Prerequisites

Prerequisites for Upgrading

You must complete the system updates before you can perform package updates. Do not download or install any package updates until all system updates have been installed.

Important

- In a multihop upgrade, you must confirm that the applications have been updated successfully before you begin the next system update. If you skip to the next system update without first updating the applications, you will have to reimage your Cisco Catalyst Center appliance.
- If you are running Cisco DNA Center release 2.1.2.8 or earlier, you must first upgrade to 2.2.2.9 before you can upgrade to release 2.2.3.6 or later. Contact your Cisco sales representative if you need assistance.

Note the following points:

- You cannot upgrade the packages individually. You must follow all of the steps that are described in this guide.
- Before you upgrade, make sure that the cluster link interface is connected to a switch port and is in the up state. To confirm that the interface is up, complete these steps:
  1. In an SSH client, log in to Catalyst Center on your appliance.
  2. Enter the **ifconfig** *interface-name* command:
     - For a 44-core first-generation appliance (Cisco part number DN1-HW-APL), specify **enp10s0** as the interface name.
     - For a 44- or 56-core second-generation appliance (Cisco part number DN2-HW-APL or DN2-HW-APL-L), specify **enp94s0f1** as the interface name.
     - For a 112-core second-generation appliance (Cisco part number DN2-HW-APL-XL), specify **enp69s0f1** as the interface name.

3. In the resulting output, check the last line and verify that data has been received and transmitted. Nonzero values indicate that the interface is up and operational.

Review the following list of prerequisites before upgrading your installed instance of Catalyst Center:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see the *Cisco Catalyst Center Administrator Guide*.
- Create a backup of your Catalyst Center database. For more information, see the *Cisco Catalyst Center Administrator Guide*.
- If you have a firewall, allow Catalyst Center to access the following location on each node in your cluster for all system and package downloads: https://www.ciscoconnectdna.com:443. To ensure that you have cloud connectivity to AWS, log in to the cluster and enter the following CLI command: **maglev catalog settings validate**. For more information, see the Internet Connectivity Traffic table in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.
- While the Catalyst Center GUI is compatible with the following HTTPS-enabled browsers, we recommend that you use Chrome, not Firefox, during the upgrade:
  - Google Chrome: Version 93 or later (recommended for upgrade)
  - Mozilla Firefox: Version 92 or later (not recommended for upgrade)
- Have the username and password for a cisco.com user account available during the upgrade. You might be prompted, once, for the account credentials during package installations. This can be any valid cisco.com user account.
- Allocate enough time for the upgrade process. Upgrading can take longer than 6 hours to complete.
- We strongly recommend that you do not use Catalyst Center or any of its applications or tools while the upgrade is in process.
- Confirm that the minimum disk requirements are met:
  - The / partition has at least 2 GB of free space.
  - The /data partition has at least 35 GB of free space and is not more than 70% full.

  If you receive a `storage validations failed` error, contact the Cisco TAC.
- If the Catalyst Center download, update, or install procedures fail for any reason, always retry the procedure a second time using the GUI.
- If your environment uses Catalyst Center's disaster recovery implementation, see the "Implement Disaster Recovery" chapter in the *Cisco Catalyst Center Administrator Guide* for upgrade information specific to a disaster recovery setup.
- Before you upgrade your disaster recovery system or update your Cisco IMC firmware, first place your system on pause. For more information, see the "Pause Your Disaster Recovery System" section in the *Cisco Catalyst Center Administrator Guide*.

In a three-node cluster, you can trigger an upgrade of the entire cluster from the Catalyst Center GUI (the GUI represents the entire cluster and not just a single host). An upgrade triggered from the GUI automatically upgrades all hosts in the cluster.

Note To upgrade a three-node cluster, Service Distribution (or high availability) must be enabled.

Factors That Affect the Upgrade

Download Times for Upgrade

The download time for the Catalyst Center software upgrade, which is approximately 40 GB in size, depends significantly on your internet connection's bandwidth. The following table provides estimates of the expected download times based on various common bandwidth speeds.

These estimates are based on ideal conditions. Factors such as network congestion and connection stability can affect actual download times.

