



First Time Setup Wizard

This chapter contains the following sections:


- [About the First Time Setup Wizard, on page 1](#)

About the First Time Setup Wizard

Use the First Time Setup wizard to set up your Cisco APIC for the first time.

- You can access the First Time Setup wizard when it automatically appears the first time you log into your Cisco APIC through the GUI.
- For Cisco APIC Releases 4.2(3) and later, you can also access the First Time Setup wizard when you



click the System Tools icon () in the upper right corner of the Cisco APIC GUI window, then select **What's New in APIC_release_number**.

The **Welcome to APIC** window appears, providing information on the new features that are part of this particular release.

To access the First Time Setup wizard, click **Begin First Time Setup** or **Review First Time Setup** at the bottom right of the window. The **Let's Configure the Basics** window appears, with links to the individual pages that you can use to set up your Cisco APIC.

When you have completed the initial setup that includes at least one BGP route reflector, the **Proceed to Summary** button is enabled. Click this button to view summary tiles of the configuration. Additional tiles appear under the heading **You Might Want To...**. These additional topics are optional but recommended.

The following sections provide more information for each of the first-time setup pages available from this window.

Fabric Membership

Use the **Fabric Membership** window to register the leaf and spine switches detected by the ACI fabric. You can also manually add leaf and spine switches to the fabric using the serial number listed on the box.




Note We recommend registering at least two leaf switches and two spine switches. You must register at least one leaf switch and one spine switch in order to proceed through the First Time Setup wizard.

The **Fabric Membership** window contains two sections:

- **Discovered:** This section provides information on newly-discovered but unregistered switches. These nodes will have a node ID of 0 and will have no IP address.
- **Registered:** This section provides information on all of the registered switches in your ACI fabric.

You can register a switch using either of these methods:

- If the switch is shown in the **Discovered** section, click the **Register** button next to that switch to open the **Create Fabric Node Member** window. Note that the **Pod ID** and **Serial Number** fields will be automatically populated in the **Create Fabric Node Member** window in this case.
- If the switch is not shown in the **Discovered** section, click the Action icon (), then select **Create Fabric Node Member** from the drop-down list.

In the **Create Fabric Node Member** window, enter the following information:

Field	Setting
Pod ID	Identify the pod where the node is located.
Serial Number	Required: Enter the serial number of the switch.
Node ID	<p>Required: Enter a number greater than 100. The first 100 IDs are reserved for APIC appliance nodes.</p> <p>Note We recommend that leaf nodes and spine nodes be numbered differently. For example, number leafs in the 100 range (such as 101, 102) and number spines in the 200 range (such as 201, 202).</p> <p>Note After the node ID is assigned, it cannot be updated. After the node has been added to the Registered Nodes tab table, you can update the node name by right-clicking the table row and choosing Edit Node and Rack Name.</p>
Switch Name	The node name, such as leaf1 or spine3.

Field	Setting
Node Type	<p>Choose the assigned node role. The options are:</p> <ul style="list-style-type: none"> • leaf <p>Check one of the following boxes if applicable:</p> <ul style="list-style-type: none"> • Is Remote • Is Virtual • Is Tier-2 Leaf <ul style="list-style-type: none"> • spine <p>Check the following box if applicable:</p> <ul style="list-style-type: none"> • Is Virtual <ul style="list-style-type: none"> • unknown

Click **Submit** when you have completed the information in the **Create Fabric Node Member** window, then click **Continue** in the **Fabric Membership** to continue to the next window in the First Time Setup wizard.

BGP

Use the **BGP** window to configure ACI fabric route reflectors, which use multiprotocol BGP (MP-BGP) to distribute external routes within the fabric. Once you have enabled the route reflectors in the ACI fabric, you can configure connectivity to external networks.



Note Select spine switches to configure as route reflectors. You must configure at least one route reflector in order to proceed through the First Time Setup wizard. If you do not see any spine switches in the table in this window, verify that the switch is registered with the correct type or has been discovered by APIC.

In the **BGP** window, check the box next to the spine switches that you want to use as route reflectors and enter the ASN for this spine switch in the **Autonomous System Number** field. Click **Save and Continue** to continue to the next window in the First Time Setup wizard.

Out-of-Band Management

Use the **Out Of Band Management** window to configure the management interface IP address for leaf switches, spine switches, and APIC nodes to connect to the Out of Band (OOB) network. Select several nodes to begin assigning IP addresses to them.



