Cisco Catalyst Center Standard Air Gap Deployment Guide

First Published: 2020-03-13

Last Modified: 2024-01-18

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

CONTENTS

CHAPTER 1

Introduction

About the Standard Air Gap Deployment

Catalyst Center supports offline software updates, allowing Catalyst Center appliances deployed in secure, air-gapped networks to be updated to the latest Catalyst Center software and application versions, without having to access the Cisco Connected DNA Cloud.

Note If you installed from an ISO image in an air-gapped environment, and you don’t need to update yet, you must still accept the end-user license agreement (EULA) as explained in this guide.

PART I

Standard Air Gap Deployment: 2.3.2.x, 2.3.3.x, or 2.3.4.x to 2.3.5.x

CHAPTER 2

2.3.2.x, 2.3.3.x, or 2.3.4.x to 2.3.5.x

Fresh Install from the Catalyst Center ISO Image

Offline Install Workflow

An offline Catalyst Center installation involves the following steps:

1. Download the image.
2. Verify the downloaded file.
3. Create a bootable USB drive.
4. Install the Catalyst Center ISO image.
5. Configure the Catalyst Center appliance.
6. Complete the first-time setup.
7. Accept the device EULA.
8. Install the applications.

Download the Image

You or your Cisco account representative must raise a TAC request. A TAC representative then gives you access and instructions for downloading the binary image from a Cisco file server.

Step 1 Log in to the Cisco file server, which is accessible via the internet.

Step 2 Download the Catalyst Center binary image (.bin) from the location specified.

Step 3 Download the Cisco public key (cisco_image_verification_key.pub) for signature verification.

Step 4 Download the secure hash algorithm (SHA512) checksum file for the image.

Step 5 Download the binary image's signature file (.sig).

Verify the Downloaded File

Verify the integrity of the downloaded image using Cisco signature verification and the SHA512 checksum provided on the portal.

Step 1 (Optional) Perform SHA verification to determine whether the binary image is corrupted due to a partial download.

Depending on your OS, enter one of the following commands:

- Linux:

```
sha512sum Catalyst-Center-image-filename
```

- Mac:

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows does not include a built-in checksum utility, but you can use the certutil tool:

```
certutil -hashfile <filename> sha256 | md5
```

For example:

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

On Windows, you can also use the Windows PowerShell to generate the digest. For example:

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

Compare the output of the command you run to the SHA512 checksum file that you downloaded. If the command output does not match, download the binary image again and run the appropriate command a second time. If the output still does not match, contact Cisco support.

Step 2 Verify that the binary image is genuine and from Cisco by verifying its signature:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
signature-filename Catalyst-Center-image-filename
```

This command works in both Mac and Linux environments. For Windows, you must download and install OpenSSL, if you haven’t done so already.

If the binary image is genuine, entering this command displays a **Verified OK** message. If this message fails to appear, do not install the binary image and contact Cisco support.

Create a Bootable USB Drive

After confirming that you downloaded a Cisco ISO image, create a bootable USB drive that contains the Catalyst Center ISO image. For details, see the "Create a Bootable USB Flash Drive" topic in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide's* "Prepare the Appliance for Configuration" chapter.

Install the Catalyst Center ISO Image

Step 1 Connect the bootable USB drive with the Catalyst Center ISO image to the appliance.

Step 2 Log in to Cisco IMC and start a KVM session.

Step 3 Power on or power cycle the appliance:

- If the appliance is not currently running, choose **Power** > **Power On System**.
- If the appliance is already running, choose **Power** > **Power Cycle System (cold boot)**.

Step 4 In the resulting pop-up window, click **Yes** to acknowledge that you are about to execute a server control action.

Step 5 When the Cisco logo appears, either press the **F6** key or choose **Macros** > **User Defined Macros** > **F6** from the KVM menu. The boot device selection menu appears.

Step 6 Select your USB drive and then press **Enter**.

Step 7 In the GNU GRUB bootloader window, choose **Cisco DNA Center Installer** and then press **Enter**.

Note The bootloader automatically boots the Maglev installer if you don't make a selection within 30 seconds.

Configure the Catalyst Center Appliance

When installation of the Catalyst Center ISO image completes, the installer reboots and opens the Maglev Configuration wizard's welcome screen. To configure your appliance for day-to-day use in your network, complete the steps described in one of the following sections:

- If you are using the Maglev Configuration wizard, see "Configure the Appliance Using the Maglev Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.
- If you are using the browser-based configuration wizard to configure a 44- or 56-core appliance, see "Configure the 44/56-Core Appliance Using the Browser-Based Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.
- If you are using the browser-based configuration wizard to configure a 112-core appliance, see "Configure the 112-Core Appliance Using the Browser-Based Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.

Complete the First-Time Setup

Step 1 After the Catalyst Center appliance reboot is completed, launch your browser.

Step 2 Enter the host IP address to access the Catalyst Center GUI, using HTTPS:// and the IP address of the Catalyst Center GUI that was displayed at the end of the configuration process.

After entering the IP address, one of the following messages appears (depending on your browser):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

Step 3 Ignore the message and click **Advanced**. One of the following messages appears:

- Google Chrome: `This server could not prove that it is` *`GUI-IP-address`*`; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.`
- Mozilla Firefox: `Someone could be trying to impersonate the site and you should not continue. Websites prove their identity via certificates. Firefox does not trust` *`GUI-IP-address`* `because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.`

These messages appear because the controller uses a self-signed certificate. For information on how Catalyst Center uses certificates, see the "Certificate and Private Key Support" section in the *Cisco Catalyst Center Administrator Guide*.

Step 4 Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to <*GUI-IP-address*> (unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

The Catalyst Center **Login** window appears.

Step 5 In the Login window, enter the admin's username (admin) and password that you set when you configured Catalyst Center, then click **Log In**.
The **Reset Login** window appears.

Step 6 Enter the old password, enter and confirm a new password for the admin superuser, and then click **Save**.
The **Enter Cisco.com ID** window appears.

Step 7 (*Skip this step*) Enter the username and password for the cisco.com user, then click **Next**. If the cisco.com user login does not match any known Cisco Smart Account user login, the **Smart Account** window appears.

Step 8 (*Skip this step*) If the **Smart Account** window appears, enter the username and password for your organization's Smart Account, or click the corresponding link to open a new Smart Account. After you are finished, click **Next**.
The **IP Address Manager** window appears.

Step 9 If your organization uses an external IP address manager (IPAM), do the following and then click **Next**:

- Enter your IPAM server's name and URL.
- Enter the username and password required for server access.
- Choose your IPAM provider (such as Infoblox).
- Choose the specific view of IP addresses available in the IPAM server database that you want Catalyst Center to use.

The **Enter Proxy Server** window appears.

Step 10 Click **Next**.
The software **EULA** window appears.

Step 11 Click **Next** to accept the software End User License Agreement and continue.
The **Ready to go!** window appears.

Step 12 We recommend that you click the **User Management** link to display the User Management window. Then click **Add** to begin adding new Catalyst Center users. After you have entered the new user's name and password, and selected the

user's role, click **Save** to create the new user. Repeat this as needed until you have added all the new users for your initial deployment. Be sure to create at least one user with the NETWORK-ADMIN-ROLE.

Accept the Device EULA

To complete the device EULA, complete the procedure specific to your Catalyst Center version:

- Cisco DNA Center 2.3.4.0 and Later, on page 9
- Cisco DNA Center 2.3.3.7 and Earlier, on page 9

Cisco DNA Center 2.3.4.0 and Later

To accept the device EULA, log in to your Catalyst Center cluster and run the following command: **maglev catalog airgap install /mnt/install-artifacts/eula/finalize_offline_installation-1.7.609.bin**

Note In the Catalyst Center GUI under **Design** > **Image Repository**, the image EULA is still shown as not accepted, but this is expected and has no functional impact.

Cisco DNA Center 2.3.3.7 and Earlier

To accept the device EULA, complete the following steps.

Step 1 Log in to the Catalyst Center cluster and change directories to the desired location. For example:

```
$ cd /mnt/install-artifacts/eula
$ ls
finalize_offline_installation-1.3.0.147.bin
```

Step 2 Change the permissions:

```
$ sudo chmod 755 finalize_offline_installation-1.3.0.147.bin
[sudo] password for maglev:
```

Step 3 Enter the following command:

```
$ sudo ./finalize_offline_installation-1.3.0.147.bin -Y
```

The **-Y** argument indicates that you are accepting the Catalyst Center software license EULA.

Note In the Catalyst Center GUI under **Design** > **Image Repository**, the image EULA is still shown as not accepted, but this is expected and has no functional impact.

Install the Applications

After completing the preceding tasks, the uber ISO has a number of applications that are loaded and must be installed.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Note At this point, Catalyst Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window will not display application updates that are currently available.

Step 2 If any application updates are available, they are displayed at the bottom of the window. Do one of the following:

- To install all of the available application updates, click the **Select All** link.
- To install individual application updates, check the appropriate check boxes.

Note To open a slide-in pane that indicates an update's file size and provides a brief description of the corresponding application, click its **View Details** link.

Step 3 Click **Install**.

Step 4 After Catalyst Center completes a dependency check, click **Continue**.
The window displays a progress bar for each application that's being updated. The **Software Management** window updates after all of the updates have been installed.

Step 5 Click the **Currently Installed Applications** link and confirm that the applications you selected have been updated.

Update from the Catalyst Center Binary Image

Prerequisites

Before upgrading your installed instance of Catalyst Center, review the following prerequisites:

- Ensure that Catalyst Center does not have internet connectivity.
- Only a user with SUPER-ADMIN-ROLE permissions can perform a Catalyst Center software update.
- Create a backup of your Catalyst Center database. For instructions on creating a backup, see the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.
- Have the username and password for a cisco.com user account available for the download. This can be any valid cisco.com user account.
- Allocate enough time for the upgrade process, which 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.
- Use the **df -h** command to verify the disk space:

```
$ df -h
Filesystem        Size  Used Avail Use% Mounted on
udev                                126G     0  126G   0% /dev
tmpfs                               26G   14M   26G   1% /run
```

```
/dev/sdb2                           29G   23G  4.5G  84% /
tmpfs                               126G     0  126G   0% /dev/shm
tmpfs                               5.0M     0  5.0M   0% /run/lock
tmpfs                               126G     0  126G   0% /sys/fs/cgroup
/dev/sdb3                           29G   44M   27G   1% /install2
/dev/sdb5                           374G   99G  256G  28% /data
/dev/sdb4                           9.3G  601M  8.2G   7% /var
/dev/sdc1                           420G  1.4G  397G   1%
/data/maglev/srv/fusion
/dev/sdc2                           1.4T   41G  1.3T   4%
/data/maglev/srv/maglev-system
/dev/sdd1                           3.5T  243M  3.3T   1% /data/maglev/srv/ndp
glusterfs-server.maglev-…ault_vol   1.4T   54G  1.3T   5%
/mnt/glusterfs/default_vol
[Fri Jan 10 18:59:27 UTC] maglev@10.82.128.100 (maglev-master-10-82-128-100) /
$
```

If you receive a storage validation 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.

Offline Update Workflow

An offline Catalyst Center update involves the following steps:

1. Raise a TAC request to get access to the image for the air gap/offline update.
2. Download the Catalyst Center binary image from a Cisco file server (requires access to the internet).
3. Verify the integrity of the downloaded image.
4. Transfer the downloaded image to the Catalyst Center cluster in the secure, air gap environment.
5. SSH to the Catalyst Center cluster and execute the binary.
6. Log in to the Catalyst Center GUI and perform a system update and an applications update.

Download the Image

You or your Cisco account representative must raise a TAC request. A TAC representative then gives you access and instructions for downloading the binary image from a Cisco file server.

Step 1 Log in to the Cisco file server, which is accessible via the internet.

Step 2 Download the Catalyst Center binary image (.bin) from the location specified.

Step 3 Download the Cisco public key (cisco_image_verification_key.pub) for signature verification.

Step 4 Download the secure hash algorithm (SHA512) checksum file for the image.

Step 5 Download the binary image's signature file (.sig).

Verify the Downloaded File

Verify the integrity of the downloaded image using Cisco signature verification and the SHA512 checksum provided on the portal.

Step 1 (Optional) Perform SHA verification to determine whether the binary image is corrupted due to a partial download.

Depending on your OS, enter one of the following commands:

- Linux:

