Cisco Catalyst Center SD-Access LAN Automation Deployment Guide

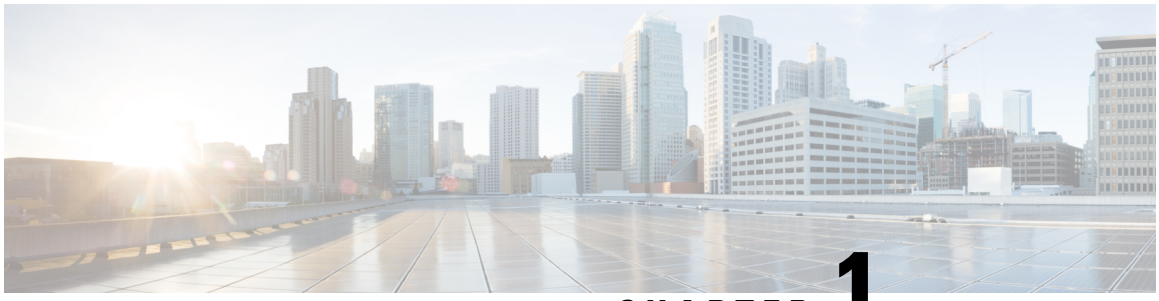
First Published: 2018-12-19

Last Modified: 2026-05-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

?



CHAPTER 1

LAN automation

LAN automation is a network management process that

- simplifies network operations,
- eliminates manual, repetitive network configuration tasks, and
- establishes a standard, error-free underlay network.

LAN automation accelerates the creation of the underlay network without the traditional network planning and implementation process.

This guide is based on Catalyst Center Release 2.3.3; however, an additional topic in the guide provides some information on the LAN automation process based on Catalyst Center Release 2.3.5 and later.

Note Cisco DNA Center has been rebranded as Catalyst Center. During the rebranding process, you will see both names used in different collaterals, but both names refer to the same product.

The steps and examples may vary based on your Catalyst Center version. For more information on configuring LAN automation and related features, see *Cisco Catalyst Center User Guide*.

• LAN automation workflow, on page 1

LAN automation workflow

Cisco LAN automation provides these key benefits:

- Zero-touch provisioning: Network devices are dynamically discovered, onboarded, and automated from their factory default state to fully integrated state in the network.
- End-to-end topology: You can model and program dynamic discovery of new network systems and their physical connectivity. These new systems can be automated with Layer 3 IP addressing and routing protocols to dynamically build end-to-end routing topologies.
- Resilience: Cisco LAN automation integrates system and network configuration parameters that optimize forwarding topologies and redundancy. Cisco LAN automation enables system-level redundancy and automates best practices to ensure resiliency during planned or unplanned network outages.

- Security: The network access and infrastructure protection parameters recommended by Cisco are automated, providing security from the initial deployment.
- Compliance: LAN automation helps eliminate errors, misconfigurations, and inconsistent rules and settings that drain IT resources. LAN automation provides compliance across the network infrastructure during new system onboarding by automating globally managed parameters from Catalyst Center.

The Cisco LAN automation workflow helps enterprise IT administrators prepare, plan, and automate greenfield networks in four main steps:

Procedure

Step 1 **Plan**:

- Understand the different roles in the LAN automation domain.
- Plan the site and IP pool requirements.
- Understand the prerequisites for seed devices.

Step 2 **Design**:

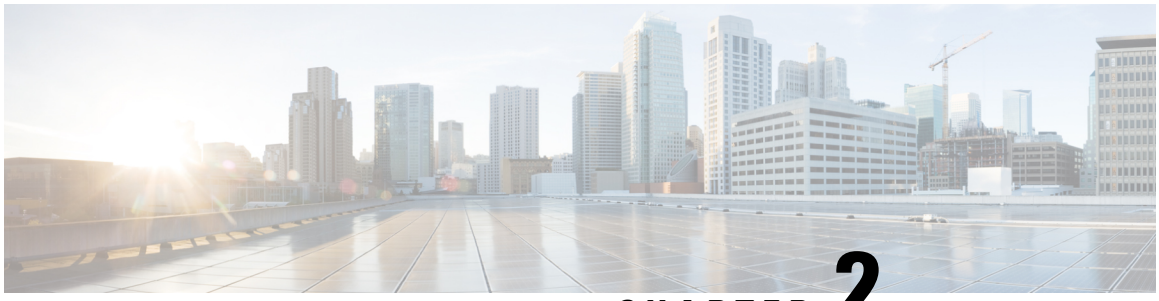
- Design and build global sites.
- Configure global network services and site-level network services.
- Configure global device credentials.
- Design the global IP address pool and assign the LAN automation pool.

Step 3 **Discover**:

- Discover the seed devices.
- Assign the discovered devices to sites.

Step 4 **Provision**:

- Start LAN automation: Push the temporary configuration to seed devices, discover devices, upgrade the image, and push the initial configuration to discovered devices.
- Stop LAN automation: Convert all point-to-point links to Layer 3.



CHAPTER 2

Planning LAN Automation

System roles and network topologies

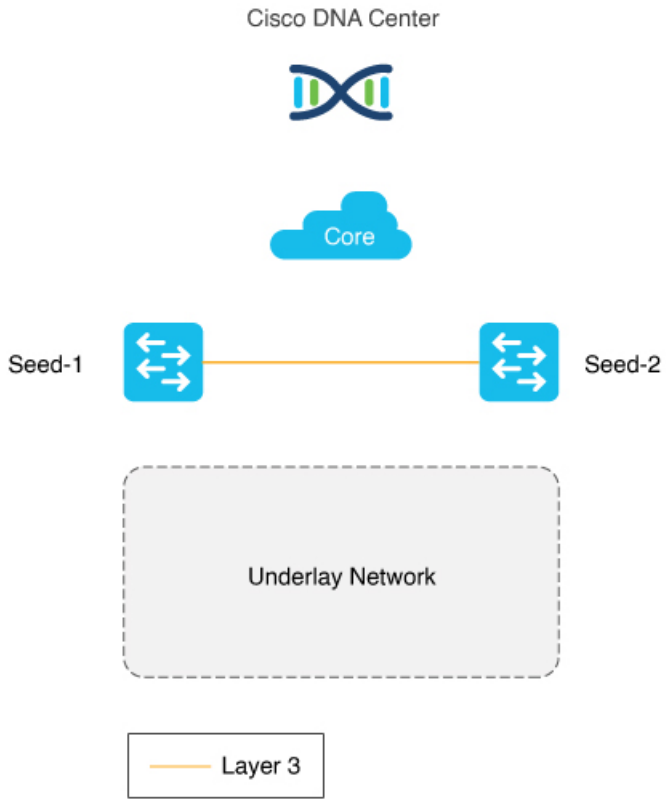
This section describes the device roles and the supported network topologies for LAN automation.

Seed device

The seed device is a predeployed system in the network and is the initial point through which LAN automation discovers and onboards new switches downstream. The seed device can be automated through technologies such as Plug and Play (PnP) and zero-touch provisioning or configured manually. Device discovery happens only on the primary seed device interfaces.

The figure illustrates the network boundaries of the seed device from the Catalyst Center connection in the IP core to the underlay network that LAN automation will discover. The peer seed (*Seed-2*) can also be automated through LAN automation. However, only one seed device is required.

Figure 1: Seed devices in a LAN automated network

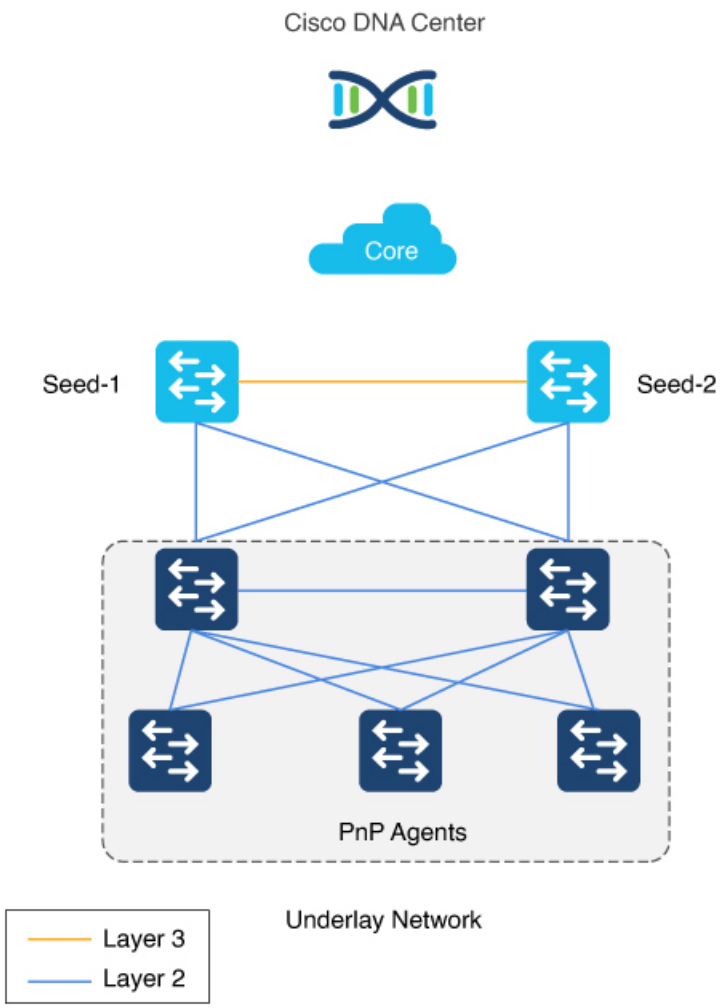


PnP agent

The PnP agent is a Cisco Catalyst switch with factory default settings. The switch uses the built-in day-0 mechanism to communicate with Catalyst Center and support the integrated PnP server function. Catalyst Center dynamically builds the PnP profile and configuration sets that enable complete day-0 automation.

The figure shows the PnP agent physical connection to the seed device.

Figure 2: PnP agents in a LAN automated network



Automation boundary

In general, we recommend building structured and hierarchical network designs in enterprise networks to provide scalability and redundancy at every network tier. While the three-tier architecture is proven in large-scale enterprise campus networks, the network design varies based on the overall network size and physical connections. As part of the initial planning, the network admin must determine the physical topology to automate with Cisco LAN automation.

LAN automation in Catalyst Center supports a maximum of two hops from the initial automation boundary point device. To build the underlay network up to the access layer, the network admin must start the automation boundary from the core or distribution layer. Any additional network devices beyond two hops might be discovered but cannot be automated.

LAN automation initiates only on directly connected neighbors.

These two scenarios illustrate the LAN automation process in a three-tier network:

- Scenario 1: You have a three-tier network and you want to LAN automate distribution- and access-layer switches. Because distribution-layer switches (which are directly connected to the seed) participate in LAN automation, both distribution- and access-layer switches will be discovered and LAN automated.
- Scenario 2: You have a three-tier network and you want to LAN automate distribution- and access-layer switches. You already LAN automated the distribution layer. Later, you add access-layer switches to your network and you want to LAN automate these switches. Because the distribution switches are already LAN automated and links converted to Layer 3, Tier 1 switches cannot be used as the seed. You must choose distribution as the seed in this scenario.

Figure 3: Automation boundary for LAN automation

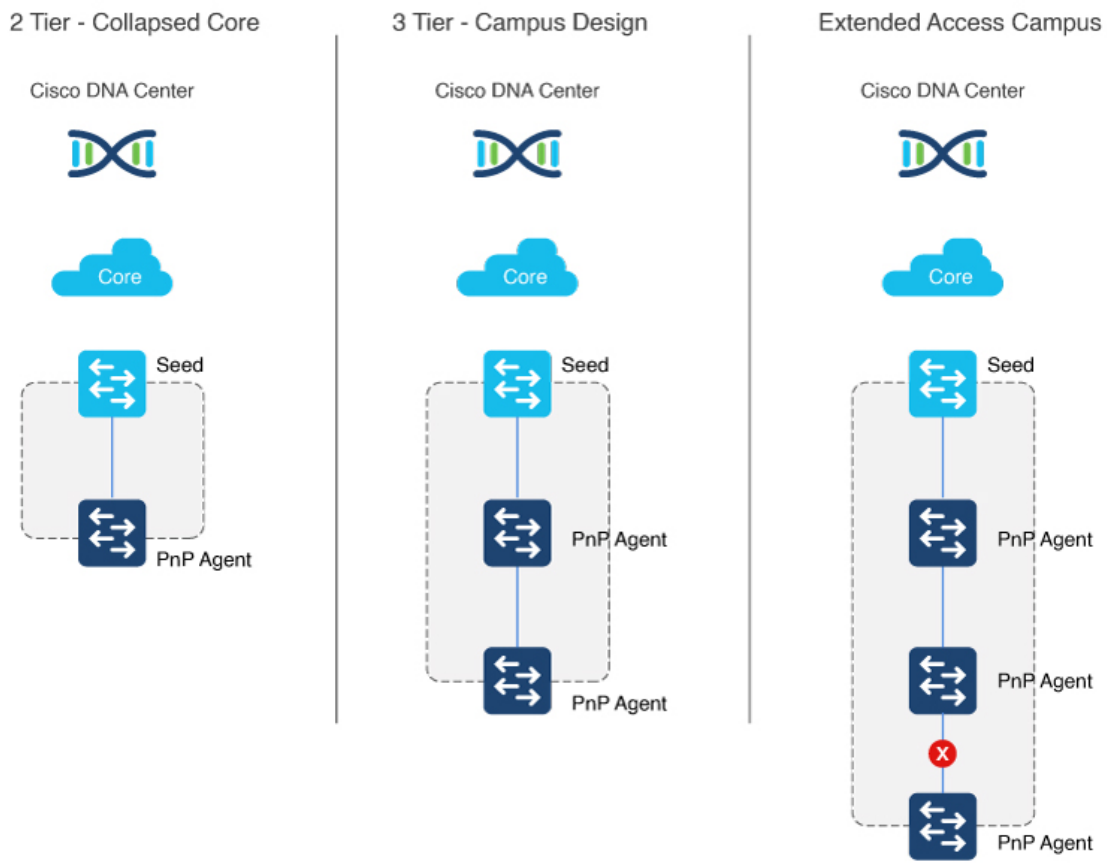
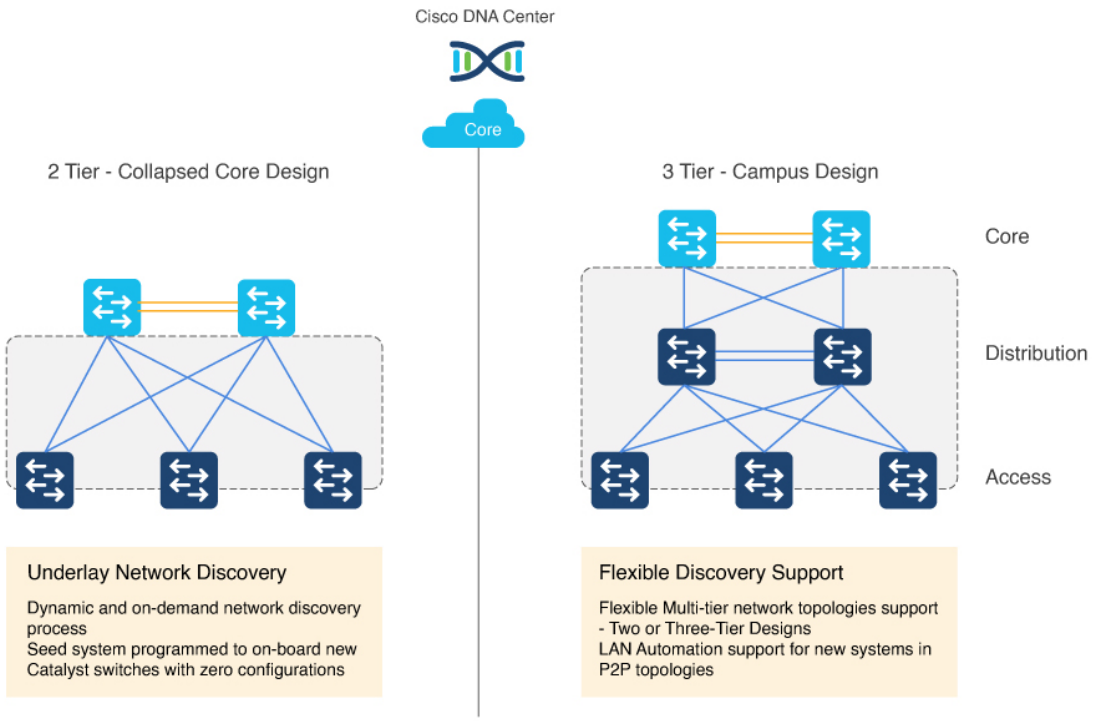


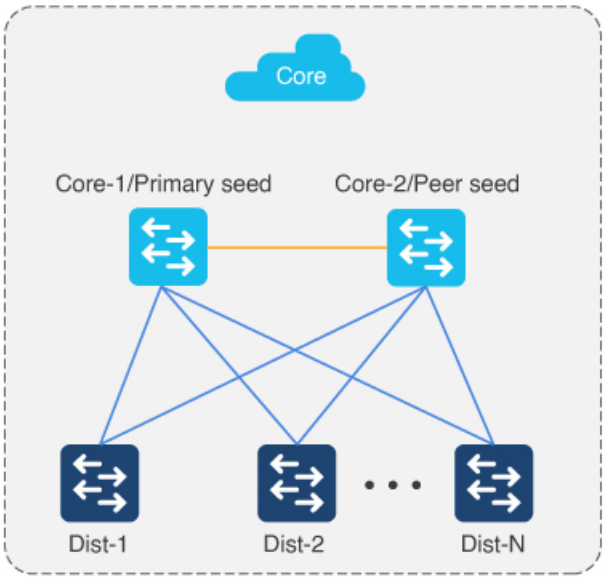
Figure 4: Two-tier and three-tier network design



Multistep LAN automation for large topologies: First pass

Large topologies are brought up by performing LAN automation multiple times. During the first pass, core devices are chosen as seed devices to bring up the distribution switches as new devices.

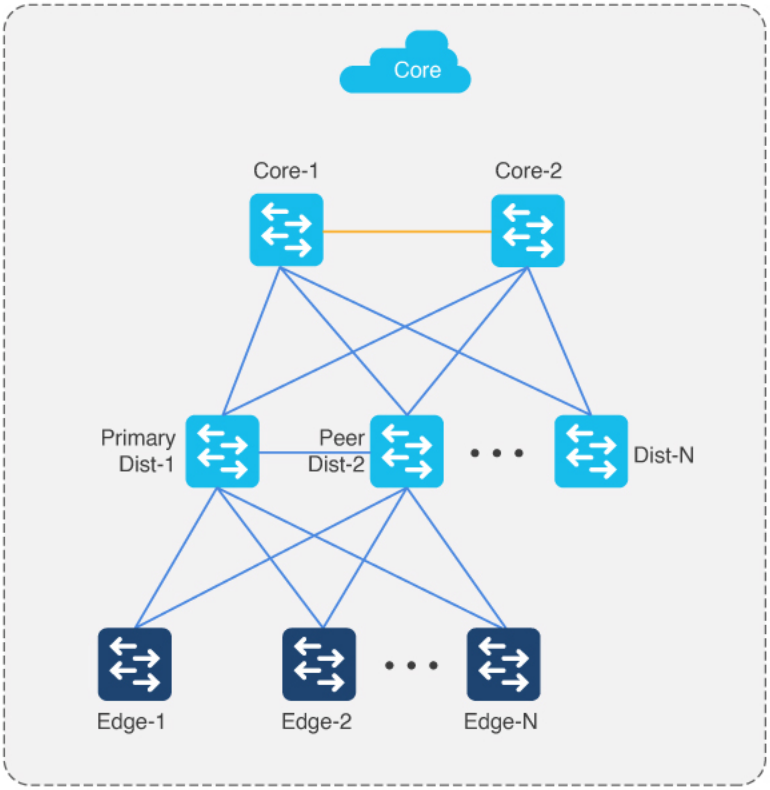
Note *N* is 50 devices or fewer at a time. All switches in the group can be booted in parallel or in a staggered fashion.



Multistep LAN automation for large topologies: Second pass with first group

During the second pass, two of the distribution switches act as seed devices to bring up the edge devices as new devices. All new devices in this session must connect directly to the two distribution switches that act as seed devices. Repeat this process for the remaining set of distribution switches, two at a time.

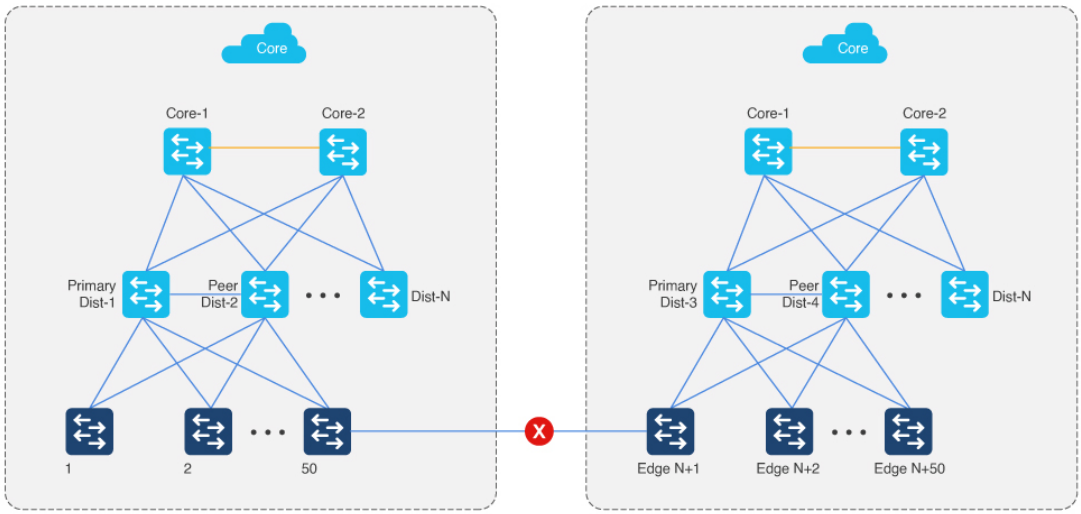
1. Repeat the second pass for each set of distribution to bring up the access/edge switches (where *N* is 50 devices or fewer at a time).
2. Connect uplinks from edges to the primary and peer distribution switches only.
3. Power down IOT/extended devices during the LAN automation session.
4. Distribution switches can be connected to other distribution switches.
5. There can be two tiers of devices below the seeds.
6. Always connect new devices to the primary seed device. Connection to the peer seed device is optional.



Multistep LAN Automation for large topologies: Second pass with second group

Edge devices in one group cannot be connected to edge devices in another group. Newly discovered PnP devices in the LAN automation session cannot be connected to existing nonseed inventory devices.

Note In Catalyst Center 2.3.5 and later, you can establish links between the devices after LAN automation stops using the **Add Link** feature. For more information, see Create a link between interfaces, on page 71.



Constraints

- LAN automation does not automate the onboarding of a StackWise Virtual (SVL) switch through PnP. SVL switch can only be used as a seed device.
- LAN automation does not support stack renumbering.
- For platform support, see Supported switches for each role at different layers, on page 11.

Layer 3 link configuration

After all devices are added to the Catalyst Center inventory, you can stop the LAN automation session on the GUI to begin the Layer 3 link configuration process.

If you accidentally stop the LAN automation process before all PnP devices are added to the Catalyst Center inventory, links are not configured on in-progress devices. You must delete the in-progress devices from the inventory, begin a new LAN automation session, bring the in-progress devices to the factory-default state, and reload the devices to rediscover them and get their links configured.

Catalyst Center Release 2.3.5 and later provide the support for day-*n* link configurations (add and delete link). For more information, see Create a link between interfaces, on page 71.

Layer 3 link configuration process

The Layer 3 link configuration process starts by converting Layer 2 links to Layer 3 links, which is done by traversing the network graph built during new device onboarding. First, the lower device link is converted to a Layer 3 IP address. Next, the upper device link is converted to a Layer 3 IP address. Router IS-IS configuration is also performed during this step in the connecting links. During this phase, there might be a temporary loss of connectivity to the lower-tier device until the upper-tier link is configured. This phase can also result in an STP topology change when the Layer 2 links are converted to Layer 3.

The process follows an algorithm that begins with the tier-three devices, followed by the tier-two devices, and completes with the tier-one devices.

It is important to note that only the links between devices that participate in the current LAN automation session are converted to Layer 3 links. Links between the newly discovered PnP device and the existing nonseed inventory device are not converted to Layer 3.

Link configuration use cases

Link configuration process when a LAN-automated device is deleted from the inventory:

- Use case 1: The edge device is single-homed—connected to only one intermediate node and the intermediate node is deleted from the inventory.

  In this case, the /31 point-to-point link IP address is deleted from Catalyst Center (IPAM) but may not be unconfigured from the edge device, which is still in the inventory. This is because the edge device can become unreachable from Catalyst Center due to the point-to-point interface between the intermediate node and the fabric border being unconfigured before the one on the edge device. In this case, log in to the edge device CLI and set the interface connected to the deleted device to default configuration. This avoids duplicate IP address assignment during LAN automation workflows later due to the released IP addresses still being present on the device. Use the LAN automation workflow to add the intermediate nodes or edge devices again instead of manual point-to-point link configurations. Ensure to delete the edge device from the inventory before adding again using LAN automation.

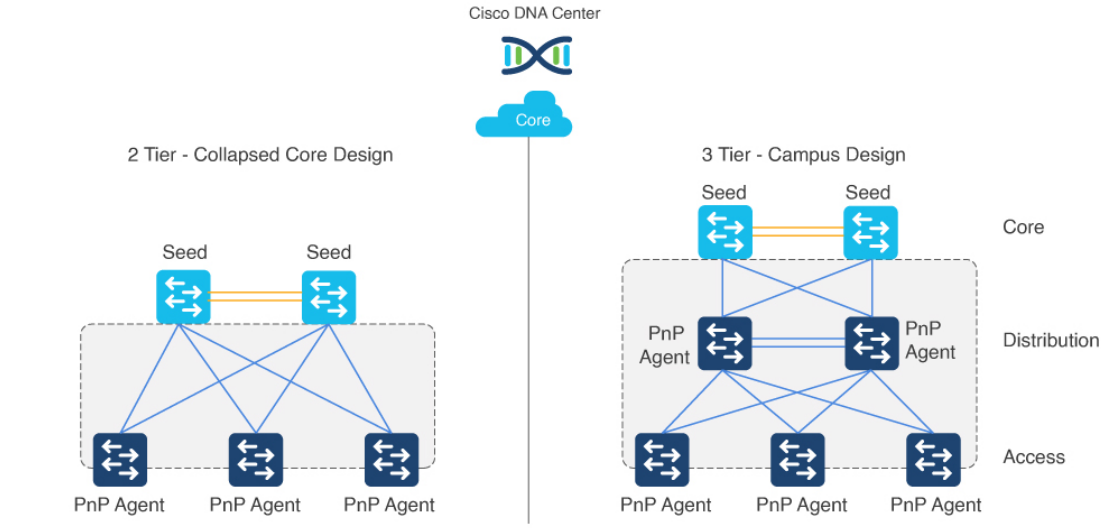
- Use case 2: The edge device is dual-homed—connected to two intermediate nodes and one of the intermediate nodes is deleted from the inventory.

  In this case, the /31 point-to-point link IP address is deleted from Catalyst Center (IPAM) and is unconfigured from the edge device as well. There is no manual configuration required on the edge devices.

Supported switches for each role at different layers

The figure shows supported device families for the seed and PnP agent at different layers.

Supported switches for each role at different layers



Layer	Role	Supported Switch Series
Distribution	Seed	Catalyst 3850, 9200, 9400, 9500, 9600
Access	PnP Agent	Catalyst 3850, 9200, 9300, 9400, 9500, 9600

Layer	Role	Supported Switch Series
Core	Seed	Catalyst 3850, 9200, 9300, 9400, 9500, 9600
Distribution	Pnp Agent	Catalyst 3850, 9200, 9300, 9500, 9600
Access	PnP Agent	Catalyst 3850, 9200, 9300, 9400, 9500, 9600

LAN automation product support matrix

Role[1]	Product model[2]	Network module[3][4]
Seed or PnP agent	C9606R C9600-SUP-1 C9600-SUP-1/2 C9600X-SUP-2	Seed: Any uplinks and module ports are supported. PnP agent: 100G interfaces are not supported.
Seed or PnP agent	C9500-32C C9500-32QC C9500-24Y4C C9500-48Y4C C9500X-28C8D C9500X-60L4D	—
Seed or PnP agent	C9500-12Q C9500-24Q C9500-40X C9500-16X	Any front-panel ports[5]

Role[1]	Product model[2]	Network module[3][4]
Seed or PnP agent	C9404R C9407R C9410R	Sup-1[6] Sup-1XL[3] Sup-1XL-Y[3] Any line card
Seed or PnP agent	C9400-SUP-1 C9400-SUP-1XL C9400-SUP-1XL-Y C9400X-SUP-2XL C9400X-SUP-2	—

Role[1]	Product model[2]	Network module[3][4]
Seed or PnP agent	C9300-24S C9300-24T C9300-24P C9300-24U C9300-24H C9300-48S C9300-48T C9300-48P C9300-48U C9300-48H C9300-24UX C9300-24UXB C9300-24UB C9300-48UXM C9300-48UN C9300-48UB C9300L-48UXG C9300L-24UXG C9300L-24P C9300L-48P C9300L-48T C9300L-24T C9300LM-48UX-4Y C9300LM-48U-4Y C9300LM-24U-4Y C9300LM-48T-4Y C9300X-12Y C9300X-24Y C9300X-24HX C9300X-48HXN C9300X-48HX C9300X-48TX	Any uplinks and module ports

Role[1]	Product model[2]	Network module[3][4]
Seed or PnP agent	C9200-24T C9200-24P C9200-24PB C9200-48T C9200-48P C9200-48PB C9200-48PL C9200-24PXG C9200-48PXG C9200L-24T C9200L-24P C9200L-48T C9200L-48P C9200L-48PL C9200L-24PXG C9200L-48PXG C9200CX-12T-2X2G C9200CX-12P-2X2G C9200CX-8P-2X2G	Any uplinks and module ports
Seed or PnP agent	WS-C3850-24T WS-C3850-48T WS-C3850-24P WS-C3850-48P WS-C3850-48F WS-C3850-24U WS-C3850-48U WS-C3850-24XU WS-C3850-12X48U WS-C3850-12S WS-C3850-24S WS-C3850-12XS WS-C3850-24XS WS-C3850-48XS	Any uplinks and module ports

Role[1]	Product model[2]	Network module[3][4]
Seed or PnP agent	IE-9310-26S2C IE-9320-26S2C	Any uplinks and module ports

1 Catalyst Center 2.1.2 and later supports configuring C9400, C9500, or C9600 StackWise Virtual (SVL) switches as a seed for LAN automation. LAN automation does not automate the onboarding of StackWise Virtual switches through PnP. StackWise Virtual switches can only be used as seed devices.

