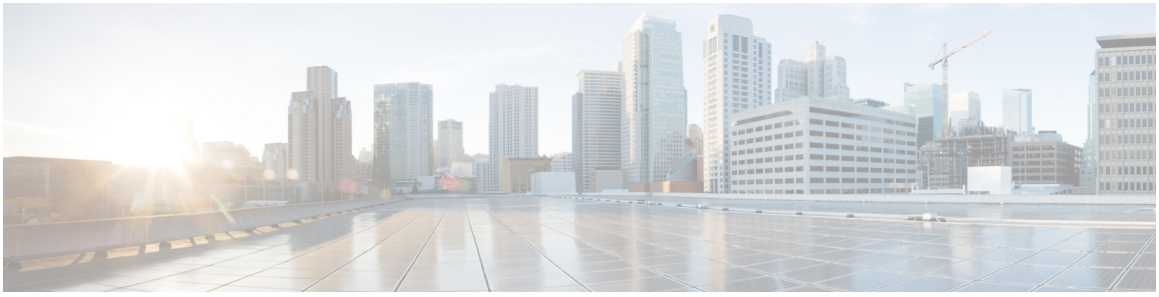
Web User Interface

First Published: 2025-09-15

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

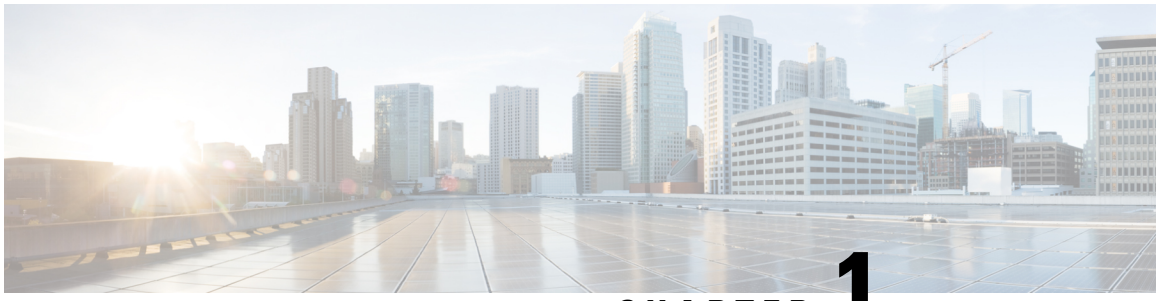
Read Me First



Read Me First

Only supported features are documented. To confirm or clarify all the supported features for a platform, go to Cisco Feature Navigator.

CONTENTS



CHAPTER 1

Web User Interface

Web UI

The Web User Interface (Web UI) is an embedded GUI-based device-management tool that provides the ability to

- provision the device
- simplify device deployment and manageability, and
- enhance the user experience.

You can use WebUI to build configurations, monitor, and troubleshoot the device without having CLI expertise.

When to use the Web UI

After you complete the hardware installation, you need to setup the switch with configuration required to enable traffic to pass through the network. On your first day with your new device, you can use the Web UI to perform several tasks to ensure that your device is online, reachable and easily configured.

Note If your network is managed by Cisco Meraki, then the switch will be automatically detected and onboarded to the network. You are not required to configure the Web UI in this case.

Configure the switch using Web UI

There are two methods to configure the switch using Web UI:

- To onboard the switch using basic and advanced configuration, refer to Classic Day 0 Wizard.
- To onboard the switch to Cisco Catalyst Center using Web UI, refer to Cisco Catalyst Center Cloud Onboarding Day 0 Wizard.

Method 1: Classic Day 0 Wizard

The classic Day 0 wizard assists in onboarding the switch to your network by guiding you through the configuration of essential network settings. This wizard is especially useful for networks that are managed locally rather than through cloud-based interfaces such as Cisco Catalyst Center or Cisco Meraki. The classic Day 0 wizard is more suitable for devices managed through on-premises solutions like SSM On-Prem, making it an ideal choice for organizations with local network management requirements.

Once you have completed the wizard configurations, you can access the device through the WebUI using the management interface IP address.

Before using the Classic Day 0 wizard

Before you use the Classic Day 0 Wizard, you need to set up the DHCP Client Identifier, based on your OS, and connect to the switch.

Set up the DHCP client identifier on the client for Windows

You need to set up the DHCP Client Identifier on the client to get the IP address from the switch, and to be able to authenticate with Day 0 login credentials.

