Release Notes for Cisco DNA Center, Release 1.2.6

First Published: 2018-10-31

Last Modified: 2019-07-19

Release Notes for Cisco Digital Network Architecture Center, Release 1.2.6

We are pleased to announce the availability of Cisco DNA Center, Release 1.2.6 to further accelerate the intent-based networking journey for our customers. The new release contains support for SD-Access native fabric multicast, plus quality improvements in the areas of installation and upgrade, platform stability, and bug fixes.

Cisco DNA Center 1.2.6 is now the recommended release for all customers who are ready to move from laboratory trials into a production environment, or new customers who are just starting on the intent-based networking journey with Cisco DNA Center.

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 1.2.6.

Change History

The following table lists changes to this document since its initial release.

Table 1: Document Change History

Date	Change	Location
2019-07-19	Clarified that you can back up and restore Automation data only or both Automation and Assurance data. But you cannot use the GUI or the CLI to back up or restore only Assurance data.	Limitations and Restrictions, on page 19
2018-10-31	Initial release.	—

Guidance for New and Existing Deployments

- New customers: Go directly to Cisco DNA Center 1.2.6 via the cloud update.
- Existing SD-Access production deployments on 1.2.x: Upgrade to Cisco DNA Center 1.2.6 via the cloud update.
- Existing Assurance/non-fabric deployments on 1.2.x: Upgrade to Cisco DNA Center 1.2.6 only if you want to benefit from the quality improvements in this release.

- Earlier production deployments (both SD-Access and Assurance) on 1.1.x: Upgrade to Cisco DNA Center 1.2.6 after an assessment of your migration requirements with the Cisco TAC. This is to ensure a smooth migration given the number of changes from 1.1.x to 1.2.x. See Get Assistance from the Cisco TAC, on page 21.

Note We recommend that all customer deployments on Release 1.1.6 or earlier (SDA or non-SDA) upgrade first to Cisco DNA Center 1.1.8. Contact the TAC if you are on a release earlier than Cisco DNA Center 1.1.8.

Compatible Browsers

The Cisco DNA Center web interface is compatible with the following HTTPS-enabled browsers:

- Google Chrome: version 62.0 or later
- Mozilla Firefox: version 54.0 or later

We recommend that the client systems you use to log in to Cisco DNA Center be equipped with 64-bit operating systems and browsers.

SD-Access Compatibility Matrix

For information on SD-Access hardware and software support for Cisco DNA Center 1.2.6, see the SD-Access 1.2.x Hardware and Software Compatibility Matrix.

What's New in Cisco DNA Center, Release 1.2.6

Cisco DNA Center, Release 1.2.6 resolves several pre-existing issues and is designed to enhance your product's performance and stability.

Table 2: Updated Packages and Versions in This Release

Update Type	Package Name	Version
System Updates	System	1.1.0.659

Update Type	Package Name	Version
Package Updates	Application Policy	2.1.23.170130
	Assurance - Base	1.2.6.63
	NCP - Services	2.1.24.60052
	Automation - Base	2.1.24.60052
	Command Runner	2.1.24.60052
	Device Onboarding	2.1.24.60052
	Device Onboarding UI	2.1.23.60287
	Cisco DNA Center Platform	1.0.4.14
	Automation - Intelligent Capture	2.1.24.60052
	Image Management	2.1.24.60052
	NCP - Base	2.1.23.60287
	Network Data Platform - Base Analytics	1.1.7.590
	Network Data Platform - Core	1.1.7.765
	Network Data Platform - Manager	1.1.7.645
	Network Controller Platform	2.1.24.60052
	Path Trace	2.1.24.60052
	Cisco DNA Center UI	1.2.0.55
	SD Access	2.1.24.60052
	Assurance - Sensor	1.2.6.76
	Automation - Sensor	2.1.24.60052

RFC 6598 Support

By adding support of the IETF RFC 6598 specification for private networks, Cisco DNA Center now supports the 100.64.0.0/10 IP address range. For more information on this specification, see RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space.

What's New in SD-Access

The following table lists the new software features in SD-Access 1.2.6.

Table 3: New Software Features in SDA Release 1.2.6

Feature	Description	Platforms and Images Supported
Native Fabric Multicast	Currently, multicast SD-Access offers limited scale because of head-end replication in the fabric overlay. It is suited for small-scale deployments. With native multicast, the load of replicating multicast traffic is distributed in the underlay, making it more efficient for multicast traffic handling. This feature enables multicast in the underlay using multicast trees. The overlay multicast traffic uses the underlay multicast tree as the core transport for traffic. Layer 3 multicast traffic through the underlay uses Protocol Independent Multicast source-specific mode (PIM-SSM). Each multicast group in the overlay is mapped to a multicast group in the underlay and the traffic is forwarded using the underlay group.	• Cisco Catalyst 3000 Series Switches: IOS XE 16.9.2 • Cisco Catalyst 6000 Series Switches: IOS 15.5(1)SY2 • Cisco Catalyst 9000 Series Switches: IOS XE 16.9.2 • Cisco ASR 1000 Router Series: IOS XE 16.9.1s • Cisco CSR 1000 Router Series: IOS XE 16.9.1s • Cisco ISR 4000 Router Series: IOS XE 16.9.1s

Beta Features

The following features in this release are in beta or are being released as an engineering field trial (EFT):

- High Availability
- SD-Access Extension for IoT
- Network Plug and Play application
- Intelligent Capture support
- Skype for Business Application Experience

Cisco DNA Center Scale

For Cisco DNA Center scale numbers, see the Cisco DNA Center Data Sheet.