2 LAN automation is supported only on the products or platforms listed here. For the supported Cisco IOS XE and Catalyst Center versions, see *Cisco Catalyst Center Compatibility Matrix*.

3 LAN automation does not support a dedicated management port. For C9500H and C9600 switches, the convertible ports can only be used in seed device. The convertible ports do not come up when the switches are used as PnP device.

4 Line cards and SPF ports, which do not support autonegotiation rely on speed or enable CLI commands to enable the ports. Such Line cards and SPFs are not supported as part of the day-zero LAN automation workflow. You can use the day-*n* LAN automation workflow to enable the ports and then use the **Add Link** workflow to configure the point-to-point IP addresses.

5 Breakout cable support is available only on the seed devices. For discovered devices, LAN automation does not support a breakout cable, because it requires some extra configurations that will stop the PnP agent on the factory-default devices.

6 The 40-G uplink is supported on Cisco IOS XE 16.11.1 and later.

Site planning

Use the Catalyst Center Design feature to create the required sites, buildings, and floors. Consider how the primary seed and peer seed will be connected to the new devices—for example, will they all belong to the same site or follow a hierarchy? Also consider how to share IP pools across different sites, buildings, and floors. One option is to have a pool specific to a site. Another option is to share a common LAN pool for all sites in the hierarchy. If the devices are onboarded across multiple LAN automation sessions, ensure that the required IP pools are available across the sites within the hierarchy.

Note You cannot change the site after provisioning the devices. For this reason, we recommend that you complete LAN automation before you provision devices.

IP pool planning

To create IP pools for LAN automation, begin with creating a global pool in Catalyst Center, followed by a site-specific LAN IP pool, which LAN automation allocates internally.

LAN IP pool allocation

1. One part of the IP pool is reserved for a temporary DHCP server. The size of this pool depends on the size of the parent LAN pool. For example, if the parent pool is 192.168.10.0/24, a /26 subpool is allocated for the DHCP server. If the pool size is larger than /24, the DHCP pool size is increased up to a maximum of /23 subpool (512 IP addresses). Therefore, a /24 pool reserves 64, a /23 pool reserves 128, a /22 pool reserves 256, and larger pools reserve 512 IP addresses for the DHCP server. To start LAN automation, the pool size must be atleast /25, which reserves a /27 pool or 32 IP addresses for the DHCP pool. This

IP pool is reserved temporarily for the duration of the LAN automation discovery session. After the LAN automation discovery session completes, the DHCP pool is released, and the IPs are returned to the LAN pool. Because the DHCP pool is usually the largest contiguous segment of IPs required, the pool should have at least one such segment available. If the pool is too fragmented, it cannot allocate the DHCP pool and the LAN automation session ends with an IP pool allocation error.

2. Another part of the IP pool is reserved internally with a subpool size of /27. This subpool is for allocating single IPs for Loopback0 and Loopback60000 always. Also, two consecutive IPs for point-to-point L3 links are allocated from this subpool if no separate overlapping IP pool is provided. This internally reserved subpool is used throughout the LAN automation sessions for providing IPs as long as it has IPs available. If exhausted, a new /27 subpool is created for allocating IPs. These subpools are released only when all the allocated IPs are released as part of the devices being deleted from Catalyst Center. Otherwise, the subpools remain throughout the process and are not allowed to be removed. Due to this internal subpool allocation logic, the IP pool usage in IPAM counts the subpools instead of the actual IPs allocated to the devices.
3. If a shared or link overlapping IP pool is provided for the point-to-point Layer 3 links, then the subpool of size /27 is reserved internally from the shared pool instead of the main IP pool. The subpools are automatically deleted when all the allocated IPs from the pool are released.

Single and shared IP pool

When a dedicated (single) IP pool is used to build the underlay networks, each of the devices discovered via LAN automation gets a unique /31 per interface for point-to-point connection, and a unique /32 for Loopback0 and the underlay multicast.

A link overlapping IP pool or shared IP pool is used to optimize the IPv4 addressing in the underlay network by allowing overlapping /31 IP addresses for a multisite deployment. Hosts in different sites can get duplicate IP addresses on the /31 links. The /31s in the underlay are not advertised outside of the fabric site and hence there is no need for them to be unique. However, the /32 loopback needs to be unique to every device, and should be advertised to the global routing table to identify the device in the entire network.

IP pool roles

The LAN IP pool can have these two valid roles:

- **Link Overlapping IP Pool**: This pool role is optional for a LAN automation session. If provided, the allocation of IP addresses is only on the point-to-point Layer 3 links.

Note In Catalyst Center Release 3.2.2 and later, for an IPv6 address pool, the **Link Overlapping IP Pool** field is not displayed. Select the **Point-to-point IPv6 Link-Local addressing** check box to enable link-local addressing for point-to-point links in the underlay.

- **Main IP Pool** (**Principal IP Address Pool** in Catalyst Center Release 2.3.5 and later): This pool role is mandatory for every LAN automation session. This is the pool that is used for all management-related IP addressing such as loopbacks, multicast, and DHCP. If the **Link Overlapping IP Pool** is not provided, then the **Main IP Pool** is the default fallback pool for the Layer 3 links IP addressing.

IP address allocation in Catalyst Center Release 2.3.7.x and later

In Catalyst Center Release 2.3.7.x and later, IP address allocation from LAN pool is based on IP address range instead of subnet allocation. This approach helps in minimizing the issue of IP address loss during subnet creation and in effective management of the IP addresses. Instead of creating a subnet, IP address range is blocked for both DHCP pool allocation and IP address assignment for point-to-point links, loopback, and multicast. The LAN automation workflow supports assignment of IP address pools with /27, /28, and /29 subnet masks.

IP pool usage example

Imagine you want to LAN automate 10 devices using the same pool, where each device has one link to the primary seed and another link to the secondary.

Consider a 192.168.199.0/24 pool. When LAN automation starts, a /26 pool is reserved for the DHCP addresses. In this example, 192.168.199.1 to 192.168.199.63 are reserved and assigned to VLAN 1 for the 10 devices.

Next, a /27 pool is reserved for loopback addresses. If there is no shared IP pool, then this pool is used for point-to-point links as well. Because there are 10 devices with two links each, a total of 2*10*2 = 40 IP addresses are reserved for point-to-point links, and 10 loopback addresses are reserved.

In total, 60 IP addresses are reserved for the 10 devices: 10 for each VLAN 1, 10 for each loopback, and 40 for the point-to-point links between devices and seeds.

After LAN automation stops, the VLAN 1 IP addresses are released back to the pool, and 90 addresses are allocated for the LAN automation session.

Guidelines for IP pool allocation

- The same IP pool can be used for multiple discovery sessions. For example, you can run one discovery session and discover the first set of devices. After discovery completes, you can provide the same IP pool for a subsequent LAN automation session. Similarly, you can choose one LAN pool for one discovery session and another LAN pool for a second discovery session.

Note When the seed device for LAN automation session is in a different site than the discovered device site, then the same shared IP pool cannot be used with the same seed and different discovered device site. This is to avoid the allocation of duplicate IP to the same seed device.

- Every time you start LAN automation, it checks for 64 available IP addresses in the IP pool. If you decide to run LAN automation multiple times with the same pool, use at least a /24 pool. If you plan to LAN automate only once for the IP pool, a /25 pool suffices.
- Avoid using an address pool that is already utilized elsewhere in the network, such as an address pool that belongs to the loopback or to other addresses configured on the device.

Site-specific CLI and SNMP configuration

To start LAN automation, a site-specific CLI and SNMPv2 read or SNMPv3 configuration is required. Use the Catalyst Center Design feature to configure the site-specific CLI and SNMP configurations. Save the site configuration used for LAN automation. When you configure credentials globally, they become visible at the

site level. You must click the radio button for the specific site and then save the configuration to make it available for LAN automation.

Note SNMPv2 write credentials are not required. If they are configured, they will not be pushed to the device during LAN automation.

Configuration on seed devices

Follow these guidelines when configuring the seed devices:

- Ensure that the system MTU (maximum transmission unit) value is at least 9100. Use the **show system mtu** command to check the configured value.
- Turn on IP routing on the seed devices. Use the **sh run | i routing** command to check the IP routing configurations.
- Set up routing between the seed service and Catalyst Center so that Catalyst Center has IP reachability to the LAN IP pool subnet.
- We recommend that you use the default interfaces connected to PnP agents. If the peer seed device has IP interfaces configured on the interfaces connected to PnP agents, those links are not configured. If you want to configure the peer device interfaces connected to PnP agents, use the default interfaces and perform an inventory synchronization on the peer seed device. LAN automation works only when the ports are Layer 2. The ports on the Cisco Catalyst 6000 Series Switches are Layer 3 by default. Convert the ports to Layer 2 before starting LAN automation.
- Configure device credentials and SNMP credentials on the seed devices. You can verify the configurations using the **sh run | i snmp-server community** command.
- If the seed devices have Layer 3 interfaces configured, ensure that there are no conflicts with any of the IP pools provided in Catalyst Center. Check the IP addresses which are configured manually.
- Ensure that the seed devices don't have any other interfaces connected to another DHCP server running in VLAN 1.
- LAN automation configures loopback on the seed devices if they are not configured.
- If you change configuration on the seed devices before running LAN automation, synchronize the seed devices with the Catalyst Center inventory (Select the device in the inventory and from the Actions drop-down list, choose **Resync**)
- Assign the seed devices to a site (Select the device in the inventory and from the Actions drop-down list, choose **Assign Device to Site**). It is not necessary to provision the seed devices for LAN automation.
- Ensure that **shell processing full** command is not enabled on the seed devices because this can lead to LAN automation failure.

Additional recommended configurations on seed devices

Multiple discovery sessions

If you plan to run multiple discovery sessions to onboard devices across different buildings and floors connected to the same seed devices, we recommend that you block the ports for PnP agents that do not participate in the upcoming discovery session.

For example, imagine seed devices in Building-23 connected to PnP agents on Floor-1 and Floor-2. Floor-1 devices are connected on interfaces Gig 1/0/10 through Gig 1/0/15. Floor-2 devices are connected on interfaces Gig 1/0/16 through Gig 1/0/20. For the discovery session on Floor-1, we recommend that you shut down ports connected to Gig 1/0/16 through Gig 1/0/20. Otherwise, the PnP agents connected to Floor-2 might also get DHCP IPs from the server running on the primary seed device. Because these interfaces aren't selected for the discovery session, they remain as stale entries in the PnP database. When you run the discovery session for Floor-2, the discovery doesn't function correctly until these devices are deleted from the PnP application and write erase/reloaded. Therefore, we recommend that you shut down other discovery interfaces.

Endpoint/client integration

For Catalyst Center Release 1.2.8 and earlier, if clients are connected to a switch being discovered, they may contend for DHCP IP and exhaust the pool, causing LAN automation to fail. Therefore, we recommend that you connect the client after LAN automation is complete.

This endpoint/client integration restriction does not apply to Catalyst Center Release 1.2.10 and later. Clients can remain connected while the switch is undergoing LAN automation.

PnP agent initial state

Ensure that the device that you want to LAN automate is running the Advantage license level. Otherwise, you cannot execute certain commands.

Note Catalyst Center 2.3.5 and later support automatic license upgrade for C9000 and C3850 series switches.

New PnP agents have factory defaults and are ready to start LAN automation.

If you are reusing existing network devices, follow these steps:

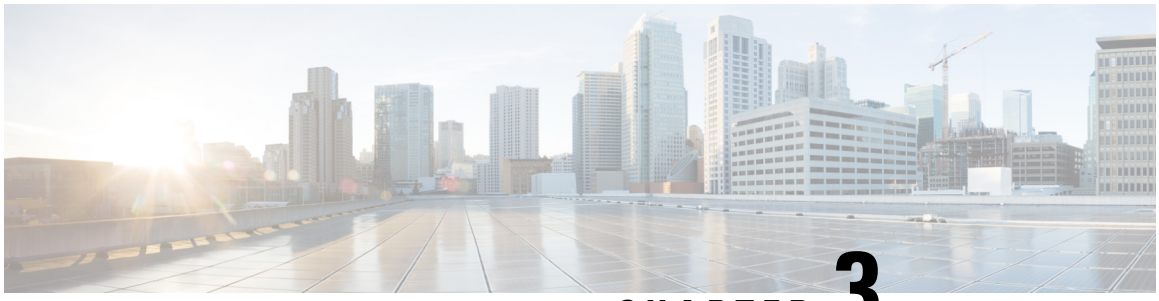
1. Ensure that PnP agents have the required license to execute LISP, IS-IS routing, and CTS-related CLI commands. Use the **show license summary** or **sh ver | i License** command to view the current license level. If required, upgrade the license.
2. Ensure that PnP agents do not have stale certificates or keys from the previous runs. Use the **show pnp status** and **show crypto pki trustpoints** to view the PnP status and certificates.
3. Use these commands to restore the switch configurations to factory default:
   - For Cisco IOS XE 16.11 and earlier, use:

```
[CLI config mode]

    no pnp profile pnp-zero-touch
    no crypto pki certificate pool
    Also remove any other crypto certs shown by "show run | inc crypto"
    crypto key zeroize
    config-register 0x2102 or 0x0102 (if not already)
    do write
    end
```

```
[CLI exec mode]

    delete /force nvram:*.cer
    delete /force stby-nvram:*.cer (if a stack)
    delete /force flash:pnp-reset-config.cfg
    write erase
    reload (enter no if asked to save)
```

- For Cisco IOS XE 16.12.x or later, use:

```
[CLI exec mode]

pnpa service reset no-prompt
```



CHAPTER 3

Network Design and Device Discovery

The design phase is the second step in the LAN automation process. It involves these steps:

1. Design and build global sites.
2. Configure the global and local network services.
3. Configure global device credentials.
4. Design the global IP address pool, and assign the LAN automation pool for the required site from the global pool.

Device discovery is the third step in building the underlay network. It scans the devices within a network and sends the list of discovered devices to the inventory.

Review the underlay configuration of the seed device before creating and running a discovery profile.

- Design your network, on page 23
- Create discovery profile, on page 26

Design your network

Use this procedure to create your network, configure device credentials, and add IP address pools for LAN automation.

Procedure

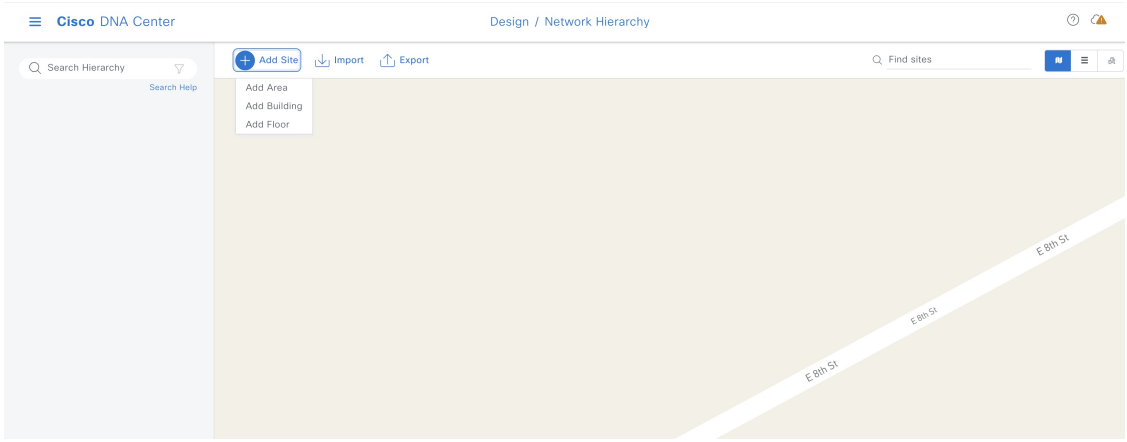
Step 1 Set up a network hierarchy.

a) From the Catalyst Center home page, click the menu icon and choose **Design** > **Network Hierarchy**.

b) Follow these steps to add sites, buildings, and floors.

To...	Do this...
Create a site (area)	Select **+ Add Site** > **Add Area** or hover your cursor over the ellipsis ••• next to the parent site in the left pane, and select **Add Area**.

To...	Do this...
Add a building	Select + **Add Site** > **Add Building** or hover your cursor over the ellipsis ••• next to the parent site in the left pane, and select **Add Building**.
Add a floor	Hover your cursor over the ellipsis ••• next to the desired building and select **Add Floor**.



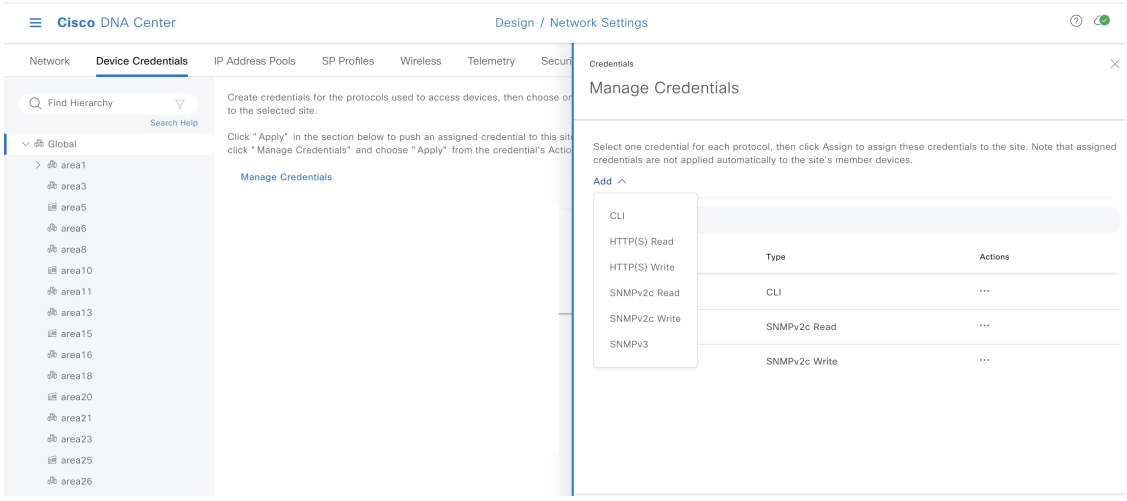
Step 2 Configure the device credentials.

a) From the main menu, choose **Design** > **Network Settings** > **Device Credentials**.

b) From the left hierarchy tree, choose a site.

c) Click **Manage Credentials** and add these credentials:

- **CLI**
- **SNMPV2C Read**



d) Check the **Assign credential to site** check box to assign the CLI credential to the selected site.

Note

If you want to apply the same device credentials to all sites, click **Global** in the left navigation tree and set the credentials.

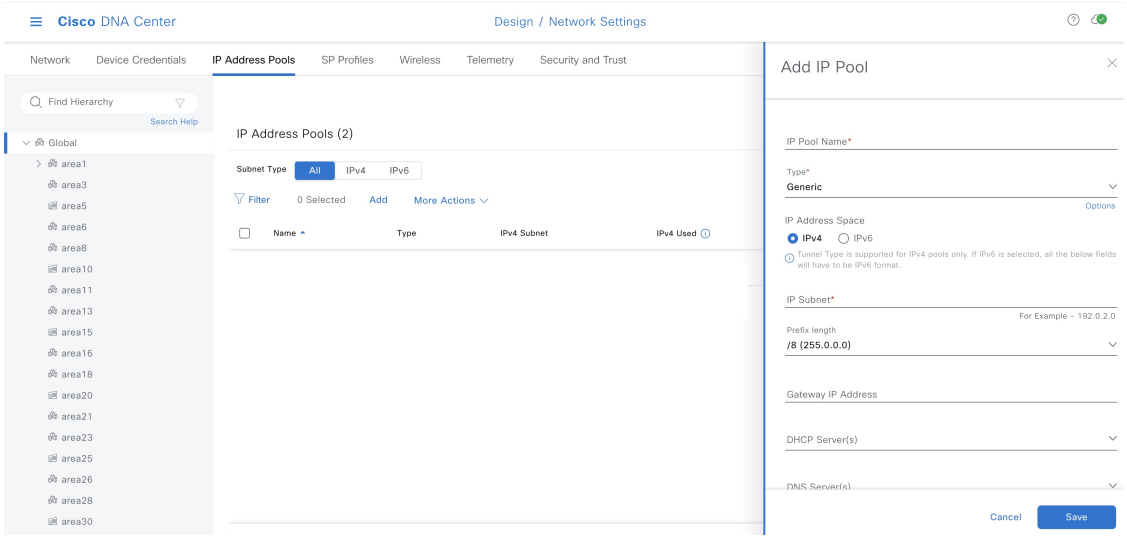
Avoid using `cisco` as the username.

Step 3 Configure IP address pools.

a) From the main menu, choose **Design** > **Network Settings** > **IP Address Pools**.

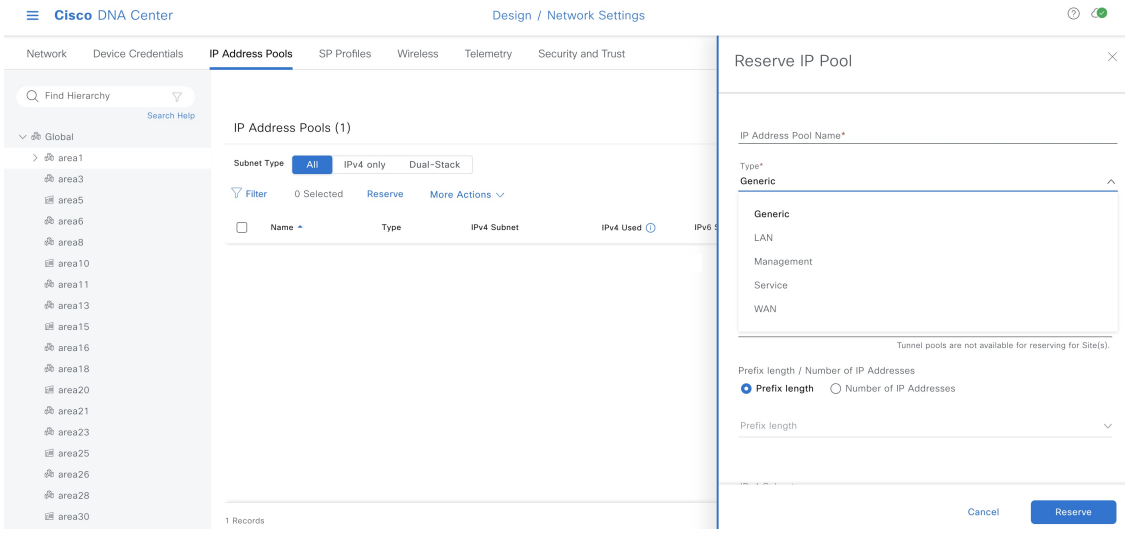
b) From the left hierarchy tree, choose **Global** and click **Add**.

Create a dedicated IP address pool for the underlay infrastructure. Ensure this pool is not already used in the network. For example, do not use an address pool that belongs to a loopback or other addresses configured on the device.



c) From the left hierarchy tree, choose a site and click **Reserve**.

d) In the **Reserve IP Pool** window, choose **Type** > **LAN**.



Create discovery profile

This section explains how to create a discovery profile.

Procedure

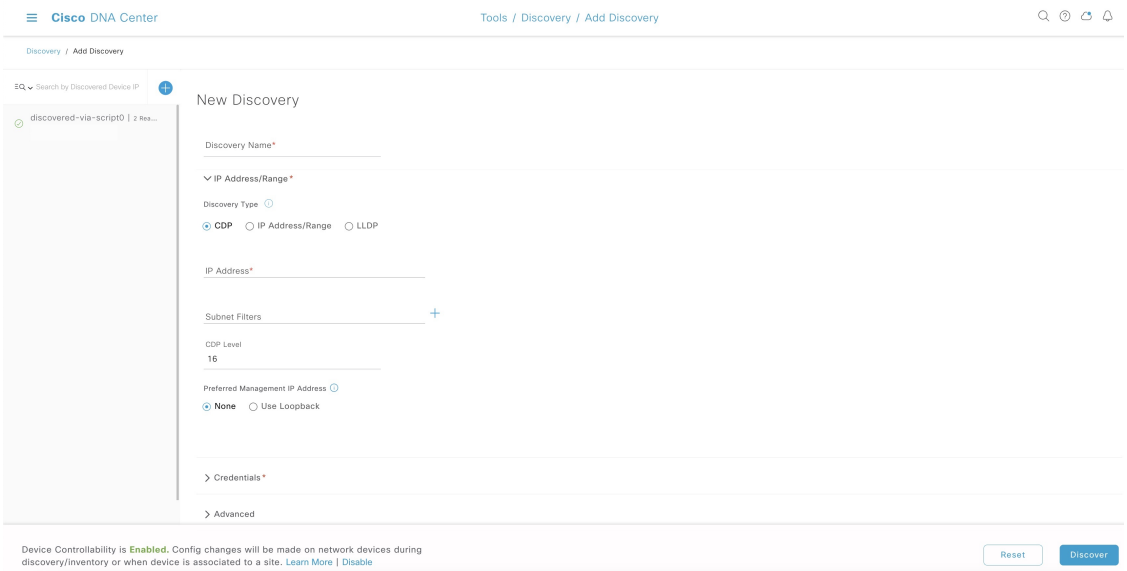
Step 1 From the Catalyst Center home page, click the menu icon and choose **Tools** > **Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.

Step 3 Configure the required details in the workflow:

- **Discovery Name**: Enter a name for the discovery profile.
- **IP Address/Range**: Enter the beginning and ending IP addresses. To discover a single device, you can enter the same address in the **From** and **To** field. The IP address can be any Layer 3 interface or loopback on any switch that Catalyst Center can access. If you are discovering the primary and peer seeds together, enter an IP range. Click the appropriate radio button and enter the details accordingly.
- **Credentials**: Enable at least one CLI and one SNMP credential. Click **Add Credentials** to add the credentials.
- **Advanced**: Specify one or more protocols for the discovery scan to use. Choose **SSH** or **Telnet** or both.

  Note
  If you choose SSH, ensure that the seed is configured for SSH.

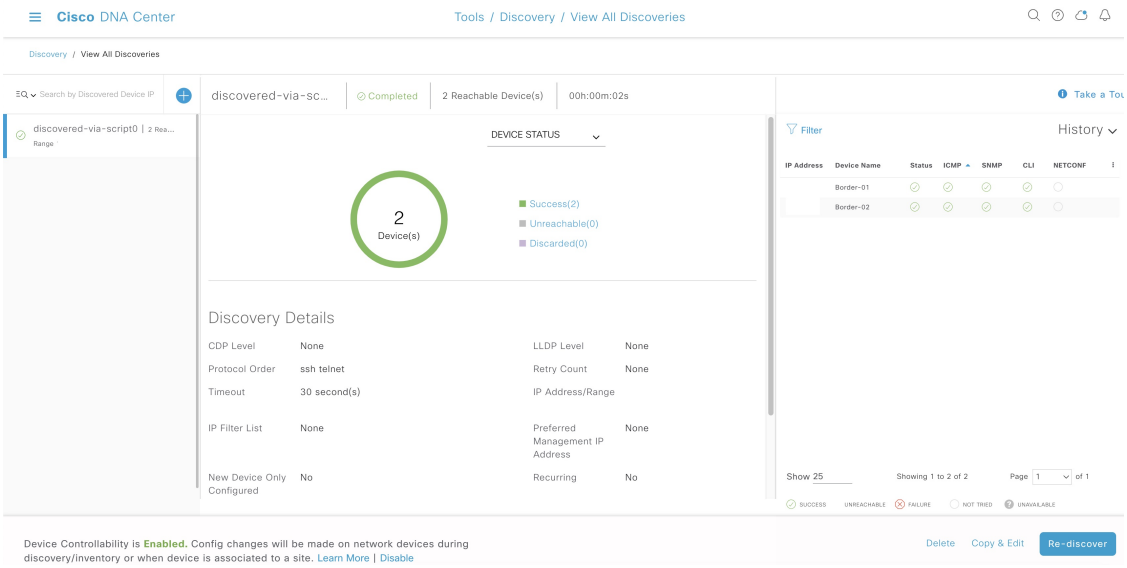


Step 4 Choose a discovery schedule and start the discovery.

In the **Schedule Job** window, click **Assign devices to an existing site** to assign devices to a site.