Procedure

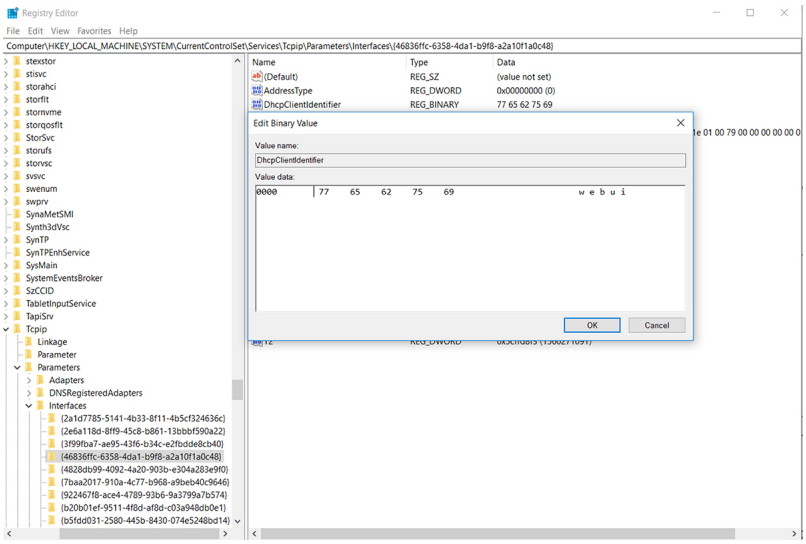
Step 1 Type `regedit` in the Windows search box on the taskbar and press `enter`.

Step 2 If prompted by User Account Control, click **Yes** to open the Registry Editor.

Step 3 Navigate to **Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces** and locate the **Ethernet Interface** Global Unique Identifier (GUID).

Step 4 Add a new REG_BINARY **DhcpClientIdentifier** with Data **77 65 62 75 69** for webui. You need to manually type in the value.

Figure 1: Setting up DHCP Client Identifier on Windows



Step 5 Restart the PC for the configuration to take effect.

What to do next

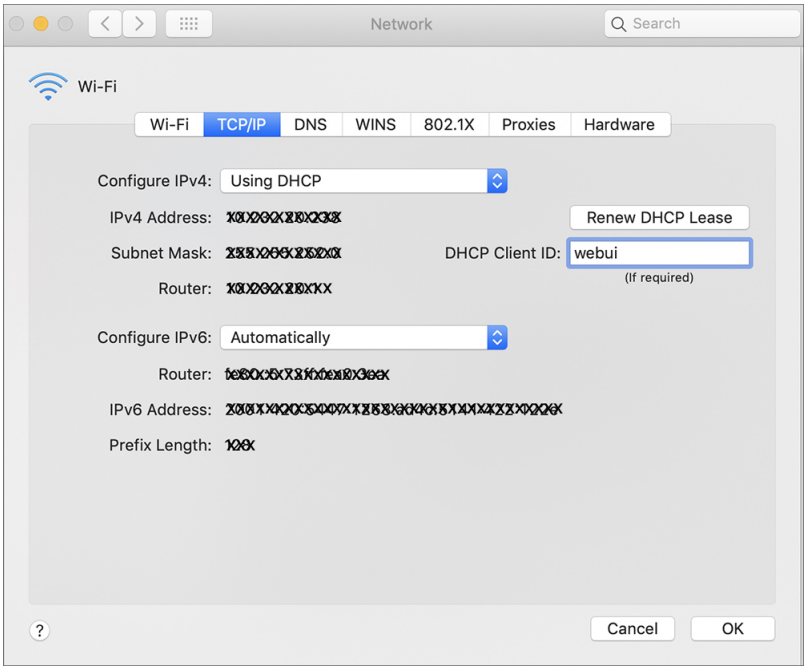
Follow the procedure detailed in Connect to the Switch

Set up the DHCP client identifier on the client for MAC

Procedure

Step 1 Go to **System Preferences** > **Network** > **Advanced** > **TCP** > **DHCP Client ID:** and enter webui.

Figure 2: Setting up DHCP Client Identifier on MAC



Step 2 Click **OK** to save the changes.

Step 3 The bootup script runs the configuration wizard, which prompts you for basic configuration input: (**Would you like to enter the initial configuration dialog? [yes/no]:**).

To configure Day 0 settings using the web UI, do not enter a response.