```
sha512sum Catalyst-Center-image-filename
```

- Mac:

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows does not include a built-in checksum utility, but you can use the certutil tool:

```
certutil -hashfile <filename> sha256 | md5
```

For example:

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

On Windows, you can also use the Windows PowerShell to generate the digest. For example:

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

Compare the output of the command you run to the SHA512 checksum file that you downloaded. If the command output does not match, download the binary image again and run the appropriate command a second time. If the output still does not match, contact Cisco support.

Step 2 Verify that the binary image is genuine and from Cisco by verifying its signature:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
signature-filename Catalyst-Center-image-filename
```

This command works in both Mac and Linux environments. For Windows, you must download and install OpenSSL, if you haven’t done so already.

If the binary image is genuine, entering this command displays a **Verified OK** message. If this message fails to appear, do not install the binary image and contact Cisco support.

Transfer the File to Catalyst Center

Step 1 Use a supported file transfer mechanism (SCP or SFTP) to transfer the downloaded image to the Catalyst Center cluster and the /data/tmp partition. When using USB, transfer the image to a terminal in the air-gapped network and then transfer the image to the Catalyst Center cluster and the /data/tmp partition (via SCP or SFTP).

Step 2 After transferring the image to the Catalyst Center cluster, perform SHA verification again to check if the file was corrupted in the process.

Considerations for a Three-Node Cluster

Step 1 For a three-node Catalyst Center cluster, copy the bin file to the node where the catalogserver pod is running.

Step 2 To determine the IP address of the node where the catalog server is running, enter:

```
magctl service status catalogserver | grep Node:
```

For example, the output is similar to the following:

```
$ magctl service status catalogserver | grep Node:
Node: 192.192.192.72/192.192.192.72

[Thu Mar 19 22:59:48 UTC]maglev@192.192.192.68(maglev-master-192-192-192-68) ~
$
```

In this example, copy the bin file to one of the following partitions on **192.192.192.72**:

- Cisco DNA Center 2.3.2.x and 2.3.3.x: `/data/tmp`
- Cisco DNA Center 2.3.4.x and later: `/artifacts`

Execute the Binary File

To execute the binary file, complete the procedure specific to your Catalyst Center version:

- Cisco DNA Center 2.3.4.0 and Later
- Cisco DNA Center 2.3.3.7 and Earlier

Cisco DNA Center 2.3.4.0 and Later

Step 1 Use an SSH client to log in to your Catalyst Center cluster. For a three-node cluster, log in to the node with the **catalogserver** pod.

Step 2 Execute the update binary by running the following command: **maglev catalog airgap install /artifacts/**<*update-binary-filename*>**.bin**

Cisco DNA Center 2.3.3.7 and Earlier

Step 1 Use SSH to log in to the Catalyst Center cluster.

Step 2 Enter the following command to add execute permission:

```
chmod +x <uber-bin-file>
```

Step 3 Enter the following command to execute the binary file:

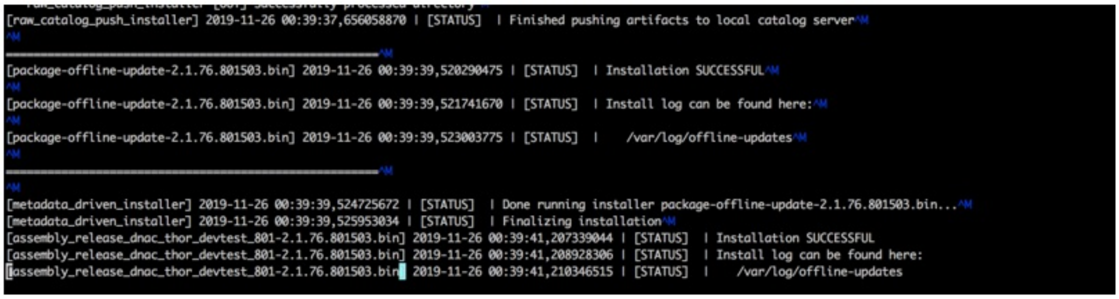
```
sudo ./<uber-bin-file>
```

The command has the following output:

```
$ sudo ./<bin-filename>.bin
[sudo] password for maglev:
=============================
Welcome to DNAC offline update
=============================
Please provide your credentials to get started
[administration] username: admin <Catalyst Center login/password combo>
[administration] password for admin: <Catalyst Center password>
```

Step 4 Executing the binary file updates the local catalog for the system and application packages. Locate the **Installation SUCCESSFUL** status message, which indicates that the bin file executed successfully.

You can track the current status of the process by tailing the log file <*bin-filename*>-install.log. If required, you can also verify the logs under /var/log/offlineupdates/.



```
[raw_catalog_push_installer] 2019-11-26 00:39:37,656058870 | [STATUS]  | Finished pushing artifacts to local catalog server^M
^M
-------------------------------------------------------------^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,520290475 | [STATUS]  | Installation SUCCESSFUL^M
^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,521741670 | [STATUS]  | Install log can be found here:^M
^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,523003775 | [STATUS]  |    /var/log/offline-updates^M
^M
-------------------------------------------------------------^M
^M
[metadata_driven_installer] 2019-11-26 00:39:39,524725672 | [STATUS]  | Done running installer package-offline-update-2.1.76.801503.bin...^M
[metadata_driven_installer] 2019-11-26 00:39:39,525953034 | [STATUS]  | Finalizing installation^M
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,207339044 | [STATUS]  | Installation SUCCESSFUL
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,208928306 | [STATUS]  | Install log can be found here:
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,210346515 | [STATUS]  |    /var/log/offline-updates
```

Perform an Offline Update

Complete the following procedure to upgrade from Cisco DNA Center 2.3.2.x, 2.3.3.x, or 2.3.4.x to 2.3.5.x.

Step 1 After successful execution of the binary file, install the necessary patch:

Important Step 1 is valid only if you are upgrading from either 2.3.2.0 or 2.3.2.1. If you are upgrading from 2.3.2.3, start with Step 2 of this procedure.

a) Download a local copy of **CSCwb00526.sh.zip** from the following URL: https://software.cisco.com/download/specialrelease/46a2ecbbe1219e5184d0094771637b2a
b) Unzip this zip file.
c) Run the **ssh maglev@***cluster's-IP-address***:/data/tmp** command to copy the file **CSCwb00526.sh** to your Cisco DNA Center cluster.
d) Run the following commands:

   sudo chmod 777 CSCwb00526.sh

   sudo bash CSCwb00526.sh

e) Run the **magctl appstack status | grep catalogs** command to confirm that the catalog service is running.
f) View the output. It should look similar to the following example:

```
$ magctl appstack status | grep catalogs
maglev-system catalogserver 1/1 Running
```

Step 2 Log in to the Cisco DNA Center GUI.

Step 3 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Step 4 Confirm that the **Software Management** window indicates that Cisco DNA Center <*version*> is available.

Step 5 Click **Install now**.

Step 6 After Cisco DNA Center completes its prechecks, click **Install**.

Step 7 After the upgrade completes, click the **Currently Installed Applications** link and confirm that each application has been updated.

Update the Knowledge Pack for a PSIRT Scan

Offline Update of Knowledge Pack

An offline knowledge pack update involves the following steps:

1. Download the knowledge pack file.
2. Export the file to USB or other transferrable medium.
3. Import the file to Catalyst Center on an air-gap device.

Download the File

Step 1 Confirm that you are using one of the recommended search engines: Chrome or Firefox.

Step 2 Select the following link to begin downloading:

https://tools.cisco.com/cscrdr/security/center/files/mre/mre_workflow_signed.tar.gz

Export to USB or Other Transferrable Medium

Step 1 Confirm that the file is in .tar.gz format.

Step 2 Transfer the downloaded file to USB (or other medium).

Import to Catalyst Center on an Air-Gap Device

Step 1 Insert the USB into the device.

Step 2 In the Catalyst Center GUI, click the menu icon and choose **System** > **Settings** > **Machine Reasoning**.

Step 3 To import to Catalyst Center, click **Import**.

Step 4 Select the .tar.gz file from the USB to upload.

Download the Latest KGV File for Integrity Verification

Complete the following procedure to download the KGV file you'll use for integrity verification.

Step 1 Using a device with internet access, download the **Cisco_KnownGoodValues.tar** KGV file from the following URL: https://tools.cisco.com/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar.

Step 2 Transfer this file to storage media or a device in your air-gapped environment.

Step 3 Using a device with browser access to your air-gapped Catalyst Center cluster, import the file:

a) On your Catalyst Center cluster, open the following URL in a browser: /dna/systemSettings/settings?settings-item=IntegrityVerficationSettings.

b) Choose **Import New from Local**.

c) Import the KGV file you downloaded in Step 1.

PART II

Standard Air Gap Deployment: 2.3.2.x to 2.3.3.x or 2.3.4.x

CHAPTER 3

2.3.2.x to 2.3.3.x or 2.3.4.x

Fresh Install from the Catalyst Center ISO Image

Offline Install Workflow

An offline Catalyst Center installation involves the following steps:

1. Download the image.
2. Verify the downloaded file.
3. Create a bootable USB drive.
4. Install the Catalyst Center ISO image.
5. Configure the Catalyst Center appliance.
6. Complete the first-time setup.
7. Accept the device EULA.
8. Install the applications.

Download the Image

You or your Cisco account representative must raise a TAC request. A TAC representative then gives you access and instructions for downloading the binary image from a Cisco file server.

Step 1 Log in to the Cisco file server, which is accessible via the internet.

Step 2 Download the Catalyst Center binary image (.bin) from the location specified.

Step 3 Download the Cisco public key (cisco_image_verification_key.pub) for signature verification.

Step 4 Download the secure hash algorithm (SHA512) checksum file for the image.

Step 5 Download the binary image's signature file (.sig).

Verify the Downloaded File

Verify the integrity of the downloaded image using Cisco signature verification and the SHA512 checksum provided on the portal.

Step 1 (Optional) Perform SHA verification to determine whether the binary image is corrupted due to a partial download.

Depending on your OS, enter one of the following commands:

- Linux:

```
sha512sum Catalyst-Center-image-filename
```

- Mac:

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows does not include a built-in checksum utility, but you can use the certutil tool:

```
certutil -hashfile <filename> sha256 | md5
```

For example:

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

On Windows, you can also use the Windows PowerShell to generate the digest. For example:

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

Compare the output of the command you run to the SHA512 checksum file that you downloaded. If the command output does not match, download the binary image again and run the appropriate command a second time. If the output still does not match, contact Cisco support.

