



# Configuring the Switch Using the Web User Interface

---

**Note**

Any figures included in the document are shown for illustrative purposes only.

---

- [Introduction to Day 0 WebUI Configuration, on page 1](#)
- [Cisco DNA Center Cloud Onboarding Day 0 Wizard, on page 2](#)
- [Classic Day 0 Wizard, on page 5](#)

## Introduction to Day 0 WebUI Configuration

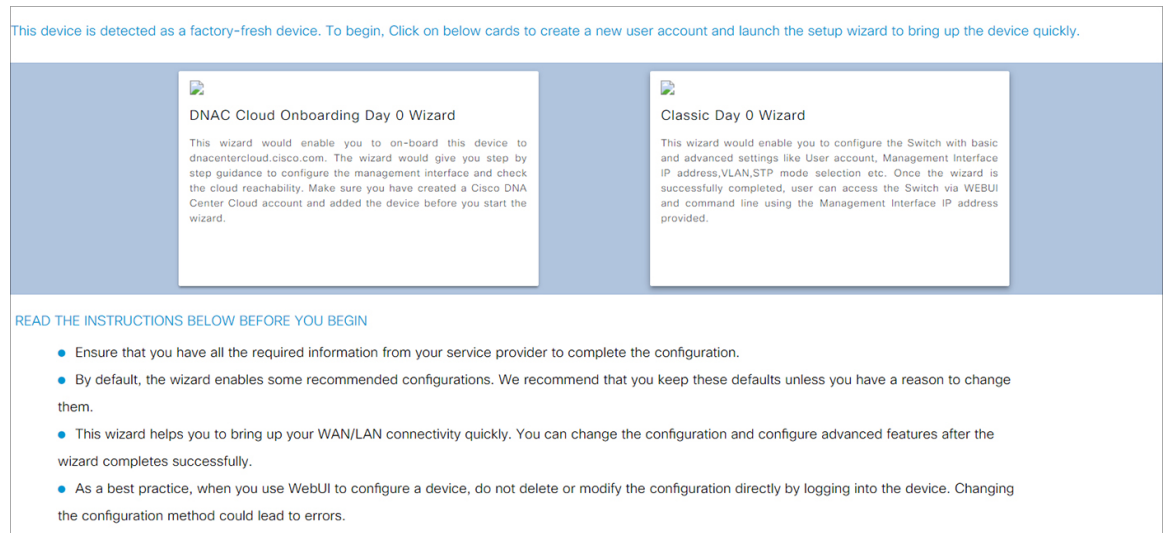
After you complete the hardware installation, you need to setup the switch with configuration required to enable traffic to pass through the network. On your first day with your new device, you can perform a number of tasks to ensure that your device is online, reachable and easily configured.

The Web User Interface (Web UI) is an embedded GUI-based device-management tool that provides the ability to provision the device, to simplify device deployment and manageability, and to enhance the user experience. You can use WebUI to build configurations, monitor, and troubleshoot the device without having CLI expertise.

You have two methods to configure the switch using the WebUI.

- [Cisco DNA Center Cloud Onboarding Day 0 Wizard](#)
- [Classic Day 0 Wizard](#)

Figure 1: WebUI Day 0 Wizard



# Cisco DNA Center Cloud Onboarding Day 0 Wizard

Use this wizard to configure the management interface and check if it is reachable through the cloud.



## Note

You must add the device to your Cisco DNA Center Cloud account before proceeding with this wizard.

## Configuring Account Settings

Setting a username and password is the first task you will perform on your device. Typically, as a network administrator, you will want to control access to your device and prevent unauthorized users from seeing your network configuration or manipulating your settings.

**Step 1** Log on using the default username **webui** and password **cisco**.

**Step 2** Set a password of up to 25 alphanumeric characters.

The username password combination you set gives you privilege 15 access. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces.

**Step 3** In the **Device ID Settings** section, type a unique name in the **Device Name** field to identify your device in the network.

**Step 4** Enter the date and time for your device manually in the **Time & Device Mode** field. To synchronize your device with an external timing mechanism such as a Network Time Protocol (NTP) clock source, enter the IP address in the **NTP Server** field.

Figure 2: Account Settings

Cisco Configuration Setup Wizard

ACCOUNT SETTINGS BASIC SETTINGS TEST CONNECTIVITY SUMMARY

Create New Account

Login Name\* testuser

Login User Password\* .....

Confirm Login User Password\*

Device ID Settings

Device Name\* testdevice

NTP Server X.X.X.X

Date & Time Mode NTP Time

< Welcome Page Basic Settings >

HELP AND TIPS

Establish a new Username and Password for the Device. Please remember it for next Login.

Establish a new password for the privileged command level.

Device name is an identification that is given to the physical hardware device.