You can view the status and results of the scan in the **Discoveries** window.

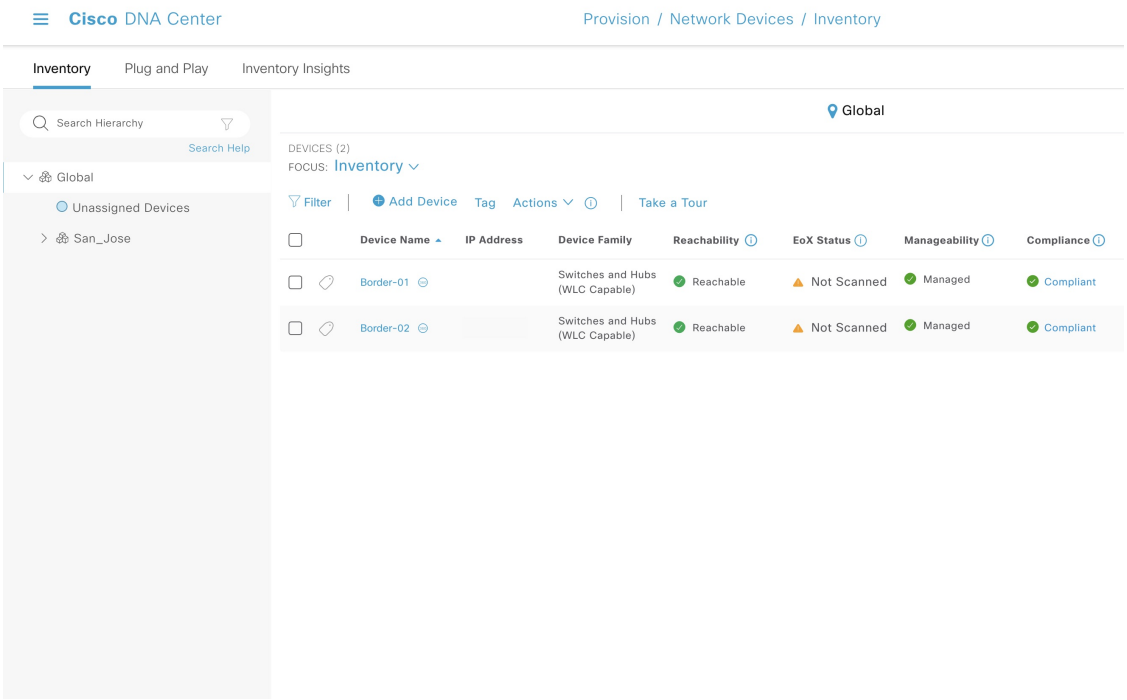
Note
The discovery process takes some time. Ensure that there are no failures after the process completes.



Step 5 Verify that the discovered device is added to the inventory.

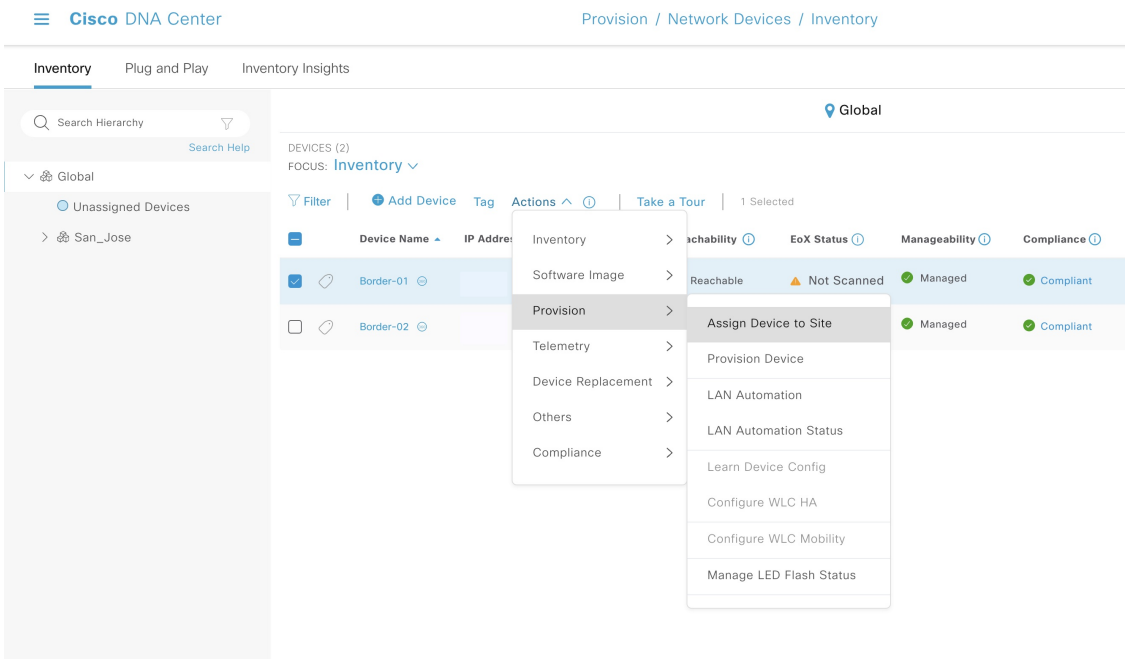
a) From the main menu, choose **Provision** > **Inventory**.

b) Make sure that the discovered device is in the inventory and the device is in *Reachable* and *Managed* state.



Step 6 (Optional: If you've not assigned the device during discovery) Assign devices to a site.

a) Check the check box next to the device and choose **Actions** > **Provision** > **Assign Device to Site** to assign the device to a site.

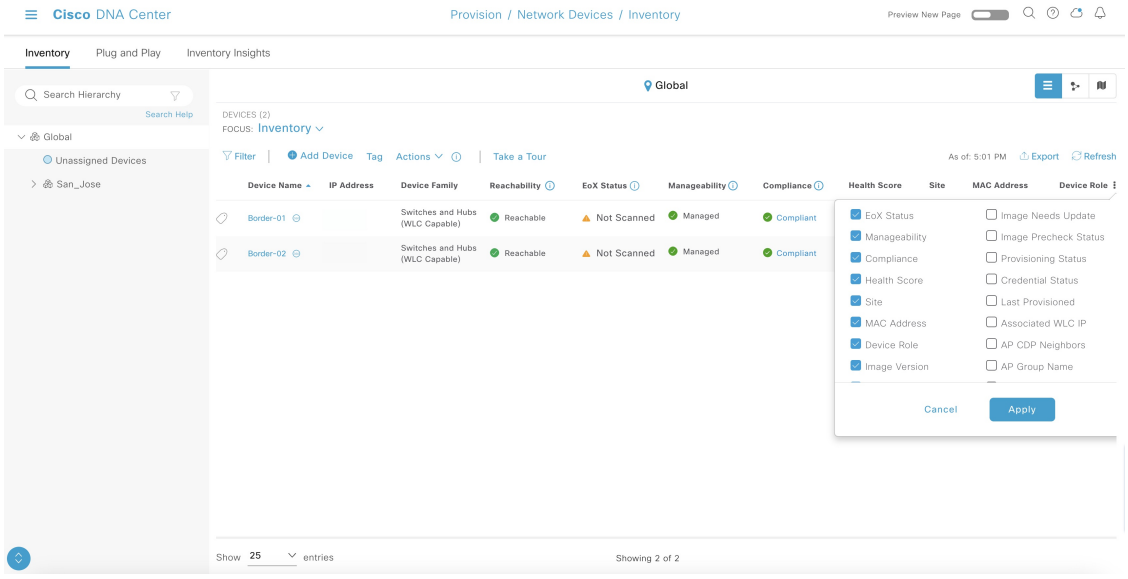


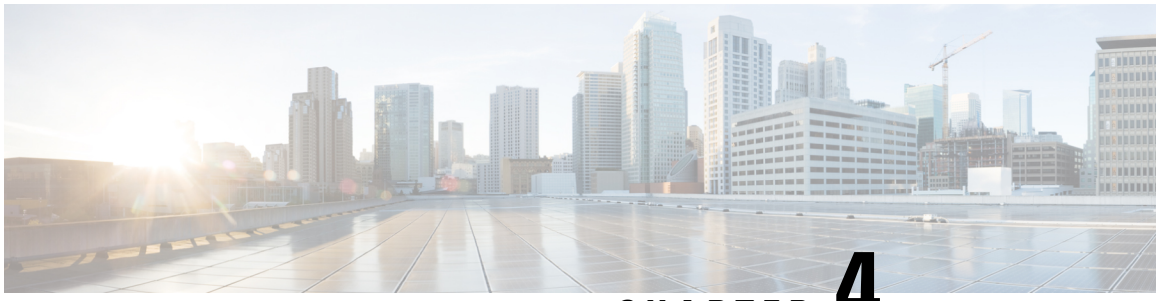
b) In the **Assign Device to Site** window, choose a site and click **Apply**.

For Catalyst Center 1.2.6 and earlier, ensure that both the primary and peer seeds are in the same site and same floor (although they can be physically on different floors).

The discovered device is added to the selected site.

Note
If you don't see the **Site** column in the **Inventory** window, go to settings, check the **Site** check box, and click **Apply**.





CHAPTER 4

Provisioning LAN Automation

Provisioning is the final step in the LAN automation process. It is divided into two stages:

1. **Device discovery and onboarding (starting LAN automation)**

   When LAN automation starts, Catalyst Center

   a. pushes the loopback and IS-IS configuration to the primary and peer seed devices and the temporary configuration to the primary seed device, enabling discovery and onboarding of the PnP agent.

Note Catalyst Center Release 2.3.3 and later support `is-type level-2-only` as part of IS-IS configurations.

   b. discovers new devices.

   c. upgrades the device software image and pushes the configuration to discovered devices.

Note The image is updated only if a golden image is marked for that switch type in Catalyst Center under **Design** > **Image repository**.

   When LAN automation starts, the temporary configuration is pushed to the primary seed device. This allows the device to discover and onboard the PnP agent. Next, the PnP agent image is upgraded and basic configurations such as loopback address, system MTU, and IP routing are pushed to the PnP agent.

2. **Interface configuration (stopping LAN automation)**

   When the LAN automation process stops,

   a. the discovery phase ends, and all point-to-point links between the seed and discovered devices and between the discovered devices (maximum of two hops) are converted to Layer 3.

   b. all temporary DHCP and VLAN 1 configurations on the seed and discovered devices are removed. The DHCP subpool is returned to the LAN automation pool.

Predeployment checklist for LAN automation

Review the essential prerequisites and validation steps before you start LAN automation, such as configuring IP pools, verifying the PnP agent, managing device inventory, and checking license compliance.

IP pool subnet reachability

A LAN pool is an IP address pool that is used for IP address allocation during LAN automation. LAN automation discovery uses the LAN pool to reach PnP agents.

Before starting LAN automation, make sure that Catalyst Center can reach the IP addresses allocated from the LAN pool.

Example

For example, if the LAN pool is 192.168.10.0, Catalyst Center should have the correct route to reach this subnet.

Refer to this sample code to test IP pool reachability:

1. Create an SVI (VLAN 1 interface) on the primary seed device.

```
[On seed device]

Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.99.1 255.255.255.0
Switch(config-if)#end
```

2. From the Catalyst Center console, ping the seed device.

```
[On Catalyst Center CLI console]

[Sat Jun 23 05:55:18 UTC] maglev@10.195.192.157
$ ping 192.168.99.1
PING 192.168.99.1 (192.168.99.1) 56(84) bytes of data.
64 bytes from 192.168.99.1: icmp_seq=1 ttl=252 time=0.579 ms
64 bytes from 192.168.99.1: icmp_seq=2 ttl=252 time=0.684 ms
64 bytes from 192.168.99.1: icmp_seq=3 ttl=252 time=0.541 ms
```

3. Reset the SVI configuration on the seed device when finished.

```
[On seed device]

Switch(config)#default int vlan 1
Interface Vlan1 set to default configuration
```

If the ping test fails, check the route configuration on Catalyst Center.

Add a static route for LAN pool

Catalyst Center hardware includes multiple physical interfaces. Each interface serves a different communication category. See the *Cisco Digital Network Architecture Center Appliance Installation Guide* for recommended interface connections, IP routing, and static assignment. In a single-home design, Catalyst Center performs the host function with the default gateway providing IP routing. In a multi-home design, Catalyst Center must have a static route to the LAN automation networks through the enterprise-facing interface.

Figure 5: IP addressing for single-home and multi-home designs

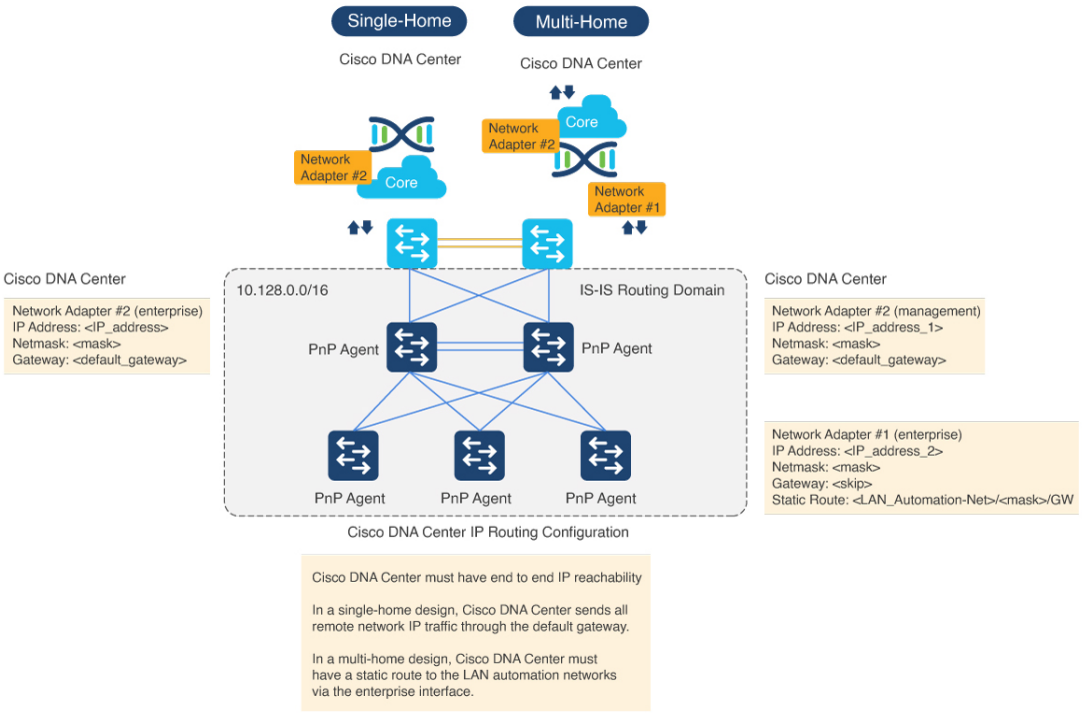
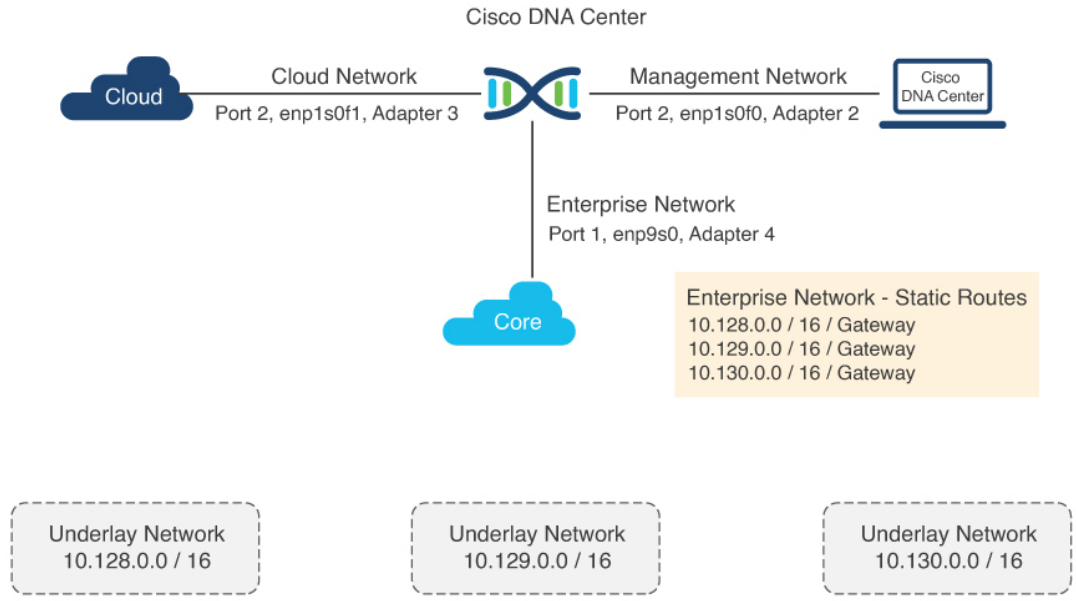


Figure 6: Static IP routing design



For a multi-home design, add a static route on Catalyst Center to resolve the IP reachability issue. You can add a static route during the initial Catalyst Center configuration or later using a maglev command. Do not use the Linux `route` command, because maglev APIs might not retrieve the correct information if the route is modified using the `route` command.

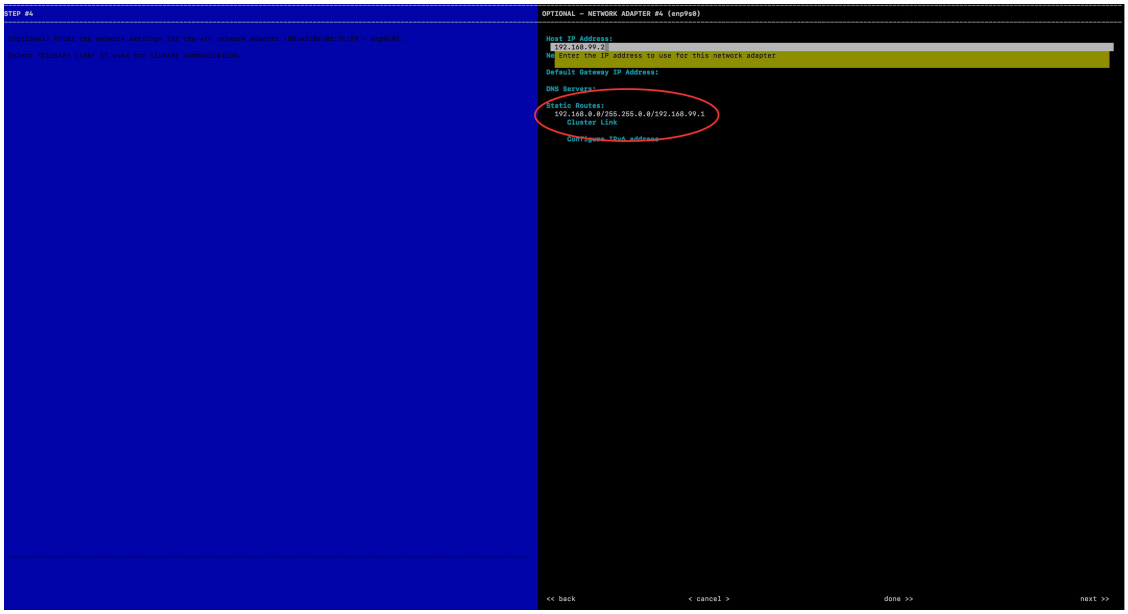
For a single-home design, verify routing between the seed device and Catalyst Center.

Follow these steps to add a static route on Catalyst Center:

Procedure

Step 1 On the Catalyst Center console, enter the command `sudo maglev-config update`.

The configuration wizard opens.



Step 2 Enter the static route and click **Next**.

The config wizard validates and configures host networking.

Step 3 Ensure that you select the correct interface to add the static route. If the correct interface is not displayed, click **Next** until it appears.

Step 4 Leave the **Network Proxy** field blank. If proxy validation fails, skip the proxy settings.

Step 5 To apply the changes to the controller, click **Proceed**.
Adding a static route takes five to six minutes (5-6 minutes). Ignore any warning messages.

Verify the PnP agent initial state

Procedure

Step 1 Before starting LAN automation, make sure that the PnP agent is in **System Configuration Dialog** state.

```
FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled
cisco C9300-24T (X86) processor with 1418286K/6147K bytes of memory.
```

```
Processor board ID FCW2137G032
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address          : f8:7b:20:48:d8:80
Motherboard Assembly Number        : 73-17952-06
Motherboard Serial Number          : FOC21354B06
Model Revision Number              : A0
Motherboard Revision Number        : A0
Model Number                       : C9300-24T
System Serial Number               : FCW2137G032


%INIT: waited 0 seconds for NVRAM to be available


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

Step 2 Do not press **Yes** or **No**. Leave the device in the same state.

Note

- If the device does not stop at this initial prompt and moves ahead, check the device config-register value using the CLI command `show ver | inc register`. In some cases, the value might be *0x142*. Change the config-register value to *0x102* or *0x2102* and save the configuration. Check the CLI again; it shows *Configuration register is 0x142 (will be 0x102 at next reload)*.
- If the device comes up with the older config-register value even after changing the value to 0x102 or 0x2102 and reloading the device, configure `no system ignore startupconfig switch all` on the device, save the configuration, and reload.
- For Cisco Catalyst 9000 series switches, use `pnpa service reset no-prompt`.

Step 3 Follow the same steps (*Step 1 and Step 2*) for stack switches.

- Allow extra time to make sure that all members in the stack are up. Do not start LAN automation until all switches are up.
- LAN automation always begins on the active switch. When all switches in a stack are booted together, the switch with the lowest MAC address (assuming no switch priority is configured) becomes active. The switch with the second lowest MAC address becomes the standby, and so on. Some customers require the first switch to always be active. In this case, if all the switches are booted together and the first switch does not have the lowest MAC address, it does not become the active switch. To ensure that the first switch is active, boot the switches in a staggered manner: boot *Switch 1*; after 120 seconds, boot *Switch 2*, and so on. This approach ensures that the switch becomes active in the correct order—*Switch 1* is active, *Switch 2* is standby, and so on. However, after a reload, the order may change because switches obtain their role based on their MAC address.
- To make sure that the switches maintain their order after reload, it is a good practice to assign switch priorities to ensure that the switches always come up in the same order. The highest priority is 15. During LAN automation, the priority of active switch is set to 15 by default. The priority of other switches is not altered. When priorities are assigned, they take precedence over the switch MAC address. Assigning switch priorities does not change the NVRAM configuration. The values are written to ROMMON and persist after reload or write erase. Refer to this sample code:

```
3850_edge_2#switch 1 priority ?
  <1-15>  Switch Priority
3850_edge_2#switch 1 priority 14
WARNING: Changing the switch priority may result in a configuration change for that switch. Do
you want to continue?[y/n]? [yes]: y
```

You might have to clean up the switch after assigning priorities because some certificates are configured on the switch during boot up. For instructions on cleaning up the switch, see PnP Agent Initial State.

Note
Do not start LAN automation until all switches in the stack are up.

If you are consoled in to the standby/member switches, do not press Enter, even though the screen says *console is now available, Press RETURN to get started*. Monitor the active switch, which should be at the **System Configuration Dialog** state.

If LAN automation is already running and you do not want to stop it, shut the seed link connecting to the PnP agent. That way, discovery doesn't occur until you are ready to bring up the link.

Port connections and license levels

Before starting LAN automation, verify the port connections and the license level on the devices.

- Connect PnP agents directly to seed devices. Do not connect PnP agents to any other network (for example, the management network) or any network that can provide DHCP through another server on VLAN 1.
- Ensure that the seed ports connected to the PnP agents use Layer 2 and are in the default state. For example, ports on Cisco Catalyst 6500 and 9500H switches use Layer 3 by default.
- Ensure that the port on the primary seed that connects to the PnP agents does not block STP.
- Ensure that the PnP agent is running the Advantage license level.

Remove a device from inventory

This section applies to devices that were discovered or LAN automated at any point.

If the devices to discover in an upcoming LAN automation session are already present in the inventory, remove them from inventory.

Before you begin

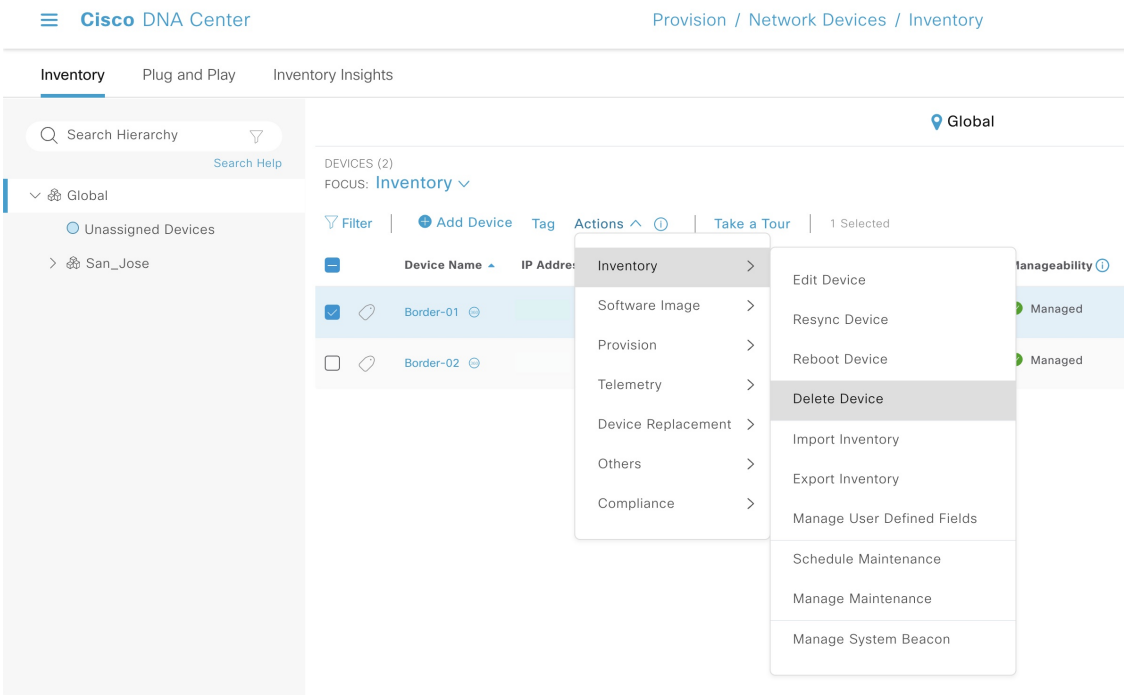
If a device was provisioned and added to the fabric, remove it from the fabric and unprovision it. Then, remove it from the inventory.

Procedure

Step 1 From the Catalyst Center home page, click the menu icon and choose **Provision** > **Inventory**.

Step 2 Filter the devices by **Serial Number**.

Step 3 Choose a device and from the **Actions** drop-down list, choose **Inventory** > **Delete Device**.



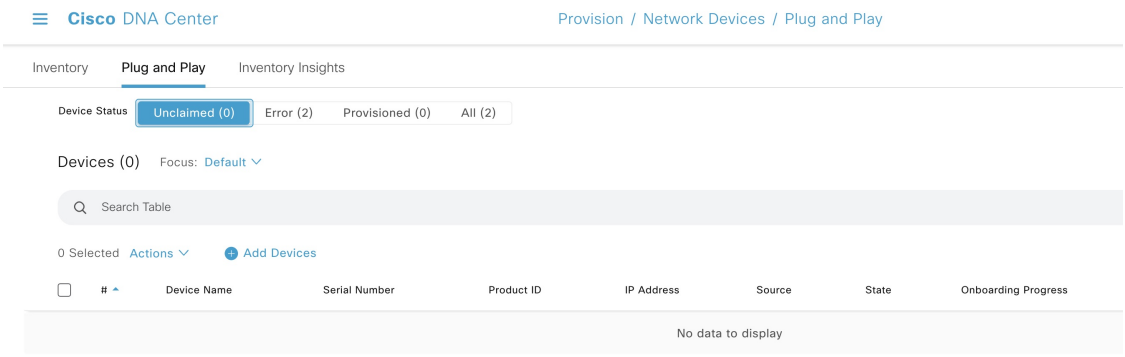
Remove devices from PnP before discovery

Before starting a LAN automation session, check whether the devices you want to discover are already listed in PnP. Remove them from PnP so that device discovery works as intended.

Procedure

Step 1 From the Catalyst Center home page, click the menu icon and choose **Provision** > **Plug and Play**.

Step 2 From the **Device Status** filter, choose **Unclaimed**. Make sure that the device (**Serial Number**) being discovered is not available under **Unclaimed**.



Step 3 If the device is available, log in to the device console and remove the PnP profile.