What to do next

Follow the procedure detailed in Connect to the Switch

Connect to the switch

To connect to a switch, follow this procedure.

Procedure

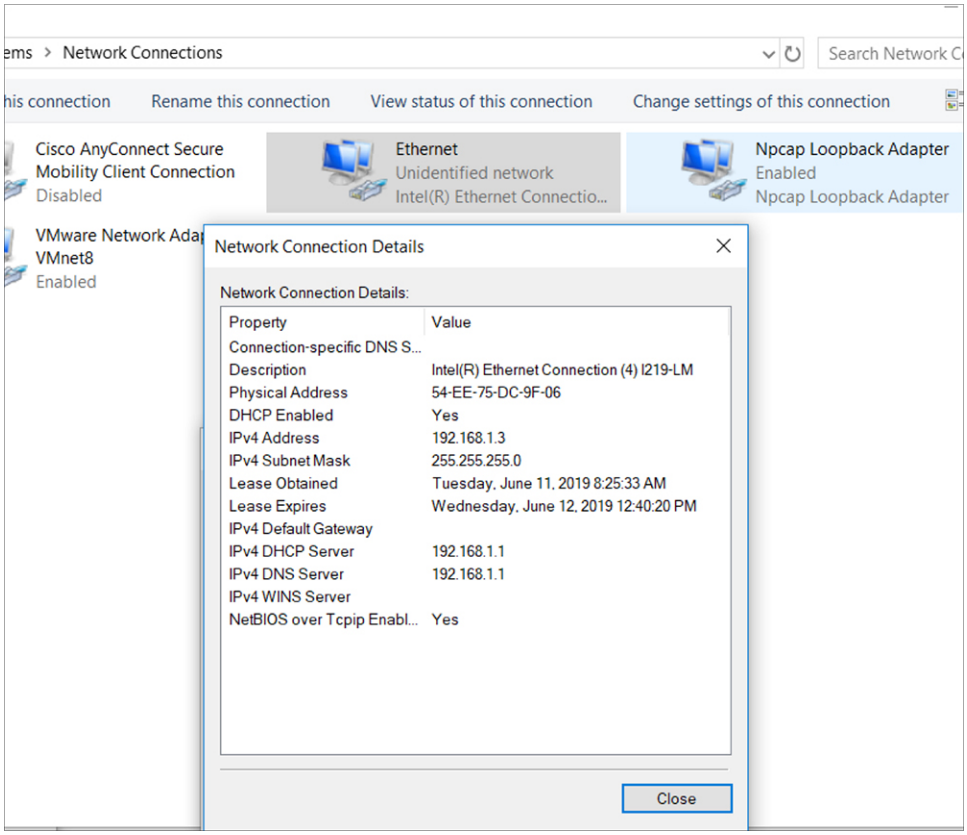
Step 1 Make sure that no devices are connected to the switch.

Step 2 Connect one end of an ethernet cable to one of the downlink (non-management) ports on the active supervisor and the other end of the ethernet cable to the host (PC/MAC).

Step 3 Set up your PC/MAC as a DHCP client, to obtain the IP address of the switch automatically. You should get an IP address within the 192.168.1.x/24 range.

This figure shows the network connection details for a Windows

Figure 3: Obtaining the IP Address (Windows)



It may take up to three mins.

First time logging in to the Web UI

Perform this task to log in to the Web UI for the first time.

Procedure

Step 1 Launch a web browser on the PC and enter the device IP address, `https://192.168.1.1`, in the address bar.

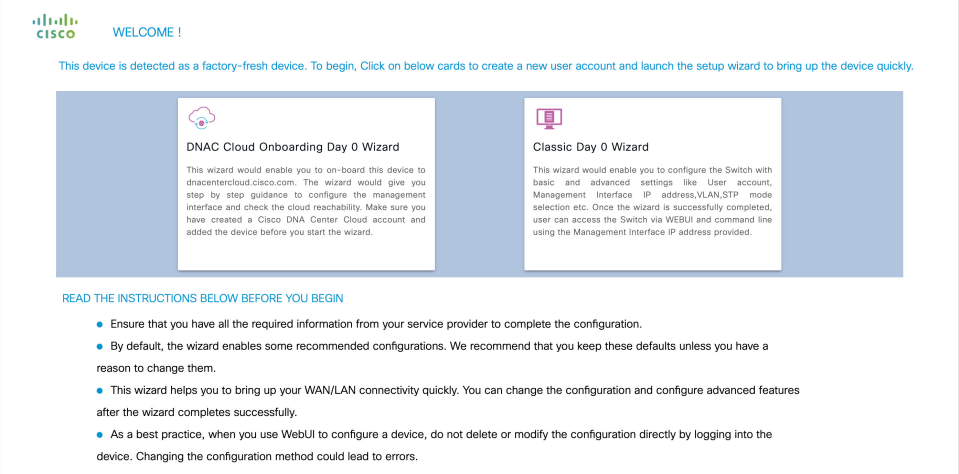
Step 2 Log on to the Web UI by entering the following default credentials:

- username: *webui*
- password: *cisco*

Note
It is recommended to change these default credentials immediately after the initial setup. Once you have changed the password, these default credentials become invalid.

The following screen is displayed.

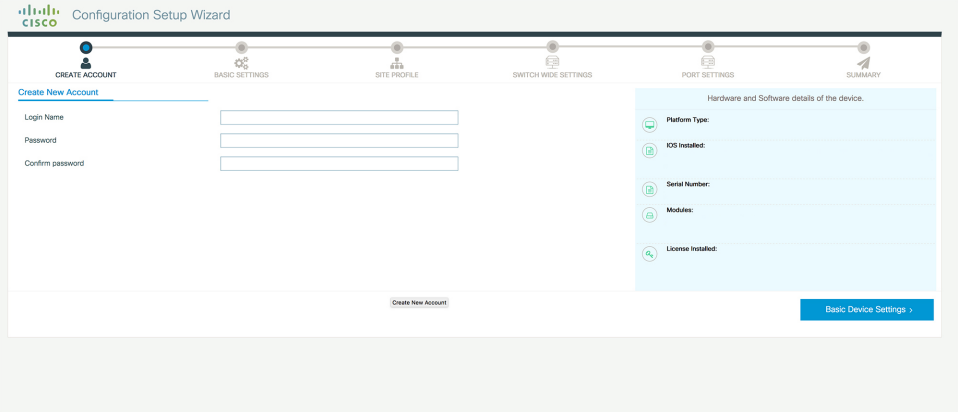
Figure 4: WebUI Day 0 Wizard



Step 3 Select the Classic Day 0 Wizard pane.

The Classic Day 0 Wizard is displayed.

Figure 5: Classic Day 0 Wizard



Configure using the classic day 0 wizard

Procedure

Step 1 In the **Create Account** page, you can configure the following:

a. Enter the user name to access the Web UI.

b. Enter the password in the **Password** and **Confirm Password** field.

The password

- must contain 25 alphanumeric characters.
- is case sensitive
- cannot start with a number
- allows spaces but ignores leading spaces.

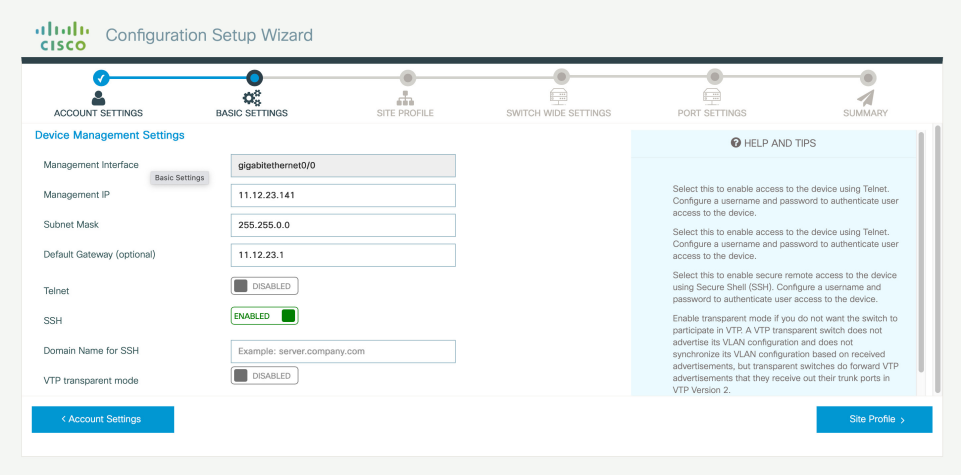
By default, you are assigned full administrative access (privilege level 15).

c. Click **Create New Account** button to create the account.