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. Enter the IP address of the NTP server.

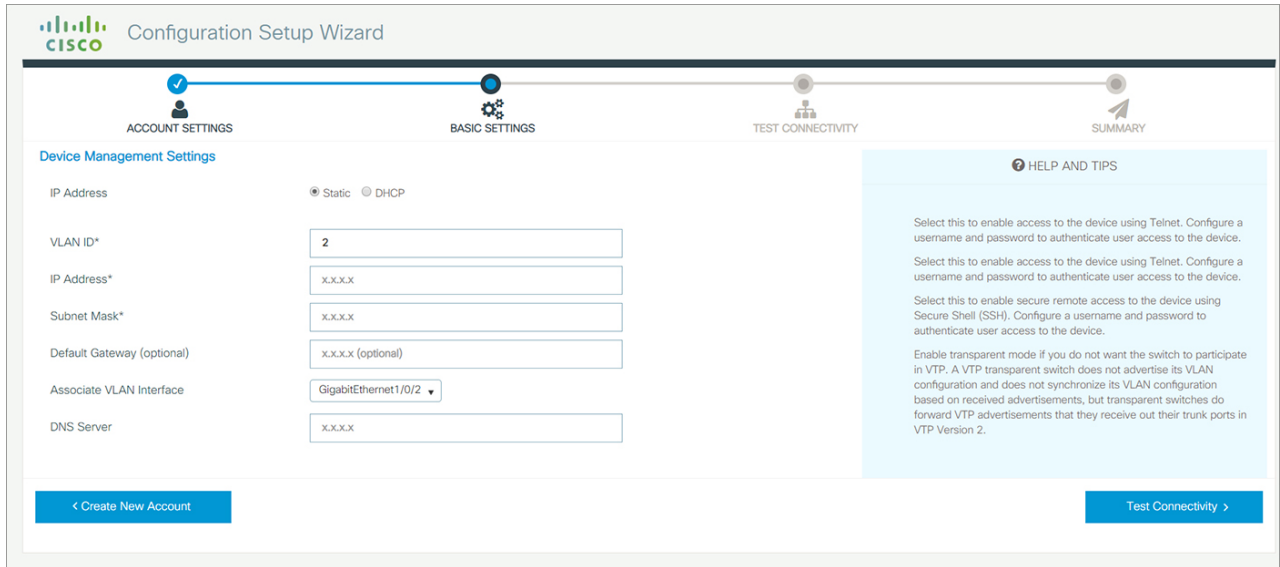
If manual time is set then the difference in time will be adjusted at the time of configuring the device.

## Configuring Basic Device Settings

On the **Basic Settings** page configure the following information:

- Step 1** In the **Device Management Settings** section, assign an IP address to the management interface using either *Static* or *DHCP* address.
- Step 2** If you chose *Static*, perform the following steps:
- Enter a VLAN ID to associate with the interface in the **Associate VLAN Interface** drop-down list.
  - Ensure that the IP address you assign is part of the subnet mask you enter.
  - Optionally, enter an IP address to specify the default gateway.
  - Enter the address of the DNS Server.

Figure 3: Basic Settings - Static Configuration



The screenshot shows the Cisco Configuration Setup Wizard in the 'BASIC SETTINGS' step. The 'Device Management Settings' section is active, with the 'Static' radio button selected for IP Address configuration. The fields are as follows:

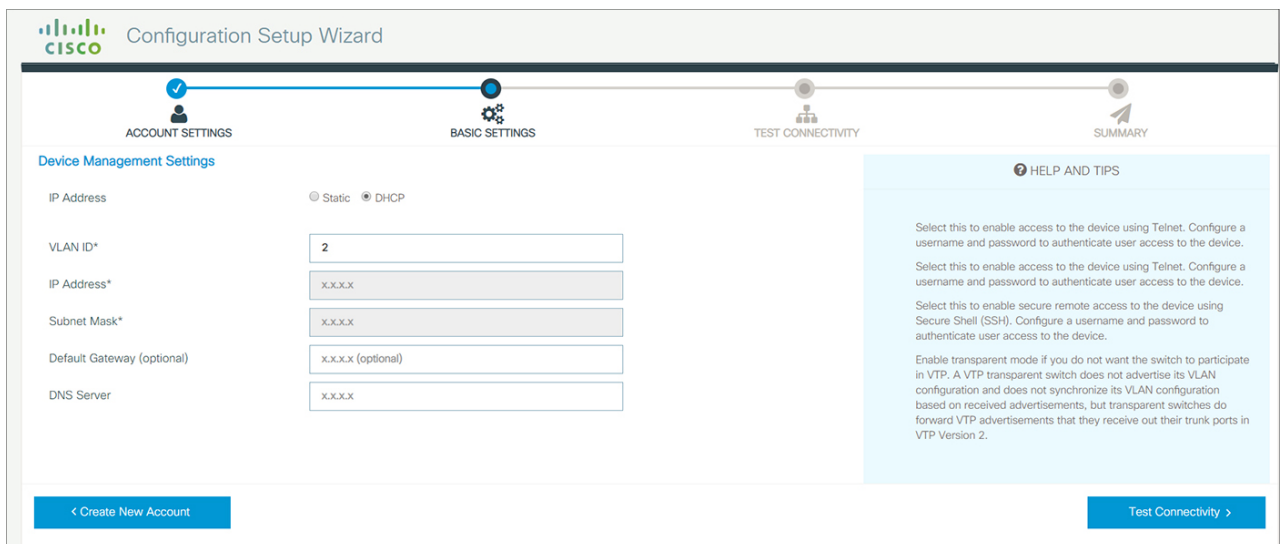
Field	Value
VLAN ID*	2
IP Address*	x.x.x.x
Subnet Mask*	x.x.x.x
Default Gateway (optional)	x.x.x.x (optional)
Associate VLAN Interface	GigabitEthernet1/0/2
DNS Server	x.x.x.x