Step 2 Verify that the binary image is genuine and from Cisco by verifying its signature:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
signature-filename Catalyst-Center-image-filename
```

This command works in both Mac and Linux environments. For Windows, you must download and install OpenSSL, if you haven’t done so already.

If the binary image is genuine, entering this command displays a **Verified OK** message. If this message fails to appear, do not install the binary image and contact Cisco support.

Create a Bootable USB Drive

After confirming that you downloaded a Cisco ISO image, create a bootable USB drive that contains the Catalyst Center ISO image. For details, see the "Create a Bootable USB Flash Drive" topic in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide's* "Prepare the Appliance for Configuration" chapter.

Install the Catalyst Center ISO Image

Step 1 Connect the bootable USB drive with the Catalyst Center ISO image to the appliance.

Step 2 Log in to Cisco IMC and start a KVM session.

Step 3 Power on or power cycle the appliance:

- If the appliance is not currently running, choose **Power** > **Power On System**.
- If the appliance is already running, choose **Power** > **Power Cycle System (cold boot)**.

Step 4 In the resulting pop-up window, click **Yes** to acknowledge that you are about to execute a server control action.

Step 5 When the Cisco logo appears, either press the **F6** key or choose **Macros** > **User Defined Macros** > **F6** from the KVM menu. The boot device selection menu appears.

Step 6 Select your USB drive and then press **Enter**.

Step 7 In the GNU GRUB bootloader window, choose **Cisco DNA Center Installer** and then press **Enter**.

Note The bootloader automatically boots the Maglev installer if you don't make a selection within 30 seconds.

Configure the Catalyst Center Appliance

When installation of the Catalyst Center ISO image completes, the installer reboots and opens the Maglev Configuration wizard's welcome screen. To configure your appliance for day-to-day use in your network, complete the steps described in one of the following sections:

- If you are using the Maglev Configuration wizard, see "Configure the Appliance Using the Maglev Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.
- If you are using the browser-based configuration wizard to configure a 44- or 56-core appliance, see "Configure the 44/56-Core Appliance Using the Browser-Based Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.
- If you are using the browser-based configuration wizard to configure a 112-core appliance, see "Configure the 112-Core Appliance Using the Browser-Based Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.

Complete the First-Time Setup

Step 1 After the Catalyst Center appliance reboot is completed, launch your browser.

Step 2 Enter the host IP address to access the Catalyst Center GUI, using HTTPS:// and the IP address of the Catalyst Center GUI that was displayed at the end of the configuration process.

After entering the IP address, one of the following messages appears (depending on your browser):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

Step 3 Ignore the message and click **Advanced**. One of the following messages appears:

- Google Chrome: `This server could not prove that it is` *`GUI-IP-address`*`; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.`
- Mozilla Firefox: `Someone could be trying to impersonate the site and you should not continue. Websites prove their identity via certificates. Firefox does not trust` *`GUI-IP-address`* `because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.`

These messages appear because the controller uses a self-signed certificate. For information on how Catalyst Center uses certificates, see the "Certificate and Private Key Support" section in the *Cisco Catalyst Center Administrator Guide*.

Step 4 Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to <*GUI-IP-address*> (unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

The Catalyst Center **Login** window appears.

Step 5 In the Login window, enter the admin's username (admin) and password that you set when you configured Catalyst Center, then click **Log In**.
The **Reset Login** window appears.

Step 6 Enter the old password, enter and confirm a new password for the admin superuser, and then click **Save**.
The **Enter Cisco.com ID** window appears.

Step 7 (*Skip this step*) Enter the username and password for the cisco.com user, then click **Next**. If the cisco.com user login does not match any known Cisco Smart Account user login, the **Smart Account** window appears.

Step 8 (*Skip this step*) If the **Smart Account** window appears, enter the username and password for your organization's Smart Account, or click the corresponding link to open a new Smart Account. After you are finished, click **Next**.
The **IP Address Manager** window appears.

Step 9 If your organization uses an external IP address manager (IPAM), do the following and then click **Next**:

- Enter your IPAM server's name and URL.
- Enter the username and password required for server access.
- Choose your IPAM provider (such as Infoblox).
- Choose the specific view of IP addresses available in the IPAM server database that you want Catalyst Center to use.

The **Enter Proxy Server** window appears.

Step 10 Click **Next**.
The software **EULA** window appears.

Step 11 Click **Next** to accept the software End User License Agreement and continue.
The **Ready to go!** window appears.

Step 12 We recommend that you click the **User Management** link to display the User Management window. Then click **Add** to begin adding new Catalyst Center users. After you have entered the new user's name and password, and selected the

user's role, click **Save** to create the new user. Repeat this as needed until you have added all the new users for your initial deployment. Be sure to create at least one user with the NETWORK-ADMIN-ROLE.

Accept the Device EULA

Step 1 Log in to the Catalyst Center cluster and change directories to the desired location. For example:

```
$ cd /mnt/install-artifacts/eula
$ ls
finalize_offline_installation-1.3.0.147.bin
```

Step 2 Change the permissions:

```
$ sudo chmod 755 finalize_offline_installation-1.3.0.147.bin
[sudo] password for maglev:
```

Step 3 Enter the following command:

```
$ sudo ./finalize_offline_installation-1.3.0.147.bin -Y
```

The **-Y** argument indicates that you are accepting the Catalyst Center software license EULA.

Note In the Catalyst Center GUI under **Design** > **Image Repository**, the image EULA is still shown as not accepted, but this is expected and has no functional impact.

Install the Applications

After completing the preceding tasks, the uber ISO has a number of applications that are loaded and must be installed.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Note At this point, Catalyst Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window will not display application updates that are currently available.

Step 2 If any application updates are available, they are displayed at the bottom of the window. Do one of the following:

- To install all of the available application updates, click the **Select All** link.
- To install individual application updates, check the appropriate check boxes.

Note To open a slide-in pane that indicates an update's file size and provides a brief description of the corresponding application, click its **More details** link.

Step 3 Click **Install**.

Step 4 After Catalyst Center completes a dependency check, click **Continue**.
The window displays a progress bar for each application that's being updated. The **Software Management** window updates after all of the updates have been installed.

Step 5 Click the **Currently Installed Applications** link and confirm that the applications you selected have been updated.

Update from the Catalyst Center Binary Image

Prerequisites

Before upgrading your installed instance of Catalyst Center, review the following prerequisites:

- Ensure that Catalyst Center does not have internet connectivity.
- Only a user with SUPER-ADMIN-ROLE permissions can perform a Catalyst Center software update.
- Create a backup of your Catalyst Center database. For instructions on creating a backup, see the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.
- Have the username and password for a cisco.com user account available for the download. This can be any valid cisco.com user account.
- Allocate enough time for the upgrade process, which 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.
- Use the **df -h** command to verify the disk space:

```
$ df -h
Filesystem        Size  Used Avail Use% Mounted on
udev                                126G     0  126G   0% /dev
tmpfs                               26G   14M   26G   1% /run
/dev/sdb2                           29G   23G  4.5G  84% /
tmpfs                               126G     0  126G   0% /dev/shm
tmpfs                               5.0M     0  5.0M   0% /run/lock
tmpfs                               126G     0  126G   0% /sys/fs/cgroup
/dev/sdb3                           29G   44M   27G   1% /install2
/dev/sdb5                           374G   99G  256G  28% /data
/dev/sdb4                           9.3G  601M  8.2G   7% /var
/dev/sdc1                           420G  1.4G  397G   1%
/data/maglev/srv/fusion
/dev/sdc2                           1.4T   41G  1.3T   4%
/data/maglev/srv/maglev-system
/dev/sdd1                           3.5T  243M  3.3T   1% /data/maglev/srv/ndp
glusterfs-server.maglev-…ault_vol   1.4T   54G  1.3T   5%
/mnt/glusterfs/default_vol
[Fri Jan 10 18:59:27 UTC] maglev@10.82.128.100 (maglev-master-10-82-128-100) /
$
```

If you receive a storage validation 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.

Offline Update Workflow

An offline Catalyst Center update involves the following steps:

1. Raise a TAC request to get access to the image for the air gap/offline update.
2. Download the Catalyst Center binary image from a Cisco file server (requires access to the internet).
3. Verify the integrity of the downloaded image.
4. Transfer the downloaded image to the Catalyst Center cluster in the secure, air gap environment.
5. SSH to the Catalyst Center cluster and execute the binary.
6. Log in to the Catalyst Center GUI and perform a system update and an applications update.

Download the Image

You or your Cisco account representative must raise a TAC request. A TAC representative then gives you access and instructions for downloading the binary image from a Cisco file server.

Step 1 Log in to the Cisco file server, which is accessible via the internet.

Step 2 Download the Catalyst Center binary image (.bin) from the location specified.

Step 3 Download the Cisco public key (cisco_image_verification_key.pub) for signature verification.

Step 4 Download the secure hash algorithm (SHA512) checksum file for the image.

Step 5 Download the binary image's signature file (.sig).

Verify the Downloaded File

Verify the integrity of the downloaded image using Cisco signature verification and the SHA512 checksum provided on the portal.

Step 1 (Optional) Perform SHA verification to determine whether the binary image is corrupted due to a partial download.

Depending on your OS, enter one of the following commands:

- Linux:

```
sha512sum Catalyst-Center-image-filename
```

- Mac:

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows does not include a built-in checksum utility, but you can use the certutil tool:

```
certutil -hashfile <filename> sha256 | md5
```

For example:

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

On Windows, you can also use the Windows PowerShell to generate the digest. For example:

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

Compare the output of the command you run to the SHA512 checksum file that you downloaded. If the command output does not match, download the binary image again and run the appropriate command a second time. If the output still does not match, contact Cisco support.

Step 2 Verify that the binary image is genuine and from Cisco by verifying its signature:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
signature-filename Catalyst-Center-image-filename
```

This command works in both Mac and Linux environments. For Windows, you must download and install OpenSSL, if you haven't done so already.

If the binary image is genuine, entering this command displays a **Verified OK** message. If this message fails to appear, do not install the binary image and contact Cisco support.

Transfer the File to Catalyst Center

Step 1 Use a supported file transfer mechanism (SCP or SFTP) to transfer the downloaded image to the Catalyst Center cluster and the /data/tmp partition. When using USB, transfer the image to a terminal in the air-gapped network and then transfer the image to the Catalyst Center cluster and the /data/tmp partition (via SCP or SFTP).

Step 2 After transferring the image to the Catalyst Center cluster, perform SHA verification again to check if the file was corrupted in the process.

Considerations for a Three-Node Cluster

Step 1 For a three-node Catalyst Center cluster, copy the bin file to the node where the catalogserver pod is running.

Step 2 To determine the IP address of the node where the catalog server is running, enter:

```
magctl service status catalogserver | grep Node:
```

For example, the output is similar to the following:

```
$ magctl service status catalogserver | grep Node:
Node: 192.192.192.72/192.192.192.72

[Thu Mar 19 22:59:48 UTC]maglev@192.192.192.68(maglev-master-192-192-192-68) ~
$
```

In this example, copy the bin file to the /data/tmp partition on **192.192.192.72**.

