Configure the Appliance Using the Maglev Wizard

- Appliance Configuration Overview, on page 1
- Configure the Primary Node Using the Maglev Wizard, on page 1
- Configure a Secondary Node Using the Maglev Wizard, on page 23
- Upgrade to the Latest Cisco DNA Center Release, on page 42

Appliance Configuration Overview

You can deploy the appliance in your network in one of the following two modes:

- Standalone: As a single node offering all the functions. This option is usually preferred for initial or test deployments and in smaller network environments. If you choose Standalone mode for your initial deployment, you can add more appliances later to form a cluster. When configuring the standalone host, ensure that it is set it up as the first, or primary, node in the cluster.
- Cluster: As a node that belongs to a three-node cluster. In this mode, all the services and data are shared among the hosts. This is the preferred option for large deployments. If you choose Cluster mode for your initial deployment, be sure to finish configuring the primary node before configuring the secondary nodes.

To proceed, complete the following tasks:

1. Configure the primary node in your cluster. See Configure the Primary Node Using the Maglev Wizard, on page 1.
2. If you have installed three appliances and want to add the second and third nodes to your cluster, see Configure a Secondary Node Using the Maglev Wizard, on page 23.

Configure the Primary Node Using the Maglev Wizard

Perform the steps in this procedure to configure the first installed appliance as the primary node. You must always configure the first appliance as the primary node, whether it will operate standalone or as part of a cluster.

If you are configuring the installed appliance as a secondary node for an existing cluster that already has a primary node, follow the steps described in Configure a Secondary Node Using the Maglev Wizard, on page 23 instead.

Important

- Ensure that all of the IP addresses you enter while completing this procedure are valid IPv4 addresses with valid IPv4 netmasks. Also make sure that the addresses and their corresponding subnets do not overlap. Service communication issues can result if they do.
- Before you configure the appliances in a three-node cluster, ensure that you have logged out of those appliances. Otherwise, the Quick Start workflow (which you complete to discover your network's devices and enable telemetry) will not start after you have configured your cluster's appliances and log in to Cisco DNA Center for the first time.

Before you begin

Ensure that you:

- Collected all of the information specified in Required IP Addresses and Subnets and Required Configuration Information.
- Installed the first appliance, as described in Appliance Installation Workflow.
- Configured Cisco IMC browser access on the primary node, as described in Enable Browser Access to Cisco Integrated Management Controller.
- Checked that the primary node appliance's ports, and the switches they use, are properly configured, as described in Execute Preconfiguration Checks.
- Confirmed that you are using a compatible browser. For a list of compatible browsers, see the Release Notes document for the release of Cisco DNA Center you are installing.
- Enabled ICMP on the firewall between Cisco DNA Center and both the default gateway and the DNS server you specify in the following procedure. The Maglev Configuration wizard uses ping to verify the gateway and DNS server you specify. This ping might get blocked if a firewall is in place and ICMP is not enabled on that firewall. When this happens, you will not be able to complete the wizard.

Step 1 Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, and log in to the Cisco IMC GUI as the Cisco IMC user (see Enable Browser Access to Cisco Integrated Management Controller).

After successful login, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window, with a hyperlinked menu at the top of the window, as shown below.

Step 2 From the hyperlinked menu, choose **Launch KVM** and then choose either **Java-based KVM** or **HTML-based KVM**. If you choose **Java-based KVM**, you will need to launch the Java startup file from your browser or file manager in order to view the KVM console in its own window. If you choose **HTML-based KVM**, it launches the KVM console in a separate window or tab automatically.

Irrespective of the KVM type you choose, use the KVM console to monitor the progress of the configuration and respond to the Maglev Configuration wizard prompts.

Step 3 With the KVM displayed, reboot the appliance by making one of the following selections:

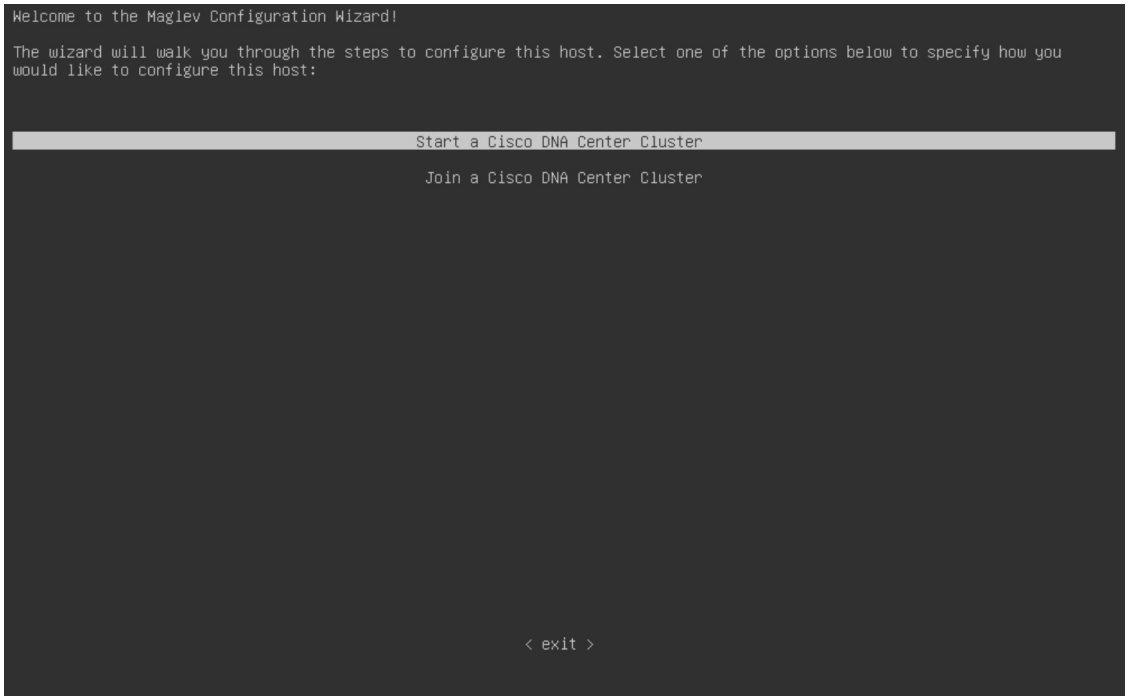
- In the main Cisco IMC GUI browser window: Choose **Host Power** > **Power Cycle**, and switch to the KVM console to continue.
- In the KVM console: Choose **Power** > **Power Cycle System (cold boot)**.

If you are asked to confirm your choice to reboot the appliance, click **OK**.

After displaying reboot messages, the KVM console displays the **Static IP Configuration** screen.

Step 4 Click **Skip**.

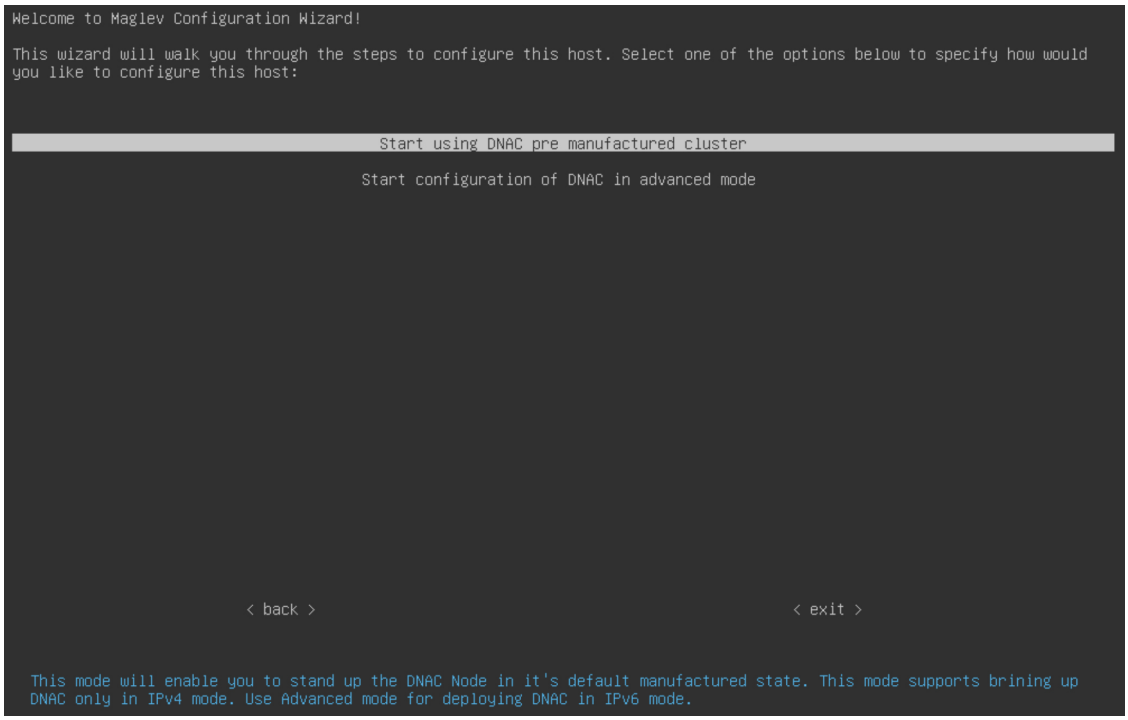
The KVM console displays the Maglev Configuration wizard welcome screen.



Note Only users that want to configure their appliance using one of the browser-based wizards without using the IP address, subnet mask, and default gateway assigned to the appliance's Enterprise interface by a DHCP server need to complete this screen.

Step 5 Click **Start a Cisco DNA Center Cluster** to begin configuring the primary node.

The screen updates.



Step 6 Choose one of the following options:

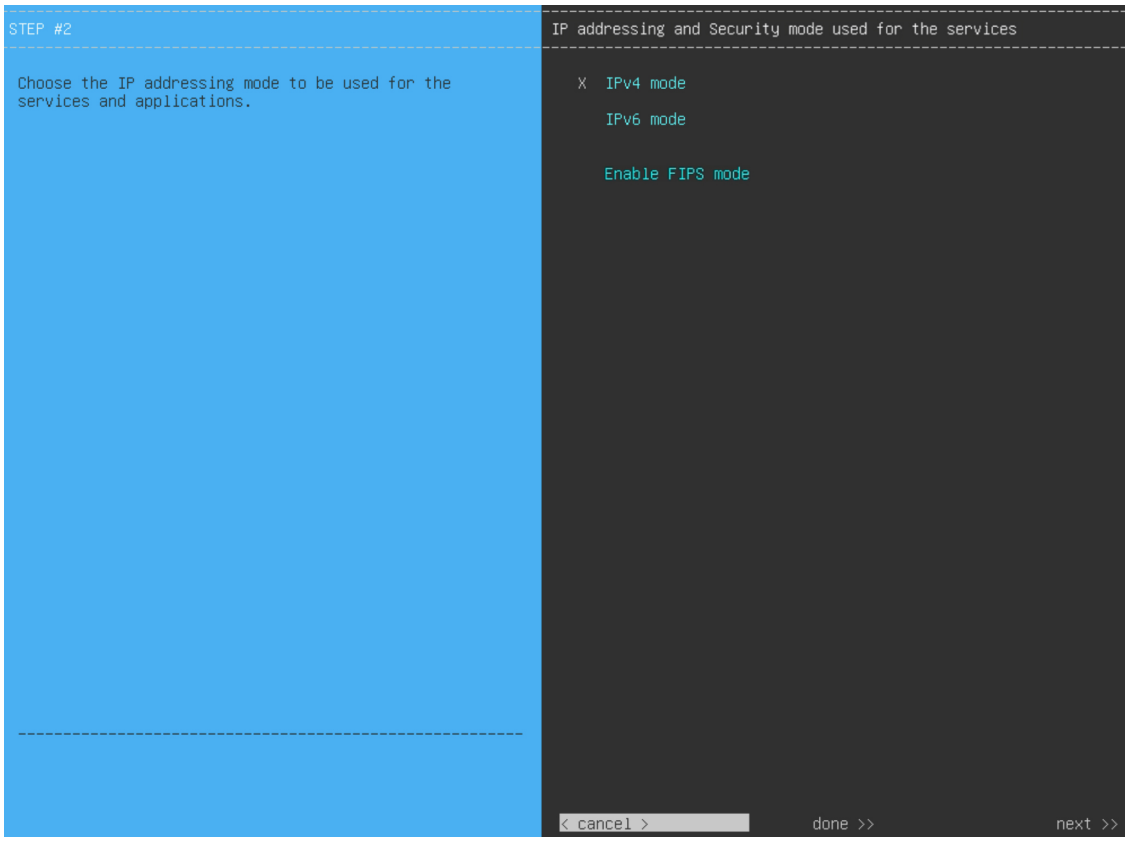
- **Start using DNAC pre manufactured cluster**: Choose this option to configure an appliance with its default settings in place:
  - Intracluster interface IP address: **169.254.6.66**
  - Intracluster interface subnet mask: **255.255.255.128**
  - Container subnet: **169.254.32.0/20**
  - Cluster subnet: **169.254.48.0/20**
  - IPv4 addressing
  - Admin superuser's password: **maglev1@3**

  You will *not* be able to change any of these settings, so choose this option only if you want to use them.

  Important This option is only available if you are configuring a new Cisco DNA Center appliance. If you are reimaging your appliance, the wizard proceeds with the **Start configuration of DNAC in advanced mode** option selected.

- **Start configuration of DNAC in advanced mode**: Choose this option to configure an appliance that doesn't use one or more of the default settings listed in the previous bullet. Also choose this option if you want to use IPv6 addressing on your appliance.

The screen updates.



Step 7 Do the following, then click **next>>** to proceed:

a) Specify whether the applications and services running on your Cisco DNA Center appliance will use IPv4 or IPv6 addressing.

