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

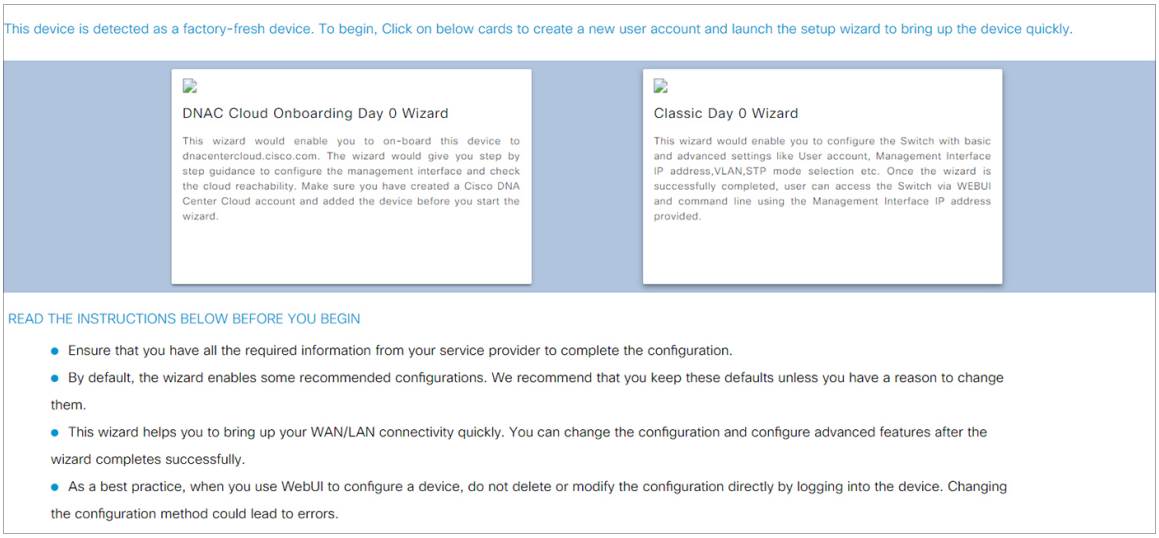
After you complete the hardware installation, you need to setup the switch with configuration required to enable traffic to pass through the network. On your first day with your new device, you can perform a number of tasks to ensure that your device is online, reachable and easily configured.

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.

Procedure

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

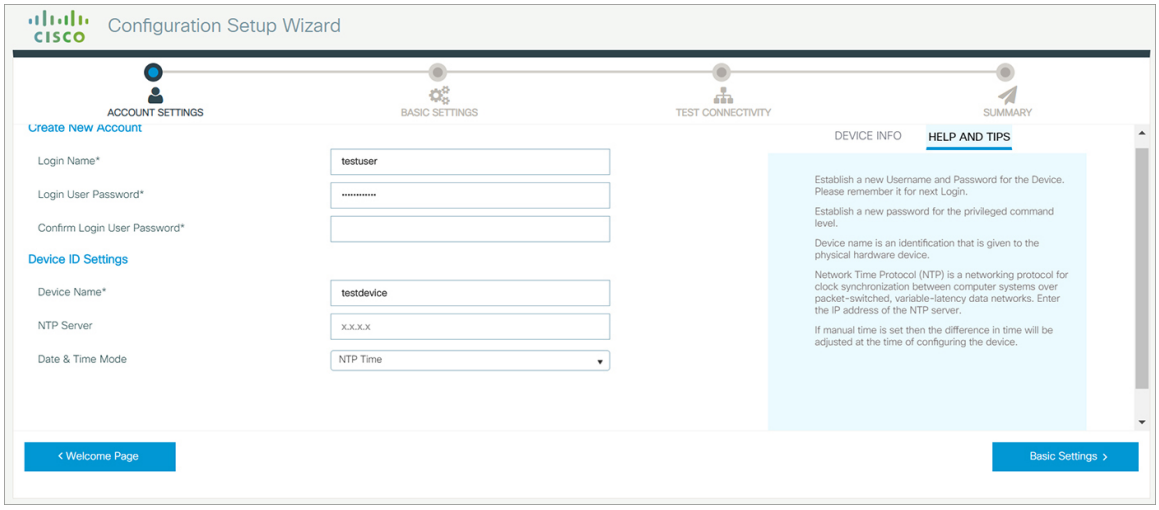
Step 2 Set a password of up to 25 alphanumeric characters.