Execute the Binary File

Step 1 Use SSH to log in to the Catalyst Center cluster.

Step 2 Enter the following command to add execute permission:

```
chmod +x <uber-bin-file>
```

Step 3 Enter the following command to execute the binary file:

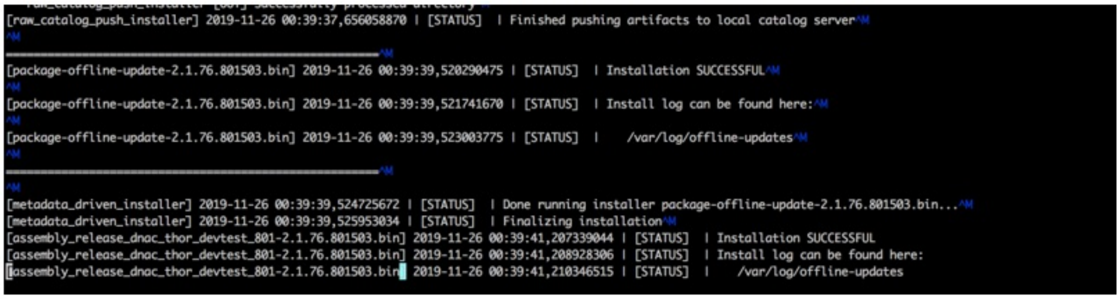
```
sudo ./<uber-bin-file>
```

The command has the following output:

```
$ sudo ./<bin-filename>.bin
[sudo] password for maglev:
=============================
Welcome to DNAC offline update
=============================
Please provide your credentials to get started
[administration] username: admin <Catalyst Center login/password combo>
[administration] password for admin: <Catalyst Center password>
```

Step 4 Executing the binary file updates the local catalog for the system and application packages. Locate the **Installation SUCCESSFUL** status message, which indicates that the bin file executed successfully.

You can track the current status of the process by tailing the log file <*bin-filename*>-install.log. If required, you can also verify the logs under /var/log/offlineupdates/.



```
[raw_catalog_push_installer] 2019-11-26 00:39:37,656058870 | [STATUS]  | Finished pushing artifacts to local catalog server^M
^M
------------------------------------------------------------^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,520290475 | [STATUS]  | Installation SUCCESSFUL^M
^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,521741670 | [STATUS]  | Install log can be found here:^M
^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,523003775 | [STATUS]  |    /var/log/offline-updates^M
^M
------------------------------------------------------------^M
^M
[metadata_driven_installer] 2019-11-26 00:39:39,524725672 | [STATUS]  | Done running installer package-offline-update-2.1.76.801503.bin...^M
[metadata_driven_installer] 2019-11-26 00:39:39,525953034 | [STATUS]  | Finalizing installation^M
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,207339044 | [STATUS]  | Installation SUCCESSFUL
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,208928306 | [STATUS]  | Install log can be found here:
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,210346515 | [STATUS]  |    /var/log/offline-updates
```

Perform an Offline Update

Complete the following procedure to upgrade from Cisco DNA Center 2.3.2.x or 2.3.3.x to 2.3.4.x.

Step 1 After successful execution of the binary file, install the necessary patch:

Important Step 1 is valid only if you are upgrading from either 2.3.2.0 or 2.3.2.1. If you are upgrading from 2.3.2.3, start with Step 2 of this procedure.

a) Download a local copy of **CSCwb00526.sh.zip** from the following URL: https://software.cisco.com/download/specialrelease/46a2ecbbe1219e5184d0094771637b2a

b) Unzip this zip file.

c) Run the **ssh maglev@***cluster's-IP-address***:/data/tmp** command to copy the file **CSCwb00526.sh** to your Cisco DNA Center cluster.

d) Run the following commands:

sudo chmod 777 CSCwb00526.sh

sudo bash CSCwb00526.sh

e) Run the **magctl appstack status | grep catalogs** command to confirm that the catalog service is running.

f) View the output. It should look similar to the following example:

```
$ magctl appstack status | grep catalogs
maglev-system catalogserver 1/1 Running
```

Step 2 Log in to the Cisco DNA Center GUI.

Step 3 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Step 4 Confirm that the **Software Management** window indicates that Catalyst Center <*version*> is available.

Step 5 Click **Install now**.

Step 6 After Cisco DNA Center completes its prechecks, click **Install**.

Step 7 After the upgrade completes, click the **Currently Installed Applications** link and confirm that each application has been updated.

Update the Knowledge Pack for a PSIRT Scan

Offline Update of Knowledge Pack

An offline knowledge pack update involves the following steps:

1. Download the knowledge pack file.
2. Export the file to USB or other transferrable medium.
3. Import the file to Catalyst Center on an air-gap device.

Download the File

Step 1 Confirm that you are using one of the recommended search engines: Chrome or Firefox.

Step 2 Select the following link to begin downloading:

https://tools.cisco.com/cscrdr/security/center/files/mre/mre_workflow_signed.tar.gz

Export to USB or Other Transferrable Medium

Step 1 Confirm that the file is in .tar.gz format.

Step 2 Transfer the downloaded file to USB (or other medium).

Verify the Downloaded File

Verify the integrity of the downloaded image using Cisco signature verification and the SHA512 checksum provided on the portal.

Step 1 (Optional) Perform SHA verification to determine whether the binary image is corrupted due to a partial download.

Depending on your OS, enter one of the following commands:

- Linux:

```
sha512sum Catalyst-Center-image-filename
```

- Mac:

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows does not include a built-in checksum utility, but you can use the certutil tool:

```
certutil -hashfile <filename> sha256 | md5
```

For example:

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

On Windows, you can also use the Windows PowerShell to generate the digest. For example:

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

Compare the output of the command you run to the SHA512 checksum file that you downloaded. If the command output does not match, download the binary image again and run the appropriate command a second time. If the output still does not match, contact Cisco support.

Step 2 Verify that the binary image is genuine and from Cisco by verifying its signature:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
signature-filename Catalyst-Center-image-filename
```

This command works in both Mac and Linux environments. For Windows, you must download and install OpenSSL, if you haven’t done so already.

If the binary image is genuine, entering this command displays a **Verified OK** message. If this message fails to appear, do not install the binary image and contact Cisco support.

Download the Latest KGV File for Integrity Verification

Complete the following procedure to download the KGV file you'll use for integrity verification.

Step 1 Using a device with internet access, download the **Cisco_KnownGoodValues.tar** KGV file from the following URL: https://tools.cisco.com/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar.

Step 2 Transfer this file to storage media or a device in your air-gapped environment.

Step 3 Using a device with browser access to your air-gapped Catalyst Center cluster, import the file:

a) On your Catalyst Center cluster, open the following URL in a browser: /dna/systemSettings/settings?settings-item=IntegrityVerficationSettings.

b) Choose **Import New from Local**.

c) Import the KGV file you downloaded in Step 1.

PART III

Standard Air Gap Deployment: 2.2.2.x or 2.2.3.x to 2.3.3.x

CHAPTER 4

2.2.2.x or 2.2.3.x to 2.3.3.x

Fresh Install from the Catalyst Center ISO Image

Offline Install Workflow

An offline Catalyst Center installation involves the following steps:

1. Download the image.
2. Verify the downloaded file.
3. Create a bootable USB drive.
4. Install the Catalyst Center ISO image.
5. Configure the Catalyst Center appliance.
6. Complete the first-time setup.
7. Accept the device EULA.
8. Install the applications.

Download the Image

You or your Cisco account representative must raise a TAC request. A TAC representative then gives you access and instructions for downloading the binary image from a Cisco file server.

Step 1 Log in to the Cisco file server, which is accessible via the internet.

Step 2 Download the Catalyst Center binary image (.bin) from the location specified.

Step 3 Download the Cisco public key (cisco_image_verification_key.pub) for signature verification.

Step 4 Download the secure hash algorithm (SHA512) checksum file for the image.

Step 5 Download the binary image's signature file (.sig).

Verify the Downloaded File

Verify the integrity of the downloaded image using Cisco signature verification and the SHA512 checksum provided on the portal.

Step 1 (Optional) Perform SHA verification to determine whether the binary image is corrupted due to a partial download.

Depending on your OS, enter one of the following commands:

- Linux:

```
sha512sum Catalyst-Center-image-filename
```

- Mac:

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows does not include a built-in checksum utility, but you can use the certutil tool:

```
certutil -hashfile <filename> sha256 | md5
```

For example:

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

On Windows, you can also use the Windows PowerShell to generate the digest. For example:

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

Compare the output of the command you run to the SHA512 checksum file that you downloaded. If the command output does not match, download the binary image again and run the appropriate command a second time. If the output still does not match, contact Cisco support.

Step 2 Verify that the binary image is genuine and from Cisco by verifying its signature:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
signature-filename Catalyst-Center-image-filename
```

This command works in both Mac and Linux environments. For Windows, you must download and install OpenSSL, if you haven’t done so already.

If the binary image is genuine, entering this command displays a **Verified OK** message. If this message fails to appear, do not install the binary image and contact Cisco support.

Create a Bootable USB Drive

After confirming that you downloaded a Cisco ISO image, create a bootable USB drive that contains the Catalyst Center ISO image. For details, see the "Create a Bootable USB Flash Drive" topic in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide's* "Prepare the Appliance for Configuration" chapter.

Install the Catalyst Center ISO Image

Step 1 Connect the bootable USB drive with the Catalyst Center ISO image to the appliance.

Step 2 Log in to Cisco IMC and start a KVM session.

Step 3 Power on or power cycle the appliance:

- If the appliance is not currently running, choose **Power** > **Power On System**.
- If the appliance is already running, choose **Power** > **Power Cycle System (cold boot)**.

Step 4 In the resulting pop-up window, click **Yes** to acknowledge that you are about to execute a server control action.

Step 5 When the Cisco logo appears, either press the **F6** key or choose **Macros** > **User Defined Macros** > **F6** from the KVM menu. The boot device selection menu appears.

Step 6 Select your USB drive and then press **Enter**.

Step 7 In the GNU GRUB bootloader window, choose **Cisco DNA Center Installer** and then press **Enter**.

Note The bootloader automatically boots the Maglev installer if you don't make a selection within 30 seconds.

Configure the Catalyst Center Appliance

When installation of the Catalyst Center ISO image completes, the installer reboots and opens the Maglev Configuration wizard's welcome screen. To configure your appliance for day-to-day use in your network, complete the steps described in one of the following sections:

- If you are using the Maglev Configuration wizard, see "Configure the Appliance Using the Maglev Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.
- If you are using the browser-based configuration wizard to configure a 44- or 56-core appliance, see "Configure the 44/56-Core Appliance Using the Browser-Based Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.
- If you are using the browser-based configuration wizard to configure a 112-core appliance, see "Configure the 112-Core Appliance Using the Browser-Based Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.

Complete the First-Time Setup

Step 1 After the Catalyst Center appliance reboot is completed, launch your browser.

Step 2 Enter the host IP address to access the Catalyst Center GUI, using HTTPS:// and the IP address of the Catalyst Center GUI that was displayed at the end of the configuration process.

