Adding Devices by Using Discovery

Cisco DNA Center 1.3 Training

Copyright Page

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Adding Devices by Using Discovery

Quick Reference

…with links to the details that you need.

What Should I Know Before I Start?

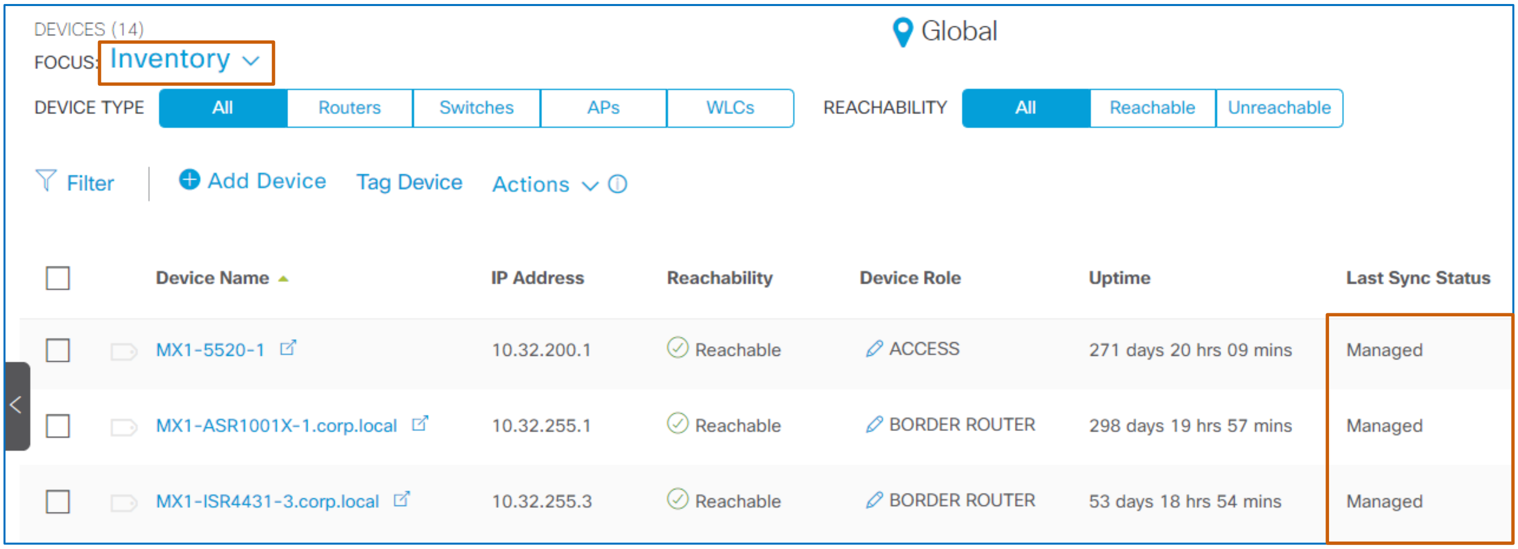
Discovering Devices Establishes Connectivity to the Network

To manage the enterprise network by using Cisco DNA Center, you first perform device discovery to add the switches, routers, and wireless LAN controllers (WLCs) to the Cisco DNA Center inventory. The discovery process:

- Establishes and validates device communication with the system.
- On success, adds the devices to the system inventory, and moves the devices into managed states.

You must ensure that devices appear in the inventory in managed states to be able to use Cisco DNA Center for most management tasks.

Note: To review a list of compatible devices, **refer to the Cisco DNA Center Supported Devices List**.



DEVICES (14)

FOCUS: Inventory

□	Device Name	IP Address	Reachability	Device Role	Uptime	Last Sync Status
□	MX1-5520-1	10.32.200.1	Reachable	ACCESS	271 days 20 hrs 09 mins	Managed
□	MX1-ASR1001X-1.corp.local	10.32.255.1	Reachable	BORDER ROUTER	298 days 19 hrs 57 mins	Managed
□	MX1-ISR4431-3.corp.local	10.32.255.3	Reachable	BORDER ROUTER	53 days 18 hrs 54 mins	Managed

Discovery provides the following methods to add devices:

- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (LLDP)
- IP address ranges

This training addresses the key concepts that you need to know and the steps that you take to add devices to Cisco DNA Center by using each device discovery method.

Tip: At the beginning of the document, refer to the **Quick Reference** for key information with links to the details that you need.

> To keep your place as you read, refer to the titles in the headers at the top of each page and the titles in the content.

The Skills That I Need

To perform device discovery, you need the following skills.

Proficient

- Cisco DNA Center user interface and navigation
- Networking concepts, including SNMP, CLI, and device credentials

How Do I Prepare?

By Recognizing the Available Discovery Processes

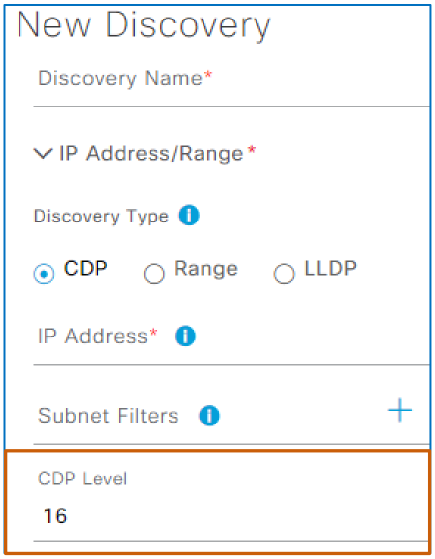
You can add devices to Cisco DNA Center by using.

- **Cisco Discovery Protocol (CDP)**
  A Layer 2, media-independent, and network-independent device discovery protocol that runs on all Cisco network equipment
- **Link Layer Discovery Protocol (LLDP)**
  A standardized method of adding network devices in multivendor networks
- **IP address ranges (Range)**
  A process using ping sweep to determine device reachability, incrementing through the range sequentially

When configuring the discovery task, you can define the number of hops that the system will take from the seed IP address to look for network devices.

Caution: When you configure a discovery task that will use the CDP or LLDP discovery method, the default setting (**CDP Level** or **LLDP Level** field) for the number of hops is 16, which is extensive and potentially can discover a large number of devices.

Adjust the number of hops based on the goals of the discovery task that you are running and the number of devices that you need the task to discover to ensure that you add only those devices that you need.



New Discovery

Discovery Name*

IP Address/Range*

Discovery Type

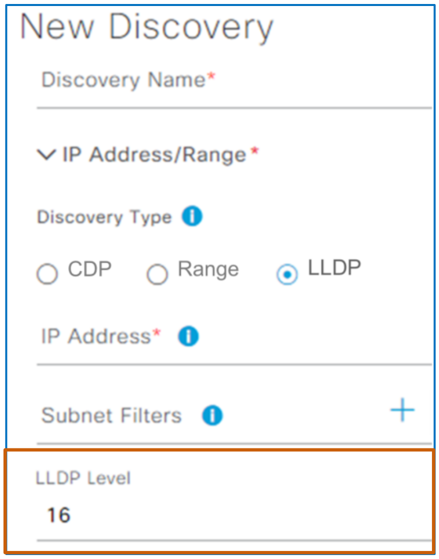
● CDP ○ Range ○ LLDP

IP Address*

Subnet Filters +

CDP Level

16



New Discovery

Discovery Name*

IP Address/Range*

Discovery Type

○ CDP ○ Range ● LLDP

IP Address*

Subnet Filters +

LLDP Level

16

On successful ping of each device, the process validates the SNMP, CLI, and other credentials, and if valid, adds the device to the inventory.

By Ensuring Device Support and Reachability

You can help ensure successful device discovery by validating that:

- Cisco DNA Center has IP connectivity to all devices.

  Cisco Best Practice: Although you can use layer 3 interfaces or switch virtual interfaces (SVIs) for connectivity, Cisco recommends that you use device loopback addresses for Cisco DNA Center manageability, which supports link redundancy.

  When you are configuring SD-Access, you must use the loopback address, which supports the control plane and VXLAN communication on layer 3 interfaces in fabric topologies.

- Device access control lists (ACLs) include the interfaces that Cisco DNA Center will use for communication.
- The interface firewalls between a device and Cisco DNA Center are open.
- Cisco DNA Center can access each device by either SSH or Telnet.

  Note: For detailed information on pre-requisite tasks and settings, refer to the **Cisco Digital Network Architecture Center User Guide**.

  For guidelines and the limitations that apply to discovering Cisco Catalyst 3000 and 6000 series switches, refer to the **Discovery Configuration Guidelines and Limitations** topic in **Discover Your Network** in the guide.

By Recognizing That Latency Among Devices and Cisco DNA Center…

…Affects How Long It Takes the System to Complete Various Processes

For optimal performance, Cisco recommends that latency among devices and Cisco DNA Center be 50 milliseconds or less.

When latency times are longer than 50 milliseconds, various processes can take longer to complete, such as device discovery, inventory collection, or device provisioning, correspondingly.

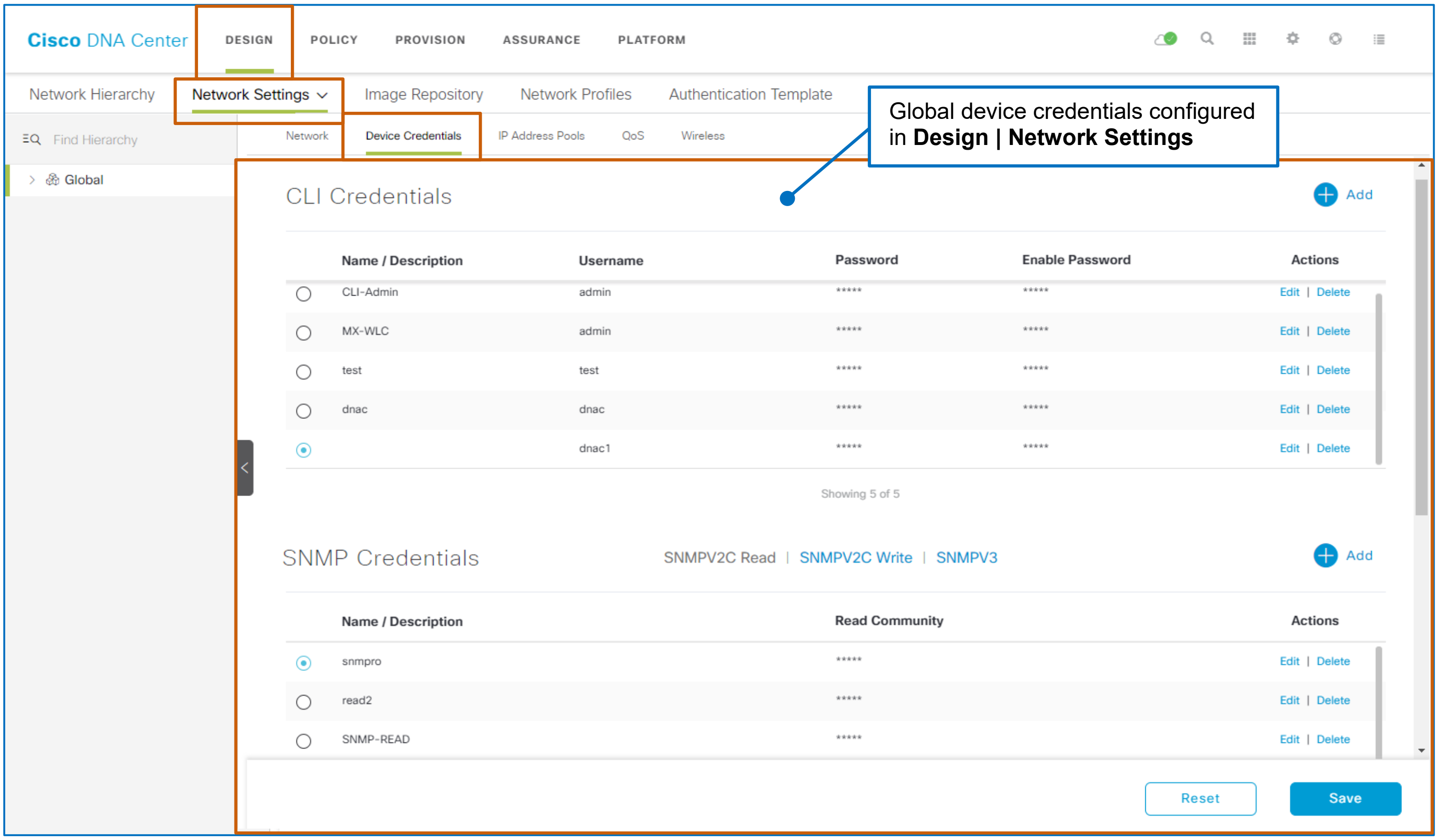
Depending on network conditions, extensive latency also can cause timeouts during these processes.

By Recognizing How the Global Credential Settings in Design…

…Appear in and Are Available for Use in Discovery Tasks

During initial system configuration, a network designer can configure global credentials in **Design | Network Settings**.

When designers configure global credentials in **Network Settings**, illustrated in the screenshot below…



Global device credentials configured in **Design | Network Settings**

CLI Credentials

	Name / Description	Username	Password	Enable Password	Actions
○	CLI-Admin	admin	*****	*****	Edit | Delete
○	MX-WLC	admin	*****	*****	Edit | Delete
○	test	test	*****	*****	Edit | Delete
○	dnac	dnac	*****	*****	Edit | Delete
●		dnac1	*****	*****	Edit | Delete

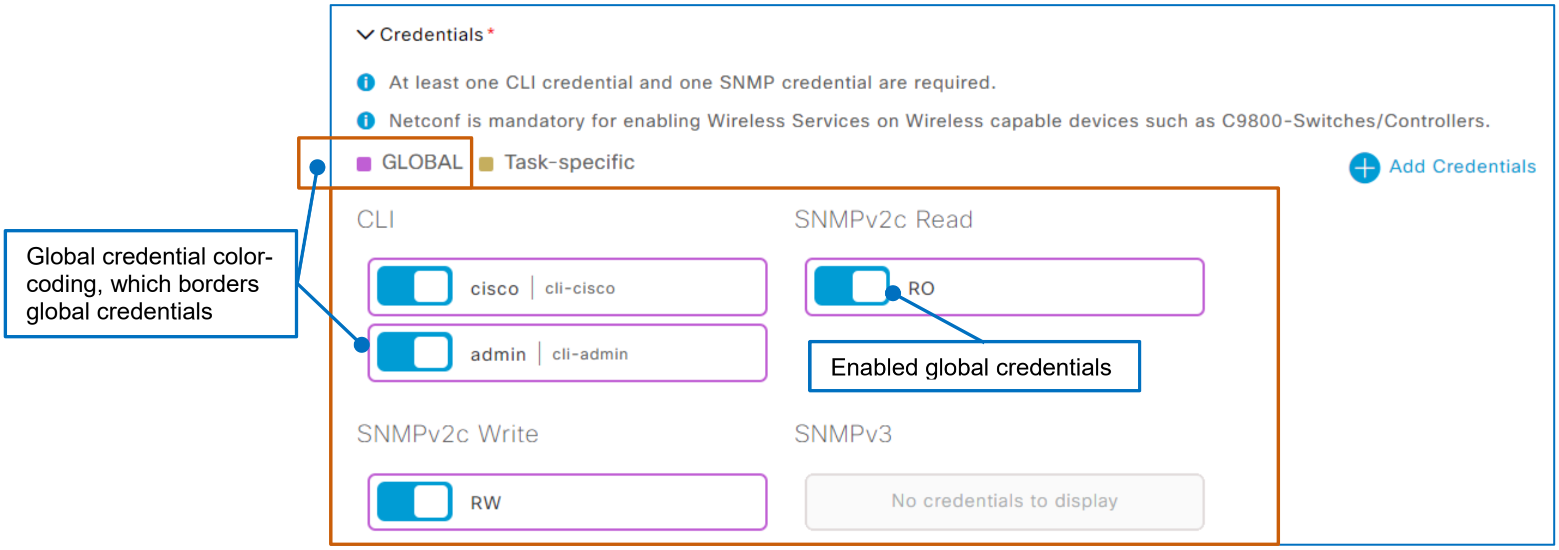
Showing 5 of 5

SNMP Credentials

	Name / Description	Read Community	Actions
●	snmpro	*****	Edit | Delete
○	read2	*****	Edit | Delete
○	SNMP-READ	*****	Edit | Delete

…they appear in and are available to use in new discovery tasks. Global credentials are indicated with unique color-coding and, by default, all of the credentials are enabled.

> **Cisco Best Practice:** Cisco recommends that users configure device credentials in **Design | Network Settings** before using **Discovery**, so that they are available for use in discovery tasks.
>
> Using global credentials also helps ensure that the system can add devices to the inventory and can manage and poll them successfully.



Credentials *

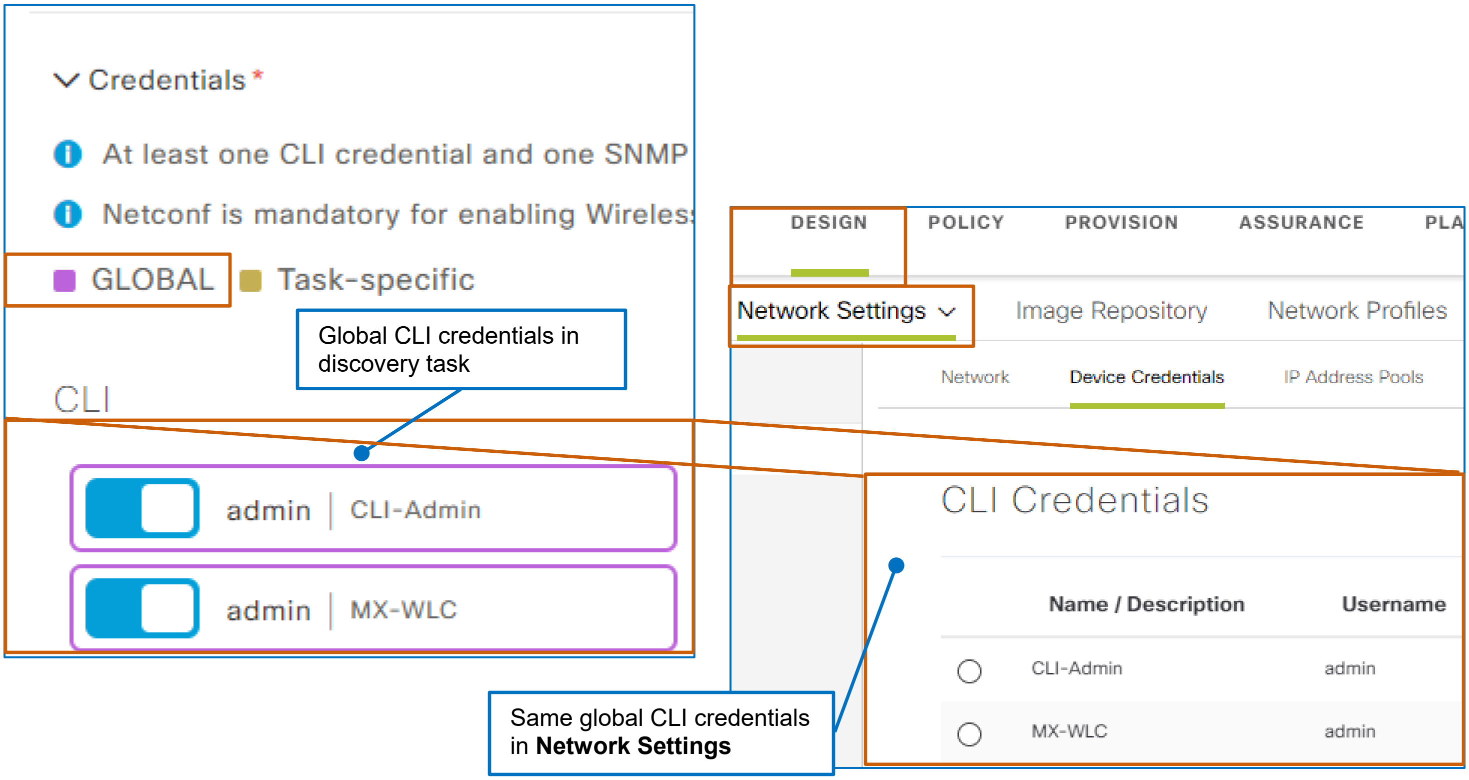
ℹ At least one CLI credential and one SNMP credential are required.

ℹ Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers.

Global credential color-coding, which borders global credentials

Enabled global credentials

In **Discovery** each on and off button, which is blue when enabled, indicates the names and descriptions, and for CLI credentails, user names, as they appear in **Network Settings**.



