least Crosswork Manager v7.1.0-rc.39+build.39

Execute mcp based fleet upgrade, generate conformance report, manage image repository.


Install Upgrade Activate Uninstall View details

Step 7

Click the **More** icon (three dots) on the **Workflow Manager Solutions** tile to display the **Workflow Manager Solutions** installation pop up, then click **Install**.

← Crosswork Manager

Application Installation



Workflow Manager Solutions

Description Execute mop based fleet upgrade, run software conformance report, manage image repository.

Installation Information

Current status

Version

Install instructions Requires at least Crosswork Platform Infrastructure 7.1.0

[Install](#) [Cancel](#)

Step 8

The **Application Management > Job History** tab should display an "Activation of application Workflow Manager Solutions Successful" message.

Crosswork Manager

Crosswork summary Crosswork health **Application management** NSO deployment manager System management

Applications **Job history** Showtech requests Smart licenses

Job sets Total 8

Status	Job ID	Actions	User
In progress	AJ8	install and activate	admin
Completed	AJ7	add to repository	admin
Completed	AJ6	install and activate	admin
Completed	AJ5	add to repository	admin
Completed	AJ4	install and activate	orchestrator
Completed	AJ3	add to repository	orchestrator
Completed	AJ2	install and activate	orchestrator
Completed	AJ1	add to repository	orchestrator

Job details

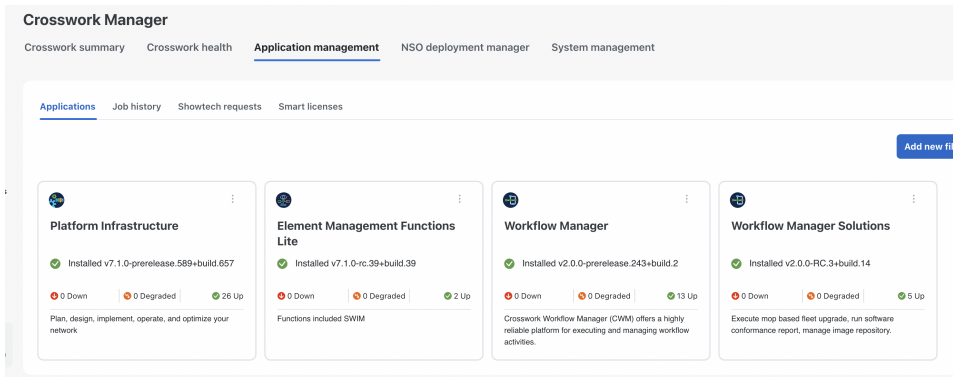
Job ID: AJ8 Status: In progress User: admin Start: End:

Jobs (70)

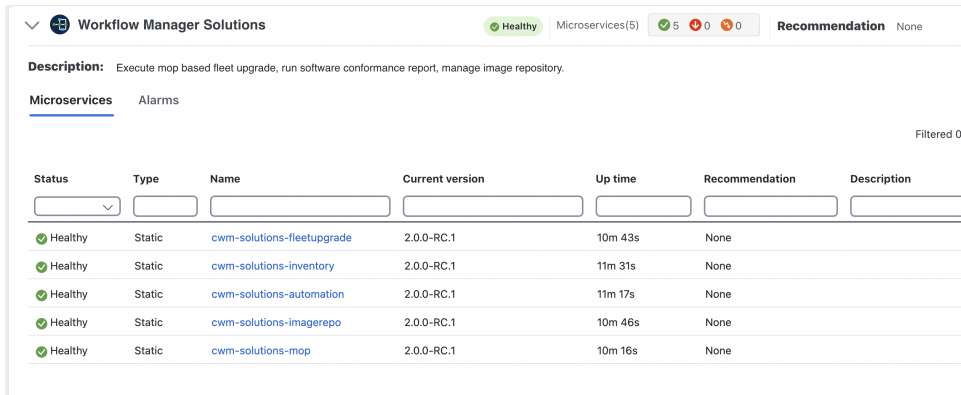
Time stamp	Description
25-Mar-2025 01:38:19 PM PDT	Activation of application Workflow Manager Solutions successful
25-Mar-2025 01:38:19 PM PDT	Workflow Manager Solutions services are healthy after 2m21s
25-Mar-2025 01:38:19 PM PDT	Waiting for services to be healthy 2m21s
25-Mar-2025 01:37:59 PM PDT	Waiting for services to be healthy 2m1s
25-Mar-2025 01:37:39 PM PDT	Waiting for services to be healthy 1m41s
25-Mar-2025 01:37:19 PM PDT	Waiting for services to be healthy 1m21s
25-Mar-2025 01:36:59 PM PDT	Waiting for services to be healthy 1m1s

Step 9

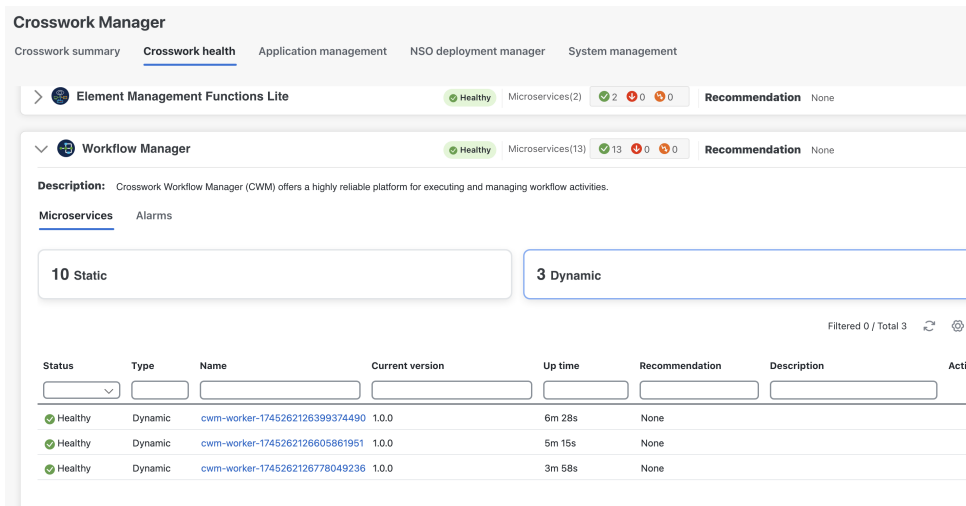
Application Management > Applications tab should show all four applications are up.

**Step 10**

Choose **Administration > Crosswork Manager > Crosswork Health > Workflow Manager Solutions**. The **Microservices** tab should show all five CWM Solutions microservices are in a **Healthy** state.

**Step 11**

Finally, CWM Solutions will add three dynamic service pods to CWM. These are worker pods for the three CWM adapters that CWM Solutions installed automatically. You will find them under **Administration > Crosswork Manager > Crosswork Health > Workflow Manager** (not under Workflow Manager Solutions).



What to do next

[Use the GUI to create Credential Profiles, on page 16](#)

Use the GUI to create Credential Profiles

Credential profiles allow CWM Solutions to authenticate when it attempts to access NSO and your devices. In this procedure, we'll create the NSO credential profile first and then the device profile.

Before you begin

Ensure that you've already installed CWM Solutions per the instructions in the main [CWM Solutions installation workflow, on page 3](#).

Procedure

Step 1 Log in to Crosswork Workflow Manager and select **Device Management > Credential Profiles**. CWM displays the **Credential Profiles** list.

Step 2 Click + to add a credential profile for NSO.

Step 3 Complete the fields on the **Add New Profile** window as follows:

In this field...	Enter or select:
Profile name	NSO-Credential (or any unique name you find meaningful)
Connectivity type	SSH
User name	The username for an admin user on the NSO server. This can be a dedicated CWM Solutions user with admin privileges that you create on the NSO server.
Password	The password for this username.
Confirm password	The same password you entered in Password .
Enable password	Leave this field blank.