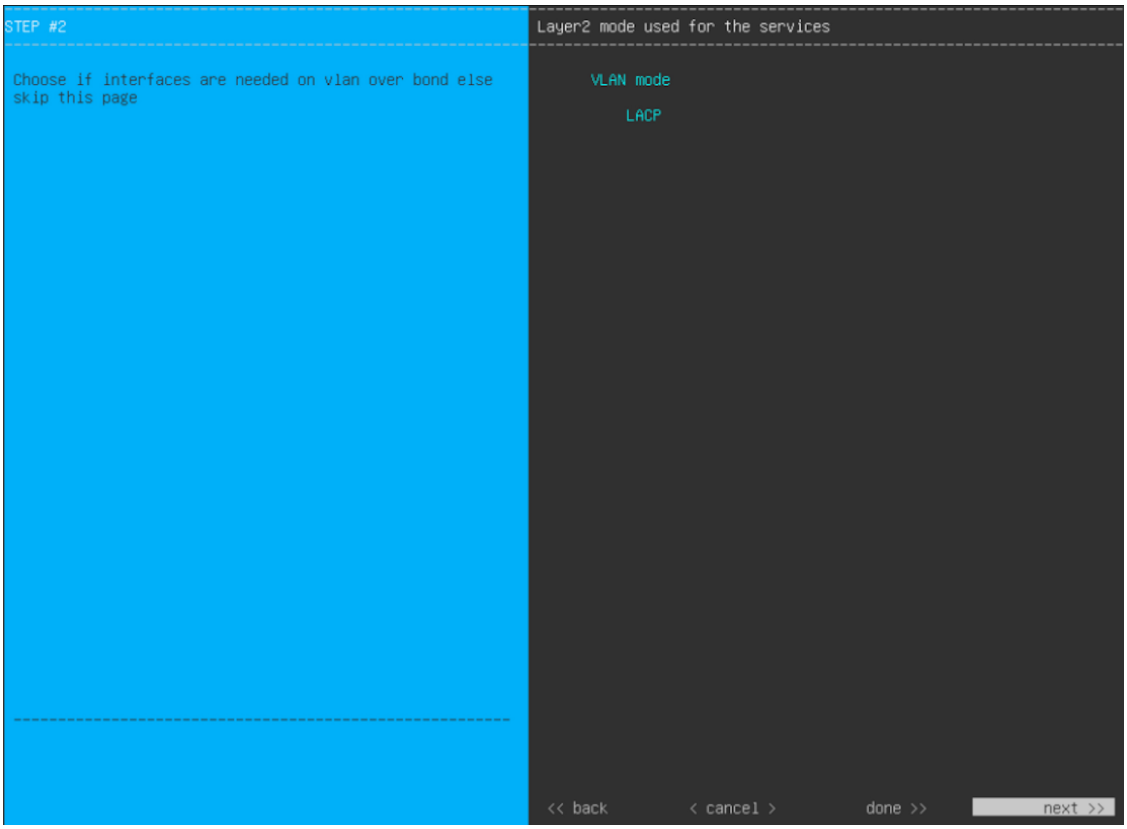
b) (Optional) Check the **Enable FIPS Mode** check box to enable FIPS mode on your Cisco DNA Center appliance.

See FIPS Mode Support, on page 22 for things to keep in mind when enabling FIPS mode on an appliance.

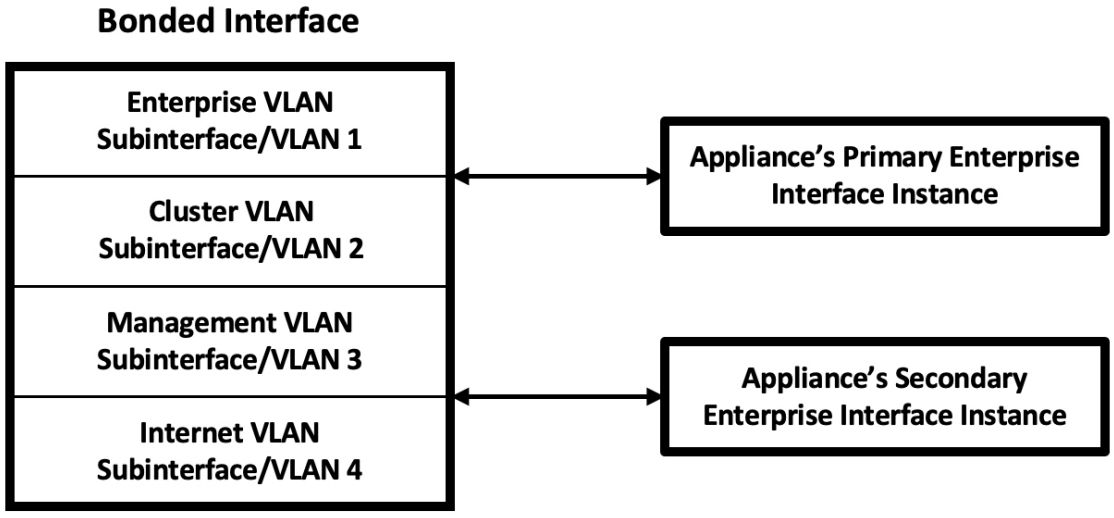
Important In the next wizard screen, you can enable the **VLAN mode** feature, which creates a single bonded interface that connects to your network using both the primary and secondary instance of your appliance's Enterprise interface. This feature is not commonly used, so only enable it if you know it's required by your Cisco DNA Center deployment.

- If this is the case, complete the next step.
- Otherwise, click **next>>** in the next wizard screen without making any selections. You can enable the NIC bonding functionality that was described previously in this guide in the wizard's Enterprise and Intracluster interface configuration screens.

Step 8 (Optional) Do the following to enable Layer 2 port channel mode (with VLAN tagging) for the appliance. After making your selections, click **next>>** to proceed.



a) Choose the **VLAN mode** option to enable dot1q/VLAN trunking and convert your appliance's Enterprise, Cluster, Management, and Internet interfaces into VLAN subinterfaces that reside on the bonded interface (as illustrated in the following figure). By default, this interface operates in Active-Backup mode (which enables HA).



b) If you want this interface to operate in LACP mode instead (which enables load balancing and higher bandwidth), you must also choose the **LACP** option.

c) When you enter the settings for your appliance's Enterprise and Cluster interfaces, ensure that you enter a unique VLAN ID in the **VLAN ID of Interface** field for the subinterfaces you want to configure on the virtual bonded interface.

Important Even though one physical appliance interface (the Enterprise interface) is connected, you can configure all of the subinterfaces that reside on the virtual bonded interface.

The wizard discovers all of the ports on the appliance and presents them to you one by one, in separate screens, in the following order:

a. (Required) 10-Gbps Enterprise Port—Network Adapter #1

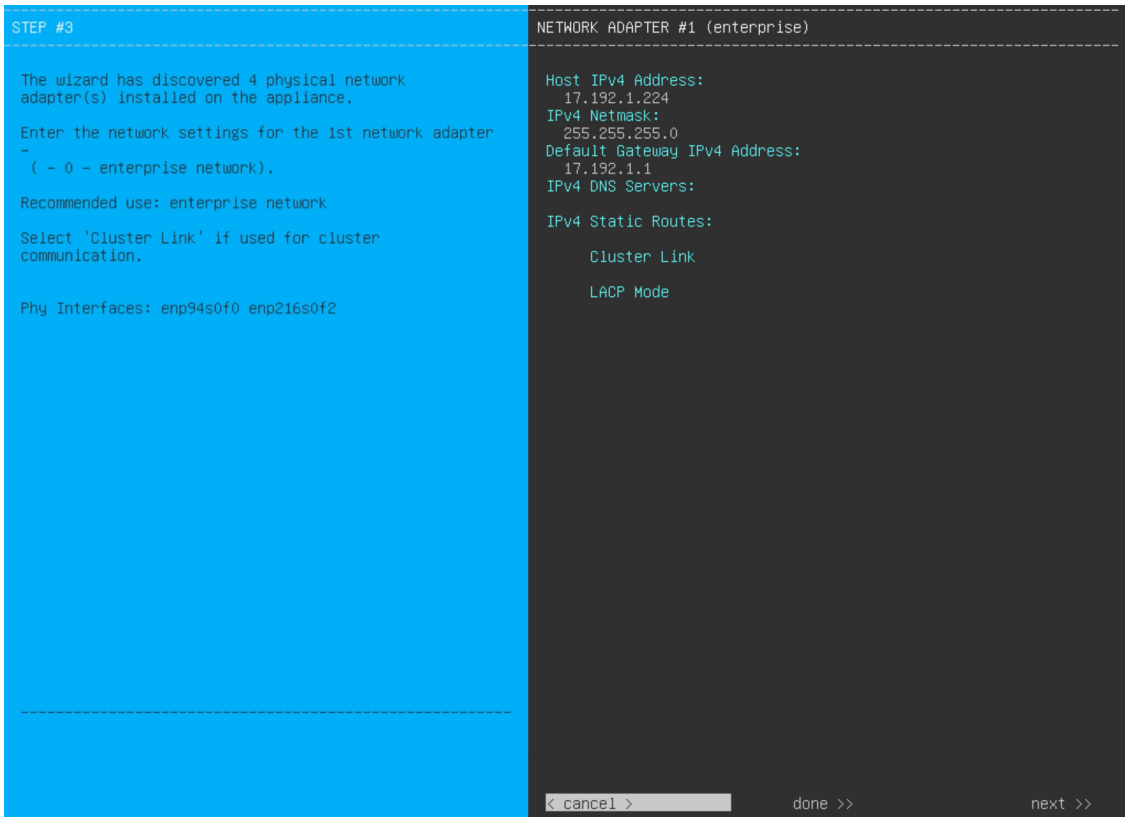
b. (Required) 10-Gbps Cluster Port—Network Adapter #2

c. (Optional) 1-Gbps/10-Gbps Management Port—Network Adapter #3

d. (Optional) 1-Gbps/10-Gbps Internet Port—Network Adapter #4

If the wizard fails to display either or both of the Enterprise and Cluster ports during the course of configuration, it might indicate that these ports are nonfunctional or disabled. These two ports are required for Cisco DNA Center functionality. If you discover that they are nonfunctional, choose **cancel** to exit the configuration wizard immediately. Be sure that you have completed all of the steps provided in Execute Preconfiguration Checks before resuming the configuration or contacting the Cisco Technical Assistance Center (for more information, see the "Get Assistance from the Cisco TAC" topic in the Release Notes document).

Step 9 The wizard first presents the 10-Gbps Enterprise port as **NETWORK ADAPTER #1**. As explained in Interface Cable Connections, this is a required port used to link the appliance to the enterprise network. Apply the host IP address, netmask, and other values that are appropriate for this purpose (see Required IP Addresses and Subnets and Required Configuration Information for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #1**, as shown in the table below.

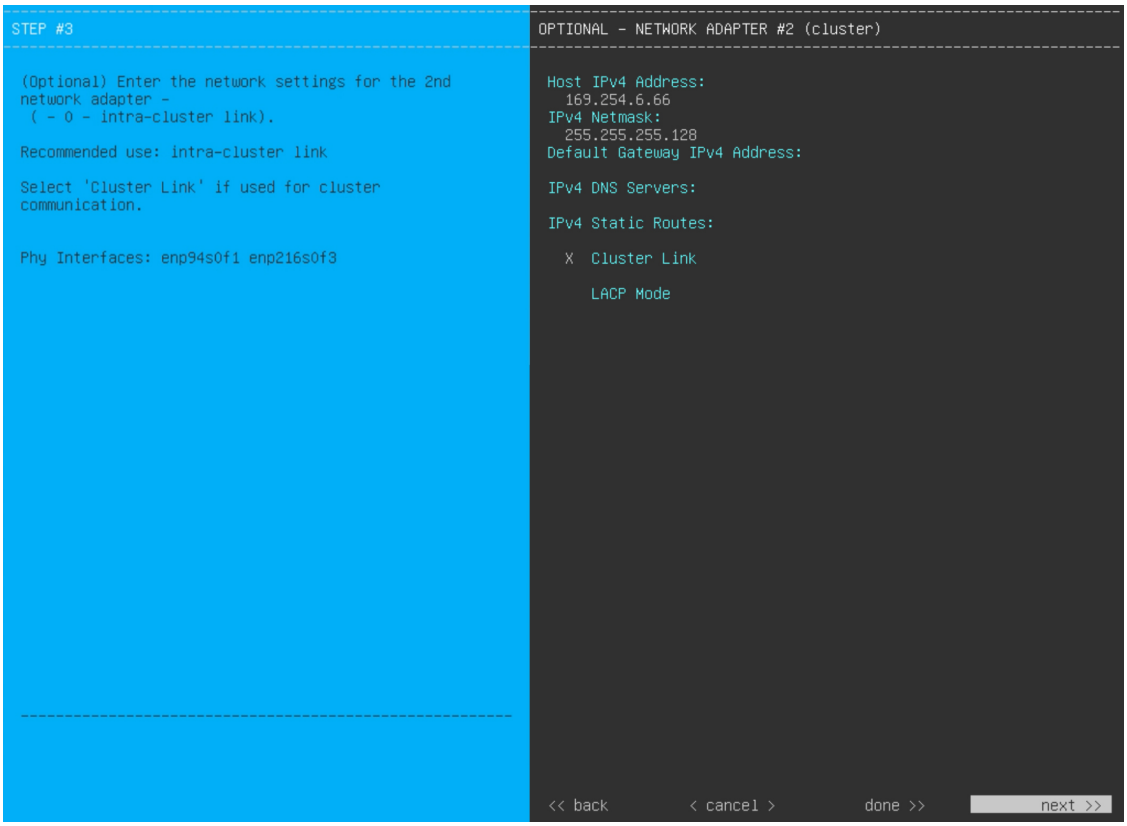
Table 1: Primary Node Entries for Network Adapter #1: 10-Gbps Enterprise Port

Host IPv4/IPv6 Address field	Enter the IP address for the Enterprise port. This is required.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 Address field	Enter a default gateway IP address to use for the port. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4/IPv6 DNS Servers field	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. **Important** For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.

IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*. This is usually required on the Cisco DNA Center Management port only.
Vlan ID of Interface field	Enter the VLAN ID for the bonded interface you enabled in the previous step. If you didn't enable it, this field will not be displayed.
Cluster Link field	Leave this field blank. It is required on the Cluster port only.
LACP Mode field	Do one of the following: • Leave this field blank and the port will operate in **Active-Backup** mode. This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active. • Check the check box to enable **LACP** mode on this port. This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth. For more information about Cisco DNA Center's implementation of NIC bonding, see NIC Bonding Overview. **Note** This field is displayed if you didn't choose any of the options in the previous step.

After you finish entering the configuration values, click **next>>** to proceed. The wizard validates the values you entered and issues an error message if any are incorrect. If you receive an error message, check that the value you entered is correct, then reenter it. If needed, click **<<back** to reenter it.

Step 10 After successful validation of the Enterprise port values you entered, the wizard presents the 10-Gbps Cluster port and presents it as **NETWORK ADAPTER #2**. As explained in Interface Cable Connections, this port is used to link the appliance to the cluster, so apply the host IP address, netmask, and other values that are appropriate for this purpose (see Required IP Addresses and Subnets and Required Configuration Information for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #2**, as shown in the table below.