Step 2 Click **Basic Device Settings** button to move to the **Basic Settings** page.

The Basic Settings page is displayed.

Figure 6: Basic Settings



Step 3 In the **Basic Settings** page, you can configure the following:

Section	Field	Description
Device ID and Location Settings	**Device Name**	Name to identfify the device.
	Date & Time Mode	The date and time mode.
Device Management Settings	**Management Interface**	Displays information about the management interface.
	Management IP	The IP address to the management interface. Ensure that the IP address you assign is part of the subnet mask you enter.
	Subnet Mask	The subnet mask you want to associate with the IP address.
	Default Gateway (optional)	IP address to specify the default gateway.
	Telnet	Enables access to the device using telnet.
	ssh	Enables secure remote access to the device using Secure Shell (SSH)
	VTP transparent mode	Prevents device from particpating in VTP.

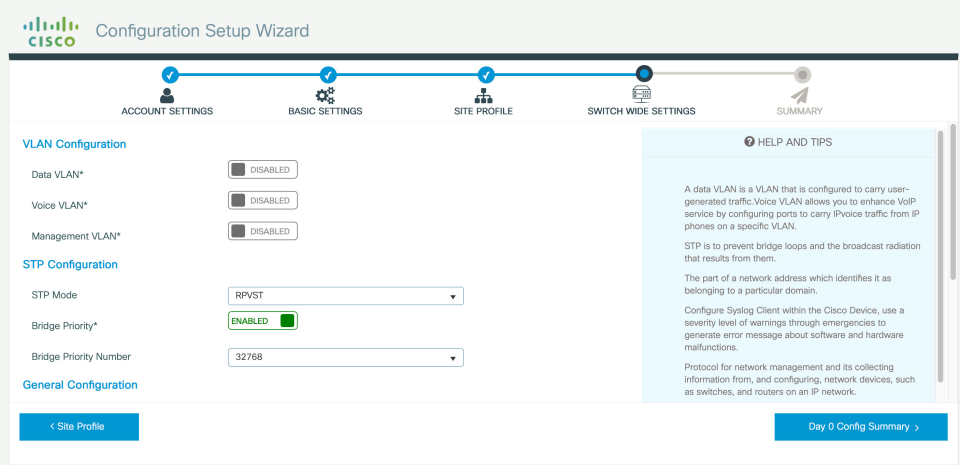
Step 4 Click the **Site Profile** button.

To ease your configuration tasks and save time, choose a site profile based on where your device may be installed and managed in your network. Based on the site profile you choose, your device is automatically configured according to Cisco best practices. You can easily modify this default configuration, from the corresponding detailed configuration screens.

Choosing a site profile as part of Quick Setup allows you to configure your device based on the business needs of your enterprise. For example, you could use your device as an access switch, to connect client nodes and endpoints on your network, or as a distribution switch, to route packets between subnets and VLANs.

Step 5 Click **Switch Wide Settings** button to move to the **Switch Wide Settings** page.

Figure 7: Switch Wide Settings



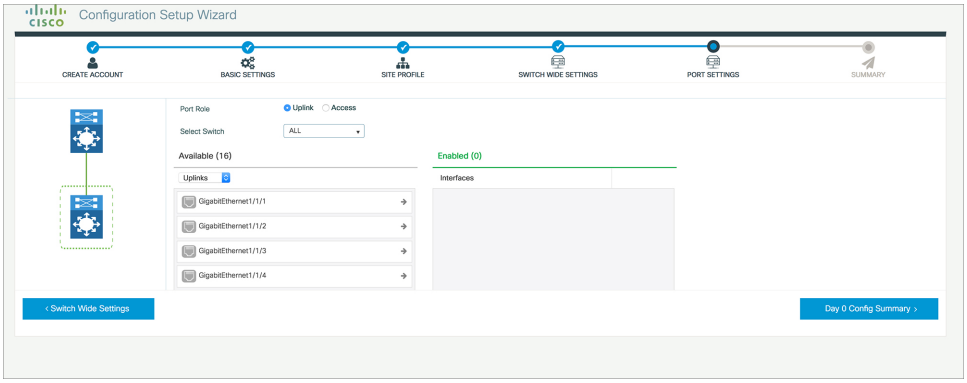
Step 6 In the **Switch Wide Settings** section, you can configure the following:

Section	Field	Description
VLAN Configuration	**Data VLAN**	Enable the check box to configure a data VLAN. Type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range.
	Voice VLAN	Enable the check box to configure a voice VLAN. Type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range.
	Management VLAN	Enable the check box to configure a management VLAN. Type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range.
STP Configuration	**STP Mode**	Select the STP mode. You can select • RPVST: This is the default mode. • PVST
	Bridge Priority	Select the check box to change a bridge priority number from the default value 32748. Choose a priority number from the drop-down list.