Step 4 Click + **Add another** to display another set of connectivity protocol to the same NSO credential profile. This time, select **HTTPS** as the **Connectivity type**, and enter the appropriate NSO user and password information for this protocol, just as you did for Step 3. For example:

Credential Profiles

Add New Profile

Profile name *
NSO-credentials

Add credential protocols

Connectivity type: SSH, User name: admin1, Password: [masked], Confirm password: [masked], Enable password: [checked]

Connectivity type: HTTPS, User name: admin1, Password: [masked], Confirm password: [masked], Enable password: [checked]

+ Add another

Cancel Save

Step 5 When you are finished, click **Save** to save the NSO credential profile. You should see the profile appear on the **Credential Profiles** list.

Step 6 Repeat Steps 2 through 5 to create another credential profile for your devices, adding as many device login credentials and protocols (SSH, NETCONF, HTTP, HTTPS) as are appropriate for the devices you intend to manage using CWM Solutions. The following figure shows how you might create a single device credential profile. You might create multiple credential profiles if you have groups of devices using the same protocols but with different credentials. For example:

Credential Profiles

Add New Profile

Profile name *
devices-profile

Add credential protocols

Connectivity type: SSH, User name: admin, Password: [masked], Confirm password: [masked], Enable password: [checked]

Connectivity type: SNMPv2, Read community: [masked], Write community: [masked]

+ Add another

Cancel Save

What to do next

Record the name of the NSO credential profile you created during this task, as you will need it in the next task, [Use the GUI to add an NSO Provider, on page 18](#).

Use the GUI to add an NSO Provider

Providers let Crosswork Workflow Manager know which helper applications control your devices. In this step, we'll create an NSO provider and assign it the Credential Profile we created in the last step, so CWM can authenticate when it communicates with NSO.

Before you begin



Ensure that you've already created the two Credential Profiles as explained in [Use the GUI to create Credential Profiles](#), on page 16. You will need the name of the NSO Credential Profile to complete the following task.



Procedure













Step 1 Log in to Crosswork Workflow Manager and select **Administration > Manage Provider Access**.

Step 2 Click + to add an NSO provider.

Step 3 Complete the fields on the **Add New Profile** window as follows:

In this field...	Enter or select:
Provider name	The name of the provider, such as NSO .
Credential profile	The name of the NSO credential profile you created in Use the GUI to create Credential Profiles , on page 16.
Family	NSO
Connection type(s)	
Protocol	<p>Select the principal protocol that the Cisco Crosswork application will use to connect to the provider. NSO typically uses HTTPS and/or SSH.</p> <p>To add more connectivity protocols for this provider, click the  icon at the end of the first row. To delete a protocol you have entered, click the  icon shown next to that row.</p> <p>You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol.</p>
Server details	<p>One of these options:</p> <ul style="list-style-type: none"> • IP Address (IPv4 or IPv6) and subnet mask of the provider's server. • FQDN (Domain name and Host name)
Port	The port number to use to connect to the provider's server. This is the port corresponding to the protocol being configured. For example, if the protocol used to communicate with the provider server is SSH, the port number is usually 22. NSO often uses 8888 as a default.
Timeout	The amount of time (in seconds) to wait before the connection times out. The default is 30 seconds.

In this field...	Enter or select:
Model Prefix Info	
Model	<p>Select the model prefix that matches the NED CLI used by Cisco NSO. Valid values are:</p> <p>Cisco-IOS-XR</p> <p>Cisco-NX-OS</p> <p>Cisco-IOS-XE</p> <p>For telemetry, only Cisco-IOS-XR is supported.</p> <p>To add more model prefix information for this Cisco NSO provider, click the  icon at the end of any row in the Model Prefix Info section. To delete a model prefix you have entered, click the  icon shown next to that row.</p>
Version	Enter the Cisco NSO NED driver version used on the NSO server.
Provider Properties	
Property Key	Enter the name of the key for the special provider property you want to configure. For details on NSO and special properties, see Add Cisco NSO Providers .
Property Value	Enter the value to assign to the property key.

Manage Provider Access											
<div>      </div> <div>Selected 0 / Total 1   </div>											
Reachability	State	Provider name	UUID	Credentia...	Connectivity type	Family	Type	Model prefix	Model ver...	Site	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	 Reachable	 Unlock	NSO	 	f8868040-4003-4656-917d-e3c...	NSO-cred...	HTTPS	 NSO	Cisco-IOS-XR	 7.8.2	

Step 4

When you are finished, click **Save** to save the NSO Provider profile. After a delay while Crosswork attempts to reach NSO, you should see the profile appear on the **Manage Provider Access** list, as shown in the example below.

Add Provider

Provider name *

NSO

Credential profile *

NSO-credentials

Family *

NSO

Connection type(s)

Protocol *	Server details *	Port *	Timeout(sec)	
<div> <div>HTTPS</div> <div></div> </div>	<div> <div> <input checked="" type="radio"/> IP Address <input type="radio"/> FQDN </div> <div>10.195.73.106</div> </div>	<div>8888</div>	<div>600</div>	<div></div>

+ Add another

Provider properties

Property key	Property value	
nso_crosslaunch_url		<div></div> <div></div>

+ Add another

Model Prefix Info

<div> <div>Model *</div> <div>Cisco-IOS-XR</div> </div>	<div> <div>Version *</div> <div>7.8.2</div> </div>	<div></div>
---	--	-------------

Cancel

Save

What to do next

Follow the steps in [Install the CWM Solutions packages on NSO, on page 20](#).

Install the CWM Solutions packages on NSO

Use Crosswork's NSO Deployment Manager to deploy the CWM Solutions function pack bundles on NSO. These packages will provide the basic inventory management and other NSO capabilities needed to use CWM Solutions. You will also need to log in to NSO to ensure that NACM is enabled and other NSO settings are properly configured.

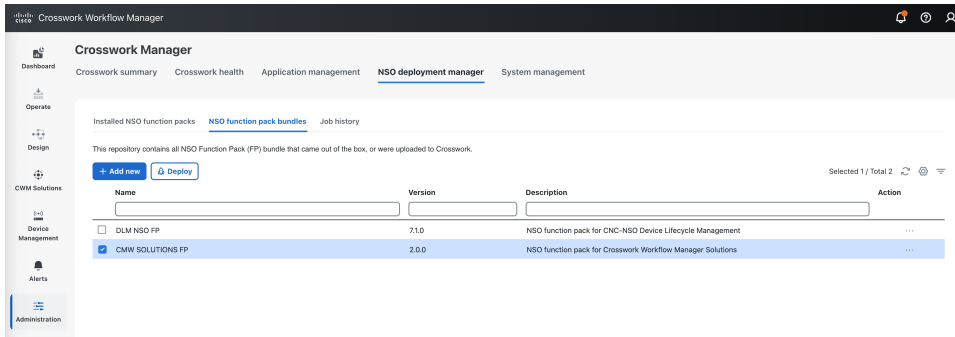
Before you begin

Ensure you have added NSO as a provider as explained in [Use the GUI to add an NSO Provider, on page 18](#)

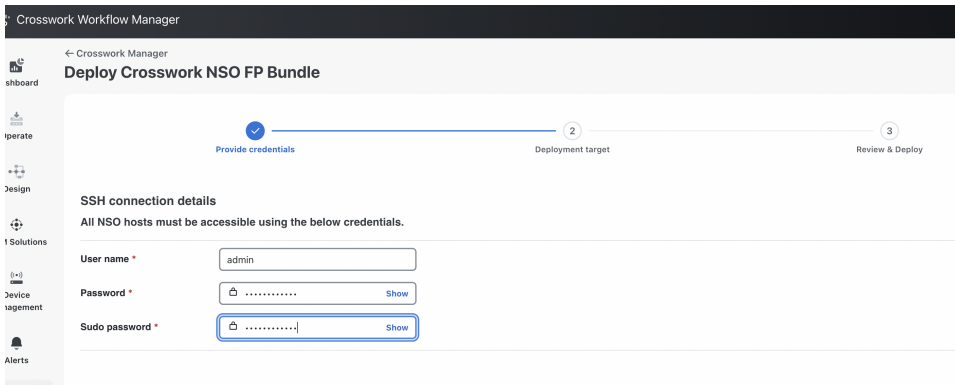
Procedure

Step 1 Log in to Crosswork and choose **Administration > Crosswork Manager > NSO Deployment Manager**.

