



## **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

---

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.





# CONTENTS

**PREFACE**

**Read Me First**    **ii**

**CHAPTER 1**

**Web User Interface**    **1**

    Web UI    **1**

        When to use the Web UI    **1**

    Configure the switch using Web UI    **1**

        Method 1: Classic Day 0 Wizard    **2**

            Before using the Classic Day 0 wizard    **2**

            Configure using the classic day 0 wizard    **6**

            Configure VTY Lines    **10**

        Method 2: Cisco Catalyst Center cloud onboarding Day 0 wizard    **11**

            Before using the Cisco Catalyst Center cloud onboarding Day 0 wizard    **11**

            Configure using the Cisco Catalyst Center cloud onboarding Day 0 wizard    **11**





## CHAPTER 1

# Web User Interface

---

- [Web UI, on page 1](#)
- [Configure the switch using Web UI, on page 1](#)

## 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.

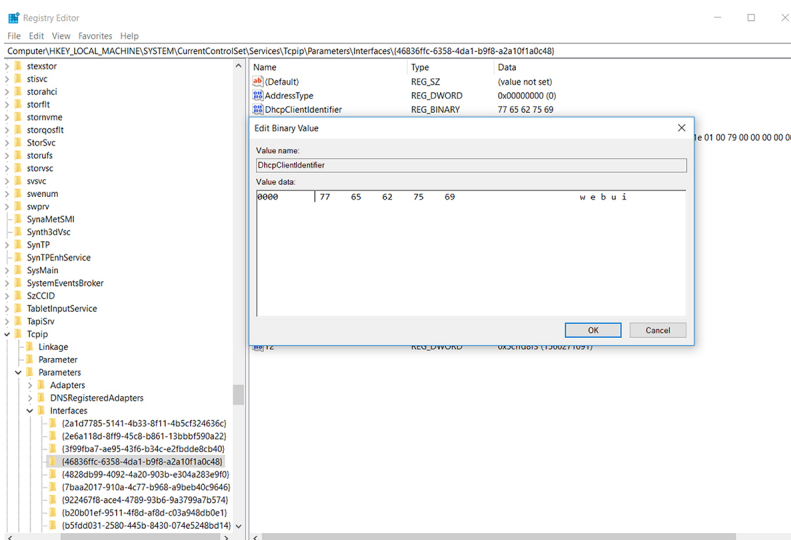
#### Set up the DHCP client identifier on the client for Windows

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

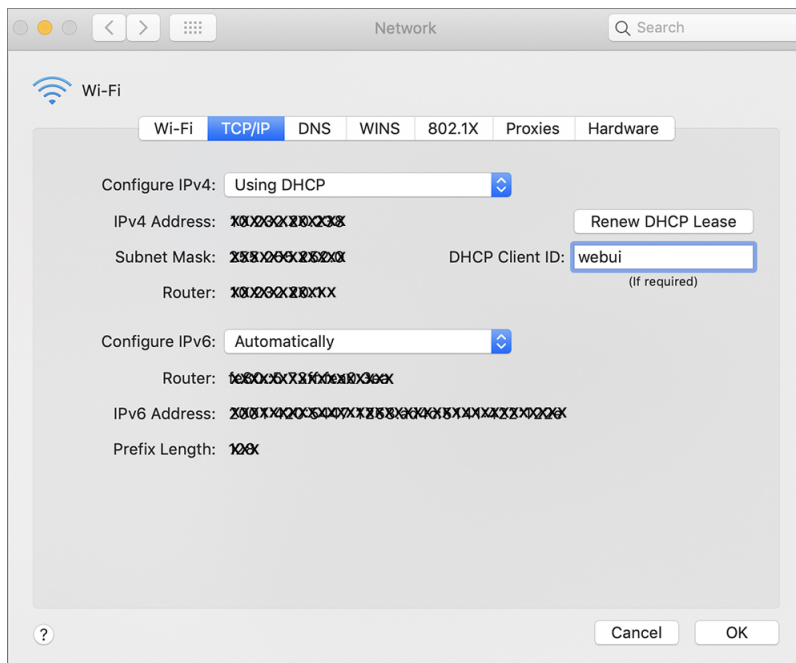
Follow the procedure detailed in [Connect to the Switch](#)