IP Address and FQDN Firewall Requirements

To determine the IP addresses and fully qualified domain names (FQDNs) that must be made accessible to Cisco DNA Center through any existing network firewall, see "Required Internet URLs and FQDNs" in the *Cisco Digital Network Architecture Center Installation Guide*.

Installing Cisco DNA Center

You install Cisco DNA Center as a dedicated physical appliance purchased from Cisco with the Cisco DNA Center ISO image preinstalled. Refer to the Cisco DNA Center Installation Guide for information about installation and deployment procedures.

Note The following applications are not installed on Cisco DNA Center by default. If you need any of these applications, you must manually download and install the packages separately.

- SD Access
- Assurance - Sensor
- Automation - Sensor
- Application Policy
- Device Onboarding UI (for Cisco Plug and Play)
- Cisco DNA Center platform

For more information about downloading and installing a package, see the "Manage Applications" chapter in the Cisco DNA Center Administrator Guide.

Border Node Requirements on Cisco Nexus 7700 Series Switches

To configure a Cisco Nexus 7700 Series Switch as a border, ensure that the following actions are performed:

- A valid MPLS_PKG license is installed on the switch.
- The **install feature-set fabric** and **install feature-set mpls** commands are enabled in the Admin VDC or in the default VDC if Admin VDC is not present.

Note Only Cisco Nexus 7700 Series Switch with M3 line card supports the border role.

Prerequisites for Upgrading to Cisco DNA Center, Release 1.2.6

You can perform the package updates only after completing the system updates. Do not attempt to either download or install package updates until all system updates have been installed. Failure to download and install system updates first can cause problems with package updates.

Note You cannot upgrade the packages individually. You must follow all the steps in this procedure.

Before you upgrade, make sure the cluster link interface is connected to a switch port and is in the up state.

Review the following list of prerequisites and perform the following procedures before upgrading your installed instance of Cisco DNA Center:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see the Cisco Digital Network Architecture Center Administrator Guide.
- You can upgrade to this Cisco DNA Center release from the following releases only:
  - Cisco DNA Center 1.2.5 (October 1, 2018)

- Cisco DNA Center 1.2.4 (September 10, 2018)
- Cisco DNA Center 1.2.3 (August 10, 2018)
- Cisco DNA Center 1.2.2 (July 12, 2018)
- Cisco DNA Center 1.2.1 (June 15, 2018)
- Cisco DNA Center 1.2 (June 5, 2018)
- Cisco DNA Center 1.1.8 (July 17, 2018)
- Cisco DNA Center 1.1.7 (June 9, 2018)
- Cisco DNA Center 1.1.6 (May 18, 2018)

Important You must contact the Cisco TAC for help with upgrading from Cisco DNA Center 1.1.x to 1.2.6.

Note Do not perform any activities on the cluster until after both the system (platform) and application updates are complete. After the system update is installed, the GUI displays "complete." Before you choose **Download All**, you must ensure all services are up and running, which might take 10 to 15 minutes after the system upgrade has completed. Before choosing the **Download All** option, SSH to the Cisco DNA Center cluster IP with the Linux username (**maglev**) and the password that was configured for the maglev user. Then, enter the following command and make sure no results are returned:

```
magctl appstack status | grep 0/
```

If results are returned, it means services are disrupted and the system is working to restore services. If services are not restored within 20 minutes, contact the Cisco TAC.

- Create a backup of your Cisco DNA Center database. For information about backing up and restoring, see the Cisco Digital Network Architecture Center Administrator Guide.
- If you have a firewall, make sure you allow Cisco DNA Center to access the following location for all system and package downloads: https://www.ciscoconnectdna.com:443. To ensure that you have cloud connectivity to AWS, log in to the cluster and run the following CLI command: **maglev catalog settings validate**. For more information, see the Cisco Digital Network Architecture Center Installation Guide.
- Have the username and password for at least one cisco.com user account. You might be prompted, once, for the account credentials during package installations. This can be any valid cisco.com user account.
- Allocate the appropriate time for the upgrade process. Upgrading from Cisco DNA Center 1.2.x can take approximately 6 hours to complete. If you are upgrading from Cisco DNA Center 1.1.x, you can expect the upgrade to take considerably longer.
- We strongly recommend that you do not use Cisco DNA Center or any of its applications or tools when it is in the process of being upgraded.

- Before you upgrade, make sure that there are no packages with the status **installing** or **downloading**. The packages displayed should have a status of **running**.
  - For upgrades from Cisco DNA Center 1.1.6, 1.1.7, or 1.1.8, check the ⚙ > **System Settings** > **App Management** > **Packages & Updates** page for package status.
  - For upgrades from Cisco DNA Center 1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4, or 1.2.5, check the ⚙ > **System Settings** > **Software Updates** > **Updates** page for package status.
- If the Cisco DNA Center download, update, or install procedures fail for any reason, always retry the procedure a second time using the GUI. If the procedure fails a second time, contact Cisco TAC for support.