Navigation buttons at the bottom include '< Create New Account' and 'Test Connectivity >'. A 'HELP AND TIPS' sidebar on the right provides instructions for enabling Telnet, SSH, and VTP transparent mode.

**Step 3** If you chose *DHCP*, perform the following steps:

- Enter a value in the VLAN ID field.  
VLAN ID must be a value other than 1.
- Ensure that the IP address you assign is part of the subnet mask you enter.
- Optionally, enter an IP address to specify the default gateway.
- Enter the address of the DNS Server.

Figure 4: Basic Settings - DHCP Configuration



The screenshot shows the Cisco Configuration Setup Wizard in the 'BASIC SETTINGS' step. The 'Device Management Settings' section is active, with the 'DHCP' radio button selected for IP Address configuration. The fields are as follows:

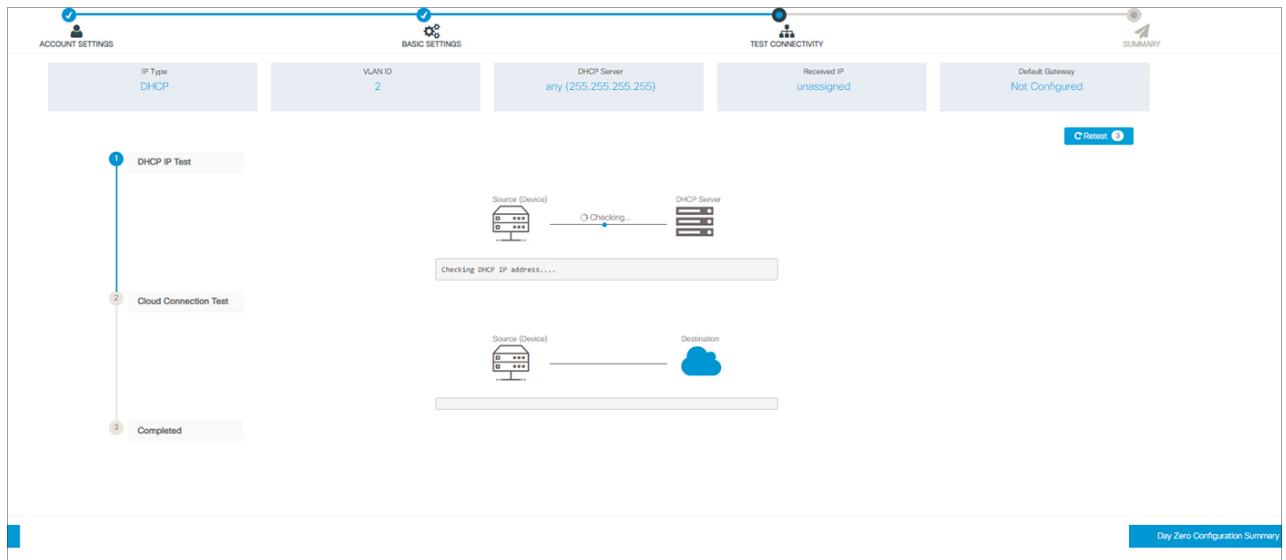
Field	Value
VLAN ID*	2
IP Address*	x.x.x.x
Subnet Mask*	x.x.x.x
Default Gateway (optional)	x.x.x.x (optional)
DNS Server	x.x.x.x

Navigation buttons at the bottom include '< Create New Account' and 'Test Connectivity >'. A 'HELP AND TIPS' sidebar on the right provides instructions for enabling Telnet, SSH, and VTP transparent mode.