Note The First Time Setup wizard helps with configuring nodes that have not already been configured for Out of Band management.

Click the box next to the nodes that you want to configure for Out of Band management, or click the box next to **Select All** to select all the nodes in the list. Then click **Configure OOB IPs for selected nodes** to configure the nodes for Out of Band management.

Enter the necessary information in the following fields:

- **IPv4 Starting Address:** The IPv4 address and netmask that you use to access the switches through the GUI, CLI, or API.
- **IPv4 Gateway:** The IPv4 default gateway address for communication to external networks using out-of-band management.
- **IPv6 Starting Address:** The IPv6 address and netmask that you use to access the switches through the GUI, CLI, or API.
- **IPv6 Gateway:** The IPv6 default gateway address for communication to external networks using out-of-band management.

The fields in the Selected Nodes area are automatically populated, based on the information that you enter in the fields above. For example, if you entered 192.0.2.1/24 in the **IPv4 Starting Address** field above, the values in the IPv4 Address column in the Selected Nodes area would be automatically populated with these values:

- First node: 192.0.2.1/24
- Second node: 192.0.2.2/24
- Third node: 192.0.2.3/24
- Fourth node: 192.0.2.4/24

Double-click on an entry in the table to change any of the automatically-populated entries.

Click **Edit Node Selection** if you want to change the nodes that you had selected to configure for Out of Band management.

Click **Save and Continue** to continue to the next window in the First Time Setup wizard.

DNS

Use the **DNS** window to configure DNS servers and search domains to allow leaf switches, spine switches and APIC nodes to query DNS names. The OOB connection will be used for DNS communication.



Note The First Time Setup wizard configures DNS servers and DNS domains under the **default** DNS Policy.

To configure the DNS servers, click + in the DNS Servers area, then enter the following information:

- **Address:** Enter the provider address.
- **Preferred:** Check the check box if you want to have this address as the preferred provider.
- **Status:** Provides the status of the configuration request.

Click **Update**, then repeat this process to configure additional DNS servers, if necessary.

To configure the search domains, click + in the Search Domains area, then enter the following information:

- **Name:** Enter the domain name (cisco.com).
- **Default:** Check the check box to make this domain the default domain. You can have only one domain name as the default.
- **Status:** Provides the status of the configuration request.

Click **Update**, then repeat this process to configure additional search domains, if necessary.

To delete an entry either from the DNS Servers table or from the Search Domains table, select the entry that you would like to delete, then click the trash can icon in that table.

Click **Save and Continue** to continue to the next window in the First Time Setup wizard.

NTP

Use the **NTP** window to configure a timezone and assign NTP servers to synchronize leaf switches, spine switches, and APIC nodes to a valid time source. The OOB connection will be used for NTP communication.



Note The First Time Setup wizard configures servers under the **default** NTP Policy.

In the Display Format area, click **local** to display the date and time in a local time zone format, or click **utc** to display the date and time in the UTC time zone format. The default is **local**.

If you selected **local** above, in the Time Zone area, click the drop-down arrow to choose the time zone for your domain. You can also type in the drop down menu area to filter the drop down options. The default is **Coordinated Universal Time**.

To configure the NTP servers, click + in the NTP Servers area, then enter the following information:

- **Host Name/IPAddress:** Enter the host name and IP address of the NTP server.
- **Preferred:** If you are creating multiple providers, check the **Preferred** check box for the most reliable NTP source.
- **Status:** Provides the status of the configuration request.

Click **Update**, then repeat this process to configure additional NTP servers, if necessary.

To delete an entry from the NTP Servers table, select the entry that you would like to delete, then click the trash can icon in that table.

Click **Save and Continue** to continue to the next window in the First Time Setup wizard.

Global Configurations

Use the **Global Configurations** window to configure certain areas, which we recommend as best practices during the first time set up of your ACI fabric. Click **Okay, Got it!** when you are ready to configure these areas:

- [Subnet Check, on page 6](#)
- [Domain Validation, on page 6](#)

- [Intermediate System to Intermediate System for redistributed routes, on page 6](#)
- [IP Aging Administrative State, on page 6](#)
- [Rogue EP Control, on page 7](#)
- [COOP Group Policy, on page 7](#)



Note Some settings in this window are configurable after the First Time Setup, such as the Subnet Check and Domain Validation settings, which can be configured in the **Fabric Wide Setting Policy** page (**System > System Settings > Fabric-Wide Settings**). However, configuring those settings after the First Time Setup might cause issues with other existing configurations. For example, enabling the **Enforce Subnet Check** and **Enforce Domain Validation** settings in the **Fabric Wide Setting Policy** page could break a configured L3Out connection without the proper policy chain in place for the interface or for a statically-assigned port to an EPG.