```
[on PNP agent]

3850_edge_2#show run | sec pnp-zero-touch
pnp profile pnp-zero-touch
 transport https ipv4 192.168.99.2 port 443

3850_edge_2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
3850_edge_2(config)#no pnp profile pnp-zero-touch
3850_edge_2
```

For Cisco IOS XE 16.12.x or later, use this command:

```
pnpa service reset no-prompt
```

Step 4 Check the check box next to the device in the **Unclaimed** section and choose **Actions** > **Delete**.

Verify the PnP agent mode

The PnP agent must be in INSTALL mode for image upgrade during LAN automation.

Image upgrade through LAN automation occurs in the background.

Note For modular switch platforms (Catalyst 9400 and 9600 series) with chassis plus supervisor, day-zero image upgrade is not supported. Instead, use day-*n* SWIM for image upgrade for these series of modular chassis.

Procedure

Step 1 Under **Design** > **Image Repository**, check whether a golden image is selected for the discovered device.

After PnP discovers the device, Catalyst Center checks if a golden image is marked for the switch family (Cisco Catalyst 9300 or 3850). If the golden image is marked and the discovered device is not running it, LAN automation upgrades the discovered device to the golden image. If not, Catalyst Center skips the image upgrade and pushes the initial device configuration.

Step 2 Ensure that the discovered device is running in INSTALL mode to allow LAN automation to upgrade the image. If the device is in BUNDLE mode, LAN automation will not upgrade the image.

Use the **show version** command to check the device mode.

Step 3 If the device is in BUNDLE mode and you want to proceed with LAN automation, remove the golden image for the relevant switch family under **Design** > **Image Repository**.

Configuring LAN automation attributes

To set up LAN automation, select the primary seed device, peer seed device, site for seed device, a LAN IP pool, and an interface. Optionally, configure other attributes such as, the device prefix, hostname CSV file, a configurable IS-IS password, discovery depth, device matching mode, and session timeout details.

- **Interface selection**

  The interfaces on the primary seed device are used for new device discovery and Layer 3 configuration. The interfaces on seed devices provide a filter to directly connect PnP agents that can be onboarded through the LAN automation session. For example, consider four directly connected PnP agents: *device 1* is connected through Gig1/0/10, *device 2* through Gig 1/0/11, *device 3* through Gig 1/0/12, and *device 4* through Gig 1/0/13. If you choose Gig 1/0/11 and Gig 1/0/12 as discovery interfaces, LAN automation discovers only *device 1* and *device 2*. If *device 3* and *device 4* try to initiate the PnP flow, LAN automation filters them because they connect through unselected interface. You can use this mechanism to restrict the discovery process.

  You can also choose interfaces between the primary seed and the peer seed to configure with Layer 3 links. If there are multiple interfaces between the primary and peer seeds, you can choose to configure any set of these interfaces with Layer 3 links. If no interfaces are chosen, they aren't configured with Layer 3 links.

  The option to choose a peer seed interface is not available. Interfaces between peer seed and PnP agents are automatically identified based on the topology information gathered from the device. The topology information is derived from the CDP data available on the device.

- **Site selection**: You can select sites for both seed devices and PnP agents. Currently, one site is designated for seed devices and one site for PnP agents.

- **LAN pool selection**

  The LAN pool is selected based on PnP agent site information. To start LAN automation, select a LAN pool from the list of pools available for a particular site. You can reuse the same LAN pool for multiple LAN automation sessions. For example, you can run a discovery session to find the initial set of devices. After the session completes, you can provide the same IP pool for subsequent LAN automation sessions. Similarly, you can choose a different LAN pool for other discovery sessions. Make sure the LAN pool you select has enough capacity.

- **IS-IS password**

  - If you enter a password, make sure it matches the password configured on the seed. If the entered value does not match the password on the primary and peer seeds, an error is returned.
  - If the password on the primary and peer seeds does not match, an error is returned.

*If you enter a value in the **IS-IS Password** field:*

- If the primary seed has an IS-IS password configured, LAN automation configures the primary seed's IS-IS password on the PnP devices (and on the peer seed, if it doesn't already have the password).
- If the primary seed doesn't have an IS-IS password but the peer does, LAN automation configures the peer seed's IS-IS password on the PnP devices and on the primary seed.
- If the primary and peer seeds don't have an IS-IS password configured and you enter a value in the password field, LAN automation configures the user-entered password on the PnP devices and on the primary and peer seeds.

*If you leave the **IS-IS Password** field blank:*

- If the primary seed has an IS-IS password configured, LAN automation configures the primary seed's IS-IS password on the PnP devices (and on the peer seed, if it doesn't already have the password).
- If the primary seed doesn't have an IS-IS password but the peer does, LAN automation configures the peer seed's IS-IS password on the PnP devices and on the primary seed.
- If the primary and peer seeds don't have an IS-IS password configured, LAN automation uses the default value "cisco" for the PnP devices and for both seeds.

- **OSPF** (Catalyst Center Release 3.1.x and later)
  - **Process Id**: The OSPF routing process identifier.
  - **Area Id**: OSPF area identifier for the network.
  - **Authentication key**: Password or key used for OSPF message authentication.

Note OSPF feature support is in beta and is not supported for IPv6 deployments.

- **Hostname mapping**
  - **Default**: If no value is entered, LAN automation sets the hostname as **Switch**, followed by the loopback address. Example: **Switch-192-168-199-100**.
  - **Device Name Prefix**: The device prefix is used to generate hostnames for discovered devices. LAN automation maintains the site counter and generates the name using the prefix and the current site counter. For example, if the device prefix is *Building-23-First-Floor*, LAN automation generates device names such as *Building-23-First-Floor-1*, and *Building-23-First-Floor-2*.
  - **Hostname Map File Format**: Catalyst Center expects a CSV file with the hostname and serial number along with site and IP address details. For stack LAN automation, the CSV file lets you enter one hostname and multiple serial numbers per row. Use commas to separate serial numbers.

Note If both a device name prefix and a hostname map file are used, the hostname map file takes precedence, and the device name prefix is not used.

Figure 7: Example of hostname file format

A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

- Attributes supported in Catalyst Center Release 2.3.7.5 and later.
  - **Discovery depth**: Devices are LAN automated up to the specified level under the primary seed device. The default value for **Discovery Depth** is 2, and the maximum value is 5.
  - **Device matching**: Specifies the method for device discovery.
    - **Relaxed**: Hostname and loopback IP is assigned to the discovered device if the device's serial number matches the uploaded device list.
    - **Strict**: Device discovery is restricted to the list of devices provided. You can discover a maximum of 50 devices.

    You can also download a sample CSV file for reference.
  - **Session Timeout**: Specifies a timeout value for the LAN automation session. LAN automation stops automatically when the specified time limit is reached. The value is specified in minutes, and the valid range is 20 to 10080 minutes.

Start LAN automation

Start the LAN automation process to discover and onboard PnP agents.

Before you begin

For Catalyst Center Release 2.3.5 and later, see Provision LAN automation, on page 61.

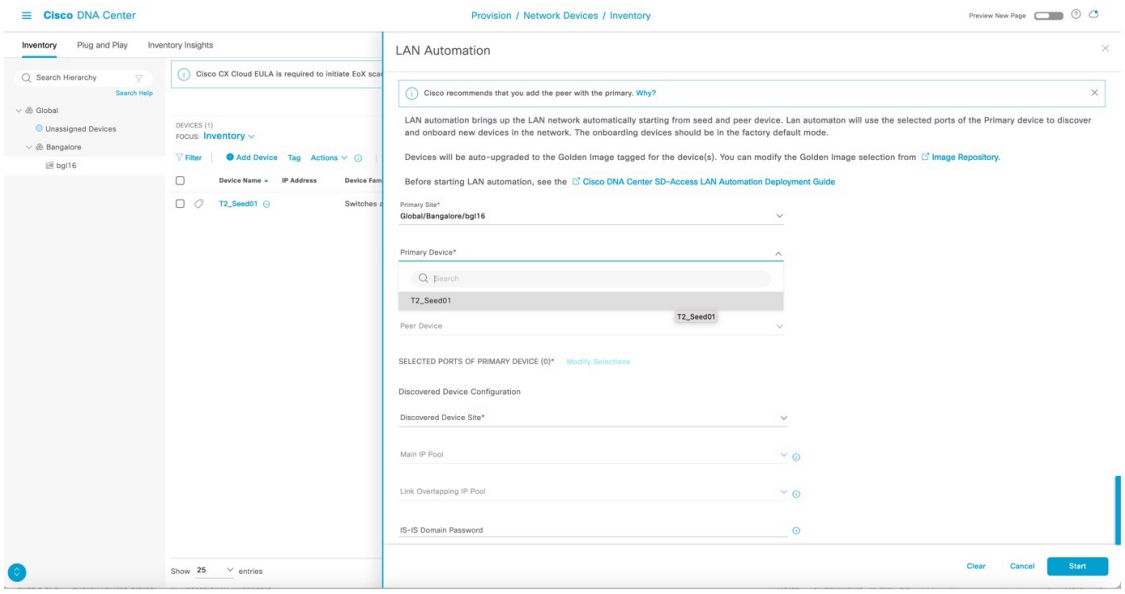
Procedure

Step 1 From the Catalyst Center GUI, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

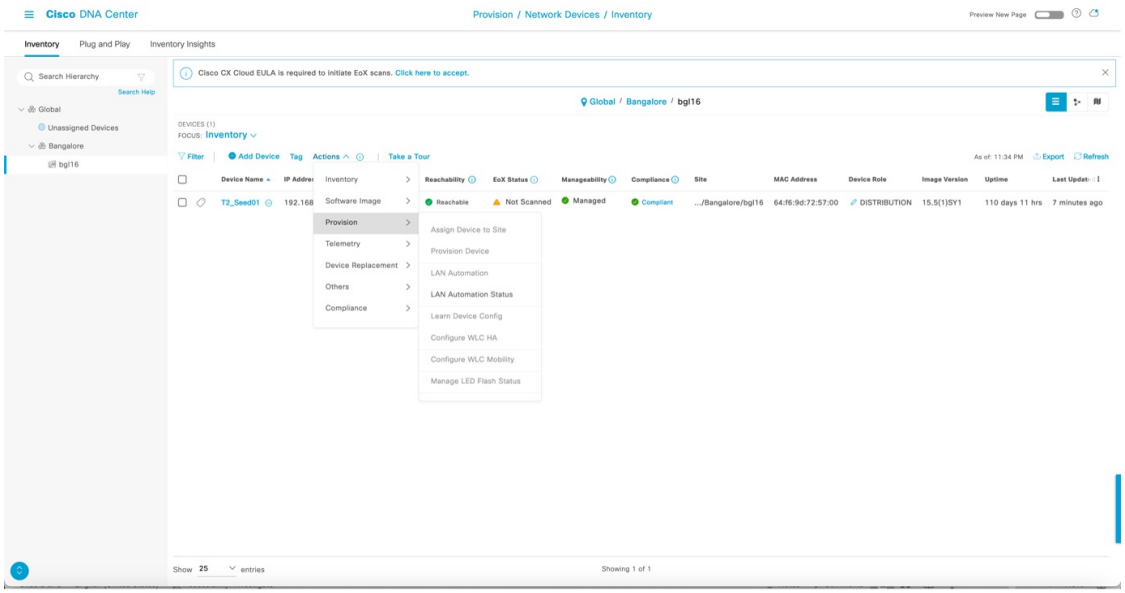
Step 2 In the **Inventory** window, choose **Actions** > **Provision** > **LAN Automation**.

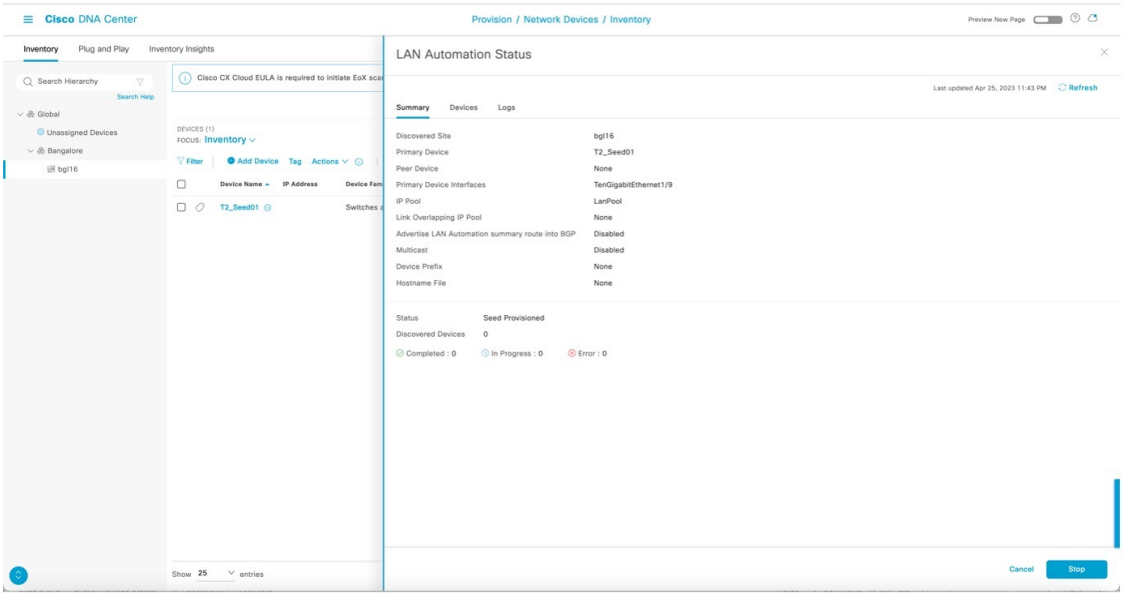
Step 3 Enter the required details and click **Start**.

For more information on the attributes, see Configuring LAN automation attributes, on page 37.



Step 4 After LAN automation starts, click **LAN Automation Status** to monitor the progress.





Sample configuration for seed devices

After LAN automation starts, the loopback and IS-IS configuration is pushed to the seed devices.

You can refer to these commands to view device configurations:

- System MTU and IP multicast routing information

```
show running-config | section system mtu
show running-config | section ip multicast
show running-config | section ip pim
```

- Loopback IP and IS-IS configuration

```
show running-config interface Loopback0
show running-config | section router isis
```

- DHCP pool information

```
show running-config | section ip dhcp
```

- VLAN 1

```
sh run int vlan1
```

- Other interface configurations

```
sh run int <interface_name>
```

This table lists sample configurations for the primary seed device.

Table 1: Primary seed configuration

Configuration type	Sample code
System MTU and IP multicast routing information	!exec: enable ! system mtu 9100 ! ip multicast-routing ip pim ssm default !
Loopback IP and IS-IS configuration If the secondary seed is configured, it also gets configured with the loopback IP and IS-IS configuration.	interface Loopback0 ip address 10.4.210.123 255.255.255.255 description Fabric Node Router ID ! router isis net 49.0000.0100.0421.0123.00 domain-password * is-type level-2-only metric-style wide nsf ietf log-adjacency-changes bfd all-interfaces passive-interface Loopback0 default-information originate ! interface Loopback0 ip router isis clns mtu 1400 ip pim sparse-mode exit !
DHCP pool information	ip dhcp pool nw_orchestration_pool network 10.4.218.0 255.255.255.192 option 43 ascii 5A1D;B2;K4;I10.4.249.241;J80; default-router 10.4.218.1 class ciscopnp address range 10.4.218.2 10.4.218.62 ! ip dhcp class ciscopnp option 60 hex 636973636f706e70 ! ip dhcp excluded-address 10.4.218.1 !
VLAN 1 configuration	vlan 1 ! interface Vlan1 ip address 10.4.218.1 255.255.255.192 no shutdown ip router isis clns mtu 1400 bfd interval 500 min_rx 500 multiplier 3 no bfd echo exit !

Configuration type	Sample code

Switch port configuration on interfaces used for discovery
Each discovery interface on the primary seed device gets this configuration.
	interface TenGigabitEthernet1/1/8
	  switchport
	  switchport mode access
	  switchport access vlan 1
	!
	interface TenGigabitEthernet1/1/7
	  switchport
	  switchport mode access
	  switchport access vlan 1
	exit

Multicast configuration (optional; only configured if the multicast check box is checked)
If the Rendezvous Point (RP) for the underlay multicast needs to be the border, ensure to start LAN automation with multicast enabled using a switch that is planned to be the border as the seed device.
If the peer seed is configured, these multicast CLIs are pushed on the peer seed as well. The same `rp-address` is used to configure Loopback60000 on both the primary and peer seeds.
	interface Loopback60000
	  ip address 10.4.218.67 255.255.255.255
	  ip pim sparse-mode
	  ip router isis
	
	ip pim register-source Loopback0
	ip pim rp-address 10.4.218.67

This table lists sample configurations for the secondary seed device.

Table 2: Secondary seed configuration

Configuration type	Sample code
System configuration and IP multicast routing information	!exec: enable ! system mtu 9100 ! ip multicast-routing ip pim ssm default !

Configuration type	Sample code

Loopback IP and IS-IS configuration	interface Loopback0
	  ip address 10.4.210.124 255.255.255.255
	  description Fabric Node Router ID
	!
	router isis
	  net 49.0000.0100.0421.0124.00
	  domain-password *
	  is-type level-2-only
	  metric-style wide
	  nsf ietf
	  log-adjacency-changes
	  bfd all-interfaces
	  passive-interface Loopback0
	  default-information originate
	!
	interface Loopback0
	ip router isis
	clns mtu 1400
	ip pim sparse-mode
	exit
	!

Note

- Catalyst Center Release 2.3.3 and later support `is-type level-2-only` as part of the IS-IS configuration.
- In Catalyst Center Release 2.3.7.5 and later, the `clns mtu` value is configured as 1492 instead of 1400.

Step 5 After device discovery starts, view the logs on the PnP agent.

Note
Do not press the Enter key on the PnP agent yet.

```
%INIT: waited 0 seconds for NVRAM to be available

         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!

*Aug  2 23:13:50.440: %SMART_LIC-5-COMM_RESTORED: Communications with the Cisco Smart Software Manager
 or satellite restored
*Aug  2 23:13:51.314: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1875844429 has been
 generated or imported
*Aug  2 23:13:51.315: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Aug  2 23:13:51.355: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to
 save new IOS PKI configuration
*Aug  2 23:13:51.418: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1875844429.server
has been generated or imported
*Aug  2 23:13:52.071: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively
 down
*Aug  2 23:13:53.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to down
*Aug  2 23:14:00.112: %HMANRP-6-EMP_ELECTION_INFO: EMP active switch 1 elected: EMP_RELAY: Mgmt port
 status DOWN, reelecting EMP active switch

*Aug  2 23:14:00.112: %HMANRP-6-EMP_NO_ELECTION_INFO: Could not elect active EMP switch, setting emp
 active switch to 0: EMP_RELAY: Could not elect switch with mgmt port UP
```

```
*Aug  2 23:14:02.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 23:14:04 UTC Thu Aug 2
 2018 to 23:14:02 UTC Thu Aug 2 2018, configured from console by vty0.
Aug  2 23:14:02.000: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
Aug  2 23:14:02.462: %PNP-6-PNP_DISCOVERY_DONE: PnP Discovery done successfully
Aug  2 23:14:07.847: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to
save new IOS PKI configuration
Aug  2 23:14:16.348: %AN-6-AN_ABORTED_BY_CONSOLE_INPUT: Autonomic disabled due to User intervention
 on console. configure 'autonomic' to enable it.
%Error opening tftp://255.255.255.255/network-confg (Timed out)
Aug  2 23:14:25.263: AUTOINSTALL: Tftp script execution not successful for Vl1.
```

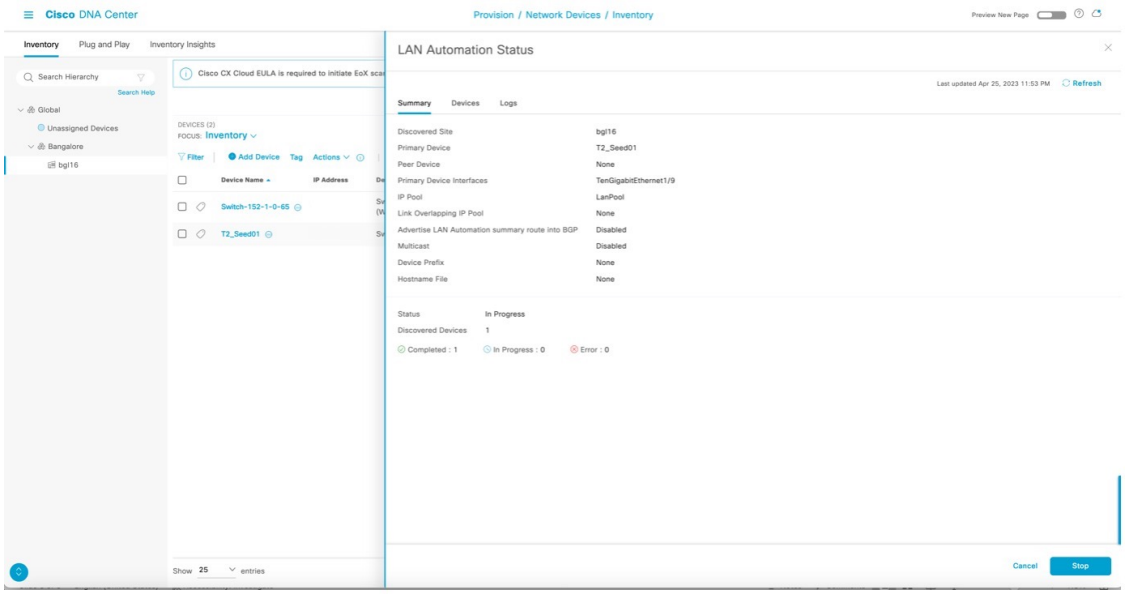
Step 6 After the device is discovered, Catalyst Center checks if a golden image is marked for the switch family of the discovered device. If a golden image is marked and the discovered device is not running it, LAN automation first upgrades the discovered device to the golden image. If not, Catalyst Center skips the image upgrade and pushes the initial device configuration.

Sample logs for image upgrade:

```
Oct  5 19:20:11.437: MCP_INSTALLER_NOTICE:
Installer: Source file flash:cat9k_iosxe.16.06.04s.SPA.bin is in flash, Install directly
Oct  5 19:20:12.450: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct  5 19:20:12 provision.sh:
%INSTALL-5-OPERATION_START_INFO: Started install package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct  5 19:20:22.778: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct  5 19:20:22 packtool.sh:
%INSTALL-5-OPERATION_START_INFO: Started expand package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct  5 19:21:26.034: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct  5 19:21:26 packtool.sh:
%INSTALL-5-OPERATION_COMPLETED_INFO: Completed expand package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct  5 19:22:09.861: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct  5 19:22:09 provision.sh:
%INSTALL-5-OPERATION_COMPLETED_INFO: Completed install package flash:{<package_name>}


***
*** --- SHUTDOWN NOW ---
***

Oct  5 19:22:20.950: %SYS-5-RELOAD: Reload requested by controller. Reload Reason: Image Install.
                          Chassis 1 reloading, reason - Reload command
                                                Oct  5 19:22:30.501 FP0/0: %PMAN-5-EXITACTION: Process
 manager is exiting: reload fp action requested
Oct  5 19:22:

Initializing Hardware...
```

Catalyst Center pushes part of the configuration, allowing the devices to be onboarded and managed by Catalyst Center. In the **LAN Automation Status** window,

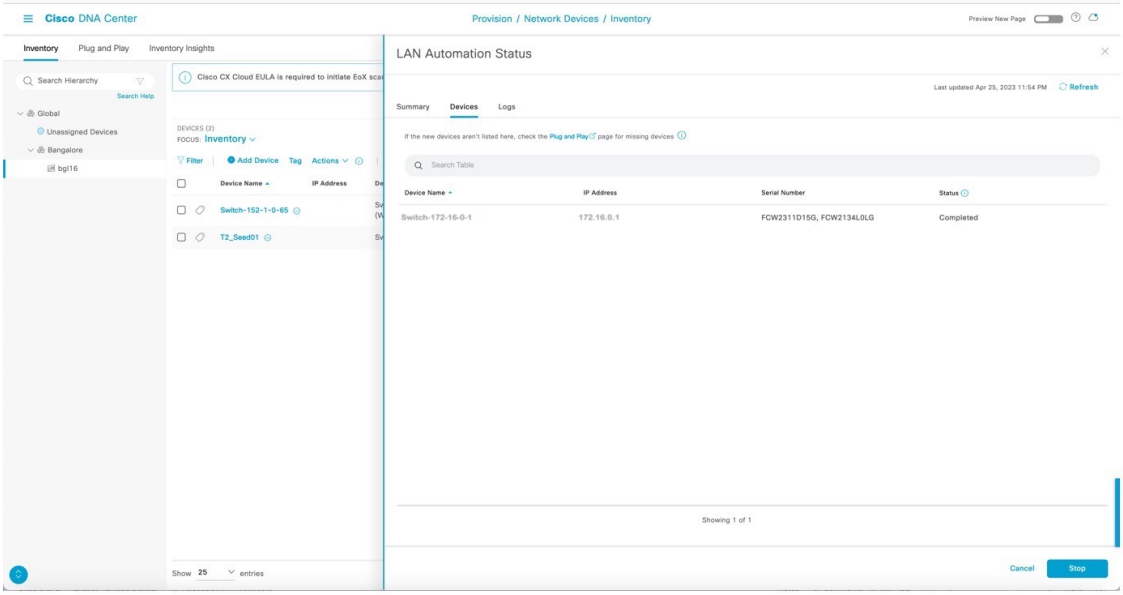
- **Status** displays *In Progress*.
- **Discovered Devices** displays the aggregate status of all devices being discovered.
- **Devices** tab displays the status of individual devices being discovered.

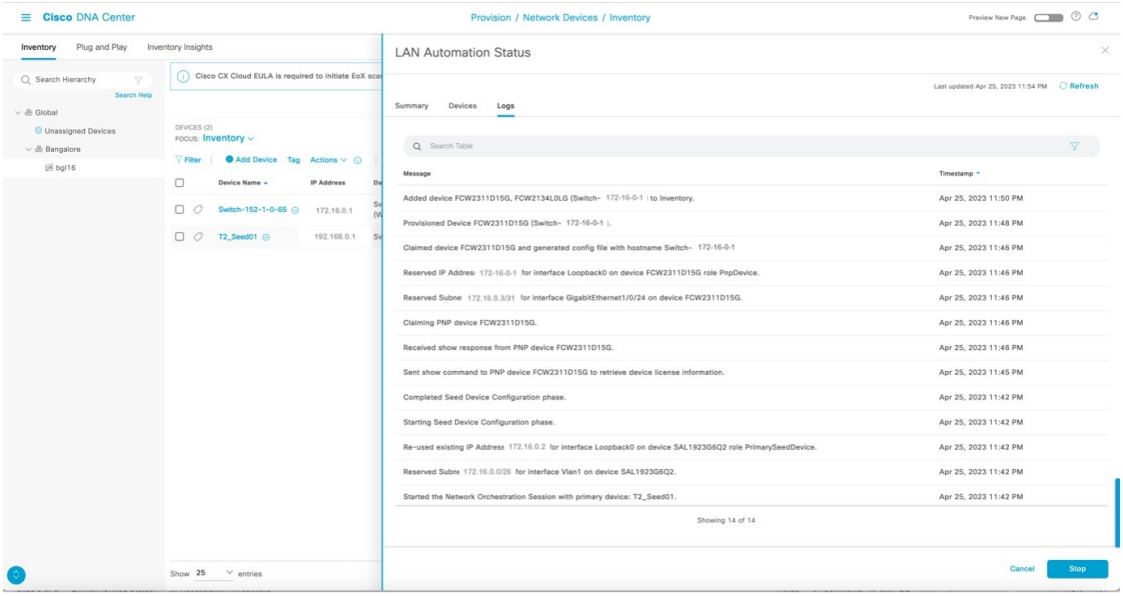


Step 7 View the logs on the PnP agent, as shown in the example. It is safe to press return on the console if you want to. When you press return, the hostname changes to the value entered in the **Hostname Mapping** field when you started LAN automation.

```
Aug  2 23:14:50.682: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to up
Aug  2 23:14:51.487: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
Aug  2 23:14:51.681: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed
state to up
Aug  2 23:14:51.854: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/23, changed state to up
Aug  2 23:14:52.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed
 state to up
Aug  2 23:14:52.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed
 state to up
000123: Aug  2 23:16:17.345: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named dnac-sda has been generated
 or imported
000124: Aug  2 23:16:17.423: Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...

000125: Aug  2 23:16:17.474: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
 to up
000126: Aug  2 23:16:17.479: %CLNS-6-DFT_OPT: Protocol timers for fast convergence are Enabled.
000128: Aug  2 23:16:17.489: %BFD-6-BFD_IF_CONFIGURE: BFD-SYSLOG: bfd config apply, idb:Vlan1
000129: Aug  2 23:16:18.423: %CLNS-3-BADPACKET: ISIS: LAN L1 hello, packet (9097) or wire (8841)
length invalid from f87b.2077.b147 (Vlan1)
000130: Aug  2 23:16:18.502: %BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 204.1.183.1
 proc:ISIS, idb:Vlan1 handle:1 act
000131: Aug  2 23:16:19.269: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:1 handle:1 is going
UP
000132: Aug  2 23:16:19.494: %CLNS-5-ADJCHANGE: ISIS: Adjacency to 0100.1001.0001 (Vlan1) Up, new
adjacency
000133: Aug  2 23:16:20.289: %PNPA-DHCP Op-43 Msg: Op43 has 5A. It is for PnP
000134: Aug  2 23:16:20.289: %PNPA-DHCP Op-43 Msg: After stripping extra characters in front of 5A,
 if any

000135: Aug  2 23:16:20.289: %PNPA-DHCP Op-43 Msg: _pdoon.2.ina=[Vlan1]
000136: Aug  2 23:16:20.289: %PNPA-DHCP Op-43 Msg: _papdo.2.eRr.ena
000137: Aug  2 23:16:20.289: %PNPA-DHCP Op-43 Msg: _pdoon.2.eRr.pdo=-1
000138: Aug  2 23:16:30.010: %CLNS-5-ADJCHANGE: ISIS: Adjacency to 9324-SN-BCP-1 (Vlan1) Up, new
adjacency
```

After all devices are discovered, the **Discovered Devices** status changes to *Completed* and the discovered devices are added to the inventory.





Step 8 From the Catalyst Center home page, click the menu icon and choose **Provision** > **Inventory** and filter the devices by serial number.

The newly discovered switches appear as *Managed*.

The example shows a sample configuration pushed to the discovered devices.