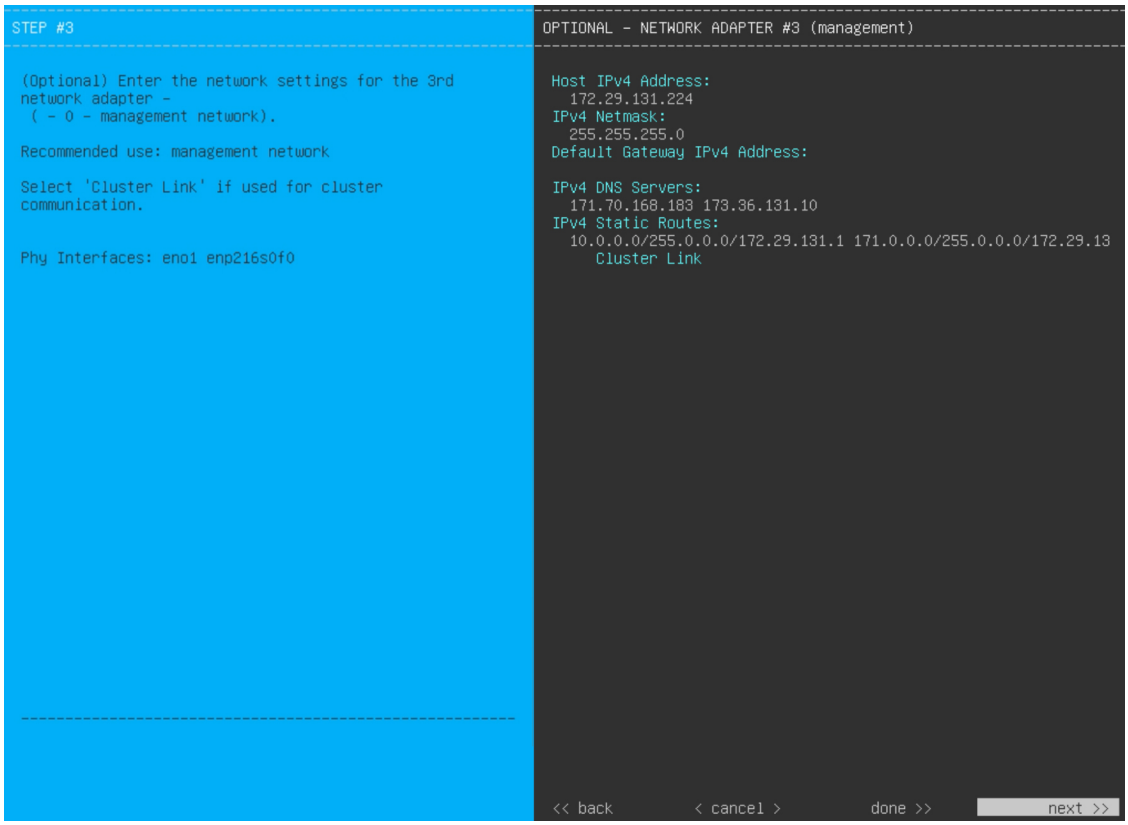
Table 2: Primary Node Entries for Network Adapter #2: 10-Gbps Cluster Port

Host IPv4/IPv6 address field	Enter the IP address for the Cluster port. This is required. Note that you cannot change the address of the Cluster port later. **Note** If you selected the **Start using DNAC pre manufactured cluster** option previously, **169.254.6.66** will already be set in this field and you will not be able to enter a different address.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. **Note** If you selected the **Start using DNAC pre manufactured cluster** option previously, **255.255.255.128** will already be set in this field and you will not be able to enter a different netmask. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.

Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4/IPv6 DNS Servers field	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. **Important** For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*. This is usually required on the Management port only.
Vlan ID of Interface field	Enter the VLAN ID for the bonded interface you enabled previously. If you didn't enable it, this field will not be displayed.
Cluster Link field	Check the check box to set this port as the link to a Cisco DNA Center cluster. This is required on the Cluster port only.
LACP Mode field	Do one of the following: • Leave this field blank and the port will operate in **Active-Backup** mode. This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active. • Check the check box to enable **LACP** mode on this port. This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth. For more information about Cisco DNA Center's implementation of NIC bonding, see NIC Bonding Overview. **Note** This field is displayed if you didn't choose any of the options in Step 8.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

Step 11 After successful validation of the Cluster port values you entered, the wizard presents the 1-Gbps/10-Gbps Management port and presents it as **NETWORK ADAPTER #3**. As explained in Interface Cable Connections, this port is used to access the Cisco DNA Center GUI from your management network. Apply the host IP address, netmask, and other values that are appropriate for this purpose (see Required IP Addresses and Subnets and Required Configuration Information for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #3**, as shown in the table below.

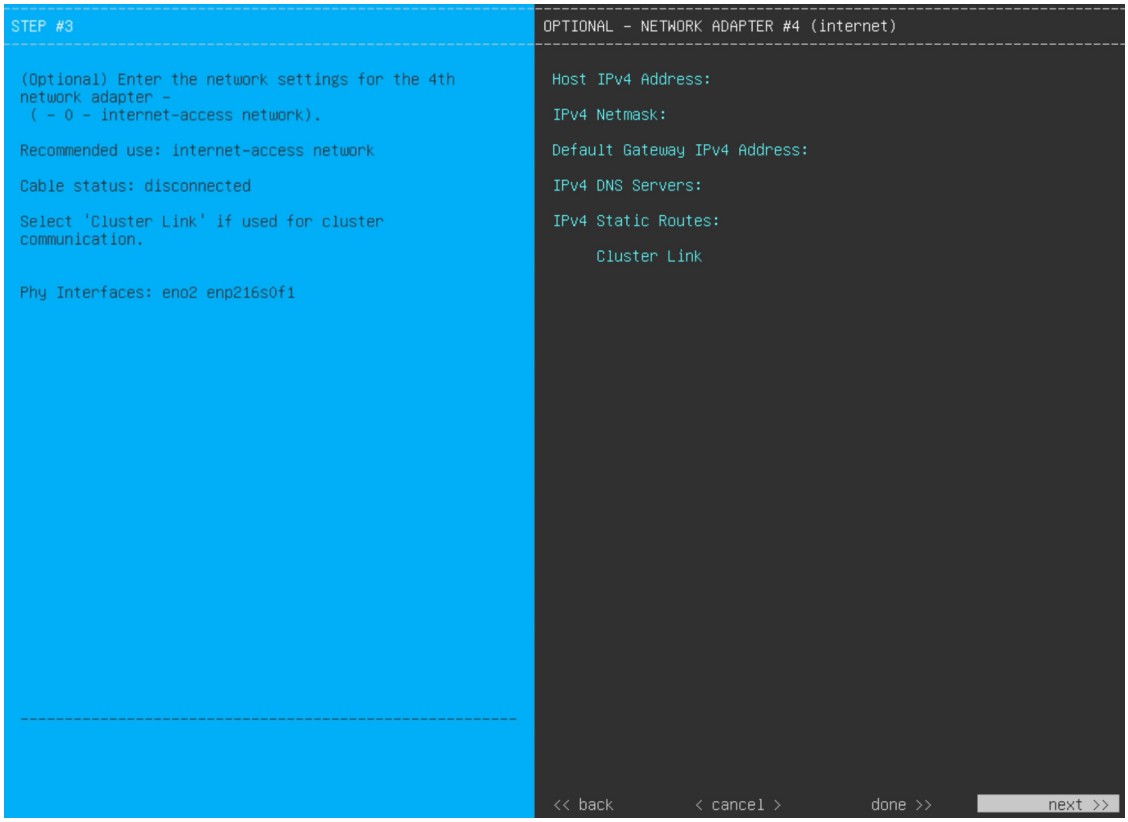
Table 3: Primary Node Entries for Network Adapter #3: 1-Gbps/10-Gbps Management Port

Host IPv4/IPv6 address field	Enter the IP address for the Management Port. This is required only if you are using this port to access the Cisco DNA Center GUI from your management network; otherwise, you can leave it blank.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following if you entered an IP address: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.

IPv4/IPv6 DNS Servers field	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. **Important** • For NTP, ensure port 123 (UDP) is open between Cisco DNA Center and your NTP server. • For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*.
Cluster Link field	Leave this field blank. It is required on the Cluster port only.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

Step 12 After successful validation of the Management port values you entered, the wizard presents the 1-Gbps/10-Gbps Internet port as **NETWORK ADAPTER #4**. As explained in Interface Cable Connections, this is an optional port used to link the appliance to the Internet when you cannot do so through the 10-Gbps Enterprise port. Apply the host IP address, netmask, and other values that are appropriate for this purpose (see Required IP Addresses and Subnets and Required Configuration Information for the values to enter).



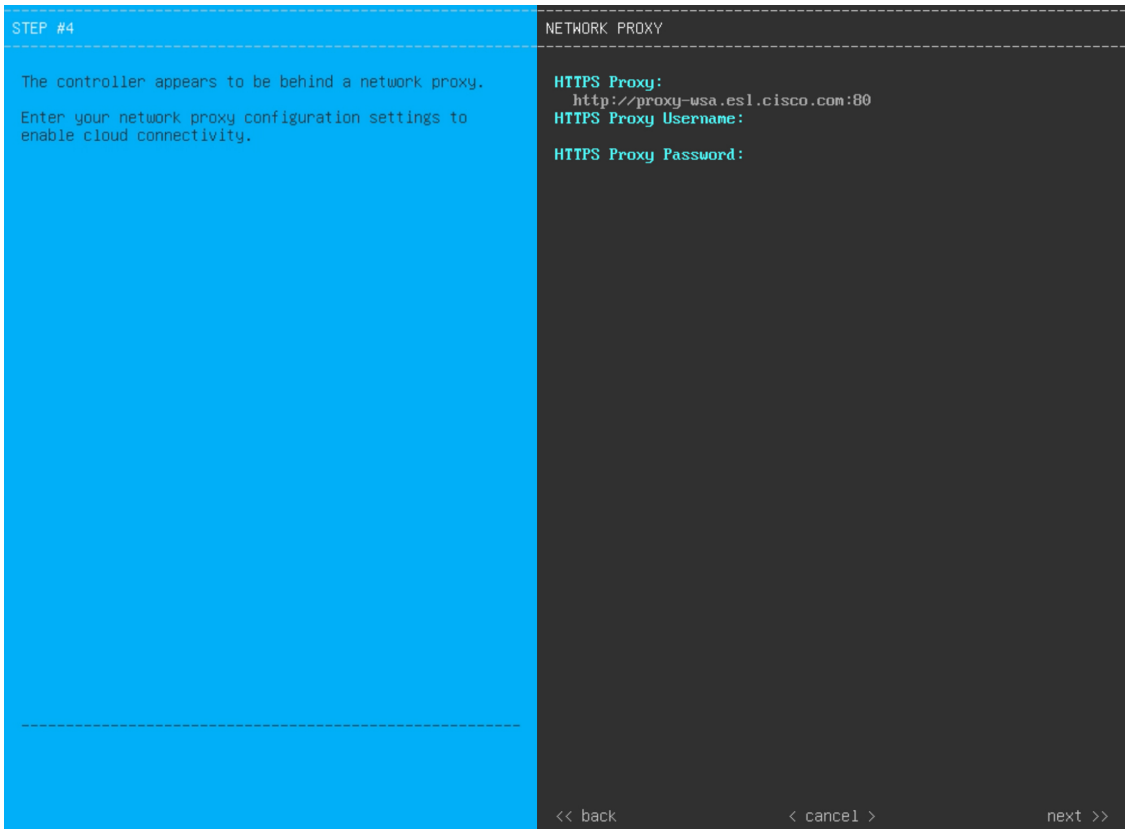
Enter the configuration values for **NETWORK ADAPTER #4**, as shown in the table below.

Table 4: Primary Node Entries for Network Adapter #4: 1-Gbps/10-Gbps Internet Port

Host IPv4/IPv6 address field	Enter the IP address for the Internet port. This is required only if you are using the Internet port for internet connection; otherwise, you can leave it blank.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following if you entered an IP address: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the Internet port. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4/IPv6 DNS Servers field	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. **Important** For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: <*network*>/<*netmask*>/<*gateway*>. This is usually required on the Management port only.
Cluster Link field	Leave this field blank. It is required on the Cluster port only.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

Step 13 After the network adapter configuration is complete, the wizard prompts you to enter configuration values for the **NETWORK PROXY** that you are using, as shown below.



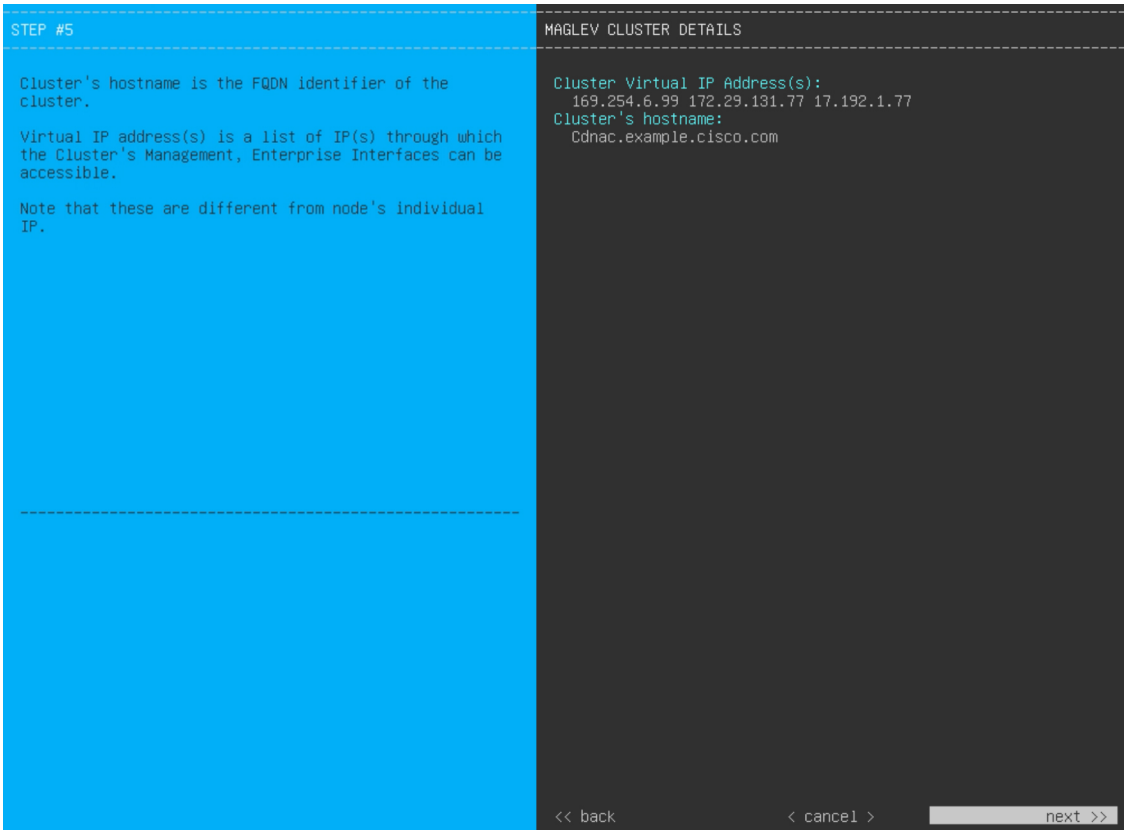
Enter the configuration values for the **NETWORK PROXY**, as shown in the table below.

Table 5: Primary Node Entries for Network Proxy

HTTPS Proxy field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. **Note** • Connection from Cisco DNA Center to the HTTPS proxy is supported only through HTTP in this release. • If you enter an IPv6 URL that contains a port number, enclose the IP address portion of the URL in square brackets. In this example, 443 is the port number: http://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:443/
HTTPS Proxy Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
HTTPS Proxy Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

Step 14 After network proxy configuration completes, the wizard prompts you to enter virtual IP addresses for the primary node, in **MAGLEV CLUSTER DETAILS** (as shown below).



Enter a space-separated list of the virtual IP addresses used for traffic between the cluster and your network. This is required for both three-node clusters and single-node clusters that will be converted into a three-node cluster in the future. If you have a single-node cluster setup and plan to stick with it, skip this step and proceed to the next step.