## Configuring Test Connectivity

- Step 1** Use the **Test Connectivity/Retest** button to ensure that connection is established between the device to the Cisco DNAC Cloud.
- Step 2** If connection is not established, click the **Retest** button.
- If connection still fails, go to the previous **Basic Settings** page, make changes to the settings, and test connectivity again.
- Step 3** Once connectivity is established, go to the **Day Zero Configuration Summary** to save the configurations.

Figure 5: Test Connectivity



- Step 4** Verify that the configurations are applied successfully, and the device is redirected to Cisco DNAC Cloud.

### What to do next

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

## Classic Day 0 Wizard

Use this wizard to configure the device with basic and advanced settings. Once complete, you can access the device through the WebUI using the management interface IP address.

## Connecting to the Switch

### Before you begin

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.

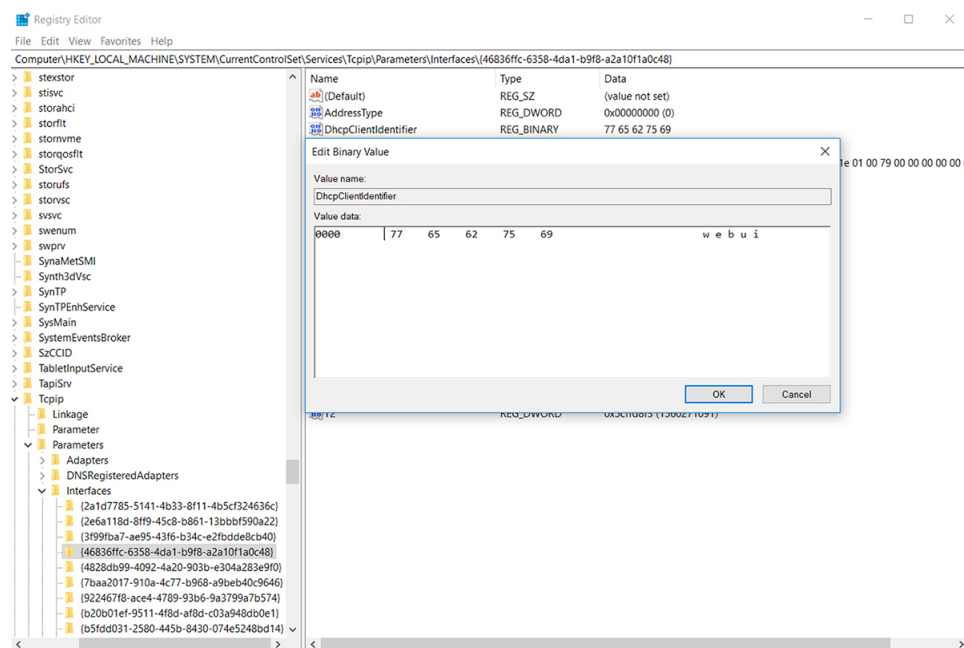
### Setting up the DHCP Client Identifier on the client for Windows

1. Type **regedit** in the Windows search box on the taskbar and press **enter**.
2. If prompted by User Account Control, click **Yes** to open the Registry Editor.
3. Navigate to

**Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\** and locate the **Ethernet Interface** Global Unique Identifier (GUID).

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 6: Setting up DHCP Client Identifier on Windows**