```
!
archive
log config
logging enable
logging size 500
```

```
hidekeys
!
!
!
service timestamps debug datetime msec
!
service timestamps log datetime msec
!
service password-encryption
!
service sequence-numbers
!
! Setup NTP Server
! Setup Timezone & Daylight Savings
!
ntp server 10.4.250.104
!
! ntp update-calendar
!
! clock timezone <timezoneName> <timezoneOffsetHours> <timezoneOffsetMinutes>
! clock summer-time <timezoneName> recurring
!
! Disable external HTTP(S) access
! Disable external Telnet access
! Enable external SSHv2 access
!
no ip http server
!
no ip http secure-server
!
ip ssh version 2
!
ip scp server enable
!
line vty 0 15
! maybe redundant
login local
transport input ssh
! maybe redundant
transport preferred none
! Set VTP mode to transparent (no auto VLAN propagation)
! Set STP mode to Rapid PVST+ (prefer for non-Fabric compatibility)
! Enable extended STP system ID
! Set Fabric Node to be STP Root for all local VLANs
! Enable STP Root Guard to prevent non-Fabric nodes from becoming Root
! Confirm whether vtp mode transparent below is needed
vtp mode transparent
!
spanning-tree mode rapid-pvst
!
spanning-tree extend system-id
! spanning-tree bridge priority 0
! spanning-tree rootguard
! spanning-tree portfast bpduguard default
no udld enable
!
errdisable recovery cause all
!
errdisable recovery interval 300
!
ip routing
!Config below applies only on underlay orchestration
!
! Setup a Loopback & IP for Underlay reachability (ID)
```

```
! Add Loopback to Underlay Routing (ISIS)
!
interface loopback 0
description Fabric Node Router ID
ip address 10.4.218.97 255.255.255.255
ip router isis
!
!
! Setup an ACL to only allow SNMP from Fabric Controller
! Enable SNMP and RW access based on ACL
!
snmp-server view DNAC-ACCESS iso in
!
snmp-server group DNACGROUPAuthPriv v3 priv read DNAC-ACCESS write DNAC-ACCESS
!
snmp-server user admin DNACGROUPAuthPriv v3 auth MD5 C1sco123 priv AES 128 C1sco123
!
!
! Set MTU to be Jumbo (9100, some do not support 9216)
!
system mtu 9100
! FABRIC UNDERLAY ROUTING CONFIG:
!
! Enable ISIS for Underlay Routing
! Specify the ISIS Network ID (e.g. encoded Loop IP)
! Specific the ISIS domain password
! Enable ISPF & FRR Load-Sharing
! Enable BFD on all (Underlay) links
!
router isis
net 49.0000.0100.0421.8097.00
domain-password <password>
is-type level-2-only
metric-style wide
nsf ietf
! fast-reroute load-sharing level-1
log-adjacency-changes
bfd all-interfaces
! passive-interface loopback 0
!
!
!
interface vlan1
bfd interval 500 min_rx 500 multiplier 3
no bfd echo
!
!
!This config goes to subtended node

username lan-admin privilege 15 password 0 C1sco123
!
enable password C1sco123
!
!
hostname CL-9300_7
!
interface vlan1
ip router isis
!
!
end
```

Note

Catalyst Center 2.3.3 and later support `is-type level-2-only` as part of the IS-IS configuration.

Step 9 After the **Discovered Devices** status changes to *Completed* and all discovered devices are displayed in the inventory as *Managed*, you can stop LAN automation.

However, before stopping LAN automation, check the **Topology** page to make sure that the links between the discovered device and primary and peer seed are displayed.

a. Choose **Tools** > **Topology** or **Provision** > **Inventory** and click the topology icon on the right.

b. Click the physical links between the seed and discovered device.

Make sure that the interfaces are correct. If the physical links are not visible, resynchronize the seed device where the physical links connect. After resynchronization, check the **Topology** window again to make sure that the links are visible before stopping LAN automation.

Stop LAN automation

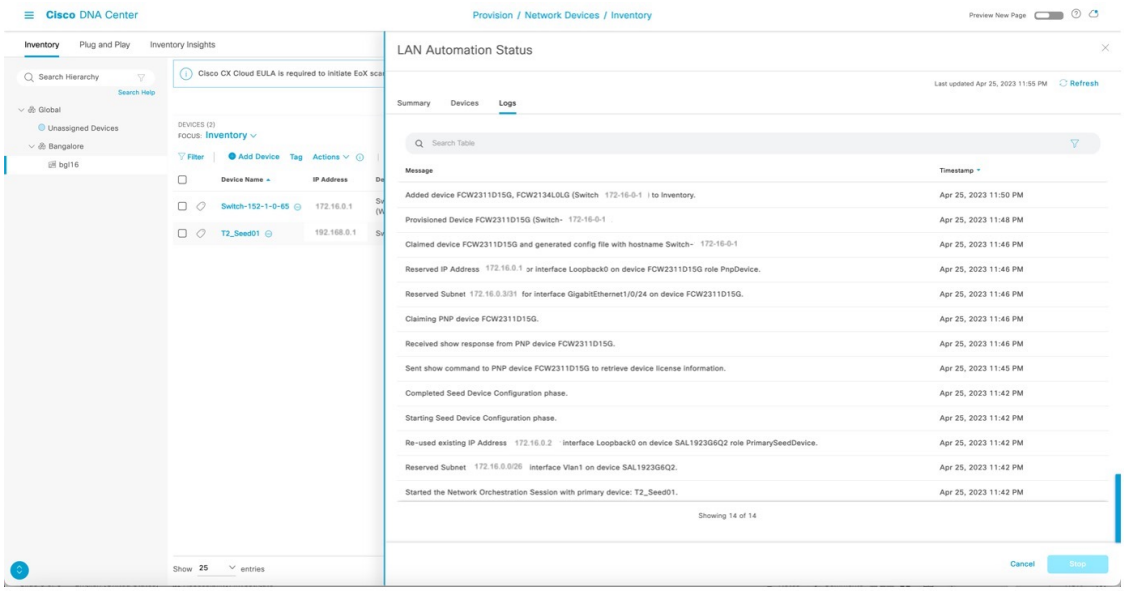
Stop LAN automation to finish discovering required devices and to prevent inadvertent discovery of additional devices.

When LAN automation stops, these actions occur:

- The remainder of the configuration is pushed to network devices, which includes converting the point-to-point links from Layer 2 to Layer 3.
- The configuration for VLAN 1 is removed, and the IP addresses for VLAN 1 are returned to the LAN automation pool.
- The device is onboarded in Catalyst Center and assigned to the site.

Stop LAN automation process

1. In the **LAN Automation Status** window, click **Stop**.



2. After the LAN automation stop process starts, the **LAN Automation Status** changes to **STOP in Progress**.
3. The network orchestration service issues a synchronization operation (RESYNC) for seed and PnP devices to retrieve the state of all links. After the initial RESYNC completes, the service pushes the Layer 3 configuration on all Layer 2 links. It then reissues RESYNC to resynchronize the cluster's link state.

   The Layer 3 link configuration is pushed when network orchestration stops. Each interface pair receives its configuration.

   Sample configuration

   Command:

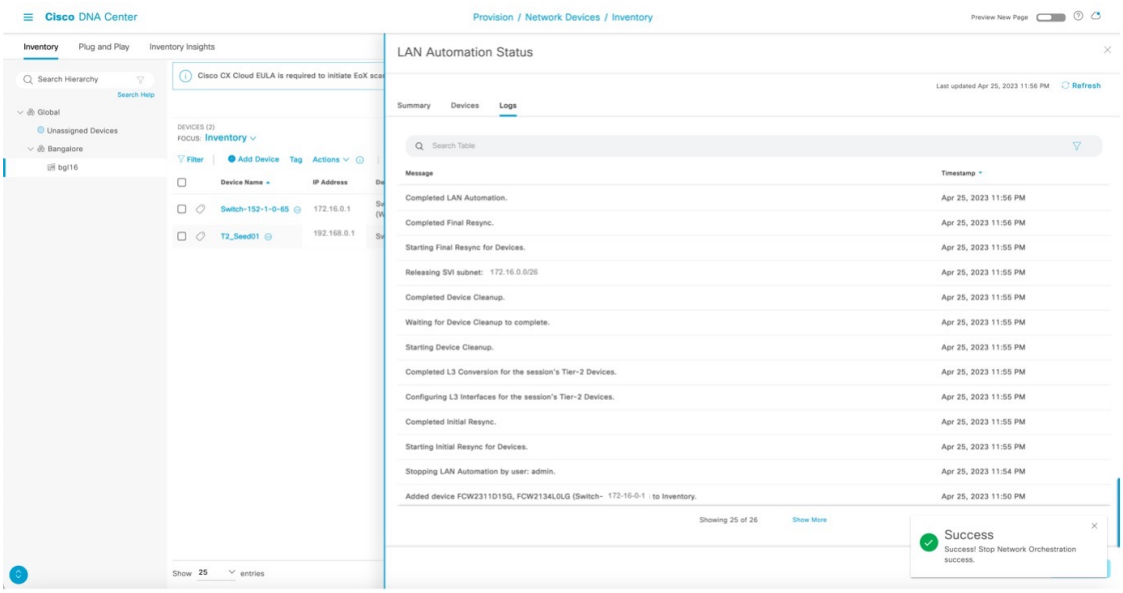
   ```
   show run int <int_name>
   ```

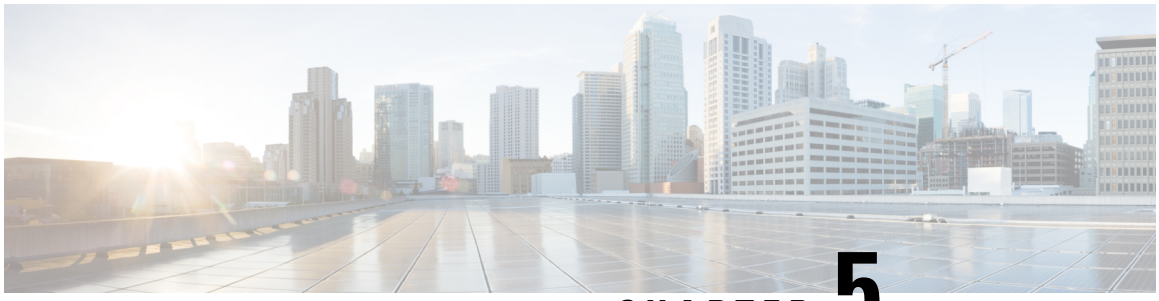
   Sample output:

   ```
   interface GigabitEthernet1/0/13
    description Fabric Physical Link
    no switchport
    dampening
    ip address 192.168.2.97 255.255.255.252
    ip router isis
    logging event link-status
    load-interval 30
    bfd interval 500 min_rx 50 multiplier 3
    no bfd echo
    isis network point-to-point
   ```

4. After all the point-to-point links between the seeds and discovered devices, including links between peer seed and discovered devices, are configured, the devices are added to the site and synced to Catalyst Center.
5. The LAN automation process completes and the **LAN Automation Status** changes to **Completed**.
6. Check the LAN automation logs to verify the status.

Stop LAN automation





CHAPTER 5

Manage a LAN-Automated Stack

Add a new switch

You can add switches to a stack that is already LAN automated and in a provisioned state without LAN automating or discovering the new switch.

Before you begin

Ensure that these conditions are met.

- The switch is not discovered and not present in the Catalyst Center inventory.
- The switch has the same image and license version as the provisioned standalone or stack. Use the `show ver` and `show license right-to-use` commands to verify the image and license version.
- The switch is in the same boot mode as the stack: INSTALL (preferred) or BUNDLE mode.

  Refer to this sample configuration to verify the boot mode:

```
9300_Edge_1#show ver | inc INSTALL
*    1 62    C9300-48U          16.6.3           CAT9K_IOSXE           INSTALL
     2 62    C9300-48U          16.6.3           CAT9K_IOSXE           INSTALL
     3 62    C9300-48U          16.6.3           CAT9K_IOSXE           INSTALL
     4 62    C9300-48U          16.6.3           CAT9K_IOSXE           INSTALL
```

Procedure

Step 1 Use the stack cable to connect the new switch to the stack, and then power it on.

After two to three minutes, the new switch is added to the stack as a standby if only one switch is present in the stack, or as a member if two or more switches are present.

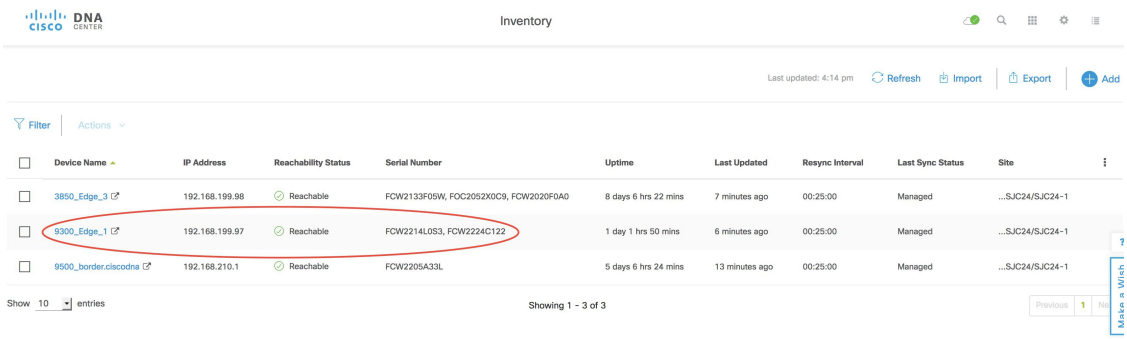
Step 2 Use the commands `show ver` and `show switch` to make sure that the new switch is added. The `show ver` command displays the serial numbers for all switches.

Step 3 After adding the switch to the stack, open the Catalyst Center inventory, choose the original provisioned switch or stack, and resynchronize.

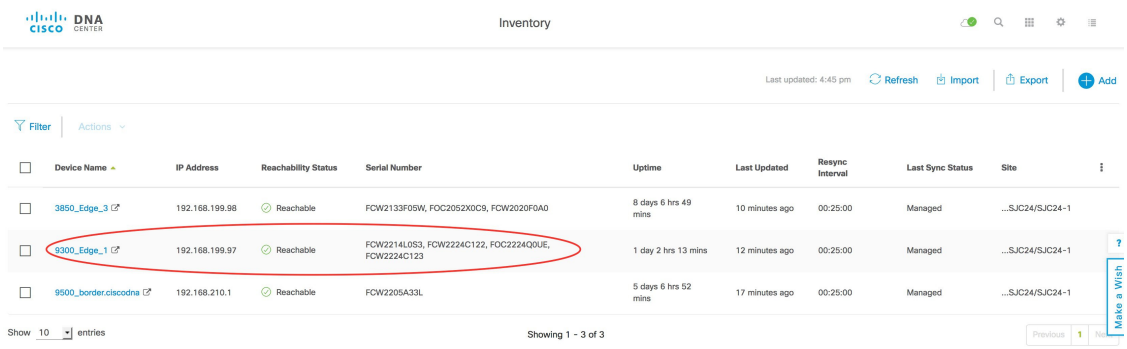
Step 4 After the synchronization completes, the new serial number is displayed in the inventory. This completes the addition process.

Note
You can add more than one switch at a time. Repeat the procedure and ensure that you use correct cabling.

This image displays the serial number before adding the new switch.



This image displays the serial number after adding the new switch.



Add an existing switch

This section shows how to add an existing switch that was already present in Catalyst Center.

If the switch was previously LAN-automated, either as part of another stack or as a standalone device, or was discovered by PnP, remove the switch physically before adding it. Next, remove its entry from the inventory, and from the PnP application or database

Remove the switch from inventory

If the switch is...	Then...
standalone	1. From the Catalyst Center home page, choose **Provision** > **Inventory**. 2. Choose the switch to remove, and from the **Actions** drop-down list, choose **Inventory** > **Delete Device**.
part of a stack	1. Remove the switch physically. 2. Resynchronize the original stack. After synchronization completes, check that the removed switch is no longer listed in the inventory.

Remove the switch from PnP

If the switch is...	Then...
standalone	1. Remove the PnP profile (`pnp profile pnp-zero-touch`) from the switch. 2. Delete the entry from the PnP database under **Device**.
part of a stack	1. Remove the switch physically. 2. Verify that the removed switch does not have the PnP profile (`pnp profile pnp-zero-touch`). 3. Delete the entry from the PnP database under **Device**.

Configure additional links between devices

Use this procedure to configure

- additional links between the primary and peer seed devices or between distribution devices after LAN automation stops, and
- uplinks from the newly added stack switch to the primary and peer seed devices.

If you chose the Enable Multicast option the first time LAN automation ran on the device, do not choose Enable Multicast when you configure additional links.

Follow these steps to configure the Layer 3 links using LAN automation. When LAN automation stops, go to the newly configured Layer 3 ports and manually configure **ip pim sparse-mode** under the interface.

Before you begin

For Catalyst Center Release 2.3.5 and later, refer Create a link between interfaces, on page 71.

Procedure

Step 1 Run the **show cdp neighbors** command to ensure that the neighbor connected to the new link is displayed.

For example, a new link connects the *Ten 4/1/5* port on switch *9300_Edge-7* to the *For 1/0/1* port on switch *9500_border-6* as shown in this sample configuration.

```
9300_Edge-7#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
9500_border.cisco.com
                 Ten 1/1/5         173             R S I  C9500-12Q For 1/0/1
9500_border-6.cisco.com
                 Ten 4/1/5         136             R S I  C9500-12Q For 1/0/1
```

Step 2 Ensure that both ports to which the link is connected (*Ten 4/1/5* and *For 1/0/1*) do not have any Layer 3 configurations on them. If Layer 3 configurations exist, use the default interfaces for the new uplink and resynchronize both devices.

Step 3 From the Catalyst Center home page, choose **Provision** > **LAN Automation**.

Step 4 In the **Primary Device** field, enter the switch (for example, **`9500_border-6`**) to which the new link is connected.

Step 5 In the **Peer Device** field, enter the switch (for example, **`9300_Edge-7`**) where you want to configure the new link.

Step 6 Select the port on the primary device where the uplink connects; that is, the port where the PnP device is connected (for example, **`For 1/0/1`**).

Step 7 Use the same LAN automation pool that was used to provision the original stack.

Step 8 Start LAN automation. Wait for two minutes, and then stop LAN automation. Because no new device discovery is necessary, skip the full LAN automation process. After you stop LAN automation, both ports connected to the uplink are configured with an IP address from the same LAN automation pool.

Step 9 As shown in the example, after LAN automation stops and completes, both ports are configured for Layer 3 from the LAN pool.

```
9300_Edge-7#show run int t4/1/5
Building configuration...

Current configuration : 325 bytes
!
interface TenGigabitEthernet4/1/5
 description Fabric Physical Link
 no switchport
```

```
 dampening
 ip address 192.168.199.85 255.255.255.252
 ip router isis
 logging event link-status
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 isis network point-to-point

9500_border-6#show run int Fo1/0/1
Building configuration...