Section	Field	Description
General Configuration	**Domain Name**	Enter a domain name that the software uses to resolve unqualified hostnames.
	DNS Server	Enter the IP address to identify the DNS server. This server is used for name and address resolution on your device.
	DHCP Server	Enter the IP address of the DNS server that you want to make available to DHCP clients.
	Syslog Server	Enter the IP address of the server to which you want to send syslog messages.
	NTP Server	Enter the IP address of the NTP server with which you want to synchronize the device time.
	IP address	Enter the IP address to identify the SNMP server. SNMPv1, SNMPv2, and SNMPv3 are supported on your device.
	SNMP community	Specify the SNMP community string to permit access to the SNMP protocol.

Step 7 Click **Port Settings** button to move to the **Port Settings** page.

Figure 8: Port Settings



Step 8 In the **Port Settings** page, you can configure the following:

a. Select one of the following port roles, based on the site profile you selected

- Uplink – For connecting to devices towards the core of the network.
- Downlink – For connecting to devices further down in the network topology.
- Access – For connecting guest devices that are VLAN-unaware.

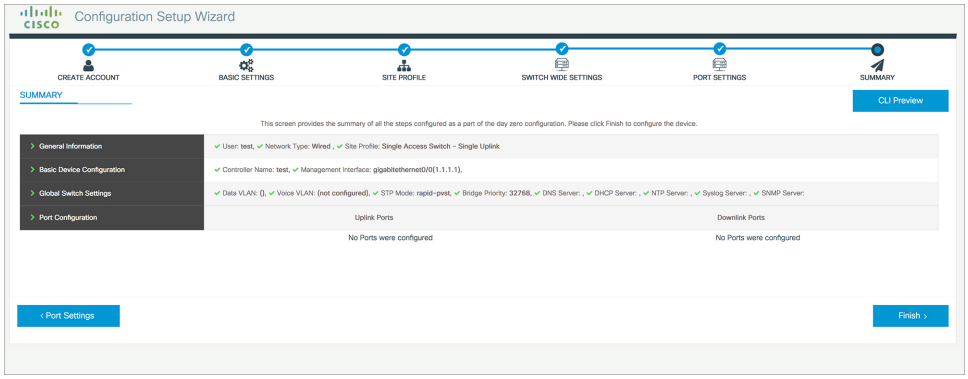
b. Choose an option from the **Select Switch** drop-down list.

c. Make selections from the **Available** list of interfaces based on how you want to enable them and move them to the **Enabled** list.

Step 9 Click **Day 0 Config Summary** to verify your setup.

The **Summary** page is displayed.

Figure 9: Day 0 Config Summary



Step 10 Click **Finish**.

Configure VTY Lines

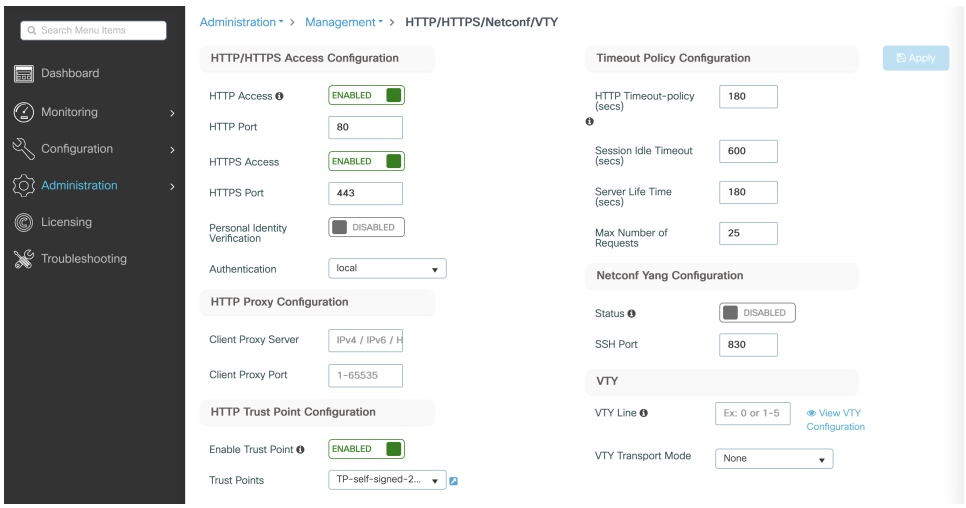
You use Virtual Terminal Lines (VTY) to connect to the device through Telnet or SSH. VTY lines determine the maximum number of simultaneous remote connections. If the device does not have enough VTY lines configured, multiple users might not be able to connect to the WebUI. The number of configured VTY lines decides the number of simultaneous sessions allowed by the device.