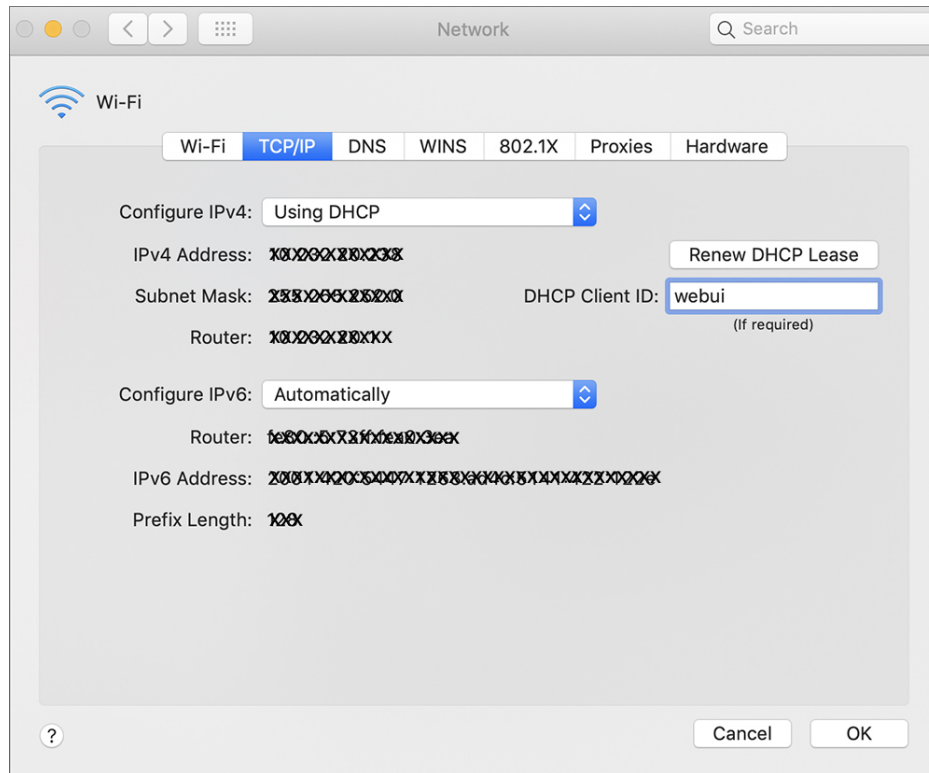


5. Restart the PC for the configuration to take effect.

### Setting up the DHCP Client Identifier on the client for MAC

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

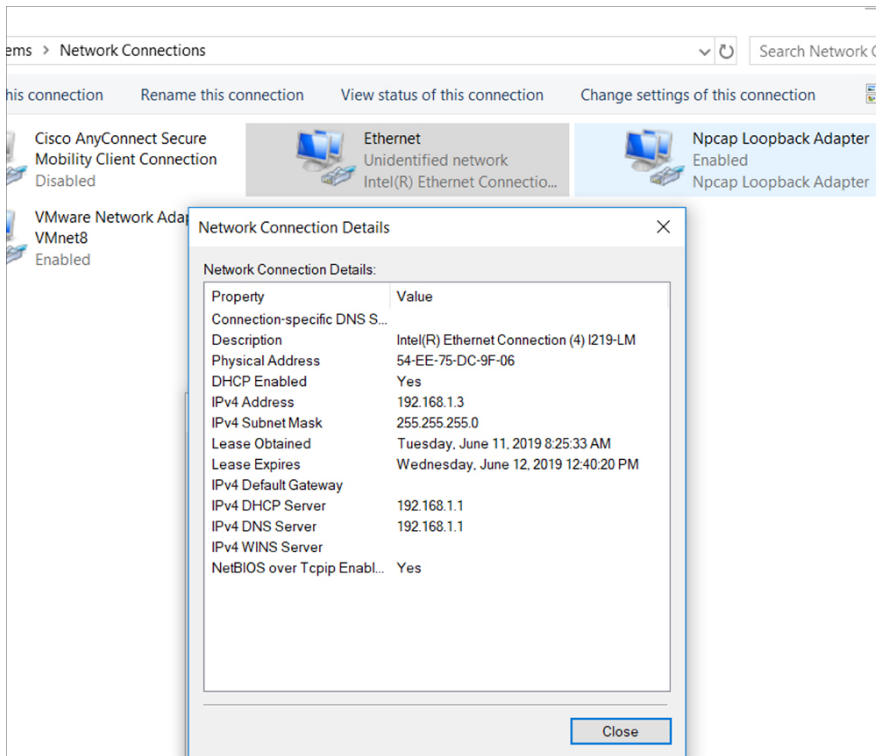
Figure 7: Setting up DHCP Client Identifier on MAC



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

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. Perform the following tasks instead:

- 
- 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.

**Figure 8: Obtaining the IP Address**

It may take up to three mins. You must complete the Day 0 setup through the web UI before using the device terminal.

**Step 4** Launch a web browser on the PC and enter the device IP address (**https://192.168.1.1**) in the address bar.

**Step 5** Enter the Day 0 **username webui** and **password cisco**.

### What to do next

Create a user account.

## Creating User Accounts

Setting a username and password is the first task you will perform on your device. Typically, as a network administrator, you will want to control access to your device and prevent unauthorized users from seeing your network configuration or manipulating your settings.

**Step 1** Log on using the default username and password provided with the device.

**Step 2** Set a password of up to 25 alphanumeric characters. The username password combination you set gives you privilege 15 access. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces.



Figure 9: Create Account

The screenshot shows the 'Create Account' step of the Cisco Configuration Setup Wizard. The wizard has six steps: CREATE ACCOUNT, BASIC SETTINGS, SITE PROFILE, SWITCH WIDE SETTINGS, PORT SETTINGS, and SUMMARY. The 'CREATE ACCOUNT' step is active, showing fields for 'Login Name', 'Password', and 'Confirm password'. A 'Create New Account' button is at the bottom center. On the right, a light blue sidebar titled 'Hardware and Software details of the device.' contains sections for 'Platform Type:', 'IOS Installed:', 'Serial Number:', 'Modules:', and 'License Installed:'. A 'Basic Device Settings >' button is at the bottom right of the sidebar.

