Upgrade

This section contains the following topics:

- Upgrade Cisco Crosswork Change Automation and Health Insights, on page 1
- Upgrade Cisco Crosswork Data Gateway, on page 14
- Crosswork Patch Framework, on page 14

Upgrade Cisco Crosswork Change Automation and Health Insights

This section explains the migration procedure from Cisco Crosswork Network Automation VM version 3.0 to version 3.1. The Cisco Crosswork Network Automation VM is referring to the common product suite name and VM where you will be installing Cisco Crosswork Change Automation and Health Insights. One of the primary changes in the version 3.1 is the collection mechanism. The collection architecture used in version 3.0 has been changed to independent and scalable Crosswork Data Gateway VMs in version 3.1.

The upgrade process retains the following:

- User uploaded inventory (devices, providers, credential profiles, and tags).
- Platform details (database credentials).
- User configurations (Playbooks, Topology).
- Cisco Crosswork Network Automation VM version 3.0 settings for any rollback scenario.

Note Consider the following inventory changes in Cisco Crosswork Network Automation VM version 3.1:

- CSV file template has been updated in Cisco Crosswork Network Automation VM version 3.1. Make sure to use the latest template for managing inventory.
- Configured state of devices being onboarded needs to be marked as DOWN.

Limitations:

- The data from Cisco Crosswork Change Automation and Health Insights version 3.0 applications (Change Automation, Health Insights, Topology) cannot be migrated, as the schema has been updated in the version 3.1.
- AAA remote authentication server settings, custom local users and custom roles are not retained in the migration from Cisco Crosswork Change Automation and Health Insights version 3.0 to version 3.1.

Note The upgrade process for Cisco Crosswork Network Automation VM requires two instances (old and new) to exist at the same time. As a result you should plan to have resources (storage, disk and memory) within your data center (even if only temporarily) to support two VMs.

Before you begin, ensure that:

- You meet the system requirements to install Cisco Crosswork Change Automation and Health Insights and Cisco Crosswork Data Gateway. For more information, see Install Cisco Crosswork Change Automation and Health Insights Via vCenter and Install Cisco Crosswork Data Gateway.
- You have details of the Cisco Crosswork Network Automation VM version 3.0 including the Management IPv4 address, username and password.
- You have a public IP address (IPv4 or IPv6) to assign to the Cisco Crosswork Network Automation VM version 3.1 management network virtual interface. This can be a temporary address if you wish to retain the Management IPv4 address from Cisco Crosswork Network Automation VM version 3.0.

  Note It is preferred that the DNS and NTP servers are reachable via the Management Network Interface. However, it is not mandatory. The only requirement is that they are reachable on one of the network interfaces connected to the server.

- You have a public or private IP address (IPv4 or IPv6) to assign to the Cisco Crosswork Network Automation VM's data network virtual interface. This IP address must be able to reach your managed devices, and be reachable by Cisco Network Services Orchestrator.
- The Cisco Network Services Orchestrator (NSO) is migrated to the supported version (version 5.2).

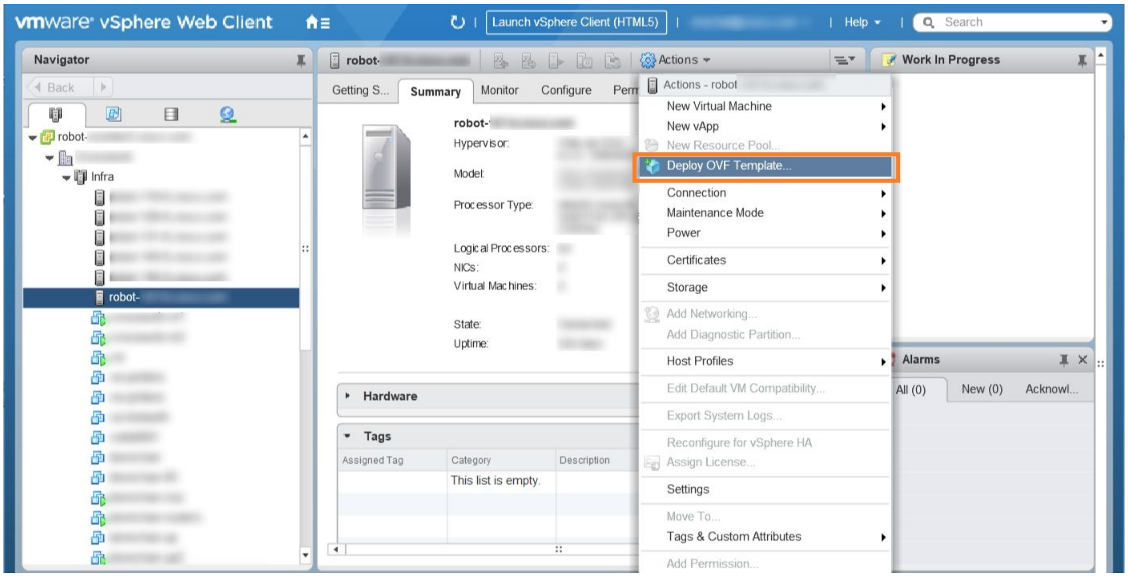
Note Before upgrading, it is recommended to move the Cisco Crosswork Network Automation VM version 3.0 to maintenance mode.

Note VMware vCenter supports vSphere Web Client (flash mode) and vSphere Client (HTML5 mode), however vSphere Web Client (flash mode) is recommended for the Cisco Crosswork Network Automation VM deployment and is explained in this procedure. The vSphere Client (HTML5 mode) is supported only on VMware vCenter Server 6.7 Update 3b.

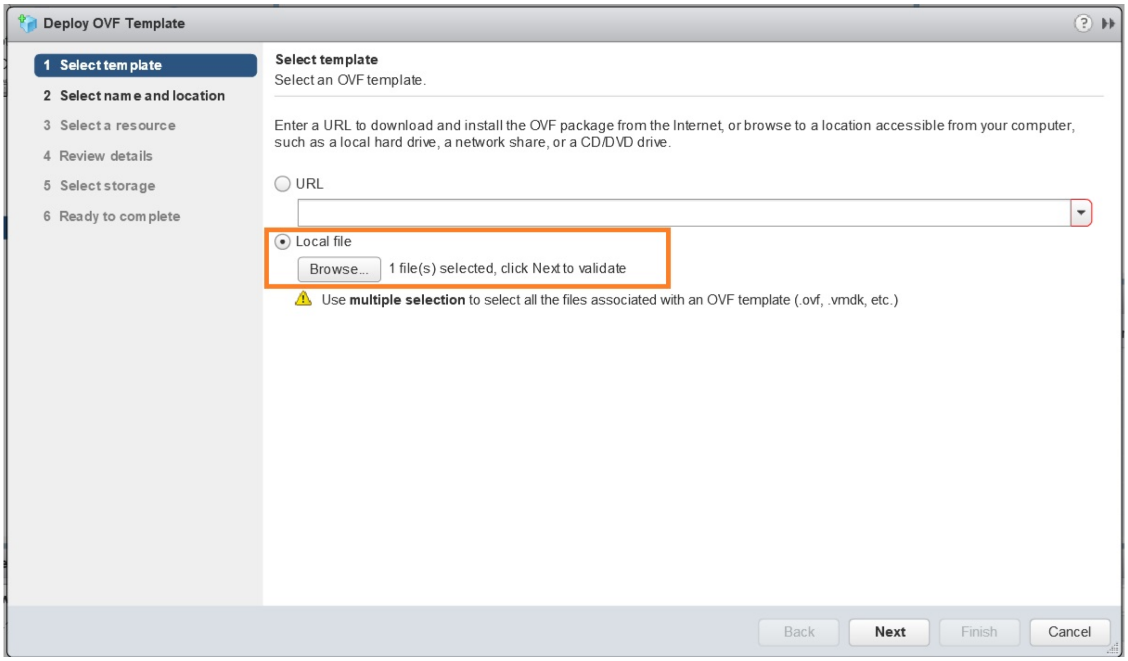
Step 1 Download the latest available Cisco Crosswork Change Automation and Health Insights image file (*.ova) to your system.