Procedure

Step 1 From the WebUI, navigate to **Administration** > **Management** and select the **HTTP/HTTPS/Netconf/VTY** page.

Step 2 In the **VTY** section, enter the number of VTY lines you want to configure in the **VTY Line** field.

Figure 10: Configuring VTY Line



Method 2: Cisco Catalyst Center cloud onboarding Day 0 wizard

The Cisco Catalyst Center cloud onboarding Day 0 wizard streamlines the device onboarding process by guiding you through the configuration of the management interface and verifying connectivity to the Cisco Catalyst Center cloud. This ensures that the device is properly set up and ready for centralized cloud-based management.

Before using the Cisco Catalyst Center cloud onboarding Day 0 wizard

Before using the Cisco Catalyst Center cloud onboarding Day 0 wizard, you need to add the device to the Cisco Catalyst Center. Refer to the Cisco Catalyst Center User Guide to configure and maintain network devices.

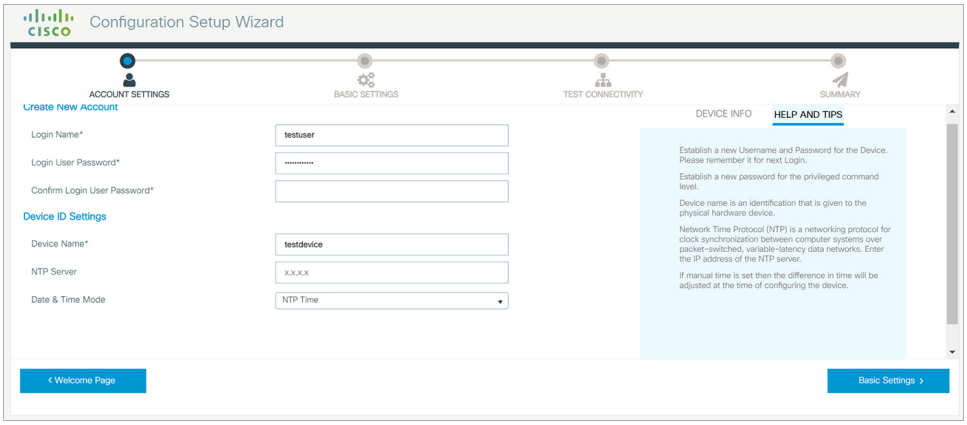
Configure using the Cisco Catalyst Center cloud onboarding Day 0 wizard

Procedure

Step 1 Select the **Cisco Catalyst Center Cloud Onboarding Day 0 Wizard** card.

The **Account Settings** page is displayed.

Figure 11: Account Settings



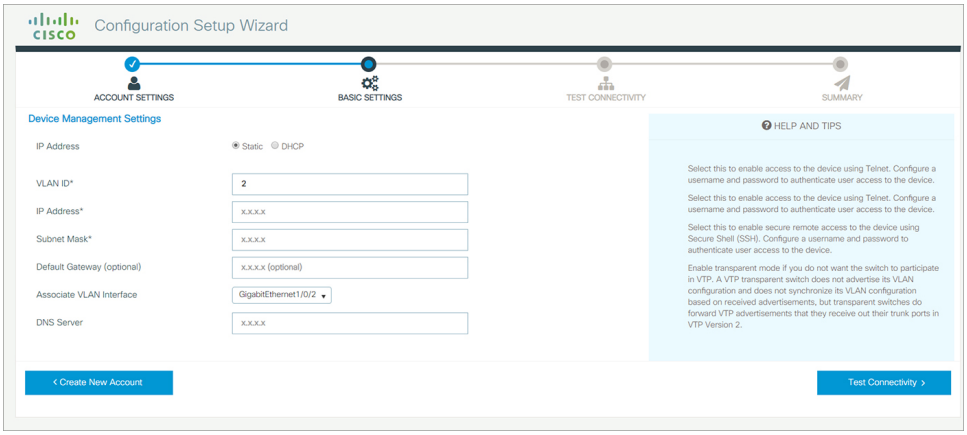
Step 2 In the **Account Settings** page, you can configure the following:

Section	Field	Description
Create New Account	**Login Name**	Enter the user name you would like to configure to log in to the Web UI.
	Login User Password **and** **Confirm Login User Password**	Enter the password you would like to configure. The password must meet the following requirements: • The password must contain 25 alphanumeric characters. • The password must be case sensitive • The password cannot start with a number • The password allows spaces but ignores leading spaces. By default, you are assigned full administrative access (privilege level 15).
Device ID Settings	**Device Name**	Enter the name that will identfify the device.
	NTP Server	Enter the IP address of an external Network Time Protocol (NTP) server to sychronize your device clock.
	Date & Time Mode	Select the date and time mode.

Step 3 Click **Basic Settings** button to move to the **Basic Settings** page.

The **Basic Settings** page is displayed.

Figure 12: Basic Settings - Static Configuration



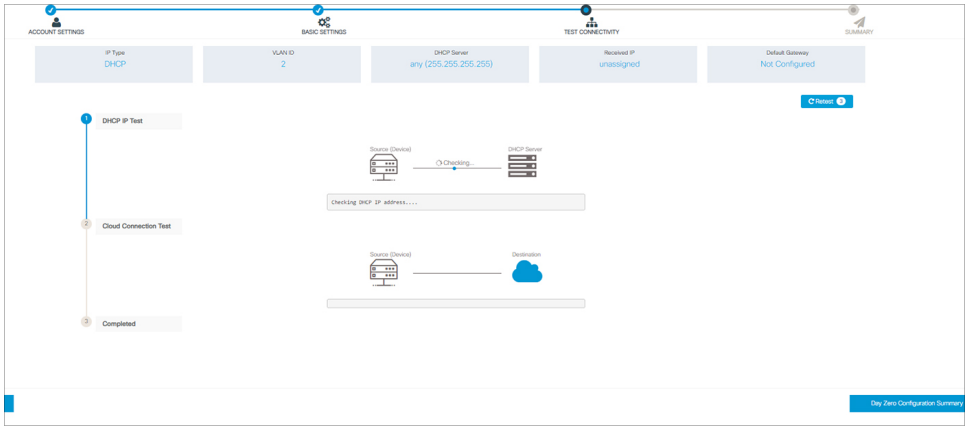
Step 4 In the **Basic Settings** page, you can configure the following:

Field	Description
IP Address	Select the method you want to assign IP address • **Static**: A static IP address • **DHCP**: DHCP assigns the IP address.
Associate VLAN Interface	Select the interface you want to associate with the VLAN. **Note** This option is available if you have selected the **IP address** as **static**.
VLAN ID	• For Static: A VLAN ID that you can want to associate with the interface you have selected in the **Associate VLAN Interface** drop-down list. • For DHCP: A VLAN ID. The VLAN ID must be a value other than 1
IP Address	• For Static: The static IP address you want to associate with the interface • For DHCP: The IP address is automatically assigned.
Subnet Mask	• For Static: The subnet mask you want to associate with the IP address. • For DHCP: The subnet mask is automatically assigned.
Default Gateway (Optional)	IP address to specify the default gateway.
DNS Server	IP address of the DNS Server.

Step 5 Click **Test Connectivity** button to move to the **Test Connectivity** page.

The **Test Connectivity** page is displayed.

Figure 13: Test Connectivity



Step 6 In the **Test Connectivity** page, you can configure the following:

a. Click the **Test Connectivity/Retest** button to ensure that connection is established between the device to the Cisco Catalyst Centre Cloud.

b. Click the **Reset** button if the connection is not established.

If connection still fails, go to the previous **Basic Settings** page, make changes to the settings, and test connectivity again.

c. Once connectivity is established, go to the **Day Zero Configuration Summary** to save the configurations.

Step 7 Verify that the configurations are applied successfully, and the device is redirected to Cisco Catalyst Center Cloud.

If redirection does not succeed, verify if the device is associated with a redirection controller profile on *Cisco PnP Connect (devicehelper)*.