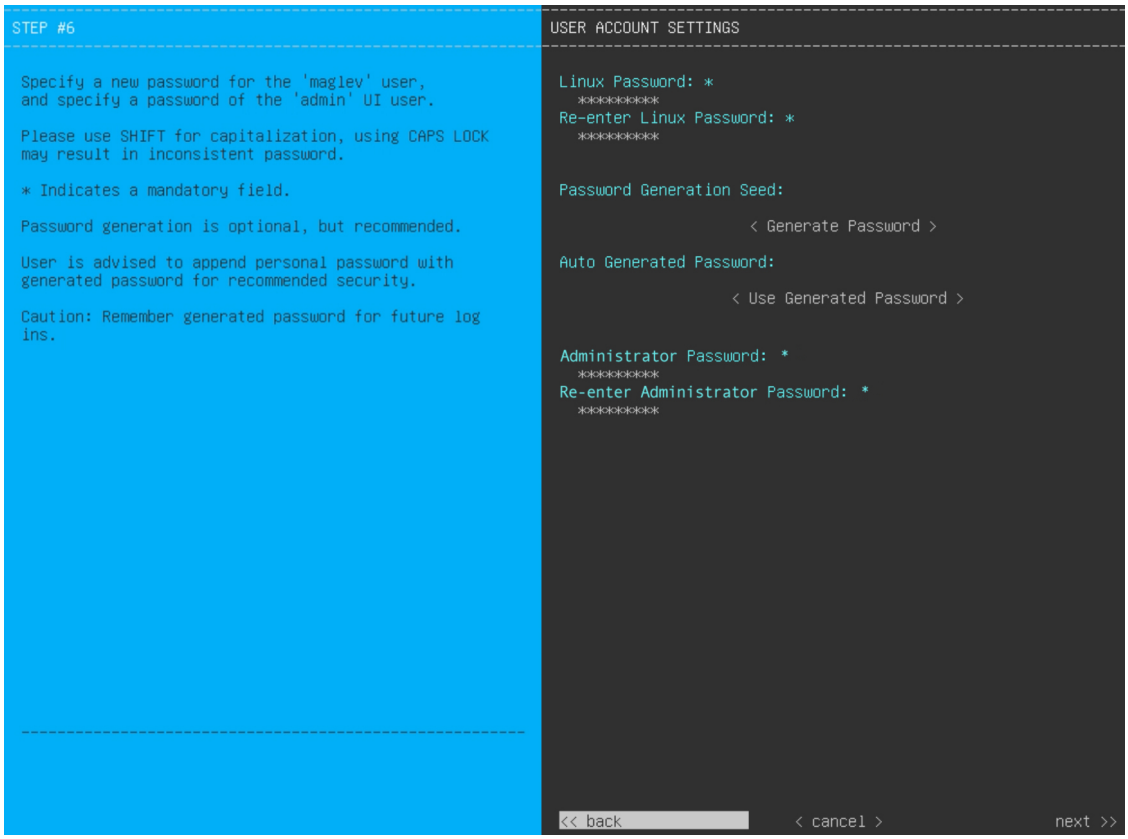
Important You must enter one virtual IP address for each configured network interface. You will not be able to complete the wizard unless you do so. These addresses are tied to the cluster link's status, which must be in the **UP** state.

You also have the option to specify the fully qualified domain name (FQDN) for your cluster. Cisco DNA Center uses this domain name to do the following:

- It uses this hostname to access your cluster's web interface and the Representational State Transfer (REST) APIs used by devices in the enterprise network that Cisco DNA Center manages.
- In the Subject Alternative Name (SAN) field of Cisco DNA Center certificates, it uses the FQDN to the define the Plug and Play server that should be used for device provisioning.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

Step 15 After you have entered the cluster details, the wizard prompts you to enter **USER ACCOUNT SETTINGS** values, as shown below.



Enter the values for **USER ACCOUNT SETTINGS**, as shown in the table below.

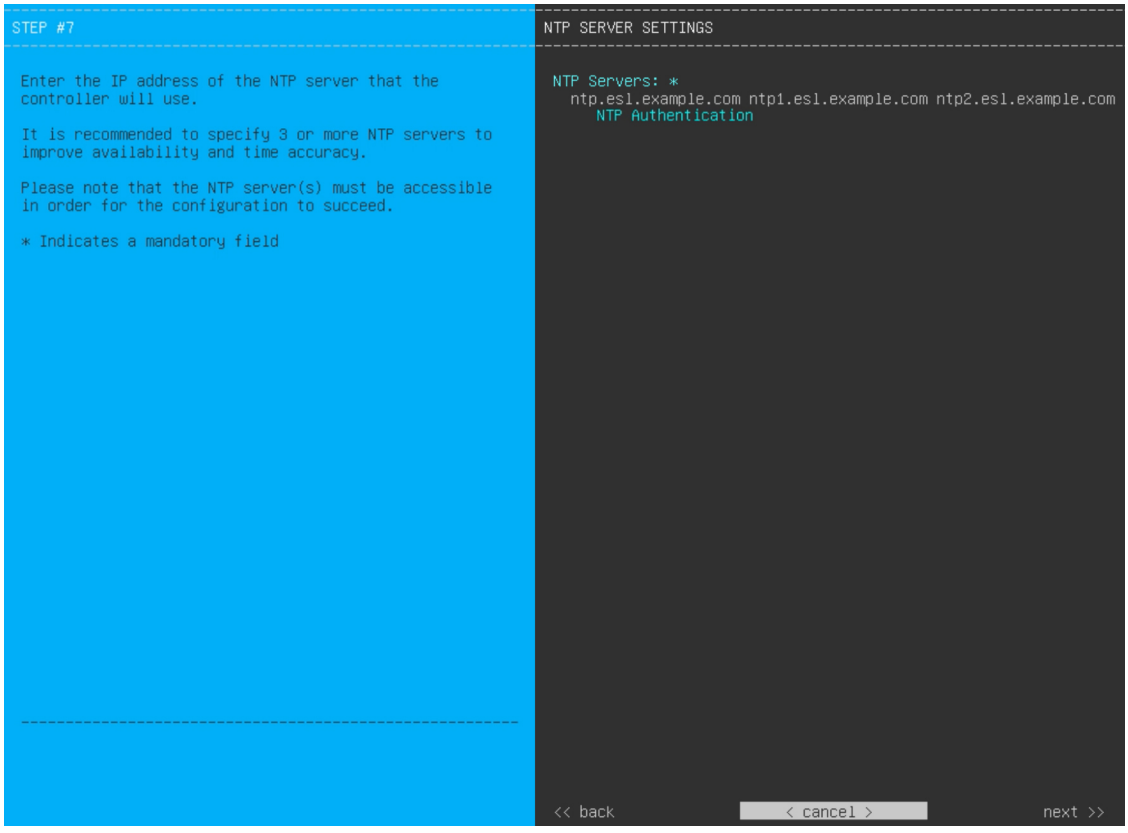
Table 6: Primary Node Entries for User Account Settings

Linux Password field	Enter a Linux password for the maglev user that's a minimum of 8 characters long.
Re-enter Linux Password field	Confirm the Linux password by entering it a second time.
Password Generation Seed field	If you do not want to create the Linux password yourself, enter a seed phrase in this field and then press <**Generate Password**> to generate the password.
Auto Generated Password field	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto-generated password. Press <**Use Generated Password**> to save the password.

Administrator Password field	Enter a password for the default admin superuser, used to log in to Cisco DNA Center for the first time. Note the following points: • If you enabled FIPS mode earlier in the wizard, ensure that this password is at least 8 characters long. • If you chose the **Start using DNAC pre manufactured cluster** option previously, the default password (**maglev1@3**) has already been set for the appliance and cannot be changed in the configuration wizard. As a result, this and the following field are not displayed in this screen.
Re-enter Administrator Password field	Confirm the administrator password by entering it a second time.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

Step 16 After you have entered the user account details, the wizard prompts you to enter **NTP SERVER SETTINGS** values.



Enter the values for **NTP SERVER SETTINGS**, as shown in the table below.

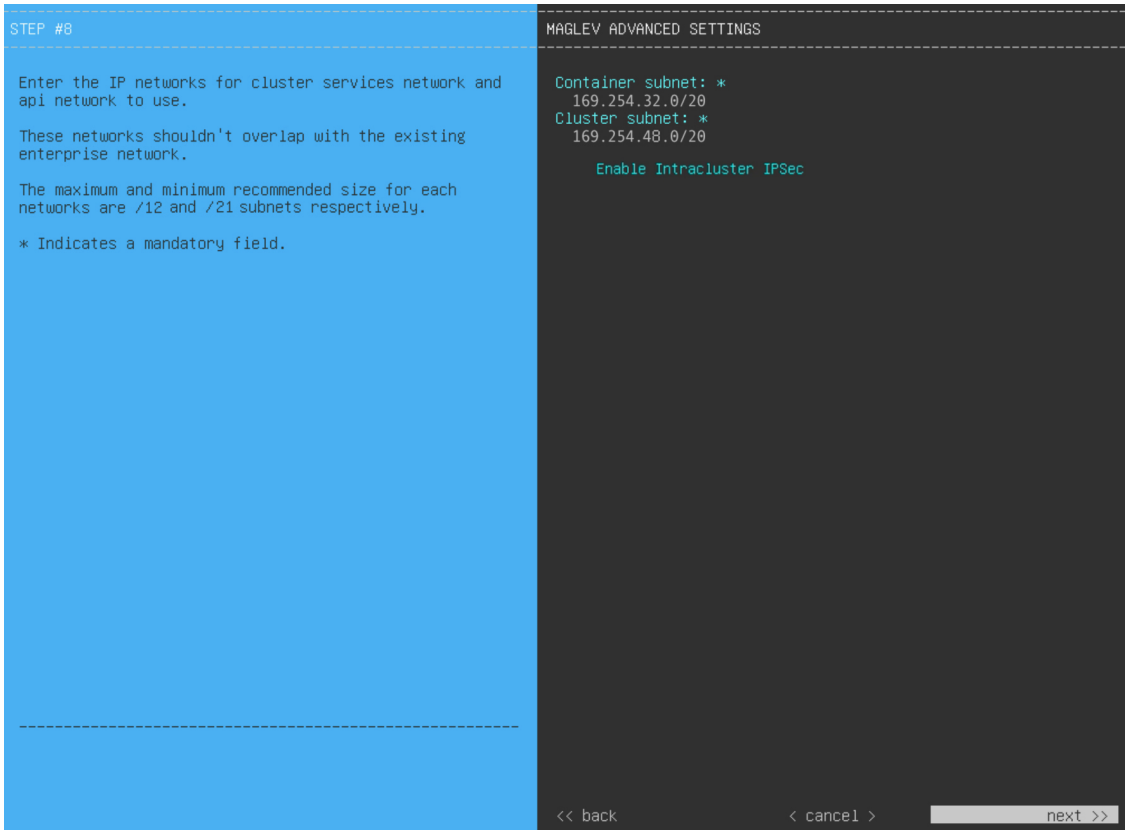
NTP Servers field	Enter one or more NTP server addresses or hostnames, separated by spaces. At least one NTP address or hostname is required. For a production deployment, we recommend that you configure a minimum of three NTP servers.

NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Cisco DNA Center, check this check box and then enter the following information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file. **Note** Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your NTP server configuration.

Step 17 After you have specified the appropriate NTP servers, the wizard prompts you to enter **MAGLEV ADVANCED SETTINGS** values, as shown below.

Note If you chose the **Start using DNAC pre manufactured cluster** option previously, the default Container and Cluster subnets have already been set for the appliance and cannot be changed in the configuration wizard. As a result, you will not see the following wizard screen. Proceed to Step 17.



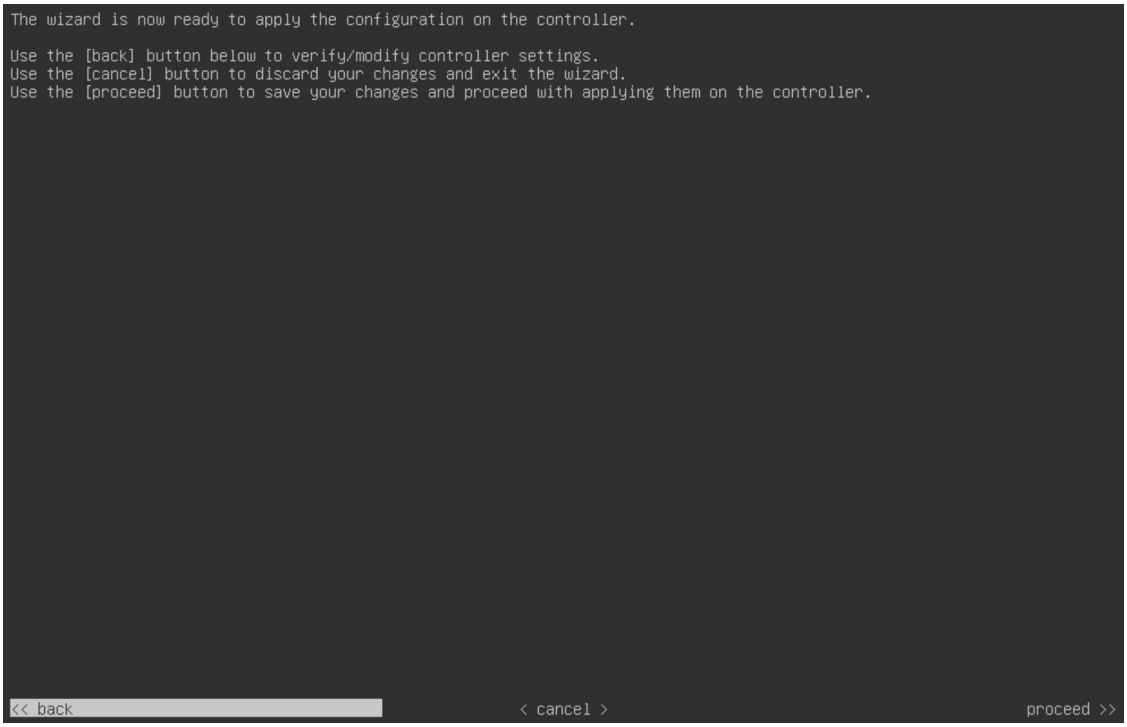
Enter the configuration values for **MAGLEV ADVANCED SETTINGS**, as shown in the table below.

Table 7: Primary Node Entries for Maglev Advanced Settings

Container Subnet field	A dedicated, non-routed IP subnet that Cisco DNA Center uses to manage internal services. By default, this is already set to **169.254.32.0/20**, and we recommend that you use this subnet. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Cisco DNA Center internal network or an external network. For more information, see the Container Subnet description in Required IP Addresses and Subnets.
Cluster Subnet field	A dedicated, non-routed IP subnet that Cisco DNA Center uses to manage internal cluster services. By default, this is already set to **169.254.48.0/20**, and we recommend that you use this subnet. If you choose to enter another subnet, ensure that it does not conflict with or overlap any other subnet used by the Cisco DNA Center internal network or an external network. For more information, see the Cluster Subnet description in Required IP Addresses and Subnets.
Enable Intracluster IPSec check box	Check to enable IPsec connections between the nodes in a three-node high HA cluster.