Credentials *

ℹ At least one CLI credential and one SNMP

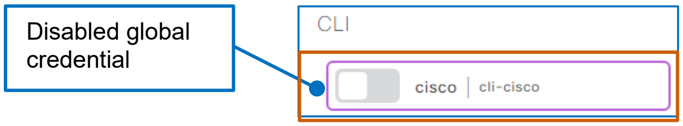
ℹ Netconf is mandatory for enabling Wireles

	Name / Description	Username
○	CLI-Admin	admin
○	MX-WLC	admin

Global CLI credentials in discovery task

Same global CLI credentials in **Network Settings**

You can disable global credentials that do not apply to the devices that you need to include in the task by toggling the button off, which disables it and changes the color coding to gray.

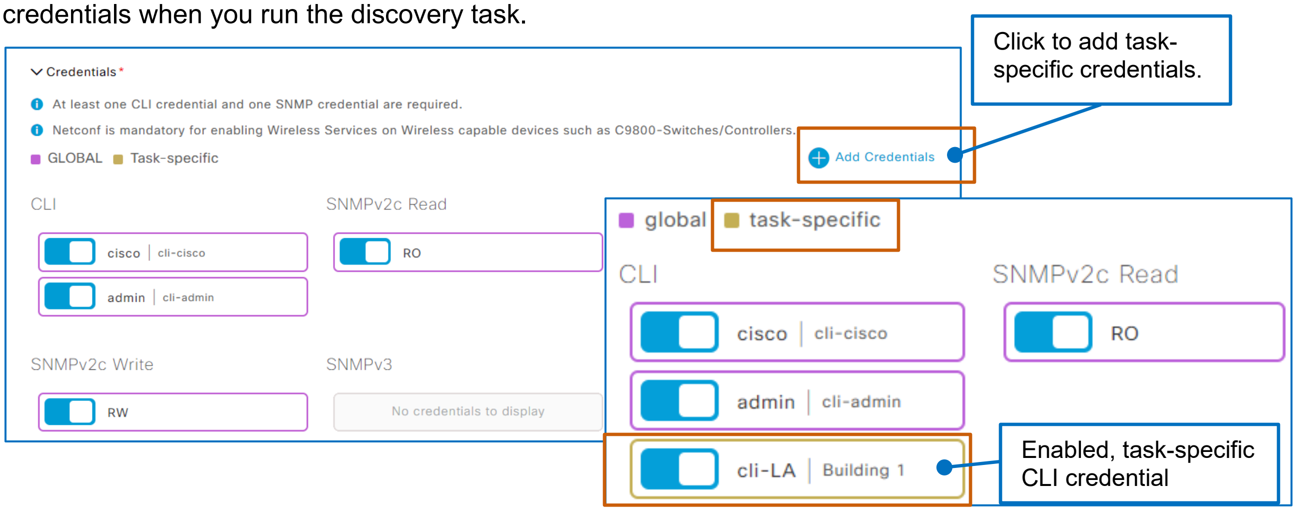

Disabled global credential

CLI

cisco | cli-cisco

You also can add unique credentials, referred to as task-specific, as needed. This feature helps optimize the discovery workflow when global credentials are not available.

When you add credentials, the system enables them by default and applies color-code to emphasize that they are unique. The system applies all of the enabled task-specific and global credentials when you run the discovery task.


Credentials*

ⓘ At least one CLI credential and one SNMP credential are required.

ⓘ Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers.

GLOBAL   Task-specific

Add Credentials

Click to add task-specific credentials.

CLI	SNMPv2c Read
cisco | cli-cisco	RO
admin | cli-admin	

SNMPv2c Write	SNMPv3
RW	No credentials to display

global   task-specific

CLI	SNMPv2c Read
cisco | cli-cisco	RO
admin | cli-admin	
cli-LA | Building 1	

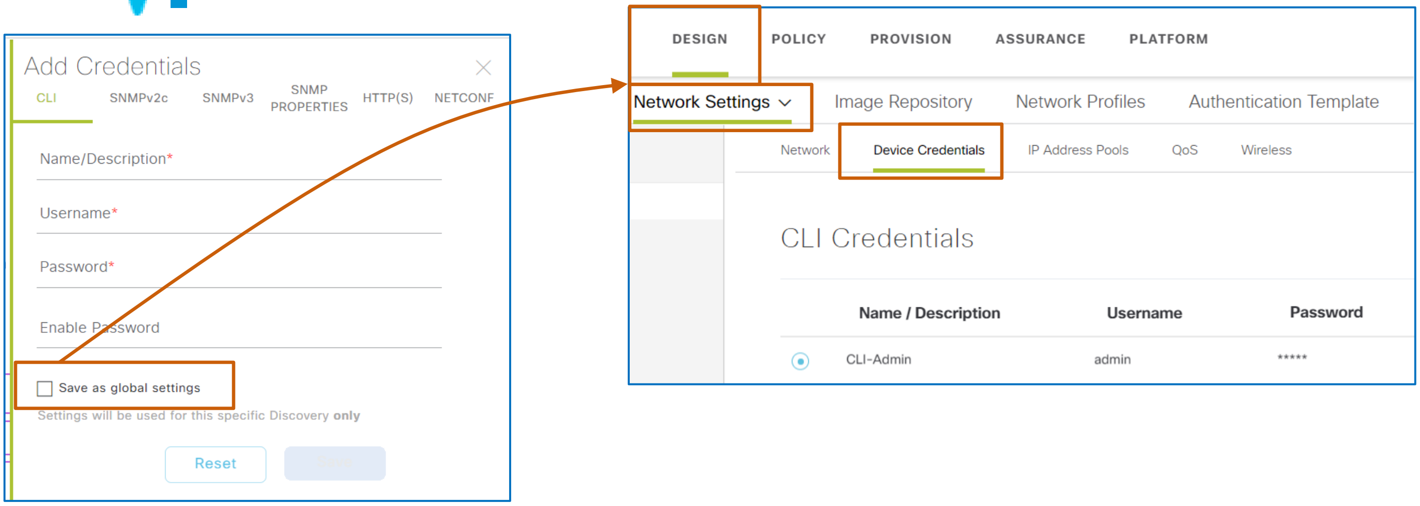
Enabled, task-specific CLI credential

When you add credentials at the task level, you also can add them to the global credentials in **Network Settings** for later use by selecting the **Save as global settings** check box.

Important Notes: To modify the credentials that system users save as global settings, you must navigate to **Design | Network Settings | Device Credentials**.

When someone changes credentials on devices after discovery, a system user must run another discovery task using the updated credentials so that Cisco DNA Center can include them in **Inventory** and continue to manage them.

Tip: it also is easier to make changes to the global credentials in **Design** rather than add them as task-specific credentials for individual discovery jobs.


Add Credentials

Name/Description*

Username*

Password*

Enable Password

□ Save as global settings

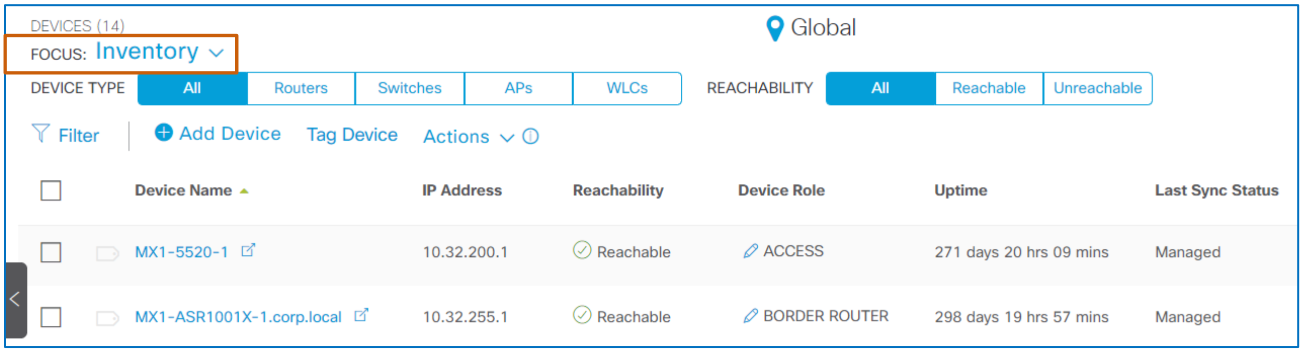
Settings will be used for this specific Discovery **only**

CLI Credentials

	Name / Description	Username	Password
◉	CLI-Admin	admin	*****

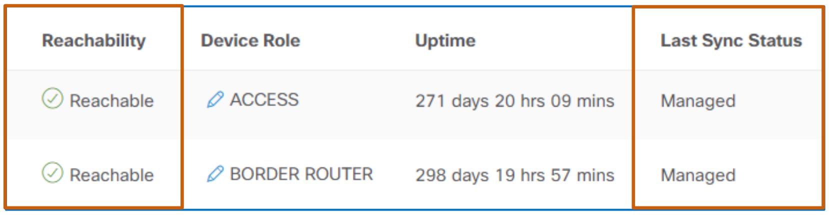
By Recognizing the System Actions That Occur in This Process

For successfully discovered devices, the system adds them to the inventory…



□	Device Name	IP Address	Reachability	Device Role	Uptime	Last Sync Status
□	MX1-5520-1	10.32.200.1	✓ Reachable	ACCESS	271 days 20 hrs 09 mins	Managed
□	MX1-ASR1001X-1.corp.local	10.32.255.1	✓ Reachable	BORDER ROUTER	298 days 19 hrs 57 mins	Managed

…and indicates that they are reachable by ping and are in a managed state.



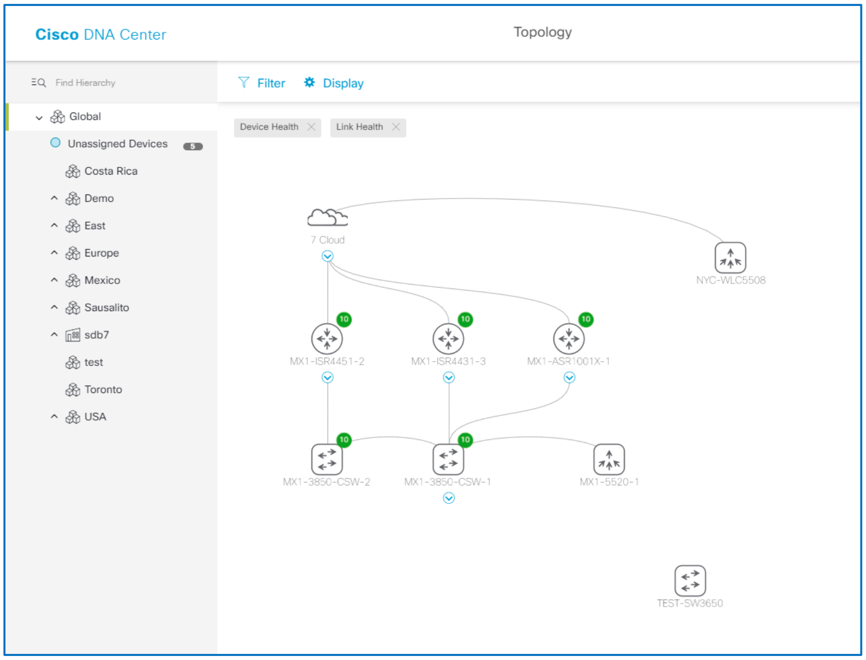
Reachability	Device Role	Uptime	Last Sync Status
✓ Reachable	ACCESS	271 days 20 hrs 09 mins	Managed
✓ Reachable	BORDER ROUTER	298 days 19 hrs 57 mins	Managed

When devices are in the inventory and in a managed state, Cisco DNA Center:

- Applies the **Device Controllability** configuration feature, which is enabled by default, that changes device configurations automatically based on system requirements or user actions.

  Important Note: To provide Assurance metrics, **Device Controllability** also automatically initiates the collection of streaming telemetry data from wireless LAN controllers when they become managed.

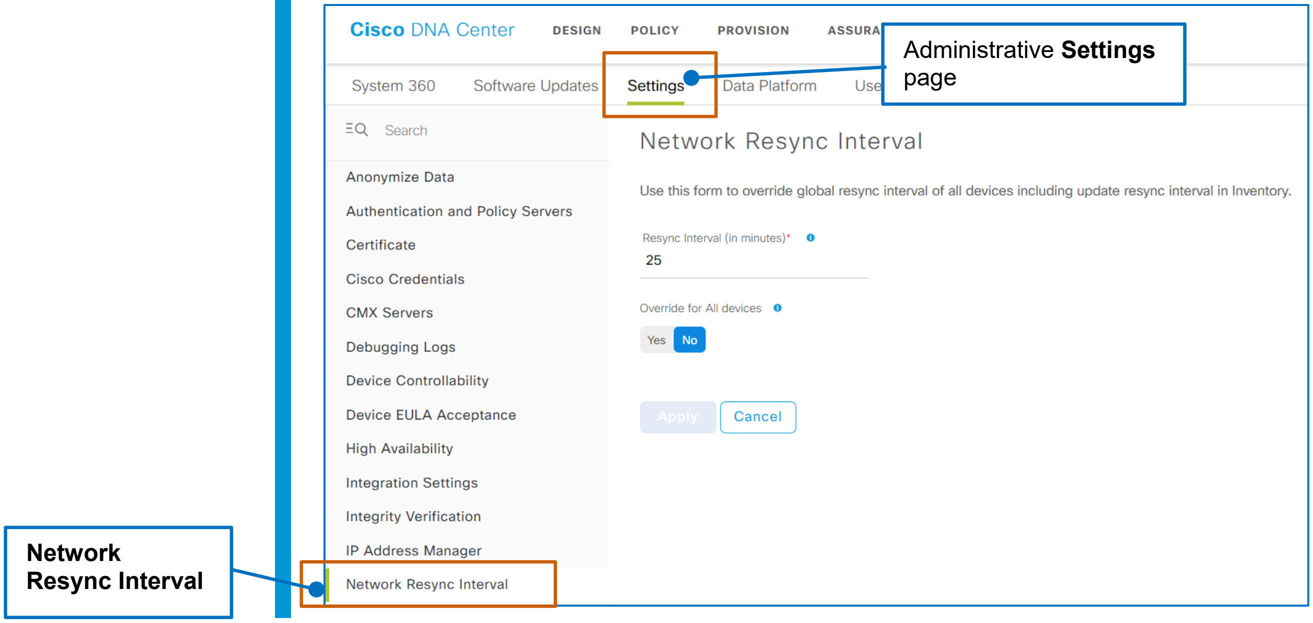
- Builds the device connectivity layout in the **Topology** tool based on the device roles that the system assigns during discovery.



- Initiates router and switch polling at 25-minute intervals, by default, to collect devices' states, configurations, software and versions, and other data.

Important Note: Administrators can configure polling intervals for all devices in **System Settings | Settings | Network Resync Interval**.

The minimum time interval an administrator can apply is 25 minutes.



Network Resync Interval

Use this form to override global resync interval of all devices including update resync interval in Inventory.

Resync Interval (in minutes)*: 25

Override for All devices: Yes [✓ No]

Administrative **Settings** page

Network Resync Interval

By Recognizing the Device Configuration Changes that Can Occur in this Process

During discovery, Cisco DNA Center connects to devices and determines their reachability by using the applicable SNMP or NetConf device credentials, which can be added by:

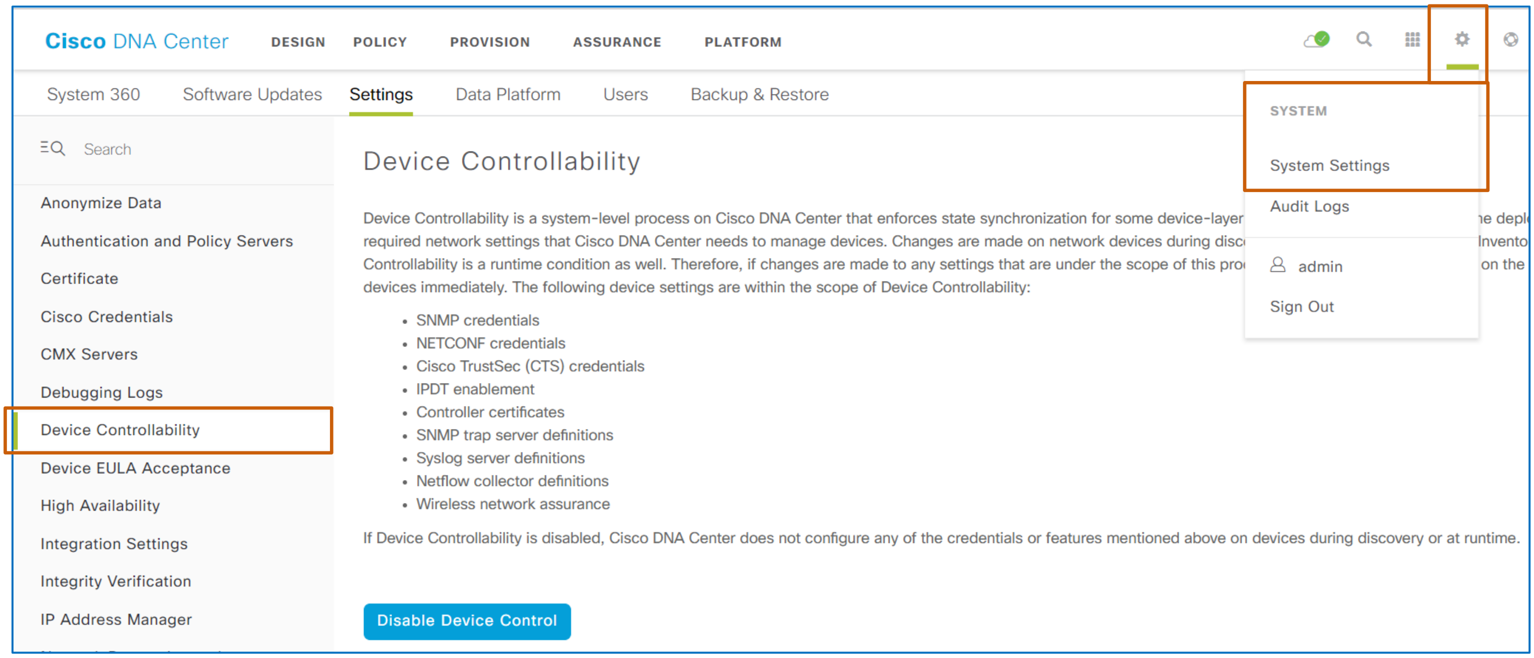
- A network administrator who is completing the initial configuration of Cisco DNA Center at the time of first login to the system.
- System users, who can configure credentials:
  - In **Design | Network Settings**.
  - When adding and running a discovery task.

When devices do not have credentials, or when their credentials do not match the ones that were configured previously, Cisco DNA Center logs in to the device by using CLI and applies the credentials that are included in the task, which causes a device configuration change.

Configuration Change: Because Cisco DNA Center must have device credentials to complete discovery and add devices to **Inventory**, the system applies the configuration that adds those credentials to the devices.

The system does not overwrite or delete any existing configuration in this process.

The automated process that applies device credentials occurs by using **Device Controllability**, which is an administrative setting in **System Settings**.



Device Controllability

Device Controllability is a system-level process on Cisco DNA Center that enforces state synchronization for some device-layer ne depl
required network settings that Cisco DNA Center needs to manage devices. Changes are made on network devices during disc Invento
Controllability is a runtime condition as well. Therefore, if changes are made to any settings that are under the scope of this pro on the
devices immediately. The following device settings are within the scope of Device Controllability:

- SNMP credentials
- NETCONF credentials
- Cisco TrustSec (CTS) credentials
- IPDT enablement
- Controller certificates
- SNMP trap server definitions
- Syslog server definitions
- Netflow collector definitions
- Wireless network assurance

If Device Controllability is disabled, Cisco DNA Center does not configure any of the credentials or features mentioned above on devices during discovery or at runtime.

On installation of Cisco DNA Center, **Device Controllability** is enabled by default.

Caution: While administrators can disable **Device Controllability** at any time, including before or after discovery, use caution because the changes that system users make when the feature is disabled might not be recoverable.

The feature also supports critical aspects of system and SD-Access automation.

For more information, refer to the detailed answer.

When devices become available in **Inventory** and are in a managed state, **Device Controllability** also automatically configures the following.

- Cisco TrustSec (CTS) credentials, which support enforcing policies that define access to the network and applications
- IP device tracking (IPDT enablement), which it applies to every host port on the device so that Cisco DNA Center can determine connectivity

For all switches other than Nexus series switches, all routers, and AireOS-WLCs:

- The Cisco DNA Center certificate, which also includes:
  - The public key infrastructure (PKI)
  - The http source interface configuration, which enables to Cisco DNA Center to reach the device by using the source interface

  The certificate enables HTTPS communication and file transfer from the device to Cisco DNA Center.

> **Important Note:** The software image management and upgrade process (SWIM) requires devices to have the certificate to support file transfers.
>
> During upgrades, the system validates that the certificate is available on the device before the upgrade can continue.

For wireless LAN controllers, the Wireless Network Assurance function:

- Installs a streaming telemetry certificate.
- Configures the streaming telemetry service, which enables Cisco DNA Center to capture a continuous flow of operational status data as it occurs.