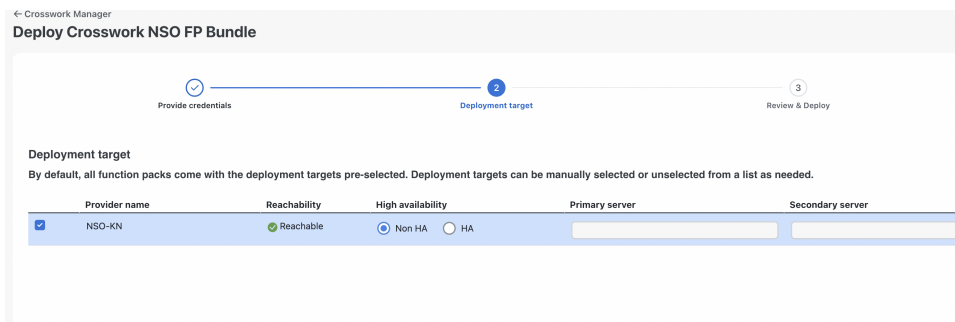
Step 2 Under **NSO Deployment Manager**, choose the **NSO function pack bundles** tab and click the check box next to **CWM SOLUTIONS FP**. Then click the **Deploy** button to start the deployment process.



Step 3 When prompted on the first **Provide credentials** page, provide the **SSH User name**, **password** and **Sudo password** credentials.



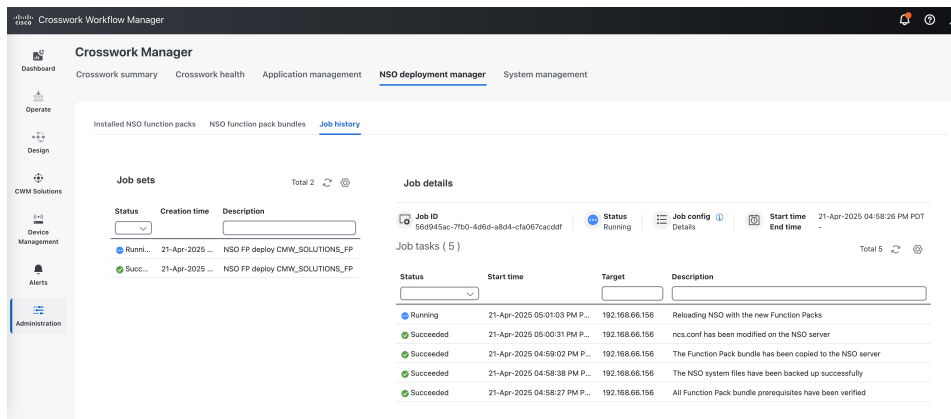
Step 4 On the **Deployment target** page, select **Non-HA** in the **High Availability** column, as shown below.



Step 5 When prompted on the **Review & Deploy** page, click **Deploy**.

Step 6 Click the **Job History** tab to monitor the NSO deployment as it proceeds. You will see the CWM Solutions packages listed in the **Job Details** window for the running job.

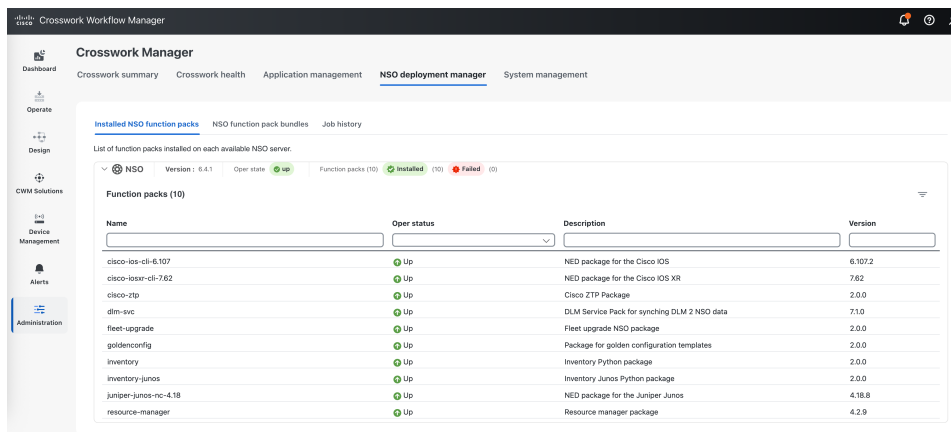
Install the CWM Solutions packages on NSO



Step 7

When the job is listed as **Succeeded**, click the **Installed NSO function packs** tab and expand the NSO provider to verify that the packages are all installed.

The package list should look like the illustration below.



You can also verify that all the packages are installed correctly by running the `show packages` command on NSO and comparing the command output with the list shown below.

```
admin1@ncs% run show packages package oper-status | tab
```

PACKAGE		PROGRAM								
META		FILE	CODE		JAVA	PYTHON	BAD NCS	PACKAGE	PACKAGE	CIRCULAR
DATA	LOAD	ERROR	UP	ERROR	UNINITIALIZED	UNINITIALIZED	VERSION	NAME	VERSION	
NAME	DEPENDENCY	ERROR	ERROR	INFO	WARNINGS					
cisco-ios-cli-6.107	-	X	-	-	-	-	-	-	-	-
cisco-iosxr-cli-7.62	-	X	-	-	-	-	-	-	-	-
cisco-ztp	-	X	-	-	-	-	-	-	-	-
dlm-svc	-	X	-	-	-	-	-	-	-	-
fleet-upgrade	-	X	-	-	-	-	-	-	-	-
goldenconfig	-	X	-	-	-	-	-	-	-	-

```

- - - - -
inventory          X - - - - -
- - - - -
inventory-junos    X - - - - -
- - - - -
juniper-junos-nc-4.18 X - - - - -
- - - - -
resource-manager   X - - - - -
- - - - -

```

```
[ok] [2025-04-22 12:06:26]
```

```
[edit]
```

```
admin1@ncs% run show packages package package-version | tab
```

```

      PACKAGE
NAME      VERSION
-----
cisco-ios-cli-6.107  6.107.2
cisco-iosxr-cli-7.62  7.62
cisco-ztp             2.0.0
dlm-svc               7.1.0
fleet-upgrade         2.0.0
goldenconfig          2.0.0
inventory             2.0.0
inventory-junos       2.0.0
juniper-junos-nc-4.18 4.18.8
resource-manager      4.2.9

```

Step 8

If you haven't already done so, log in to NSO and set the following device global settings in configuration mode. These NSO settings are required for Fleet Upgrade.

```

admin@ncs% set devices global-settings connect-timeout 600
admin@ncs% set devices global-settings read-timeout 600
admin@ncs% set devices global-settings write-timeout 600
admin@ncs% set devices global-settings ssh-algorithms public-key ssh-rsa
admin@ncs% set devices global-settings trace pretty
admin@ncs% set devices global-settings ned-settings cisco-iosxr read admin-show-running-config false
admin@ncs% commit

```

```

admin@ncs% show devices global-settings
connect-timeout 600;
read-timeout    600;
write-timeout   600;
ssh-algorithms {
  public-key [ ssh-rsa ];
}
trace           pretty;
ned-settings {
  cisco-iosxr {
    read {
      admin-show-running-config false;
    }
  }
}

```

Step 9

Note that NACM is required for NSO. Ensure the Linux user has ncsadmin rights to perform functions on NSO.

```

admin@ncs% set nacm groups group ncsadmin user-name admin
admin@ncs% commit

```

```

admin@ncs% show nacm
read-default    deny;
write-default   deny;

```

```
exec-default    deny;
groups {
    group ncsadmin {
        user-name [ admin private ];
    }
    group ncsoper {
        user-name [ public ];
    }
}
```

Step 10

Copy the `ncs_backup.sh`, `ncs_restore.sh` and `get_technical_support_data.sh` scripts from the provided bundle to the `scripts` directory under the `NCS_RUN_DIR`, and update the permissions of the copied scripts to make them executable.

```
# Locate the NCS_RUN_DIR using the following command
cat /etc/systemd/system/ncs.service | grep NCS_RUN_DIR=

# Update the permission
chmod +x ncs_backup.sh ncs_restore.sh get_technical_support_data.sh
```

What to do next

Follow the steps in [Get Started With Fleet Upgrade](#), on page 25.



