Get Started with Cisco DNA Center

About Cisco DNA Center

Cisco Digital Network Architecture offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center GUI provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

Log In

Access Cisco DNA Center by entering its network IP address in your browser. For compatible browsers, see the Cisco DNA Center Release Notes. This IP address connects to the external network and is configured during the Cisco DNA Center installation. For more information about installing and configuring Cisco DNA Center, see the Cisco DNA Center Installation Guide.

You should continuously use Cisco DNA Center to remain logged in. If you are inactive for too long, Cisco DNA Center logs you out of your session automatically.

Step 1 Enter an address in your web browser's address bar in the following format. Here, *server-ip* is the IP address (or the hostname) of the server on which you have installed Cisco DNA Center:

https://*server-ip*

Example: https://192.0.2.1

Depending on your network configuration, you might have to update your browser to trust the Cisco DNA Center server security certificate. Doing so will help ensure the security of the connection between your client and Cisco DNA Center.

Step 2   Enter the Cisco DNA Center username and password assigned to you by the system administrator. Cisco DNA Center displays its home page.

If your user ID has the SUPER-ADMIN-ROLE and no other user with the same role has logged in before, you will see a first-time setup wizard instead of the home page.

Step 3   To log out, click the **Menu** icon (≡) and choose **Sign Out**.

Complete the Quick Start Workflow

After you have installed and configured the Cisco DNA Center appliance, you can log in to its GUI. Use a compatible, HTTPS-enabled browser when accessing Cisco DNA Center.

When you log in for the first time as the admin superuser (with the username `admin` and the SUPER-ADMIN-ROLE assigned), the Quick Start workflow automatically starts. Complete this workflow to discover the devices that Cisco DNA Center will manage and enable the collection of telemetry from those devices.

Before you begin

To log in to Cisco DNA Center and complete the Quick Start workflow, you will need:

- The *admin* superuser username and password that you specified while completing one of the following procedures in the Cisco DNA Center Second-Generation Appliance Installation Guide:

    - Configure the Primary Node Using the Maglev Wizard

    - Configure the Primary Node Using the Expert Configuration Wizard (44- or 56-core appliance)

    - Configure the Primary Node Using the Expert Configuration Wizard (112-core appliance)

- The information described in the installation guide's Required First-Time Setup Information topic.

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

Step 2   Enter the host IP address to access the Cisco DNA Center GUI, using **HTTPS://** and the IP address of the Cisco DNA 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 the browser you are using):

- 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 Cisco DNA Center uses certificates, see the "Certificate and Private Key Support" section in the Cisco DNA 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 Cisco DNA Center login screen appears.

Step 5   Do one of the following and then click **Log In**:

       • If you completed the Maglev configuration wizard and chose the **Start using DNAC pre manufactured cluster** option, enter the admin's username (**admin**) and password (**maglev1@3**).

       • If you completed the Maglev configuration wizard and chose the **Start configuration of DNAC in advanced mode** option, enter the admin's username (**admin**) and password that you set when you configured your Cisco DNA Center appliance.

       • If you completed the Install configuration wizard, enter the admin's username (**admin**) and password (**maglev1@3**).

       • If you completed the Advanced Install configuration wizard, enter the admin's username (**admin**) and password that you set when you configured your Cisco DNA Center appliance.

In the next screen, you are prompted to specify a new admin password (as a security measure).

Step 6   Do the following, then click **Next**:

    a)   Enter the same admin password you specified in Step 5.

    b)   Enter and confirm a new admin password.

Step 7   In the resulting screen, enter your cisco.com username and password and then click **Next**.

These credentials are used to register software downloads and receive system communications.

The **Terms & Conditions** screen opens, providing links to the software End User License Agreement (EULA) and any supplemental terms that are currently available.

Step 8   After reviewing these documents, click **Next** to accept the EULA.

The **Quick Start Overview** slider opens. Click > to view a description of the tasks that the Quick Start workflow will help you complete in order to start using Cisco DNA Center.

Step 9   Complete the Quick Start workflow:

    a)   Click **Let's Do it**.

    b)   In the **Discover Devices: Provide IP Ranges** screen, enter the following information and then click **Next**:

          • The name for the device discovery job.

          • The IP address ranges of the devices you want to discover. Click + to enter additional ranges.