On an ongoing basis, when changes to various credentials, certificates, servers, or protocol definitions occur in Cisco DNA Center, **Device Controllability** applies those configuration changes to the applicable devices automatically and immediately.

What Are The Steps That I Take To…

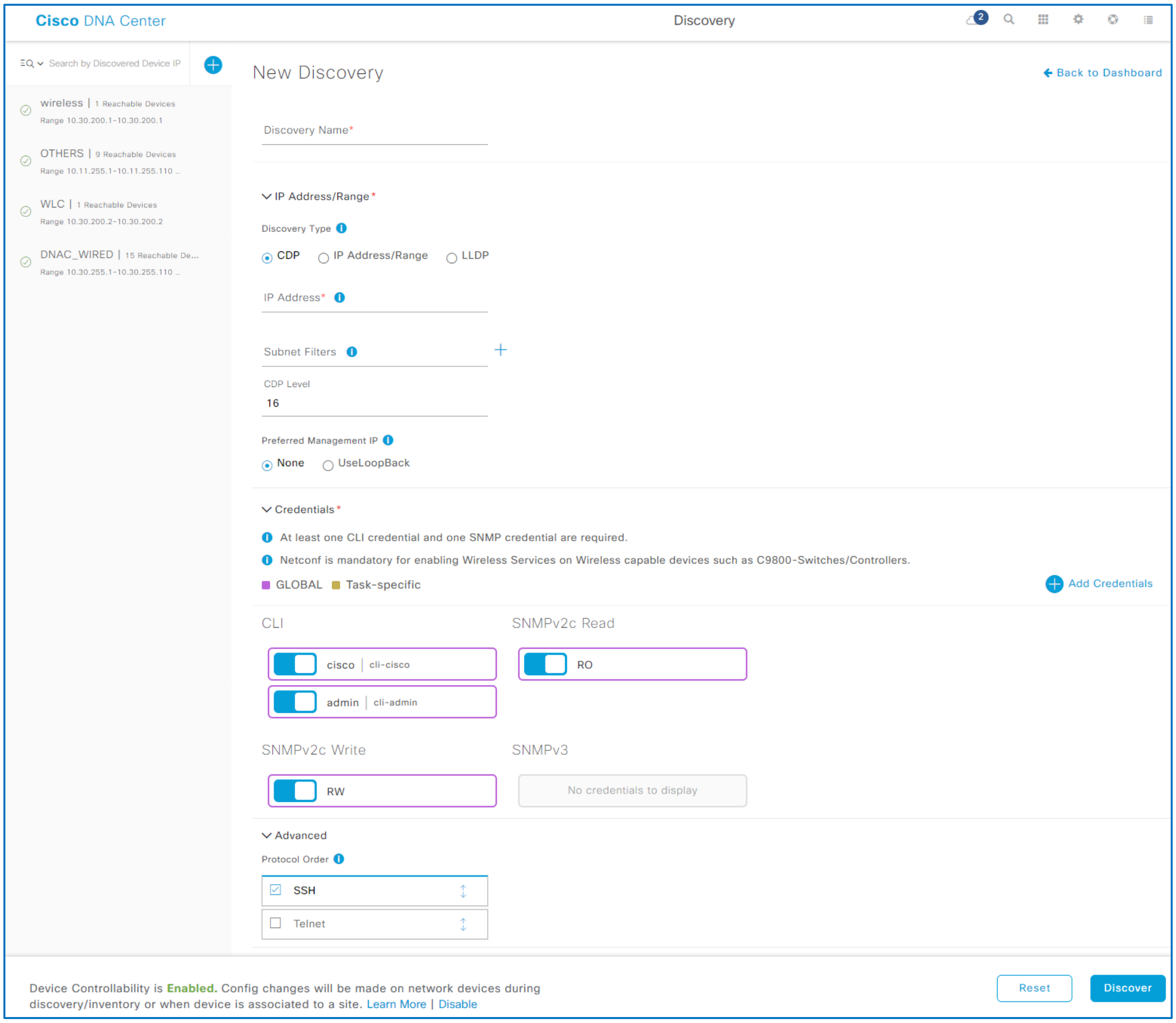
…Open the Discovery Dashboard?

You configure and run discovery tasks on the **New Discovery** page, which is accessible on the **Discovery Dashboard**.

Configuration Change: Be aware that device configuration changes occur during and after discovery by using the **Device Controllability** feature.

When you run a discovery task, **Device Controllability** applies configuration changes automatically that allow it to establish communication with and manage devices.

For more information, refer to the **By Recognizing the Device Configuration Changes That Occur in this Process** topic.



wireless | 1 Reachable Devices
Range 10.30.200.1-10.30.200.1

OTHERS | 9 Reachable Devices
Range 10.11.255.1-10.11.255.110 ..

WLC | 1 Reachable Devices
Range 10.30.200.2-10.30.200.2

DNAC_WIRED | 15 Reachable De...
Range 10.30.255.1-10.30.255.110 ..

New Discovery

Discovery Name*

IP Address/Range*

Discovery Type

● CDP ○ IP Address/Range ○ LLDP

IP Address*

Subnet Filters

CDP Level
16

Preferred Management IP

● None ○ UseLoopBack

Credentials*

At least one CLI credential and one SNMP credential are required.

Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers.

GLOBAL Task-specific

CLI
- cisco | cli-cisco
- admin | cli-admin

SNMPv2c Read
- RO

SNMPv2c Write
- RW

SNMPv3
- No credentials to display

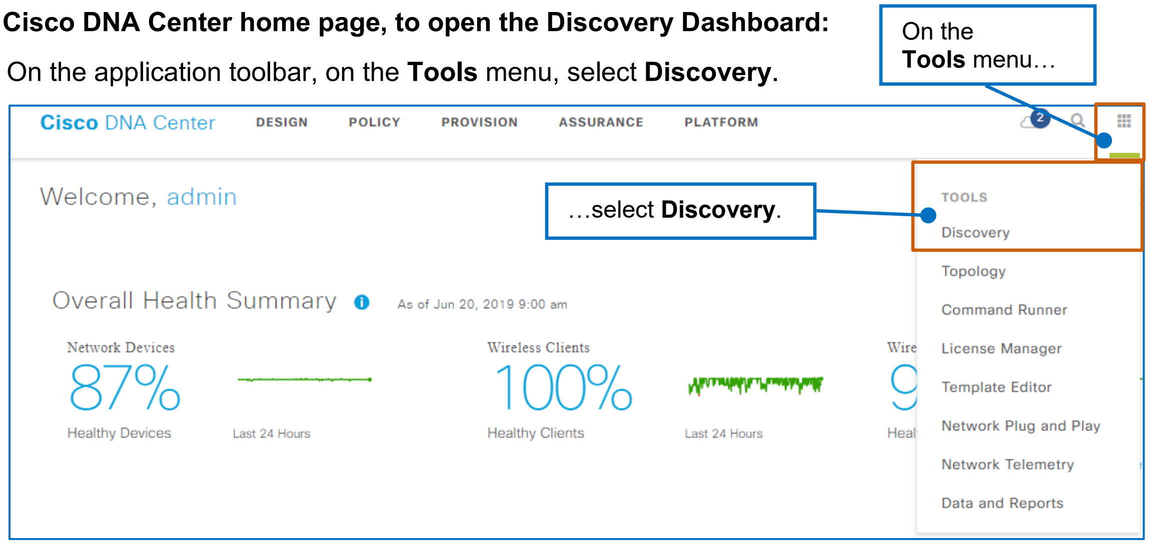
Advanced

Protocol Order
- ☑ SSH
- □ Telnet

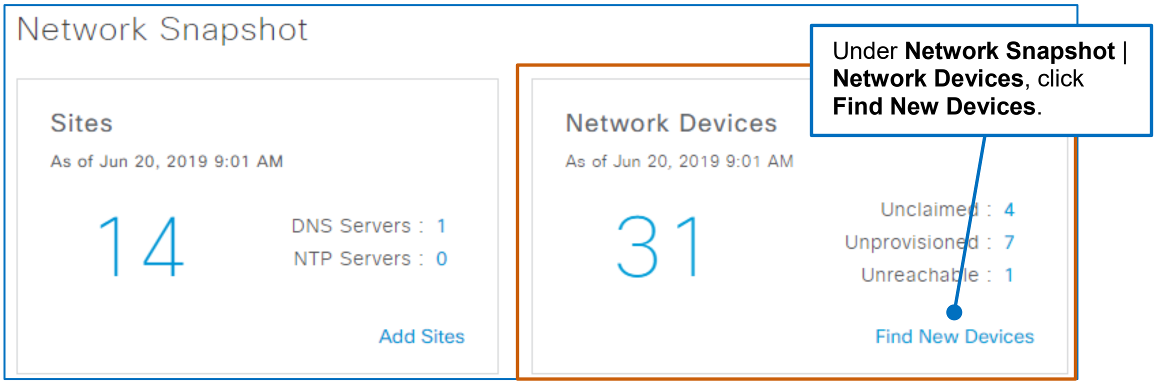
Device Controllability is **Enabled.** Config changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn More | Disable

On the Cisco DNA Center home page, to open the Discovery Dashboard:

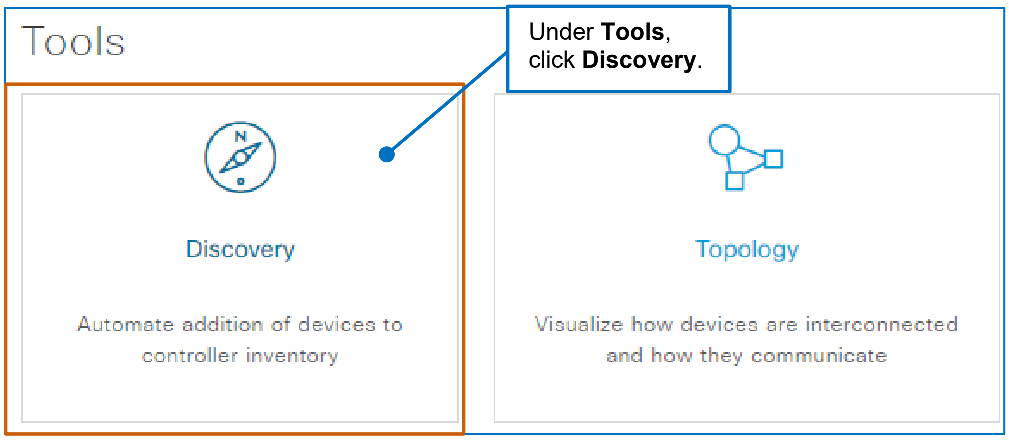
- On the application toolbar, on the **Tools** menu, select **Discovery**.



- Under **Network Snapshot | Network Devices**, click **Find New Devices**.



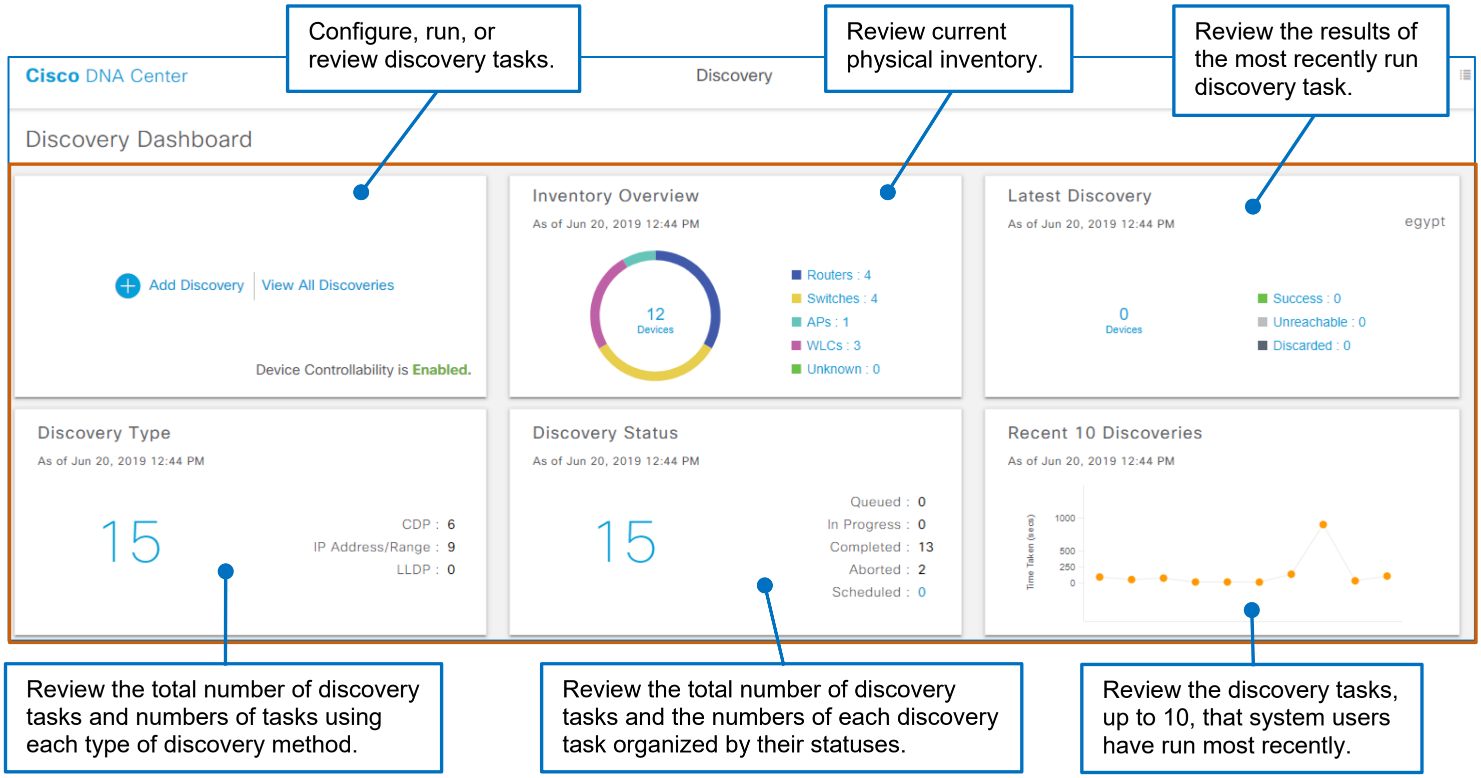
- Under **Tools**, click **Discovery**.


Tools
Under **Tools**, click **Discovery**.
Discovery
Automate addition of devices to controller inventory
Topology
Visualize how devices are interconnected and how they communicate

Each of these actions opens the **Discovery Dashboard** page.

…Navigate the Discovery Dashboard?

The **Discovery Dashboard** page provides an overview of discovery-related tasks, types, and statuses and the Cisco DNA Center physical device inventory.



Configure, run, or review discovery tasks.

Review current physical inventory.

Review the results of the most recently run discovery task.

Cisco DNA Center — Discovery

Discovery Dashboard

⊕ Add Discovery | View All Discoveries

Device Controllability is **Enabled.**

Inventory Overview
As of Jun 20, 2019 12:44 PM
12 Devices
■ Routers : 4
■ Switches : 4
■ APs : 1
■ WLCs : 3
■ Unknown : 0

Latest Discovery
As of Jun 20, 2019 12:44 PM
egypt
0 Devices
■ Success : 0
■ Unreachable : 0
■ Discarded : 0

Discovery Type
As of Jun 20, 2019 12:44 PM
15
CDP : 6
IP Address/Range : 9
LLDP : 0

Discovery Status
As of Jun 20, 2019 12:44 PM
15
Queued : 0
In Progress : 0
Completed : 13
Aborted : 2
Scheduled : 0

Recent 10 Discoveries
As of Jun 20, 2019 12:44 PM

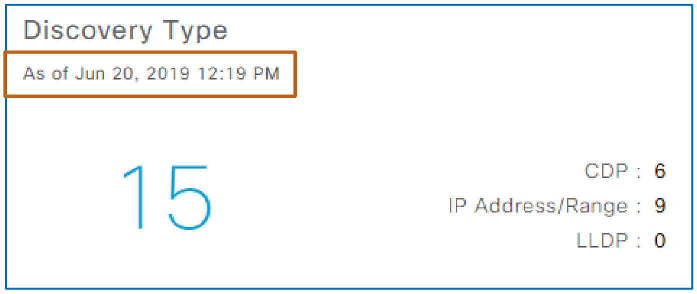
Review the total number of discovery tasks and numbers of tasks using each type of discovery method.

Review the total number of discovery tasks and the numbers of each discovery task organized by their statuses.

Review the discovery tasks, up to 10, that system users have run most recently.

The data is current as of the time that you opened the page; or you refreshed the page manually. The dashlet time stamps indicate the most recent time that the page refreshed.

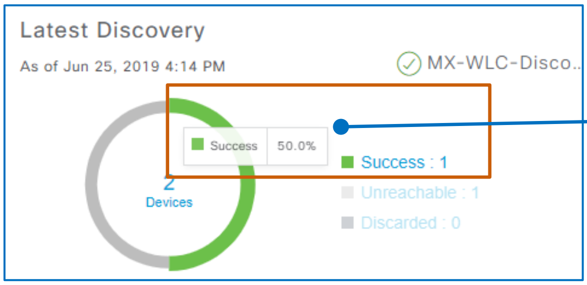
Tip: To ensure that you are seeing current information, refresh the page manually.



Discovery Type
As of Jun 20, 2019 12:19 PM
15
CDP : 6
IP Address/Range : 9
LLDP : 0

When you click links or chart segments on discovery-related dashlets, the system opens the results page with the applicable task active and, on the left, filters the device list based on the link or chart segment that you clicked.

For example, in the screenshots below, in the **Latest Discovery** dashlet, when you click the **Success** segment for the **MX-WLC Discovery** task…

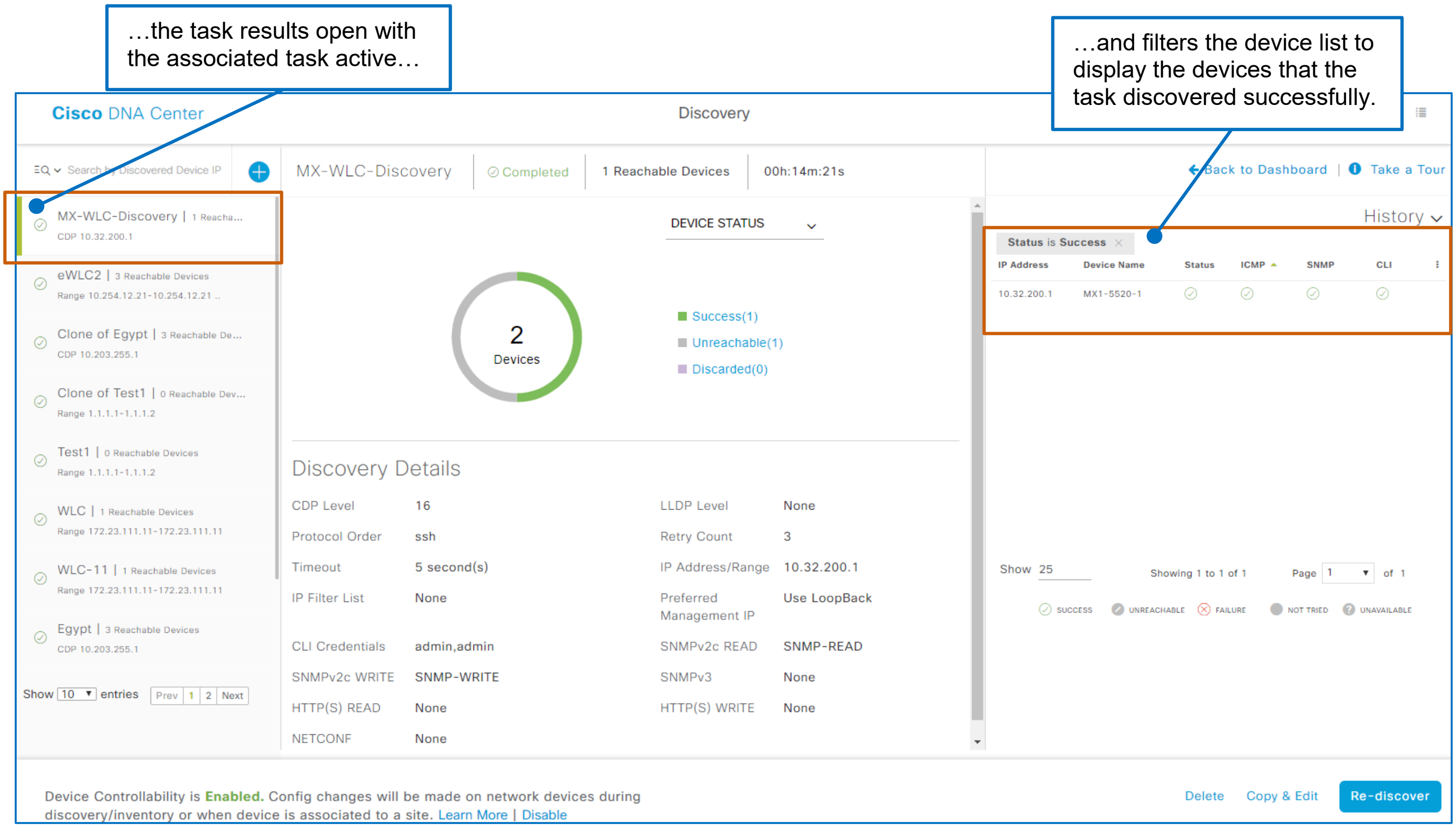


Latest Discovery

As of Jun 25, 2019 4:14 PM

When you click the **Success** segment or link…

…the task results page opens with the results of the **MX-WLC Discovery** task active, and the list filtered to display only those devices that the task discovered successfully.