CHAPTER 2

Get Started With Fleet Upgrade

This document covers the following topics:

- [Onboard Devices, on page 25](#)
- [Populate the Image Repository, on page 29](#)
- [Create Image Policies, on page 31](#)
- [Run a Policy Conformance Report, on page 33](#)
- [Monitor Conformance Report Jobs, on page 35](#)
- [Run a Fleet Upgrade, on page 37](#)
- [Monitor Fleet Upgrade Jobs, on page 39](#)

Onboard Devices

Before you can test devices for compliance with software image standards, or upgrade them, the devices must be part of your device inventory. Follow the steps below to add devices one by one to your inventory, using the CWM user interface.

You can also add devices using the method in Import Devices in Bulk. You may also want to consider making a backup of your device information by following the steps in Export Devices.

Procedure

- Step 1** Log in to Crosswork Workflow Manager and, from the main menu, choose **Device Management** > **Network Devices**.

Onboard Devices

Network Devices Last update: 24-Mar-2025 03:34:19 PM PDT Refresh

Selected 0 / Total 4

	IP address	Host name	Admin state	NSO state	Lock status	Last updated time	Product type	Provider type
<input type="checkbox"/>	172.22.141.152/24	PE1-152	Up	Synced	Unlocked	09-Mar-2025 04:...	Cisco 8201 R...	NSO
<input type="checkbox"/>	172.22.142.94/24	ncs5501-94	Up	Synced	Unlocked	11-Mar-2025 12:4...	Cisco NCS 55...	NSO
<input type="checkbox"/>	172.22.142.137/24	r9-asr9-142-...	Up	Synced	Unlocked	14-Mar-2025 03:...	Cisco ASR 10...	NSO
<input type="checkbox"/>	172.22.142.134/24	ASR1002-X-1...	Up	Synced	Unlocked	19-Mar-2025 09:...	Cisco ASR 10...	NSO

Step 2 Click the  icon to display the **Add New Device** window.

← Network Devices

Add New Device

Device Info

Admin state *

Host name *

Software type *

Software version

UUID

[Other device settings](#)

Connectivity details

Credential profile *

Protocol *	Device IP *	Port *
<input type="text" value="SSH"/>	<input type="text" value="000.000.000.000"/>	<input type="text" value="/ 00 22"/>
<input type="text" value=""/>	<input type="text" value="000.000.000.000"/>	<input type="text" value="/ 00"/>
<input type="text" value=""/>	<input type="text" value="000.000.000.000"/>	<input type="text" value="/ 00"/>

[+ Add another](#)

Providers and access

Providers family	Provider name	Credential	Device key	NED ID
<input type="text" value="NSO"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Location

Building

Street

City

State

Country

Region

Zip

Latitude


Longitude

Altitude

[Add device](#) [Cancel](#)

Step 3 Enter the required values for the new device, as listed in the table below. The **Add device** device button is disabled until all required fields are completed.

Table 3: Add New Device (*=Required)

Field	Description
Device info Provide basic device information.	
Admin state *	The management state of the device. Options are: <ul style="list-style-type: none"> • DOWN—The device is not being managed and is down. • UP—The device is being managed and is up.
Host name *	The hostname of the device.
Software type *	Enter the software type of the device (such as <code>IOS-XE</code>).
Software version	Software version of the operating system.
UUID	Universally unique identifier (UUID) for the device.
Connectivity details Provide basic connectivity information.	
Credential profile *	The name of the credential profile to be used to access the device for data collection and configuration changes. For example: <code>nso-51</code> .
Protocol *	The connectivity protocols used by the device. Choices are: SSH , NETCONF , and HTTP . To add more connectivity protocols for this device, click + Add another at the end of the last row in the Connectivity Details panel. To delete a protocol you have entered, click  shown next to that row in the panel. You can enter as many sets of connectivity details as you want, but only one set for each protocol. You must enter details for at least SSH and HTTP .
Device IP *	Enter the device's IP address (IPv4 or IPv6) and subnet mask. Please ensure that the subnets chosen for the IP networks (including devices and destinations) do not have overlapping address space (subnets/supernets) as it may result in unpredictable connectivity issues.
* Port	The port used for this connectivity protocol. Each protocol is mapped to a port, so be sure to enter the port number that corresponds to the protocol you chose. The standard port assignments for each protocol are: <ul style="list-style-type: none"> • SSH: 22 • NETCONF: 830 • HTTP: 80

Field	Description
Timeout (sec)	The elapsed time (in seconds) before communication attempts using this protocol will time out. The default value is 30 seconds. For XE devices using NETCONF, the recommended minimum timeout value is 90 seconds. For all other devices and protocols, the recommended minimum timeout value is 60 seconds.
Providers and access Give information about the access provider.	
Providers family	Provider type used for topology computation. Choose a provider from the list (the default is NSO and should be the only option).
Provider name	Provider name used for topology computation. Choose a provider from the list.
Credential	The credential profile used for the provider. This field is read-only and is autopopulated based on the provider you select.
Device key	The host name used for the provider.
NED ID	The ID of the Cisco NSO Network Element Driver (NED) used to manage the device. For example: <code>cisco-iosxr-cli-7.61.</code>
Location Provide location information for the device.	
Building	The name or number of the building where the device is located
Street	The street address where the device is located.
City	The name of the city where the device is located.
State	The name of the state, district or province where the device is located.
Country	The name of the nation or country where the device is located.
Region	Where applicable, the name of the geographical region where the device is located.
Zip	The zip or postal code of the device location.
Latitude	The geographical latitude of the device location, entered in Decimal Degrees (DD) format.
Longitude	The geographical longitude of the device location, entered in Decimal Degrees (DD) format.
Altitude	The altitude at which the device is located, in feet or meters. For example, 123m .

Step 4 When you are finished, click **Add device**.

Step 5 (Optional) Repeat steps 3 and 4 to add another device.

What to do next

Follow the steps in [Populate the Image Repository](#), on page 29.

Populate the Image Repository

Before you use Fleet Upgrade to standardize, test conformance, and upgrade the images installed on your network devices, you must first populate the local software image repository with the images you need. Follow these steps to populate the repository.

Before you begin

CWM Solutions provides a local software image repository that you can use to set up policies that establish your software-image standards. You can then use the same repository to test whether your devices are in conformance with those standards, and deploy software images and upgrades to your managed devices. You can browse, choose and automatically download SMUs to the local repository directly from Cisco.com, using your Cisco customer login. You can also upload software images to the repository.

Fleet Upgrade image repository downloading is not yet available for Cisco ISO network operating system files, or the network OS files offered by supported third parties. For this reason, Cisco recommends that you download network OS files in advance, so that they are ready for upload to the Fleet Upgrade repository when you follow the steps in this topic.