## 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

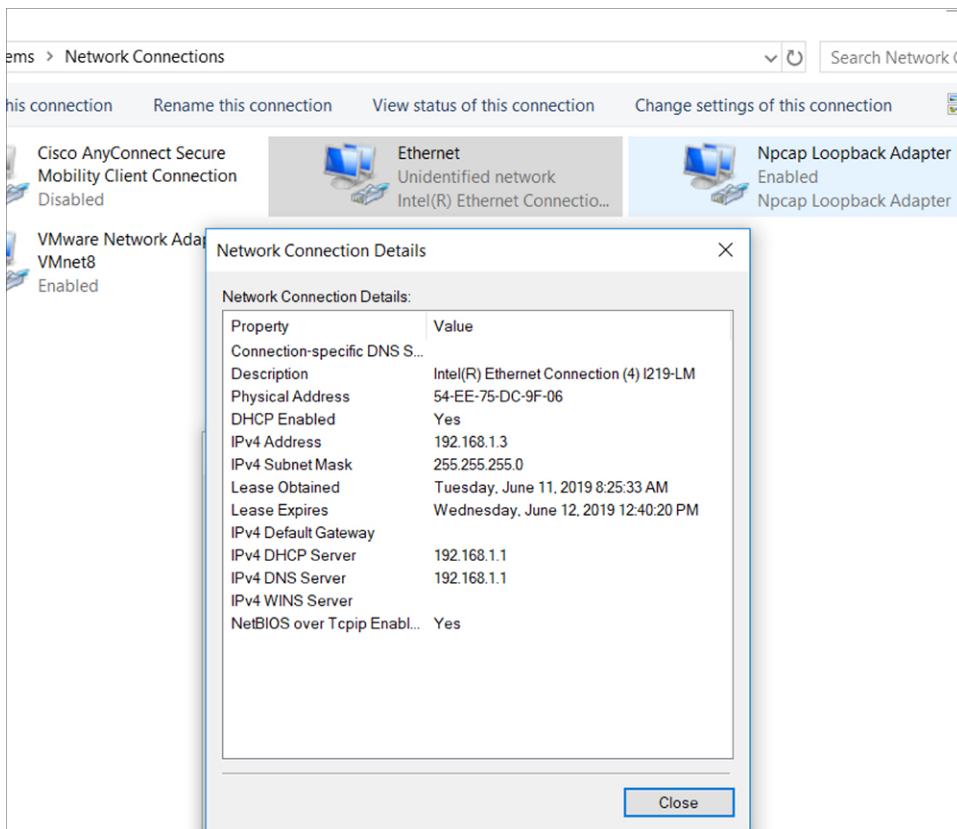
To connect to a switch, follow this procedure.