Subnet Check

This feature disables IP address learning outside of subnets configured in a VRF, for all other VRFs.

This feature enforces subnet checks at the VRF level, when the Cisco Application Centric Infrastructure (Cisco ACI) learns the IP address as an endpoint from the data plane. If you put a check in the box for this option, the fabric will not learn IP addresses from a subnet other than the one configured on the bridge domain. This feature prevents the fabric from learning endpoint information in this scenario.

Check the box next to **Enforce** to enable the subnet check feature, which is highly recommended.

Domain Validation

This feature enforces a validation check if a static path is added but no domain is associated to an EPG.

When enabled, a validation check is performed when a static path is added to an EPG, to determine if the path is part of a domain that is associated with the EPG. The scope of this policy is fabric-wide. After configuration, a policy is pushed to each leaf switch as it comes up.

Check the box next to **Enforce** to enable the domain validation feature, which is highly recommended.

Intermediate System to Intermediate System for redistributed routes

This is the IS-IS metric that is used for all imported routes into IS-IS. Configuring a metric lower than 64 (max) with this option, such as 63, allows ACI switches to prefer routes from stable spines until the routing convergence is achieved on a new spine.

Enter the appropriate value in the **IS-IS metric** field.

IP Aging Administrative State

Enabling this policy allows ACI to track each IP individually and age out unused IPs efficiently. Otherwise, unused IPs remain learned until the base MAC address ages out. This does not affect remote endpoints.

When enabled, the IP aging policy ages unused IPs on an endpoint. In this situation, the IP aging policy sends ARP requests (for IPv4) and neighbor solicitations (for IPv6) to track IPs on endpoints. If no response is given, the policy ages the unused IPs.

Following are the options for this field:

- **Disabled:** The default setting. APIC disregards the IP aging policy.
- **Enabled:** APIC observes the IP aging policy.

We highly recommend enabling this feature.

Rogue EP Control

A rogue endpoint can attack top of rack (ToR) switches through frequently, repeatedly injecting packets on different ToR ports and changing 802.1Q tags (emulating endpoint moves), resulting in IP and MAC addresses being learned rapidly in different EPGs and ports. Misconfigurations can also cause frequent IP and MAC address changes (moves).

The Rogue EP Control feature addresses this vulnerability. Enabling this policy allows ACI to detect and delete unauthorized endpoints.

Following are the options for this field:

- **Disabled:** The default setting. APIC disregards the Rogue EP Control policy.
- **Enabled:** APIC observes the Rogue EP Control policy.

We highly recommend enabling this feature.

Additional settings for Rogue EP Control, such as Rogue EP Detection Interval, Rogue EP Detection Multiplication Factor, and Hold Interval, are available through the Endpoint Controls panel. To access the Endpoint Controls panel, on the menu bar, click **System > System Settings > Endpoint Controls**, then click the **Rogue EP Control** tab.

Following are the valid and default settings for the fields in the **Rogue EP Control** tab in the **Endpoint Controls** window:

- **Rogue EP Detection Interval:** Valid values are from 0 to 65535 seconds. Default value is 60.
- **Rogue EP Detection Multiplication Factor:** Valid values are from 2 to 65535. Default value is 4.
- **Hold Interval:** Valid values are from 1800 to 3600 seconds. Default value is 1800.

COOP Group Policy

Council of Oracle Protocol (COOP) is used to communicate the mapping information (location and identity) to the spine proxy. A leaf switch forwards endpoint address information to the spine switch 'Oracle' using Zero Message Queue (ZMQ). COOP running on the spine nodes will ensure all spine nodes maintain a consistent copy of endpoints and location information in the mapping database.

COOP protocol supports two ZMQ authentication modes:

- **Compatible Type:** The default setting. COOP accepts both MD5 authenticated and non-authenticated ZMQ connections for message transportation.



Note

The APIC manages the token used as MD5 password for COOP. This token is automatically rotated by APIC every hour. This token cannot be displayed.

- **Strict Type:** COOP allows MD5 authenticated ZMQ connections only.