Note

To reduce your internet visibility, you can configure Fleet Upgrade to download SMUs from Cisco.com using a proxy server. For details, see [Download Software Upgrades Using a Proxy Server](#).

Procedure

- Step 1** From the main menu, choose **CWM Solutions > Image Repository**. The **Fleet Upgrade** window's **Image repository** tab displays the list of ISOs and SMUs loaded to the local image repository.

Image name	Vendor	Software type	Product series	Image version	Functional area	Actions
asr1000-universalk9.17.09.04a.1	Cisco Systems	IOS XE	ASR1000	17.09.04a		...
asr1000-universalk9.17.09.04a.1	Cisco Systems	IOS XE	ASR1000	17.09.04a		...
asr1000-universalk9.17.09.04a.1	Cisco Systems	IOS XE	ASR1000	17.09.04a		...
asr1000-universalk9.17.09.04a.1	Cisco Systems	IOS XE	ASR1000	17.09.04a		...
asr1000-universalk9.17.09.04a.1	Cisco Systems	IOS XE	ASR1000	17.09.04a		...
asr1000-universalk9.17.09.05.C	Cisco Systems	IOS XE	ASR1000	17.09.05		...

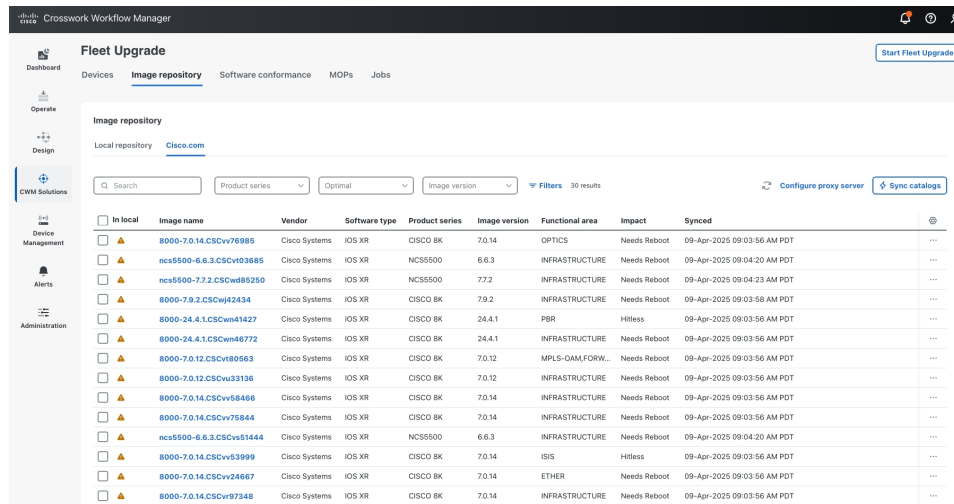
- Step 2** There are two ways to load images into the local repository:

Populate the Image Repository

- If you want to load Cisco SMUs, go to Step 3.
- If you want to load Cisco or third-party network OS software images you have previously downloaded, go to Step 4.

Step 3 To load Cisco SMUs:

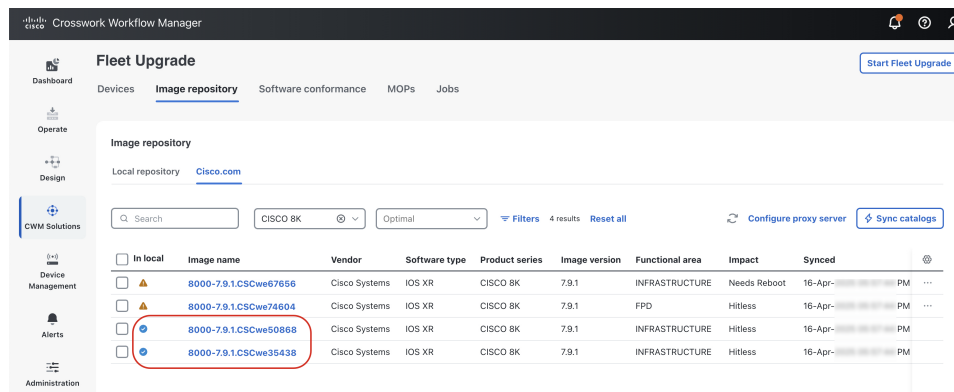
- a) Click the **Cisco.com** tab. The window's **Image repository** section now displays the catalog of all SMUs available from the Cisco.com software image download site.

**Tip**

Cisco releases many new SMUs each quarter. Use the **Filters** button to limit the display to the SMUs of interest to you. If you don't see the ones you want, or the timestamps shown under **Synced** are more than three months old, click **Sync catalogs** to update the list.

- b) Choose one or more of the SMUs you want to download by clicking the checkboxes shown next to each SMU image's name in the far left column.

A blue check mark shown next to the SMU image's name under the **In local** column (circled in the image below) indicates that the image is already in the local repository. You need not select it and try to download it again.



- c) To begin the download, click the **More** icon (...) in the far right column in the same row as any of the SMUs you chose.

- d) Choose **Download to local**. You will be shown a list of the SMUs you chose and a device activation code. Click **Authenticate to download**, and log in with the activation code. Record the activation code and follow the instructions on your device for the next steps.

Step 4

To load Cisco or third-party network OS software images you have previously downloaded:

- a) Click **Upload image**.
 b) Complete the fields on the **Upload Image** window as shown in the following table (the **Vendor** and **Image File Name** are required):

In this field...	Enter or choose:
Vendor *	Cisco or Juniper .
Software Type *	If Vendor is Cisco, IOS XR or IOS XE . If Vendor is Juniper, MX 960 .
Product Series *	A supported Product Series for the chosen Vendor and Software Type (for example, "CAT2000" for Cisco IOS XE).
Functional area (optional)	A description of the OS functional area affected by the upgrade (such as: "ACL" or "Infrastructure").
Impact (optional)	A description of the operational impact of the upgrade installation (such as: "Requires reboot" or "Hitless").
Choose image file *	The path and filename of (or click Browse to choose) the software image file to be uploaded

- c) When you are finished, click **Upload image**.

What to do next

Follow the steps in [Create Image Policies, on page 31](#).

Create Image Policies

Software image policies are a critical part of the Fleet Upgrade workflow. Whenever you create a software image policy, you choose one or more software image versions stored in your local repository, making them part of that image policy. Choosing them establishes those images as the standards that are supposed to be installed on your devices. As different types of devices run different types of software images, you'll need to establish image policies for each type of device. Whenever you run a Fleet Upgrade conformance report against a particular type of device, you will also need to pick the appropriate image policy for that device type. The Fleet Upgrade workflow will then check the software actually installed on those devices against the standard image established in the policy. If the installed and standard image versions don't match, then the device is non-conformant.

Note that Fleet Upgrade will rate as conformant only those devices that have *all* the chosen target images and image versions in the image policy installed at the time you run the conformance report. If you run a conformance report against a device that does not have one or more of the policy's images or versions installed, the report will rate that device as non-conformant.

Before you begin

Ensure you have downloaded one or more SMUs and network OS software images to your local CWM Solutions image repository, as explained in [Populate the Image Repository, on page 29](#).

Procedure

Step 1 From the main menu, choose **CWM Solutions > Software conformance > Image policies**

Step 2 Click + **Add image policy** to display the **New image policy** window.