After entering the IP address, one of the following messages appears (depending on your browser):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

Step 3 Ignore the message and click **Advanced**. One of the following messages appears:

- Google Chrome: `This server could not prove that it is` *`GUI-IP-address`*`; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.`
- Mozilla Firefox: `Someone could be trying to impersonate the site and you should not continue. Websites prove their identity via certificates. Firefox does not trust` *`GUI-IP-address`* `because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.`

These messages appear because the controller uses a self-signed certificate. For information on how Catalyst Center uses certificates, see the "Certificate and Private Key Support" section in the *Cisco Catalyst Center Administrator Guide*.

Step 4 Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to <*GUI-IP-address*> (unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

The Catalyst Center **Login** window appears.

Step 5 In the Login window, enter the admin's username (admin) and password that you set when you configured Catalyst Center, then click **Log In**.
The **Reset Login** window appears.

Step 6 Enter the old password, enter and confirm a new password for the admin superuser, and then click **Save**.
The **Enter Cisco.com ID** window appears.

Step 7 (*Skip this step*) Enter the username and password for the cisco.com user, then click **Next**. If the cisco.com user login does not match any known Cisco Smart Account user login, the **Smart Account** window appears.

Step 8 (*Skip this step*) If the **Smart Account** window appears, enter the username and password for your organization's Smart Account, or click the corresponding link to open a new Smart Account. After you are finished, click **Next**.
The **IP Address Manager** window appears.

Step 9 If your organization uses an external IP address manager (IPAM), do the following and then click **Next**:

- Enter your IPAM server's name and URL.
- Enter the username and password required for server access.
- Choose your IPAM provider (such as Infoblox).
- Choose the specific view of IP addresses available in the IPAM server database that you want Catalyst Center to use.

The **Enter Proxy Server** window appears.

Step 10 Click **Next**.
The software **EULA** window appears.

Step 11 Click **Next** to accept the software End User License Agreement and continue.
The **Ready to go!** window appears.

Step 12 We recommend that you click the **User Management** link to display the User Management window. Then click **Add** to begin adding new Catalyst Center users. After you have entered the new user's name and password, and selected the

user's role, click **Save** to create the new user. Repeat this as needed until you have added all the new users for your initial deployment. Be sure to create at least one user with the NETWORK-ADMIN-ROLE.

Accept the Device EULA

Step 1 Log in to the Catalyst Center cluster and change directories to the desired location. For example:

```
$ cd /mnt/install-artifacts/eula
$ ls
finalize_offline_installation-1.3.0.147.bin
```

Step 2 Change the permissions:

```
$ sudo chmod 755 finalize_offline_installation-1.3.0.147.bin
[sudo] password for maglev:
```

Step 3 Enter the following command:

```
$ sudo ./finalize_offline_installation-1.3.0.147.bin -Y
```

The **-Y** argument indicates that you are accepting the Catalyst Center software license EULA.

Note In the Catalyst Center GUI under **Design** > **Image Repository**, the image EULA is still shown as not accepted, but this is expected and has no functional impact.

Install the Applications

After completing the preceding tasks, the uber ISO has a number of applications that are loaded and must be installed.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Software Management**.

Note At this point, Catalyst Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window will not display application updates that are currently available.

Step 2 If any application updates are available, they are displayed at the bottom of the window. Do one of the following:

- To install all of the available application updates, click the **Select All** link.
- To install individual application updates, check the appropriate check boxes.

Note To open a slide-in pane that indicates an update's file size and provides a brief description of the corresponding application, click its **More details** link.

Step 3 Click **Install**.

Step 4 After Catalyst Center completes a dependency check, click **Continue**.
The window displays a progress bar for each application that's being updated. The **Software Management** window updates after all of the updates have been installed.

Step 5 Click the **Currently Installed Applications** link and confirm that the applications you selected have been updated.

Update from the Catalyst Center Binary Image

Prerequisites

Before upgrading your installed instance of Catalyst Center, review the following prerequisites:

- Ensure that Catalyst Center does not have internet connectivity.
- Only a user with SUPER-ADMIN-ROLE permissions can perform a Catalyst Center software update.
- Create a backup of your Catalyst Center database. For instructions on creating a backup, see the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.
- Have the username and password for a cisco.com user account available for the download. This can be any valid cisco.com user account.
- Allocate enough time for the upgrade process, which 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.
- Use the **df -h** command to verify the disk space:

```
$ df -h
Filesystem        Size  Used Avail Use% Mounted on
udev                                126G     0  126G    0% /dev
tmpfs                               26G   14M   26G    1% /run
/dev/sdb2                           29G   23G  4.5G  84% /
tmpfs                               126G     0  126G    0% /dev/shm
tmpfs                               5.0M     0  5.0M    0% /run/lock
tmpfs                               126G     0  126G    0% /sys/fs/cgroup
/dev/sdb3                           29G   44M   27G    1% /install2
/dev/sdb5                           374G   99G  256G  28% /data
/dev/sdb4                           9.3G  601M  8.2G    7% /var
/dev/sdc1                           420G  1.4G  397G    1%
/data/maglev/srv/fusion
/dev/sdc2                           1.4T   41G  1.3T    4%
/data/maglev/srv/maglev-system
/dev/sdd1                           3.5T  243M  3.3T    1% /data/maglev/srv/ndp
glusterfs-server.maglev-…ault_vol   1.4T   54G  1.3T    5%
/mnt/glusterfs/default_vol
[Fri Jan 10 18:59:27 UTC] maglev@10.82.128.100 (maglev-master-10-82-128-100) /
$
```

If you receive a storage validation 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.

Offline Update Workflow

An offline Catalyst Center update involves the following steps:

1. Raise a TAC request to get access to the image for the air gap/offline update.
2. Download the Catalyst Center binary image from a Cisco file server (requires access to the internet).
3. Verify the integrity of the downloaded image.
4. Transfer the downloaded image to the Catalyst Center cluster in the secure, air gap environment.
5. SSH to the Catalyst Center cluster and execute the binary.
6. Log in to the Catalyst Center GUI and perform a system update and an applications update.

Download the Image

You or your Cisco account representative must raise a TAC request. A TAC representative then gives you access and instructions for downloading the binary image from a Cisco file server.

Step 1 Log in to the Cisco file server, which is accessible via the internet.

Step 2 Download the image from the Cisco file server. This includes the secure hash algorithm (SHA512) checksum file for the image.

Verify the Downloaded File

Verify the integrity of the downloaded image using Cisco signature verification and the SHA512 checksum provided on the portal.

Step 1 Perform SHA verification to determine whether the binary image is corrupted due to a partial download.

Depending on your OS, enter one of the following commands:

- Linux:

```
sha512sum Catalyst-Center-image-filename
```

- Mac:

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows does not include a built-in checksum utility, but you can install a utility from Microsoft at http://www.microsoft.com/en-us/download/details.aspx?id=11533.

Step 2 Compare the command output (or Microsoft Windows utility) to the SHA512 checksum file. If the command output does not match, download the binary image again and enter the appropriate command a second time. If the output still does not match, contact Cisco support.

Transfer the File to Catalyst Center

Step 1 Use a supported file transfer mechanism (SCP or SFTP) to transfer the downloaded image to the Catalyst Center cluster and the /data/tmp partition. When using USB, transfer the image to a terminal in the air-gapped network and then transfer the image to the Catalyst Center cluster and the /data/tmp partition (via SCP or SFTP).

Step 2 After transferring the image to the Catalyst Center cluster, perform SHA verification again to check if the file was corrupted in the process.

Considerations for a Three-Node Cluster

Step 1 For a three-node Catalyst Center cluster, copy the bin file to the node where the catalogserver pod is running.

Step 2 To determine the IP address of the node where the catalog server is running, enter:

```
magctl service status catalogserver | grep Node:
```

For example, the output is similar to the following:

```
$ magctl service status catalogserver | grep Node:
Node: 192.192.192.72/192.192.192.72

[Thu Mar 19 22:59:48 UTC]maglev@192.192.192.68(maglev-master-192-192-192-68) ~
$
```

In this example, copy the bin file to the /data/tmp partition on **192.192.192.72**.

Execute the Binary File

Step 1 Use SSH to log in to the Catalyst Center cluster.

Step 2 Enter the following command to add execute permission:

```
chmod +x <uber-bin-file>
```

Step 3 Enter the following command to execute the binary file:

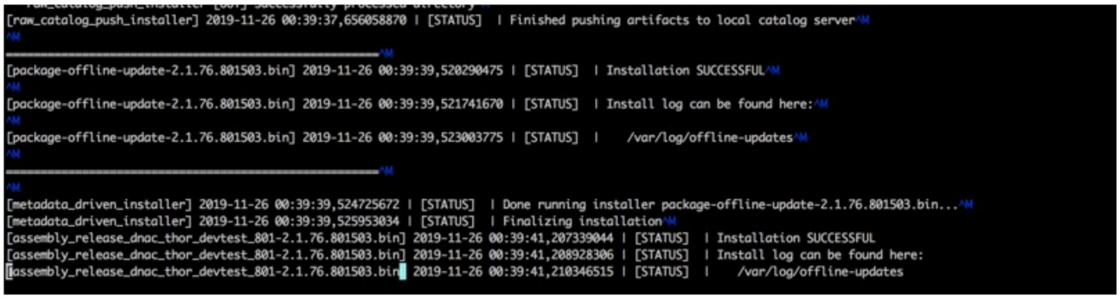
```
sudo ./<uber-bin-file>
```

The command has the following output:

```
$ sudo ./<bin-filename>.bin
[sudo] password for maglev:
=============================
Welcome to DNAC offline update
=============================
Please provide your credentials to get started
[administration] username: admin <Catalyst Center login/password combo>
[administration] password for admin: <Catalyst Center password>
```

Step 4 Executing the binary file updates the local catalog for the system and application packages. Locate the **Installation SUCCESSFUL** status message, which indicates that the bin file executed successfully.

You can track the current status of the process by tailing the log file <*bin-filename*>-install.log. If required, you can also verify the logs under /var/log/offlineupdates/.



```
[raw_catalog_push_installer] 2019-11-26 00:39:37,656058870 | [STATUS]  | Finished pushing artifacts to local catalog server^M
^M
=======================================================^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,520290475 | [STATUS]  | Installation SUCCESSFUL^M
^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,521741670 | [STATUS]  | Install log can be found here:^M
^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,523003775 | [STATUS]  |    /var/log/offline-updates^M
^M
=======================================================^M
^M
[metadata_driven_installer] 2019-11-26 00:39:39,524725672 | [STATUS]  | Done running installer package-offline-update-2.1.76.801503.bin...^M
[metadata_driven_installer] 2019-11-26 00:39:39,525953034 | [STATUS]  | Finalizing installation^M
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,207339044 | [STATUS]  | Installation SUCCESSFUL
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,208928306 | [STATUS]  | Install log can be found here:
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,210346515 | [STATUS]  |    /var/log/offline-updates
```

Perform an Offline Update

This section applies only if you are upgrading from Cisco DNA Center 2.2.2.x or 2.2.3.x to 2.3.3.x.

If you are on a release earlier than 2.2.2.x, you must first upgrade to at least 2.2.2.x before completing the following steps.

Step 1 After successful execution of the binary file, log in to the Cisco DNA Center GUI.

Step 2 From the top-left corner, click the menu icon and choose **System** > **Software Updates**.
A system update appears on the **Software Updates** window. Click **Update**.