…the task results open with the associated task active…

…and filters the device list to display the devices that the task discovered successfully.

Cisco DNA Center
Discovery
Search by Discovered Device IP
MX-WLC-Discovery
Completed
1 Reachable Devices
00h:14m:21s
Back to Dashboard | Take a Tour
MX-WLC-Discovery | 1 Reacha...
CDP 10.32.200.1
eWLC2 | 3 Reachable Devices
Range 10.254.12.21-10.254.12.21 ..
Clone of Egypt | 3 Reachable De...
CDP 10.203.255.1
Clone of Test1 | 0 Reachable Dev...
Range 1.1.1.1-1.1.1.2
Test1 | 0 Reachable Devices
Range 1.1.1.1-1.1.1.2
WLC | 1 Reachable Devices
Range 172.23.111.11-172.23.111.11
WLC-11 | 1 Reachable Devices
Range 172.23.111.11-172.23.111.11
Egypt | 3 Reachable Devices
CDP 10.203.255.1
Show 10 entries Prev 1 2 Next
DEVICE STATUS
2
Devices
Success(1)
Unreachable(1)
Discarded(0)
History
Status is Success
Show 25
Showing 1 to 1 of 1
Page 1 of 1
SUCCESS
UNREACHABLE
FAILURE
NOT TRIED
UNAVAILABLE
Delete
Copy & Edit
Re-discover

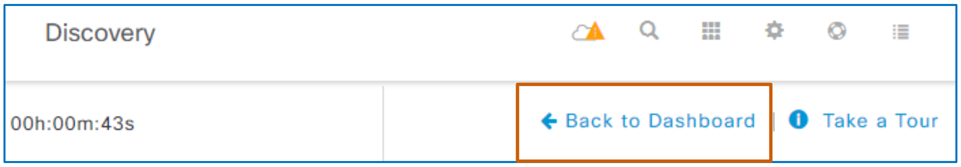
Discovery Details

CDP Level	16	LLDP Level	None
Protocol Order	ssh	Retry Count	3
Timeout	5 second(s)	IP Address/Range	10.32.200.1
IP Filter List	None	Preferred Management IP	Use LoopBack
CLI Credentials	admin,admin	SNMPv2c READ	SNMP-READ
SNMPv2c WRITE	SNMP-WRITE	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None
NETCONF	None		

IP Address	Device Name	Status	ICMP	SNMP	CLI
10.32.200.1	MX1-5520-1	✓	✓	✓	✓

Device Controllability is **Enabled.** Config changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn More | Disable

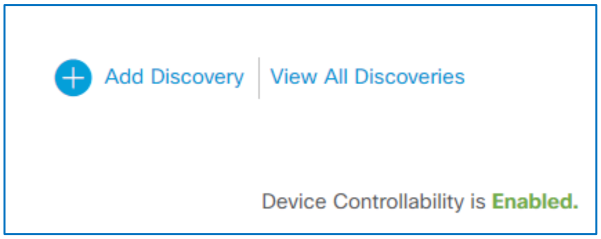
When you open a discovery-related page by using a link on the **Discovery Dashboard** page, a **Back to Dashboard** link is available below the application menu bar for efficient navigation back to the **Discovery Dashboard** page.



Starting or Reviewing Discovery Tasks

The **Add Discovery | View All Discoveries** dashlet provides links to the pages on which you can:

- Configure and run a custom discovery task.
- Review the list of all of the discovery tasks that system users have run previously.



Device Controllability is Enabled.

Tip: You can copy and customize discovery tasks that system users have run previously.

When you need to run the same, or a similar task, this method provides an efficient way to configure it.

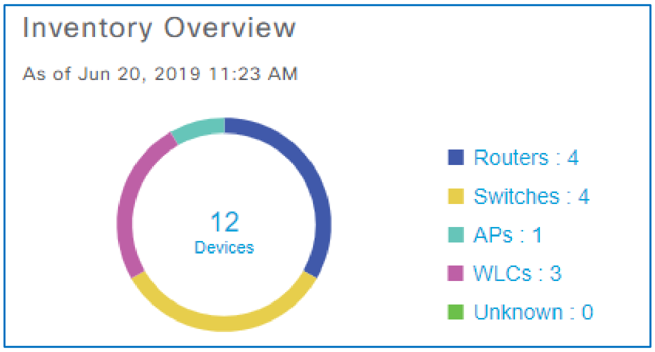
The dashlet also indicates whether **Device Controllability** is enabled in the system. Because **Device Controllability** applies various types of configuration to devices in the discovery process, it is important to know whether these configurations will occur when you run a discovery task.

Note: For more information, refer to the **By Recognizing the Device Configuration Changes that Can Occur in this Process** topic.

Reviewing or Navigating to Cisco DNA Center Inventory

The **Inventory Overview** dashlet presents an interactive chart and list of the current Cisco DNA Center inventory in all management states. The list indicates the total number of each device type in the inventory.

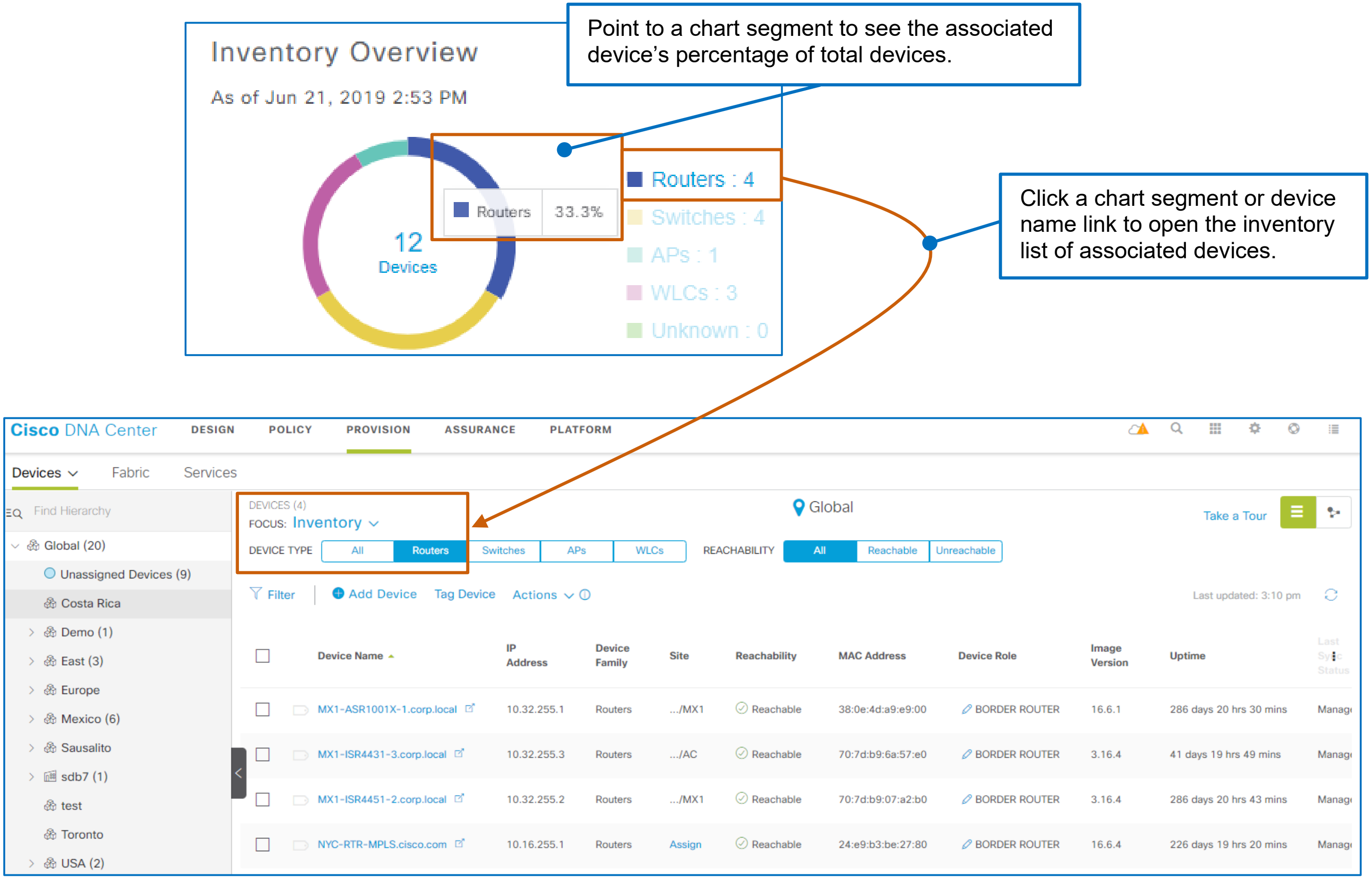
The **Unknown** category includes devices from which the system cannot collect data. Data collection can fail, for example, when the system cannot query the system-defined standard MIBs on the device or the device credentials are not valid.



When you open **Inventory** by using the chart or links on the **Inventory Overview** dashlet, you can return to the **Discovery Dashboard** page by using the various available methods.

To see the percentage of a device type out of the total number of devices, you can point to a chart segment. This action also emphasizes the associated device type in the list.

To navigate to **Inventory** and see the list of associated devices, you can click a chart segment or device name link.



Point to a chart segment to see the associated device's percentage of total devices.

Click a chart segment or device name link to open the inventory list of associated devices.

DEVICES (4)
FOCUS: Inventory

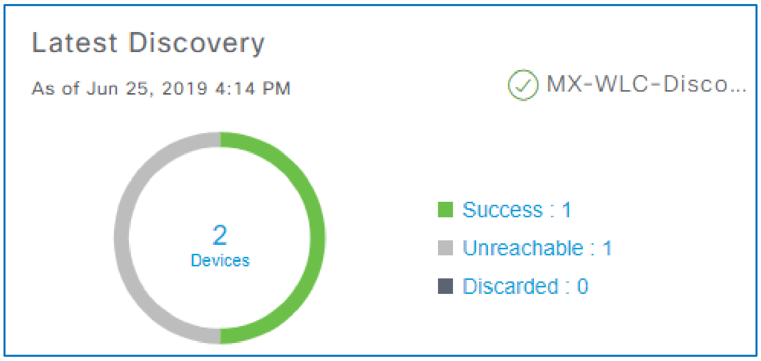
DEVICE TYPE: All | **Routers** | Switches | APs | WLCs

REACHABILITY: **All** | Reachable | Unreachable

□	Device Name	IP Address	Device Family	Site	Reachability	MAC Address	Device Role	Image Version	Uptime	Last Sync Status
□	MX1-ASR1001X-1.corp.local	10.32.255.1	Routers	.../MX1	Reachable	38:0e:4d:a9:e9:00	BORDER ROUTER	16.6.1	286 days 20 hrs 30 mins	Manag
□	MX1-ISR4431-3.corp.local	10.32.255.3	Routers	.../AC	Reachable	70:7d:b9:6a:57:e0	BORDER ROUTER	3.16.4	41 days 19 hrs 49 mins	Manag
□	MX1-ISR4451-2.corp.local	10.32.255.2	Routers	.../MX1	Reachable	70:7d:b9:07:a2:b0	BORDER ROUTER	3.16.4	286 days 20 hrs 43 mins	Manag
□	NYC-RTR-MPLS.cisco.com	10.16.255.1	Routers	Assign	Reachable	24:e9:b3:be:27:80	BORDER ROUTER	16.6.4	226 days 19 hrs 20 mins	Manag

Reviewing the Results of the Most Recently Run Discovery Task

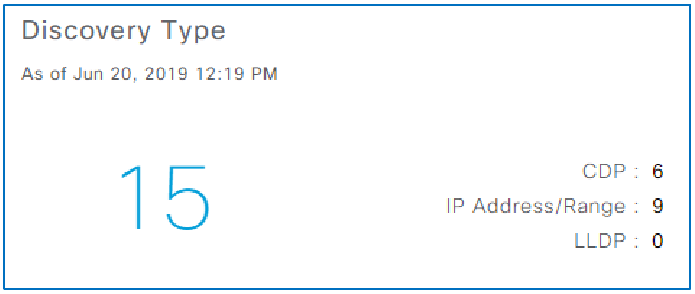
The **Latest Discovery** dashlet presents an interactive chart and list of status results for the discovery task that a system user has run most recently based on the Cisco DNA Center server time.



Reviewing Numbers of Discovery Tasks Categorized by Their Method Types

The **Discovery Type** dashlet indicates the total number of completed tasks in the system with a link.

It also categorizes the number of tasks that used each type of discovery method.



Discovery Type

As of Jun 20, 2019 12:19 PM

15

CDP : 6
IP Address/Range : 9
LLDP : 0

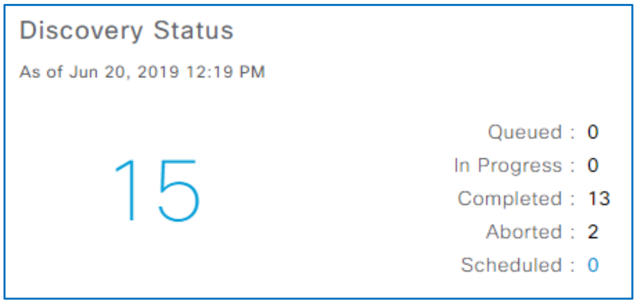
Reviewing Numbers of Discovery Tasks Categorized by Their Running Statuses

The **Discovery Status** dashlet indicates the total number of completed tasks in the system with a link.

It also categorizes the number of tasks based on their running statuses, which include:

- **Queued**
  Tasks that the system is preparing to run

  The system briefly queues tasks when system users run them immediately. When system users initiate several tasks to run immediately, the system queues the tasks and runs them consecutively in the order that they were initiated. The total number of tasks will appear as **Queued** until the you refresh the page.



Discovery Status

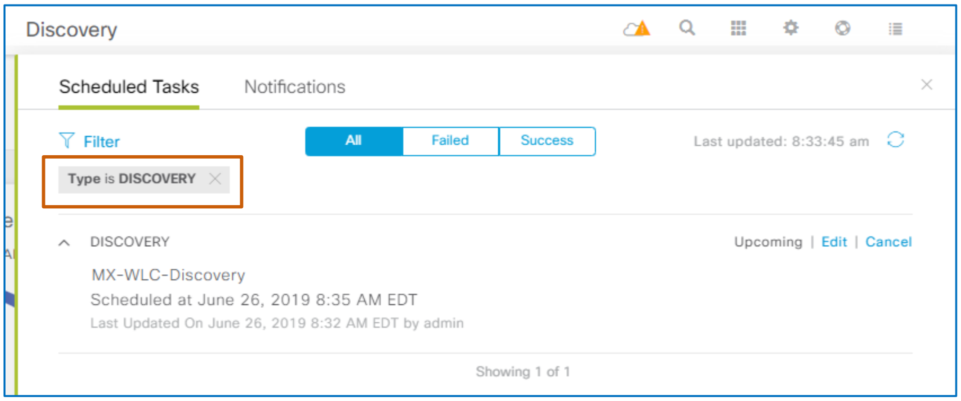
As of Jun 20, 2019 12:19 PM

15

Queued : 0
In Progress : 0
Completed : 13
Aborted : 2
Scheduled : 0

- **In Progress**
  Tasks that the system is preparing to run
- **Completed**
  Tasks that have finished running
- **Aborted**
  Tasks that system users started and then stopped before the tasks completed
- **Scheduled**
  Tasks that system users scheduled to run later

The **Scheduled** status provides a number link, which opens a panel. The **Scheduled Task**s tab is filtered automatically to list the discovery tasks that system users have scheduled to run later.



Discovery

Scheduled Tasks | Notifications

Filter | All | Failed | Success

Last updated: 8:33:45 am

Type is DISCOVERY

DISCOVERY — Upcoming | Edit | Cancel

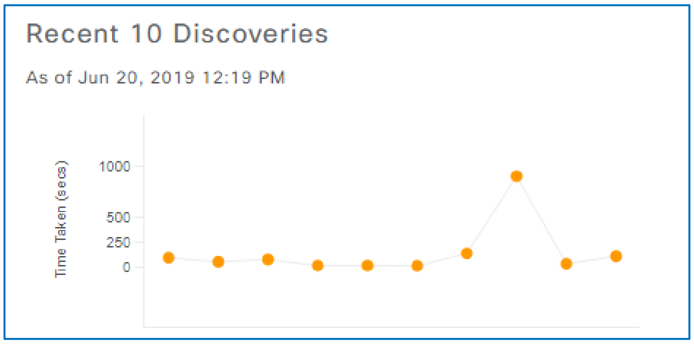
MX-WLC-Discovery
Scheduled at June 26, 2019 8:35 AM EDT
Last Updated On June 26, 2019 8:32 AM EDT by admin

Showing 1 of 1

Reviewing the Time the Most Recent Discovery Tasks Took to Complete

The **Recent 10 Discoveries** dashlet illustrates the amount of time each of the most recently completed discovery tasks, up to 10, took to complete. The data point color helps illustrate the time of each job and does not indicate their statuses.

This information provides insight into the amount of time you might expect a discovery task to run, which can be helpful when determining whether a task is taking an extensive amount of time to complete.



Recent 10 Discoveries

As of Jun 20, 2019 12:19 PM

…Add Devices by Using CDP or LLDP?

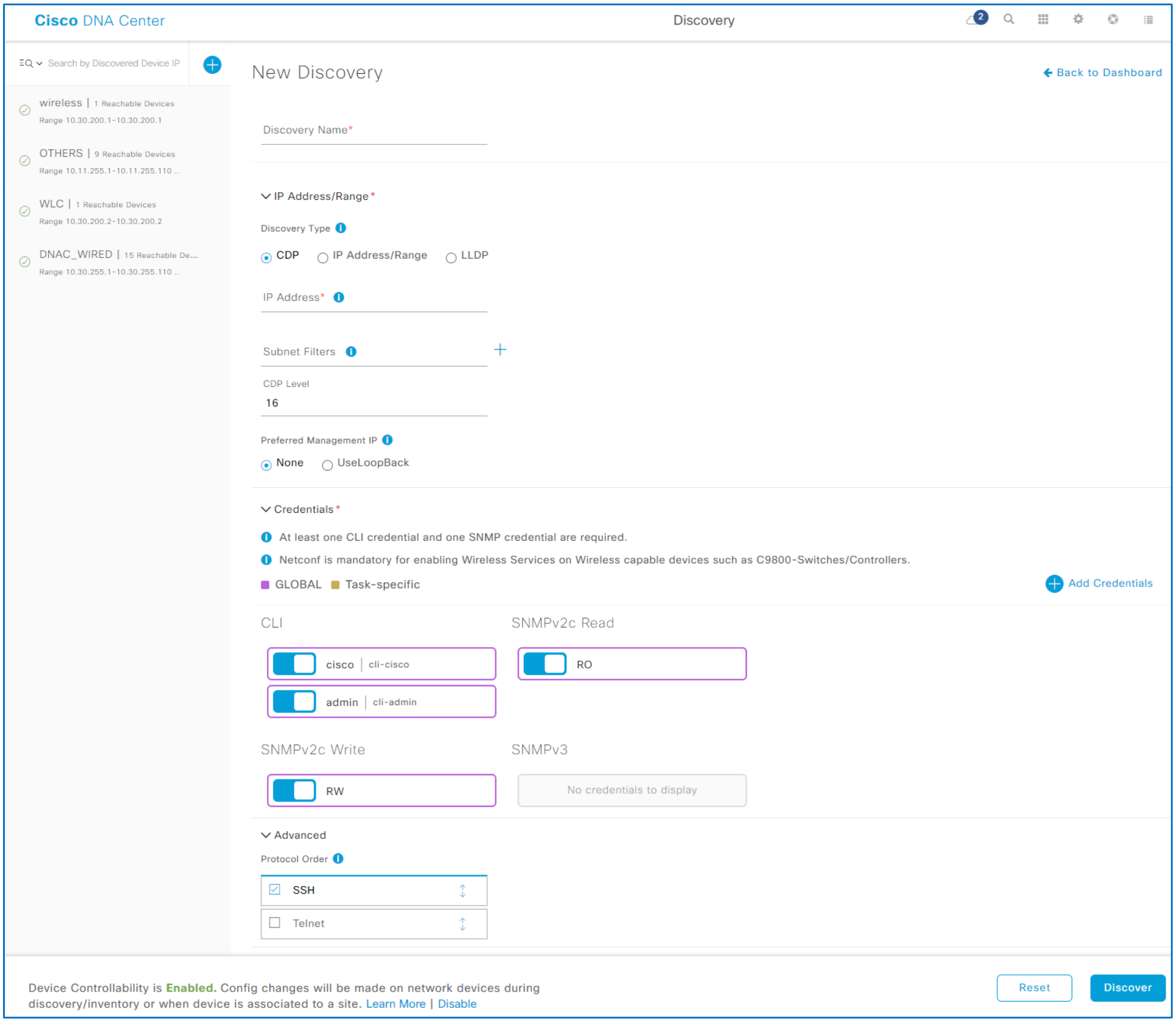
You add devices on the **New Discovery** page.