Bandwidth	Estimated Download Time
25 Mbps	3 hours, 38 minutes
50 Mbps	1 hour, 49 minutes
100 Mbps	54 minutes
200 Mbps	27 minutes

Connection Throttling

During the software upgrade process, many objects are downloaded. If a web security appliance is in place that limits connections based on various criteria, such as the total amount of data transferred within a specific period or the number of concurrent connections, this throttling can interrupt the download process, potentially leading to failure. To ensure a smooth software upgrade, we recommend that you configure exceptions for Catalyst Center traffic to prevent it from being throttled.

Proxy/Firewall

The proxy or firewall must allow the software management URLs that are listed in "Required Internet URLs and Fully Qualified Domain Names" in the *Cisco Catalyst Center Appliance Installation Guide*.

TLS Intercept Proxy

The TLS intercept proxy will disrupt the software download activity initiated by Catalyst Center if the TLS intercept proxy's certificate is not installed on Catalyst Center. To add the TLS intercept proxy certificate, see "Upload an SSL Intercept Proxy Certificate" in the *Cisco Catalyst Center Administrator Guide*.

Antimalware

The Catalyst Center software management system retrieves files from Cisco's connected catalog server and retrieves Docker images from a remote Docker registry. To prevent interruptions and failures in the software download process, the following compressed file formats must be excluded from antimalware scans.

Application Package Data

Files	content-type	content-encoding	Notes
tar.gz	application/x-compressed	gzip	Commonly used for compressed archives. Also seen as application/x-gzip or application/x-compressed.
.json	application/json	None	Text-based format for representing structured data. Typically UTF-8 encoded.

Docker Images

Component	File Extension	content-type	content-encoding
Docker image layers	.tar.gz	application/gzip	gzip
Docker image manifest	.json	application/json	None
Docker configuration object	.json	application/json	None
YAML configuration	.yaml/yml	text/yaml or application/x-yam	None
Docker image archive	.tar or .tar.gz	application/x-tar or application/gzip	None or gzip

Update the Cisco IMC Firmware

To update your Cisco IMC firmware, first see the release notes for the corresponding release of Catalyst Center that you are installing. In the release notes, the “Supported Firmware” section shows the Cisco IMC firmware version for your Catalyst Center release.

Then, see the *Cisco Host Upgrade Utility User Guide* for instructions on updating the firmware.

In a three-node cluster configuration, we recommend that you shut down all three nodes in the cluster before updating the Cisco IMC firmware. However, you can upgrade the cluster nodes individually if that's what you prefer. See “Typical Cluster Node Operations” in the *Cisco Catalyst Center High Availability Guide* and follow the steps provided to shut down one or all of the nodes for maintenance.

Supported Upgrade Paths for Hot Fixes

If your release is…	You can upgrade to…	Recommendation
2.3.5.5-HF20	2.3.7.5	
	2.3.7.4	
	2.3.5.6	Recommended for fixes

If your release is…	You can upgrade to…	Recommendation
• 2.3.5.5-HF12 • 2.3.5.5-HF11 • 2.3.5.5-HF10	2.3.7.5	Recommended for fixes
• 2.3.5.5-HF30 • 2.3.5.5-HF1	2.3.7.5	
	2.3.5.6	Recommended for fixes
• 2.3.5.4-70852-HF5 • 2.3.5.4-70852-HF4	2.3.7.5	
	2.3.7.4	
	2.3.5.6	Recommended for fixes
2.3.5.4-70852-HF3	2.3.7.5	
	2.3.7.4	
	2.3.7.3	
	2.3.5.6	Recommended for fixes
	2.3.5.5	
• 2.3.5.3-70194-HF5 • 2.3.5.3-70194-HF4 • 2.3.5.3-70194-HF3 • 2.3.5.3-70194-HF2 • 2.3.5.3-70194-HF1 • 2.3.5.3	2.3.7.5	
	2.3.7.4	
	2.3.7.3	
	2.3.5.6	Recommended for fixes
	2.3.5.5	
• 2.3.3.7-72328-HF6 • 2.3.3.7-72328-HF5 • 2.3.3.7-72328-HF4 • 2.3.3.7-72328-HF3 • 2.3.3.7-72328-HF2 • 2.3.3.7-72328-HF1 • 2.3.3.7	2.3.7.5	
	2.3.7.4	
	2.3.7.3	
	2.3.5.6	Recommended for fixes
	2.3.5.5	