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

Note If you upgrade a three-node Cisco DNA Center cluster from any version of 1.2.x, the application upgrade will fail its dependency checks. To upgrade a three-node (multihost) cluster, Service Distribution (or HA) must be enabled. Be aware that Service Distribution (or HA) for a three-node cluster is a beta feature and is not recommended for use in production deployments. You must contact the Cisco TAC for help with upgrading a three-node cluster.

Upgrading from Release 1.1.6, 1.1.7, or 1.1.8 to Release 1.2.6

Procedure

Step 1 From the Cisco DNA Center home page, choose ⚙ > **System Settings** > **App Management**.

A **Cisco DNA Center 1.2.6 is Here!** banner appears at the top of the **App Management** page with a **Switch Now** button.

The **App Management** page also displays the following side tabs:

- **Packages & Updates**: Shows the packages currently installed and updates available for installation from the Cisco cloud.
- **System Updates**: Shows the System updates currently installed and updates available for installation from the Cisco cloud.

Step 2 Click **Switch Now** in the banner.

Step 3 At the prompt, click **OK** to proceed with the upgrade.

Clicking **OK** changes the release train in the back end. The message "Connecting to... 1.2.6 cloud catalog" with a progress bar appears.

Wait for approximately 90 seconds for the progress bar to finish and the updated system version to display. Refresh the page if the new system version does not appear.

Step 4 After the release train change finishes, review the **System Updates** page.

The following information is displayed:

- **Package**: System package
- **Status**: Running
- **Installed Version**: Current Cisco DNA Center system package installed
- **Available Update**: System package available for installation

Step 5 Click **Install** in the **Available Update** column.

During the install process, the following Cisco DNA Center GUI changes are made:

- **App Management** tab: Changes to the **Software Updates** tab
- **System Updates** side panel: Changes to the **Updates** side panel
- **Packages & Updates** side panel: Changes to the **Installed Apps** side panel

Step 6 After the system installation is finished and is in **Running** state, refresh the page.

A new **Updates** page displays the following information:

- **Platform Update**: Displays the updated system version with a statement that the system is currently up to date. Additionally, a green check mark indicates a successful system upgrade.
- **Apps Updates**: Displays groupings of applications with their current file size and version.

Note After performing system updates, clear the browser cache and log in to Cisco DNA Center 1.2.6 again.

Step 7 At the top of the **Apps Updates** field, click the **Download All** button.

After clicking this button, all the application upgrade packages are downloaded.

Note There are additional **Download All** buttons for different application groups (for example, **Cisco DNA Center Core**, **Automation**, and **Assurance**). These buttons are dimmed and disabled. You need to only click the **Download All** button at the top of the page.

Step 8 After all of the application packages have been downloaded, click the **Update All** button at the top of the **Apps Updates** field.

After clicking this button, all of the applications are subsequently updated.

Note There are additional **Update All** buttons for different application groups (for example, **Cisco DNA Center Core**, **Automation**, and **Assurance**). These buttons are dimmed and disabled. You need to only click the **Update All** button at the top of the page.

Step 9 Ensure that each application has been updated by reviewing its version in the **Installed Apps** page.

The application versions should be updated in this page.

Note There may be some new application packages that were not part of your previous Cisco DNA Center configuration, and for this reason have not been installed by this procedure (for example, the Test Support package listed on this page).

Upgrading from Release 1.2, 1.2.1, 1.2.2, 1.2.3, or 1.2.4 to Release 1.2.6

Procedure

Step 1 From the Cisco DNA Center home page, choose ⚙ > **System Settings** > **Software Updates**.

A **Cisco DNA Center 1.2.6 is Here!** banner appears at the top of the **Software Updates** page with a **Switch Now** button.

Step 2 Click **Switch Now** in the banner.

Step 3 At the prompt, click **OK** to proceed with the upgrade.

Step 4 If a system update appears on the **Software Updates** page, click **Update**.

Step 5 Download the applications by doing one of the following:

- To download all applications at once, click **Download All** at the top of the **Application Updates** field.
- To download a specific application group, click **Download All** next to that group.
- To download a specific application, click **Download** next to that application.

Step 6 Update the applications by doing one of the following:

- To update all applications at once, click **Update All** at the top of the **Application Updates** field.
- To update a specific application group, click **Update All** next to that group.
- To update a specific application, click **Update** next to that application.

Step 7 Ensure that each application has been updated by reviewing its version in the **Installed Apps** page.

The application versions should be updated on this page.

Note There may be some new application packages that were not part of your previous Cisco DNA Center configuration, and for this reason have not been installed by this procedure (for example, the Test Support package listed on this page).

Upgrading from Release 1.2.5 to Release 1.2.6

Procedure

Step 1 From the Cisco DNA Center home page, choose ⚙ > **System Settings** > **Software Updates**.

Step 2 You will see a system update for 1.2.6; accept the update, download the 1.2.6 packages, and upgrade to 1.2.6.

- Download the applications by doing one of the following:
  - To download all applications at once, click **Download All** at the top of the **Application Updates** field.
  - To download a specific application group, click **Download All** next to that group.

- To download a specific application, click **Download** next to that application.

- Update the applications by doing one of the following:
  - To update all applications at once, click **Update All** at the top of the **Application Updates** field.
  - To update a specific application group, click **Update All** next to that group.
  - To update a specific application, click **Update** next to that application.