Configuration Change: Be aware that device configuration changes occur automatically in the discovery process by using the **Device Controllability** feature, including configuration that allows Cisco DNA Center to:

- Establish communication with and manage devices.
- Support ongoing device management when specific setting changes occur.

For more information, refer to the **By Recognizing the Device Configuration Changes that Can Occur in this Process** topic.

Tip: When you need to discover a group of devices that include some that share common credentials and others with discrete and varying credentials, you can run a series of discovery tasks to address the varying credential requirements.



Cisco DNA Center — Discovery

Search by Discovered Device IP

wireless | 1 Reachable Devices
Range 10.30.200.1-10.30.200.1

OTHERS | 9 Reachable Devices
Range 10.11.255.1-10.11.255.110 ..

WLC | 1 Reachable Devices
Range 10.30.200.2-10.30.200.2

DNAC_WIRED | 15 Reachable De...
Range 10.30.255.1-10.30.255.110 ..

New Discovery — Back to Dashboard

Discovery Name*

IP Address/Range*

Discovery Type: ● CDP ○ IP Address/Range ○ LLDP

IP Address*

Subnet Filters

CDP Level: 16

Preferred Management IP: ● None ○ UseLoopBack

Credentials*

At least one CLI credential and one SNMP credential are required.

Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers.

GLOBAL Task-specific — Add Credentials

CLI: cisco | cli-cisco; admin | cli-admin

SNMPv2c Read: RO

SNMPv2c Write: RW

SNMPv3: No credentials to display

Advanced

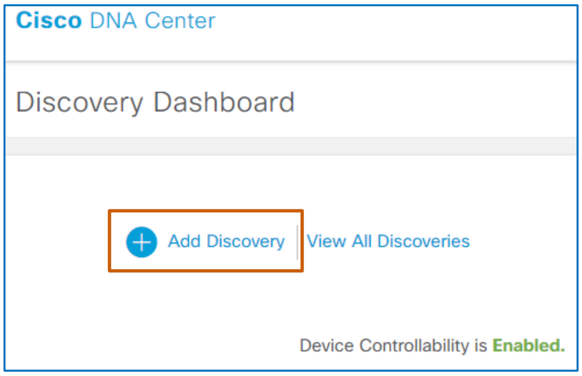
Protocol Order

☑ SSH
☐ Telnet

Device Controllability is **Enabled.** Config changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn More | Disable

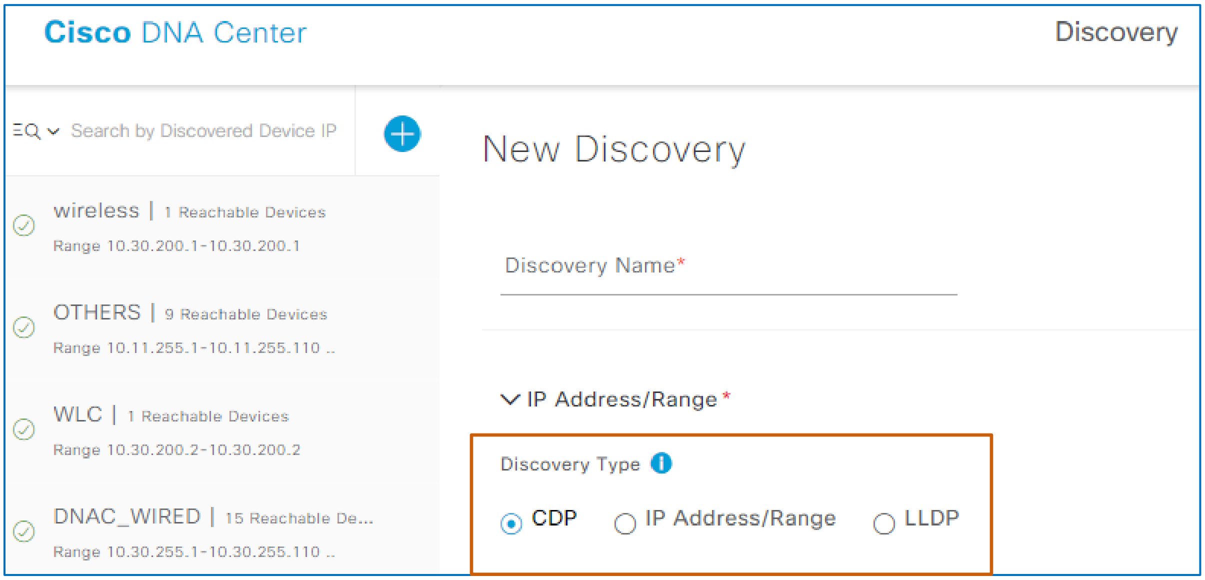
To discover devices by using CDP or LLDP:

1. On the **Discovery Dashboard**, in the dashlet, click **Add Discovery**.



Device Controllability is Enabled.

The **Discovery | New Discovery** page opens, and the **CDP** method of discovery is selected by default.



wireless | 1 Reachable Devices
Range 10.30.200.1-10.30.200.1

OTHERS | 9 Reachable Devices
Range 10.11.255.1-10.11.255.110 ..

WLC | 1 Reachable Devices
Range 10.30.200.2-10.30.200.2

DNAC_WIRED | 15 Reachable De...
Range 10.30.255.1-10.30.255.110 ..

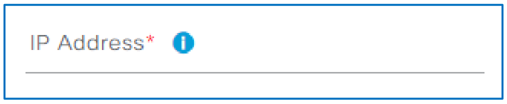
● CDP ○ IP Address/Range ○ LLDP

2. In the **Discovery Name** field, type a unique, meaningful name for the task.

3. Under **Discovery Type**:

   - To configure a CDP discovery task, accept the default selection of **CDP**.
   - To configure an LLDP discovery task, select **LLDP**.

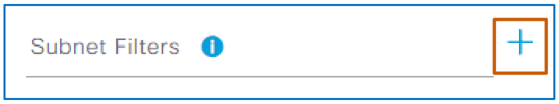
4. To identify the device that you want the task to use as a starting point (seed device), in the **IP Address** field, type the device's IP address.



5. Optionally, to exclude a subnet or subnets from the discovery process, in the **Subnet Filters** field:

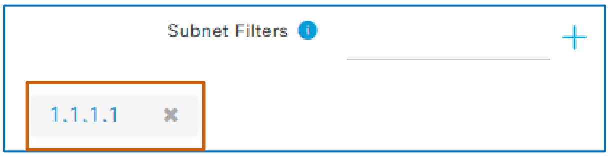
   - To exclude a specific subnet, type the subnet's IP address

- To exclude all of the subnets in an address range, type the classless inter-domain routing (CIDR) address.

  Subnet Filters

  The system adds each address below the field. You can exclude more than one subnet.

  Subnet Filters

  1.1.1.1

  Tip: Excluding subnets is helpful when you want to avoid discovering large numbers of devices that you do not need to add.

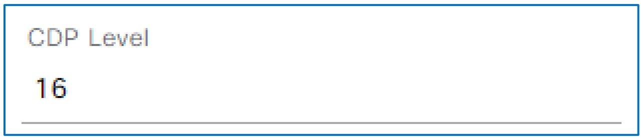
  When you exclude subnets in a discovery task and the task finds devices in those subnets during discovery, it indicates them as **Discarded** in the discovery task results.

  The task results include the total number of discarded devices only. Discarded devices are not discovered or added to the inventory.

6. To indicate the number of hops from the starting device IP address that you want the discovery task to take to discover devices, based on whether you are using the CDP or LLDP methods, in the **CDP Level** or **LLDP Level** field, type the level number.

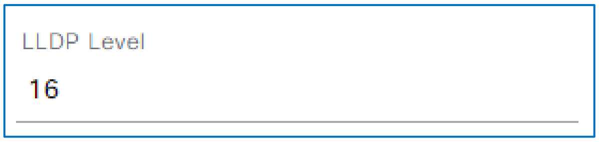
   Caution: When you are discovering a large number of devices, accepting the 16 hop default selection can cause the discovery task run time to be extensive or cause the task to discover more devices than you intended.

   Adjust the number of hops based on the goals of the discovery task that you are running and the number of devices that you need the task to discover to ensure that you add only those devices that you need.



CDP Level

16



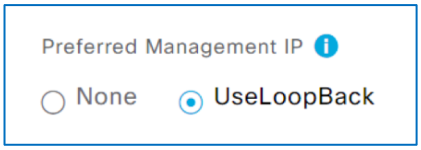
LLDP Level

16

7. To indicate the IP address type that you want the system to assign as the management IP address, in the **Preferred Management IP** drop-down list:

   - To apply the IP address in the **IP Address** field that you defined in step 4, select **None**.
   - To allow the system to determine and select the optimal management IP address on the device, select **Use Loopback**.

   > **Important Note:** To determine the IP address when there are multiple loopback addresses or no loopback address present, the system selects the highest numbered IP address based on interface type in the following order:
   >
   > a. Loopback interface
   > b. Ethernet interface
   > c. Token ring interface
   > d. Serial interface IP address with the highest increment. The system cannot apply sub-interface IP addresses.
   > e. Virtual interface
   >
   > When devices have more than one loopback address, the time to complete the discovery process can take longer because the system must connect to each IP address, test its reachability, and validate its credentials.



Preferred Management IP ⓘ

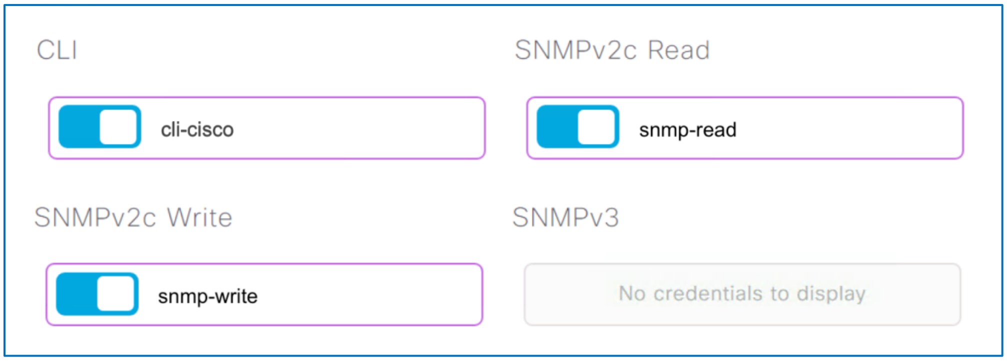
○ None ● UseLoopBack

8. To indicate the credentials that the discovery task will use to access devices:

   > **Important Note:** When you need to include Cisco Enterprise NFV Infrastructure Software (NFVIS) devices in the discovery task, you need to indicate HTTPS credentials.
   >
   > **Note:** For more information on credentials and color coding, refer to the **By Recognizing How the Global Credential Settings in Design…** topic.

   a. To manage global credentials, below **Credentials**:

      - To use global credentials in the task, accept the default selections.
      - To disable global credentials, click the credential button, which toggles the button to an inactive state and changes the color-coding to gray.



CLI: cli-cisco

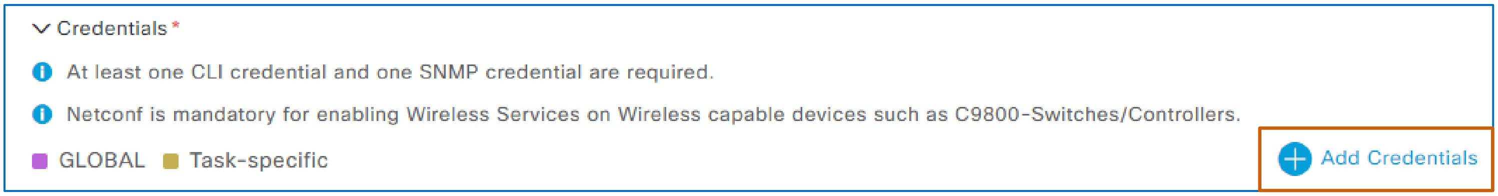
SNMPv2c Read: snmp-read

SNMPv2c Write: snmp-write

SNMPv3: No credentials to display

b. Optionally, when global credentials are unavailable, or devices have unique requirements, to add task-specific credentials:

i. Click **Add Credentials**.



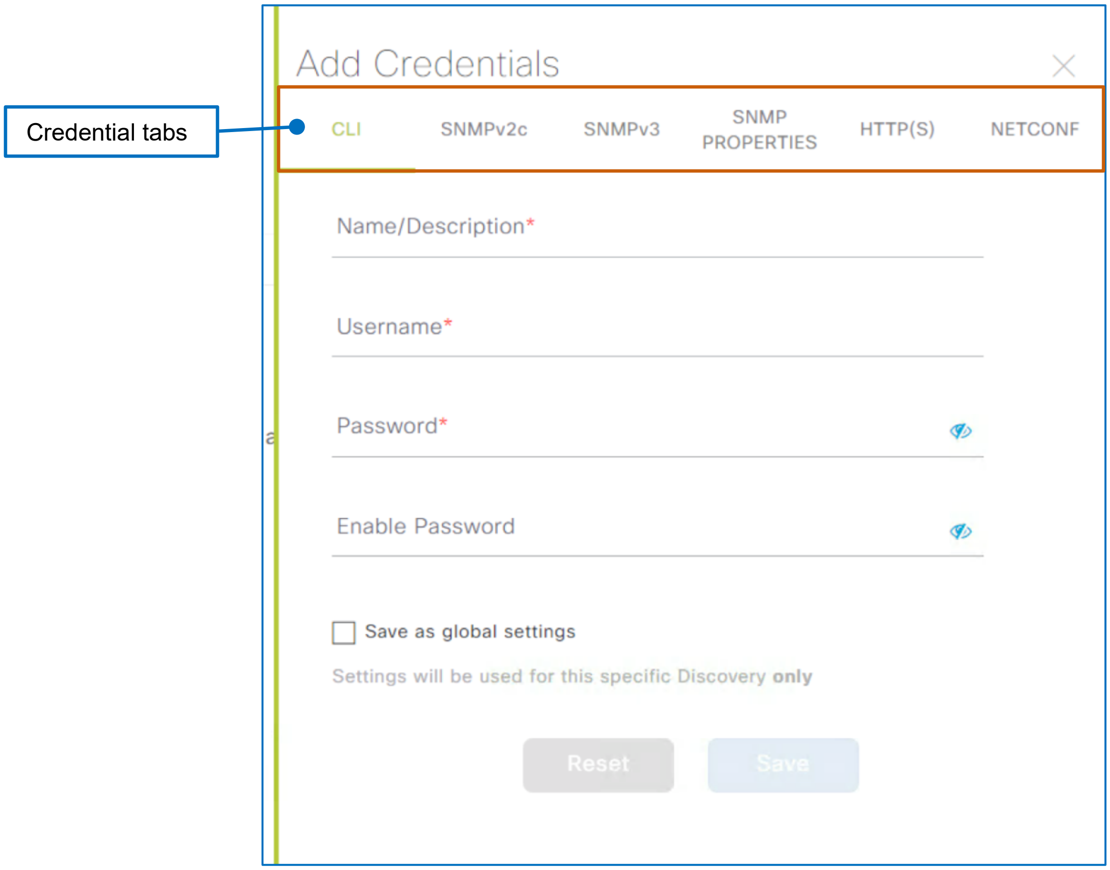
Credentials *

ℹ At least one CLI credential and one SNMP credential are required.

ℹ Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers.

🟪 GLOBAL 🟨 Task-specific

The **Add Credentials** panel opens and indicates the active credential tab in green.



Name/Description*

Username*

Password*

Enable Password

□ Save as global settings

Settings will be used for this specific Discovery **only**

ii. In the **Add Credentials** panel, click the tab for the type of credentials that you need, and then add the required details and optional details, as needed.

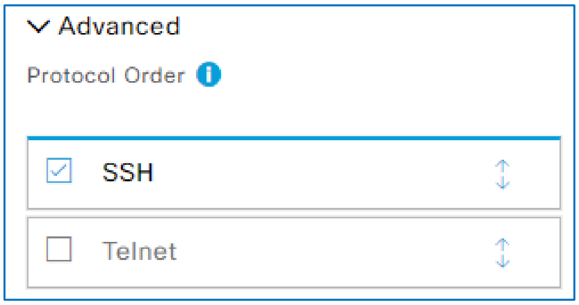
Note: To review the field level settings for each credential type, [refer to the Cisco Digital Network Architecture Center User Guide](#).

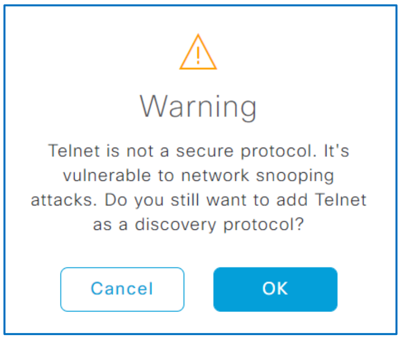
iii. Optionally, to save the credentials that you add for use in subsequent discovery tasks, select the **Save as global settings** check box.

Note: The system adds the credentials in **Design | Network Settings | Device Credentials** when you save the credentials.

iv. To finish adding credentials, click **Save**.

9. To include the Telnet communication protocol in addition to SSH, expand the **Advanced** section, select the **Telnet** check box, and then, in the system message, click **OK**.



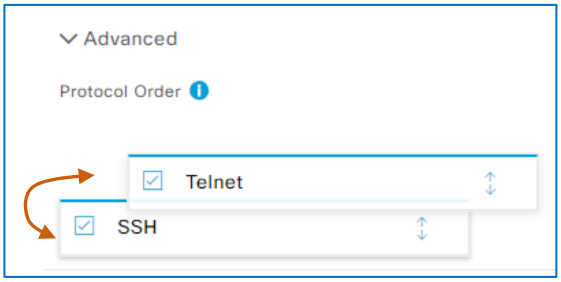


Telnet is not a secure protocol. It's vulnerable to network snooping attacks. Do you still want to add Telnet as a discovery protocol?

Tip: When using both communication protocols for discovery, the system applies the protocols in top down order. You can change the order in which the system applies each protocol when running the task.

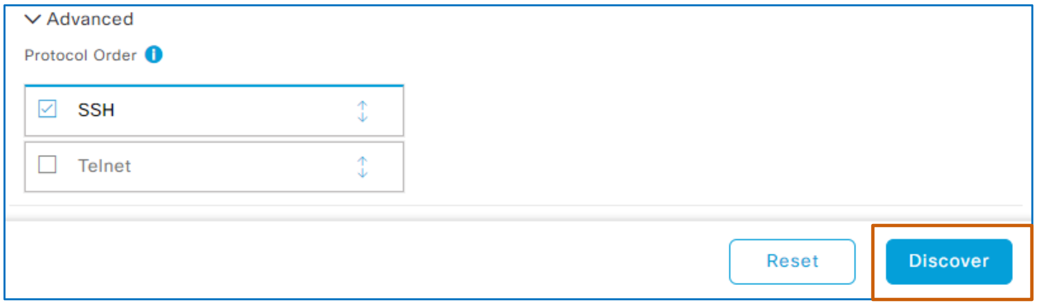
To change the order of protocols:

- Drag the protocol item to the position that you want.

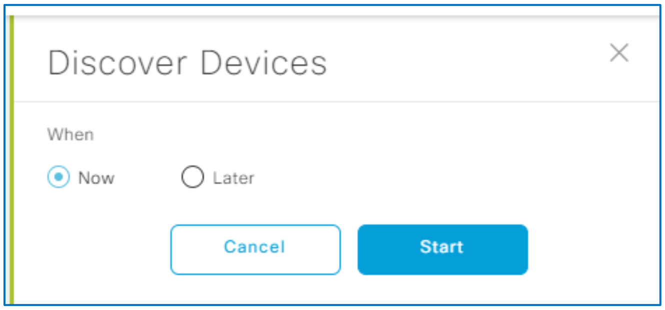


10. To initiate the discovery task, click **Discover**.

Tip: To return all of the fields to the default settings, click **Reset**.



The **Discover Devices** panel opens.



11. To start or schedule the task:

    - To start the task immediately, click **Now**, and then click **Start**.