Step 3 After the system update is complete, install the Cisco DNA Center 2.3.3.x application packages:

a) From the top-left corner, click the menu icon and choose **System** > **Software Management**.
b) The **Software Management** window indicates that Cisco DNA Center 2.3.3.x is available. Click **Install now**.
c) After Cisco DNA Center completes its prechecks, click **Install**.
d) (Optional) Click the **View Details** link to open a slide-in pane that lists the packages that are being installed and displays their progress.
e) Click the **Currently Installed Applications** link and confirm that each application has been updated.

Update the Knowledge Pack for a PSIRT Scan

Offline Update of Knowledge Pack

An offline knowledge pack update involves the following steps:

1. Download the knowledge pack file.
2. Export the file to USB or other transferrable medium.
3. Import the file to Catalyst Center on an air-gap device.

Download the File

Step 1 Confirm that you are using one of the recommended search engines: Chrome or Firefox.

Step 2 Select the following link to begin downloading:

https://tools.cisco.com/cscrdr/security/center/files/mre/mre_workflow_signed.tar.gz

Export to USB or Other Transferrable Medium

Step 1 Confirm that the file is in .tar.gz format.

Step 2 Transfer the downloaded file to USB (or other medium).

Import to Catalyst Center on an Air-Gap Device

Step 1 Insert the USB into the device.

Step 2 In the Catalyst Center GUI, click the menu icon and choose **System** > **Settings** > **Machine Reasoning**.

Step 3 To import to Catalyst Center, click **Import**.

Step 4 Select the .tar.gz file from the USB to upload.

Download the Latest KGV File for Integrity Verification

Complete the following procedure to download the KGV file you'll use for integrity verification.

Step 1 Using a device with internet access, download the **Cisco_KnownGoodValues.tar** KGV file from the following URL: https://tools.cisco.com/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar.

Step 2 Transfer this file to storage media or a device in your air-gapped environment.

Step 3 Using a device with browser access to your air-gapped Catalyst Center cluster, import the file:

a) On your Catalyst Center cluster, open the following URL in a browser: /dna/systemSettings/settings?settings-item=IntegrityVerficationSettings.

b) Choose **Import New from Local**.

c) Import the KGV file you downloaded in Step 1.

PART IV

Standard Air Gap Deployment: 1.3.3.x to 2.2.2.x

CHAPTER 5

1.3.3.x to 2.2.2.x

Fresh Install from the Catalyst Center ISO Image

Offline Install Workflow

An offline Catalyst Center installation involves the following steps:

1. Download the image.
2. Verify the downloaded file.
3. Create a bootable USB drive.
4. Install the Catalyst Center ISO image.
5. Configure the Catalyst Center appliance.
6. Complete the first-time setup.
7. Accept the device EULA.
8. Install the applications.

Download the Image

You or your Cisco account representative must raise a TAC request. A TAC representative then gives you access and instructions for downloading the ISO file from a Cisco file server.

Step 1 Log in to the Cisco file server, which is accessible via the internet.

Step 2 Download the Catalyst Center ISO image (.iso) from the location specified.

Step 3 Download the Cisco public key (cisco_image_verification_key.pub) for signature verification.

Step 4 Download the secure hash algorithm (SHA512) checksum file for the image.

Step 5 Download the binary image's signature file (.sig).

Verify the Downloaded File

Verify the integrity of the downloaded image using Cisco signature verification and the SHA512 checksum provided on the portal.

Step 1 (Optional) Perform SHA verification to determine whether the ISO image is corrupted due to a partial download.

Depending on your OS, enter one of the following commands:

- Linux:

```
sha512sum Catalyst-Center-image-filename
```

- Mac:

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows does not include a built-in checksum utility, but you can use the certutil tool:

```
certutil -hashfile <filename> sha256 | md5
```

For example:

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

On Windows, you can also use the Windows PowerShell to generate the digest. For example:

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

Compare the output of the command you run to the SHA512 checksum file that you downloaded. If the command output does not match, download the ISO image again and run the appropriate command a second time. If the output still does not match, contact Cisco support.

Step 2 Verify that the ISO image is genuine and from Cisco by verifying its signature:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
signature-filename Catalyst-Center-image-filename
```

This command works in both Mac and Linux environments. For Windows, you must download and install OpenSSL, if you haven't done so already.

If the ISO image is genuine, entering this command displays a **Verified OK** message. If this message fails to appear, do not install the ISO image and contact Cisco support.

Create a Bootable USB Drive

After confirming that you downloaded a Cisco ISO image, create a bootable USB drive that contains the Catalyst Center ISO image. For details, see the "Create a Bootable USB Flash Drive" topic in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide's* "Prepare the Appliance for Configuration" chapter.

Install the Catalyst Center ISO Image

Step 1 Connect the bootable USB drive with the Catalyst Center ISO image to the appliance.

Step 2 Log in to Cisco IMC and start a KVM session.

Step 3 Power on or power cycle the appliance:

- If the appliance is not currently running, choose **Power** > **Power On System**.
- If the appliance is already running, choose **Power** > **Power Cycle System (cold boot)**.

Step 4 In the resulting pop-up window, click **Yes** to acknowledge that you are about to execute a server control action.

Step 5 When the Cisco logo appears, either press the **F6** key or choose **Macros** > **User Defined Macros** > **F6** from the KVM menu. The boot device selection menu appears.

Step 6 Select your USB drive and then press **Enter**.

Step 7 Depending on your Catalyst Center release, do one of the following in the GNU GRUB bootloader window:

- For releases earlier than 2.2.2, choose **Maglev Installer** and then press **Enter**.
- For releases 2.2.2 and later, choose **Cisco DNA Center Installer** and then press **Enter**.

Note The bootloader automatically boots the Maglev installer if you don't make a selection within 30 seconds.

Configure the Catalyst Center Appliance

When installation of the Catalyst Center ISO image completes, the installer reboots and opens the Maglev Configuration wizard's welcome screen. To configure your appliance for day-to-day use in your network, complete the steps described in one of the following sections:

- If you are using the Maglev Configuration wizard, see "Configure the Appliance Using the Maglev Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.
- If you are using the browser-based configuration wizard to configure a 44- or 56-core appliance, see "Configure the 44/56-Core Appliance Using the Browser-Based Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.
- If you are using the browser-based configuration wizard to configure a 112-core appliance, see "Configure the 112-Core Appliance Using the Browser-Based Wizard" in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.

Complete the First-Time Setup

Step 1 After the Catalyst Center appliance reboot is completed, launch your browser.

Step 2 Enter the host IP address to access the Catalyst Center GUI, using HTTPS:// and the IP address of the Catalyst Center GUI that was displayed at the end of the configuration process.

After entering the IP address, one of the following messages appears (depending on your browser):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

Step 3 Ignore the message and click **Advanced**. One of the following messages appears:

- Google Chrome: `This server could not prove that it is` *`GUI-IP-address`*`; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.`
- Mozilla Firefox: `Someone could be trying to impersonate the site and you should not continue. Websites prove their identity via certificates. Firefox does not trust` *`GUI-IP-address`* `because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.`

These messages appear because the controller uses a self-signed certificate. For information on how Catalyst Center uses certificates, see the "Certificate and Private Key Support" section in the *Cisco Catalyst Center Administrator Guide*.

Step 4 Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to <*GUI-IP-address*> (unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

The Catalyst Center **Login** window appears.

Step 5 In the Login window, enter the admin's username (admin) and password that you set when you configured Catalyst Center, then click **Log In**.
The **Reset Login** window appears.

Step 6 Enter the old password, enter and confirm a new password for the admin superuser, and then click **Save**.
The **Enter Cisco.com ID** window appears.

Step 7 (*Skip this step*) Enter the username and password for the cisco.com user, then click **Next**. If the cisco.com user login does not match any known Cisco Smart Account user login, the **Smart Account** window appears.

Step 8 (*Skip this step*) If the **Smart Account** window appears, enter the username and password for your organization's Smart Account, or click the corresponding link to open a new Smart Account. After you are finished, click **Next**.
The **IP Address Manager** window appears.

Step 9 If your organization uses an external IP address manager (IPAM), do the following and then click **Next**:

- Enter your IPAM server's name and URL.
- Enter the username and password required for server access.
- Choose your IPAM provider (such as Infoblox).
- Choose the specific view of IP addresses available in the IPAM server database that you want Catalyst Center to use.

The **Enter Proxy Server** window appears.

Step 10 Click **Next**.
The software **EULA** window appears.

Step 11 Click **Next** to accept the software End User License Agreement and continue.
The **Ready to go!** window appears.

Step 12 We recommend that you click the **User Management** link to display the User Management window. Then click **Add** to begin adding new Catalyst Center users. After you have entered the new user's name and password, and selected the user's role, click **Save** to create the new user. Repeat this as needed until you have added all the new users for your initial deployment. Be sure to create at least one user with the NETWORK-ADMIN-ROLE.

Accept the Device EULA (1.3.3.6 and Earlier)

Complete this procedure for Cisco DNA Center **1.3.3.6** and earlier releases. For **1.3.3.7** and later releases, skip this procedure and go directly to Accept the Device EULA (1.3.3.7 and Later), on page 49.

Step 1 As part of the files that you downloaded, there is a file (<*release_name*>_accept_device_eula) to accept the EULA offline. Locate and download this file, which is available as a separate download and can be installed in the same way as the bundle described previously.

Step 2 After downloading the file, enter the following command to make it executable:

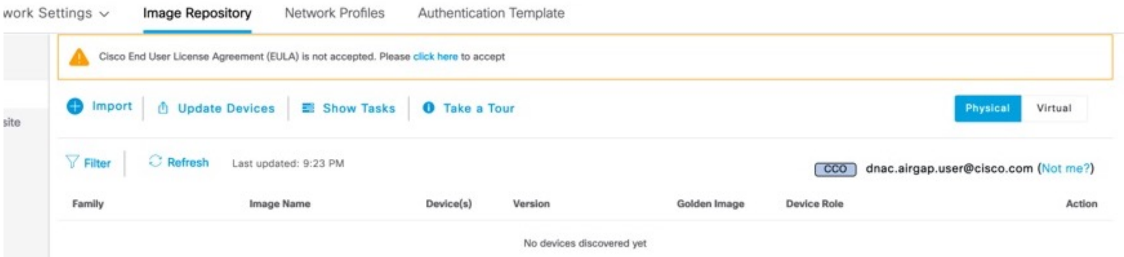
```
chmod +x <release_name>_accept_device_eula
```

Step 3 Enter the following command to run the file:

```
sudo ./ <release_name>_accept_device_eula -Y
```

The **-Y** argument indicates that you are accepting the Catalyst Center software license EULA.

Note In the Cisco DNA Center GUI under **Design** > **Image Repository**, the image EULA is still shown as not accepted, but this is expected and has no functional impact.



Cisco End User License Agreement (EULA) is not accepted. Please click here to accept

Last updated: 9:23 PM

dnac.airgap.user@cisco.com (Not me?)

Family	Image Name	Device(s)	Version	Golden Image	Device Role	Action

No devices discovered yet

Accept the Device EULA (1.3.3.7 and Later)

Complete this procedure only for Cisco DNA Center **1.3.3.7** and later releases.

Step 1 Log in to the Cisco DNA Center cluster and change directories to the desired location. For example:

```
$ cd /mnt/install-artifacts/eula
$ ls
finalize_offline_installation-1.3.0.147.bin
```

Step 2 Change the permissions:

```
$ sudo chmod 755 finalize_offline_installation-1.3.0.147.bin
[sudo] password for maglev:
```

Step 3 Enter the following command:

```
$ sudo ./finalize_offline_installation-1.3.0.147.bin -Y
```

The **-Y** argument indicates that you are accepting the Cisco DNA Center software license EULA.

Note In the Cisco DNA Center GUI under **Design** > **Image Repository**, the image EULA is still shown as not accepted, but this is expected and has no functional impact.

Install the Applications

After completing the preceding tasks, the uber ISO has a number of applications that are loaded and must be installed.

Step 1 In the Catalyst Center GUI, click the gear icon in the top-right corner.

Step 2 Choose **System Settings** > **Software Updates**.

Step 3 Click **Install All**.

Step 4 Click **Continue**.

Step 5 Click **Continue**.

Update from the Catalyst Center Binary Image

Prerequisites

Before upgrading your installed instance of Catalyst Center, review the following prerequisites:

- Ensure that Catalyst Center does not have internet connectivity.
- Only a user with SUPER-ADMIN-ROLE permissions can perform a Catalyst Center software update.
- Create a backup of your Catalyst Center database. For instructions on creating a backup, see the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.
- Have the username and password for a cisco.com user account available for the download. This can be any valid cisco.com user account.
- Allocate enough time for the upgrade process, which 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.

- Use the **df -h** command to verify the disk space:

```
$ df -h
Filesystem        Size  Used Avail Use% Mounted on
udev                                126G     0  126G   0% /dev
tmpfs                               26G   14M   26G   1% /run
/dev/sdb2                           29G   23G  4.5G  84% /
tmpfs                               126G     0  126G   0% /dev/shm
tmpfs                               5.0M     0  5.0M   0% /run/lock
tmpfs                               126G     0  126G   0% /sys/fs/cgroup
/dev/sdb3                           29G   44M   27G   1% /install2
/dev/sdb5                           374G   99G  256G  28% /data
/dev/sdb4                           9.3G  601M  8.2G   7% /var
/dev/sdc1                           420G  1.4G  397G   1%
/data/maglev/srv/fusion
/dev/sdc2                           1.4T   41G  1.3T   4%
/data/maglev/srv/maglev-system
/dev/sdd1                           3.5T  243M  3.3T   1% /data/maglev/srv/ndp
glusterfs-server.maglev-…ault_vol   1.4T   54G  1.3T   5%
/mnt/glusterfs/default_vol
[Fri Jan 10 18:59:27 UTC] maglev@10.82.128.100 (maglev-master-10-82-128-100) /
$
```

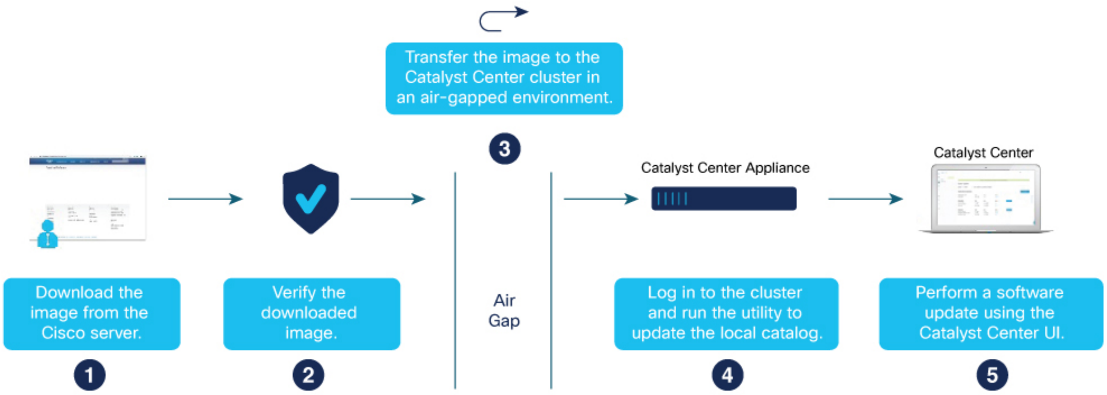
If you receive a storage validation failed error, contact the Cisco TAC.

If the Catalyst Center download, update, or install procedures fail for any reason, always retry the procedure a second time.

Offline Update Workflow

An offline Catalyst Center update involves the following steps:

1. Raise a TAC request to get access to the image for the air gap/offline update.
2. Download the Catalyst Center binary image from a Cisco file server (requires access to the internet).
3. Verify the integrity of the downloaded image.
4. Transfer the downloaded image to the Catalyst Center cluster in the secure, air gap environment.
5. SSH to the Catalyst Center cluster and execute the binary.
6. Log in to the Catalyst Center GUI and perform a system update and an applications update.


Transfer the image to the Catalyst Center cluster in an air-gapped environment.
3
Catalyst Center Appliance
Catalyst Center
Download the image from the Cisco server.
1
Verify the downloaded image.
2
Air Gap
Log in to the cluster and run the utility to update the local catalog.
4
Perform a software update using the Catalyst Center UI.
5

Download the Image

You or your Cisco account representative must raise a TAC request. A TAC representative then gives you access and instructions for downloading the binary image from a Cisco file server.

Step 1 Log in to the Cisco file server, which is accessible via the internet.

Step 2 Download the image from the Cisco file server. This includes the secure hash algorithm (SHA512) checksum file for the image.

Verify the Downloaded File

Verify the integrity of the downloaded image using Cisco signature verification and the SHA512 checksum provided on the portal.

Step 1 Perform SHA verification to determine whether the binary image is corrupted due to a partial download.

Depending on your OS, enter one of the following commands:

- Linux:

```
sha512sum Catalyst-Center-image-filename
```

- Mac:

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows does not include a built-in checksum utility, but you can install a utility from Microsoft at http://www.microsoft.com/en-us/download/details.aspx?id=11533.

Step 2 Compare the command output (or Microsoft Windows utility) to the SHA512 checksum file. If the command output does not match, download the binary image again and enter the appropriate command a second time. If the output still does not match, contact Cisco support.

Transfer the File to Catalyst Center

Step 1 Use a supported file transfer mechanism (SCP or SFTP) to transfer the downloaded image to the Catalyst Center cluster and the /data/tmp partition. When using USB, transfer the image to a terminal in the air-gapped network and then transfer the image to the Catalyst Center cluster and the /data/tmp partition (via SCP or SFTP).

Step 2 After transferring the image to the Catalyst Center cluster, perform SHA verification again to check if the file was corrupted in the process.

Considerations for a Three-Node Cluster

Step 1 For a three-node Catalyst Center cluster, copy the bin file to the node where the catalogserver pod is running.

Step 2 To determine the IP address of the node where the catalog server is running, enter:

```
magctl service status catalogserver | grep Node:
```

For example, the output is similar to the following:

```
$ magctl service status catalogserver | grep Node:
Node: 192.192.192.72/192.192.192.72

[Thu Mar 19 22:59:48 UTC]maglev@192.192.192.68(maglev-master-192-192-192-68) ~
$
```

In this example, copy the bin file to the /data/tmp partition on **192.192.192.72**.

Execute the Binary File

Step 1 Use SSH to log in to the Catalyst Center cluster.

Step 2 Enter the following command to add execute permission:

```
chmod +x <uber-bin-file>
```

Step 3 Enter the following command to execute the binary file:

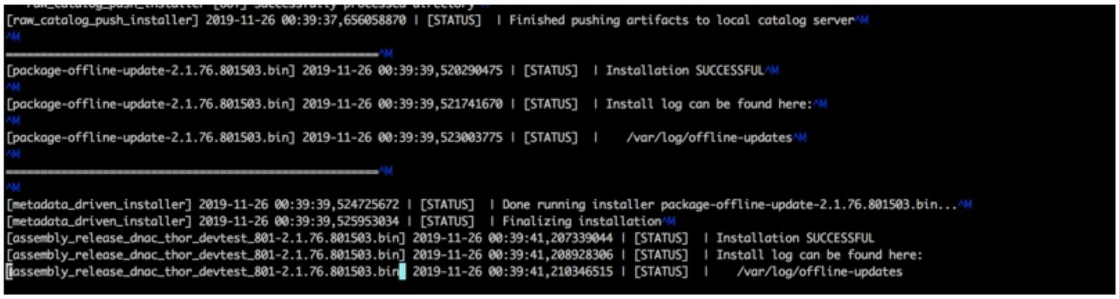
```
sudo ./<uber-bin-file>
```

The command has the following output:

```
$ sudo ./<bin-filename>.bin
[sudo] password for maglev:
=============================
Welcome to DNAC offline update
=============================
Please provide your credentials to get started
[administration] username: admin <Catalyst Center login/password combo>
[administration] password for admin: <Catalyst Center password>
```

Step 4 Executing the binary file updates the local catalog for the system and application packages. Locate the **Installation SUCCESSFUL** status message, which indicates that the bin file executed successfully.

You can track the current status of the process by tailing the log file <*bin-filename*>-install.log. If required, you can also verify the logs under /var/log/offlineupdates/.

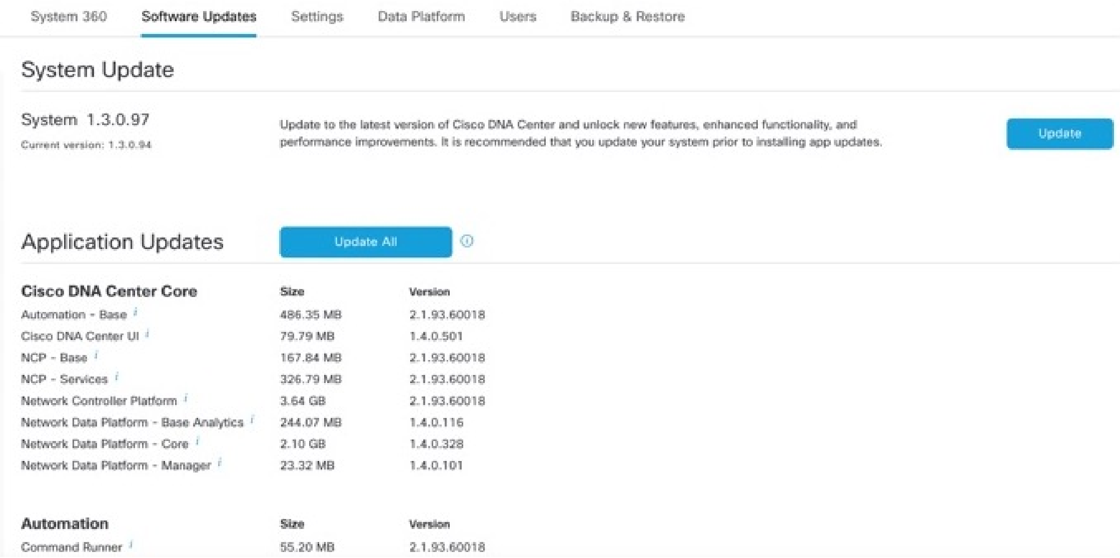