Current configuration : 327 bytes
!
interface FortyGigabitEthernet1/0/1
 description Fabric Physical Link
 no switchport
 dampening
 ip address 192.168.199.86 255.255.255.252
 ip router isis
 logging event link-status
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 isis network point-to-point
end
```

Note
If you are familiar with APIs, add the IP addresses manually using API calls. However, we recommend adding IP addresses through LAN automation, because it updates all table entries automatically. Another advantage of LAN automation is that when the device is removed from the inventory, all associated IP addresses are released. If IP addresses are configured manually through APIs, they are not released.

Move an uplink to the newly added switch

You cannot move an uplink from a stack that is already provisioned to a newly added switch in a LAN-automated stack.

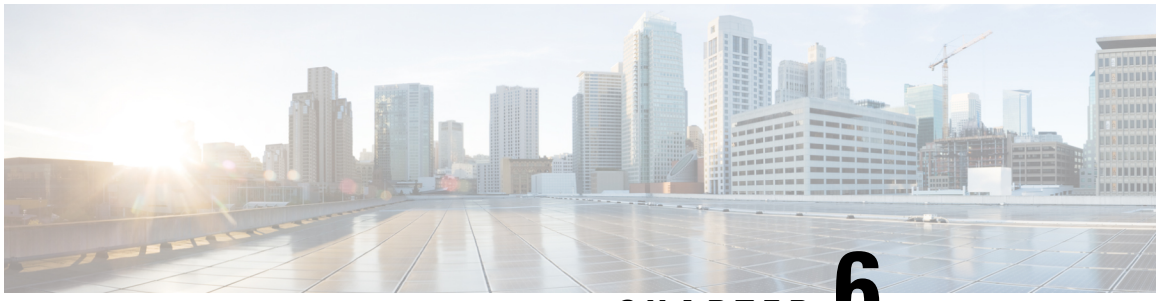
Note In Catalyst Center Release 2.3.5 and later, you can move an uplink to a newly added switch using the **Add Link** and **Delete Link** workflows.

1. Delete the existing link between the switches using the **Delete Link** option.
2. Using the **Add Link** workflow, configure a point-to-point link to the newly added switch. For more information, see Create a link between interfaces, on page 71.

40-G interface support

For Cisco IOS XE 16.11.1 and later, Cisco IOS enables the 40-G port on Cisco Catalyst 9400 Series Switches during bootup if these conditions are met.

- The switch must have its day-0, factory-default configuration. For information about how to bring a device back to its day-0 configuration, see PnP agent initial state, on page 20.
- For a single supervisor, a 10-G/1-G SFP cannot be inserted in any of the SUP ports (ports 1 to 8). A 40-G QSFP must be inserted in ports 9 or 10.
- For a dual supervisor, a 10-G/1-G SFP cannot be inserted in any of the SUP ports (ports 1 to 8). A 40-G QSFP must be inserted in port 9 only.



CHAPTER 6

Troubleshoot LAN Automation

Collect an RCA file for troubleshooting

If you encounter any problems during LAN automation, collect the root cause analysis (RCA) file. This file helps troubleshoot the issue.

Procedure

Step 1 Log in to the Catalyst Center CLI.

Step 2 Run the `$ sudo rca` command to generate the RCA file.

For a three-node cluster, collect the RCA file for each node.

What to do next

Contact Cisco TAC for further assistance.

Check session and device logs

Logs help troubleshoot LAN automation sessions by providing information about ongoing and completed activities. Reviewing session and device logs helps identify and resolve issues.

Before you begin

Use this task with Catalyst Center Release 2.3.5 and later.

Follow these steps to view session and device logs for LAN automation.

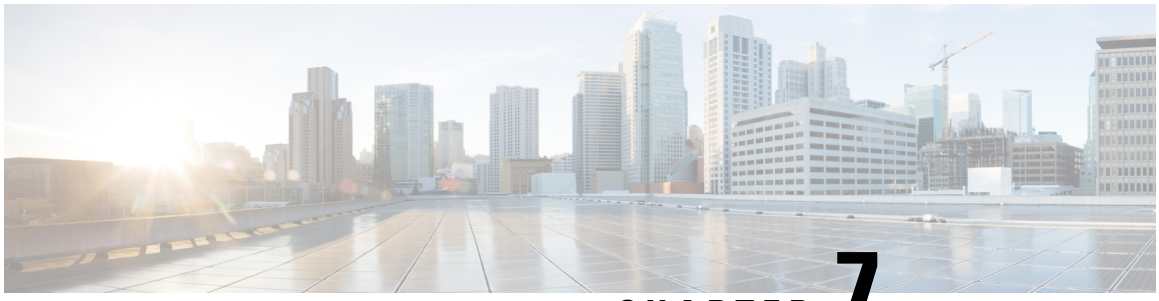
Procedure

Step 1 To view logs for an ongoing LAN automation session:

a) In the LAN automation window, under the session tile, click **See Session Details**.

b) In the session details window, click **View Session Logs**.

Step 2 To view logs for completed LAN automation sessions, refer to View device logs and configurations, on page 67.



CHAPTER 7

LAN Automation in Catalyst Center Release 2.3.5 and Later

This topic provides information on the LAN automation process based on Catalyst Center Release 2.3.5. Steps and examples may differ in later versions.

To learn more about LAN automation related features for your Catalyst Center version, refer *Cisco Catalyst Center User Guide*.

Provision LAN automation

Follow these steps to discover and provision devices using LAN automation.

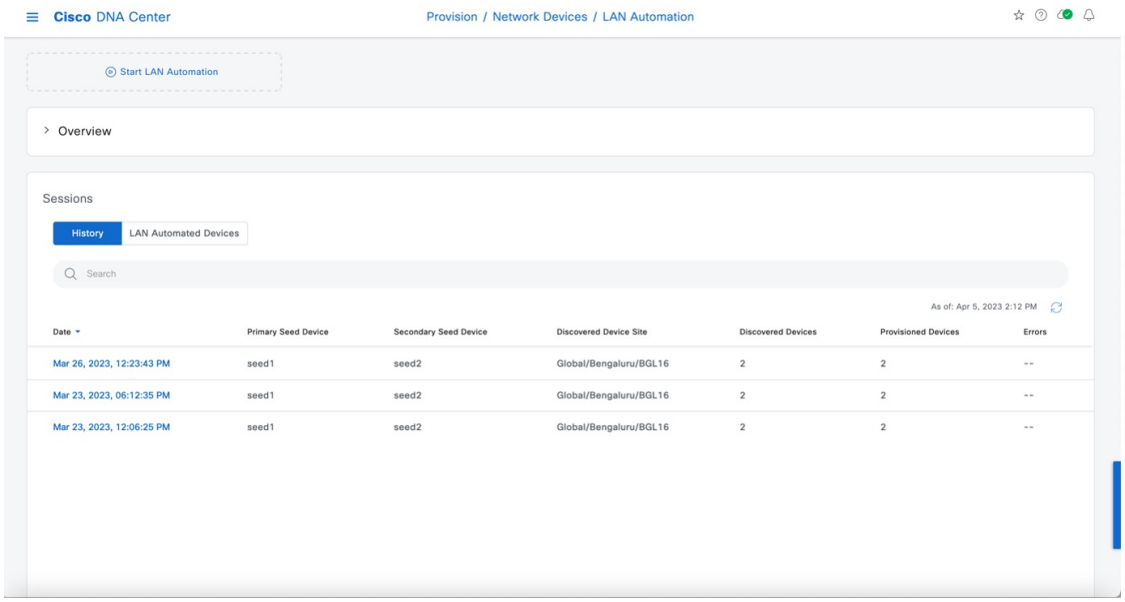
Before you begin

This topic describes the LAN automation procedure in Catalyst Center 2.3.5 and later. Steps may vary depending on your Catalyst Center version.

Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

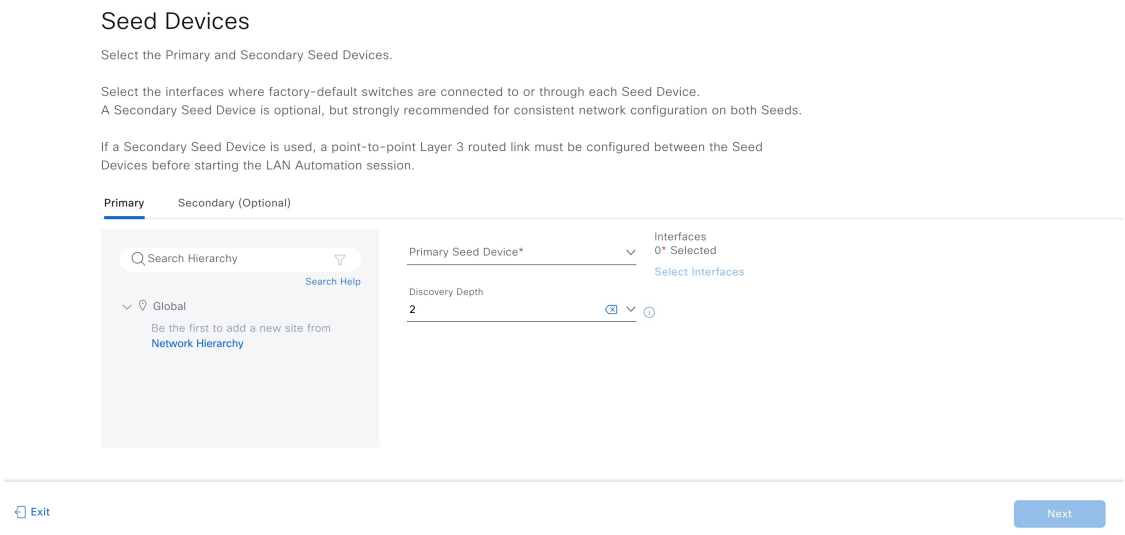
Step 2 In the **LAN Automation** window, click **Start LAN Automation**.

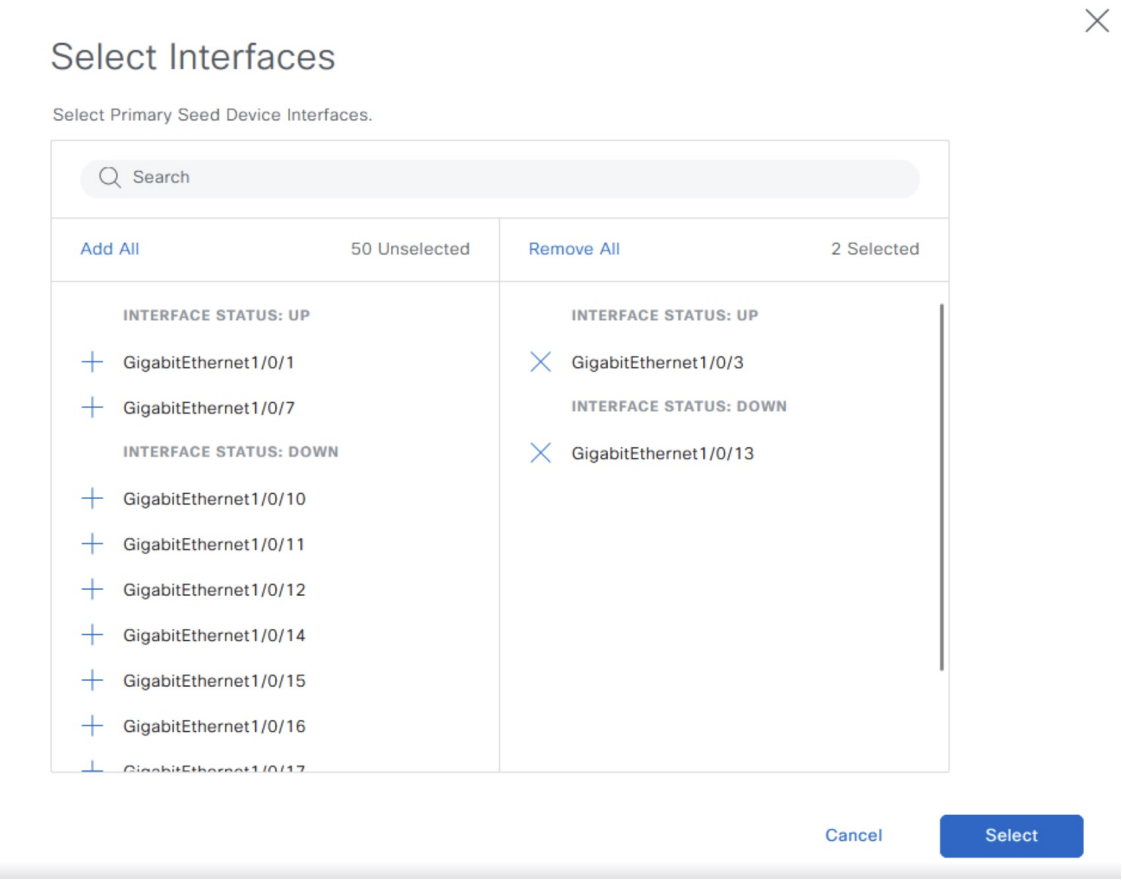


Step 3 Configure the **Seed Devices**.

- Select the **Primary Seed Device**.
- (Optional) Select the **Secondary Seed Device**.
- **Select Interfaces** on the device.

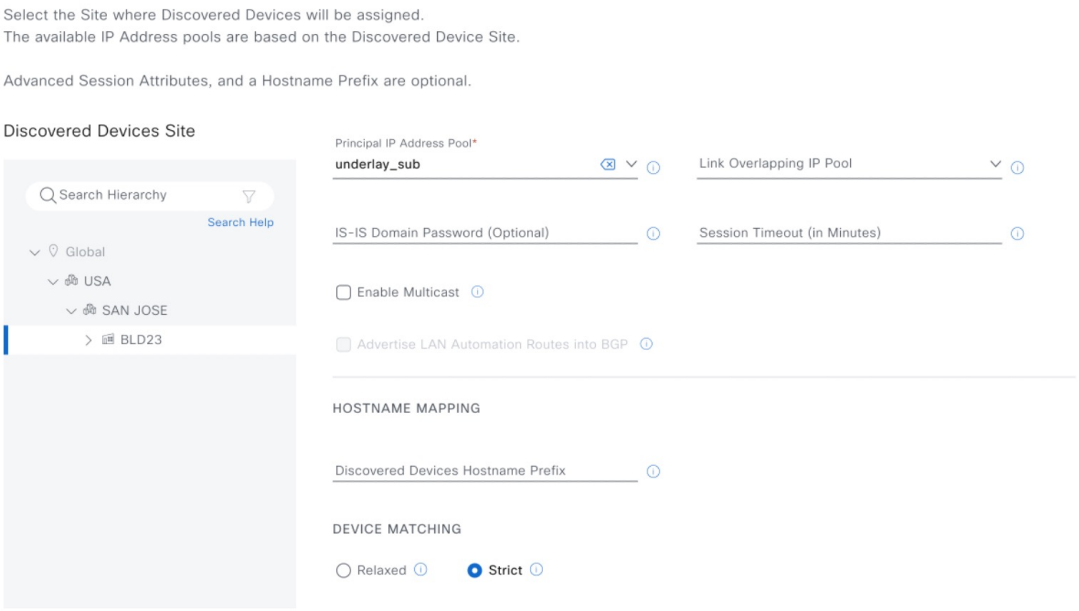
In Catalyst Center Release 2.3.7.5 and later, you can add a discovery depth level for LAN automation. Devices are LAN automated up to the specified level under the primary seed device. The default value for **Discovery Depth** is 2, and the maximum value is 5. Review the discovery depth in the summary window and see its value in the session details window after the LAN automation starts.





Step 4 In the **Session Attributes** window, select the **Principal IP Address Pool** and add the other details as required. See Configuring LAN automation attributes, on page 37 for more information.

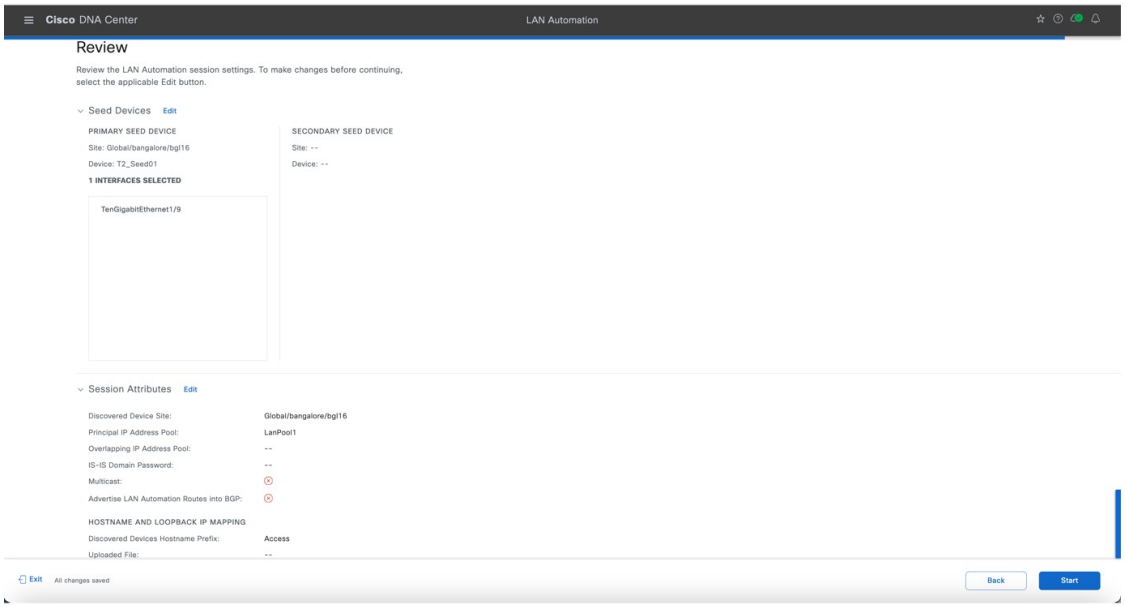
Note
In Catalyst Center Release 3.2.2 and later, for an IPv6 address pool, the **Link Overlapping IP Pool** field is not displayed. Select the **Point-to-point IPv6 Link-Local addressing** check box to enable link-local addressing for point-to-point links in the underlay.



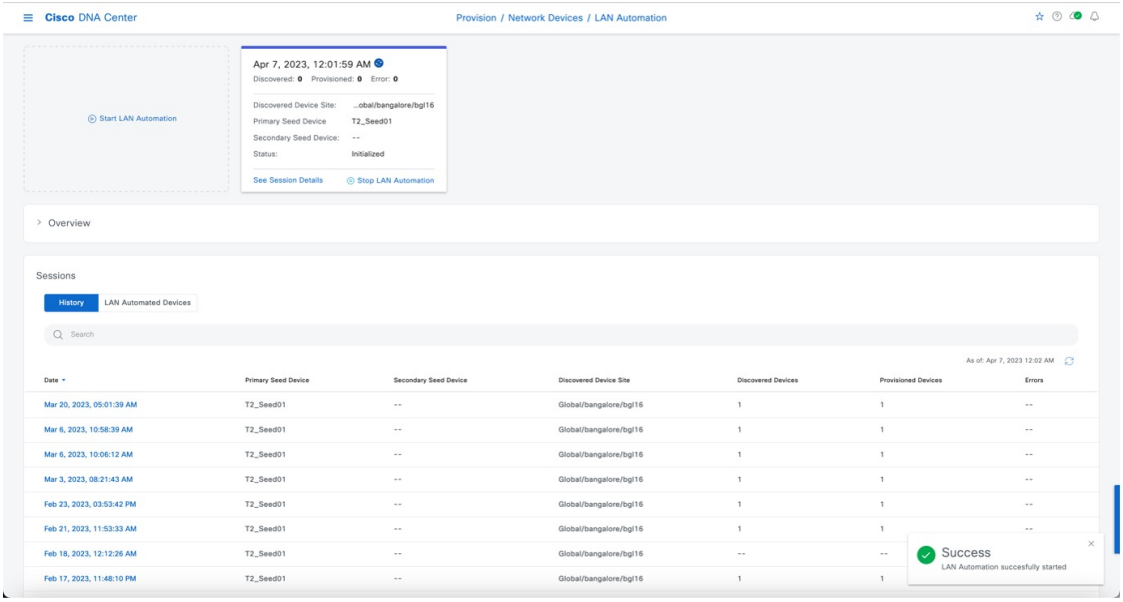
You can review the session attributes in the summary window and view them in the device details window after the LAN automation is complete.

Step 5 Click **Review**.

Step 6 After reviewing the configurations, click **Start** to begin the LAN automation.

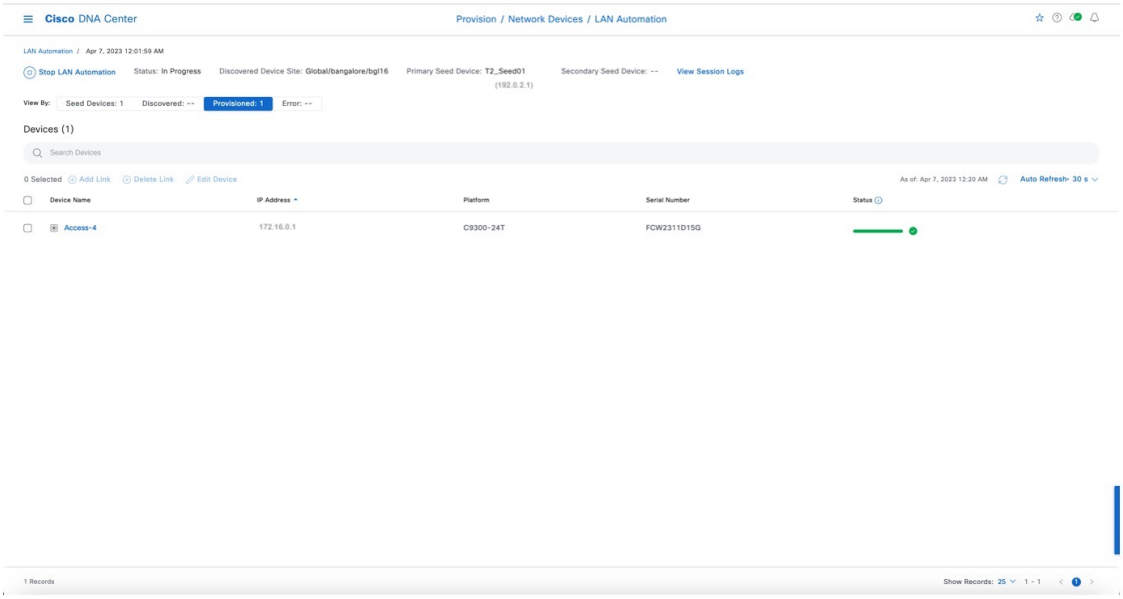


The LAN automation session is created and a tile for the session is displayed in the **LAN Automation** window.

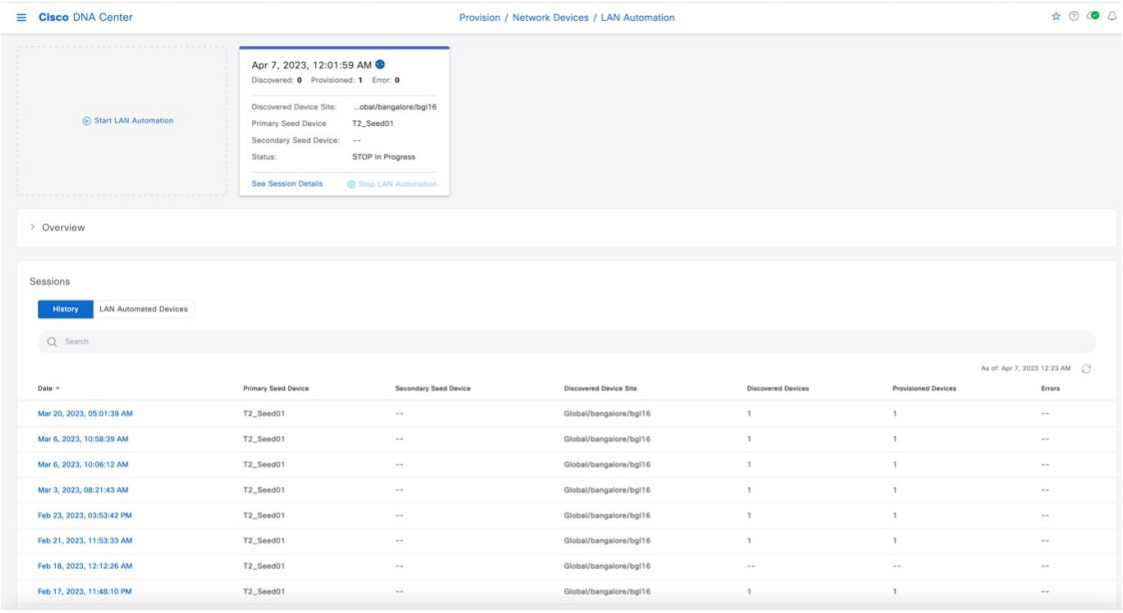


Click **See Session Details** in the tile to view session details. In the session details window, click **View Session Logs** to see session logs.

The session details window shows the status of the LAN automation session and lists the devices that are in the LAN automation process. You can filter the data and see details of the seed devices, discovered devices, provisioned devices, or the error messages. Stop the LAN automation process after all devices are provisioned and the progress bar in the **Status** column shows complete.



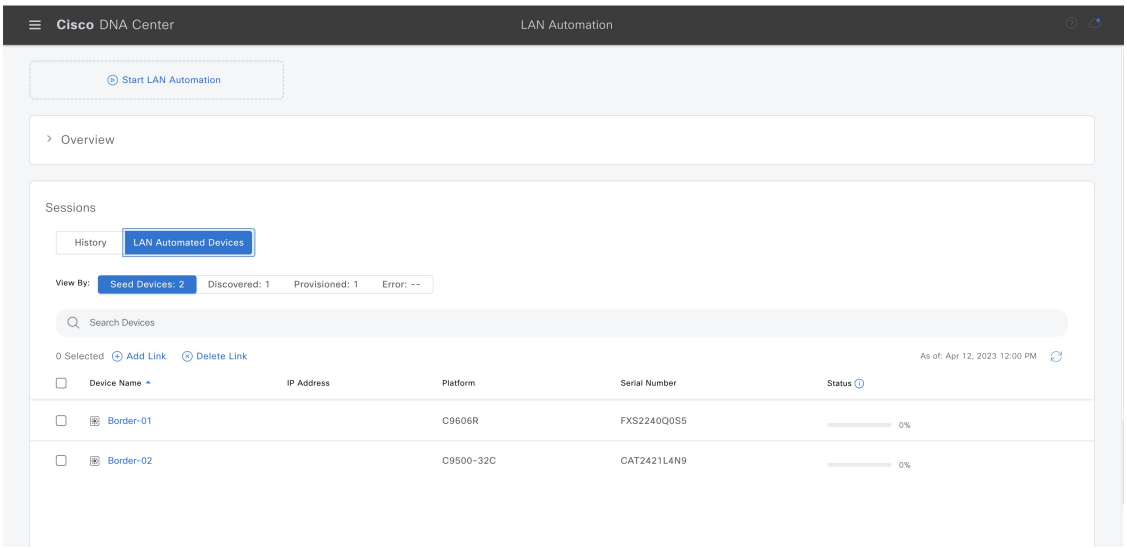