Warning The default VMware vCenter deployment timeout is 15 minutes. The total time needed to deploy the OVA image file may take much longer than 15 minutes, depending on your network speed and other factors. If vCenter times out during deployment, the resulting VM will be unbootable. To prevent this, Cisco recommends that you either set the vCenter deployment timeout to a much longer period (such as one hour), or unTAR the OVA file before continuing and then deploy using the OVA's three separate Open Virtualization Format and Virtual Machine Disk component files: `cw.ovf`, `cw_rootfs.vmdk`, and `cw_dockerfs`.vmdk.

Step 2 With VMware ESXi running, log in to the VMware vSphere Web Client. On the left side, choose the ESXi host on which you want to deploy the VM, then select **Actions** > **Deploy OVF Template**, as shown in the following figure.



Step 3 The VMware **Deploy OVF Template** wizard appears and highlights the first step, **1 - Select template**, as shown in the following figure. Click **Browse** to navigate to the location where you downloaded the OVA image file and select it. Once selected, the file name is displayed in the window.



Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete

Select template
Select an OVF template.

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

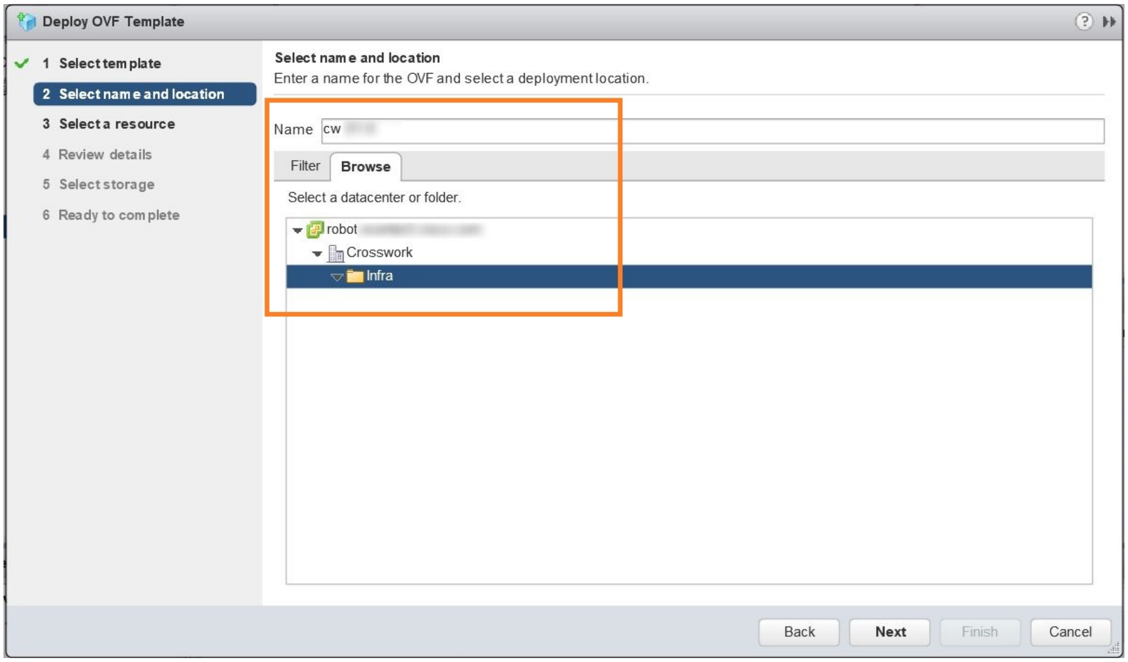
● Local file

Browse... 1 file(s) selected, click Next to validate

⚠ Use **multiple selection** to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

Step 4 Click **Next** to go to **2 - Select name and location**, as shown in the following figure. Enter a name for the Cisco Crosswork Network Automation VM you are creating.

Cisco recommends that you include the Cisco Crosswork Change Automation and Health Insights version and build number in the name (for example: `Crosswork CA/HI 3.1 Build 283`).



Deploy OVF Template

✓ 1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete

Select name and location
Enter a name for the OVF and select a deployment location.

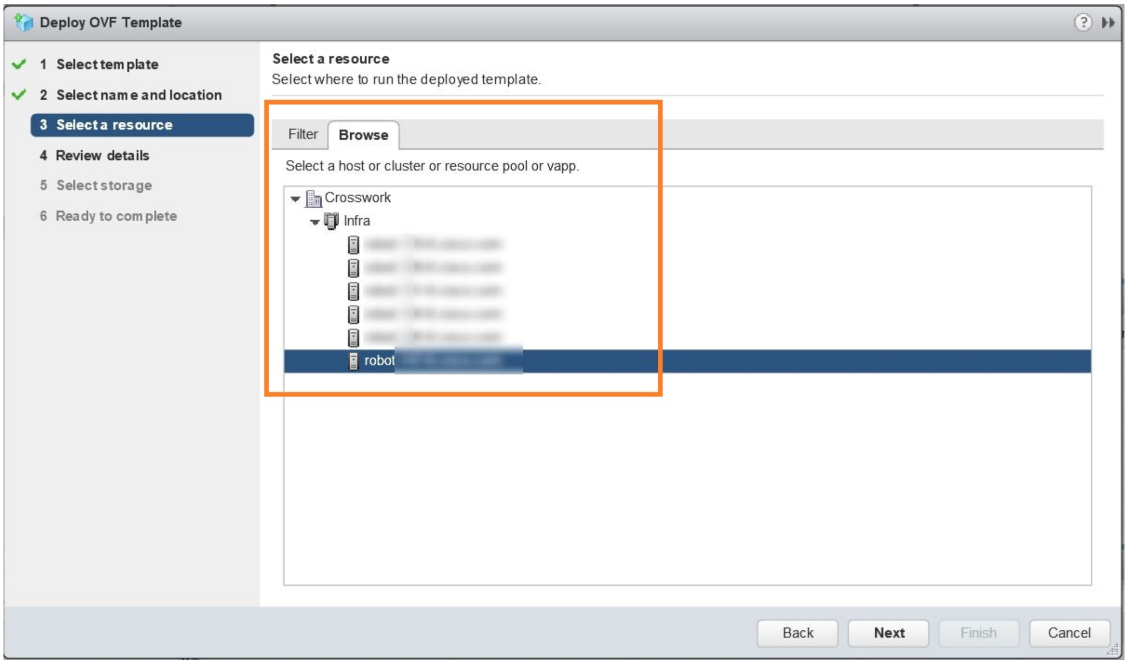
Name cw [redacted]

Filter Browse

Select a datacenter or folder.

robot [redacted]
Crosswork
Infra

Step 5 Click **Next** to go to **3 - Select a resource**, as shown in the following figure. Choose the Cisco Crosswork Network Automation VM's host.



Deploy OVF Template

✓ 1 Select template
✓ 2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete

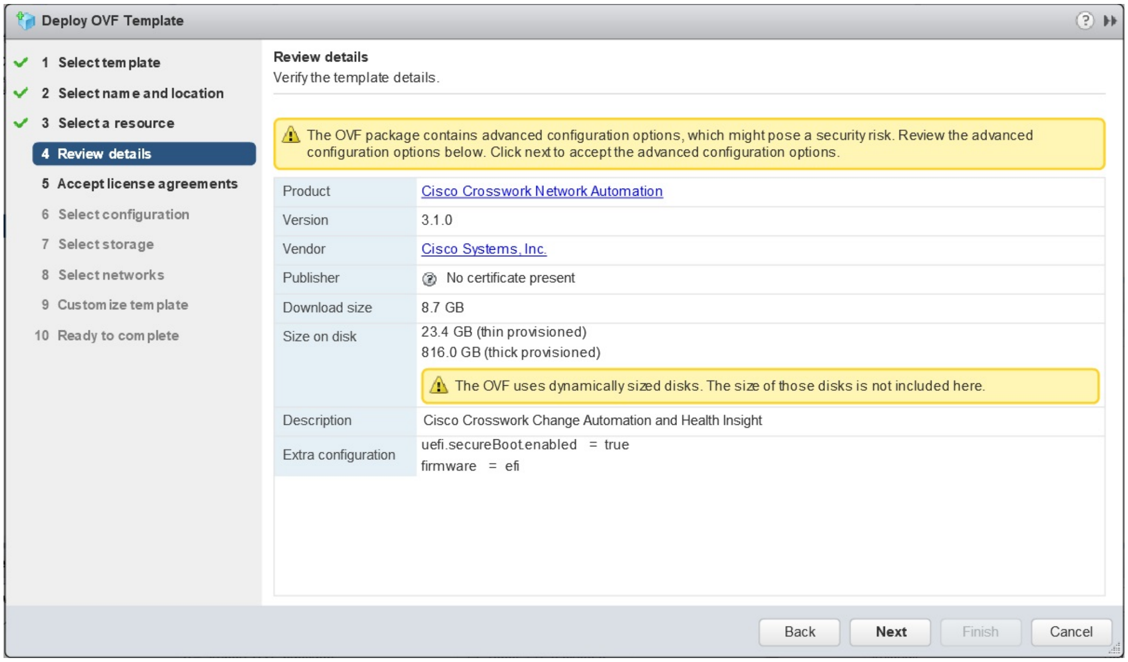
Select a resource
Select where to run the deployed template.