## Choosing Setup Options

Select **Wired Network** to configure your device based on a site profile, and continue to configure switch wide settings. Otherwise, continue to the next step and configure only basic settings for your device.

## Configuring Basic Device Settings

On the **Basic Device Settings** page configure the following information:

- Step 1** In the **Device ID and Location Settings** section, type a unique name to identify your device in the network.
- Step 2** Choose the date and time settings for your device. To synchronize your device with a valid outside timing mechanism, such as an NTP clock source, choose Automatic, or choose Manual to set it yourself.

Figure 10: Basic Settings - Device ID and Location Settings

**Step 3** In the **Device Management Settings** section, assign an **IP address** to the management interface. Ensure that the IP address you assign is part of the subnet mask you enter.

**Step 4** Optionally, enter an **IP address** to specify the default gateway.

**Step 5** To enable access to the device using telnet, check the **Telnet** check box.

**Step 6** To enable secure remote access to the device using Secure Shell (SSH), check the **SSH** check box.

**Step 7** Check the **VTP transparent mode** check box to disable the device from participating in VTP.

If you did not select **Wired Network**, in the earlier step, continue to the next screen to verify your configuration on the **Day 0 Config Summary** screen, and click **Finish**. To automatically configure your device based on a site profile, click **Setup Options**, and select **Wired Network**.

Figure 11: Basic Settings - Device Management Settings

## Configuring Your Device Based on a Site Profile

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.

**Table 1: Default Configuration Loaded with Each Site Profile (Access Switches)**

Setting	Single Access Switch (Single Uplink)	Single Access Switch (Single Port Channel Uplink)	Single Access Switch (Redundant Port Channel Uplink)
Hostname	The hostname or device name you provided as part of Quick Setup	The hostname or device name you provided as part of Quick Setup	The hostname or device name you provided as part of Quick Setup
Spanning Tree Mode	RPVST+	RPVST+	RPVST+
VTP	Mode Transparent	Mode Transparent	Mode Transparent
UDLD	Enabled	Enabled	Enabled
Error Disable Recovery	Recovery mode set to Auto	Recovery mode set to Auto	Recovery mode set to Auto
Port Channel Load Balance	Source Destination IP	Source Destination IP	Source Destination IP
SSH	Version 2	Version 2	Version 2
SCP	Enabled	Enabled	Enabled
VTY Access to Switch	Enabled	Enabled	Enabled
Service Timestamp	Enabled	Enabled	Enabled
VLAN	The following VLANs are created: <ul style="list-style-type: none"> <li>• Default VLAN</li> <li>• Data VLAN</li> <li>• Voice VLAN</li> <li>• Management VLAN</li> </ul>	The following VLANs are created: <ul style="list-style-type: none"> <li>• Default VLAN</li> <li>• Data VLAN</li> <li>• Voice VLAN</li> <li>• Management VLAN</li> </ul>	The following VLANs are created: <ul style="list-style-type: none"> <li>• Default VLAN</li> <li>• Data VLAN</li> <li>• Voice VLAN</li> <li>• Management VLAN</li> </ul>

Setting	Single Access Switch (Single Uplink)	Single Access Switch (Single Port Channel Uplink)	Single Access Switch (Redundant Port Channel Uplink)
Management Interface	Layer 3 settings configured on the management port, based on Quick Setup	Layer 3 settings configured on the management port, based on Quick Setup	Layer 3 settings configured on the management port, based on Quick Setup
IPv6 Host Policy	IPv6 host policy created	IPv6 host policy created	IPv6 host policy created
QoS Policy for Downlink Ports	Auto QoS Policy for Access defined	Auto QoS Policy for Access defined	Auto QoS Policy for Access defined
QoS Policy for Uplink Ports	QoS Policy for Distribution created	QoS Policy for Distribution created	QoS Policy for Distribution created
Uplink Interfaces	Selected uplink interfaces configured as trunk ports, set to allow all VLANs	Selected ports configured as Port-channel in trunk mode, set to allow all VLANs.	Selected ports configured as Port-channel in trunk mode, set to allow all VLANs.
Downlink Interfaces	Downlink ports configured in Access mode	Downlink ports configured in Access mode	Downlink ports configured in Access mode
Port-channel	Not configured	Port-channel to distribution created	Port-channel to distribution created