Step 3 Ensure that each application has been updated by reviewing its version in the **Installed Apps** page.

Recover from Premature Package Downloads

Successful migration to this release requires that you install all system updates before downloading or installing package updates. Due to dependencies among the updates, failure to observe this rule can make it impossible to install both system updates and package updates. Problem indicators include messages that a system update has failed and package update downloads that never exit the "Downloading" state.

As an admin user with Maglev SSH access privileges, complete the following steps to recover and install the system update.

Procedure

Step 1 Using an SSH client, log in to the Cisco DNA Center appliance using the IP address of the out-of-band management network adapter, on port 2222. Use the **maglev login** command and log in with an admin username and password (which is the same login used for the admin user on the Cisco DNA Center GUI).

Step 2 At the command line, delete all prematurely downloaded package updates by entering the following command:

```
for pkg in $(maglev package status -o json | jq -r '.[] | select(.available!="-") | [
.name,.available | tostring ] | join (":")'); do maglev catalog package delete $pkg
2>/dev/null; done
```

Important You must enter the preceding command as one line.

Step 3 Trigger the downloaded system update from the Cisco DNA Center GUI.

Step 4 After the system update installs successfully, download and install the package updates.

Supported ISE Version

Cisco DNA Center 1.2.6 uses Cisco ISE Version 2.3 patch 2 for both user authentication and access control. Ensure that Cisco DNA Center and Cisco ISE are integrated as described in the Cisco Digital Network Architecture Center Installation Guide.

Cisco DNA Center Platform Support

For information about Cisco DNA Center platform, including information about new features, installation, upgrade, and open and resolved bugs, see the separate Cisco DNA Center Platform Release Notes.

CMX Support

Cisco DNA Center supports the following CMX versions:

- CMX 10.4.1
- CMX 10.5.0

Network Plug and Play Considerations

Network Plug and Play Support

The Network Plug and Play application is not installed in Cisco DNA Center by default. You must download and install the package named Device Onboarding UI, and then you can find the application in the Tools section. For more information about installing a package, see the chapter "Manage Applications" in the Cisco Digital Network Architecture Center Administrator Guide.

General Feature Support

Network Plug and Play supports the following features, depending on the Cisco IOS software release on the device:

- AAA device credential support: The AAA credentials are passed to the device securely and the password is not logged. This feature allows provisioning a device with a configuration that contains aaa authorization commands. This feature requires software release IOS 15.2(6)E1, IOS 15.6(3)M1, IOS XE 16.3.2, or IOS XE 16.4 or later on the device.
- Image install and upgrade for Cisco Catalyst 9300 Series, Catalyst 9400 Series, Catalyst 9500 Series, Catalyst 3650 Series, and Catalyst 3850 Series switches is supported only when the switch is booted in Install mode. (Image install and upgrade is not supported for switches booted in Bundle mode.)

SUDI Support

The Secure Unique Device Identifier (SUDI) feature that allows secure device authentication is available on the following platforms:

- Cisco routers:
  - Cisco ISR 1100 Series with software release 16.6.2
  - Cisco ISR 4000 Series with software release 3.16.1 or later, except for the ISR 4221, which requires release 16.4.1 or later
  - Cisco ASR 1000 Series (except for the ASR 1002-x) with software release 16.6.1
- Cisco switches:
  - Cisco Catalyst 3850 Series with software releases 3.6.3E or 16.1.2E or later
  - Cisco Catalyst 3650 Series and 4500 Series with Supervisor 7-E/8-E, with software releases 3.6.3E, 3.7.3E, or 16.1.2E or later
  - Cisco Catalyst 4500 Series with Supervisor 8L-E with software releases 3.8.1E or later
  - Cisco Catalyst 4500 Series with Supervisor 9-E with software release 3.10.0E or later

- Cisco Catalyst 9300 Series with software release 16.6.1 or later
- Cisco Catalyst 9400 Series with software release 16.6.1 or later
- Cisco Catalyst 9500 Series with software release 16.6.1 or later

- NFVIS platforms:
  - Cisco ENCS 5400 Series with software release 3.7.1 or later
  - Cisco ENCS 5104 with software release 3.7.1 or later

Note Devices that support SUDI have two serial numbers: the chassis serial number and the SUDI serial number (called the License SN on the device label). You must enter the SUDI serial number in the Serial Number field when adding a device that uses SUDI authentication. The following device models have a SUDI serial number that is different from the chassis serial number:

- Cisco routers: ISR 43xx, ISR 44xx, ASR1001-X/HX, ASR1002-HX
- Cisco switches: Catalyst 4500 Series with Supervisor 8-E/8L-E/9-E, Catalyst 9400 Series

Management Interface VRF Support

Plug and Play operates over the device management interface on the following platforms:

- Cisco routers:
  - Cisco ASR 1000 Series with software release 16.3.2 or later
  - Cisco ISR 4000 Series with software release 16.3.2 or later

- Cisco switches:
  - Catalyst 3650 Series and 3850 Series with software release 16.6.1 or later
  - Cisco Catalyst 9300 Series with software release 16.6.1 or later
  - Cisco Catalyst 9400 Series with software release 16.6.1 or later
  - Cisco Catalyst 9500 Series with software release 16.6.1 or later

4G Interface Support

Plug and Play operates over a 4G network interface module on the following Cisco routers:

- Cisco 1100 Series ISR with software release 16.6.2 or later

Configuring Server Identity

To ensure successful Cisco DNA Center discovery by Cisco devices running newer IOS releases, the server SSL certificate offered by Cisco DNA Center during the SSL handshake must contain an appropriate Subject Alternate Name (SAN) value, so that the Cisco Plug and Play IOS Agent can verify the server identity. This

may require the administrator to upload a new server SSL certificate, which has the appropriate SAN values, to Cisco DNA Center.