Filter | **Browse**

Select a host or cluster or resource pool or vapp.

- Crosswork
  - Infra
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - robot[redacted]

Step 6 Click **Next**. The VMware vCenter Server validates the OVA. Network speed will determine how long validation takes. When validation is complete, the wizard moves to **4 - Review details**, as shown in the following figure. Take a moment to review the OVF template you are deploying. Note that this information is gathered from the OVF and cannot be modified.



Deploy OVF Template

✓ 1 Select template
✓ 2 Select name and location
✓ 3 Select a resource
4 Review details
5 Accept license agreements
6 Select configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Review details
Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

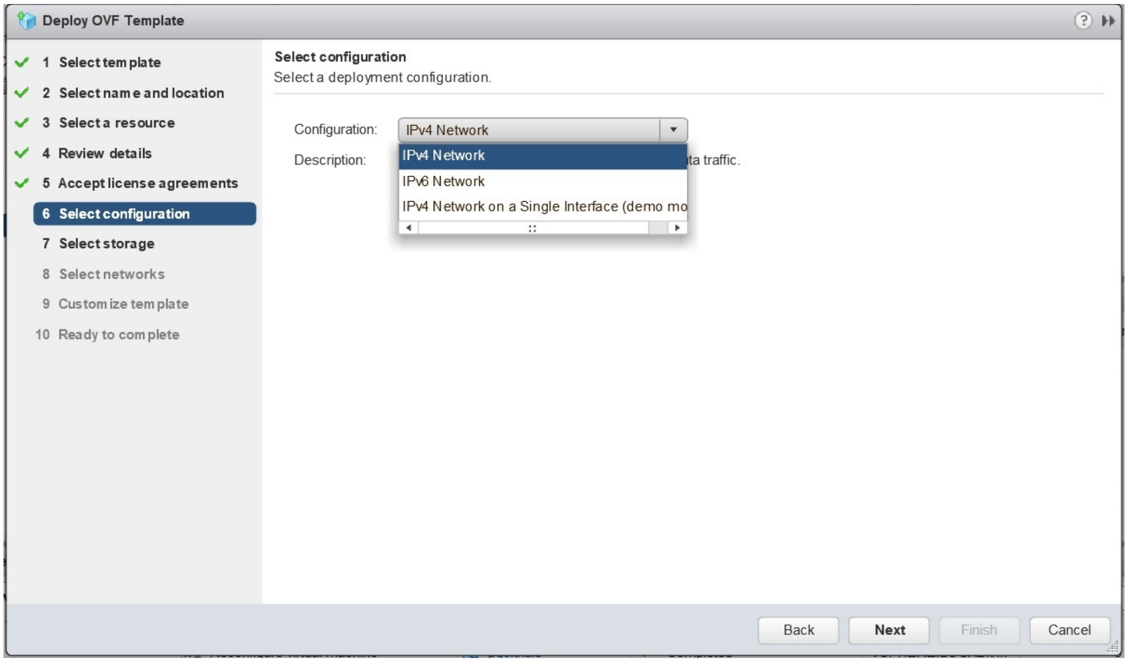
Product	Cisco Crosswork Network Automation
Version	3.1.0
Vendor	Cisco Systems, Inc.
Publisher	No certificate present
Download size	8.7 GB
Size on disk	23.4 GB (thin provisioned) 816.0 GB (thick provisioned) ⚠ The OVF uses dynamically sized disks. The size of those disks is not included here.
Description	Cisco Crosswork Change Automation and Health Insight

Extra configuration	uefi.secureBoot.enabled = true
	firmware = efi

Step 7 Click **Next** to go to **5 - Accept license agreements**. Review the End User License Agreement and click on **Accept** before you continue.

Step 8 Click **Next** to go to **6 - Select configuration**, as shown in the following figure. Select the desired deployment configuration (IPv4, IPv6 or IPv4 Network on a Single Interface).

Note As indicated, the IPv4 on a Single Interface should only be used for demonstrations and lab installations.



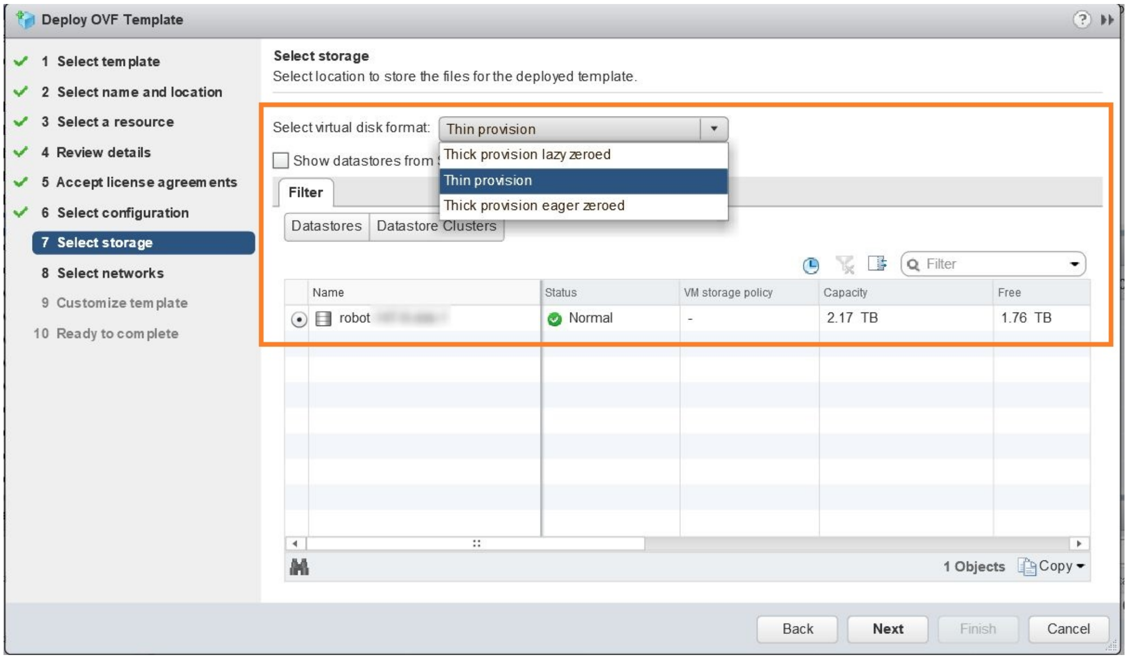
Select configuration
Select a deployment configuration.

Configuration: IPv4 Network

Description: ...ta traffic.

Step 9 Click **Next** to go to **7 - Select Storage**, as shown in the following figure. Select the relevant option from the **Select virtual disk format** drop-down list. From the table, choose the datastore you want to use and review its properties to ensure there is enough available storage.

Note For production deployment, consider choosing **Thick provision eager zeroed** as it will not have a penalty of allocating and initializing disk space at runtime. For development purposes, **Thin provision** is recommended as it saves disk space.



Select storage
Select location to store the files for the deployed template.