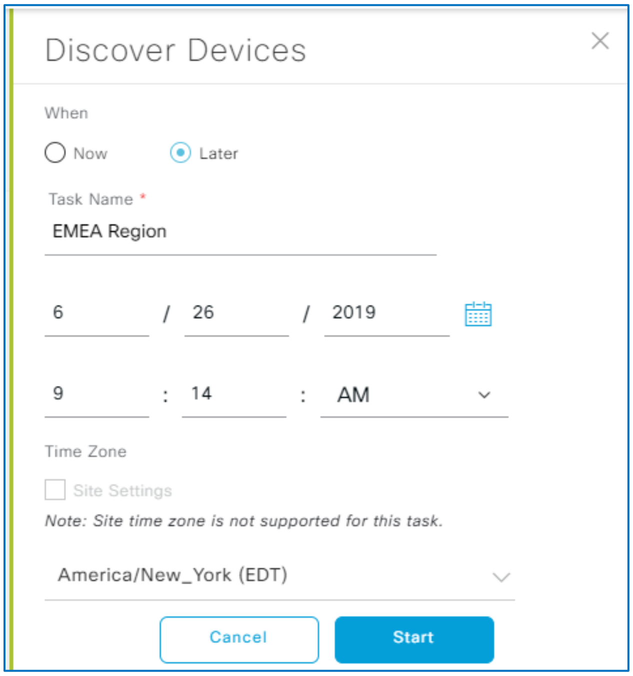
      The panel closes. The task appears in the list on the left, and the system queues and then begins running the task. You can review the task progress or its results.

      Note: The system queues the task for approximately 10 seconds before the task begins running.

      You have completed the process to run the discovery task.

    - To schedule the task to occur at specific time, click **Later**.

      The **Discover Devices** panel opens. In the panel, the **Task Name** field is populated with the name in the **Discovery Name** field and the scheduling fields are populated with the current date, time, and time zone of the local device.



Discover Devices

When

○ Now ● Later

Task Name *

EMEA Region

6 / 26 / 2019

9 : 14 : AM

Time Zone

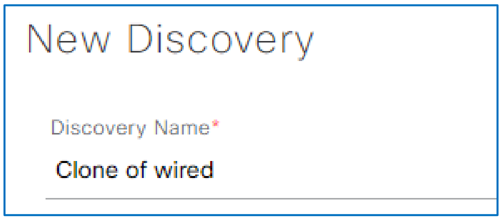
□ Site Settings

Note: Site time zone is not supported for this task.

America/New_York (EDT)

12. Based on the task, determine whether you need to change the task name.

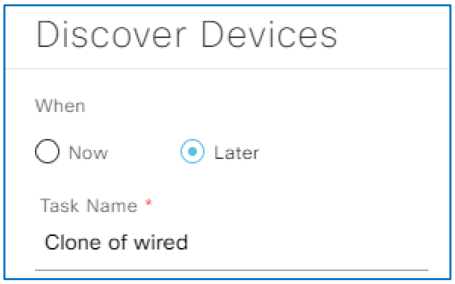
    - When adding a new discovery task or by using **Copy & Edit**, in the **Task Name** field, retain the task name that you added or changed in the **Discovery Name** field.



New Discovery

Discovery Name*

Clone of wired



Discover Devices

When

○ Now ● Later

Task Name *

Clone of wired

    - When reusing a previously run task by using **Re-discover**:
      - To add the task in the audit trail under **History**, retain the existing task name.
      - To add a discrete task entry in the list, type a new name.

13. To define the schedule:

    c. To indicate the date that the task will begin running:

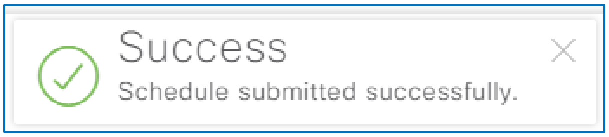
    - In the date fields, type the number of the month, day of the month, or year, as needed.
    - By using the calendar picker, select the day, the number of the month, day of the month, or year.

    d. To indicate the time that the task will begin running, type the hour or minute, and whether the time is a.m. or p.m.

    e. To indicate the time zone to which you want to apply the time that you indicated, below **Time Zone**, in the drop-down list, select the time zone.

14. To apply the schedule to the task, click **Start**.

    The panel closes, and a system message opens confirming that the system has scheduled the task.



Success

Schedule submitted successfully.

To see the schedule, return to the **Discovery Dashboard** on the **Discovery Status** dashlet, you can open a panel and review the **Scheduled Tasks** tab.

…Add Devices by Using an IP Address Range?

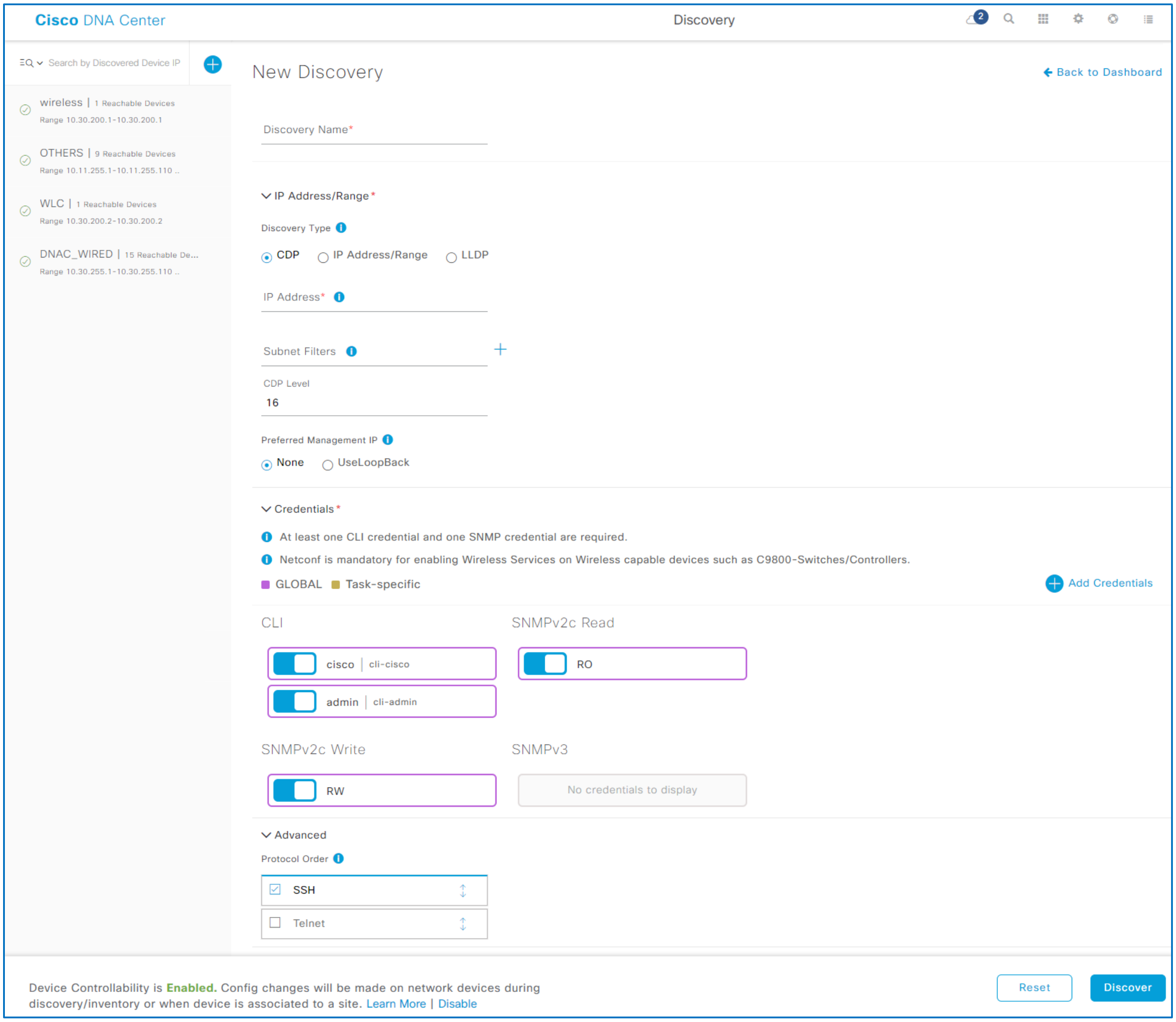
You add devices on the **New Discovery** page.

Configuration Change: Be aware that device configuration changes occur automatically in the discovery process by using the **Device Controllability** feature, including configuration that allows Cisco DNA Center to:

- Establish communication with and manage devices.
- Support ongoing device management when specific setting changes occur.

For more information, refer to the **By Recognizing the Device Configuration Changes that Can Occur in this Process** topic.

Tip: When you need to discover a group of devices that include some that share common credentials and others with discrete and varying credentials, you can run a series of discovery tasks to address the varying credential requirements.



Cisco DNA Center — Discovery

Search by Discovered Device IP

wireless | 1 Reachable Devices
Range 10.30.200.1-10.30.200.1

OTHERS | 9 Reachable Devices
Range 10.11.255.1-10.11.255.110 ..

WLC | 1 Reachable Devices
Range 10.30.200.2-10.30.200.2

DNAC_WIRED | 15 Reachable De...
Range 10.30.255.1-10.30.255.110 ..

New Discovery — Back to Dashboard

Discovery Name*

IP Address/Range*

Discovery Type: ● CDP ○ IP Address/Range ○ LLDP

IP Address*

Subnet Filters

CDP Level: 16

Preferred Management IP: ● None ○ UseLoopBack

Credentials*

At least one CLI credential and one SNMP credential are required.

Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers.

■ GLOBAL ■ Task-specific — Add Credentials

CLI: cisco | cli-cisco; admin | cli-admin

SNMPv2c Read: RO

SNMPv2c Write: RW

SNMPv3: No credentials to display

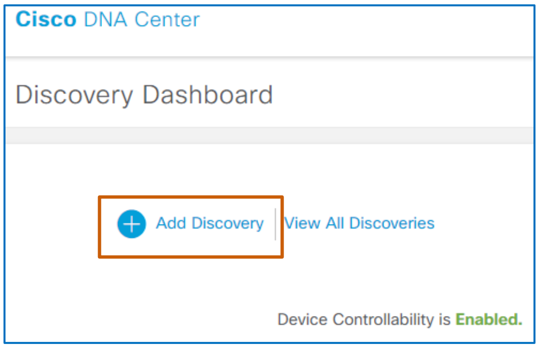
Advanced

Protocol Order: ☑ SSH; □ Telnet

Device Controllability is **Enabled**. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn More | Disable

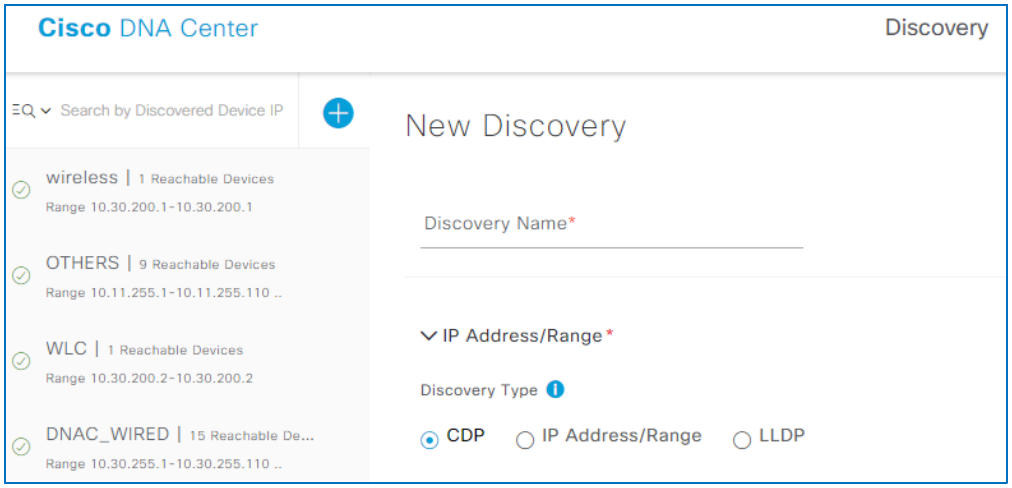
To discover devices by using an IP address range:

1. On the **Discovery Dashboard**, in the dashlet, click **Add Discovery**.



Device Controllability is Enabled.

The **Discovery | New Discovery** page opens, and the **CDP** method of discovery is selected by default.



wireless | 1 Reachable Devices
Range 10.30.200.1-10.30.200.1

OTHERS | 9 Reachable Devices
Range 10.11.255.1-10.11.255.110 ..

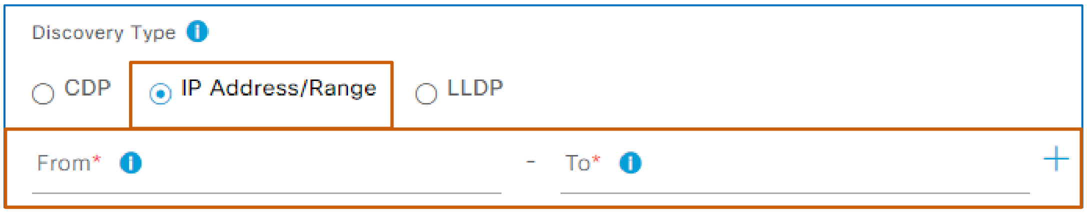
WLC | 1 Reachable Devices
Range 10.30.200.2-10.30.200.2

DNAC_WIRED | 15 Reachable De...
Range 10.30.255.1-10.30.255.110 ..

● CDP ○ IP Address/Range ○ LLDP

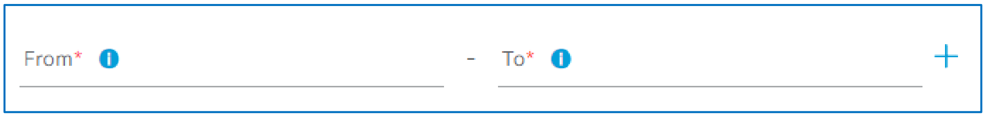
2. In the **Discovery Name** field, type a unique, meaningful name for the task.
3. Under **Discovery Type**, click **IP Address/Range**.

   The area below **Discovery Type** toggles to display the IP address range **From** and **To** fields.

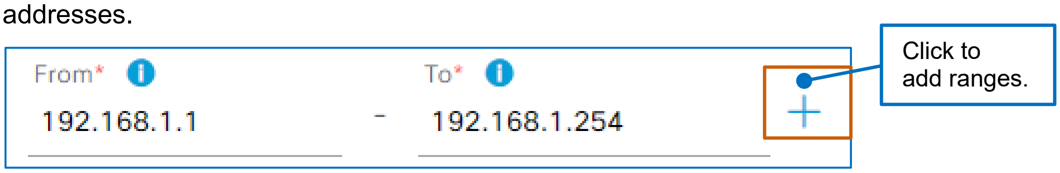


○ CDP ● IP Address/Range ○ LLDP

4. To indicate the IP address range in which the discovery process will search:
   a. To indicate the IP address at which discovery starts, in the **From** field, type the address.
   b. To indicate the IP address at which discovery ends, in the **To** field, type the address.



c. To add another range, click the **plus** icon, and then type the starting and ending IP addresses.



192.168.1.1 - 192.168.1.254

Click to add ranges.

5. To finish configuring the IP address range discovery task, follow these steps.

…Add Devices by Reusing a Previously Run Discovery Task?

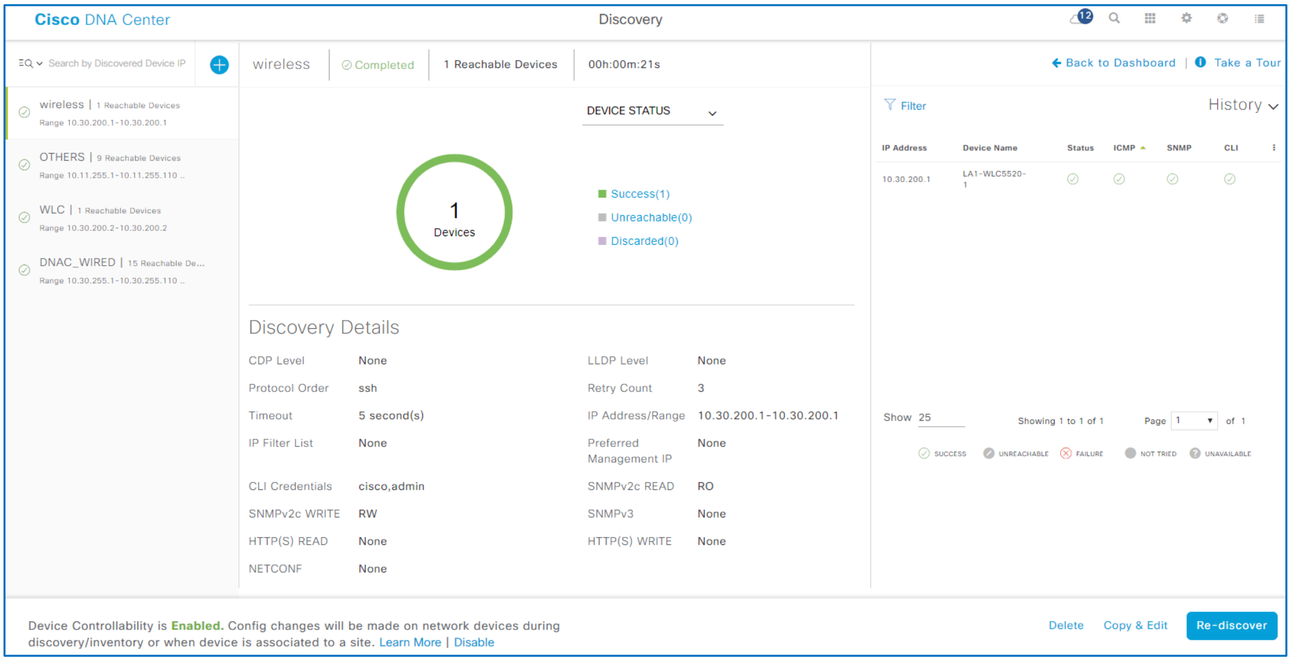
You access previously run tasks on the Discovery page that displays task results.

Configuration Change: Be aware that device configuration changes occur automatically in the discovery process by using the **Device Controllability** feature, including configuration that allows Cisco DNA Center to:

- Establish communication with and manage devices.
- Support ongoing device management when specific setting changes occur.

For more information, refer to the **By Recognizing the Device Configuration Changes that Can Occur in this Process** topic.

Tip: When you need to discover a group of devices that include some that share common credentials and others with discrete and varying credentials, you can run a series of discovery tasks to address the varying credential requirements.



wireless | 1 Reachable Devices
Range 10.30.200.1-10.30.200.1

OTHERS | 9 Reachable Devices
Range 10.11.255.1-10.11.255.110 ..

WLC | 1 Reachable Devices
Range 10.30.200.2-10.30.200.2

DNAC_WIRED | 15 Reachable De...
Range 10.30.255.1-10.30.255.110 ..

wireless | ✓ Completed | 1 Reachable Devices | 00h:00m:21s

1 Devices

🟩 Success(1)
▨ Unreachable(0)
▨ Discarded(0)

Discovery Details

CDP Level	None	LLDP Level	None
Protocol Order	ssh	Retry Count	3
Timeout	5 second(s)	IP Address/Range	10.30.200.1-10.30.200.1
IP Filter List	None	Preferred Management IP	None
CLI Credentials	cisco,admin	SNMPv2c READ	RO
SNMPv2c WRITE	RW	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None
NETCONF	None		

IP Address	Device Name	Status	ICMP	SNMP	CLI
10.30.200.1	LA1-WLC5520-1	✓	✓	✓	✓

Show 25 Showing 1 to 1 of 1 Page 1 of 1

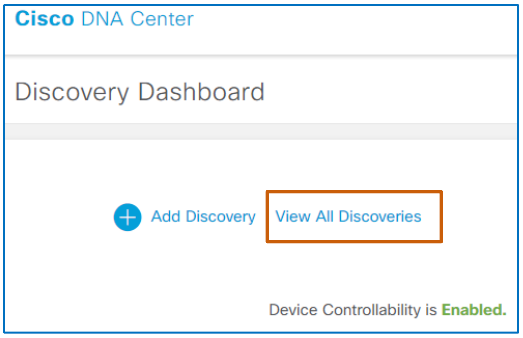
✓ SUCCESS ● UNREACHABLE ☒ FAILURE ● NOT TRIED ? UNAVAILABLE

Device Controllability is **Enabled.** Config changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn More | Disable

Delete Copy & Edit Re-discover

To discover devices by using an IP address range:

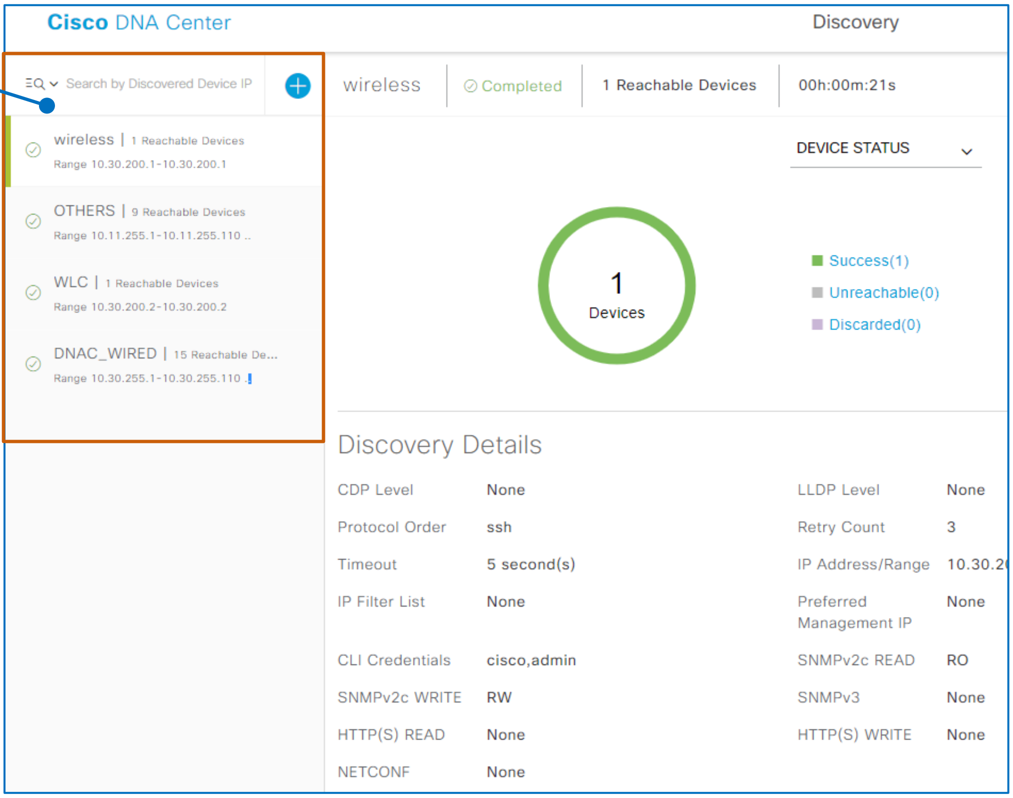
1. On the **Discovery Dashboard**, in the dashlet, click **View All Discoveries**.