When you are finished, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

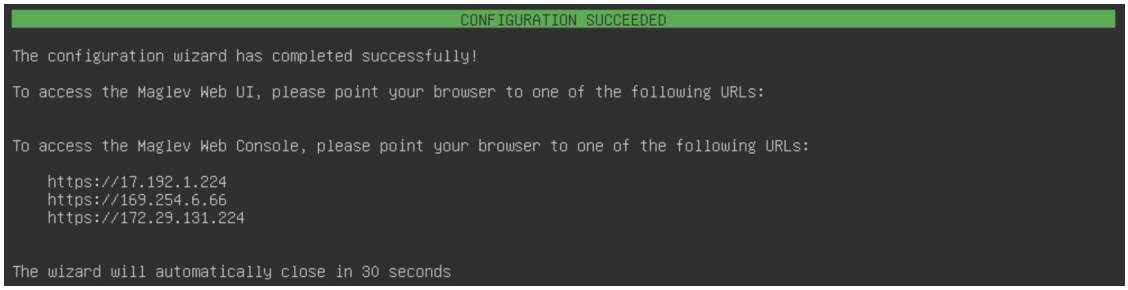
Step 18 After you have entered the Maglev advanced settings, a final message appears, stating that the wizard is ready to apply the configuration (as shown below).



Click **proceed>>** to complete the configuration wizard.

The host will reboot automatically and display messages on the KVM console as it applies your settings and brings up services. This process can take several hours. You can monitor its progress via the KVM console.

At the end of the configuration process, the appliance power cycles again, then displays a **CONFIGURATION SUCCEEDED!** message.



What to do next

- If you are deploying this appliance in standalone mode only, perform the first-time setup: First-Time Setup Workflow.
- If you are deploying this appliance as the primary node in a cluster, configure the second and third installed appliances in the cluster: Configure a Secondary Node Using the Maglev Wizard, on page 23.

FIPS Mode Support

Cisco DNA Center supports the Federal Information Processing Standard (FIPS), a government certification standard that specifies best practices for implementing cryptographic algorithms, handling key material and data buffers, and working with the operating system. Note the following points if you plan to enable FIPS mode on an appliance:

- You cannot enable FIPS mode on an appliance that has been upgraded from a previous Cisco DNA Center version. You can only enable it on an appliance that came with the latest version already installed.
- When FIPS mode is enabled, you cannot import images from a URL. You can only import images from either your computer or cisco.com.
- You will need to enter a password that's at least 8 characters long for the default admin superuser in the **USER ACCOUNT SETTINGS** screen.
- When FIPS mode is enabled on an appliance, you cannot enable external authentication.
- If you selected the **Start using DNAC pre manufactured cluster** option while completing the Maglev Configuration wizard, you will not see the **IP addressing and Security mode used for the services** screen. As a result, you will not be able to enable FIPS mode.
- Cisco DNA Center does not support SNMPv2c device credentials when FIPS mode is enabled. You must specify SNMPv3 credentials instead.
- After FIPS mode has been enabled on an appliance, the only way you can disable it is to reimage your appliance (to erase all existing data). You can then reconfigure the appliance with FIPS mode disabled. See Reimage the Appliance for more information.
- When FIPS mode is enabled, you can only enable KeyWrap if Cisco DNA Center and Cisco ISE haven't already been integrated. See Configure Authentication and Policy Servers for more information.

- After configuring your appliance, you can do the following to confirm whether FIPS mode is enabled:
  1. Open an SSH console to the appliance and run the **ssh -p 2222 maglev@***appliance's-IP-address* command.
  2. Enter the default admin superuser's password to log in to the appliance.
  3. Run the **magctl fips status** command.
- The Cisco Wide Area Bonjour application does not support FIPS mode. As a result, you cannot install this application from either the Cisco DNA Center GUI or CLI.
- When FIPS mode is enabled, some of the functions related to Endpoint Analytics are unavailable in the Cisco DNA Center GUI.
- FIPS mode affects the export and import of map archives.

  When FIPS mode is *enabled*:
  - Exported map archives are unencrypted.
  - Only unencrypted map archives can be imported.

  When FIPS mode is *disabled*:
  - Exported map archives are encrypted.
  - Both encrypted and unencrypted map archives can be imported.

Configure a Secondary Node Using the Maglev Wizard

Perform the steps in this procedure to configure the second and third appliances in the cluster.

Important

- In order to build a three-node cluster, the same version of the **System** package must be installed on your three Cisco DNA Center appliances. Otherwise, unexpected behavior and possible downtime can occur.
- Before you configure the appliances in a three-node cluster, ensure that you have logged out of those appliances. Otherwise, the Quick Start workflow (which you complete to discover your network's devices and enable telemetry) will not start after you have configured your cluster's appliances and log in to Cisco DNA Center for the first time.
- Ensure that all of the IP addresses you enter while completing this procedure are valid IPv4 addresses with valid IPv4 netmasks. Also make sure that the addresses and their corresponding subnets do not overlap. Service communication issues can result if they do.

When joining each new secondary node to the cluster, you must specify the first host in the cluster as the primary node. Note the following when joining secondary nodes to a cluster:

- Be sure to join only a single node to the cluster at a time. Do not attempt to add multiple nodes at the same time, because this results in unpredictable behavior.

- Before adding a new node to the cluster, be sure that all installed packages are deployed on the primary node. You can check this by using Secure Shell to log in to the primary node's Cisco DNA Center Management port as the Linux user (*maglev*) and then running the command `maglev package status`. All installed packages should appear in the command output as `DEPLOYED`.

```
maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]

NAME                         DISPLAY_NAME                                  DEPLOYED          AVAILABLE          STATUS            PROGRESS
-------------------------------------------------------------------------------------------------------------------------------------------
access-control-application Access Control Application                       -                2.1.369.60050    NOT_DEPLOYED
ai-network-analytics       AI Network Analytics                          -               2.6.10.494        NOT_DEPLOYED
app-hosting                Application Hosting                           -               1.6.6.2201241723 NOT_DEPLOYED
application-policy         Application Policy                            -               2.1.369.170033   NOT_DEPLOYED
application-registry       Application Registry                          -               2.1.369.170033   NOT_DEPLOYED
application-visibility-service Application Visibility Service                -              2.1.369.170033  NOT_DEPLOYED
assurance                  Assurance - Base                              2.2.2.485        -                DEPLOYED
automation-core            NCP - Services                                2.1.368.60015    2.1.369.60050    DEPLOYED
base-provision-core        Automation - Base                             2.1.368.60015    2.1.369.60050    DEPLOYED
cloud-connectivity-contextual-content Cloud Connectivity - Contextual Content  1.3.1.364     -                DEPLOYED
cloud-connectivity-data-hub Cloud Connectivity - Data Hub                  1.6.0.380      -                DEPLOYED
cloud-connectivity-tethering Cloud Connectivity - Tethering                  2.12.1.2       -                DEPLOYED
cloud-provision-core       Cloud Device Provisioning Application         -               2.1.369.60050    NOT_DEPLOYED
command-runner             Command Runner                                2.1.368.60015    2.1.369.60050    DEPLOYED
device-onboarding          Device Onboarding                             2.1.368.60015    2.1.369.60050    DEPLOYED
disaster-recovery          Disaster Recovery                             -               2.1.367.360196   NOT_DEPLOYED
dna-core-apps              Network Experience Platform - Core            2.1.368.60015    2.1.369.60050    DEPLOYED
dnac-platform              Cisco DNA Center Platform                     1.5.1.180        1.5.1.182        DEPLOYED
dnac-search                Cisco DNA Center Global Search                1.5.0.466        -                DEPLOYED
endpoint-analytics         AI Endpoint Analytics                         -               1.4.375          NOT_DEPLOYED
group-based-policy-analytics Group-Based Policy Analytics                    -              2.2.1.401        NOT_DEPLOYED
icap-automation            Automation - Intelligent Capture              -               2.1.369.60050    NOT_DEPLOYED
image-management           Image Management                              2.1.368.60015    2.1.369.60050    DEPLOYED
machine-reasoning          Machine Reasoning                             2.1.368.210017   2.1.369.210024   DEPLOYED
ncp-system                 NCP - Base                                    2.1.368.60015    2.1.369.60050    DEPLOYED
ndp-base-analytics         Network Data Platform - Base Analytics        1.6.1028         1.6.1031         DEPLOYED
ndp-platform               Network Data Platform - Core                  1.6.596          -                DEPLOYED
ndp-ui                     Network Data Platform - Manager               1.6.543          -                DEPLOYED
network-visibility         Network Controller Platform                   2.1.368.60015    2.1.369.60050    DEPLOYED
path-trace                 Path Trace                                    2.1.368.60015    2.1.369.60050    DEPLOYED
platform-ui                Cisco DNA Center UI                           1.6.2.446        1.6.2.448        DEPLOYED
rbac-extensions            RBAC Extensions                               2.1.368.1910001  2.1.369.1910003  DEPLOYED
rogue-management           Rogue and aWIPS                               -               2.2.0.51         NOT_DEPLOYED
sd-access                  SD Access                                     -               2.1.369.60050    NOT_DEPLOYED
sensor-assurance           Assurance - Sensor                            -               2.2.2.484        NOT_DEPLOYED
sensor-automation          Automation - Sensor                           -               2.1.369.60050    NOT_DEPLOYED
ssa                        Stealthwatch Security Analytics               2.1.368.1091226  2.1.369.1091317  DEPLOYED
system                     System                                        1.6.594          -                DEPLOYED
system-commons             System Commons                                2.1.368.60015    2.1.369.60050    DEPLOYED
umbrella                   Cisco Umbrella                                -               2.1.368.592066   NOT_DEPLOYED
wide-area-bonjour          Wide Area Bonjour                             -               2.4.368.75006    NOT_DEPLOYED

[Wed Nov 30 15:45:08 UTC] maglev@192.0.2.1 (maglev-master-192.0.2.1) ~
```

- Expect some service downtime during the cluster attachment process for each secondary node. Services will need to be redistributed across the nodes, and the cluster will be down for periods of time during that process.

Before you begin

Ensure that you:

- Configured the first appliance in the cluster, following the steps in Configure the Primary Node Using the Maglev Wizard, on page 1.
- Collected all of the information specified in Required IP Addresses and Subnets and Required Configuration Information.
- Installed the second and third appliances, as described in Appliance Installation Workflow.
- Have done the following:
  1. Ran the **maglev package status** command on the first appliance.

     You can also access this information from the Cisco DNA Center GUI by clicking the **Help** icon ( ) and choosing **About** > **Packages**.
  2. Contacted the Cisco TAC, gave them the output of this command, and asked them to point you to the ISO that you should install on your second and third appliances.
- Configured Cisco IMC browser access on both secondary appliances, as described in Enable Browser Access to Cisco Integrated Management Controller.

- Checked that both the secondary appliances' ports and the switches they use are properly configured (as described in Execute Preconfiguration Checks).
- Confirmed that you are using a compatible browser. For a list of compatible browsers, see the Release Notes document for the version of Cisco DNA Center you are installing.
- Enabled ICMP on the firewall between Cisco DNA Center and both the default gateway and the DNS server you specify in the following procedure. The Maglev Configuration wizard uses ping to verify the gateway and DNS server you specify. This ping might get blocked if a firewall is in place and ICMP is not enabled on that firewall. When this happens, you will not be able to complete the wizard.

Step 1 Point your browser to the Cisco IMC IP address you set during the Cisco IMC GUI configuration you performed, and log in to the Cisco IMC GUI as the Cisco IMC user (see Enable Browser Access to Cisco Integrated Management Controller).

After successful login, the appliance displays the **Cisco Integrated Management Controller Chassis Summary** window, with a hyperlinked menu at the top of the window, as shown below.

Step 2 From the hyperlinked menu, choose **Launch KVM** and then choose either **Java based KVM** or **HTML based KVM**. If you choose **Java-based KVM**, you will need to launch the Java startup file from your browser or file manager in order to view the KVM console in its own window. If you choose **HTML-based KVM**, it launches the KVM console in a separate window or tab automatically.

Irrespective of the KVM type you choose, use the KVM console to monitor the progress of the configuration and respond to the Maglev Configuration wizard prompts.

Step 3 With the KVM displayed, reboot the appliance by choosing one of the following options:

- In the main Cisco IMC GUI browser window: Choose **Host Power** > **Power Cycle**, and switch to the KVM console to continue.
- In the KVM console: Choose **Power** > **Power Cycle System (cold boot)**.

If you are asked to confirm your choice to reboot the appliance, click **OK**.

After displaying reboot messages, the KVM console displays the **Static IP Configuration** screen.

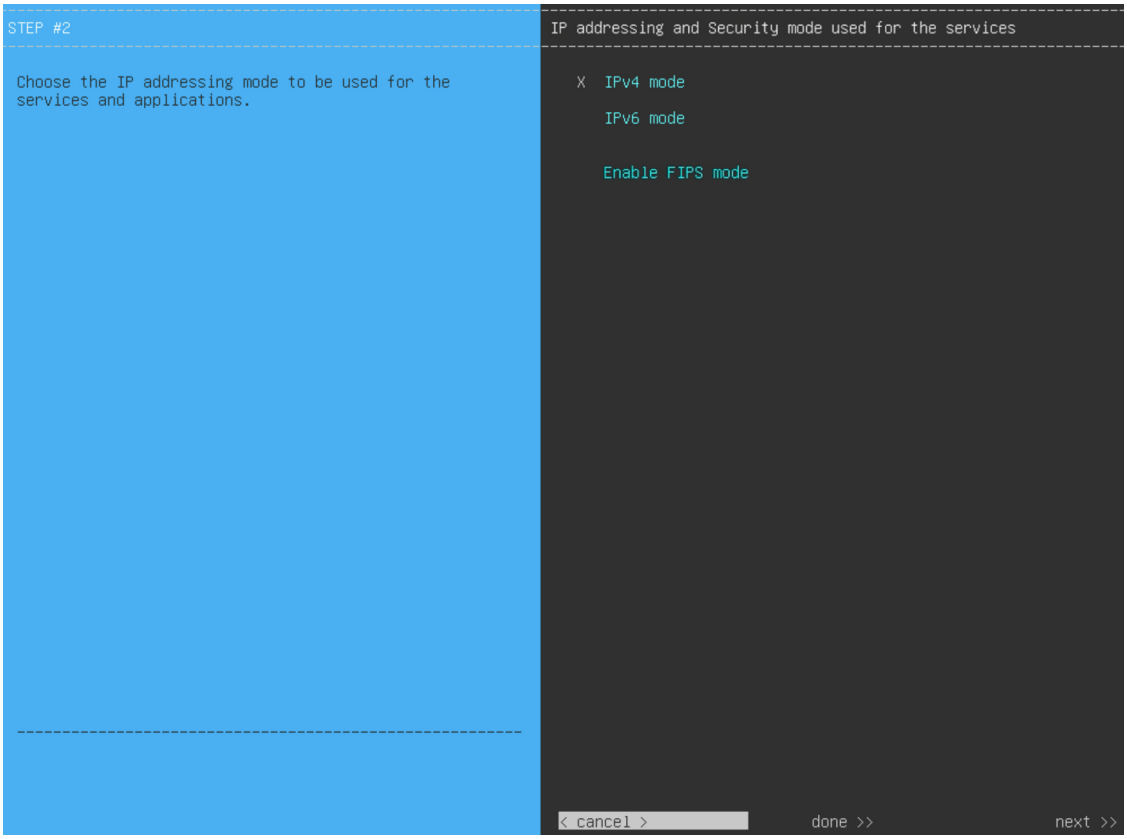
Step 4 Click **Skip**.