## 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:

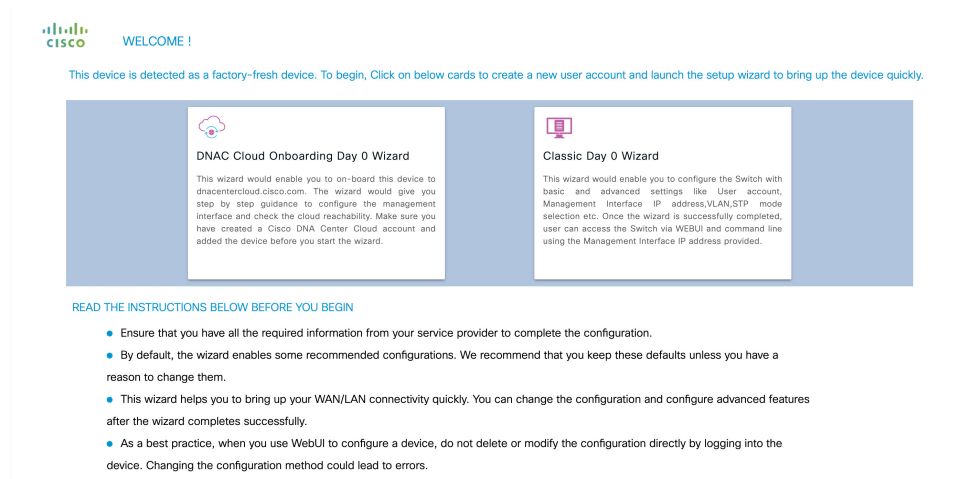
- username: *webui*
- password: *cisco*

### 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

The screenshot shows the 'Configuration Setup Wizard' interface. The top navigation bar includes the Cisco logo and the title 'Configuration Setup Wizard'. Below this, a progress bar shows six steps: 'CREATE ACCOUNT' (active), 'BASIC SETTINGS', 'SITE PROFILE', 'SWITCH WIDE SETTINGS', 'PORT SETTINGS', and 'SUMMARY'. The 'CREATE ACCOUNT' section has three input fields: 'Login Name', 'Password', and 'Confirm password'. A 'Create New Account' button is located at the bottom center. To the right, a panel titled 'Hardware and Software details of the device' contains five fields: 'Platform Type', 'IOS Installed', 'Serial Number', 'Modules', and 'License Installed'. A 'Basic Device Settings' button is at the bottom right of this panel.

## 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   |
|--|-----------------------------------|---|
| <b>Device ID and Location Settings</b> | <b>Device Name</b>                | Name to identify the device.  |
|  | <b>Date &amp; Time Mode</b>       | The date and time mode.   |
| <b>Device Management Settings</b>      | <b>Management Interface</b>       | Displays information about the management interface.  |
|  | <b>Management IP</b>              | The IP address to the management interface. Ensure that the IP address you assign is part of the subnet mask you enter. |
|  | <b>Subnet Mask</b>                | The subnet mask you want to associate with the IP address.  |
|  | <b>Default Gateway (optional)</b> | IP address to specify the default gateway.  |
|  | <b>Telnet</b>                     | Enables access to the device using telnet.  |
|  | <b>ssh</b>                        | Enables secure remote access to the device using Secure Shell (SSH)   |
|  | <b>VTP transparent mode</b>       | Prevents device from participating 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

**Configuration Setup Wizard**

ACCOUNT SETTINGS BASIC SETTINGS SITE PROFILE **SWITCH WIDE SETTINGS** SUMMARY

**VLAN Configuration**

Data VLAN\* ☐ DISABLED

Voice VLAN\* ☐ DISABLED

Management VLAN\* ☐ DISABLED

**STP Configuration**

STP Mode

Bridge Priority\* ☒ ENABLED

Bridge Priority Number

**General Configuration**

< Site Profile Day 0 Config Summary >

**HELP AND TIPS**

A data VLAN is a VLAN that is configured to carry user-generated traffic. Voice VLAN allows you to enhance VoIP service by configuring ports to carry IPvoice traffic from IP phones on a specific VLAN.

STP is to prevent bridge loops and the broadcast radiation that results from them.

The part of a network address which identifies it as belonging to a particular domain.

Configure Syslog Client within the Cisco Device, use a severity level of warnings through emergencies to generate error message about software and hardware malfunctions.

Protocol for network management and its collecting information from, and configuring, network devices, such as switches, and routers on an IP network.

**Step 6**

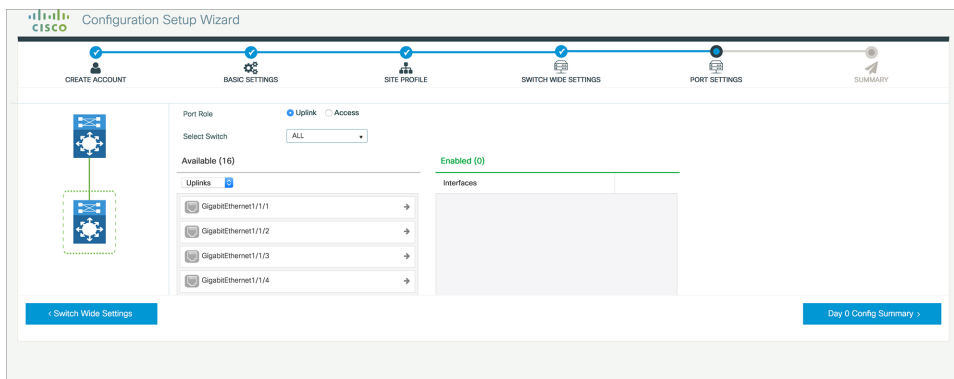
In the **Switch Wide Settings** section, you can configure the following:

| Section                   | Field                  | Description   |
|---------------------------|------------------------|---|
| <b>VLAN Configuration</b> | <b>Data VLAN</b>       | Enable the check box to configure a data VLAN.<br>Type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range.       |
|                           | <b>Voice VLAN</b>      | Enable the check box to configure a voice VLAN.<br>Type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range.      |
|                           | <b>Management VLAN</b> | Enable the check box to configure a management VLAN.<br>Type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range. |
| <b>STP Configuration</b>  | <b>STP Mode</b>        | Select the STP mode. You can select <ul style="list-style-type: none"> <li>• RPVST: This is the default mode.</li> <li>• PVST</li> </ul>                                      |
|                           | <b>Bridge Priority</b> | Select the check box to change a bridge priority number from the default value 32748.<br>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

Configuration Setup Wizard

CREATE ACCOUNT BASIC SETTINGS SITE PROFILE SWITCH WIDE SETTINGS PORT SETTINGS SUMMARY

CLI Preview

Summary

This screen provides the summary of all the steps configured as a part of the day zero configuration. Please click Finish to configure the device.

General Information

- User: test, Network Type: Wired, Site Profile: Single Access Switch - Single Uplink

Basic Device Configuration

- Controller Name: test, Management Interface: gigabitethernet0/0(1,1,1,1)

Global Switch Settings

- Data VLAN: 0, Voice VLAN: (not configured), STP Mode: rapid-pst, Bridge Priority: 32768, DNS Server: , DHCP Server: , NTP Server: , Syslog Server: , SNMP Server:

Port Configuration

Uplink Ports

No Ports were configured

Downlink Ports

No Ports were configured

Port Settings

Finish

**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

Administration > Management > HTTP/HTTPS/Netconf/VTY

HTTP/HTTPS Access Configuration

HTTP Access: ENABLED

HTTP Port: 80

HTTPS Access: ENABLED

HTTPS Port: 443

Personal Identity Verification: DISABLED

Authentication: local

HTTP Proxy Configuration

Client Proxy Server: IPv4 / IPv6 / H

Client Proxy Port: 1-65535

HTTP Trust Point Configuration

Enable Trust Point: ENABLED

Trust Points: TP-self-signed-2...

Timeout Policy Configuration

HTTP Timeout-policy (secs): 180

Session Idle Timeout (secs): 600

Server Life Time (secs): 180

Max Number of Requests: 25

Netconf Yang Configuration

Status: DISABLED

SSH Port: 830

VTY

VTY Line: 0 or 1-5

VTY Transport Mode: None

Apply

View VTY Configuration



## 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**

The screenshot shows the 'Configuration Setup Wizard' interface. At the top, there are four tabs: 'ACCOUNT SETTINGS' (selected), 'BASIC SETTINGS', 'TEST CONNECTIVITY', and 'SUMMARY'. Below the tabs, the 'ACCOUNT SETTINGS' section is active. It contains two main sections: 'Create New Account' and 'Device ID Settings'. The 'Create New Account' section has three input fields: 'Login Name\*' (containing 'testuser'), 'Login User Password\*' (masked with dots), and 'Confirm Login User Password\*'. The 'Device ID Settings' section has three input fields: 'Device Name\*' (containing 'testdevice'), 'NTP Server' (containing 'XXXX'), and 'Date & Time Mode' (a dropdown menu set to 'NTP Time'). On the right side, there is a 'HELP AND TIPS' section with text explaining the purpose of the fields. At the bottom, there are two buttons: '< Welcome Page' and 'Basic Settings >'. The Cisco logo is in the top left corner.