To stop LAN automation for the session, click **Stop LAN Automation** in the session details window or in the session tile. The LAN automation status changes to *STOP in Progress*.



Use the **History** tab to view LAN automation session history. Search for specific text using the search field. Click a date link to view session details.

Use the **LAN Automated Devices** tab to see details of LAN automated devices. Filter data using the search field. Click a toggle button to filter results by device status:

- **Seed Devices**: Displays the data for seed devices
- **Discovered**: Displays the data for discovered devices.
- **Provisioned**: Displays the data for provisioned devices.
- **Error**: Displays the data for devices with errors.

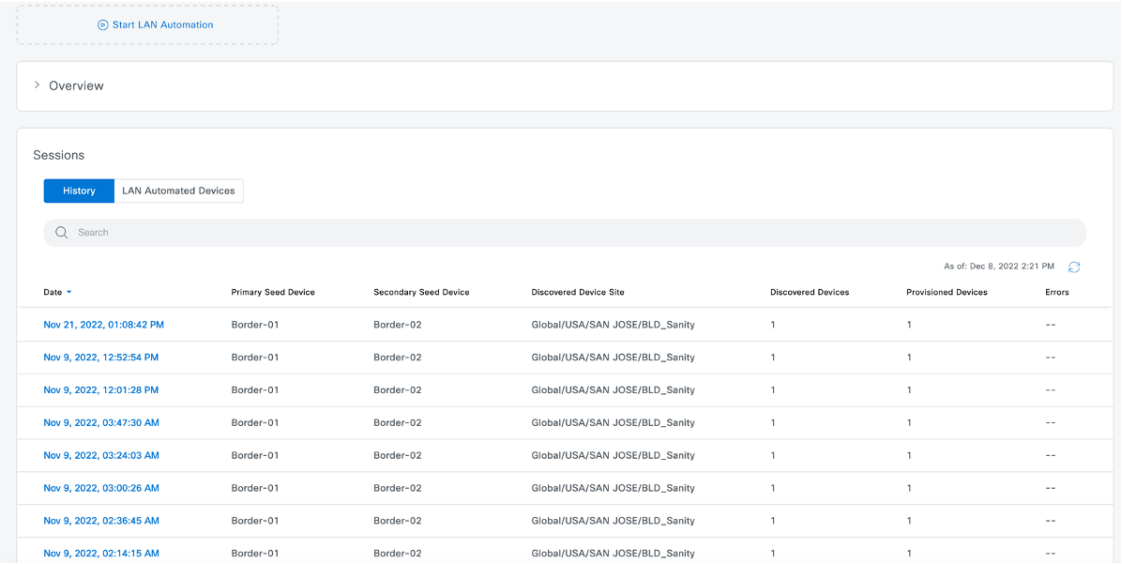


View device logs and configurations

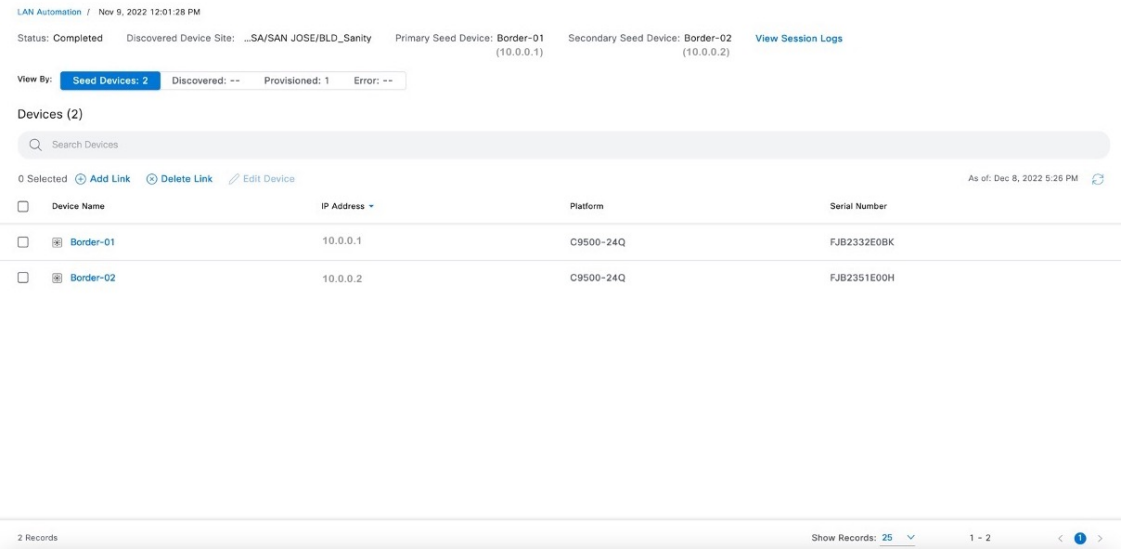
Access and review the LAN automation session logs, device-specific logs, and device configurations.

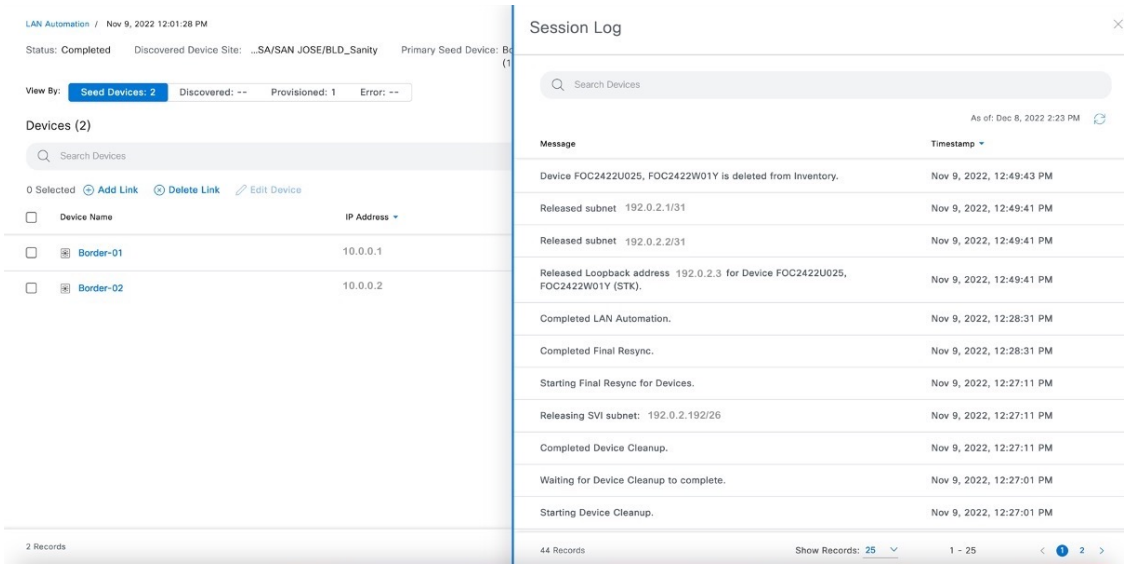
Procedure

Step 1 In the **LAN Automation** window, click the **History** tab in the **Sessions** area and click the hyperlinked date to view the session details.

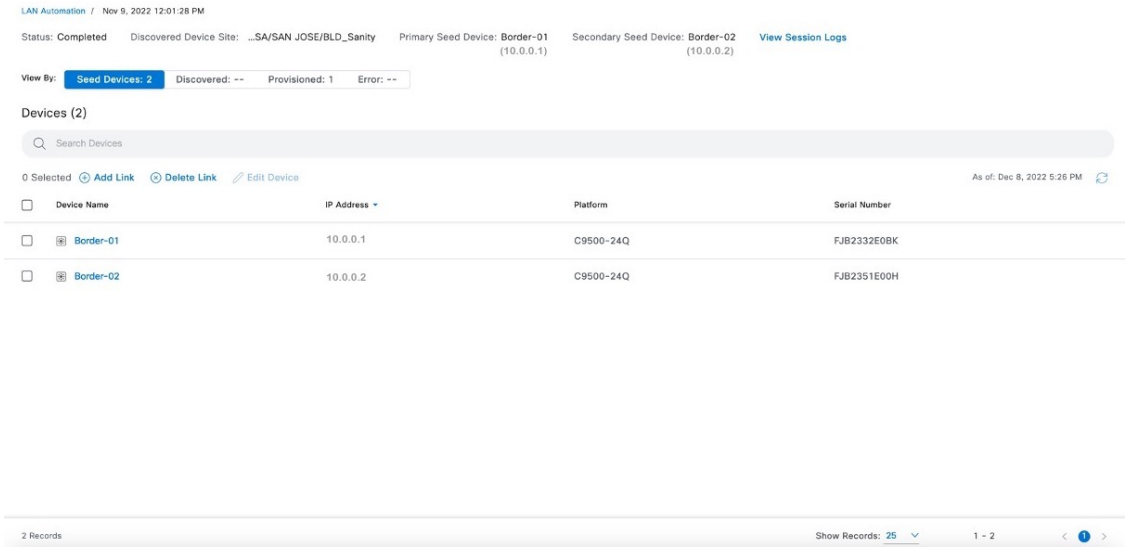


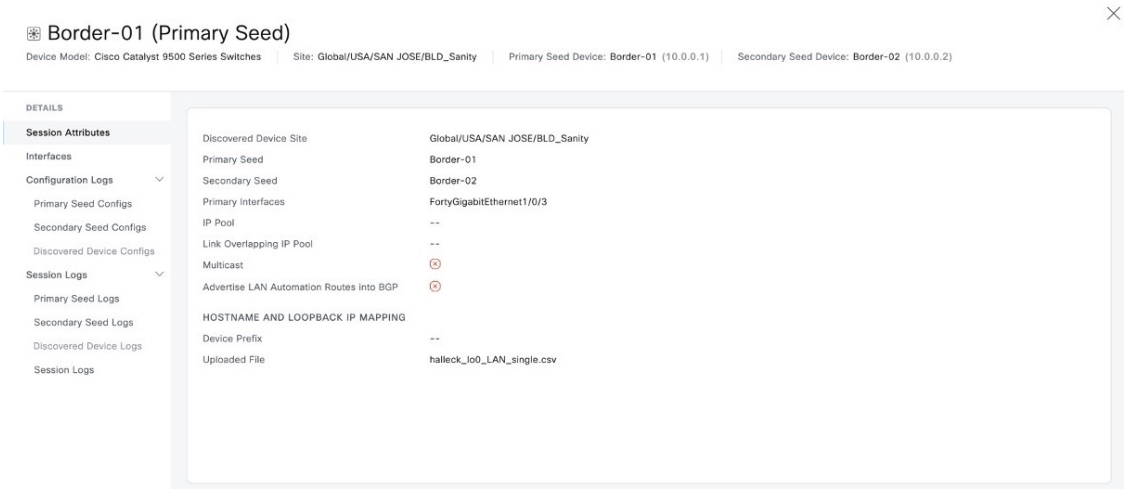
Step 2 In the session details window, click **View Session Logs**.



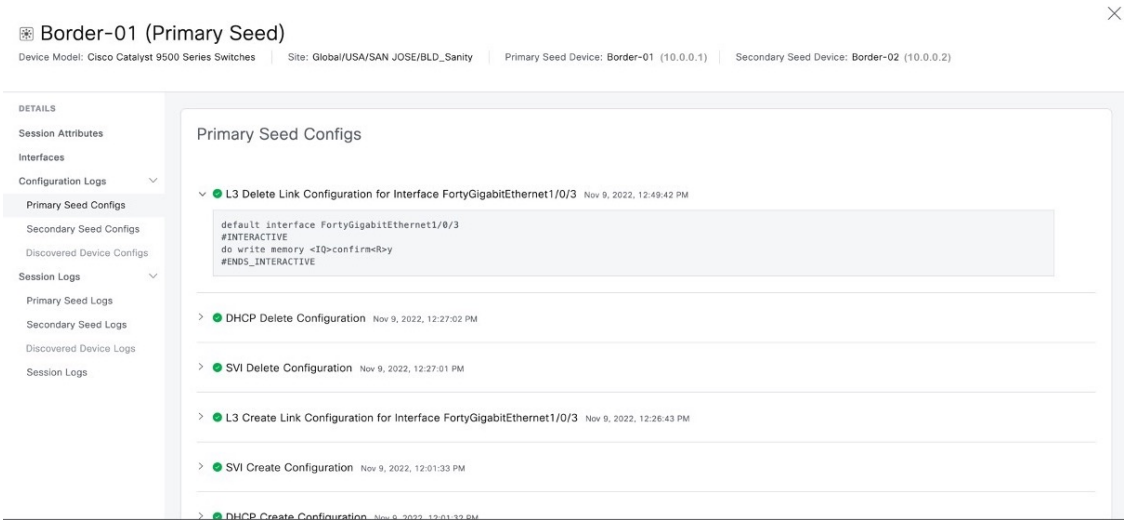


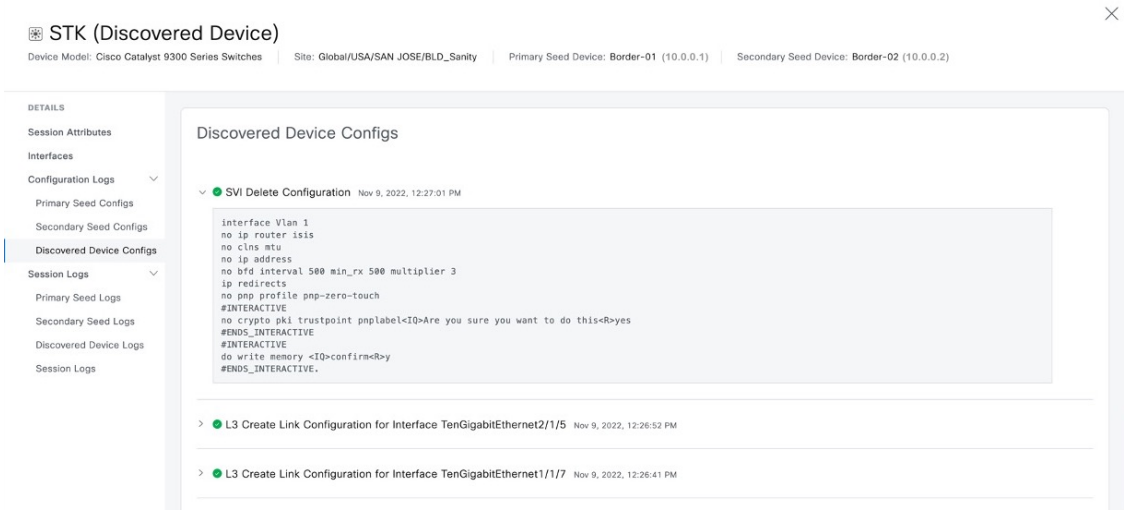
Step 3 Click the device name to view device-specific logs and configurations. Use the toggle button to filter the devices.



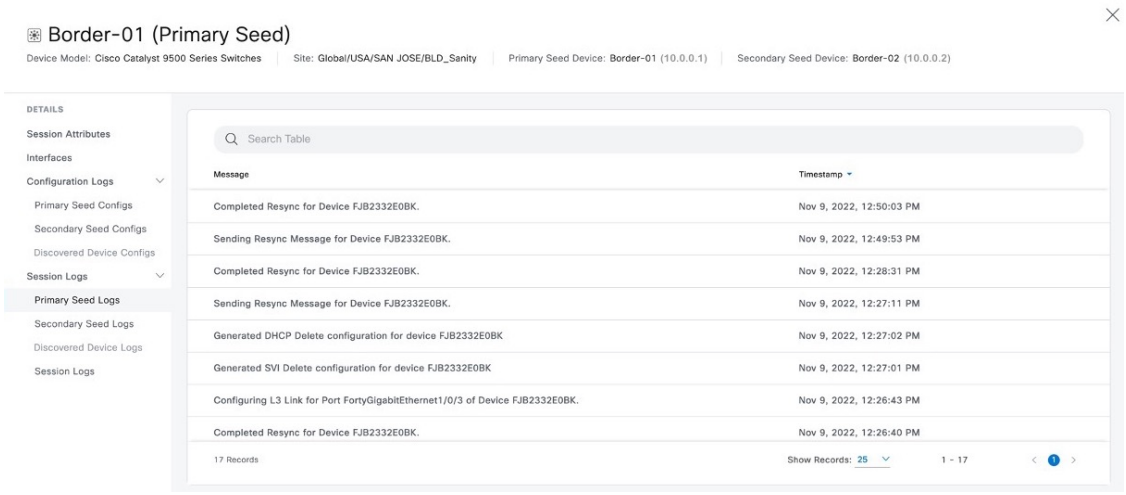


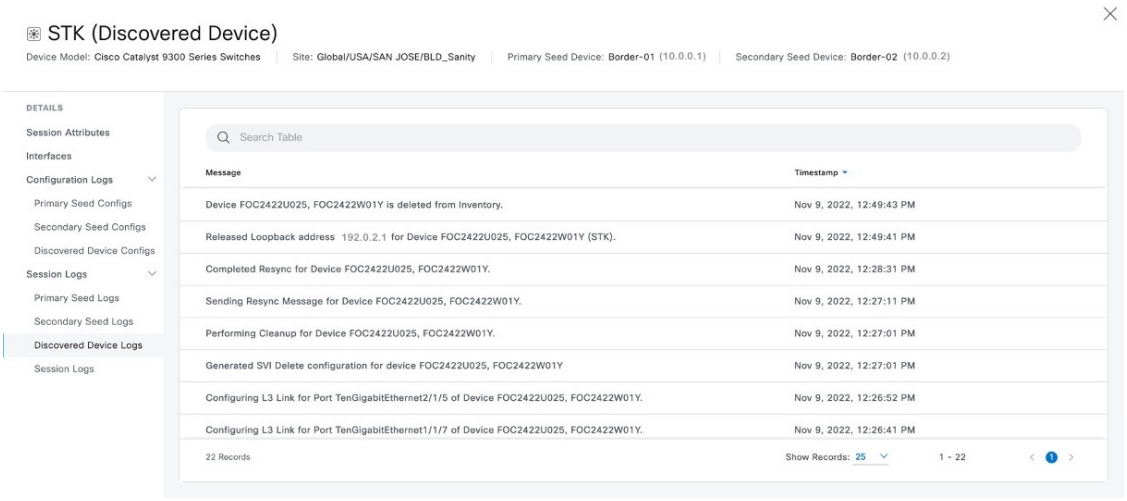
Step 4 In the left pane of the device details window, expand **Configuration Logs** to view the device configurations.





Step 5 Expand **Session Logs** to view the device-specific logs.





Create a link between interfaces

Configure additional links between interfaces after LAN automation stops.

Before you begin

This topic describes how to configure additional links between interfaces using Catalyst Center 2.3.5. Steps might differ depending on your Catalyst Center version.

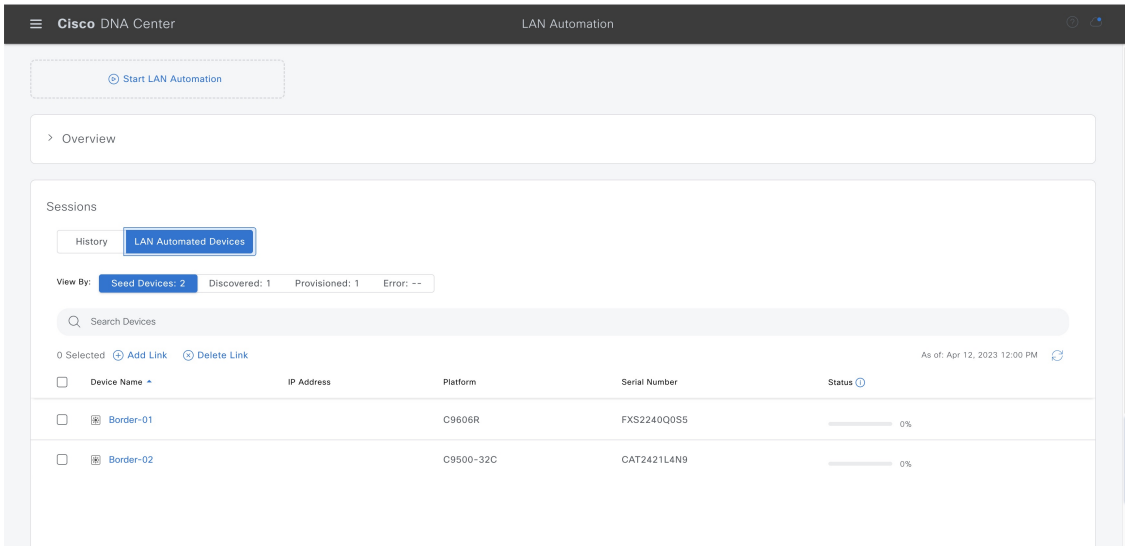
Ensure that the devices are reachable and in a managed state.

Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

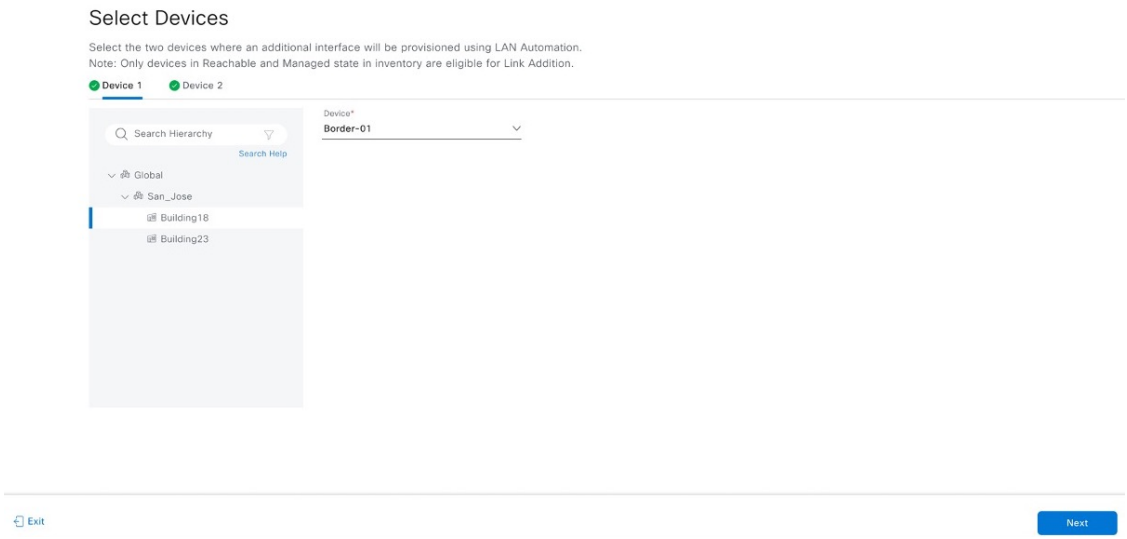
Step 2 In the **LAN Automation Devices** tab of the LAN Automation window, click **Add Link**.

Alternatively, you can check the check box next to the two devices and then click **Add Link**.

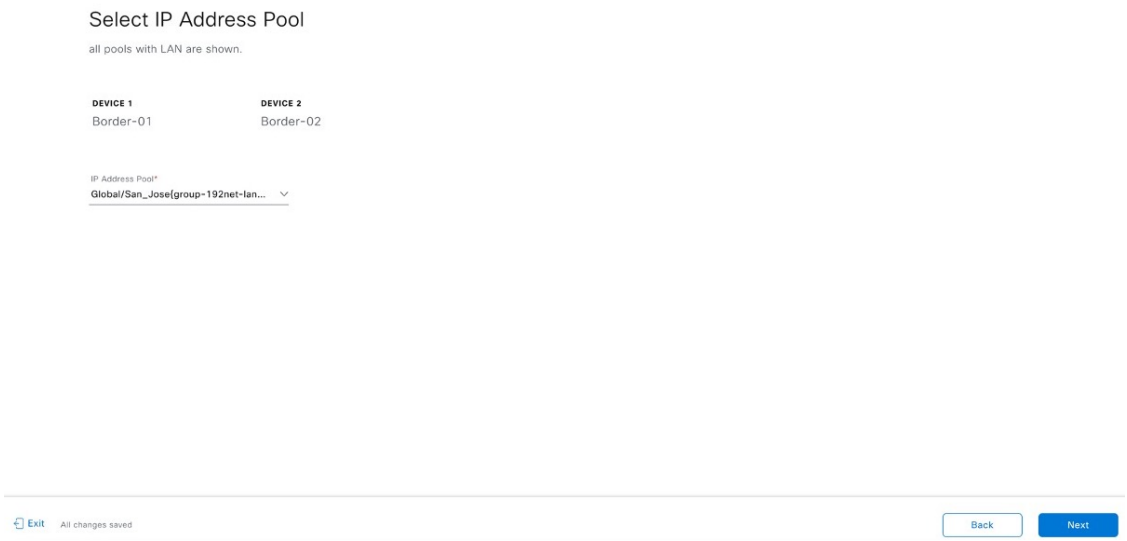


Step 3 Follow these steps in the **Add Link** workflow:

a) Select the two devices to establish the link, if you haven't already.

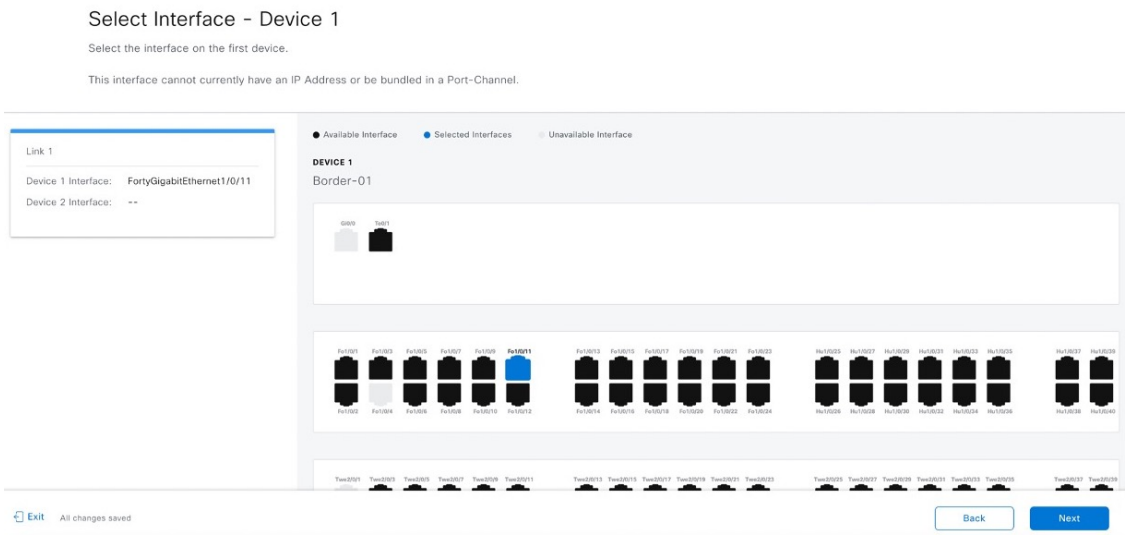


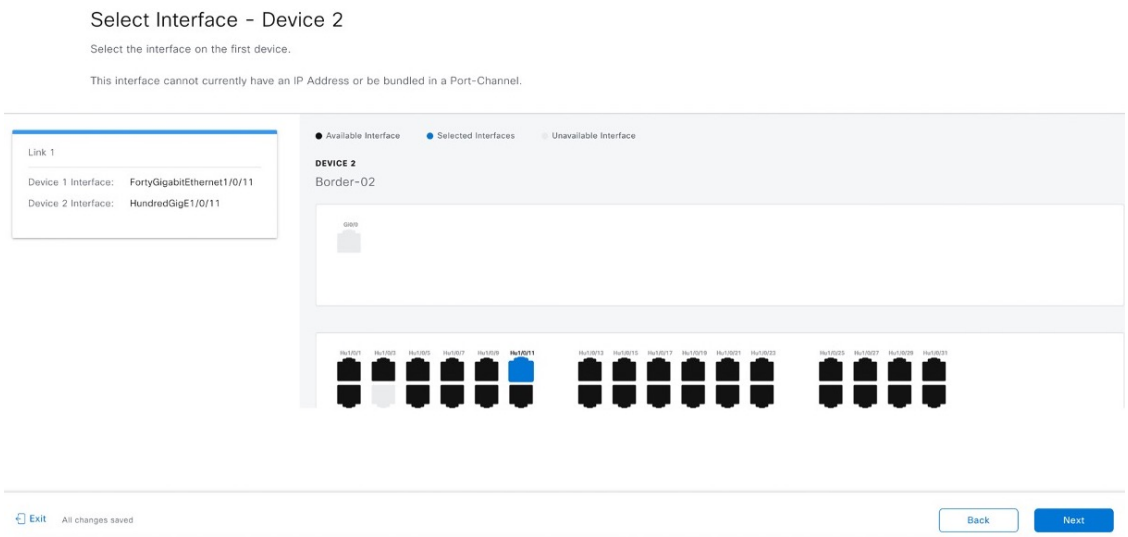
b) Select an IP address pool within the LAN. Ensure that the IP address pool is reachable from Catalyst Center.



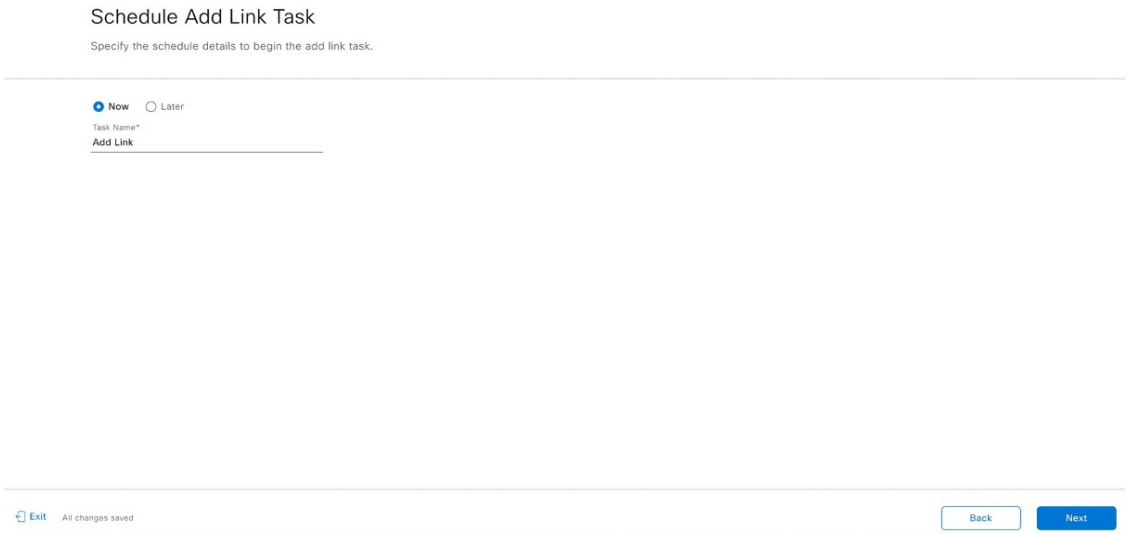
In Catalyst Center Release 3.2.2 and later, for an IPv6 address pool, you can select the **Point-to-point IPv6 Link-Local addressing** check box to configure point-to-point links using link-local addressing.

c) Select the interfaces on both devices that you want to connect.

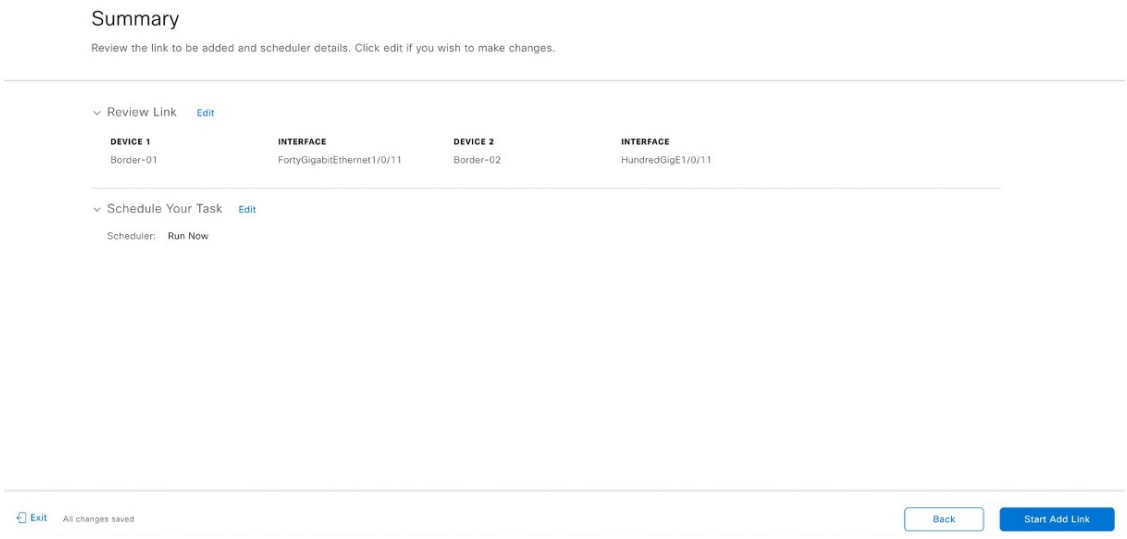




d) Click **Now** to provision the link immediately, or **Later** to schedule the provisioning. Enter a name for the task in the field provided.



e) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.



f) Click **Start Add Link**.

The **Link Configuration Started Successfully** window appears.

Step 4 You can see the status of the configuration under **Activities** > **Task**.

Delete a link between interfaces

Use this procedure to delete the interface links that were created during LAN automation or by doing an Add Link operation.

Before you begin

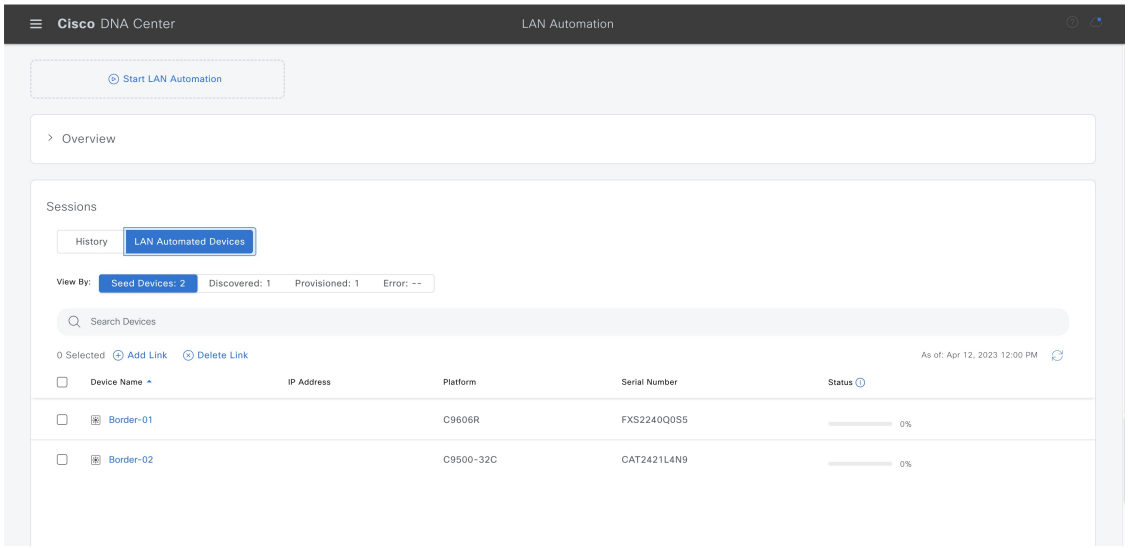
Ensure that the devices are reachable and in a managed state.

Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

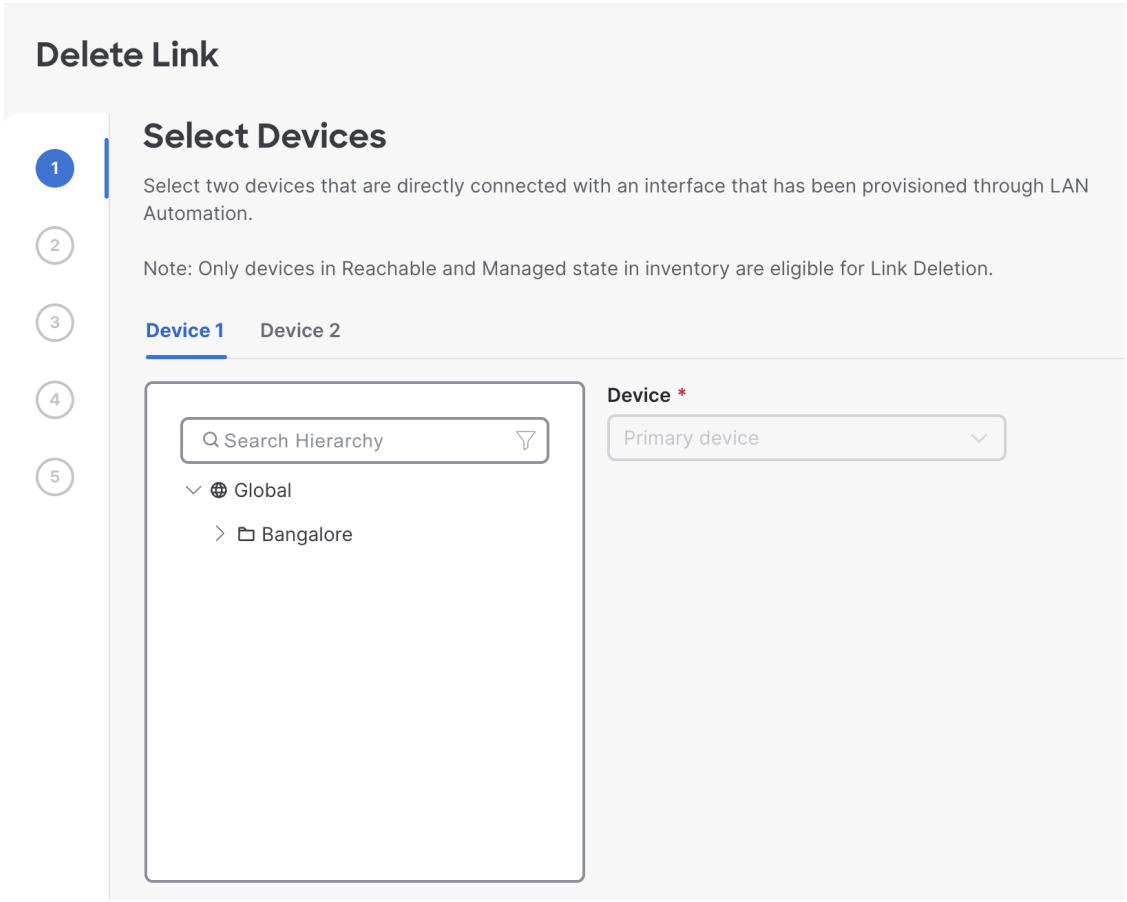
Step 2 In the **LAN Automation Devices** tab of the LAN Automation window, click **Delete Link**.

Alternatively, select the check box next to the two devices and then click **Delete Link**.



Step 3 Follow these steps in the **Delete Link** workflow:

a) Select the two devices, if you haven't already.



b) Select the interfaces on both devices.

c) Click **Now** or **Later** to indicate when you want to start the delete process. Enter a name for the task in the field provided.
d) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.
e) Click **Start Delete Link**.

Step 4 You can see the status of the configuration under **Activities** > **Task**.

Edit LAN automated devices

Use this procedure to edit the hostname and Loopback0 interface IP address of a LAN automated device in Catalyst Center Release 2.3.7.5 and later.

Before you begin

Reserve LAN IP pools and discover the devices through LAN automation.

Note

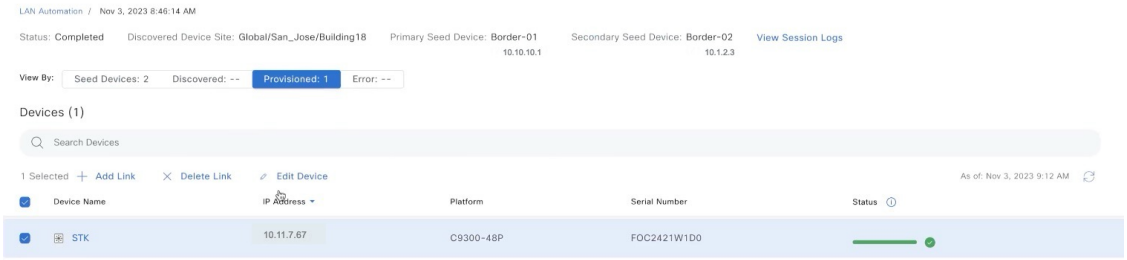
- In a Day-*1* scenario, ensure that the devices you want to edit are in a **Managed** state in the Catalyst Center inventory.
- You can edit the Loopback0 interface IP address for up to 25 devices in a single Day-*1* workflow.

Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

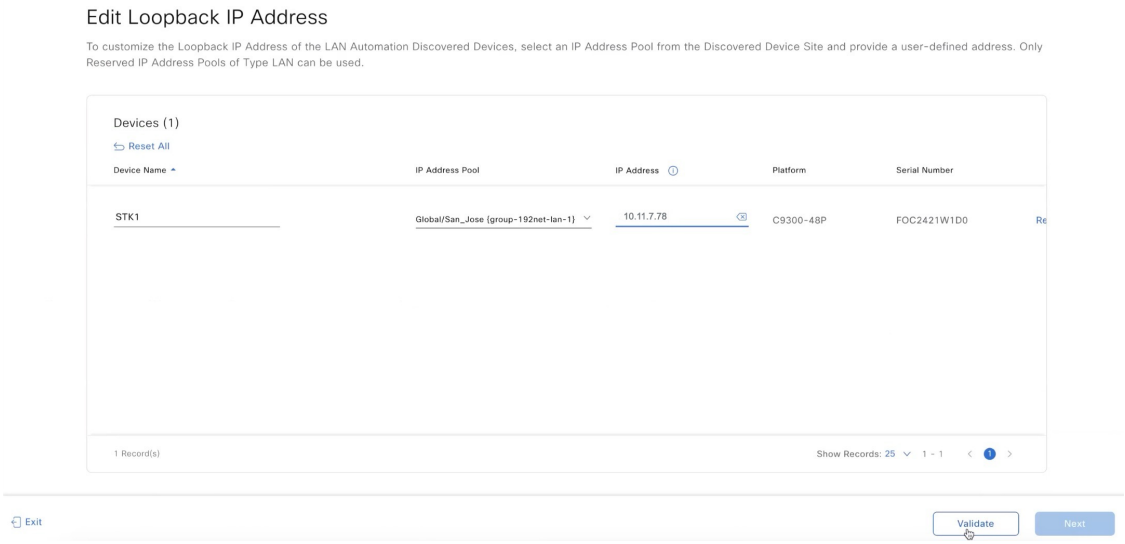
Step 2 In the **LAN Automation** window, click the **LAN Automated Devices** tab.

Step 3 Check the check box next to the device that you want to edit and click **Edit Device**.

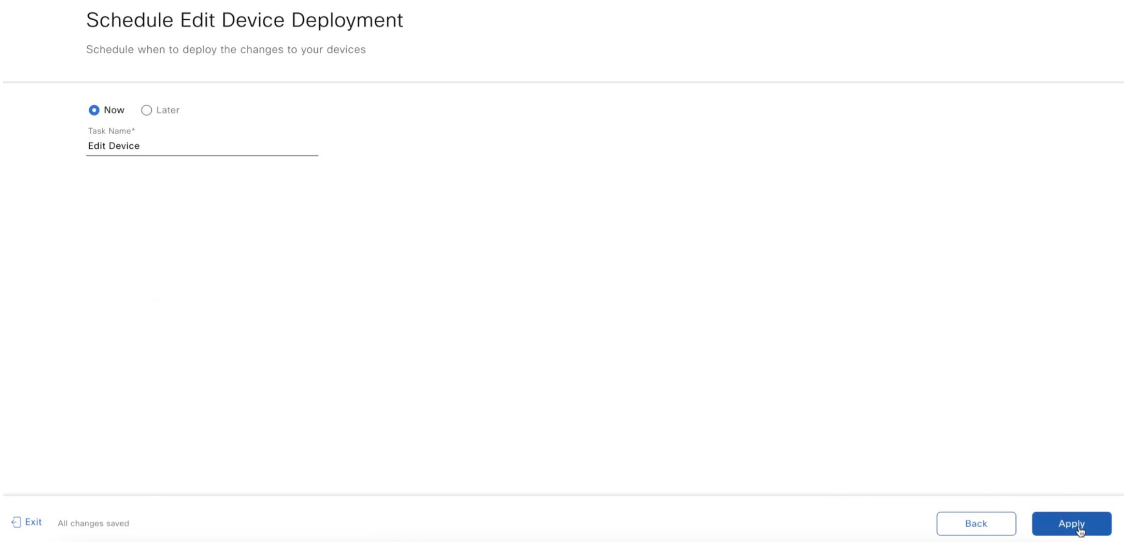


Step 4 In the **Edit Devices** window, edit the **Device Name**, **IP Address Pool**, and **IP Address** fields, as required.

Enter the IP address without a subnet mask. Ensure that the IP address is within the range of the selected IP address pool. Click **Validate** to validate the IP address allocation.

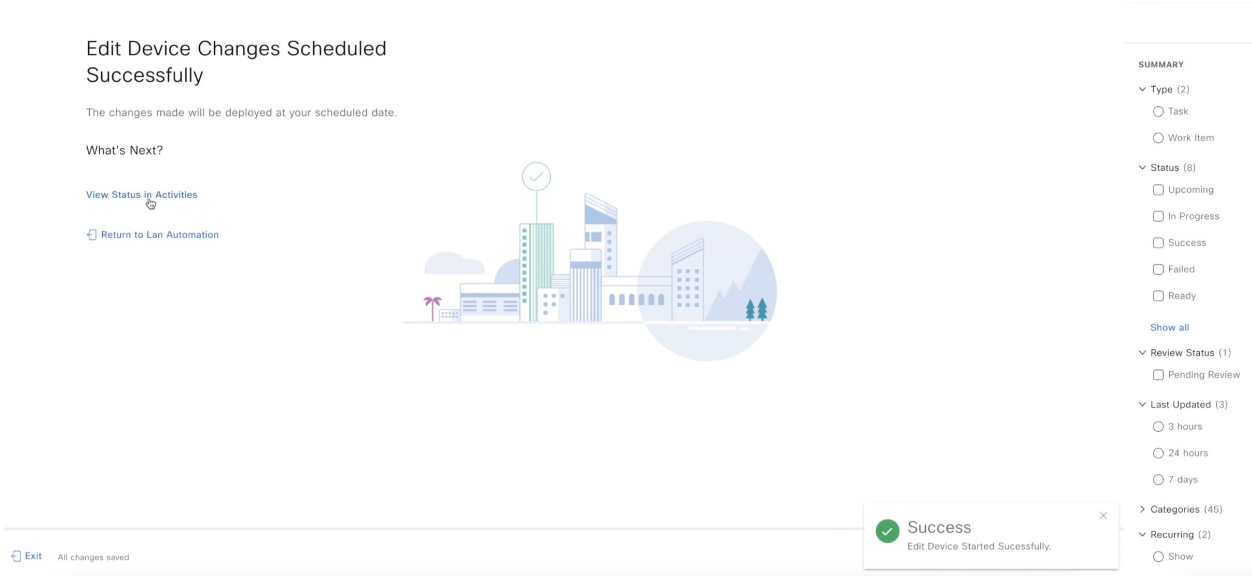


Step 5 Schedule the device deployment.



What to do next

You can view the status of the edit task under the **Activities** > **Task** window.



Manage devices in strict discovery mode

With Catalyst Center Release 2.3.7.5 and later, you can choose either **Relaxed** mode or **Strict** mode for device matching during discovery. **Strict** mode limits device discovery to a defined list. Follow these steps to add, edit, or delete devices in the discovery list.

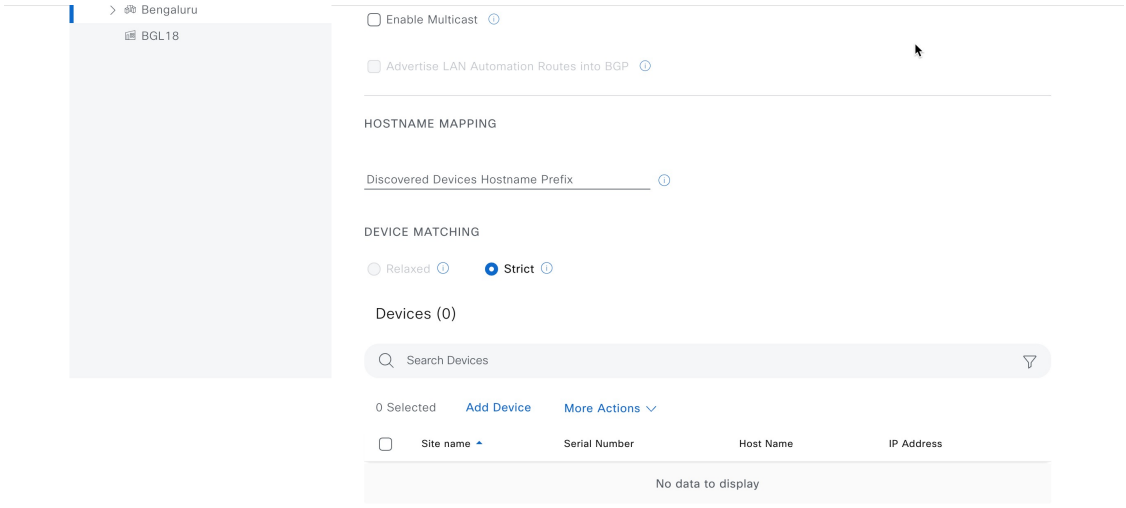
Procedure