The KVM console displays the Maglev Configuration wizard welcome screen.

Note Only users that want to configure their appliance using one of the browser-based wizards without using the IP address, subnet mask, and default gateway assigned to the appliance's Enterprise interface by a DHCP server need to complete this screen.

Step 5 Click **Join a Cisco DNA Center Cluster** to begin configuring the secondary node.

The screen updates.



Step 6 Do the following, then click **next>>** to proceed:

a) Specify whether the applications and services running on your Cisco DNA Center appliance will use IPv4 or IPv6 addressing.

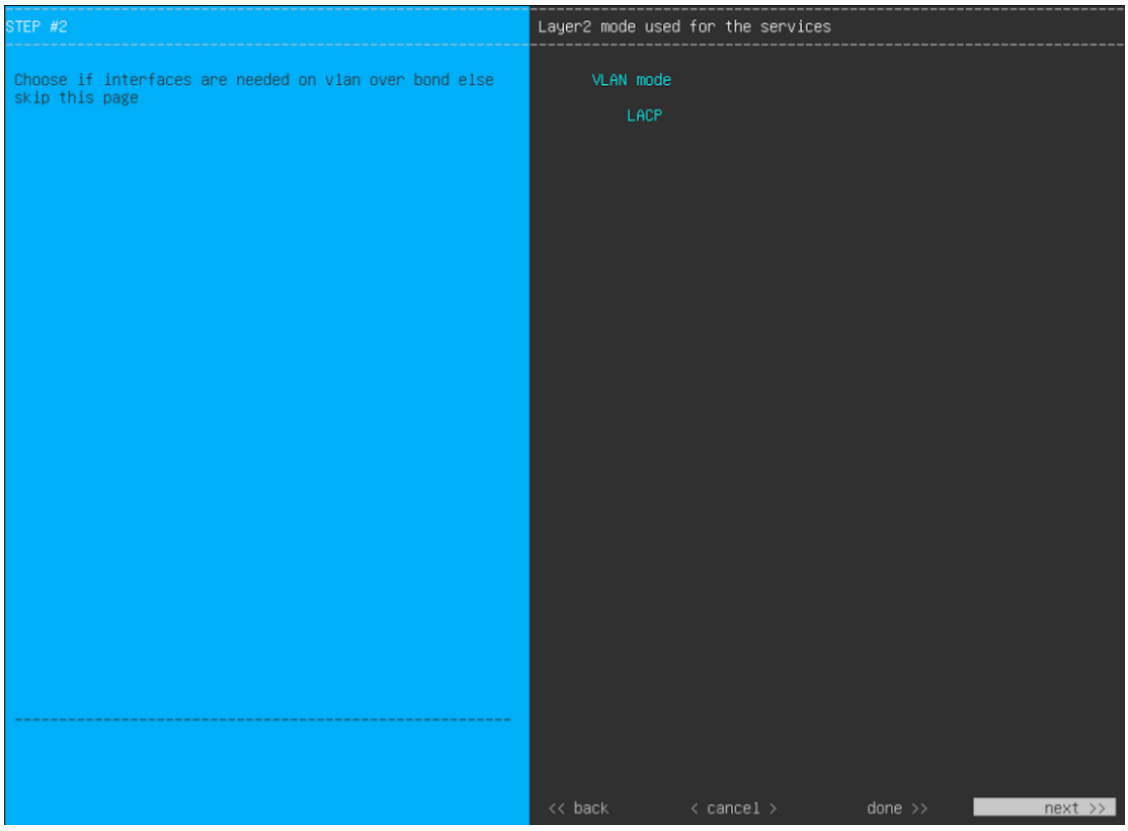
b) (Optional) Check the **Enable FIPS Mode** check box to enable FIPS mode on your Cisco DNA Center appliance.

See FIPS Mode Support, on page 22 for things to keep in mind when enabling FIPS mode on an appliance.

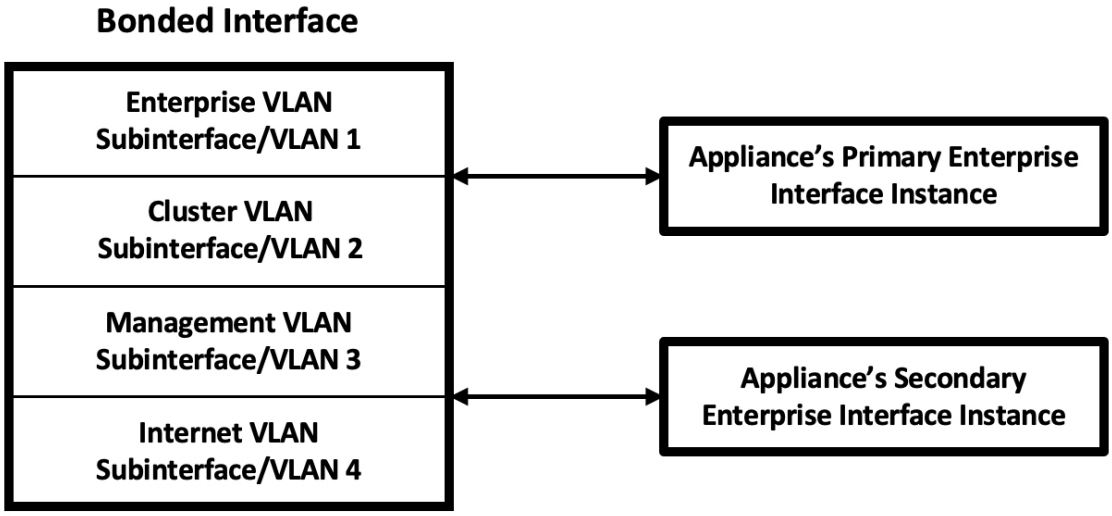
Important In the next wizard screen, you can enable the **VLAN mode** feature, which creates a single bonded interface that connects to your network using both the primary and secondary instance of your appliance's Enterprise interface. This feature is not commonly used, so only enable it if you know it's required by your Cisco DNA Center deployment.

- If this is the case, complete the next step.
- Otherwise, click **next>>** in the next wizard screen without making any selections. You can enable the NIC bonding functionality that was described previously in this guide in the wizard's Enterprise and Intracluster interface configuration screens.

Step 7 (Optional) Do the following to enable Layer 2 port channel mode (with VLAN tagging) for the appliance. After making your selections, click **next>>** to proceed.



a) Choose the **VLAN mode** option to enable dot1q/VLAN trunking and convert your appliance's Enterprise, Cluster, Management, and Internet interfaces into VLAN subinterfaces that reside on the bonded interface (as illustrated in the following figure). By default, this interface operates in Active-Backup mode (which enables HA).



b) If you want this interface to operate in LACP mode instead (which enables load balancing and higher bandwidth), you must also choose the **LACP** option.

c) When you enter the settings for your appliance's Enterprise and Cluster interfaces, ensure that you enter a unique VLAN ID in the **VLAN ID of Interface** field for the subinterfaces you want to configure on the virtual bonded interface.

Important Even though one physical appliance interface (the Enterprise interface) is connected, you can configure all of the subinterfaces that reside on the virtual bonded interface.

The wizard discovers all of the ports on the appliance and presents them to you one by one, in separate screens, in the following order:

a. (Required) 10-Gbps Enterprise Port—Network Adapter #1

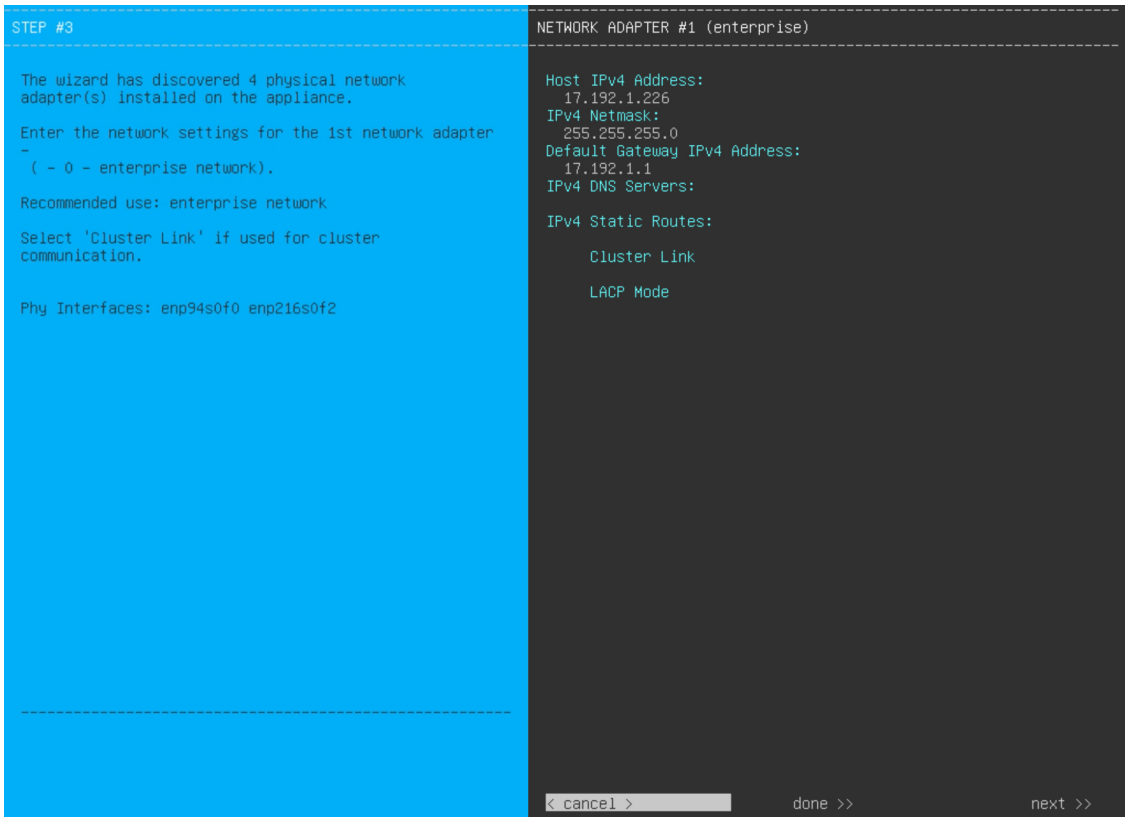
b. (Required) 10-Gbps Cluster Port—Network Adapter #2

c. (Optional) 1-Gbps/10-Gbps Management Port—Network Adapter #3

d. (Optional) 1-Gbps/10-Gbps Internet Port—Network Adapter #4

If the wizard fails to display either or both of the Enterprise and Cluster ports during the course of configuration, it might indicate that these ports are nonfunctional or disabled. These two ports are required for Cisco DNA Center functionality. If you discover that they are nonfunctional, choose **cancel** to exit the configuration wizard immediately. Be sure that you have completed all of the steps provided in Execute Preconfiguration Checks before resuming the configuration or contacting the Cisco Technical Assistance Center (for more information, see the "Get Assistance from the Cisco TAC" topic in the Release Notes document).

Step 8 The wizard first presents the 10-Gbps Enterprise port as **NETWORK ADAPTER #1**. As explained in Interface Cable Connections, this is a required port used to link the appliance to the enterprise network. Apply the host IP address, netmask, and other values that are appropriate for this purpose (see Required IP Addresses and Subnets and Required Configuration Information for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #1**, as shown in the table below.

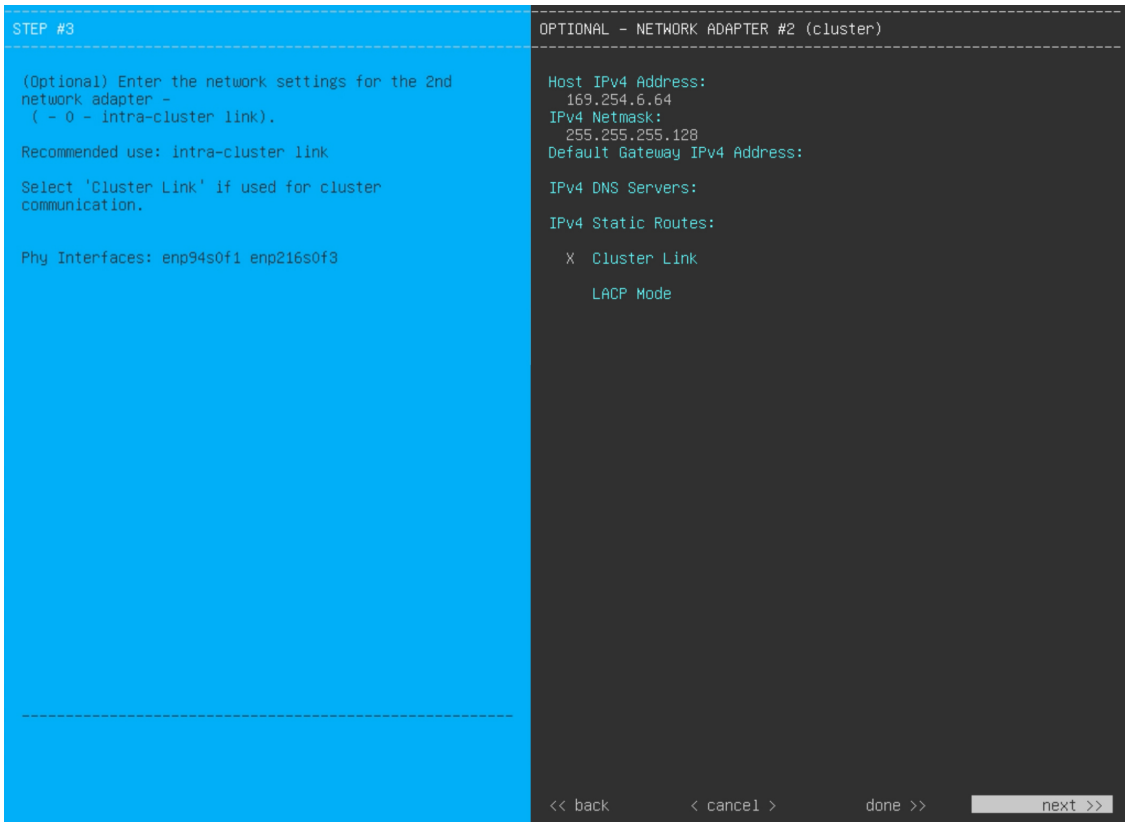
Table 8: Secondary Node Entries for Network Adapter #1: 10-Gbps Enterprise Port

Host IPv4/IPv6 Address field	Enter the IP address for the Enterprise port. This is required.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following if you entered an IP address: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4/IPv6 DNS Servers field	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. **Important** For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.

IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: <*network*>/<*netmask*>/<*gateway*>. This is usually required on the Cisco DNA Center Management port only.
Vlan Id of Interface field	Enter the VLAN ID that will be tagged over the LACP link to be created for the appliance you are configuring. **Note** This field is displayed only if you set the Layer 2 LACP port channel mode for the appliance by choosing both options in the previous step.
Cluster Link field	Leave this field blank. It is required on the Cluster port only.
LACP Mode field	Do one of the following: • Leave this field blank and the port will operate in **Active-Backup** mode. This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active. • Check the check box to enable **LACP** mode on this port. This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth. For more information about Cisco DNA Center's implementation of NIC bonding, see NIC Bonding Overview. **Note** This field is displayed if you didn't choose any of the options in the previous step.