We highly recommend the Strict Type setting for the COOP Group Policy.

SNMP

Use the SNMP window to allow leaf switches, spine switches, and APIC controllers to be polled by SNMP or to allow APIC to send SNMP trap messages. This configuration is optional.



Note For detailed information about configuring SNMP, see "Configuring SNMP for Monitoring and Managing Devices" in the *Cisco APIC Troubleshooting Guide*.

First, decide whether you'll rely on SNMP polling or whether APIC will send SNMP trap messages. You can also choose both methods.

SNMP Polling

Configure SNMP polling to allow an external management station to query leaf switches, spine switches, and APIC controllers periodically for status information.



Note The First Time Setup wizard configures SNMP settings under the **default** SNMP policy.

Select **Polling** and enter the following information:

- **Contact:** Enter user information for the SNMP contact.
- **Location:** Enter the SNMP agent location.
- **Community Strings:** To configure a community string, click + in the Community Strings bar, then enter the string and click **Update**.
- **Client Group Policies:** A client group is a group of client addresses that allows SNMP access to switches or controllers. To configure a client group, click + in the Client Group Policies bar, then configure the **Create SNMP Client Group Profile** dialog box.
- **SNMPv3 Users:** To configure SNMPv3 users, click + in the SNMPv3 Users bar, then configure the **Create User Profile** dialog box.

SNMP Traps

SNMP traps enable an agent, such as APIC, to notify an external management station of significant events by sending an unsolicited SNMP message. An SNMP agent sends traps to a configured trap destination.



Note The First Time Setup wizard configures SNMP trap settings under the **common** monitoring policy.

To configure an SNMP trap, select **Traps**, click + in the Trap Destinations bar, then enter the following information:

- **Host Name/IP:** Enter an IP address or a fully qualified domain name for the destination host.
- **Port:** Choose a port number. The range is 0 (unspecified) to 65535. The default is 162.
- **Version:** Choose the SNMP version. The supported versions are v1, v2c, and v3.
- **Community:** Enter a community string. SNMP community strings can't contain the @ symbol.
- **v3 Security Level:** For SNMP version v3, choose whether authentication is required. With authentication, choose whether to require privacy.

When you configure an SNMP trap destination using the First Time Setup Wizard, APIC creates the following entities, named using the host information and port number from the trap configuration:

- A monitoring destination group named `snmpGrp-<host>-<port>`, such as `snmpGrp-10.1.2.3-162`. This group is created in **Admin > External Data Collectors > Monitoring Destinations > SNMP**.
- An SNMP source named `snmpSrc-<host>-<port>`, such as `snmpSrc-10.1.2.3-162` as a source for the monitoring destination group. This SNMP source is created in **Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Callhome/Smart Callhome/SNMP/Syslog/TACACS** under the **SNMP** tab.

Syslog

Use the Syslog window to configure remote system log (syslog) destinations for the ACI fabric. APIC collects and exports syslog data to a syslog monitoring destination for logging and evaluation. This configuration is optional.



Note The First Time Setup wizard configures syslog destinations under the **common** monitoring policy.

To configure a syslog destination, click + in the Syslog Destinations bar, then enter the following information:

- **Host:** Enter an IP address or a fully qualified domain name for the destination host.
- **Port:** Choose a port number. The range is 0 (unspecified) to 65535. The default is 514.
- **Severity:** Select the minimum severity level for messages sent to this destination. APIC won't send messages with a severity level below this setting to this destination. The default minimum severity level is **warnings**.
- **Forwarding Facility:** Select a value to be included in syslog messages to this destination. The facility is a user-defined value that can be used for any purpose.
- **Admin State:** Select **enabled** to allow the sending of syslog messages to this destination.

When you configure a syslog destination using the First Time Setup Wizard, APIC creates the following entities, named using the host information and port number from the configuration:

- A monitoring destination group named `syslogGrp-<host>-<port>`, such as `syslogGrp-10.1.2.3-162`. This group is created in **Admin > External Data Collectors > Monitoring Destinations > Syslog**.
- A syslog source named `syslogSrc-<host>-<port>`, such as `syslogSrc-10.1.2.3-162` as a source for the monitoring destination group. This syslog source is created in **Fabric > Fabric Policies > Policies**

> **Monitoring** > **Common Policy** > **Callhome/Smart Callhome/SNMP/Syslog/TACACS** under the **Syslog** tab.