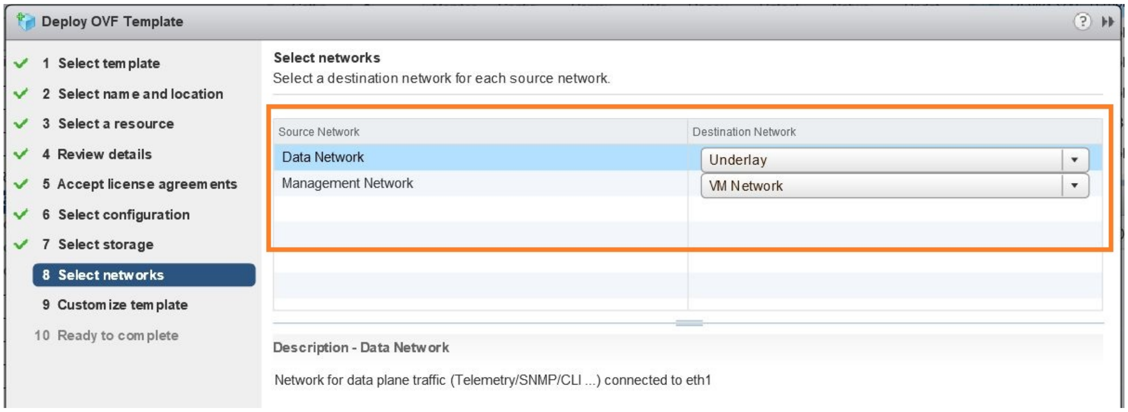
Select virtual disk format: Thin provision

□ Show datastores from ...

Name	Status	VM storage policy	Capacity	Free
○ robot [redacted]	Normal	-	2.17 TB	1.76 TB

1 Objects

Step 10 Click **Next** to go to **8 - Select networks**, as shown in the following figure. In the dropdown table at the top of the page, choose the appropriate destination network for the source **Data Network** and **Management Network**, respectively.



Select networks

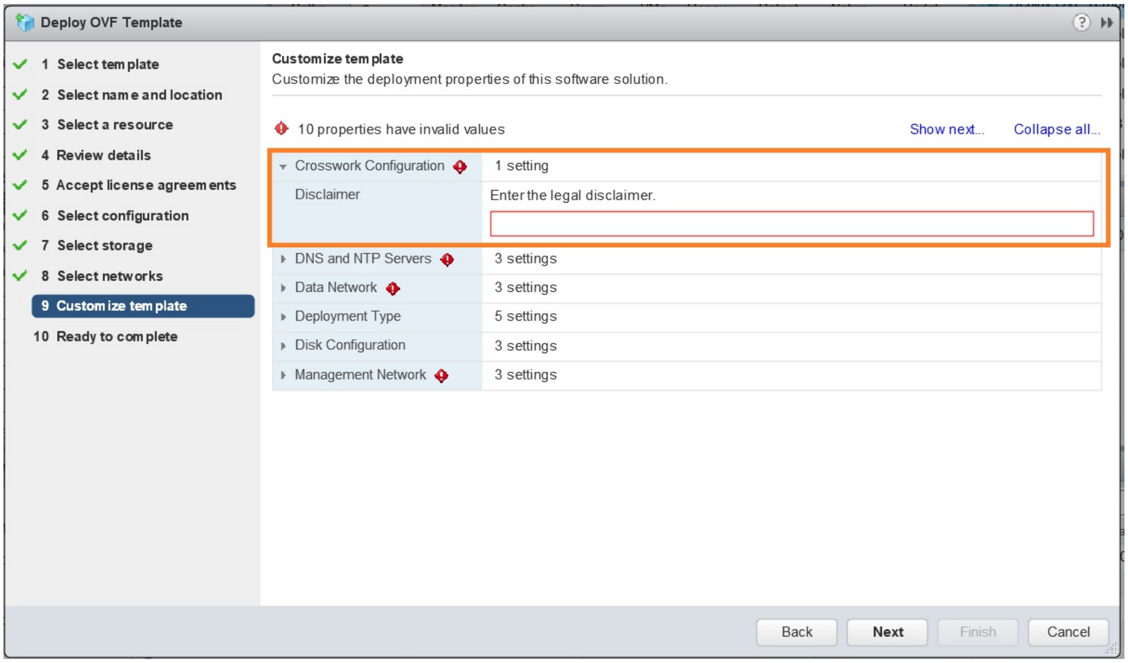
Select a destination network for each source network.

Source Network	Destination Network
Data Network	Underlay
Management Network	VM Network

Description - Data Network

Network for data plane traffic (Telemetry/SNMP/CLI ...) connected to eth1

Step 11 Click **Next** to go to **9 - Customize template**, with the **Crosswork Configuration** settings already expanded, as shown in the following figure. Make entry in the **Disclaimer** field.



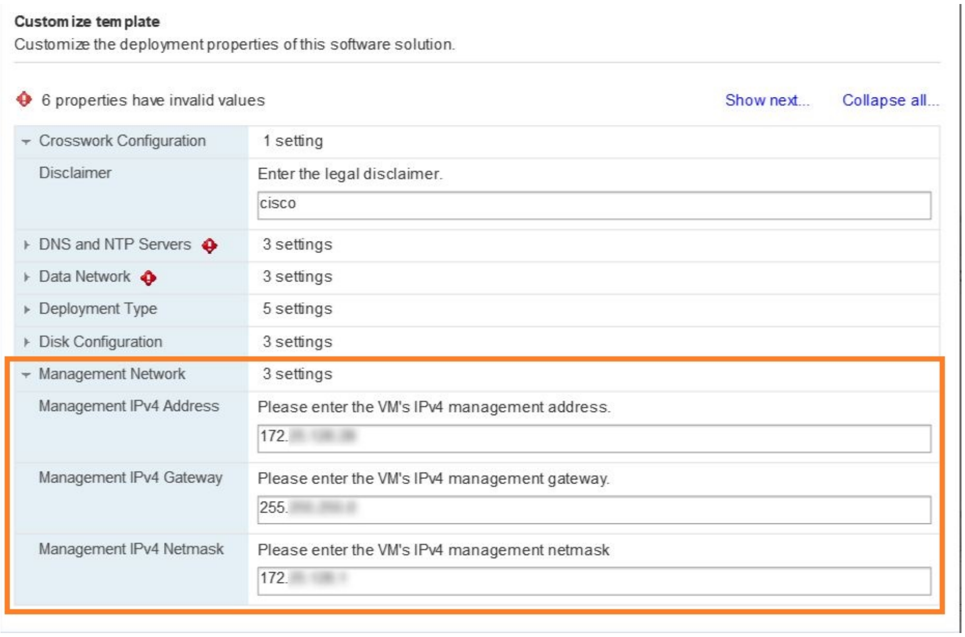
Customize template

Customize the deployment properties of this software solution.

10 properties have invalid values

Crosswork Configuration	1 setting
Disclaimer	Enter the legal disclaimer.
DNS and NTP Servers	3 settings
Data Network	3 settings
Deployment Type	5 settings
Disk Configuration	3 settings
Management Network	3 settings

Step 12 Expand the **Management Network** settings. According to your deployment configuration, the fields displayed are different. Enter the temporary IP address you want to be associated with the VM during the upgrade. If as part of the upgrade you want to keep this address associated with the VM you can select this option later in the upgrade process. See how to customize the template (step 11).