- Specify whether you want to designate your appliance's loopback address as its preferred management IP address. For more information, see the "Preferred Management IP Address" topic in the Cisco DNA Center User Guide.

c) In the **Discover Devices: Provide Credentials** screen, enter the information described in the following table for the type of credentials you want to configure and then click **Next**:

Field	Description
CLI (SSH) Credentials	
Username	Username used to log in to the CLI of the devices in your network.
Password	Password used to log in to the CLI of the devices in your network.
Name/Description	Name or description of the CLI credentials.
Enable Password	Password used to enable a higher privilege level in the CLI. Configure this password only if your network devices require it.
SNMP Credentials: SNMPv2c Read tab	
Name/Description	Name or description of the SNMPv2c read community string.
Community String	Read-only community string password used only to view SNMP information on the device.
SNMP Credentials: SNMPv2c Write tab	
Name/Description	Name or description of the SNMPv2c write community string.
Community String	Write community string used to make changes to the SNMP information on the device.
SNMP Credentials: SNMPv3	
Name/Description	Name or description of the SNMPv3 credentials.
Username	Username associated with the SNMPv3 credentials.
Mode	Security level that SNMP messages require: • **No Authentication, No Privacy** (noAuthnoPriv): Does not provide authentication or encryption. • **Authentication, No Privacy** (authNoPriv): Provides authentication, but does not provide encryption. • **Authentication and Privacy** (authPriv): Provides both authentication and encryption.

Field	Description
Authentication Password	Password required to gain access to information from devices that use SNMPv3. The password must be at least eight characters in length. Note the following points: • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Authentication Type	Hash-based Message Authentication Code (HMAC) type used when either **Authentication and Privacy** or **Authentication, No Privacy** is set as the authentication mode: • **SHA**: HMAC-SHA authentication. • **MD5**: HMAC-MD5 authentication.
Privacy Type	Privacy type used when **Authentication and Privacy** is set as the authentication mode: • **AES128**: 128-bit AES encryption. • **None**: No privacy.
Privacy Password	Password used to generate the secret key for encrypting messages that are exchanged with devices that support AES128 encryption. Passwords must be at least eight characters long. Note the following points: • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
NETCONF	
Port	The NETCONF port that Cisco DNA Center should use in order to discover wireless controllers that run Cisco IOS-XE.

d) In the **Create Site** screen, group the devices you are going to discover into one site in order to facilitate telemetry and then click **Next**.

You can enter the site's information manually or click the location you want to use in the provided map.

e) In the **Enable Telemetry** screen, check the network components that you want Cisco DNA Center to collect telemetry for and then click **Next**.

To open a pop-up window that lists the commands Cisco DNA Center will send to enable telemetry on a particular component, click its **View Sample Commands** link.

f) In the **Summary** screen, review the settings that you have entered and then do one of the following:

- If you want to make changes, click the appropriate **Edit** link to open the relevant screen.

- If you're happy with the settings, click **Start Discovery and Telemetry**. Cisco DNA Center validates your settings to ensure that they will not result in any issues. After validation is complete, the screen updates.

  Cisco DNA Center begins the process of discovering your network's devices and enabling telemetry for the network components you selected. The process will take a minimum of 30 minutes (more for larger networks).

g) Click **Launch Homepage** to open the Cisco DNA Center homepage.

While Cisco DNA Center discovers your network's devices and enables telemetry, you can familiarize yourself with the functionality that the product provides. Begin by clicking **Launch Homepage**. Then click the **Explore** link to open a page that provides pointers to product documentation and videos.

A message appears at the top of the homepage to indicate when the Quick Start workflow has completed.

Default Home Page

After you log in, Cisco DNA Center displays its home page. The home page has the following main areas: **Assurance Summary**, **Network Snapshot**, **Network Configuration**, and **Tools**.

Note By default, the login name you provided is displayed in the Welcome text. To change the name, click the name link; for example, **admin**. You are taken to the **User Management** window, where you can edit the display name.

Assurance Summary

This area includes:

- **Health**: Provides the health score of your overall enterprise, which includes network devices, wired clients, and wireless clients. Clicking **View Details** takes you to the **Overall Health** window.

- **Critical Issues**: Provides the count of P1 and P2 issues. Clicking **View Details** takes you to the **Open Issues** window.

  - **P1**: Critical issues that need immediate attention before they cause a wider impact on network operations.

  - **P2**: Major issues that can potentially impact multiple devices or clients.

- **Trends and Insights**: Provides insights about the performance of your network. Clicking **View Details** takes you to the **Network Insights** window.

Network Snapshot

This area includes:

- **Sites**: Provides the number of sites discovered on your network along with the number of DNS and NTP servers. Clicking **Add Sites** takes you to the **Add Site** window.

- **Network Devices**: Provides the number of network devices discovered on your network along with the number of unclaimed, unprovisioned, and unreachable devices. Clicking **Find New Devices** takes you to the **New Discovery** window.

- **Application Policies**: Provides the number of application policies discovered on your network along with the number of successful and errored deployments. Clicking **Add New Policy** takes you to the **Application Policies** window.

- **Network Profiles**: Provides the number of profiles discovered on your network. Clicking **Manage Profiles** takes you to the **Network Profiles** window.

- **Images**: Provides the number of images discovered on your network along with the number of untagged and unverified images. Clicking **Import Images/SMUs** takes you to the **Image Repository** window.