**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 | <p>Enter the password you would like to configure.</p> <p>The password must meet the following requirements:</p> <ul style="list-style-type: none"> <li>• The password must contain 25 alphanumeric characters.</li> <li>• The password must be case sensitive</li> <li>• The password cannot start with a number</li> <li>• The password allows spaces but ignores leading spaces.</li> </ul> <p>By default, you are assigned full administrative access (privilege level 15).</p> |
| Device ID Settings | Device Name   | Enter the name that will identify the device.   |
|                    | NTP Server  | Enter the IP address of an external Network Time Protocol (NTP) server to synchronize 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**

The screenshot shows the 'Configuration Setup Wizard' interface with the 'BASIC SETTINGS' tab selected. The 'Device Management Settings' section includes the following fields:

- IP Address:** Radio buttons for 'Static' (selected) and 'DHCP'.
- VLAN ID\*:** Text box containing '2'.
- IP Address\*:** Text box containing 'XXXXX'.
- Subnet Mask\*:** Text box containing 'XXXXX'.
- Default Gateway (optional):** Text box containing 'XXXXX (optional)'.
- Associate VLAN Interface:** Dropdown menu showing 'GigabitEthernet1/0/2'.
- DNS Server:** Text box containing 'XXXXX'.

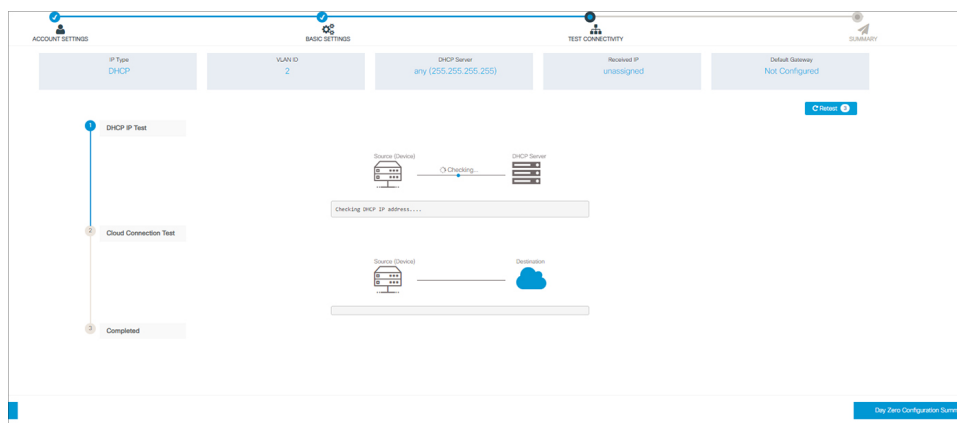
At the bottom, there are two buttons: '< Create New Account' and 'Test Connectivity >'. On the right side, there is a 'HELP AND TIPS' section with text explaining Telnet, SSH, and VTP transparent mode.

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

| Field                             | Description   |
|-----------------------------------|---|
| <b>IP Address</b>                 | Select the method you want to assign IP address <ul style="list-style-type: none"> <li>• <b>Static:</b> A static IP address</li> <li>• <b>DHCP:</b> DHCP assigns the IP address.</li> </ul>   |
| <b>Associate VLAN Interface</b>   | Select the interface you want to associate with the VLAN.<br><br><b>Note</b><br>This option is available if you have selected the <b>IP address</b> as <b>static</b> .  |
| <b>VLAN ID</b>                    | <ul style="list-style-type: none"> <li>• <u>For Static:</u><br/>A VLAN ID that you can want to associate with the interface you have selected in the <b>Associate VLAN Interface</b> drop-down list.</li> <li>• <u>For DHCP:</u><br/>A VLAN ID.<br/>The VLAN ID must be a value other than 1</li> </ul> |
| <b>IP Address</b>                 | <ul style="list-style-type: none"> <li>• <u>For Static:</u><br/>The static IP address you want to associate with the interface</li> <li>• <u>For DHCP:</u><br/>The IP address is automatically assigned.</li> </ul>   |
| <b>Subnet Mask</b>                | <ul style="list-style-type: none"> <li>• <u>For Static:</u><br/>The subnet mask you want to associate with the IP address.</li> <li>• <u>For DHCP:</u><br/>The subnet mask is automatically assigned.</li> </ul>  |
| <b>Default Gateway (Optional)</b> | IP address to specify the default gateway.  |
| <b>DNS Server</b>                 | 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)*.