This requirement applies to devices running the following Cisco IOS releases:

- Cisco IOS Release 15.2(6)E2 and later
- Cisco IOS Release 15.6(3)M4 and later
- Cisco IOS Release 15.7(3)M2 and later
- Cisco IOS XE Denali 16.3.6 and later
- Cisco IOS XE Everest 16.5.3 and later
- Cisco IOS Everest 16.6.3 and later
- All Cisco IOS releases from 16.7.1 and later

The value of the SAN field in the Cisco DNA Center certificate must be set according to the type of discovery being used by devices, as follows:

- For DHCP option-43/option-17 discovery using an explicit IPv4 or IPv6 address, set the SAN field to the specific IPv4/IPv6 address of Cisco DNA Center.
- For DHCP option-43/option-17 discovery using a hostname, set the SAN field to the Cisco DNA Center hostname.
- For DNS discovery, set the SAN field to the plug and play hostname, in the format pnpserver.*domain*.
- For Cisco Plug and Play Connect cloud portal discovery, set the SAN field to the Cisco DNA Center IP address, if the IP address is used in the Plug and Play Connect profile. If the profile uses the Cisco DNA Center hostname, then the SAN field must be set to the fully qualified domain name (FQDN) of the controller.

If the Cisco DNA Center IP address that is used in the Plug and Play profile is a public IP address that is assigned by a NAT router, then this public IP address must be included in the SAN field of the server certificate.

If an HTTP proxy server is used between the devices and Cisco DNA Center, ensure that the proxy certificate has the same SAN fields with the appropriate IP address or hostname.

We recommend that you include multiple SAN values in the certificate, in case discovery methods vary. For example, you can include both the Cisco DNA Center FQDN and IP address (or NAT IP address) in the SAN field. If you do include both, set the FQDN as the first SAN value, followed by the IP address.

If the SAN field in the Cisco DNA Center certificate does not contain the appropriate value, the device cannot successfully complete the plug and play process.

Note The Cisco Plug and Play IOS Agent checks only the certificate SAN field for the server identity. It does not check the common name (CN) field.

Important Notes

Update Telemetry Profiles to Use a New Cluster Virtual IP Address

If you are using the Cisco DNA Center Telemetry tool to monitor device data, and you need to change the Cisco DNA Center cluster virtual IP address (VIP), complete the following steps to change the VIP and to ensure that node telemetry data is sent to the new VIP.

Before you begin

You need the following:

- Determine whether the version of Cisco DNA Center you are using is in the 1.1.x or 1.2.x release train. You can check this by logging in to the Cisco DNA Center web interface and using the **About** option to check the Cisco DNA Center version number. For example, if the version you are using begins with "1.1," it is in the 1.1.x release train.
- SSH client software.
- The VIP address that was configured for the 10 GB interface facing the enterprise network on the Cisco DNA Center primary node. You log in to the appliance at this address, on port 2222. To identify this port, see the rear-panel figure in the "Front and Rear Panels" section in the Cisco DNA Center Installation Guide.
- The Linux username (**`maglev`**) and password configured on the primary node.
- The cluster VIP that you want to assign. The cluster VIP must conform to the requirements explained in the "Required IP Addresses and Subnets" section in the Cisco DNA Center Installation Guide.

Procedure

Step 1 Access the Cisco DNA Center GUI and use the Cisco DNA Center Telemetry tool to push the Disabled profile to all nodes, as follows:

a) From the Cisco DNA Center home page, click **Telemetry** in **Tools**.
b) Click the **Site View** tab.
c) In the **Site View** table in this tab, choose all the sites and devices currently being monitored.
d) Click the **Actions** button and choose the **Disable Telemetry** profile from the drop-down list.
e) Wait for the **Site View** table to show that telemetry has been disabled for the selected sites and devices.

Step 2 Use the appliance Configuration wizard to change the cluster VIP, as follows:

a) Using an SSH client, log in to the VIP address that was configured for the 10 GB interface facing the enterprise network on the Cisco DNA Center primary node. Be sure to log in on port 2222.
b) When prompted, enter the Linux username and password.
c) Enter the following command to access the Configuration wizard on the primary node:

```
$ sudo maglev-config update
```

If prompted for the Linux password, enter it again.

d) Click **[Next]** until the screen prompting you for the cluster virtual IP appears. Enter the new cluster VIP, then click **[Next]** to proceed through the remaining screens of the Configuration wizard.

e) When you reach the final screen, a message appears stating that the Configuration wizard is ready to apply your changes. Click **[proceed]** to apply the cluster VIP change.

At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears and the SSH prompt reappears.

Step 3 Restart the necessary Cisco DNA Center services by entering the following series of commands at the SSH prompt. Use the commands for the release train appropriate for your Cisco DNA Center version.