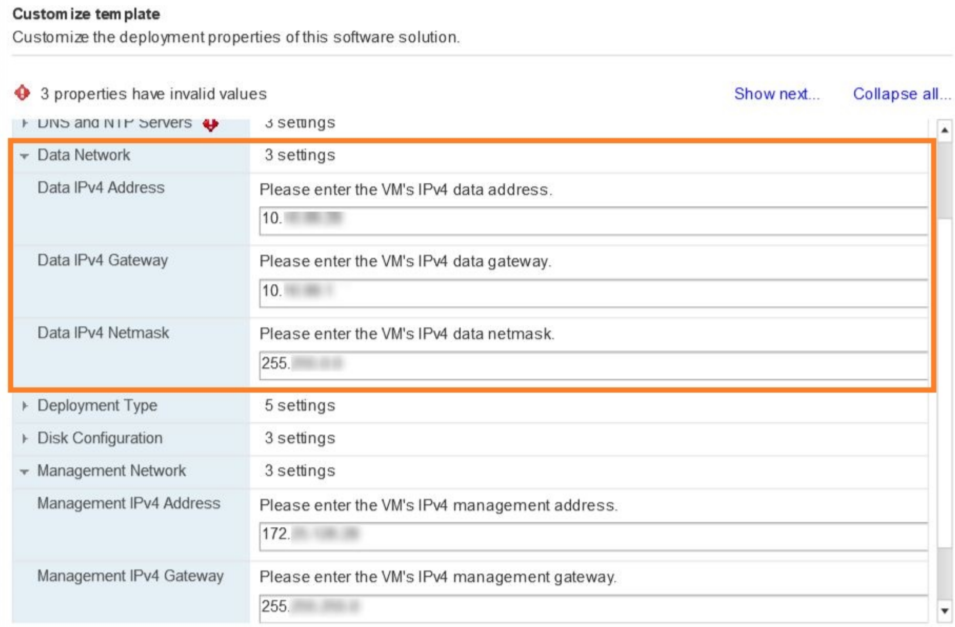


Customize template
Customize the deployment properties of this software solution.

6 properties have invalid values

Crosswork Configuration	1 setting
Disclaimer	Enter the legal disclaimer. cisco
DNS and NTP Servers	3 settings
Data Network	3 settings
Deployment Type	5 settings
Disk Configuration	3 settings
Management Network	3 settings
Management IPv4 Address	Please enter the VM's IPv4 management address. 172.[redacted]
Management IPv4 Gateway	Please enter the VM's IPv4 management gateway. 255.[redacted]
Management IPv4 Netmask	Please enter the VM's IPv4 management netmask 172.[redacted]

Step 13 Expand the **Data Network** settings. According to your deployment configuration, the fields displayed are different. Enter a temporary IP address and other information for the data network. If you want to change the IP to this value you can choose to do that in the customizing template section (step 11).



Customize template
Customize the deployment properties of this software solution.

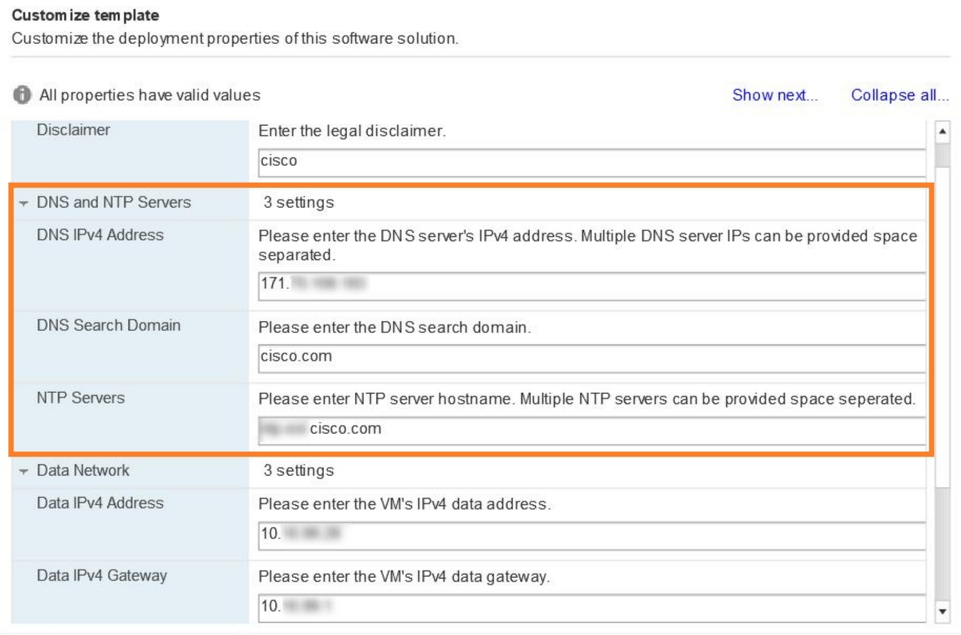
3 properties have invalid values

DNS and NTP Servers	3 settings
Data Network	3 settings
Data IPv4 Address	Please enter the VM's IPv4 data address. 10.[redacted]
Data IPv4 Gateway	Please enter the VM's IPv4 data gateway. 10.[redacted]
Data IPv4 Netmask	Please enter the VM's IPv4 data netmask. 255.[redacted]
Deployment Type	5 settings
Disk Configuration	3 settings
Management Network	3 settings
Management IPv4 Address	Please enter the VM's IPv4 management address. 172.[redacted]
Management IPv4 Gateway	Please enter the VM's IPv4 management gateway. 255.[redacted]

Step 14 Expand the **DNS and NTP Servers** settings, as shown in the following figure. According to your deployment configuration, the fields displayed are different. Make entries in three fields:

- **DNS IP Address**: The IP addresses (IPv4 or IPv6) of the DNS servers you want the Cisco Crosswork Change Automation and Health Insights server to use. Separate multiple IP addresses with spaces.
- **DNS Search Domain**: The name of the DNS search domain.

- **NTP Servers**: The IP addresses or host names of the NTP servers you want to use. Separate multiple IPs or host names with spaces.



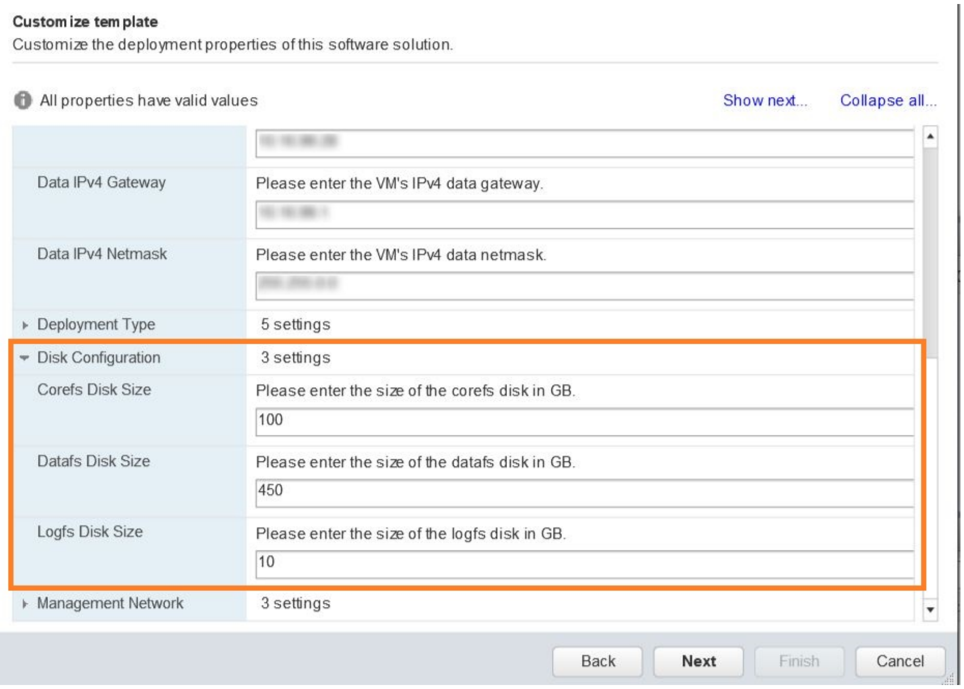
Customize template

Customize the deployment properties of this software solution.

All properties have valid values

Disclaimer	Enter the legal disclaimer. cisco
DNS and NTP Servers	3 settings
DNS IPv4 Address	Please enter the DNS server's IPv4 address. Multiple DNS server IPs can be provided space separated. 171.[redacted]
DNS Search Domain	Please enter the DNS search domain. cisco.com
NTP Servers	Please enter NTP server hostname. Multiple NTP servers can be provided space seperated. [redacted]cisco.com
Data Network	3 settings
Data IPv4 Address	Please enter the VM's IPv4 data address. 10.[redacted]
Data IPv4 Gateway	Please enter the VM's IPv4 data gateway. 10.[redacted]

Step 15 **Disk Configuration** settings allows you to adjust the amount of storage space available to Cisco Crosswork Change Automation and Health Insights. The default settings should work for most environments. For assistance in adding additional storage, contact the Cisco Customer Experience team.