- **Licensed Devices**: Provides the number of devices that have a Cisco DNA Center license along with the number of switches, routers, and access points. Clicking **Manage Licenses** takes you to the **License Management** window.

Tools

Use the **Tools** area to configure and manage your network.

Figure 1: Cisco DNA Center Home Page
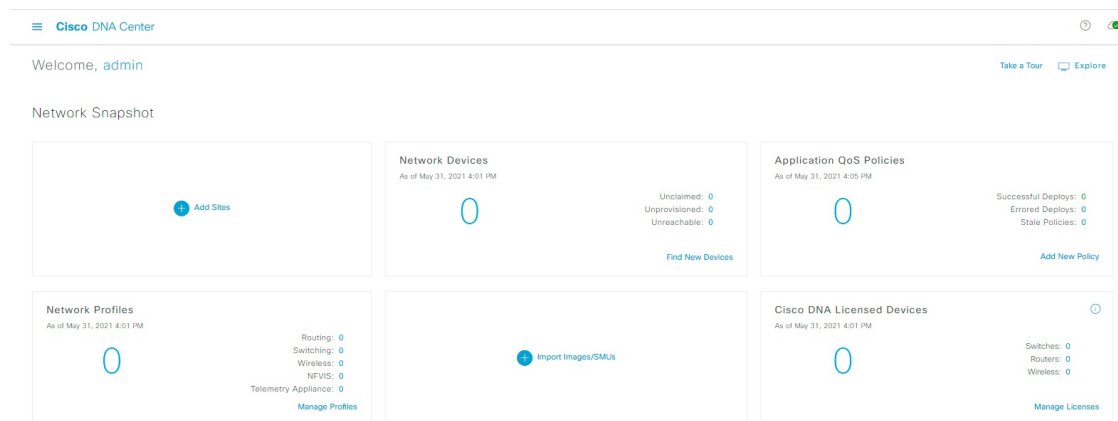
Different Views of Home Page

The home page can vary depending factors such as the different stages of Cisco DNA Center and what role is used to log in:

- **Getting Started**: When you log in to Cisco DNA Center for the first time as a Network Administrator or System Administrator, or when there are no devices in the system, you see the following dashlet. Click **Get Started** and complete the getting started workflow to discover new devices in your network.

In a few simple steps, discover your devices to begin your Cisco DNA Center journey!

Get Started

When you log in to Cisco DNA Center for the first time as an Observer, you see the following message:

Ask your Network Administrator to add Network Devices to gather Assurance data.

• **Day 0 Home Page**: If you skipped getting started, or when there are no devices in the system, you see the following home page.

When discovery is in progress, you see a progress message with a link to the **Discovery** window.

We've discovered 10 devices in your network. View Discovery

When there are devices in the system, you see a network snapshot of discovered devices.

Menu Bar

Click the **Menu** icon (☰) at the left of the menu bar to access the following menu items:

• Design

• Policy

• Provision

• Assurance

• Workflows

• Tools

• Platform

- Activities

- Reports

- System

- Explore

Icons

Click the icons at the right of the menu bar to perform common tasks:

Icon	Description
🔍	**Search**: Search for devices, users, hosts, menus, and other items that are stored anywhere in the Cisco DNA Center database.
�@	**Help** • **About**: Display the current Cisco DNA Center software version. Click **Release Notes** to launch the release notes in a separate browser tab. Click **Packages** to view the system and application package versions. Click **Serial number** to view the serial number of the Cisco DNA Center appliance. • **API Reference**: Open the Cisco DNA Center platform API documentation in Cisco DevNet. • **Developer Resources**: Open Cisco DevNet, where you can access developer tools. • **Help**: Launch context-sensitive online help in a separate browser tab. • **Contact Support**: Open a support case with the Cisco Technical Assistance Center (TAC). • **Make a Wish**: Submit your comments and suggestions to the Cisco DNA Center product team.
☁✓	**Software Updates**: See a list of available software updates. Click the **Go to Software Updates** link to view system and application updates.
🔔	**Notifications**: Displays event notifications and sets notification preferences. A red circle by the notification icon indicates that there are new notifications.

Interactive Help

Interactive Help contains walkthroughs for specific tasks in Cisco DNA Center. The walkthroughs provide on-screen guidance to help you complete the task.

The **Interactive Help** widget appears by default at the bottom-right of the Cisco DNA Center window. Click the widget to open the **Interactive Help** menu.

Figure 2: Interactive Help Widget

You can also move the **Interactive Help** widget from the default location to other locations. Drag and drop the widget to the possible locations. The possible locations are indicated by green dotted-line rectangles.

Use Global Search

Use the global Search function to find items in the following categories anywhere in Cisco DNA Center:

- **Activities**: Search for Cisco DNA Center menu items, workflows, and features by name.