For versions of Cisco DNA Center in the 1.1.x release train (versions 1.1.1 and later, up to but not including 1.2.0), enter the following series of commands:

```
magctl service restart -d netflow-go
magctl service restart -d syslog
magctl service restart -d trap
magctl service restart -d wirelesscollector
```

For Cisco DNA Center in the 1.2.x release train (versions 1.2.0 and later), enter the following series of commands:

```
magctl service restart -d collector-netflow
magctl service restart -d collector-syslog
magctl service restart -d collector-trap
magctl service restart -d wirelesscollector
```

Step 4 Wait for all services to restart. You can monitor the progress of the restarts by entering the following command, substituting service names as needed for the release train appropriate for your Cisco DNA Center version. For example, if you are using a version of Cisco DNA Center in the 1.2.x release train, enter the following command:

```
magctl appstack status | grep -i -e collector-netflow -e collector-syslog -e collector-trap
 -e wirelesscollector
```

When all necessary services are running, you see command output similar to the following, with a "Running" status for each service that has restarted successfully:

```
assurance-backend  wirelesscollector-123-bc99s  1/1   Running   0   25d   <IP>   <IP>
ndp                        collector-netflow-456-lxvlx   1/1   Running   0   1d   <IP>
<IP>
ndp                        collector-syslog-789-r0rr1    1/1   Running   0   25d   <IP>
<IP>
ndp                        collector-trap-101112-3ppllm  1/1   Running   0   25d   <IP>
<IP>
```

Step 5 Access the Cisco DNA Center GUI and use the Cisco DNA Center Telemetry tool to push the **Optimal Visibility** profile to all nodes, as you did in Step 1.

Troubleshooting WAAS Central Manager Access

If you update a non-default WAAS Central Manager (WCM) username (which doesn't have permission to access the WCM GUI) and then later receive an access error when you try to cross-launch WCM from Cisco DNA Center, you need to redo the role for that username as shown in the following steps.

Procedure

Step 1 Launch the WCM GUI by entering **`https://wcm_ip_address:8443`** and enter the admin user credentials.

Step 2 Choose **Admin** > **AAA** > **Users**.

Step 3 Select the username that you recently modified, then navigate to **Role Management**.

Step 4 Assign the role that has access for the GUI.

This gives the correct access permissions to the user and allows you to cross-launch WAAS Central Manager from Cisco DNA Center.

Bugs

Open Bugs

The following table lists the open bugs for Cisco DNA Center for this release.

Table 4: Open Bugs

Bug Identifier	Headline
CSCvj15985	There is a need to reboot the Cisco vEDGE/ISRv router if any updates are made on the VNIC.
CSCvj41522	PNP CSV with 25 APs fails.
CSCvj75410	The Elasticsearch data store moves to an available node and the old entries and mappings are removed. When this happens, no data is shown on the Assurance pages.
CSCvk33113	Editing the global PSK SSID does not change the override PSK SSID after reprovisioning the wireless controller.
CSCvk73751	Issues with the Find option in the APIs page under the Developer Toolkit.
CSCvm09710	An invalid character in the configuration on plug-and-play fails with a timeout.
CSCvm38125	Fabric-in-a-box with SDA transit creates /32 entries in the transit control plane.
CSCvm40832	Cannot enable L2 handoff if the border has SDA transit connected.
CSCvm46121	With L2 border handoff, the Catalyst 6500/Catalyst 6800 15.5(1)SY2 image does not encode DHCP option 82 in the DHCP discover packet.
CSCvm47215	Mobility Express shows as null on the provisioning page after a successful Mobility Express plug-and-play claim.
CSCvm53612	Cisco Wireless Controller provision and add to fabric succeeds, but the wireless controller shows the fabric as disabled.
CSCvm54948	After the Mobility Express controller is onboarded to Cisco DNA Center, Cisco DNA Center provisions the Mobility Express with IP addresses from the IP pool and the site username and password. The Mobility Express stays in "Cannot Sync" state and does not change to "Manage" state.

Bug Identifier	Headline
CSCvm59095	Recent tasks in image repository and device update status occasionally show no data.
CSCvm60582	SWIM: The Mobility Express upgrade succeeds but is reported as failed.
CSCvm64770	Cisco DNA Assurance 1.2.6.46 doesn't display wired endpoint information with client health filters.
CSCvm65634	Cannot access the Cisco DNA Center UI due to an error: "backendRequest failed."
CSCvm96496	3 node: After a system update from 1.2.4 to 1.2.6, system login fails and commands return an error.
CSCvm96687	Guest anchor selection from UI should be disabled when the SSID profile is fabric.
CSCvn01937	Cisco DNA Center 1.2.6 (Scale and Performance): Occasionally unable to delete NFV devices.
CSCvn02130	Device interface config validation fails: Server port assignment may not specify address or voice.
CSCvn06074	Network Controller Platform package upgrade fails from 1.1.8 to 1.2.6.
CSCvn10238	After upgrading, the Cisco Aironet 1800S inventory has the device but does not show the MAC address, and the configuration is not pushed. The workaround is to delete the device from inventory and claim it again.
CSCvn44017	After an upgrade, Cisco DNA Center's Elasticsearch pod for Assurance (NDP) goes into a CrashLoopBack state. The NDP Elasticsearch instance tries unsuccessfully to change the ownership of files and directories under the NDP Elasticsearch snapshots on the NFS mount. Doing so requires configuring the NFS server with no_root_squash. This problem occurs when the NFS server's mount location permission is not set (and the NFS mount setup is configured with root_squash). The workaround is to enter the following command to set the permission on the NSF directory to 777: **chmod 777 -R** *<your_NFS_directory>*

Resolved Bugs

The following table lists the resolved bugs for Cisco DNA Center for this release.