Customize template

Customize the deployment properties of this software solution.

All properties have valid values

	[redacted]
Data IPv4 Gateway	Please enter the VM's IPv4 data gateway. [redacted]
Data IPv4 Netmask	Please enter the VM's IPv4 data netmask. [redacted]
Deployment Type	5 settings
Disk Configuration	3 settings
Corefs Disk Size	Please enter the size of the corefs disk in GB. 100
Datafs Disk Size	Please enter the size of the datafs disk in GB. 450
Logfs Disk Size	Please enter the size of the logfs disk in GB. 10
Management Network	3 settings

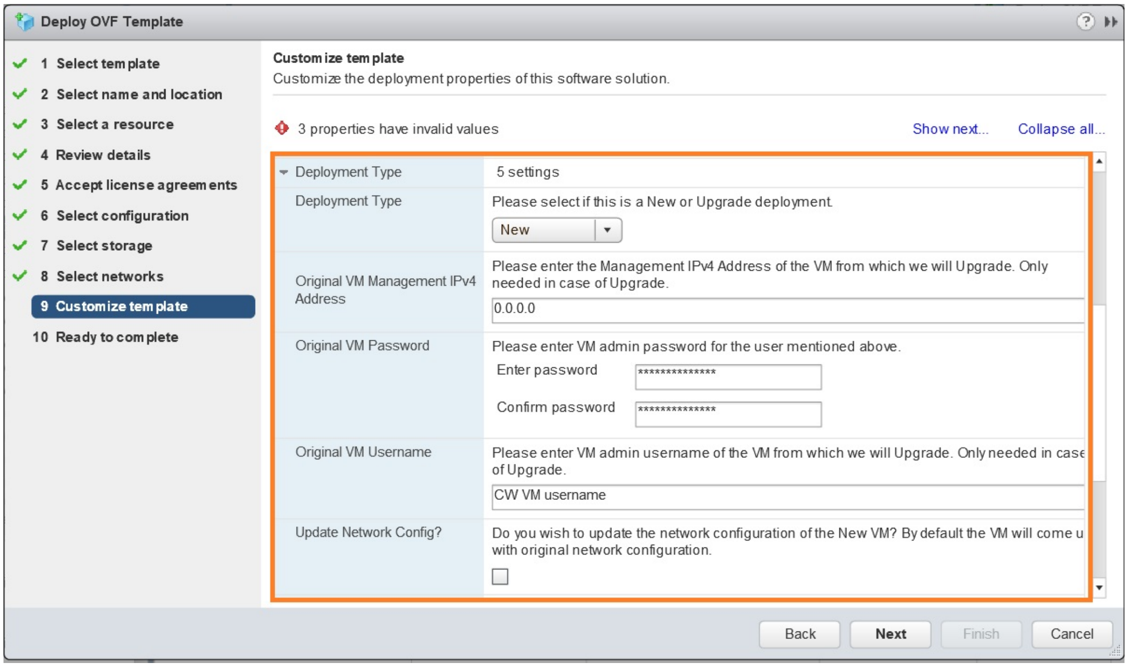
Step 16 Expand the **Deployment Type** settings, as shown in the following figure. In the **Deployment Type** dropdown, select **Upgrade**, and make relevant entries for the following fields:

a) **Original VM Management IPv4 Address**: Management IPv4 address of Cisco Crosswork Network Automation VM version 3.0.

b) **Original VM Password**: Provide the Cisco Crosswork Network Automation VM version 3.0 password in the **Enter Password** and **Confirm Password** fields.

c) **Original VM Username**: Username of Cisco Crosswork Network Automation VM version 3.0. Typically, it is `cw-admin` unless it has been changed by your system administrator.

d) **Update Network Config**: Leave the box unchecked if you want to retain the Management and Data network IP addresses assigned to the original VM. If you want to make the temporary IP addresses permanent, then check the box.



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- ✓ 5 Accept license agreements
- ✓ 6 Select configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- 9 Customize template
- 10 Ready to complete

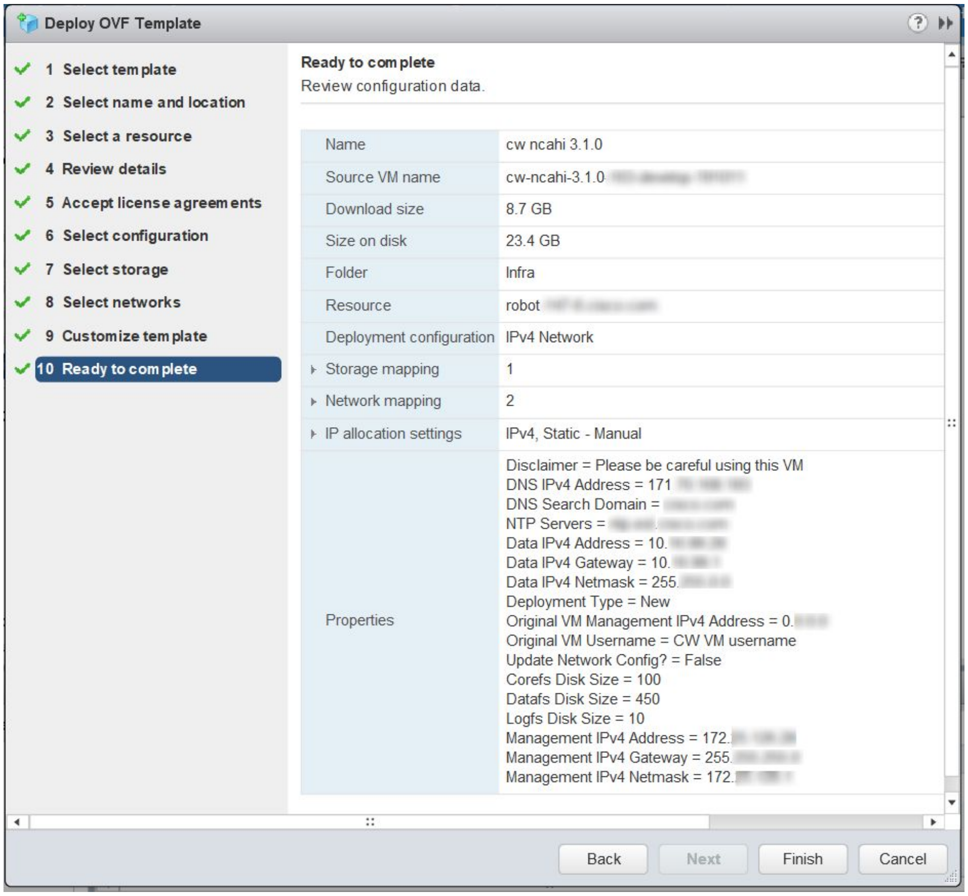
Customize template

Customize the deployment properties of this software solution.

3 properties have invalid values

Deployment Type	5 settings
Deployment Type	Please select if this is a New or Upgrade deployment. New
Original VM Management IPv4 Address	Please enter the Management IPv4 Address of the VM from which we will Upgrade. Only needed in case of Upgrade. 0.0.0.0
Original VM Password	Please enter VM admin password for the user mentioned above. Enter password ************** Confirm password **************
Original VM Username	Please enter VM admin username of the VM from which we will Upgrade. Only needed in case of Upgrade. CW VM username
Update Network Config?	Do you wish to update the network configuration of the New VM? By default the VM will come u with original network configuration. □

Step 17 Click **Next** to go to **10 - Ready to Complete**, as shown in the following figure. Review your settings and then click **Finish** if you are ready to begin deployment.



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- ✓ 5 Accept license agreements
- ✓ 6 Select configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- ✓ 9 Customize template
- ✓ 10 Ready to complete

Ready to complete

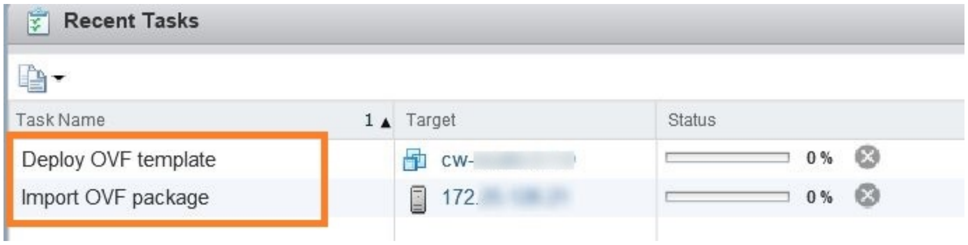
Review configuration data.