Device Controllability is **Enabled.**

The **Discovery** page opens and lists the previously run tasks on the left.

Previously run discovery tasks



Cisco DNA Center — Discovery

≡Q ⌄ Search by Discovered Device IP ⊕

- wireless | 1 Reachable Devices — Range 10.30.200.1-10.30.200.1
- OTHERS | 9 Reachable Devices — Range 10.11.255.1-10.11.255.110 ..
- WLC | 1 Reachable Devices — Range 10.30.200.2-10.30.200.2
- DNAC_WIRED | 15 Reachable De... — Range 10.30.255.1-10.30.255.110 ..

wireless | ✓ Completed | 1 Reachable Devices | 00h:00m:21s

DEVICE STATUS ⌄

1 Devices

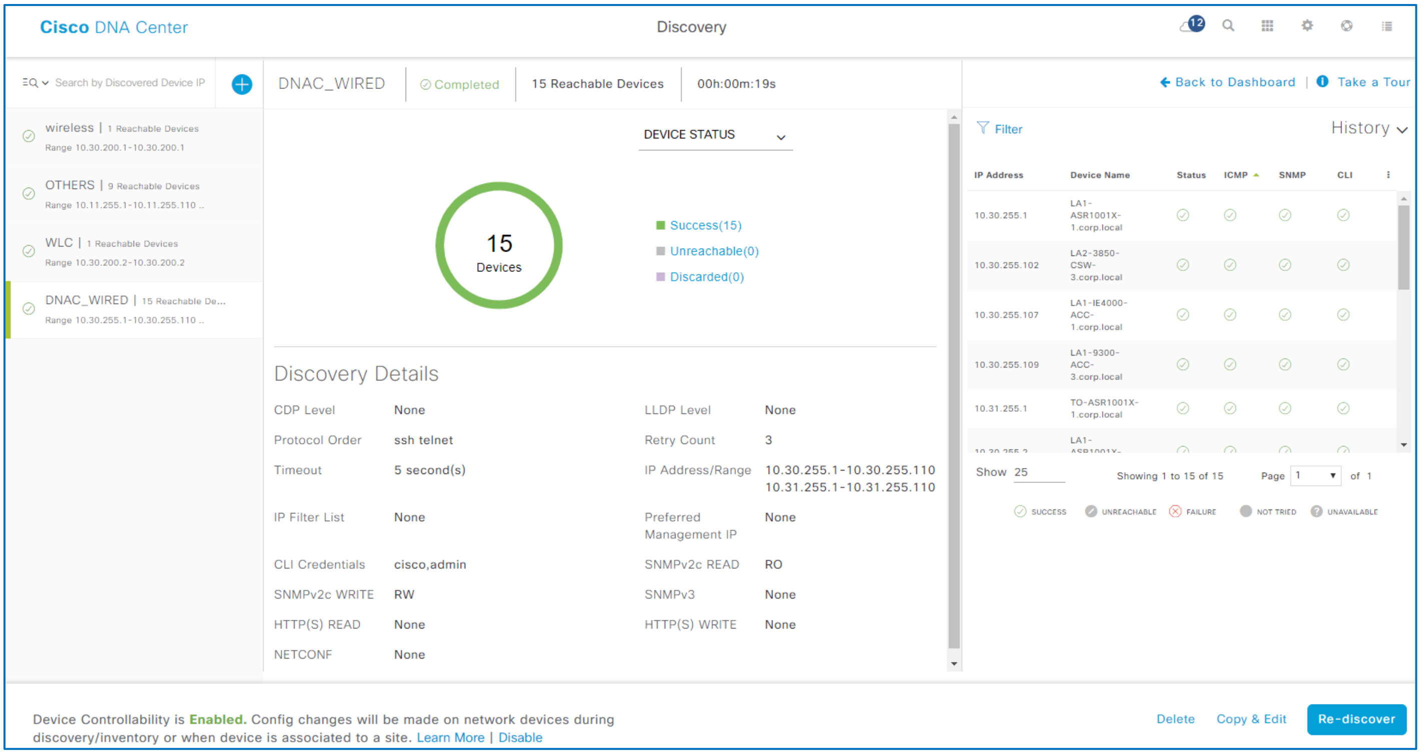
- 🟩 Success(1)
- ▨ Unreachable(0)
- ▨ Discarded(0)

Discovery Details

CDP Level	None	LLDP Level	None
Protocol Order	ssh	Retry Count	3
Timeout	5 second(s)	IP Address/Range	10.30.2
IP Filter List	None	Preferred Management IP	None
CLI Credentials	cisco,admin	SNMPv2c READ	RO
SNMPv2c WRITE	RW	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None
NETCONF	None		

2. In the list, select the task that you need to reuse.

   The page refreshes and displays the previous results of the task and its parameters.



Cisco DNA Center — Discovery

← Back to Dashboard | ⓘ Take a Tour

≡Q ⌄ Search by Discovered Device IP ⊕

- wireless | 1 Reachable Devices — Range 10.30.200.1-10.30.200.1
- OTHERS | 9 Reachable Devices — Range 10.11.255.1-10.11.255.110 ..
- WLC | 1 Reachable Devices — Range 10.30.200.2-10.30.200.2
- DNAC_WIRED | 15 Reachable De... — Range 10.30.255.1-10.30.255.110 ..

DNAC_WIRED | ✓ Completed | 15 Reachable Devices | 00h:00m:19s

DEVICE STATUS ⌄

15 Devices

- 🟩 Success(15)
- ▨ Unreachable(0)
- ▨ Discarded(0)

Discovery Details

CDP Level	None	LLDP Level	None
Protocol Order	ssh telnet	Retry Count	3
Timeout	5 second(s)	IP Address/Range	10.30.255.1-10.30.255.110 10.31.255.1-10.31.255.110
IP Filter List	None	Preferred Management IP	None
CLI Credentials	cisco,admin	SNMPv2c READ	RO
SNMPv2c WRITE	RW	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None
NETCONF	None		

Filter — History ⌄

IP Address	Device Name	Status	ICMP ▲	SNMP	CLI
10.30.255.1	LA1-ASR1001X-1.corp.local	✓	✓	✓	✓
10.30.255.102	LA2-3850-CSW-3.corp.local	✓	✓	✓	✓
10.30.255.107	LA1-IE4000-ACC-1.corp.local	✓	✓	✓	✓
10.30.255.109	LA1-9300-ACC-3.corp.local	✓	✓	✓	✓
10.31.255.1	TO-ASR1001X-1.corp.local	✓	✓	✓	✓
10.30.255.2	LA1-ASR1001X-	✓	✓	✓	✓

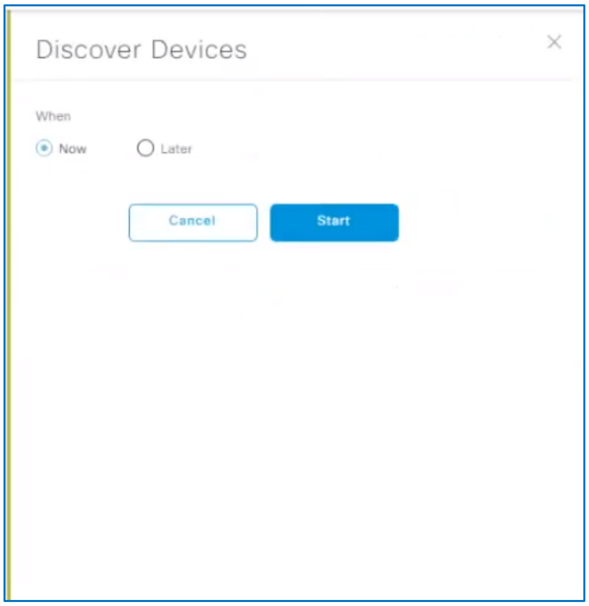
Show 25 — Showing 1 to 15 of 15 — Page 1 ▾ of 1

✓ SUCCESS · UNREACHABLE · ⊗ FAILURE · ● NOT TRIED · ? UNAVAILABLE

Device Controllability is **Enabled**. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn More | Disable

3. Under **Discovery Details**, determine whether the discovery task contains the credentials that you need.

   - If the task includes the devices and credentials that you need, click **Re-discover**, and then, in the **Discover Devices** panel, follow the steps to complete the task.

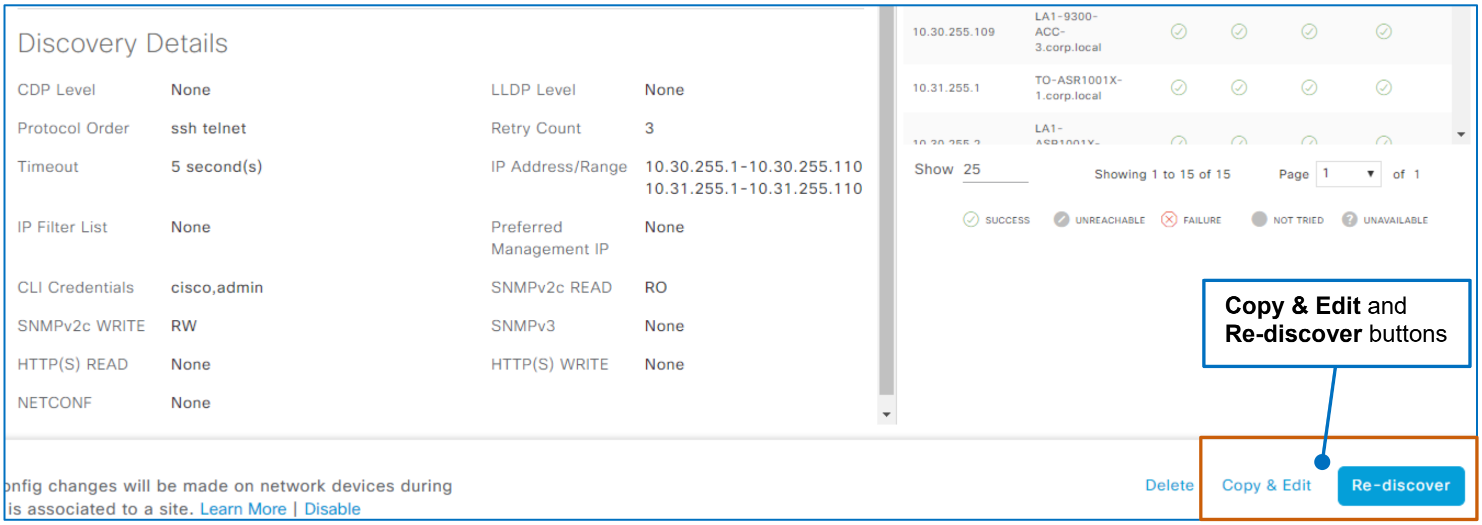


Discover Devices

When

◉ Now ○ Later

   - If the task does not include the credentials that you need, click **Copy & Edit**, and then, on the **New Discovery** page, follow the steps to change the task's current parameters and run or schedule the task, as needed, for:
     - The CDP or LLDP discovery method.
     - The IP address range discovery method.



Discovery Details

CDP Level	None	LLDP Level	None
Protocol Order	ssh telnet	Retry Count	3
Timeout	5 second(s)	IP Address/Range	10.30.255.1-10.30.255.110 10.31.255.1-10.31.255.110
IP Filter List	None	Preferred Management IP	None
CLI Credentials	cisco,admin	SNMPv2c READ	RO
SNMPv2c WRITE	RW	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None
NETCONF	None		

10.30.255.109	LA1-9300-ACC-3.corp.local	✓	✓	✓	✓
10.31.255.1	TO-ASR1001X-1.corp.local	✓	✓	✓	✓
10.30.255.2	LA1-ASR1001X-	✓	✓	✓	✓

Show 25 Showing 1 to 15 of 15 Page 1 of 1

onfig changes will be made on network devices during
is associated to a site. Learn More | Disable

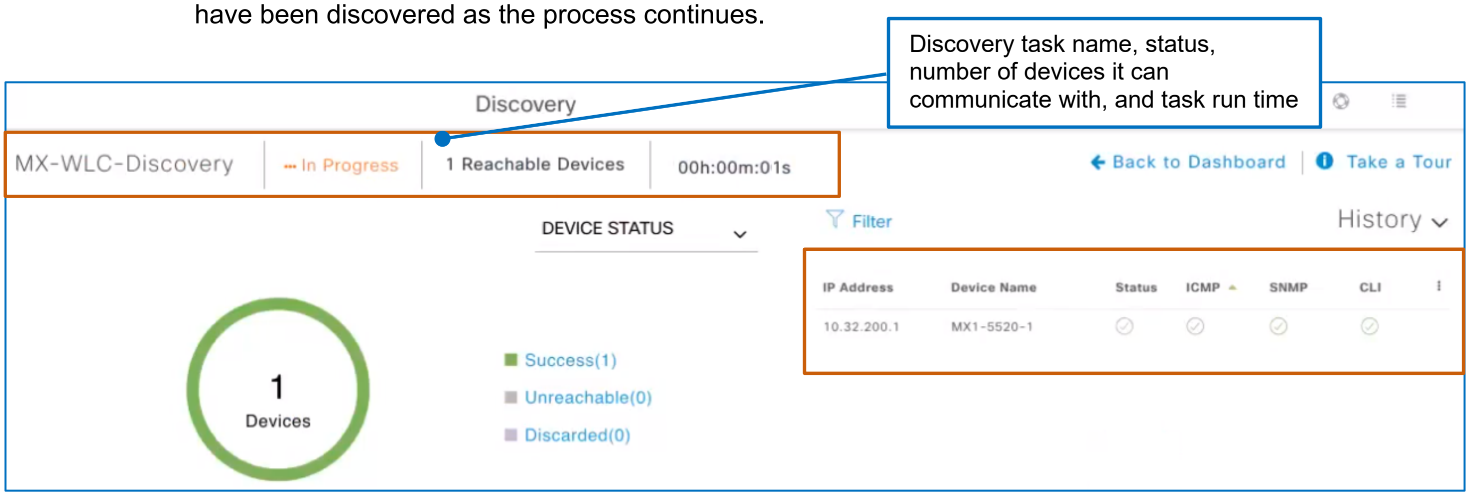
Copy & Edit and **Re-discover** buttons

…Review Task Progress or Results?

When you start a discovery task, or the system starts a discovery task by following a schedule, Cisco DNA Center:

- Queues and begins running the task.
- Lists the task below the search field on the left of the page.

The page updates automatically as the task progresses, indicating its status and the devices that have been discovered as the process continues.



Discovery task name, status, number of devices it can communicate with, and task run time

Discovery

MX-WLC-Discovery | ··· In Progress | 1 Reachable Devices | 00h:00m:01s

IP Address	Device Name	Status	ICMP	SNMP	CLI
10.32.200.1	MX1-5520-1	✓	✓	✓	✓

When the task finishes, the results include all of the devices that it identified during the process and their statuses. It also provides the configuration of the task.

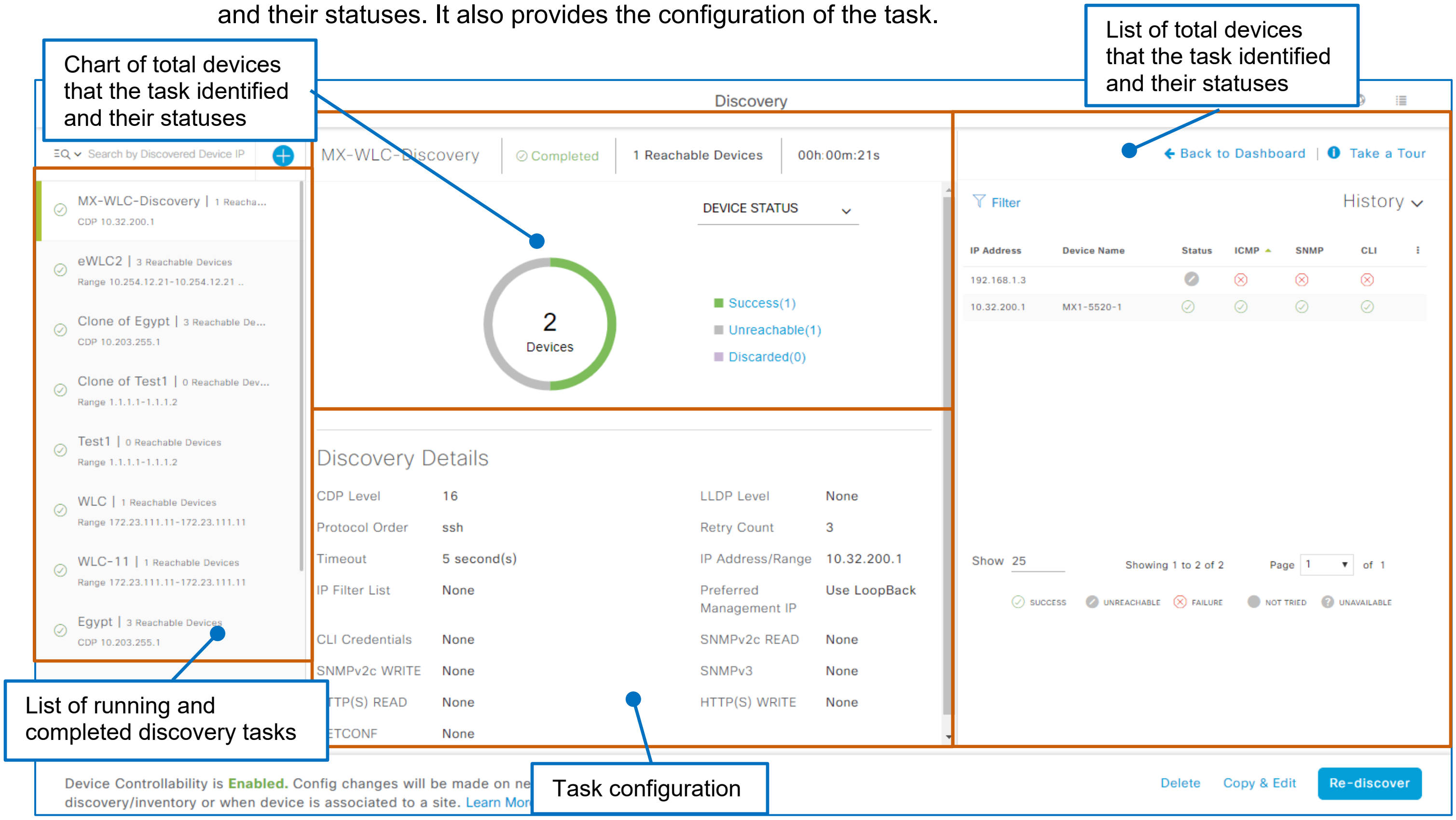


Chart of total devices that the task identified and their statuses

List of total devices that the task identified and their statuses

List of running and completed discovery tasks

Task configuration

Discovery

- MX-WLC-Discovery | 1 Reacha...
  CDP 10.32.200.1
- eWLC2 | 3 Reachable Devices
  Range 10.254.12.21-10.254.12.21 ..
- Clone of Egypt | 3 Reachable De...
  CDP 10.203.255.1
- Clone of Test1 | 0 Reachable Dev...
  Range 1.1.1.1-1.1.1.2
- Test1 | 0 Reachable Devices
  Range 1.1.1.1-1.1.1.2
- WLC | 1 Reachable Devices
  Range 172.23.111.11-172.23.111.11
- WLC-11 | 1 Reachable Devices
  Range 172.23.111.11-172.23.111.11
- Egypt | 3 Reachable Devices
  CDP 10.203.255.1