Table 5: Resolved Bugs

Bug Identifier	Headline
CSCvj99964	NFV provisioning does not support changing the management network to the LAN network in a switch configuration.
CSCvm09564	The 24-hour bar on the Sensor Management page has a grayed-out section on the far right (for the most recent interval). The sensor results are grayed out even for tests that passed.
CSCvm14997	Image copy fails to use SFTP for Mobility Express.
CSCvm21352	Global VLANs of E NCS 54xx switches are not configured.
CSCvm29623	Top N Apps by client count chart shows no data; API returns null values.

Bug Identifier	Headline
CSCvm37603	Site prefixes are not seen in the local control plane in a fabric-in-a-box scenario.
CSCvm42415	Cisco DNA Assurance should display clients from the trunk port.
CSCvm51415	Push 'advertisement-interval 0' during border automation.
CSCvm53278	Cisco DNA Center with IWAN: A hub provisioning failure occurs when adding a day-N MTT link to the border router.
CSCvm55331	Cannot delete the seed device, even though network orchestration is complete.
CSCvm55403	Cisco DNA Center with IWAN: A partial collection failure occurs on the hub border router if a day-n WAN bandwidth change is made.
CSCvm57129	Extended node C3560CX, post-provision check fails.
CSCvm57225	From the Design/Provision > Assurance page, the 24-hour duration option is unavailable.
CSCvm58872	Multicast traffic does not work on SDA in-box with SDA transit.
CSCvm58967	LAN automation is stuck in Unclaimed state with a Catalyst 6000 as the seed device.
CSCvm59016	Device tracking policy is not removed from the L2 border trunk interface.
CSCvm59169	AP-1800S image upgrade fails with a Flash error when skip activate step selected.
CSCvm59209	Cisco DNA Center - Cisco Wireless Controller: Mobility Express AP does not send WSA due to a certificate issue.
CSCvm64504	Client count doubles just before the system package upgrade.
CSCvm64749	Assurance doesn't show data under the Fabric Edge Assurance page.
CSCvm65767	Updating the management IP for NFVIS goes to partial collection failure.
CSCvm68111	After upgrading from Cisco DNA Center 1.2.4 to 1.2.5, the Cisco Aironet 1800s Active Sensor appears in the Inventory in Unclaimed state.
CSCvm82565	Sensor flashes a PnP error message while claiming the device.
CSCvm90450	2 pods of Kafka are in a crash loop after system update from 1.1.8 to 1.2.6 on 3 node

Using the Bug Search Tool

Use the Bug Search tool to search for a specific bug or to search for all bugs in this release.

Procedure

Step 1 Point your browser to http://tools.cisco.com/bugsearch.

Step 2 At the Log In screen, enter your registered cisco.com username and password; then, click **Log In**. The Bug Search page opens.

If you do not have a cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press **Return**.

Step 4 To search for bugs in the current release:

a) In the Search For field, enter Cisco DNA Center and press **Return**. (Leave the other fields empty.)

b) When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.

To export the results to a spreadsheet, click the **Export Results to Excel** link.

Limitations and Restrictions

Backup and Restore Limitations

Backup and restore limitations and restrictions include:

- You cannot take a backup from one version of Cisco DNA Center and restore it to another version of Cisco DNA Center. You can only restore a backup to an appliance that is running the same Cisco DNA Center software version, applications, and application versions as the appliance and applications from which the backup was taken. To view the current applications and versions on Cisco DNA Center, click ⚙ > **System Settings** > **App Management**.
- After performing a restore operation, update your integration of Cisco ISE with Cisco DNA Center. After a restore operation, Cisco ISE and Cisco DNA Center might not be in sync. To update your Cisco ISE integration with Cisco DNA Center, access **Settings** in the GUI, then open the **Authentication and Policy Servers** window and choose **Edit** for the server. Enter your Cisco ISE password to update.
- After performing a restore operation, the configuration of devices in the network might not be in sync with the restored database. For this reason, you might need to manually revert the CLI commands pushed for authentication, authorization, and accounting (AAA) and configuration on the network devices. Refer to the individual network device documentation for information about the CLI commands to enter.
- Re-enter the device credentials in the restored database. If you updated the site-level credentials before the database restore and the backup being restored does not have the credential change information, all devices go to partial-collection after restore. You then need to manually update the device credentials on the devices for synchronization with Cisco DNA Center or perform a rediscovery of those devices to learn the device credentials.
- Perform AAA provisioning only after adjusting network device differential changes to the restored database. Otherwise, device lockouts might occur.
- You can back up and restore Automation data only or both Automation and Assurance data. But you cannot use the GUI or the CLI to back up or restore only Assurance data.

HA Limitation

In this release, Cisco DNA Center only provides HA support for Automation functionality. HA for Assurance is not supported at this time.