Name	cw ncahi 3.1.0
Source VM name	cw-ncahi-3.1.0 [redacted]
Download size	8.7 GB
Size on disk	23.4 GB
Folder	Infra
Resource	robot [redacted]
Deployment configuration	IPv4 Network
Storage mapping	1
Network mapping	2
IP allocation settings	IPv4, Static - Manual
Properties	Disclaimer = Please be careful using this VM DNS IPv4 Address = 171 [redacted] DNS Search Domain = [redacted] NTP Servers = [redacted] Data IPv4 Address = 10. [redacted] Data IPv4 Gateway = 10. [redacted] Data IPv4 Netmask = 255. [redacted] Deployment Type = New Original VM Management IPv4 Address = 0. [redacted] Original VM Username = CW VM username Update Network Config? = False Corefs Disk Size = 100 Datafs Disk Size = 450 Logfs Disk Size = 10 Management IPv4 Address = 172. [redacted] Management IPv4 Gateway = 255. [redacted] Management IPv4 Netmask = 172. [redacted]

Step 18 Wait for the deployment to finish before continuing. To check on the deployment status:

a) Open a VMware vCenter client.

b) In the **Recent Tasks** tab for the host VM, view the status for the **Deploy OVF template** and **Import OVF package** jobs, as shown in the following figure.

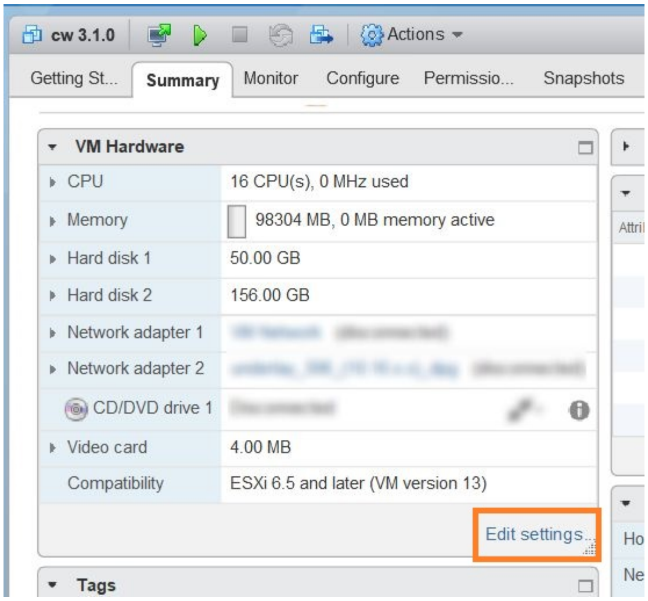


Recent Tasks

Task Name 1 ▲	Target	Status
Deploy OVF template	cw- [redacted]	0 %
Import OVF package	172. [redacted]	0 %

Step 19 After the deployment tasks are complete, check the host's VM settings to permit boot from EFI Firmware:

a) On the host VM **Summary** tab, below the **VM Hardware** table, click **Edit Settings**, as shown in the following figure.



VM Hardware

CPU	16 CPU(s), 0 MHz used
Memory	98304 MB, 0 MB memory active
Hard disk 1	50.00 GB
Hard disk 2	156.00 GB
Network adapter 1	[illegible]
Network adapter 2	[illegible]
CD/DVD drive 1	[illegible]
Video card	4.00 MB
Compatibility	ESXi 6.5 and later (VM version 13)

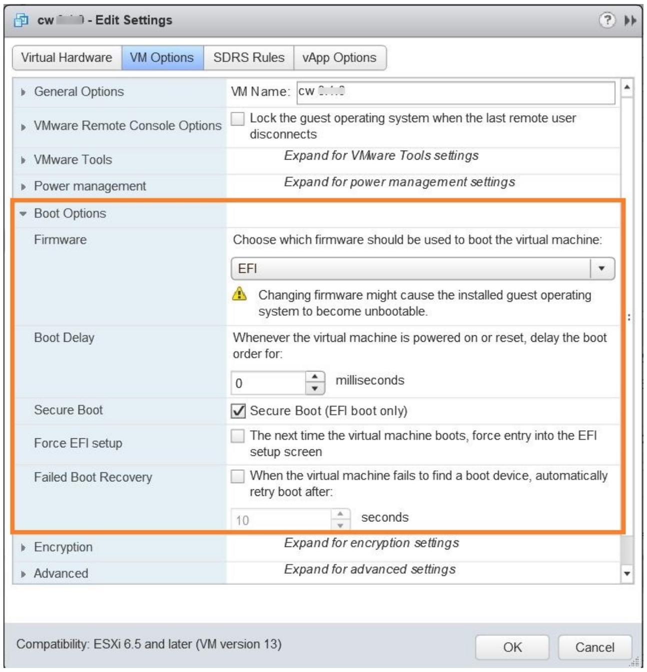
Edit settings...

Tags

b) On the **Edit Settings** page, click the **VM Options** tab.

c) Expand the **Boot Options** dropdown list and change the **Firmware** setting to **EFI**, if it not set by default. When you are finished, click **OK**. You may want to take a snapshot of the VM at this point.

Note **EFI** boot needs to be manually set when using VMware vCenter Server 6.7 (Update 1).

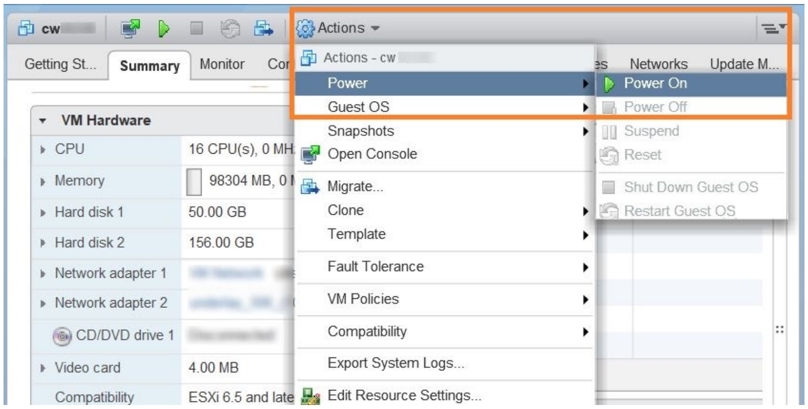


General Options	VM Name: cw [illegible]
VMware Remote Console Options	□ Lock the guest operating system when the last remote user disconnects
VMware Tools	*Expand for VMware Tools settings*
Power management	*Expand for power management settings*
Boot Options	
Firmware	Choose which firmware should be used to boot the virtual machine: EFI Changing firmware might cause the installed guest operating system to become unbootable.
Boot Delay	Whenever the virtual machine is powered on or reset, delay the boot order for: 0 milliseconds
Secure Boot	☑ Secure Boot (EFI boot only)
Force EFI setup	□ The next time the virtual machine boots, force entry into the EFI setup screen
Failed Boot Recovery	□ When the virtual machine fails to find a boot device, automatically retry boot after: 10 seconds
Encryption	*Expand for encryption settings*
Advanced	*Expand for advanced settings*

Compatibility: ESXi 6.5 and later (VM version 13)

Step 20 You can now power on the Cisco Crosswork Network Automation VM to complete the deployment process. Expand the host's entry so you can click the Cisco Crosswork Network Automation VM and then choose **Actions** > **Power** > **Power On**, as shown in the following figure.

Figure 1: Power On



From this point, the upgrade is automatically triggered. The Data and IP configurations are transferred from Cisco Crosswork Network Automation VM version 3.0 to version 3.1. Once the transfer is completed, Cisco Crosswork Network Automation VM version 3.0 will shut down. It will take 30 minutes or more for the Cisco Crosswork Network Automation VM version 3.1 to become operational. Please wait for the process to finish before continuing.