Figure 12: Site Profile - Access Switches

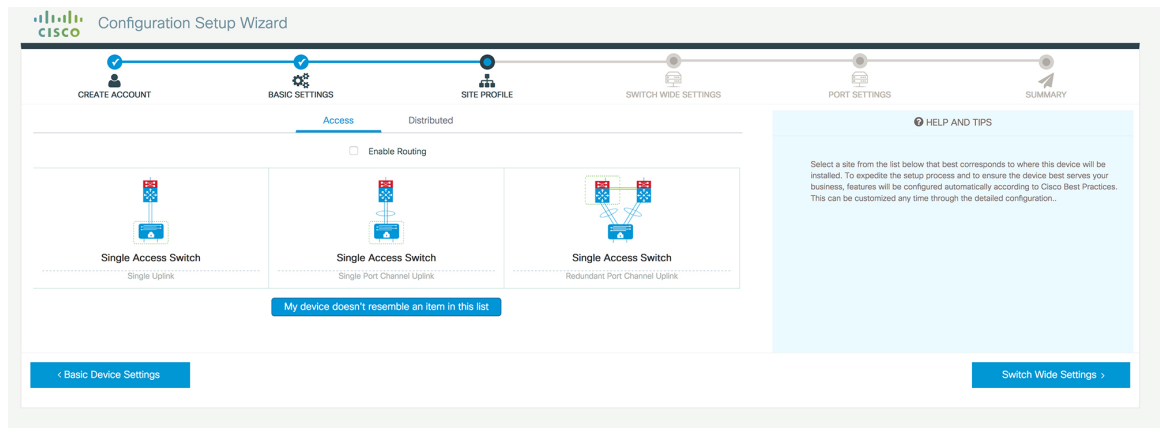
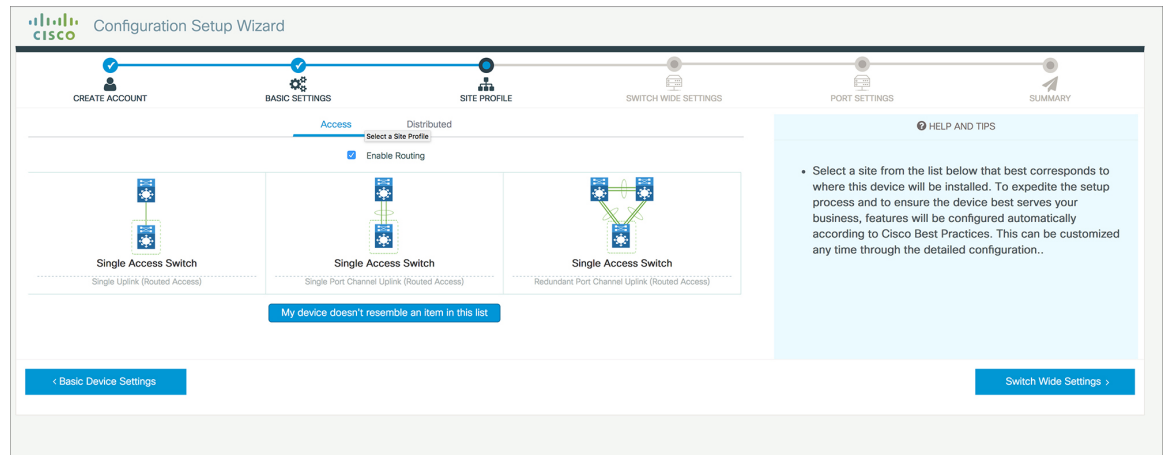


Figure 13: Site Profile - Access Switches (with Routed Access)



## Configuring VLAN Settings

- Step 1** In the **VLAN Configuration** section, you can configure both data and voice VLANs. Type a name for your data VLAN.
- Step 2** To configure a data VLAN, ensure that the **Data VLAN** check box is checked, type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range.
- Step 3** To configure a voice VLAN, ensure that the **Voice VLAN** check box is checked, type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate a VLAN range.

## Configure STP Settings

- Step 1** RPVST is the default STP mode configured on your device. You can change it to PVST from the **STP Mode** drop-down list.
- Step 2** To change a bridge priority number from the default value 32748, change **Bridge Priority** to Yes and choose a priority number from the drop-down list.

Figure 14: VLAN and STP Settings

The screenshot shows the Cisco Configuration Setup Wizard interface. At the top, a progress bar indicates the current step is 'SWITCH WIDE SETTINGS', with previous steps 'CREATE ACCOUNT', 'BASIC SETTINGS', and 'SITE PROFILE' completed. The main content area is divided into three sections: 'VLAN Configuration', 'STP Configuration', and 'General Configuration'. Under 'VLAN Configuration', there are three checkboxes: 'Data VLAN', 'Voice VLAN', and 'Management Vlan Switch Wide Settings'. Under 'STP Configuration', the 'STP Mode' is set to 'RPVST', 'Bridge Priority' is checked, and the 'Bridge Priority Number' is set to '32768'. A 'HELP AND TIPS' sidebar on the right provides information about VLANs and STP. At the bottom, there are navigation buttons: '< Site Profile' and 'Port Settings >'. The Cisco logo is in the top left corner.