Cisco ISE Integration Limitations

Cisco ISE integration limitations and restrictions include:

- ECDSA keys are not supported as either SSH keys for Cisco ISE SSH access, nor in certificates in Cisco DNA Center and Cisco ISE.
- Full certificate chains must be uploaded to Cisco DNA Center while replacing the existing certificate. If the Cisco DNA Center certificate is issued by a subCA of a rootCA, the certificate chain uploaded to Cisco DNA Center while replacing the Cisco DNA Center certificate must contain all three certificates.
- Self-signed certificates applied on Cisco DNA Center must have the Basic Constraints extension with cA:TRUE (RFC5280 section-4.2.19).
- The IP address or FQDN of both Cisco ISE and Cisco DNA Center must be present in either the Subject Name field or the Subject Alt Name field of the corresponding certificates.
- If the certificate is replaced or renewed in either Cisco ISE or Cisco DNA Center, trust must be re-established.
- Cisco DNA Center andCisco ISE IP/FQDN must be present in the proxy exceptions list if there is a web proxy between Cisco DNA Center and Cisco ISE.
- Cisco DNA Center and Cisco ISE nodes cannot be behind a NAT device.
- Cisco DNA Center does not detect pxGrid persona changes after trust establishment.
- Cisco DNA Center and Cisco ISE cannot integrate if the ISE Admin and ISE pxGrid certificates are issued by different enterprise certificate authorities.

  Specifically, if the ISE Admin certificate is issued by *CA server A*, the ISE pxGrid certificate is issued by *CA server B*, and the pxGrid persona is running on a node other than ISE PPAN, the pxGrid session from Cisco DNA Center to Cisco ISE does not work.

Brownfield Feature-Related Limitations

Brownfield feature-related limitations include:

- Cisco DNA Center cannot learn device credentials.
- You must enter the preshared key (PSK) or shared secret for the AAA server as part of the import flow.
- Details about DNS, WebAuth redirect URL, and syslog are not learned.
- Cisco DNA Center can learn only one wireless controller at a time.
- For site profile creation, only those AP groups with AP and SSID entries are considered.
- Automatic site assignment is not possible.
- SSIDs with an unsupported security type and radio policy are discarded.
- For authentication and accounting servers, if the RADIUS server is present in the device, it is given first preference. If the RADIUS server is not present, the TACACS server is considered for design.
- Cisco ISE server (AAA) configuration is not learned through brownfield provisioning.
- The authentication and accounting servers must have the same IP addresses for them to be learned through brownfield provisioning.

- When the same SSID is associated with different interfaces in different AP groups, during the provisioning, the newly created AP group with the SSID is associated with the same interface.
- A wireless conflict is based on the SSID name only and does not consider other attributes.

Wireless Policy Limitation

Wireless policy limitation includes:

- If the AP is migrated after the policy was created, you must manually edit the policy and point to an appropriate AP location before deploying the policy. Otherwise, an error message saying "Policy Deployment failed" is displayed.

Cisco Plug and Play Limitations

Plug and Play limitations and restrictions include:

- Virtual Switching System (VSS) is not supported.
- The Cisco Plug and Play Mobile app is not supported with Plug and Play in Cisco DNA Center.
- The Stack License workflow task is supported for Cisco Catalyst 3650 and 3850 Series switches running IOS XE 16.7.1 and later.
- The Plug and Play agent on the switch initiates on VLAN 1 by default. Most deployments recommend that VLAN 1 be disabled. If you do not want to use VLAN 1 when PnP starts, enter the following CLI command on the upstream device:

  pnp startup-vlan *<vlan_number>*

Get Assistance from the Cisco TAC

Use this link to open a TAC case. Choose the following when opening a TAC case:

- **Technology**: Cisco DNA - Software-Defined Access
- **Subtechnology**: Cisco DNA Center Appliance (SD-Access)
- **Problem Code**: Install, uninstall, or upgrade

Related Documentation

The following publications are available for Cisco DNA Center.

For this type of information...	See this document...
Release information, including new features, system requirements, and open and resolved bugs.	Cisco DNA Center Release Notes
Installation and configuration of Cisco DNA Center, including post-installation tasks.	Cisco DNA Center Installation Guide
Use of the Cisco DNA Center GUI and its applications.	Cisco DNA Center User Guide

For this type of information...	See this document...
Configuration of user accounts, RBAC scope, security certificates, authentication and password policies, and global discovery settings. Monitoring and managing Cisco DNA Center services. Backup and restore.	Cisco DNA Center Administrator Guide
Security features, hardening, and best practices to ensure a secure deployment.	Cisco DNA Center Security Best Practices Guide
Supported devices, such as routers, switches, wireless access points, NFVIS platforms, and software releases.	Supported Devices
Use of the Cisco DNA Assurance GUI.	Cisco DNA Assurance User Guide
Licenses and notices for open source software used in Cisco DNA Assurance.	Open Source Used in Cisco DNA Assurance
Use of the Cisco DNA Center platform GUI and its applications.	Cisco DNA Center Platform User Guide
Cisco DNA Center platform release information, including new features, deployment, and open bugs.	Cisco DNA Center Platform Release Notes
Licenses and notices for open source software used in Cisco DNA Center platform.	Open Source Used in Cisco DNA Center Platform
Key features and scale numbers.	Cisco DNA Center Data Sheet