MX-WLC-Discovery | ✓ Completed | 1 Reachable Devices | 00h:00m:21s

Discovery Details

CDP Level	16	LLDP Level	None
Protocol Order	ssh	Retry Count	3
Timeout	5 second(s)	IP Address/Range	10.32.200.1
IP Filter List	None	Preferred Management IP	Use LoopBack
CLI Credentials	None	SNMPv2c READ	None
SNMPv2c WRITE	None	SNMPv3	None
TTP(S) READ	None	HTTP(S) WRITE	None
ETCONF	None		

IP Address	Device Name	Status	ICMP	SNMP	CLI
192.168.1.3		⊘	⊗	⊗	⊗
10.32.200.1	MX1-5520-1	✓	✓	✓	✓

Show 25 Showing 1 to 2 of 2 Page 1 of 1

✓ SUCCESS ⊘ UNREACHABLE ⊗ FAILURE ● NOT TRIED ? UNAVAILABLE

Device Controllability is **Enabled.** Config changes will be made on ne discovery/inventory or when device is associated to a site. Learn Mor

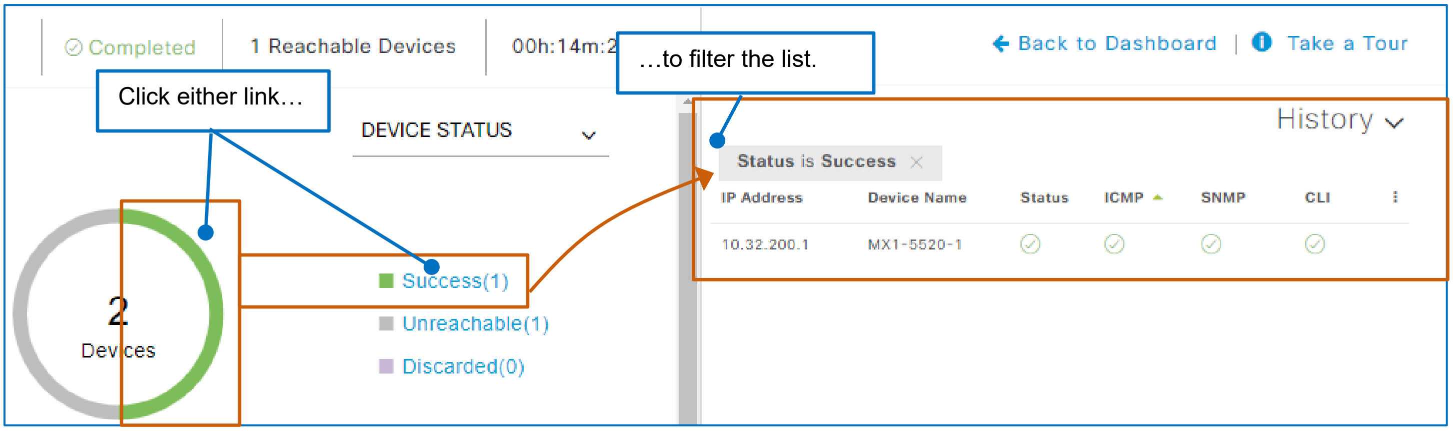
Beside the chart, the legend links indicate the numbers of devices with the following statuses:

- **Success**
  Indicates that Cisco DNA Center can communicate with and add the devices to the inventory
- **Unreachable**
  The task discovery method included these devices, but Cisco DNA Center failed to communicate with them

> **Note:** To add a device to the inventory and manage it successfully, Cisco DNA Center must be able to either:
>
> - Log in to and connect with it by using SNMP credentials
> - When SNMP login fails, and Device Controllability is enabled, the system with log in to the device by using CLI and configure the SNMP credentials.

- **Discarded**
  In CDP or LLDP discovery tasks, the system found devices on subnets that were excluded from the task by using the subnet filter

You can click a chart segment or status link to filter the device list to include only the devices with that status.

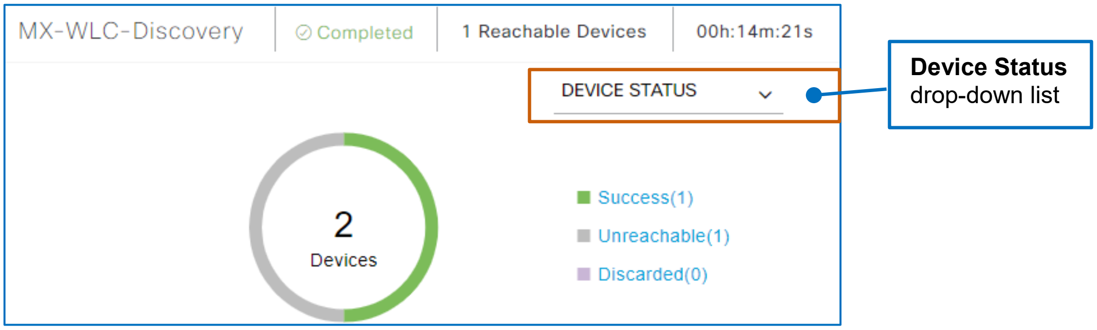


Click either link…

…to filter the list.

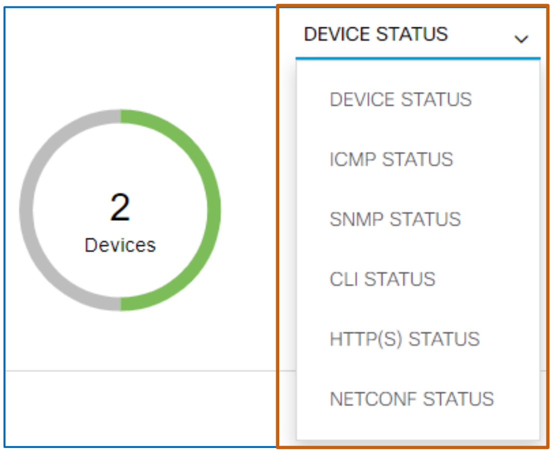
IP Address	Device Name	Status	ICMP	SNMP	CLI
10.32.200.1	MX1-5520-1	✓	✓	✓	✓

When you have a long list of devices, you also can filter the device list based on devices' statuses by protocol.

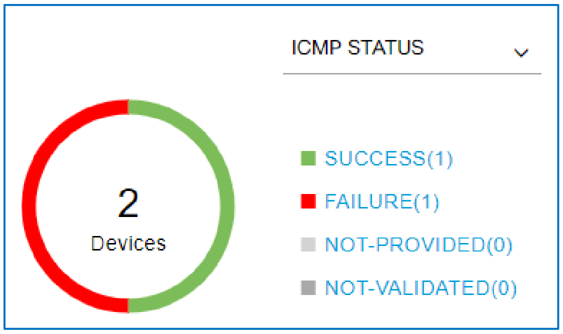


Device Status drop-down list

In the **Device Status** drop-down list, when you select a specific protocol status…



The chart updates to display color-coding and a legend opens with the numbers of devices and their statuses for the protocol.



The legend links indicate the numbers of devices with the following statuses:

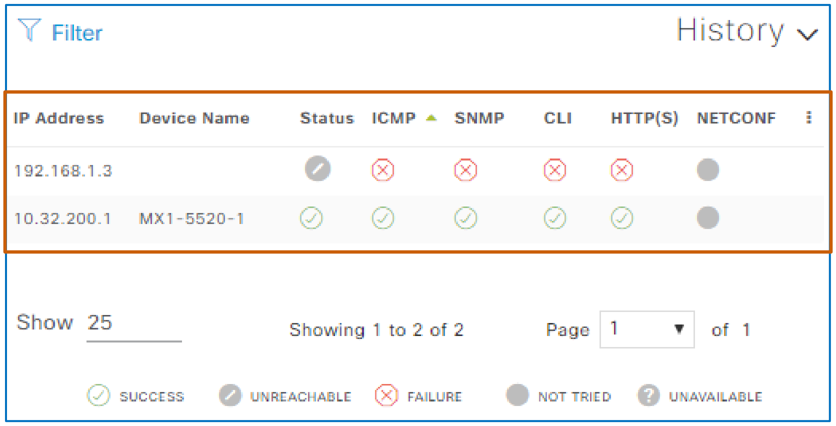
- **Success**
  Indicates that the system can communicate with the devices by using the protocol
- **Failure**
  Indicates that the system cannot communicate with the devices by using the protocol
- **Not Provided**
  Indicates that the protocol is not configured in the task
- **Not Validated**
  Indicates that the system did not attempt to communicate with the device due to a communication failure, and subsequent failure to login to the device by using CLI or SSH

  For example, when **Device Controllability** is disabled and:

  - SNMP communication fails, the system cannot attempt a CLI login, causing it not to be able to connect to device.
  - NetConf communication fails, the system cannot attempt an SSH login, causing it not to be able to connect to device.

The device list includes:

- The IP address of each device that the task included
- Its discovery status
- The status of reachability by using each protocol
- When discovery is successful, the device name.



Filter History ⌄

IP Address	Device Name	Status	ICMP ▲	SNMP	CLI	HTTP(S)	NETCONF
192.168.1.3		⊘	⊗	⊗	⊗	⊗	●
10.32.200.1	MX1-5520-1	✓	✓	✓	✓	✓	●

Show 25 Showing 1 to 2 of 2 Page 1 ▾ of 1

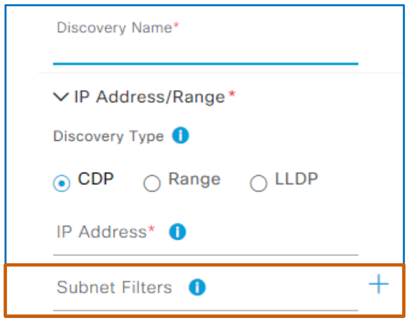
✓ SUCCESS ⊘ UNREACHABLE ⊗ FAILURE ● NOT TRIED ? UNAVAILABLE

The device status summary indicates the following:

- **Success**
  Devices are discovered, in the **Inventory**, and fully managed
- **Unreachable**
  The system cannot reach the device, which can occur when the discovery task did not have proper credentials or there are device connectivity issues.
- **Not Tried**
  SNMP validation has failed.

  In this case, the system does not attempt to log in to the device by using CLI and cannot add the device to the inventory.

  This situation can occur when the **Device Controllability** feature is disabled, for example.
- **Unavailable**
  When configuring the discovery task, the system user did not include the SNMP, CLI, or NetConf credentials that apply to the device.
- **Discarded**
  In CDP or LLDP discovery tasks, the system found devices on subnets that were excluded from the task by using the subnet filter.



Discovery Name*

⌄ IP Address/Range*

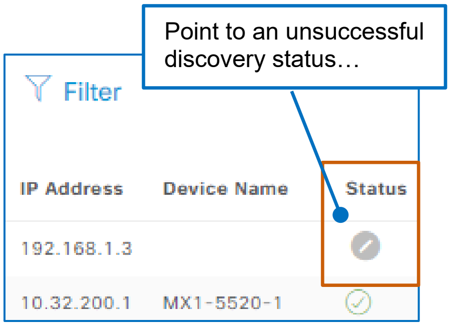
Discovery Type ℹ

● CDP ○ Range ○ LLDP

IP Address* ℹ

Subnet Filters ℹ +

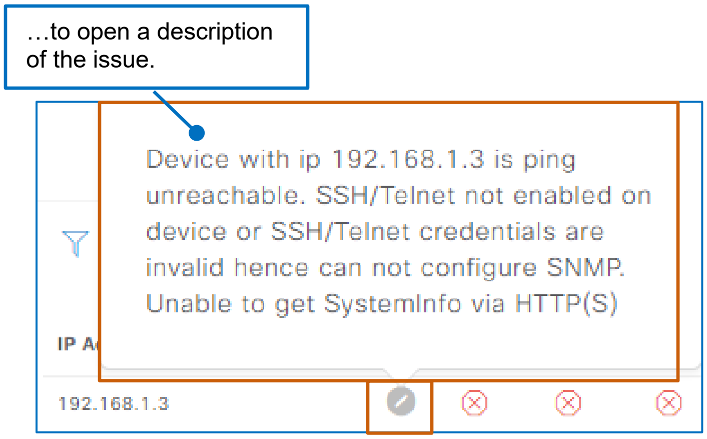
When devices' discovery statuses are not successful, you can point to the icon to open a tooltip that describes the issues.



Point to an unsuccessful discovery status…

Filter

IP Address	Device Name	Status
192.168.1.3		
10.32.200.1	MX1-5520-1	✓



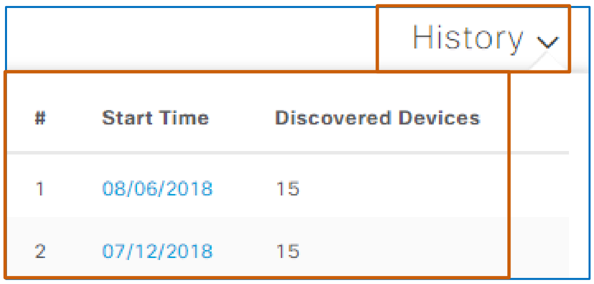
…to open a description of the issue.

Device with ip 192.168.1.3 is ping unreachable. SSH/Telnet not enabled on device or SSH/Telnet credentials are invalid hence can not configure SNMP. Unable to get SystemInfo via HTTP(S)

IP A

192.168.1.3

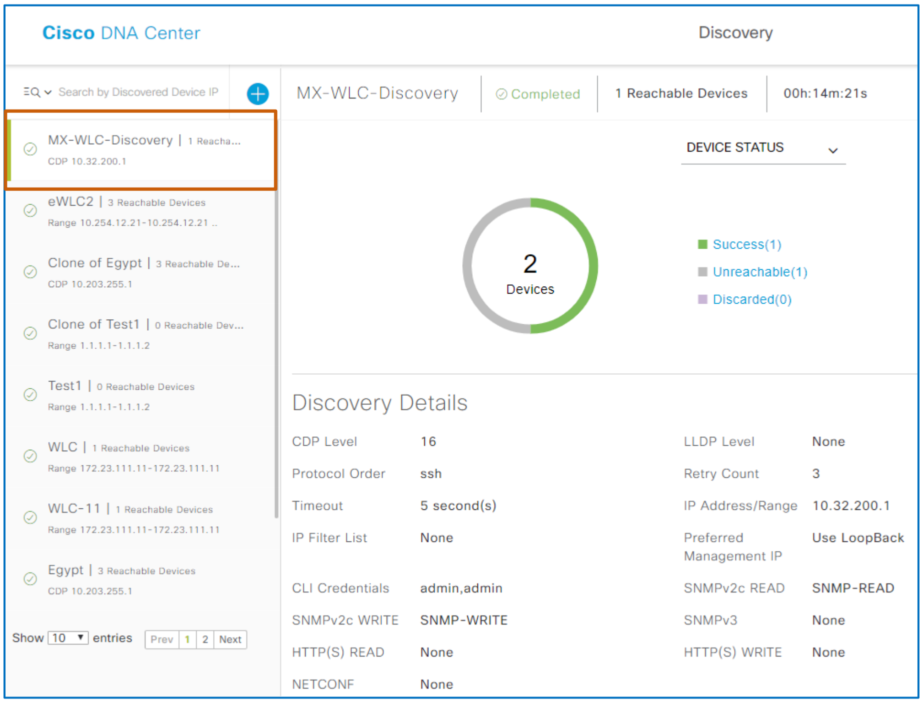
Under **History**, you can review a list of previous times that the task was run or click a time stamp link to see the list of devices that the specific task discovered.



History

#	Start Time	Discovered Devices
1	08/06/2018	15
2	07/12/2018	15

After running a discovery task, it remains available in the list so that system users can use it subsequently.



Cisco DNA Center — Discovery

Search by Discovered Device IP

- MX-WLC-Discovery | 1 Reacha… — CDP 10.32.200.1
- eWLC2 | 3 Reachable Devices — Range 10.254.12.21-10.254.12.21 ..
- Clone of Egypt | 3 Reachable De… — CDP 10.203.255.1
- Clone of Test1 | 0 Reachable Dev… — Range 1.1.1.1-1.1.1.2
- Test1 | 0 Reachable Devices — Range 1.1.1.1-1.1.1.2
- WLC | 1 Reachable Devices — Range 172.23.111.11-172.23.111.11
- WLC-11 | 1 Reachable Devices — Range 172.23.111.11-172.23.111.11
- Egypt | 3 Reachable Devices — CDP 10.203.255.1

Show 10 entries Prev 1 2 Next

MX-WLC-Discovery | Completed | 1 Reachable Devices | 00h:14m:21s

DEVICE STATUS

2 Devices

- 🟩 Success(1)
- ▨ Unreachable(1)
- ▨ Discarded(0)

Discovery Details

CDP Level	16	LLDP Level	None
Protocol Order	ssh	Retry Count	3
Timeout	5 second(s)	IP Address/Range	10.32.200.1
IP Filter List	None	Preferred Management IP	Use LoopBack
CLI Credentials	admin,admin	SNMPv2c READ	SNMP-READ
SNMPv2c WRITE	SNMP-WRITE	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None
NETCONF	None		

More To Know

Why Does An Admin Device User Name Cause an ISE Conflict?

Because ISE Sees It as a Conflict with Its Own Default Admin User

The ISE server does not distinguish between its default **admin** user name, which is used to log in to the ISE user interface administratively, and an externally-used **admin** user name.

When **admin** is applied as an external device's or system's user name, and that device or system attempts to log in to and authenticate on ISE with it, ISE rejects the attempt because of the naming conflict.

There are situations in which this conflict can occur inherently, for example, when a system or process has a standard operating procedure that requires an **admin** user name.

To resolve the conflict, you can:

- In ISE, change the user interface administrator and SSH log in user name credentials.
- After changing the credentials, restart ISE.

Then, you can provision devices in Cisco DNA Center and avoid the conflict.

What Does Disabling Device Controllability Before Discovery Affect?

Configuration Changes That Support Device Connectivity, Manageability, and Data Collection Do Not Occur

Cisco DNA Center uses valid SNMP, CLI, and in some cases, NetConf, credentials to communicate with and collect data from devices.

When **Device Controllability** is disabled and devices do not already have valid SNMP, CLI, or NetConf credentials, the system cannot apply the credentials it requires. In this case, those devices will not be discovered or added to the inventory. The discovery task results include the number of devices to which it could not apply valid credentials with a status of **Unreachable**.

When **Device Controllability** is disabled and devices have valid SNMP, CLI, or NetConf credentials that are included in the discovery task, the system can communicate with those devices and add them to the inventory. However, those devices will not receive the additional configurations, such as IP Device Tracking or Cisco TrustSec credentials.

Note: For a complete list of items that Cisco DNA Center will not configure on devices when **Device Controllability** is disabled, refer to the topic.

Discovered Devices Cannot Be Added to Fabric Topologies in Current or Future SD-A Deployments

In SD-Access deployments, **Device Controllabilit**y must be enabled during discovery to support the automated tasks that Cisco DNA Center must perform to build a fabric topology.

If **Device Controllability** is disabled during discovery, Cisco DNA Center cannot use those devices in fabric topologies later, even if **Device Controllability** is enabled later.

Return me to the caution that I was in the reading.

What Does Disabling Device Controllability After Discovery Affect?

Credential or Features Changes Cannot Be Applied to Devices

Cisco DNA Center will not apply any changes to credentials or features that occur while **Device Controllability** is disabled.

If changes occur while the feature is disabled, and then it is enabled at a later time, the system does not apply any configuration changes that occurred during the time that the feature was disabled.

Cisco DNA Center does apply all of the applicable device configuration changes that occur after enabling **Device Controllability**.

Devices Cannot Be Added to Fabric Topologies

In SD-Access deployments, **Device Controllability** must be enabled to support the automated tasks that Cisco DNA Center must perform to build fabric topologies.

Have Another Question?

For more information, visit the Cisco Web site to review or download technical documentation.

Want Even More?

Find Product Information

Visit the Cisco Web site to learn more about Cisco DNA Center.

Visit the Cisco Web site to review or download technical documentation.

Find Training

Visit the Cisco Web site to access other Cisco DNA Center learning opportunities.

Visit the Cisco Web site to access learning opportunities for other Cisco products.

Contact Us About This Training

Send us a message with questions or comments about this training.

Note: Please send messages that address training content only.

Follow your regular business process to request technical support or address technical or application-related questions.