## Configuring DHCP, NTP, DNS and SNMP Settings

- Step 1** In the **Domain Details** section, enter a domain name that the software uses to complete unqualified hostnames.
- Step 2** Type an IP address to identify the DNS server. This server is used for name and address resolution on your device.
- Step 3** In the **Server Details** section, type the IP address of the DNS server that you want to make available to DHCP clients.
- Step 4** In the **Syslog Server** field, type the IP address of the server to which you want to send syslog messages.
- Step 5** To ensure that your device is configured with the right time, date and timezone, enter the IP address of the NTP server with which you want to synchronize the device time.
- Step 6** In the **Management Details** section, type an IP address to identify the SNMP server. SNMPv1, SNMPv2, and SNMPv3 are supported on your device.
- Step 7** Specify the **SNMP community** string to permit access to the SNMP protocol.

Figure 15: DHCP, NTP, DNS and SNMP Settings

**Configuration Setup Wizard**

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

**General Configuration**

**Domain Details**

Domain Name

DNS Server

**Server Details**

DHCP Server

Syslog Server

NTP Server

**Management Details**

< Site Profile Port Settings >

**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.

**What to do next**

Configure port settings.

## Configuring Port Settings

- Step 1** Based on the site profile chosen in the earlier step which is displayed in the left-pane, select the **Port Role** from among the following options:
- 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.
- Step 2** Choose an option from the **Select Switch** drop-down list.
- Step 3** Make selections from the **Available** list of interfaces based on how you want to enable them and move them to the **Enabled** list.

Figure 16: Port Settings

The screenshot shows the 'Port Settings' step in the 'Configuration Setup Wizard'. The wizard has six steps: CREATE ACCOUNT, BASIC SETTINGS, SITE PROFILE, SWITCH WIDE SETTINGS, PORT SETTINGS (current), and SUMMARY. On the left, a network diagram shows a switch with a port highlighted. The main area has a 'Port Role' section with 'Uplink' selected and 'Access' unselected. Below it, 'Select Switch' is set to 'ALL'. A list of 'Available (16)' interfaces is shown: GigabitEthernet1/1/1, GigabitEthernet1/1/2, GigabitEthernet1/1/3, and GigabitEthernet1/1/4. To the right, an 'Enabled (0)' section shows a list of 'Interfaces'. At the bottom, there are buttons for '< Switch Wide Settings' and 'Day 0 Config Summary >'. The Cisco logo is in the top left corner.

### What to do next

- Click **Day 0 Config Summary** to verify your setup.
- Click **Finish**.

Figure 17: Day 0 Config Summary

The screenshot shows the 'Day 0 Config Summary' step in the 'Configuration Setup Wizard'. The wizard has six steps: CREATE ACCOUNT, BASIC SETTINGS, SITE PROFILE, SWITCH WIDE SETTINGS, PORT SETTINGS, and SUMMARY (current). The 'SUMMARY' section is active, showing a list of configuration items on the left and their status on the right. The items are: General Information, Basic Device Configuration, Global Switch Settings, and Port Configuration. The status for each item is: 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-pwst, Bridge Priority: 32768, DNS Server: , DHCP Server: , NTP Server: , Syslog Server: , SNMP Server: ), and Port Configuration (Uplink Ports: No Ports were configured, Downlink Ports: No Ports were configured). At the bottom, there are buttons for '< Port Settings' and 'Finish >'. The Cisco logo is in the top left corner.

## Configuring VTY Lines

For connecting to the device through Telnet or SSH, the Virtual Terminal Lines or Virtual TeleType (VTY) is used. The number of VTY lines is the maximum number of simultaneous access to the device remotely. If the device is not configured with sufficient number of VTY lines, users might face issues with connecting to the WebUI. The default value for VTY Line is 0-15. The device allows up to 98 simultaneous sessions.



**Step 1** From the WebUI, navigate through **Administration > Device** and select the **General** page.

**Step 2** In the **VTY Line** field, enter **0-xx**, depending on how many VTY lines you want to configure.

*Figure 18: Configuring VTY Line*

The screenshot shows the WebUI configuration page for the Device General settings. The breadcrumb navigation is "Administration > Device". The left sidebar contains a search bar and a menu with the following items: Dashboard, Monitoring, Configuration, Administration (highlighted), Licensing, and Troubleshooting. The main content area is divided into two columns. The left column has tabs for "General" (selected), "FTP/SFTP/TFTP", and "Bluetooth". The right column contains the following settings:

Setting	Value
IP Routing	<input type="checkbox"/> DISABLED
Host Name*	SW-9200
Banner	
Management Interface	GigabitEthernet0/0
IP Address*	
Subnet Mask*	
System MTU(Bytes)	1500
VTY Line	0-30
VTY Transport Mode	Select a value

There is a "View VTY options" link next to the VTY Line field.