To get the current status of the upgrade, login as the super user and use the cli `upgrade status` command on the VM.

Note

- Each time the Cisco Crosswork Network Automation VM is re-imaged, you need to refresh the Cisco Crosswork Change Automation and Health Insights login page to accept the new certificate. Otherwise, the error message *Http failure response for /crosswork/sso/v1/tickets: 0 Unknown Error* is displayed on the login page.
- Each time the Cisco Crosswork Network Automation VM is re-imaged, Cisco Crosswork Data Gateway must be restarted to re-initialize the certificates. Otherwise, the devices become unreachable and collection stops.

Step 21 Install Cisco Crosswork Data Gateway and complete the post-installation tasks using the instructions in Install Cisco Crosswork Data Gateway and Post-installation Tasks respectively.

Step 22 Enroll the Cisco Crosswork Data Gateway with Cisco Crosswork Change Automation and Health Insights as instructed in Enroll Cisco Crosswork Data Gateway. For information on adding devices to the Cisco Crosswork Data Gateway, see the *Manage Crosswork Data Gateway Instances* section in the *Cisco Crosswork Change Automation and Health Insights User Guide*

Step 23

What to do next

- Verify that you are able to login to Cisco Crosswork Network Automation VM version 3.1 using the 3.0 credentials (**`cw-admin`** as username and password).
- Verify if the inventory data and application configurations from Cisco Crosswork Network Automation VM version 3.0 have been retained in version 3.1.
- Verify if the device details are visible in the Topology page.

- Check the health status of Cisco Crosswork Change Automation and Health Insights version 3.1 and Cisco Crosswork Data Gateway using the **Crosswork Manager** and **Data Gateway Management**windows in the UI respectively.

  For more information, see the *Perform Administrative Tasks* chapter in the *Cisco Crosswork Change Automation and Health Insights User Guide*.

- Check if you are able to configure and use the applications in Cisco Crosswork Change Automation and Health Insights version 3.1. For more information on the UI workflow, see the *Cisco Crosswork Change Automation and Health Insights User Guide*.

Upgrade Cisco Crosswork Data Gateway

Note This procedure is required only for a Cisco Crosswork Data Gateway Base VM upgrade. Upgrade of other components, such as collectors, is performed by Crosswork as explained is Section Crosswork Patch Framework, on page 14.

Cisco Crosswork Data Gateway functions as a passive device in the network. As such, the upgrade process consists of stopping the active Cisco Crosswork Data Gateway instance and replacing it with a Cisco Crosswork Data Gateway instance that is running the new version of Cisco Crosswork Data Gateway software, essentially exchanging one Cisco Crosswork Data Gateway instance for another.

Follow the below steps.

Step 1 Put the current Cisco Crosswork Data Gateway instance in maintenance mode.

Steps to put a Cisco Crosswork Data Gateway instance in maintenance mode are described in Section: **Change the Administration State of a Cisco Crosswork Data Gateway VM** of *Cisco Crosswork Change Automation and Health Insights 3.1 User Guide*.

Step 2 Deploy the new upgraded Cisco Crosswork Data Gateway instance. See Install Cisco Crosswork Data Gateway.

Step 3 Enroll the new Cisco Crosswork Data Gateway instance with Crosswork. See Enroll Cisco Crosswork Data Gateway With Cisco Crosswork Change Automation and Health Insights.

Step 4 Uninstall the old Cisco Crosswork Data Gateway instance.

Crosswork Patch Framework

There are three types of patches in Cisco Crosswork Change Automation and Health Insights:

- **Crosswork Application Patching (PATCH_IMAGE)**: This is a patch on the Crosswork applications such as Change Automation and Health Insights, and the configuration packages within the application layer. One or more applications can be patched simultaneously.
- **Crosswork Data Gateway Patching (PATCH_CDG)**: This is a patch on the collector images for Cisco Crosswork Data Gateway VM.

- **Crosswork Data Patching (PATCH_DATA)**: This is a patch to dynamically update the pre-built set of fundamental data such as YANG models and system MIB packages used by the Crosswork applications.

The patch versioning is done in the [MAJOR: MINOR: PATCH] format, where MAJOR corresponds to every major release of the Cisco Crosswork Change Automation and Health Insights, MINOR corresponds to every critical (backward incompatible) change made during a release, and PATCH corresponds to every patch created in a release.

The unit of a patch is a TAR file. The TAR file consists of the patch metadata, list of docker images, checksum and signature. The metadata contains platform and product details, patch version, type of patch and other creation details. Signature is a security requirement in order to safeguard the patch; the signature is verified by the patch framework. It also helps to perform error correction mechanisms and detect if the patch is corrupted or not.

The platform orchestrator (such as Robot orchestrator) maintains and manages the lifecycle of all applications in the Crosswork platform. Each Crosswork product has its own centralized manifest file `<orchmanifest.json>` which contains the list of applications and the corresponding configurations. When the orchestrator is up, it goes through the manifest. Along with the manifest, the dependency diagram `<orch.yaml>` explains the logical grouping of applications and their dependencies. Currently, simultaneous application patching is possible as the applications are independent of each other. Patching the Collection Infra is a system-wide change and requires shutting down other dependent applications. A patch on the Core Infra is not allowed and is considered as a VM upgrade. Schema changes are not allowed during patching. Users are recommended to take backup of the system before patching, to restore in case of any error.

Patching Activation workflow:

1. **Validate**
    - API: **/crosswork/platform/v1/patch/validate**
    - User downloads the patch to any reachable host from the Crosswork VM. After the download, the patch is validated for accuracy and compatibility to the product version.

2. **Add**
    - API: **/crosswork/platform/v1/patch/add**
    - After the patch is validated, it is added to the corresponding registry in the system, such as updating the IMAGE registry in case of an IMAGE patch. The *add* operation prepares the system for the patch to be activated. It is an asynchronous operation and may take around 15 mins. Once *add* is initiated, user receives a corresponding job ID and the operation is performed in the background.

3. **Status**
    - There are 2 status APIs:
    - *Status* - which displays the current status of the Patch framework.
        - API: **/crosswork/platform/v1/patch/status**
        - This API displays the current status of the patch framework, such as if *add* is successful or ongoing, or if *activate* has been triggered.
    - *Job Status* - which displays the specific job status.
        - API: **/crosswork/platform/v1/patch/jobstatus**

- This API return the status of a specific job based on the Job ID.

4. **Activate**
    - API: **/crosswork/platform/v1/patch/activate**
    - After successful addition, the patching is locked. If a patch is added, it needs to be activated before another patch can be added to the application. *Activate*, like *add*, is an asynchronous operation that generates a job ID for the user and continues the process in the background. Activation takes the backup of the current state and updates the configuration. If the patch fails, the auto-roll back functionality rolls back to the previous version and the status is updated with the failure details.

5. **Summary**
    - API: **/crosswork/platform/v1/patch/summary**
    - *Summary* provides the overall summary of the Patch framework, and summary of the different patch types including patch version. This information changes each time a new patch is added and activated:
        - PATCH_IMAGE - Patch version and the applications changed as part of the patch.
        - PATCH_CDG - Patch version
        - PATCH_DATA - Patch version and the applications to which the new data has been uploaded.

6. **Remove**
    - API: **/crosswork/platform/v1/patch/remove**
    - A patch can be removed in 2 ways:
        - Flow 1: A patch can be removed after it is validated and added. For example, if user chooses to cancels after the *add* is successful, *remove* can be used.
        - Flow 2: A patch can be removed after it is validated, added and activated. For example, if user chooses to go back to a previous version after a patch is applied successfully, *remove* can be used.

For more information, refer the Swagger file for Payload https://github3.cisco.com/ROBOT/k8s-orchestrator/blob/develop/robotctl_api/robotctl_api.swagger.json

Upon successful activation of a patch, user can verify the health of the application using the **Crosswork Manager** or **Data Gateway Management** feature in Cisco Crosswork Change Automation and Health Insights, depending on the type of the patch. For more information, see the *Perform Administrative Tasks* chapter in *Cisco Crosswork Change Automation and Health Insights User Guide*.