After you finish entering the configuration values, click **next>>** to proceed. The wizard validates the values you entered and issues an error message if any are incorrect. If you receive an error message, check that the value you entered is correct, then reenter it. If needed, click **<<back** to reenter it.

Step 9 After successful validation of the Enterprise port values you entered, the wizard presents the 10-Gbps Cluster port and presents it as **NETWORK ADAPTER #2**. As explained in Interface Cable Connections, this port is used to link the appliance to the cluster, so apply the host IP address, netmask, and other values that are appropriate for this purpose (see Required IP Addresses and Subnets and Required Configuration Information for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #2**, as shown in the table below.

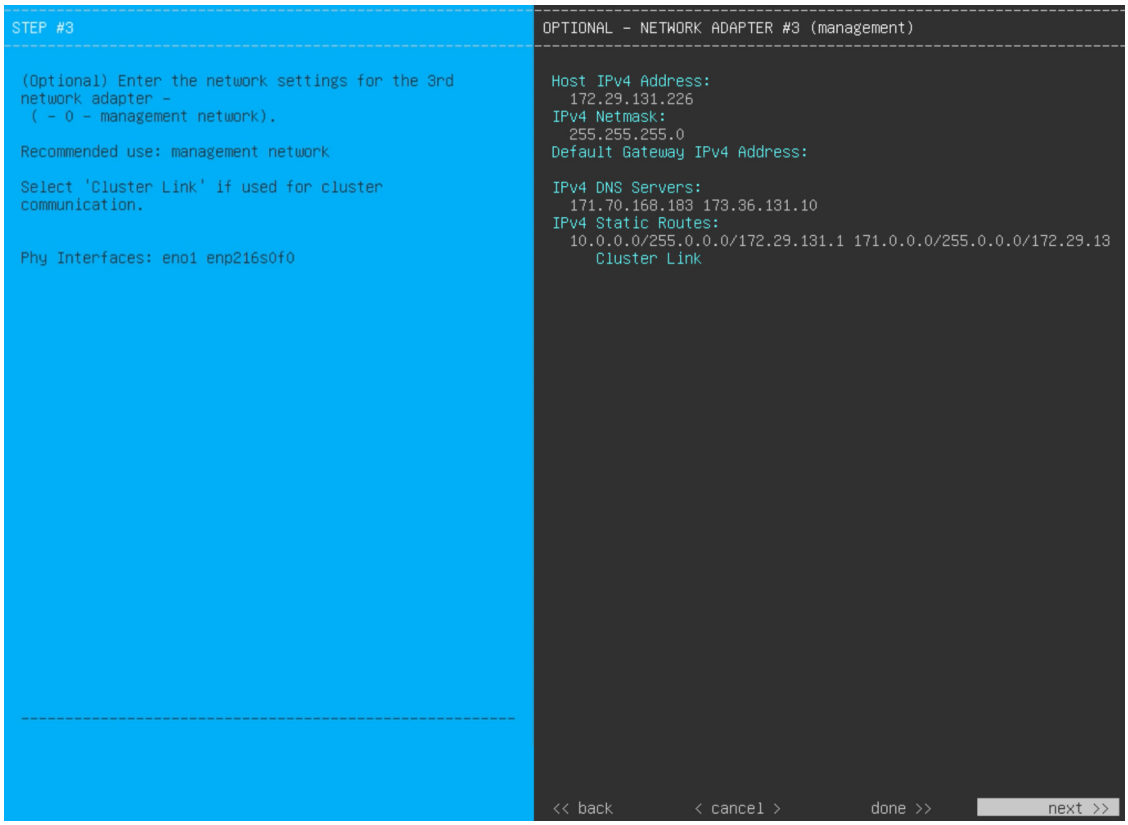
Table 9: Secondary Node Entries for Network Adapter #2: 10-Gbps Cluster Port

Host IPv4/IPv6 address field	Enter the IP address for the Cluster port. This is required. Note that you cannot change the address of the Cluster port later.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following if you entered an IP address: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4/IPv6 DNS Servers field	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. **Important** For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.

IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*. This is usually required on the Management port only.
Vlan Id of Interface field	Enter the VLAN ID that will be tagged over the LACP link to be created for the appliance you are configuring. **Note** This field is displayed only if you set the Layer 2 LACP port channel mode for the appliance by choosing both options in Step 7.
Cluster Link field	Check the check box to set this port as the link to a Cisco DNA Center cluster. This is required on the Cluster port only.
LACP Mode field	Do one of the following: • Leave this field blank and the port will operate in **Active-Backup** mode. This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active. • Check the check box to enable **LACP** mode on this port. This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth. For more information about Cisco DNA Center's implementation of NIC bonding, see NIC Bonding Overview. **Note** This field is displayed if you didn't choose any of the options in Step 7.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

Step 10 After successful validation of the Cluster port values you entered, the wizard presents the 1-Gbps/10-Gbps Management port and presents it as **NETWORK ADAPTER #3**. As explained in Interface Cable Connections, this port is used to access the Cisco DNA Center GUI from your management network. Apply the host IP address, netmask, and other values that are appropriate for this purpose (see Required IP Addresses and Subnets and Required Configuration Information for the values to enter).



Enter the configuration values for **NETWORK ADAPTER #3**, as shown in the table below.

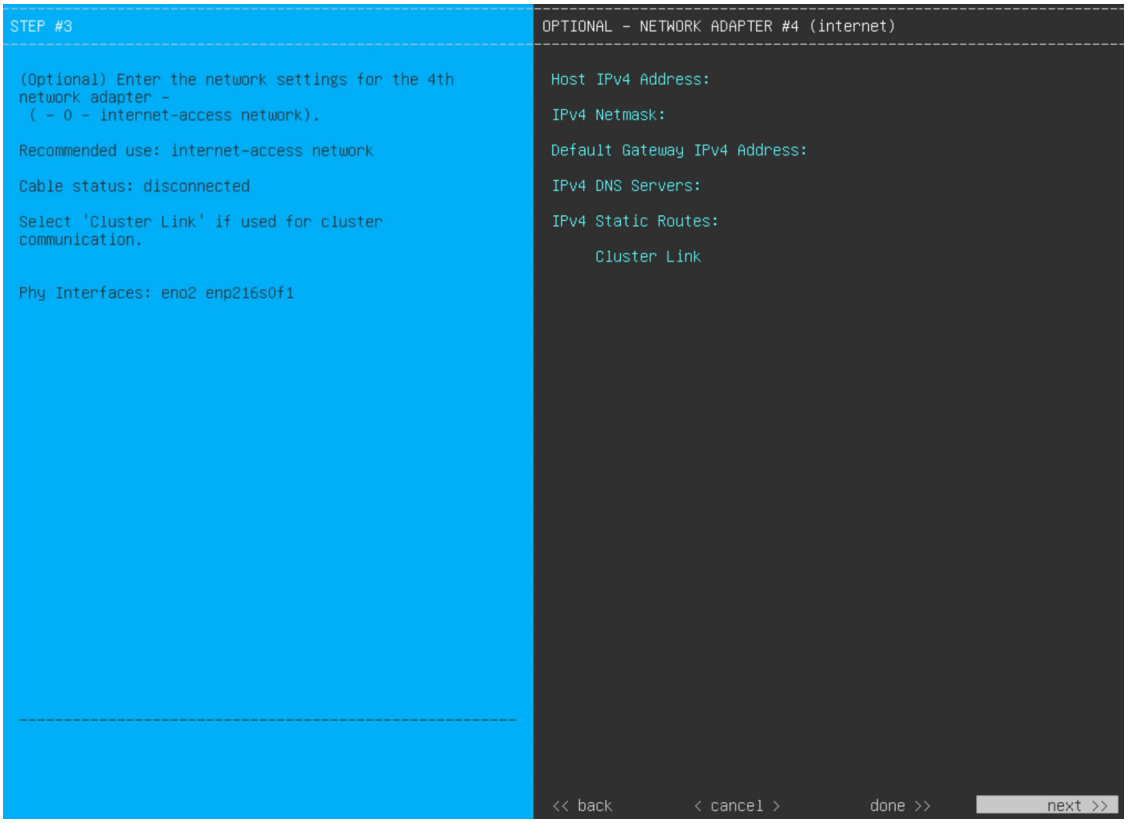
Table 10: Secondary Node Entries for Network Adapter #3: 1-Gbps/10-Gbps Management Port

Host IPv4/IPv6 address field	Enter the IP address for the Management port. This is required only if you are using this port to access the Cisco DNA Center GUI from your management network; otherwise, you can leave it blank.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the port. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.

IPv4/IPv6 DNS Servers field	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. **Important** • For NTP, ensure port 123 (UDP) is open between Cisco DNA Center and your NTP server. • For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*.
Cluster Link field	Leave this field blank. It is required on the Cluster port only.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

Step 11 After successful validation of the Management port values you entered, the wizard presents the 1-Gbps/10-Gbps Internet port as **NETWORK ADAPTER #4**. As explained in Interface Cable Connections, this is an optional port used to link the appliance to the Internet when you cannot do so through the 10-Gbps Enterprise port. Apply the host IP address, netmask, and other values that are appropriate for this purpose (see Required IP Addresses and Subnets and Required Configuration Information for the values to enter).



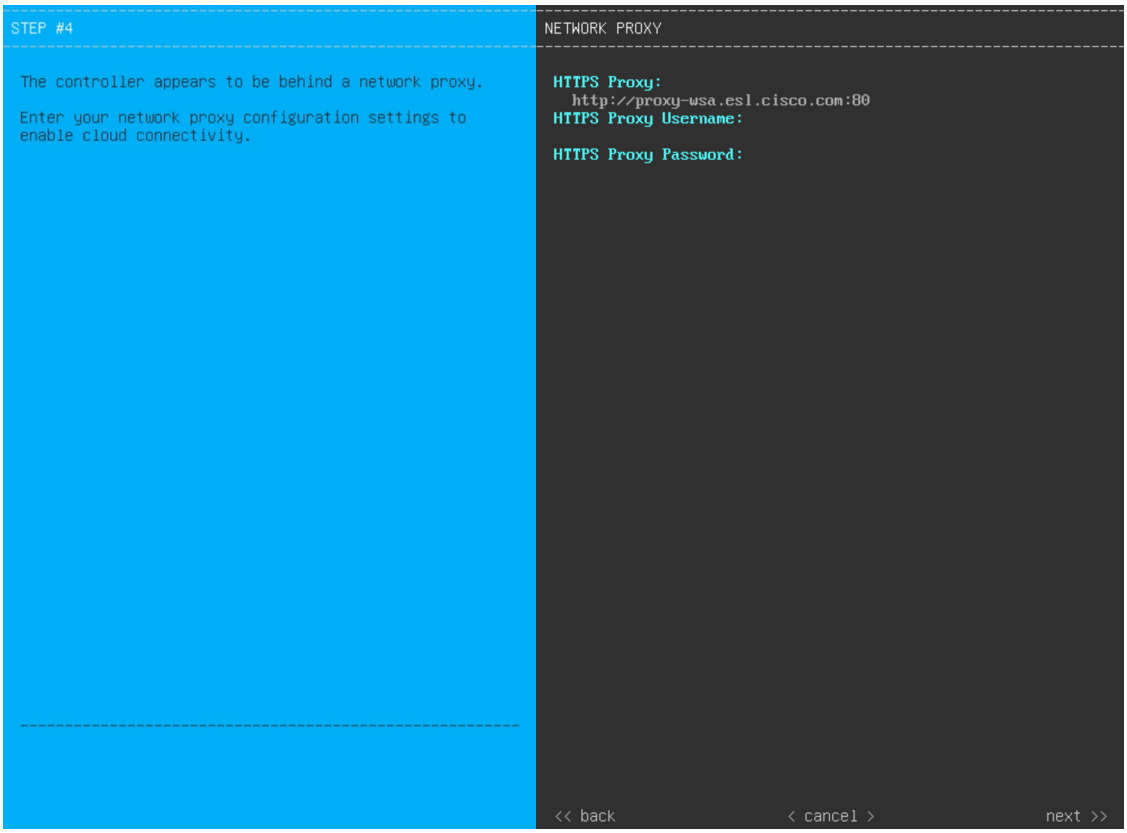
Enter the configuration values for **NETWORK ADAPTER #4**, as shown in the table below.

Table 11: Secondary Node Entries for Network Adapter #4: 1-Gbps/10-Gbps Internet Port

Host IPv4/IPv6 address field	Enter the IP address for the Internet port. This is required only if you are using the Internet port for internet connection; otherwise, you can leave it blank.
IPv4 Netmask/IPv6 Prefix Length field	Do one of the following: • If you selected IPv4 addressing, enter the netmask for the port's IP address. This is required. • If you selected IPv6 addressing, enter the prefix length (in bits). Valid values range from 10 through 127.
Default Gateway IPv4/IPv6 address field	Enter a default gateway IP address to use for the Internet port. **Important** Ensure that you enter a default gateway IP address for at least one of your appliance's interfaces. Otherwise, you will not be able to complete the configuration wizard.
IPv4/IPv6 DNS Servers field	Enter the IP address of the preferred DNS server. If you are entering multiple DNS servers, separate the IP addresses in the list with spaces. **Important** For each appliance in your cluster, configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS servers for an appliance.
IPv4/IPv6 Static Routes field	Enter one or more static routes in the following format, separated by spaces: *<network>/<netmask>/<gateway>*. This is usually required on the Management port only.
Cluster Link field	Leave this field blank. It is required on the Cluster port only.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your network adapter configurations.

Step 12 After the network adapter configuration is complete, the wizard prompts you to enter configuration values for the **NETWORK PROXY** that you are using, as shown below.