```
[raw_catalog_push_installer] 2019-11-26 00:39:37,656058870 | [STATUS]  | Finished pushing artifacts to local catalog server^M
^M
===============================================================^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,520290475 | [STATUS]  | Installation SUCCESSFUL^M
^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,521741670 | [STATUS]  | Install log can be found here:^M
^M
[package-offline-update-2.1.76.801503.bin] 2019-11-26 00:39:39,523003775 | [STATUS]  |    /var/log/offline-updates^M
^M
===============================================================^M
^M
[metadata_driven_installer] 2019-11-26 00:39:39,524725672 | [STATUS]  | Done running installer package-offline-update-2.1.76.801503.bin...^M
[metadata_driven_installer] 2019-11-26 00:39:39,525953034 | [STATUS]  | Finalizing installation^M
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,207339044 | [STATUS]  | Installation SUCCESSFUL
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin] 2019-11-26 00:39:41,208928306 | [STATUS]  | Install log can be found here:
[assembly_release_dnac_thor_devtest_801-2.1.76.801503.bin 2019-11-26 00:39:41,210346515 | [STATUS]  |    /var/log/offline-updates
```

Perform an Offline Update

Step 1 After successful execution of the binary file, log in to the Catalyst Center cluster GUI and choose **Settings** > **Software Updates** > **Updates**.

Step 2 A system update appears on the **Software Updates** window. Click **Update**.



System Update

System 1.3.0.97

Current version: 1.3.0.94

Update to the latest version of Cisco DNA Center and unlock new features, enhanced functionality, and performance improvements. It is recommended that you update your system prior to installing app updates.

Application Updates

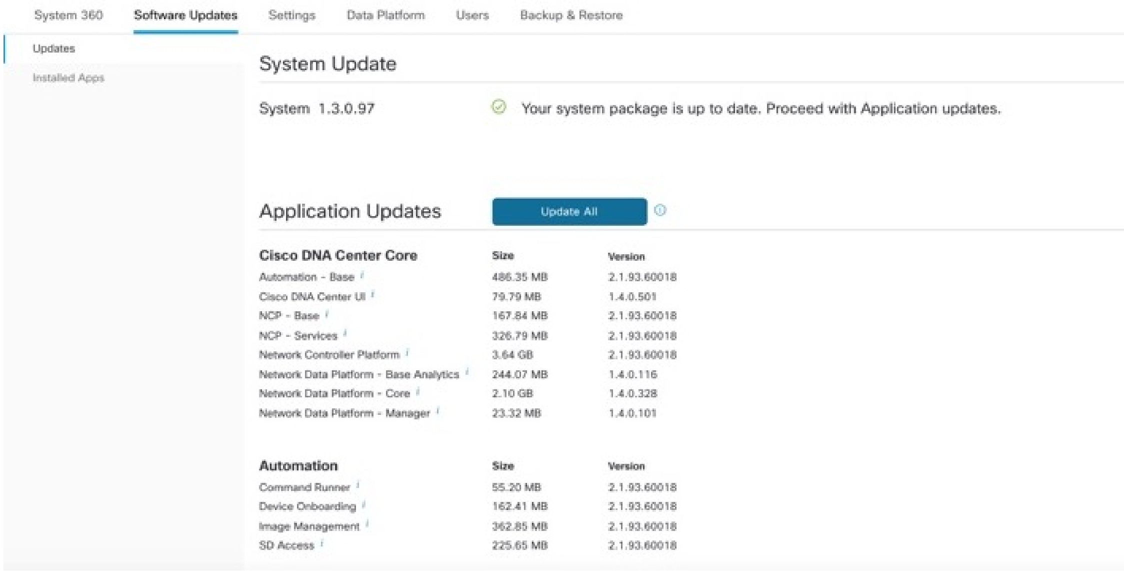
Cisco DNA Center Core	Size	Version
Automation - Base	486.35 MB	2.1.93.60018
Cisco DNA Center UI	79.79 MB	1.4.0.501
NCP - Base	167.84 MB	2.1.93.60018
NCP - Services	326.79 MB	2.1.93.60018
Network Controller Platform	3.64 GB	2.1.93.60018
Network Data Platform - Base Analytics	244.07 MB	1.4.0.116
Network Data Platform - Core	2.10 GB	1.4.0.328
Network Data Platform - Manager	23.32 MB	1.4.0.101

Automation	Size	Version
Command Runner	55.20 MB	2.1.93.60018

After a successful update, you see the following message:

```
Your system package is up to date. Proceed with Application updates.
```

Step 3 (Make sure your system is up to date before proceeding with this step). After all application packages are downloaded, at the top of the Application Updates area, click **Update All**.



System Update

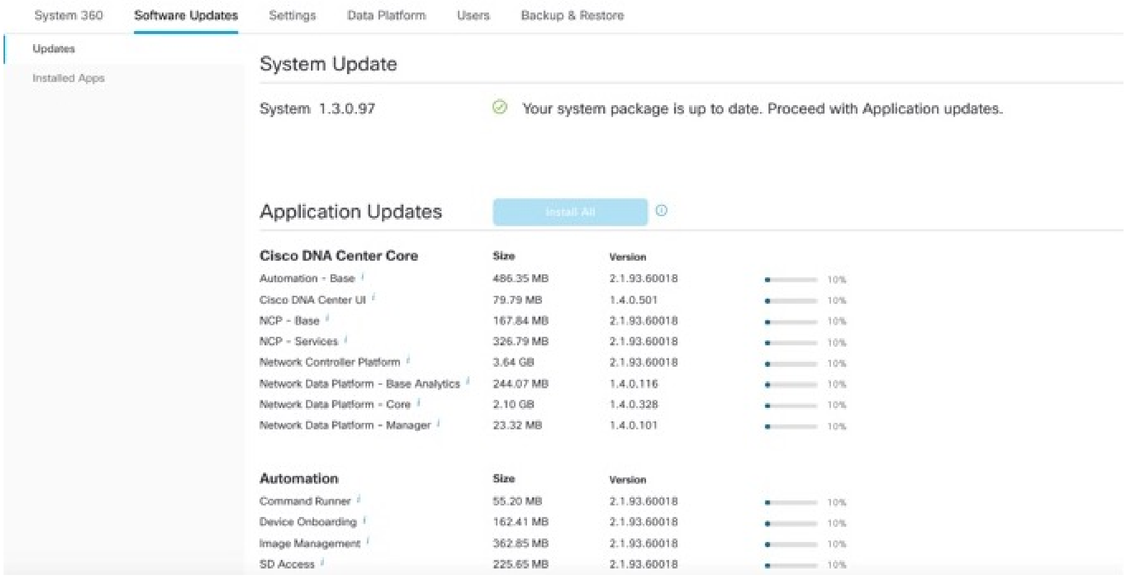
System 1.3.0.97 — Your system package is up to date. Proceed with Application updates.

Application Updates

Cisco DNA Center Core	Size	Version
Automation - Base	486.35 MB	2.1.93.60018
Cisco DNA Center UI	79.79 MB	1.4.0.501
NCP - Base	167.84 MB	2.1.93.60018
NCP - Services	326.79 MB	2.1.93.60018
Network Controller Platform	3.64 GB	2.1.93.60018
Network Data Platform - Base Analytics	244.07 MB	1.4.0.116
Network Data Platform - Core	2.10 GB	1.4.0.328
Network Data Platform - Manager	23.32 MB	1.4.0.101

Automation	Size	Version
Command Runner	55.20 MB	2.1.93.60018
Device Onboarding	162.41 MB	2.1.93.60018
Image Management	362.85 MB	2.1.93.60018
SD Access	225.65 MB	2.1.93.60018

The packages begin updating.



System Update

System 1.3.0.97 — Your system package is up to date. Proceed with Application updates.

Application Updates

Cisco DNA Center Core	Size	Version	
Automation - Base	486.35 MB	2.1.93.60018	10%
Cisco DNA Center UI	79.79 MB	1.4.0.501	10%
NCP - Base	167.84 MB	2.1.93.60018	10%
NCP - Services	326.79 MB	2.1.93.60018	10%
Network Controller Platform	3.64 GB	2.1.93.60018	10%
Network Data Platform - Base Analytics	244.07 MB	1.4.0.116	10%
Network Data Platform - Core	2.10 GB	1.4.0.328	10%
Network Data Platform - Manager	23.32 MB	1.4.0.101	10%

Automation	Size	Version	
Command Runner	55.20 MB	2.1.93.60018	10%
Device Onboarding	162.41 MB	2.1.93.60018	10%
Image Management	362.85 MB	2.1.93.60018	10%
SD Access	225.65 MB	2.1.93.60018	10%

Step 4 Ensure that each application has been updated by reviewing its version in the **Installed Apps** window.

Update the Knowledge Pack for a PSIRT Scan

Offline Update of Knowledge Pack

An offline knowledge pack update involves the following steps:

1. Download the knowledge pack file.
2. Export the file to USB or other transferrable medium.
3. Import the file to Catalyst Center on an air-gap device.

Download the File

Step 1 Confirm that you are using one of the recommended search engines: Chrome or Firefox.

Step 2 Select the following link to begin downloading:

https://tools.cisco.com/cscrdr/security/center/files/mre/mre_workflow_signed.tar.gz

Export to USB or Other Transferrable Medium

Step 1 Confirm that the file is in .tar.gz format.

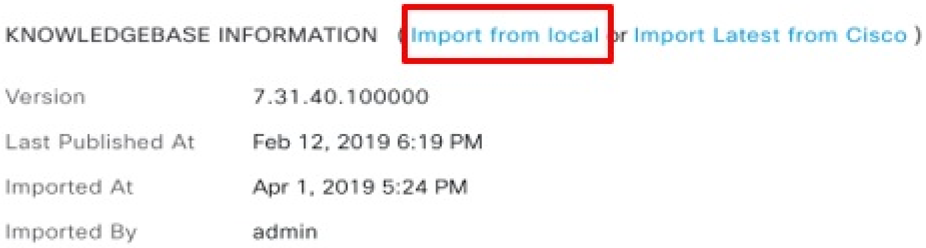
Step 2 Transfer the downloaded file to USB (or other medium).

Import to Catalyst Center on an Air-Gap Device

Step 1 Insert the USB into the device.

Step 2 From the Catalyst Center home page, click the gear icon and choose **System Settings** > **Settings** > **Machine Reasoning**.

Step 3 To import to Catalyst Center, click **Import from local**, shown as follows:



KNOWLEDGEBASE INFORMATION (Import from local or Import Latest from Cisco)

Version	7.31.40.100000
Last Published At	Feb 12, 2019 6:19 PM
Imported At	Apr 1, 2019 5:24 PM
Imported By	admin

Step 4 Select the .tar.gz file from the USB to upload.

Download the Latest KGV File for Integrity Verification

Complete the following procedure to download the KGV file you'll use for integrity verification.

Step 1 Using a device with internet access, download the **Cisco_KnownGoodValues.tar** KGV file from the following URL: https://tools.cisco.com/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar.

Step 2 Transfer this file to storage media or a device in your air-gapped environment.

Step 3 Using a device with browser access to your air-gapped Catalyst Center cluster, import the file:

a) On your Catalyst Center cluster, open the following URL in a browser: /dna/systemSettings/settings?settings-item=IntegrityVerficationSettings.

b) Choose **Import New from Local**.

c) Import the KGV file you downloaded in Step 1.

APPENDIX A

References

- Related Documentation, on page 59

Related Documentation

- Cisco DNA Center Administration Guide
- Cisco DNA Center User Guide
- Smart Software Manager On-Prem User Guide