The screenshot shows the 'New image policy' window in the Cisco Crosswork Workflow Manager. The window has a sidebar with navigation options: Dashboard, Operate, Design, CWM Solutions (selected), Device Management, Alerts, and Administration. The main content area is titled 'New image policy' and contains the following fields:

- Policy name ***: CAT 8K Basic Edge
- Description**: Basic setup for CAT 8K Edge routers
- Vendor ***: Cisco Systems
- Product series ***: CISCO 8K
- Target version ***: 24.2.11
- Software packages**: + Add

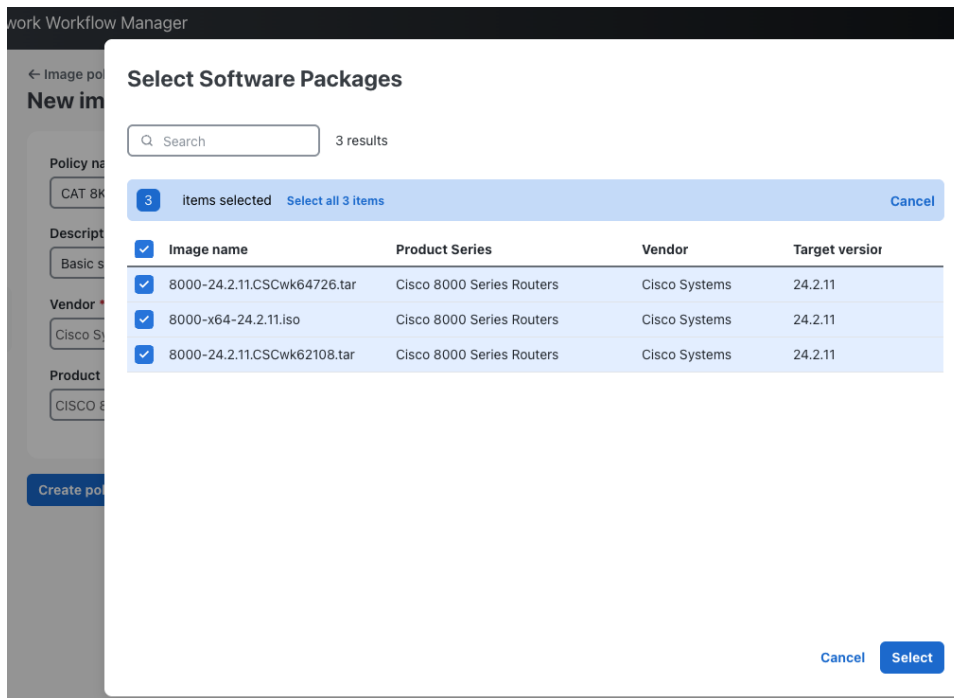
At the bottom of the form, there are 'Create policy' and 'Cancel' buttons.

Step 3 Complete the first five fields in the **New image policy** window as shown in the following table:

In this field...	Enter or choose...
Policy name	A unique name for the image policy, such as ASR1KSMU .
Description	An optional description of the policy's purpose, such as Standard minimum SMU level for all Cisco ASR 1000 routers .
Vendor	The name of the software vendor, such as Cisco Systems .
Product series	The network device product series, such as the Cisco ASR1000 .
Target version	The target version of the product series, such as 17.09.04a for the Cisco ASR1000 (supported target versions are pre-selected for you based on the target version).

Step 4 In the **Software packages** field, click the + **Add** button. The **Select Software Packages** window lists all the software images downloaded to your local repository that can be installed on the network device product series you specified.

Step 5 Click the check box next to the **Image name** of each software image you want to make part of this image policy.

**Step 6**

When you are finished selecting software images, click **Select**. You can continue revising your entries as needed, or click + **Add** again to change your software image selections. When you are finished, click **Create policy** to save the new policy.

What to do next

Follow the steps in [Run a Policy Conformance Report, on page 33](#)

Run a Policy Conformance Report

Use the policy conformance report to determine when you need to perform a Fleet Upgrade on one or more of your network devices.

You can create Fleet Upgrade conformance reports to check software image conformance for any device type and any combination of software images and versions. The core of the report is the software image policy you choose. The software image policy specifies the standard software images your devices should have installed on them. In addition, you can choose to run Fleet Upgrade conformance reports against devices on demand, at a future date or time you choose, or at regular recurring intervals. Each time the report runs, it will compare the software image installed on the devices with the software images specified in the image policy. The report will identify as "conformant" every device with all the policy's images installed. The report will flag as "non-conformant" any devices missing one or more of the policy images.



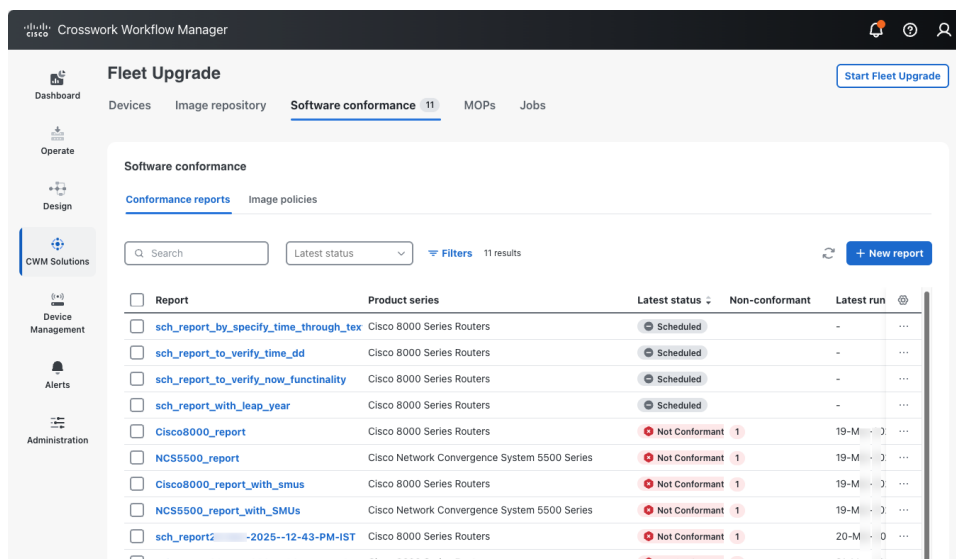
Tip You may find that the image policy that forms the basis of the conformance report you ran is out of date or otherwise incorrect. If that's the case, you can easily edit the policy and then run the report again. To edit an existing image policy, select **CWM Solutions > Fleet Upgrade > Software Conformance > Image policies** to display the list of image policies. Scroll or use **Search** to find the policy you want, then click the **More (...)** menu at the far right in the same row and select **Edit**.

Before you begin

Ensure you have created one or more software image policies, as explained in [Create Image Policies, on page 31](#).

Procedure

Step 1 From the main menu, select **CWM Solutions > Fleet Upgrade > Software conformance > Conformance reports**. The **Conformance reports** tab displays the status of all completed software conformance reports, as shown in the figure below.



Step 2 Click **+ New report**.

Step 3 Complete the first five fields in the **New image policy** window as shown in the following table:

In this field...	Enter or select...
Report name	A unique name for the conformance report, such as ASR1KStandard .
Select image policy	An optional description of the policy's purpose, such as Cisco ASR 1000 edge router SMU status .
Current version	The device software version number, such as 24.2.2 .

In this field...	Enter or select...
Run schedule	<p>One of the following:</p> <ul style="list-style-type: none"> • Run now. • Schedule for specific data and time. If you select this option, you must also specify a Time and Date. • Run recurring report. If you select this option, you must also specify an Interval between runs, or the Days of the week or Days of the month you want the recurring report to run on.

Step 4 When you are finished, click **Create Report** to save the new report. If you selected **Run now**, you will also run the new report.

Clicking **Create Report** will return you to the **Conformance reports** tab, where you can review the status of any report you have already run.

What to do next

If you're still viewing the results of a report and you see non-conforming devices, consider running a Fleet Upgrade using the steps in [Run a Fleet Upgrade, on page 37](#).

If your conformance report failed, investigate by following the steps in [Monitor Conformance Report Jobs, on page 35](#).

Monitor Conformance Report Jobs

Use the **Conformance reports** tab to monitor the results of a conformance report, including any failures that occur. The status details for failures will help you diagnose the cause and correct it.