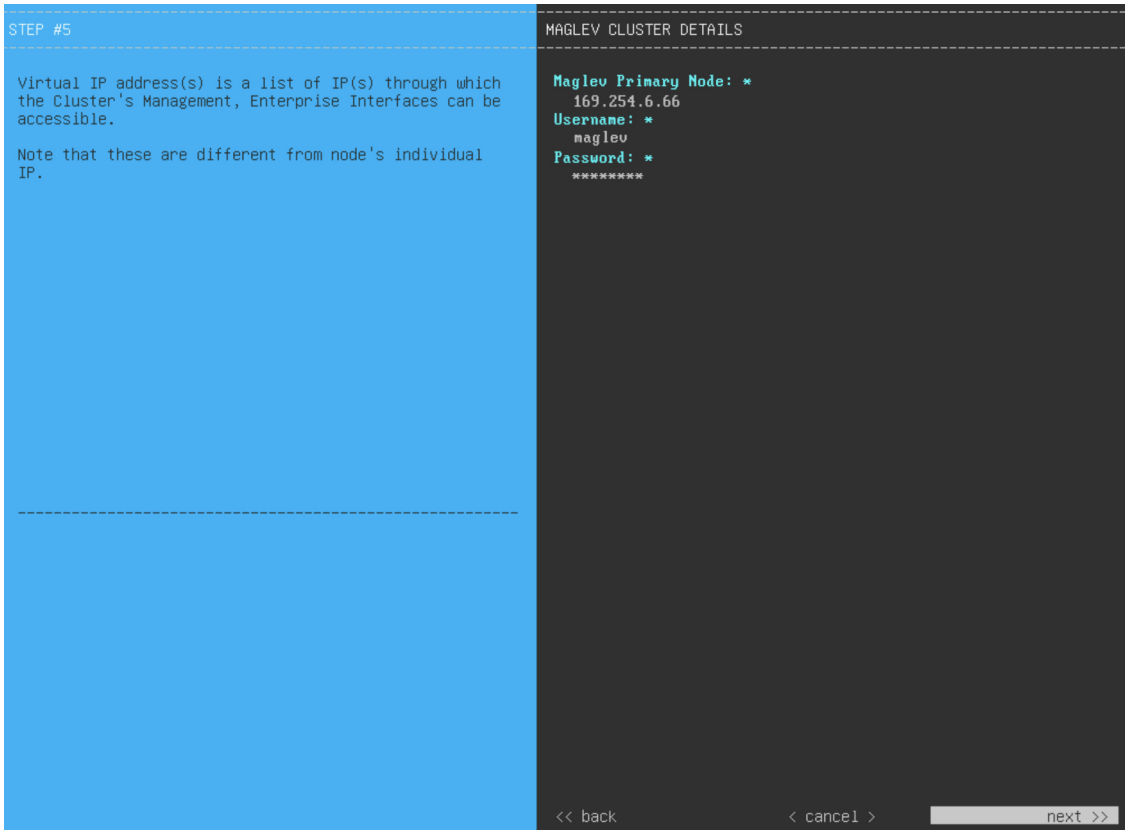
Enter the configuration values for the **NETWORK PROXY**, as shown in the table below.

Table 12: Secondary Node Entries for Network Proxy

HTTPS Proxy field	Enter the URL or host name of an HTTPS network proxy used to access the Internet. **Note** • Connection from Cisco DNA Center to the HTTPS proxy is supported only through HTTP in this release. • If you enter an IPv6 URL that contains a port number, enclose the IP address portion of the URL in square brackets. In this example, 443 is the port number: http://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:443/
HTTPS Proxy Username field	Enter the user name used to access the network proxy. If no proxy login is required, leave this field blank.
HTTPS Proxy Password field	Enter the password used to access the network proxy. If no proxy login is required, leave this field blank.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

Step 13 After the network proxy configuration completes, the wizard prompts you to identify the Cluster port on the primary node and primary node login details in **MAGLEV CLUSTER DETAILS** (as shown below).



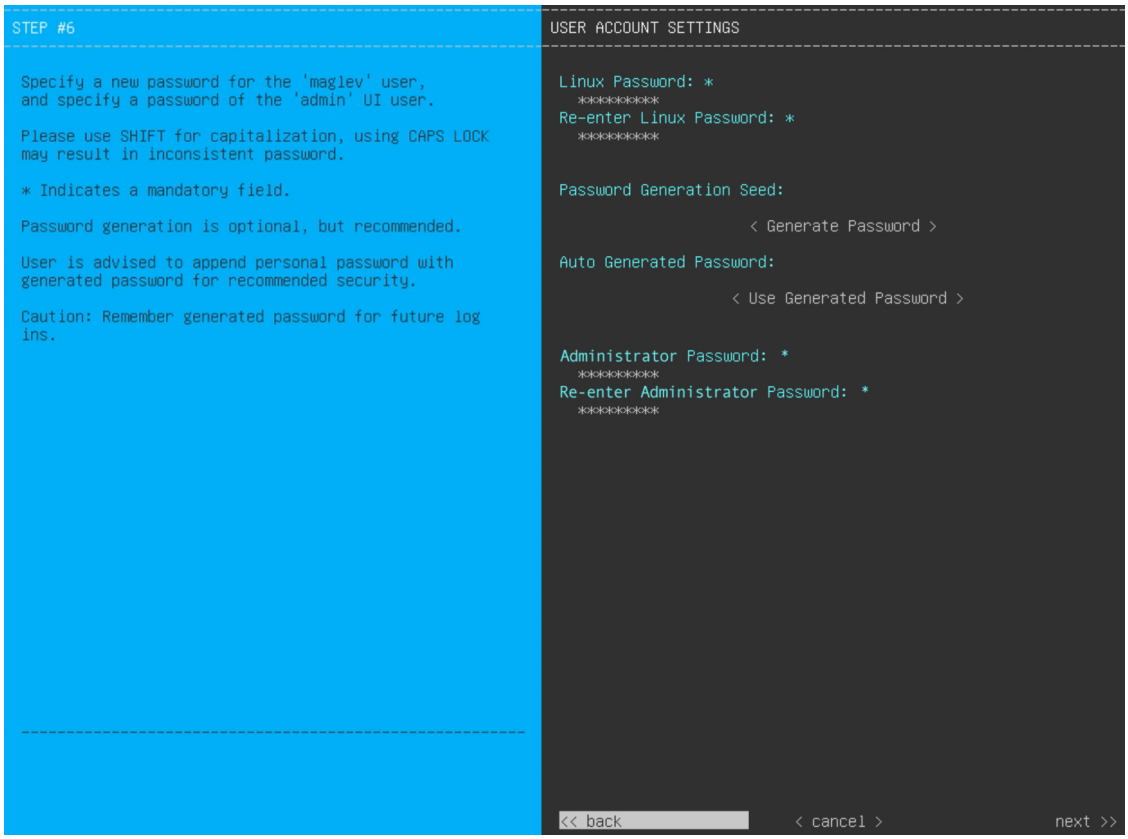
Enter the values for **MAGLEV CLUSTER DETAILS**, as shown in the table below.

Table 13: Secondary Node Entries for Maglev Cluster Details

Maglev Primary Node field	Enter the IP address of the Cluster port on the primary node in the cluster. If you have followed the recommendations for port assignment, this will be the IP address of Network Adapter #2 on the primary node.
Username field	Enter **maglev**.
Password field	Enter the Linux password you configured on the primary node.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

Step 14 After you have entered the cluster details, the wizard prompts you to enter the **USER ACCOUNT SETTINGS** values, as shown below.



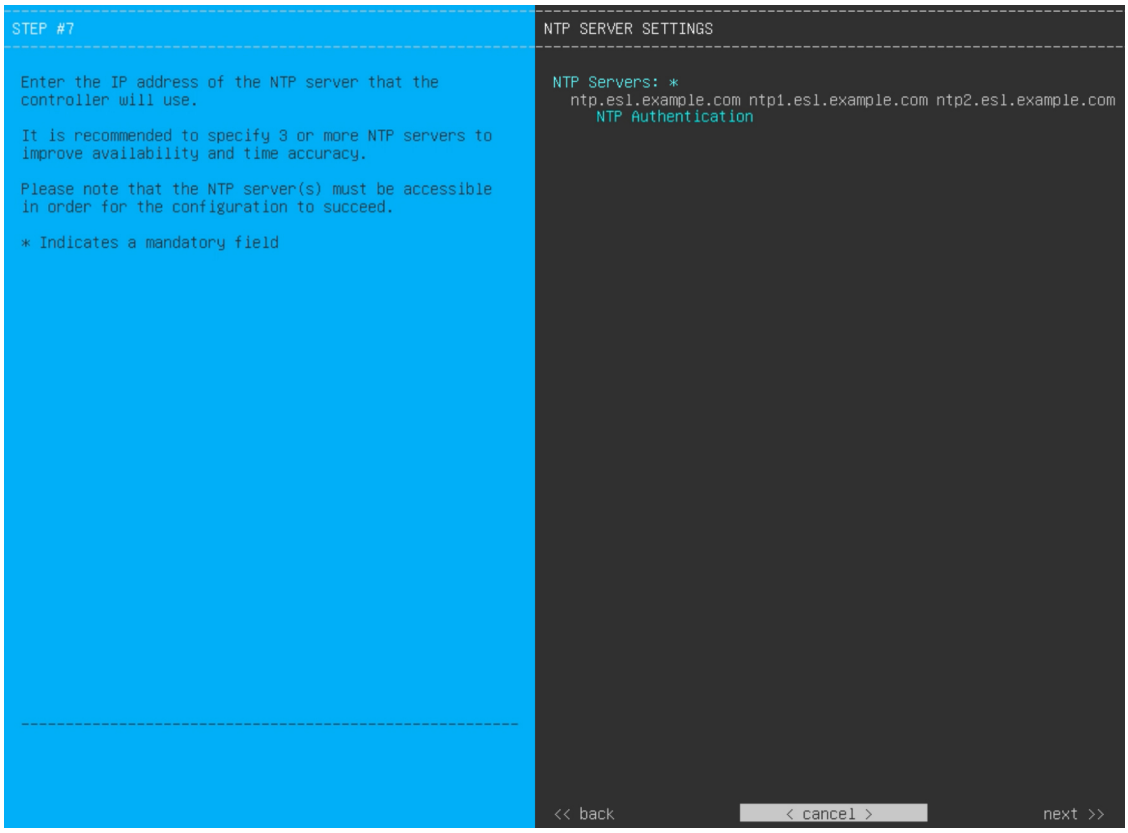
Enter the values for **USER ACCOUNT SETTINGS**, as shown in the table below.

Table 14: Secondary Node Entries for User Account Settings

Linux Password field	Enter a Linux password for the maglev user.
Re-enter Linux Password field	Confirm the Linux password by entering it a second time.
Password Generation Seed field	If you do not want to create the Linux password yourself, enter a seed phrase in this field and then press <**Generate Password**> to generate the password.
Auto Generated Password field	(Optional) The seed phrase appears as part of a random and secure password. If required, you can either use this password as is, or you can further edit this auto-generated password. Click <**Use Generated Password**> to save the password.
Administrator Password field	Enter a password for the default admin superuser, used to log in to Cisco DNA Center for the first time.
Re-enter Administrator Password field	Confirm the administrator password by entering it a second time.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens.

Step 15 After you have entered the user account details, the wizard prompts you to enter **NTP SERVER SETTINGS** values.

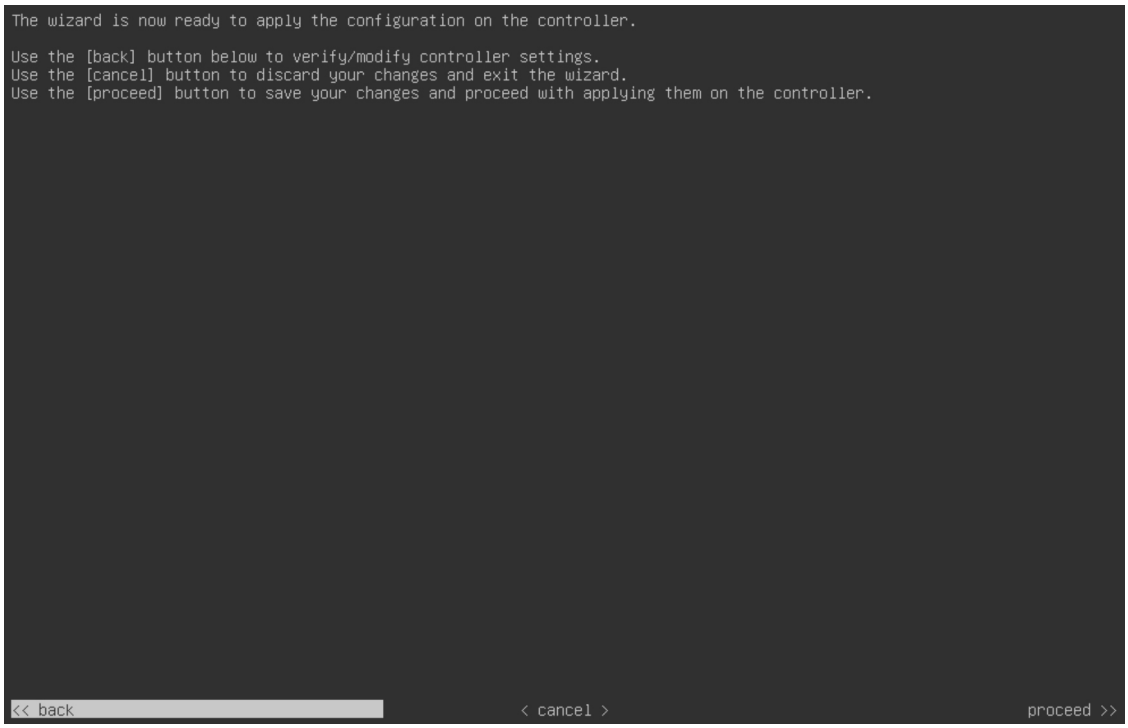


Enter the values for **NTP SERVER SETTINGS**, as shown in the table below.

NTP Servers field	Enter one or more NTP server addresses or hostnames, separated by spaces. At least one NTP address or hostname is required. For a production deployment, we recommend that you configure a minimum of three NTP servers.
NTP Authentication check box	To enable the authentication of your NTP server before it's synchronized with Cisco DNA Center, check this check box and then enter the following information: • The NTP server's key ID. Valid values range between 1 and 4294967295 (2^32-1). This value corresponds to the key ID that's defined in the NTP server's key file. • The SHA-1 key value associated with the NTP server's key ID. This 40-character hex string resides in the NTP server's key file. **Note** Ensure that you enter a key ID and key value for each NTP server that you configured in the previous field.

After you provide the necessary information, click **next>>** to proceed. Correct validation errors, if any, as you did in previous screens. The wizard validates and applies your NTP server configuration.

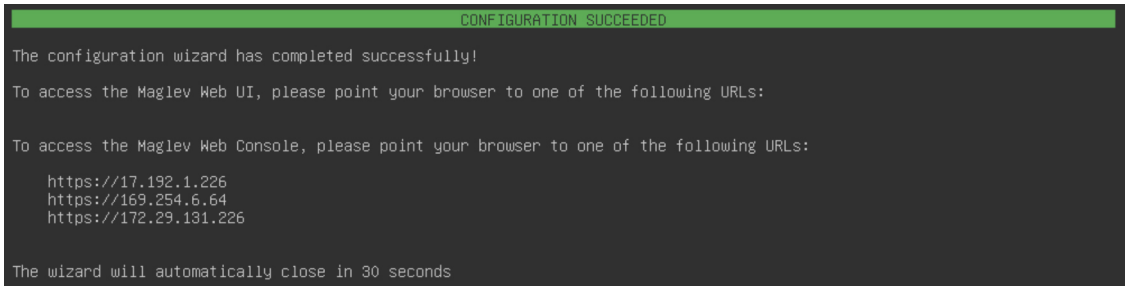
Step 16 When you are finished entering the NTP server settings, a final message appears, stating that the wizard is ready to apply the configuration (as shown below).



Click **proceed**>> to complete the configuration wizard.

The host will reboot automatically and display messages on the KVM console as it applies your settings and brings up services. This process can take several hours. You can monitor its progress via the KVM console.

At the end of the configuration process, the appliance power cycles again, then displays a **CONFIGURATION SUCCEEDED!** message.



What to do next

- If you have an additional appliance to deploy as the third and final node in the cluster, repeat this procedure.
- If you have finished adding hosts to the cluster, perform the first-time setup: First-Time Setup Workflow.

Upgrade to the Latest Cisco DNA Center Release

For information about upgrading your current release of Cisco DNA Center, see the *Cisco DNA Center Upgrade Guide*.