Step 1 In the **LAN Automation** window, click **Start LAN Automation**.

Step 2 Add the seed devices and click **Next**.

Step 3 In the **Session Attributes** window, in the left pane, select a building or a floor.

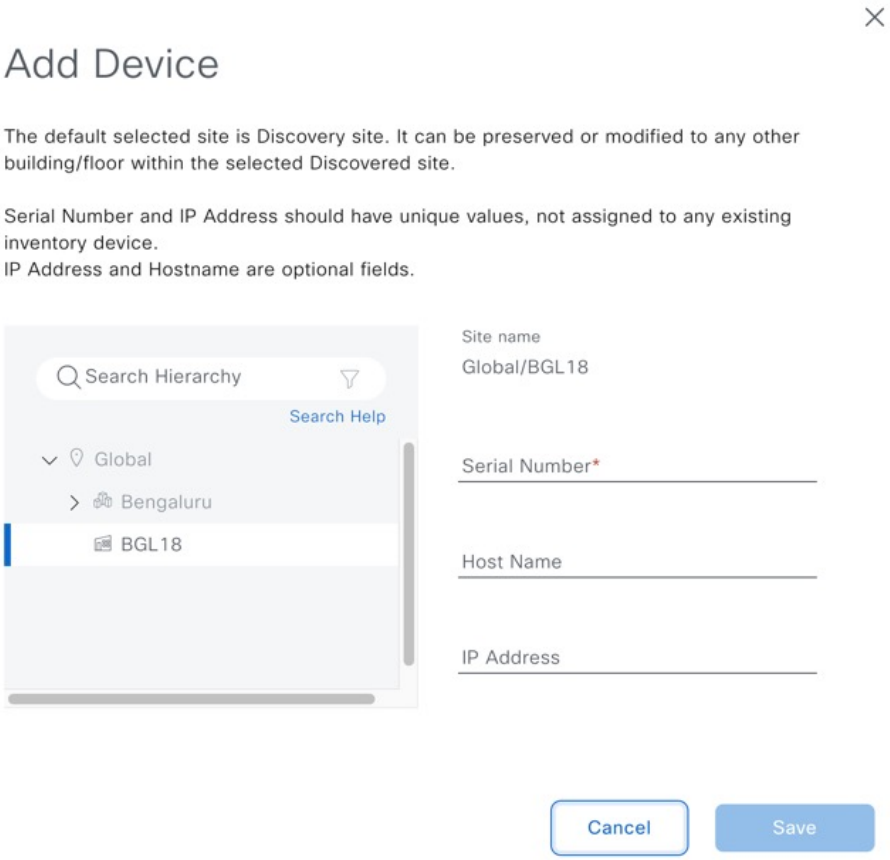
Step 4 Under **Device Matching**, select the **Strict** option.



Note
If you select an area as the site, you must add a device list. In this case, the **Strict** mode is chosen automatically, and the **Relaxed** mode is disabled.

Step 5 Add devices using one of these options for your discovery list:

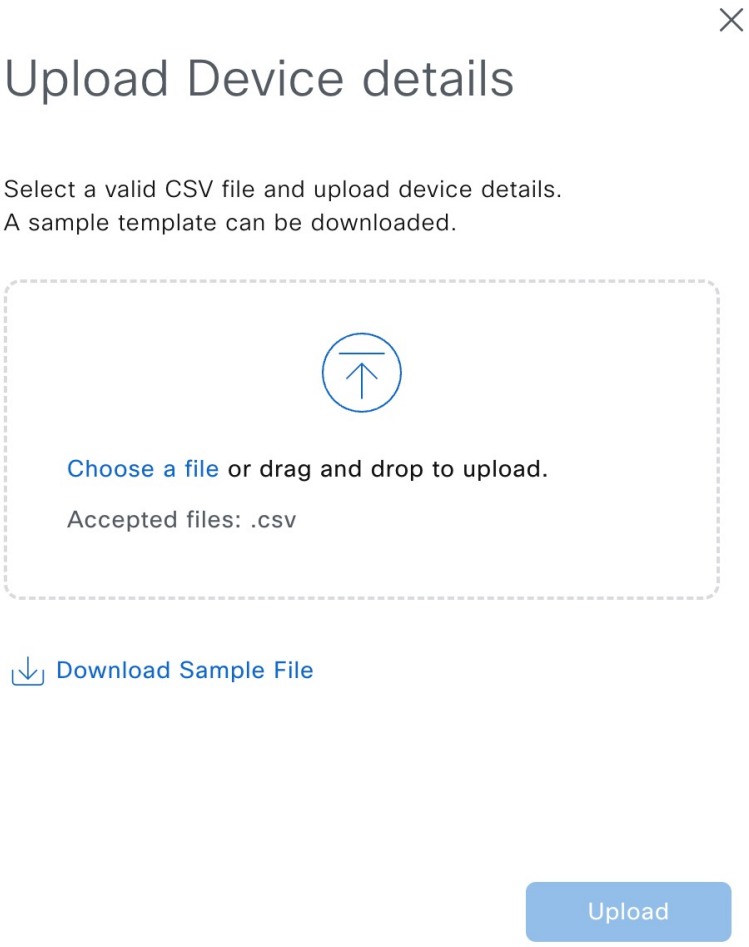
- **Add Device**: Use this option to add a single device.
  - In the **Devices** table, click **Add Device** and follow these steps:
    a. If you've chosen an area, select a building or a floor as the site.
    b. Enter a **Serial Number** for the device.
    c. (Optional) Enter the **Host Name** and **IP Address** for your device.
    d. Click **Save**.



- **Upload Device**: Use this option to add devices from a CSV file.
  a. In the **Devices** table, click **More Actions** and choose the option to upload the device CSV file.
  b. Upload the CSV file.

     Drag and drop the CSV file into the boxed area or click **Choose a file** and browse to the CSV file.

     You can also download a sample template.



Step 6 Follow these steps to edit a device from the discovery list:

a) Check the check box next to the device that you want to edit and choose **More Actions** > **Edit Device**.

b) Edit the device details as needed

You can edit only one device at a time.

c) Click **Save**.

Step 7 Follow these steps to delete a device from the discovery list:

a) Check the check box next to the device that you want to delete and choose **More Actions** > **Delete Device**.

You can select multiple devices to delete.

b) Click the **Delete** icon and confirm the delete action.

Manage port channels

Note Port channels are not supported for IPv6 deployments.

Create port channel

Use this procedure to create a port channel between two devices that are discovered through LAN automation.

Before you begin

Ensure that the devices are reachable and in a managed state.

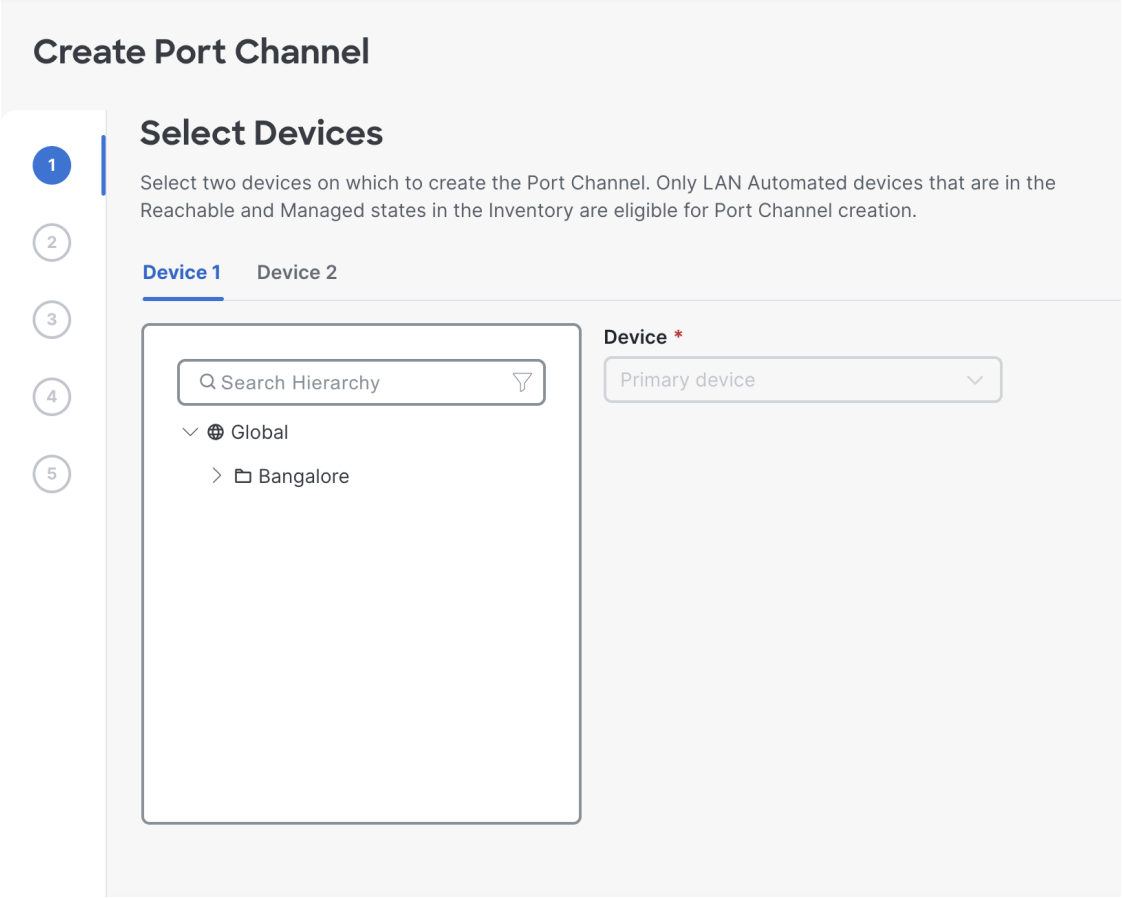
Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

Step 2 In the **LAN Automation Devices** tab, select **More Actions** > **Create Port Channel**.

Alternatively, select the check box next to the two devices on which you want to create a port channel, and then select **More Actions** > **Create Port Channel**.

Step 3 Select the two devices to create the port channel, if you haven't already.



Step 4 Select the interfaces for the port channel.

Step 5 Click **Now** or **Later** to schedule the process. Enter a name for the task in the field provided.

Step 6 In the **Summary** window, review the configuration settings (to make any changes, click **Edit**) and create the port channel.

Step 7 You can see the status of the configuration under **Activities** > **Task**.

What to do next

You can add links to the port channel. See Add links to port channel, on page 84.

Add links to port channel

Use this procedure to configure additional links to an existing port channel between two devices.

Before you begin

Ensure that the devices are reachable and in a managed state and there is an existing port channel between the devices.

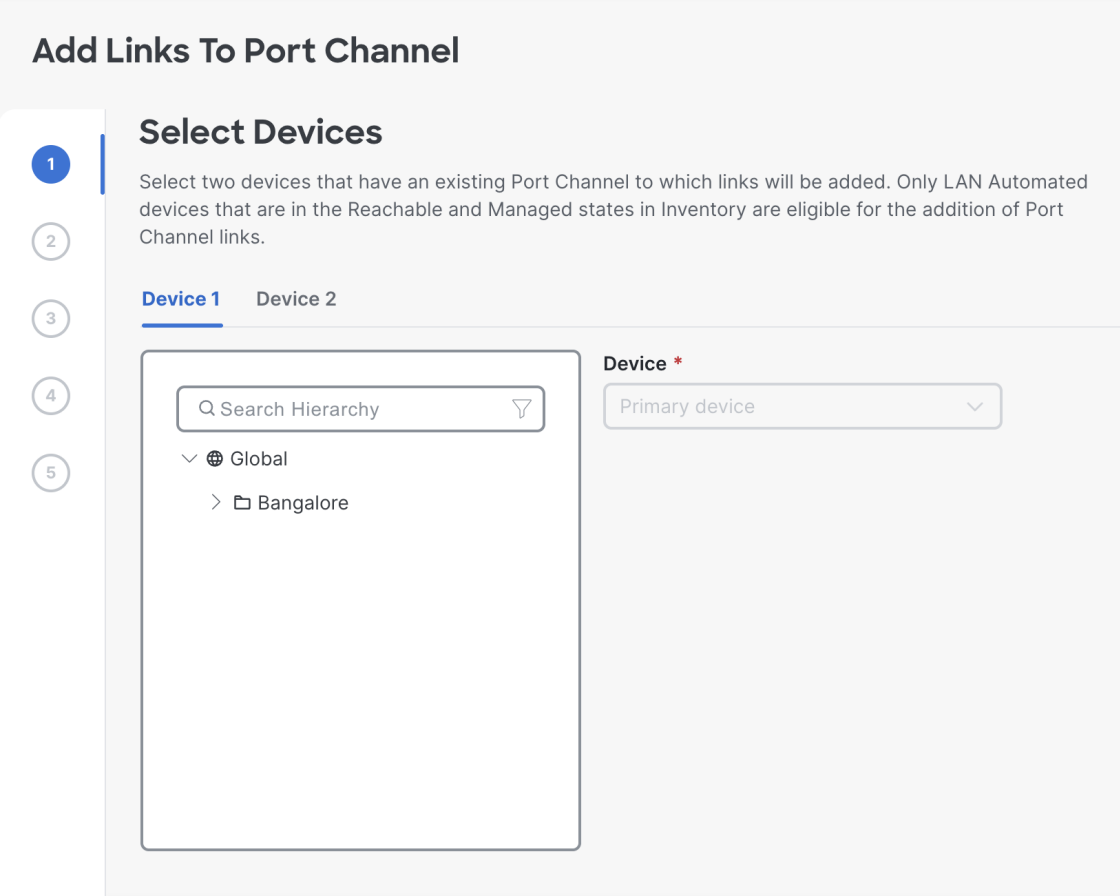
Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

Step 2 In the **LAN Automation Devices** tab, select **More Actions** > **Add Links to Port Channel**.

Alternatively, select the check box next to the two devices on which you want to add links to the port channel, and then select **More Actions** > **Add Links to Port Channel**.

Step 3 Select the two devices where you want to add links to the port channel, if you haven't already.



Step 4 Select the interfaces that you want add to the port channel.

Step 5 Click **Now** or **Later** to schedule the process. Enter a name for the task in the field provided.

Step 6 In the **Summary** window, review the configuration settings (to make any changes, click **Edit**) and configure the port channel.

Step 7 You can see the status of the configuration under **Activities** > **Task**.

Delete links from port channel

Use this procedure to delete links from an existing port channel between two devices.

Before you begin

Ensure that the devices are reachable and in a managed state and there is an existing port channel between the devices.

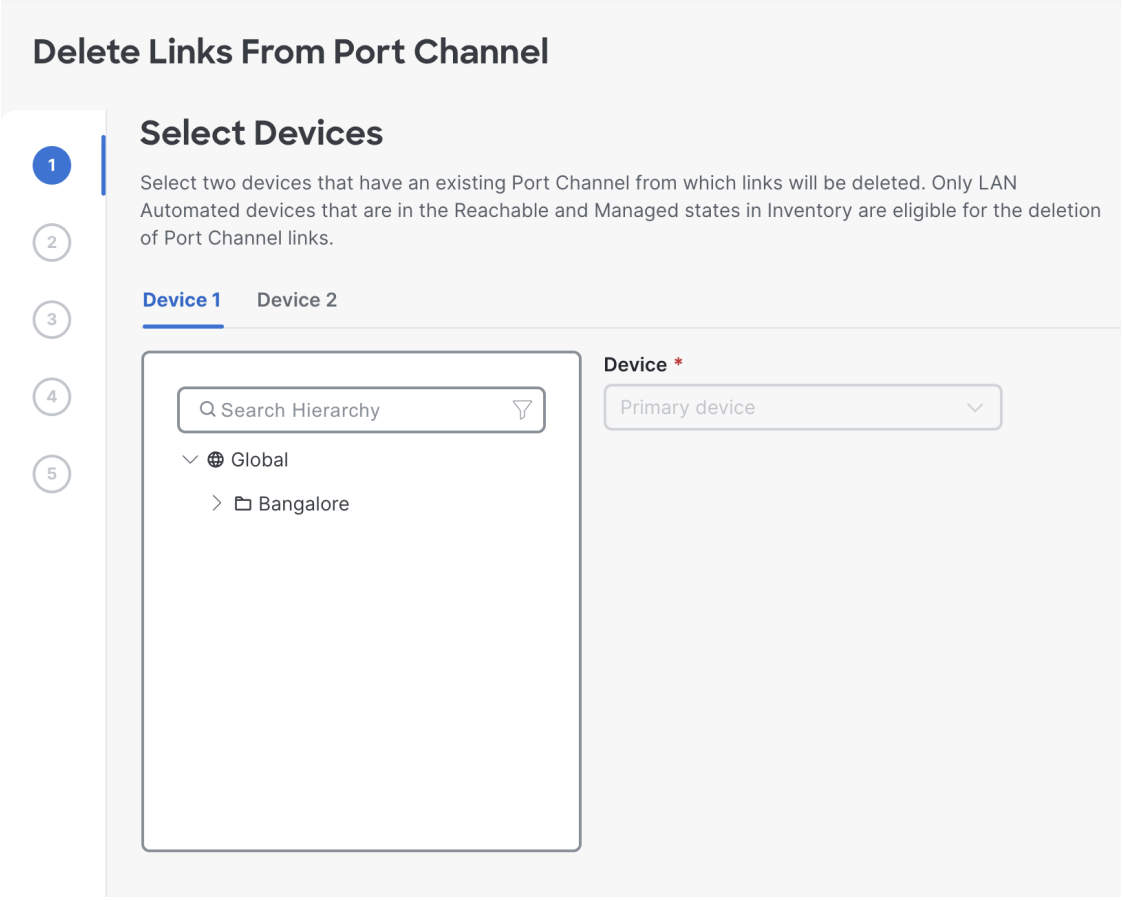
Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

Step 2 In the **LAN Automation Devices** tab, select **More Actions** > **Delete Links From Port Channel**.

Alternatively, select the check box next to the two devices on which you want to delete links from the port channel, and then select **More Actions** > **Delete Links From Port Channel**.

Step 3 Select the two devices where you want to delete the links from the port channel, if you haven't already.



Step 4 Select the interfaces that you want delete from the port channel.

Step 5 Click **Now** or **Later** to schedule the process. Enter a name for the task in the field provided.

Step 6 In the **Summary** window, review the configuration settings (to make any changes, click **Edit**) and configure the port channel.

Step 7 You can see the status of the configuration under **Activities** > **Task**.

Delete a port channel

Before you begin

Ensure that the devices are reachable and in a managed state.

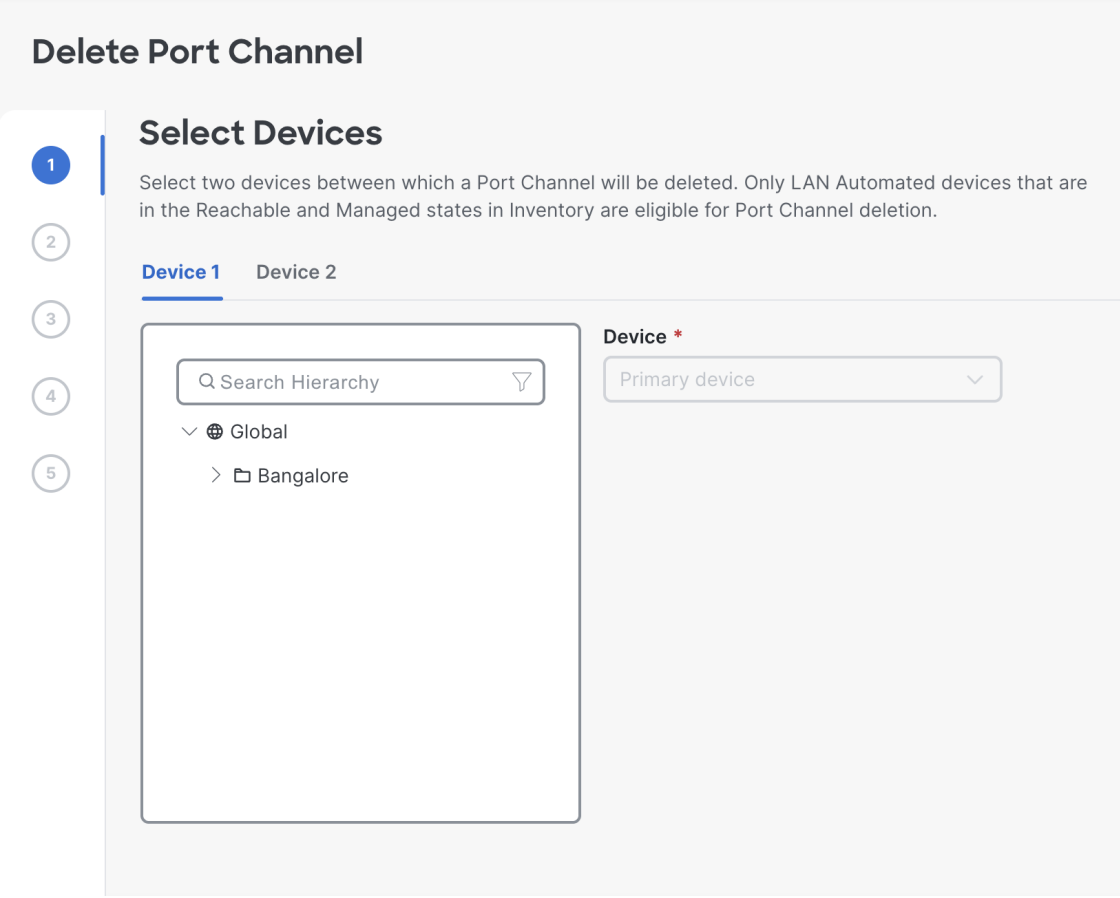
Procedure

Step 1 From the main menu, choose **Provision** > **LAN Automation**.

Step 2 In the **LAN Automation Devices** tab, select **More Actions** > **Delete Port Channel**.

Alternatively, select the check box next to the two devices on which you want to delete the port channel, and then select **More Actions** > **Delete Port Channel**.

Step 3 Select the two devices to delete the port channel, if you haven't already.



Step 4 Delete the port channel.

Step 5 Click **Now** or **Later** to schedule the process. Enter a name for the task in the field provided.

Step 6 In the **Summary** window, review the configuration settings (to make any changes, click **Edit**) and delete the port channel.

Step 7 You can see the status of the configuration under **Activities** > **Task**.