Procedure

Step 1 Choose **CWM Solutions > Software Conformance > Conformance reports**

Step 2 Click the **Latest status** column header to sort the column alphabetically. Reports with "Conformant" and "Failed" results will be sorted like those shown in the following figure.

Monitor Conformance Report Jobs

Report	Product series	Latest status	Non-conformant	Latest run
sch_report13-Feb-2025--07-25-PM-IST	Cisco 8000 Series Routers	Conformant		14-Feb-2025 04:00:02 AM PST
sch_report13-Feb-2025--07-28-PM-IST	Cisco 8000 Series Routers	Conformant		14-Feb-2025 04:00:02 AM PST
ncs5500	Cisco Network Convergence System 5500 Series	Conformant		13-Feb-2025 02:51:15 PM PST
ncs55000	Cisco Network Convergence System 5500 Series	Conformant		13-Feb-2025 02:51:15 PM PST
Sample14	Cisco Network Convergence System 5500 Series	Conformant		14-Feb-2025 09:31:01 AM PST
NCS5500_report	Cisco Network Convergence System 5500 Series	Failed		13-Feb-2025 05:37:14 AM PST
MX960_Juniper	Juniper Networks Inc. mx960 Intern	Failed		13-Feb-2025 05:38:02 AM PST
ASR9K_report_with_smus	Cisco ASR 9000 Series Aggregation Services Routers	Failed		13-Feb-2025 05:39:03 AM PST
NCS540_report_with_SMUs	Cisco Network Convergence System 540 Series Routers	Failed		13-Feb-2025 05:41:31 AM PST
NCS540L_report_with_SMUs	Cisco Network Convergence System 540L Series Rout...	Failed		13-Feb-2025 05:42:37 AM PST
NCS5500_report_with_SMUs	Cisco Network Convergence System 5500 Series	Failed		13-Feb-2025 05:43:42 AM PST
CAT	Cisco Catalyst 8000V Edge Chassis Platforms	Failed		13-Feb-2025 08:54:05 AM PST
CAT8000V_report	Cisco Catalyst 8000V Edge Chassis Platforms	Failed		13-Feb-2025 10:06:36 PM PST

Step 3

For any report that failed: Click the **Report** name. CWM displays a detail screen like the one shown below, giving the reason for the report failure. In this example, no existing devices were specified, so there was nothing against which to compare the software image policy. You can easily correct this by ensuring that the next run includes devices.

Software Conformance
NCS540_report_with_SMUs Failed 13-Feb-2025 05:41:31 AM PST

[Edit report](#) [Export to CSV](#) [Run instantly](#)

The report has failed
 Device count should not be 0, report status marked failed

Details

Image policy	NCS540_policy	Vendor	Cisco Systems
Latest run	13-Feb-2025 05:41:31 AM PST	Product series	Cisco Network Convergence System 540 Series Routers
Next run	-	Current version	-
Software packages	ncs540-7.8.2.C5Cwc96475.tar		

Device results

0 Not Conformant Failed 0 Conformant Conformant

Q Search 0 results [Show only non-conformant](#)

Device	Status	Product series	Diff
0 results			

Tip

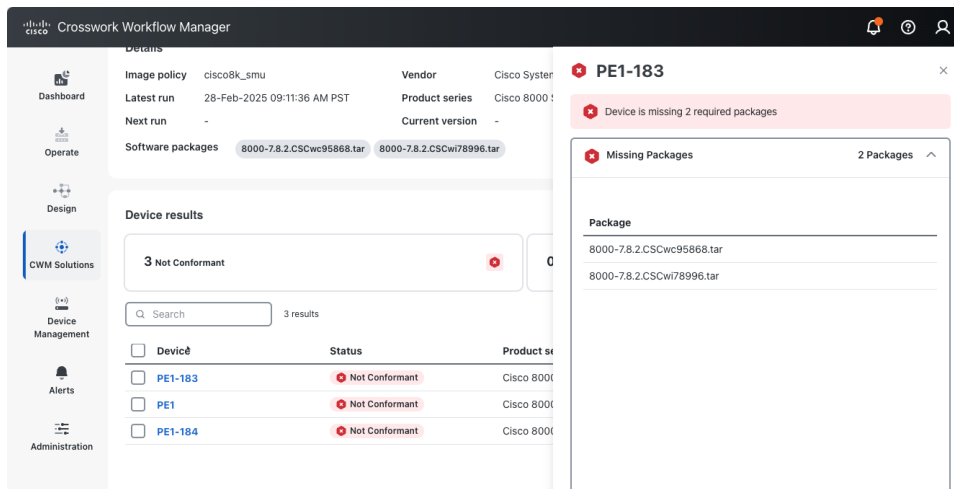
For any software conformance report whose details you're viewing:

- Click on the dropdown date field to see details for other runs of the same report.
- Click **Edit report** to change the report settings and re-run or re-schedule it.
- Click **Export to CSV** to save the report as a CSV file in your default downloads directory.
- Click **Run instantly** to re-run the report immediately with the same settings as before.

Step 4

For any report showing non-conformant devices: Click the **Report** name. CWM displays a detail screen like the one shown below, listing the non-conformant devices. If needed, click the **Device** name to see details for each non-conforming device. In this example, the first of the three devices was missing both of the required software packages.

Any non-conforming device will also be identified as non-conformant on the **Fleet Upgrade > Devices** page.



Run a Fleet Upgrade

Fleet Upgrade uses Methods Of Procedure (MOPs) to perform automated device upgrades. The definition of "MOP" varies from one industry to another, but "MOP" as used here refers to a set of pre-programmed CWM workflow Actions that are performed in sequenced phases. Each Action in the MOP is selected and (where needed) customized to deliver a complete, successful upgrade for the combination of software image and device for which it is intended. Fleet Upgrade provides default MOPs for the devices and software it supports, as well as facilities for creating custom versions of the default MOPs, and entirely new MOPs with mixtures of default and new Actions. At runtime, you have the opportunity to select which MOP your Fleet Upgrade job will use, as well as customizing other variables (such as the job name and the execution schedule). For more on these topics, see [Use the Default MOPs](#) and [Create Custom MOPs](#).

Before you begin

The easiest way to run a Fleet Upgrade is, first, to run a conformance report, as explained in [Run a Policy Conformance Report, on page 33](#), and then select the non-conforming device and click **Start Fleet Upgrade**. Running the conformance report first not only ensures that the Fleet Upgrade is really needed, it also lets you launch the upgrade automatically.

The steps below assume that you will want to launch a Fleet Upgrade from the **Software conformance > Conformance report** window. But you can also launch an upgrade by clicking the **Start Fleet Upgrade** button on any of the other **Fleet Upgrade** windows where it appears: **Devices**, **Image repository > Local repository**, **Image repository > Cisco.com Software conformance > Image policies**, **MOPs**, and **Jobs**,