- **Applications**: Search for them by name.

- **Application Groups**: Search for them by name.

- **Authentication template**: Search for them by name or type.

- **Devices**: Search for them by collection status, reachability status, location, or tag.

- **Fabric**: Search by fabric name.

- **Hosts and Endpoints**: Search for them by name, IP address, or MAC address.

- **IP Pools**: Search for them by name or IP address.

- **Network Devices**: Search for them by name, IP address, serial number, software version, platform, product family, or MAC address.

- **Network Profiles**: Search by profile name.

- **Network Settings**

  - **Device Credentials**: Search by name.

  - **IP Address Pools**: Search for them by group name or pool CIDR.

  - **Service Provider Profiles**: Search for them by profile name, WAN provider, or model.

- **Policy**: Search for them by name or description.

- **Sites**: Search for them by name.

- **Traffic copy**: Search for them by name and description.

- **Transits**: Search by transit name.

- **Users**: Search for the system settings and users by username. Case-insensitivity and substring search are not supported for usernames.

- Other items, as new versions of Cisco DNA Center are released.

To start a global Search, click the 🔍 icon in the top-right corner of any Cisco DNA Center page. Cisco DNA Center displays a pop-up global search window, with a Search field where you can begin entering identifying information about an item.

You can enter all or part of the target item's name, address, serial number, or other identifying information. The Search field is case-insensitive and can contain any character or combination of characters.

As you begin entering your search string, Cisco DNA Center displays a list of possible search targets that match your entry. If more than one category of item matches your search string, Cisco DNA Center sorts them by category, with a maximum of five items in each category. The first item in the first category is selected automatically, and summary information for that item appears in the summary panel on the right.

You can scroll the list as needed, and click any of the suggested search targets to see information for that item in the summary panel. If there are more than five items in a category, click **View All** next to the category name. To return to the categorized list from the complete list of search targets, click **Go Back**.

As you add more characters to the search string, global Search automatically narrows the displayed list.

Cisco DNA Center allows you to search for a device using its entire IPv6 address or any abbreviated form of the IPv6 address.

For example, to search for *2001:0db8:85a3:0000:0000:8a2e:0370:7334*, you can use the following search entries:

- **2001:0db8:85a3:0000:0000:8a2e:0370:7334** (using the full IPv6 address)

- **2001:db8:85a3:0:0:8a2e:0:7334** (truncating leading zeros)

- **2001:db8:85a3::8a2e:0:7334** (compressing consecutive zeros with a double colon)

- **2001:db8:85a3** (using a portion of the IPv6 address)

Cisco DNA Center allows you to search for an IPv6 address by using the double colon in the IPv6 address with prefix, postfix, or any combination.

For example, to search for *2001:db8:85a3::8a2e:0:7334*, you can use the following search entries:

- **::** (using double colon alone)

- **85a3::8a2e** (using prefix and postfix with double colon)

- **85a3::** (using prefix with double colon)

- **::8a2e** (using postfix with double colon)

You can search for devices in Cisco DNA Center by entering their MAC addresses in any format (with a hyphen or colon).

When you are finished, click ✱ to close the window.

Global search can display five results per category at a time.

Enable Localization

You can view the Cisco DNA Center GUI screens in English (the default), Chinese, Japanese, or Korean.

To change the default language, perform the following task:

Step 1   In your browser, change the locale to one of the supported languages: Chinese, Japanese, or Korean.

• From Google Chrome, do the following:

a.   Click the ⋮ icon in the top-right corner, and then choose **Settings**.

b.   Scroll down and click **Advanced**.

c.   From the **Languages** > **Language** drop-down list, choose **Add languages**.

The **Add languages** pop-up window appears.

d.   Choose **Chinese**, **Japanese**, or **Korean**, and then click **Add**.

• From Mozilla Firefox, do the following:

a.   Click the ≡ icon in the top-right corner, and then choose **Options**.

b.   From the **Language and Appearance** > **Language** area, choose **Search for more languages**.

The **Firefox Language Settings** pop-up window appears.

c.   From the **Select a language to add** drop-down list, choose **Chinese**, **Japanese**, or **Korean**.

d.   Click **Ok**.

Step 2   Log in to Cisco DNA Center.

The GUI screens are shown in the selected language.

Figure 3: Example Localized Login Screen

Where to Start

To start using Cisco DNA Center, you must first configure the Cisco DNA Center settings so that the server can communicate outside the network.

After you configure the settings, your current environment determines how you start using Cisco DNA Center:

- Existing infrastructure: If you have an existing infrastructure (brownfield deployment), start by running Discovery. After you run Discovery, all your devices are displayed on the **Inventory** window.

- New or nonexisting infrastructure: If you have no existing infrastructure and are starting from scratch (greenfield deployment), create a network hierarchy.