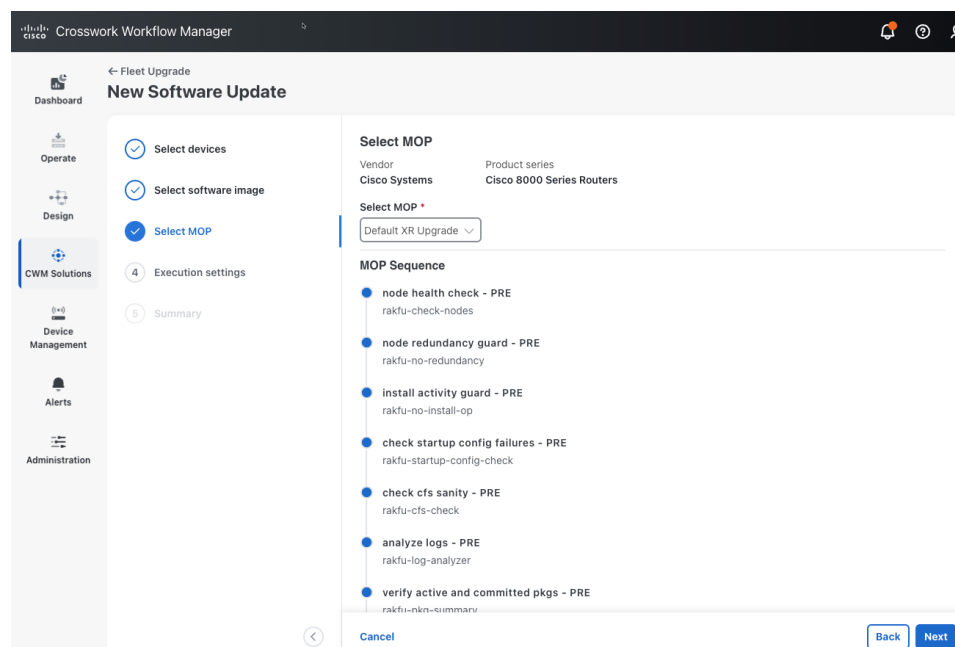
Procedure

Step 1

Choose **CWM Solutions > Software conformance** to display the **Conformance reports** list. The list should show a **Report** with one or more devices with a **Latest status** that is **Not Conformant**.

- Step 2** Click the selection checkbox shown next to the name of the **Report**. Click **Start Fleet Upgrade**. The **New Software Update** window displays a list of all the devices that were checked for conformance. The non-conformant devices are already selected for you.
- Step 3** For each additional device you want Fleet Upgrade to update, click the check box shown next to the device **Host name**. Or click the check box shown next to the **Host name** column title to select all of them.
- You can select a maximum of 50 devices to be upgraded in the same Fleet Upgrade job.
- Step 4** Click **Next** to display the **Select software image** window. If the software image policy you used to create the conformance report specified a target version and software packages, the list of software packages to be installed on the devices will be pre-selected for you.
- Step 5** If the image policy did not specify packages, or you want to install more packages, click **+Add**, then click the check box shown next to each package's **Image name**. Then click **Select** to display the list of all packages to be installed.
- Step 6** Click **Next** to display the **Select MOP** window.
- Step 7** Click the **Select MOP** drop down list to select the MOP you want to use to install the chosen software packages on the selected devices.

The drop down list will always display one or more MOPs pre-selected for the type of device series you are trying to upgrade. Unless you have a special purpose in mind, use the pre-defined MOPs supplied with Fleet Upgrade, such as the **Default XR Upgrade** MOP shown in the following figure.



- Step 8** Click **Next** to display the **Execution settings** window.
- Step 9** Complete the fields in the **Execution settings** window as shown in the following table:

In this field...	Enter or select...
Job name	A unique name for the job, such as ASR1KStandard .
Job tags	An optional, comma-separated list of search tags to help you find the job in the job listing, ASR1000 , ASRUpdates .

In this field...	Enter or select...
Parallel upgrades	Specify the number of device upgrades to be executed at the same time, in parallel. Defaults to 1. For help with setting this and the Acceptable failures value, see Use Parallel Upgrades with Acceptable Failures.
Acceptable failures	Specify the number of installation failures to be allowed before further upgrades are canceled. Defaults to 1.
Execution time	Specify one of the following: <ul style="list-style-type: none"> • Run now. CMW Solutions will begin executing the upgrade as soon as you click Submit. • Schedule for specific data and time. If you select this option, you must also specify a Time and Date.

Step 10 Click **Next** to display the **Summary** window.

Step 11 When you are finished, make sure the confirmation checkbox is selected. Then click **Submit** to save the new update job and either schedule or (if you selected **Run now**) run it.

What to do next

Follow the steps in [Monitor Fleet Upgrade Jobs, on page 39](#).

Monitor Fleet Upgrade Jobs

Use the Fleet Upgrade **Jobs** page to monitor the results of a Fleet Upgrade, including any failures that occur. The status details for failures will help you diagnose the cause and correct it.

Procedure

Step 1 Choose **CWM Solutions > Fleet Upgrade > Jobs**

Step 2 Click the **Status** column header to sort the column alphabetically. Upgrade jobs will be sorted like those shown in the following figure.

Monitor Fleet Upgrade Jobs

Fleet Upgrade

Jobs

1 Success 1 Failed 0 Running 0 Scheduled

Q Search Application group Filters 2 results

Job name	Status	Application group	Mop	Devices	Job tags	End time
New782Upgrade	Failed	Fleet Upgrade	Default XR Upgrade	1	782 NewUpgrade	24-Feb-
asr9k_multi_smu_4_156	Success	Fleet Upgrade	asr9k_mop	1	156	21-Feb-

Step 3 Click the **Job name** for a job that failed. CWM displays a **Job Summary** page like the one shown below. Under **Device results**, the page lists the **Host name** of the device where the update failed and the **Last finished stage** where the failure occurred.

New782Upgrade Failed 782 NewUpgrade

The job has failed. Please reconfigure your setting and create a new job.

Job summary

Status: Failed Application group: Fleet Upgrade MOP: Default XR Upgrade Update stages: PRE DISTRIBUTE ACTIVATE COMMIT POST

Start time: 24-Feb- 10:41:49 AM End time: 24-Feb- 10:52:10 AM Devices: 1

Update to: 8000-7.8.2.CSCwd71524.tar

Device results

0 Success 1 Failed 0 Running 0 Pending

Q Search 1 result

Result	Host name	Product series	Last finished stage	Start time
Failed	PE1-152	Cisco 8000 Series Routers	ACTIVATE	24-Feb- 10:42:02 AM

Step 4 Click the **Host name** to display a pop up screen with tabs representing the stages of the upgrade. As we can see in the example below, all the pre-checks passed.

Crosswork Workflow Manager

← Jobs **New782Upgrade** Failed 782 NewUpgrade

The job has failed. Please reconfigure your setting and click the **Retry** button.

Job summary

Status: Failed Application group: Fleet Upgrade

Start time: 24-Feb 10:41:49 AM End time: 24-Feb 10:42:57 AM

Update to: 8000-7.8.2.CSCwd71524.tar

Device results

0 Success 1 Failed

Q Search 1 result

Result	Host name	Product series
Failed	PE1-152	Cisco 8000 Series Routers

PE1-152 Cisco 8000 Series Routers

Pre Distribute **Activate**

Start time: 24-Feb 10:42:02 AM End time: 24-Feb 10:42:57 AM

- node health check
- node redundancy guard
- install activity guard
- check startup config failures
- check cfs sanity
- analyze logs
- verify active and committed pkgs
- capture package summary
- device snapshot

Step 5

Click the tab for the stage where the upgrade failed (in this example, **Activate**), and expand the tab as needed to display further detail. In this example, it appears the upgrade could not be activated due to a problem with two of the Field Programmable Devices (FPDs) in this release.

Crosswork Workflow Manager

← Jobs **New782Upgrade** Failed 782 NewUpgrade

The job has failed. Please reconfigure your setting and click the **Retry** button.

Job summary

Status: Failed Application group: Fleet Upgrade

Start time: 24-Feb 10:41:49 AM End time: 24-Feb 10:42:57 AM

Update to: 8000-7.8.2.CSCwd71524.tar

Device results

0 Success 1 Failed

Q Search 1 result

Result	Host name	Product series
Failed	PE1-152	Cisco 8000 Series Routers

PE1-152 Cisco 8000 Series Routers

Pre Distribute **Activate**

Start time: 24-Feb 10:44:04 AM End time: 24-Feb 10:52:10 AM

activate image

Performing FPDs Upgrade on the device - FPDs upgrade success except for the following FPDs : PO-PrimMCU,PO-PrimMCU