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



Configuring Basic Device Settings

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

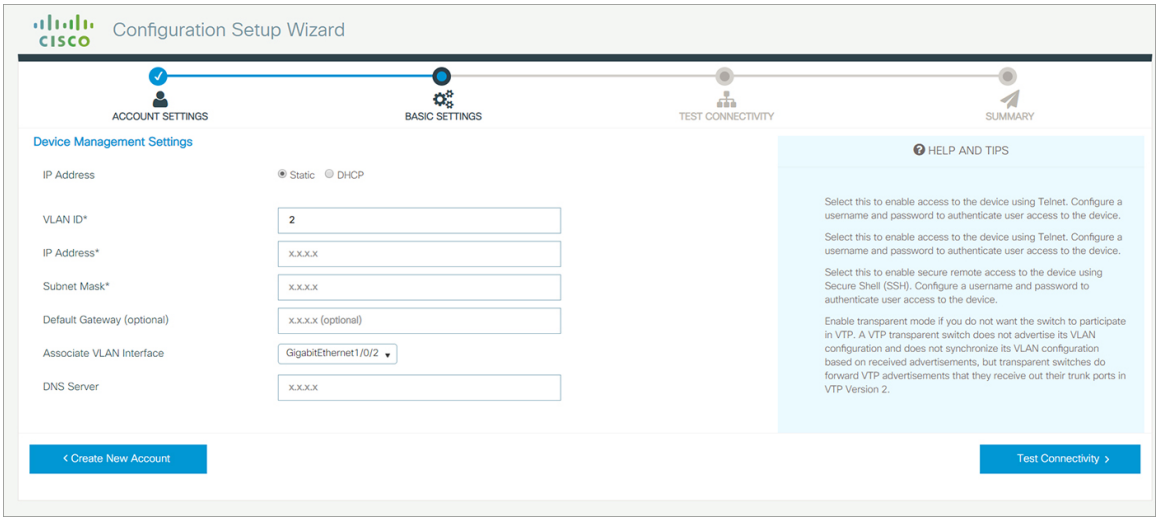
Procedure

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:

a) Enter a VLAN ID to associate with the interface in the **Associate VLAN Interface** drop-down list.
b) Ensure that the IP address you assign is part of the subnet mask you enter.
c) Optionally, enter an IP address to specify the default gateway.
d) Enter the address of the DNS Server.

Figure 3: Basic Settings - Static Configuration



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

a) Enter a value in the VLAN ID field.

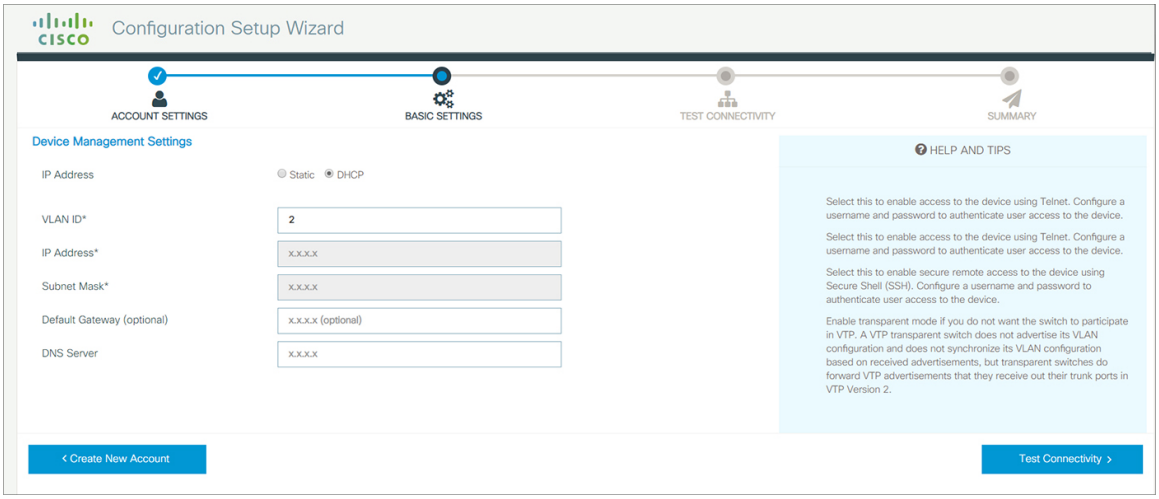
VLAN ID must be a value other than 1.

b) Ensure that the IP address you assign is part of the subnet mask you enter.

c) Optionally, enter an IP address to specify the default gateway.

d) Enter the address of the DNS Server.

Figure 4: Basic Settings - DHCP Configuration



Configuring Test Connectivity

Procedure

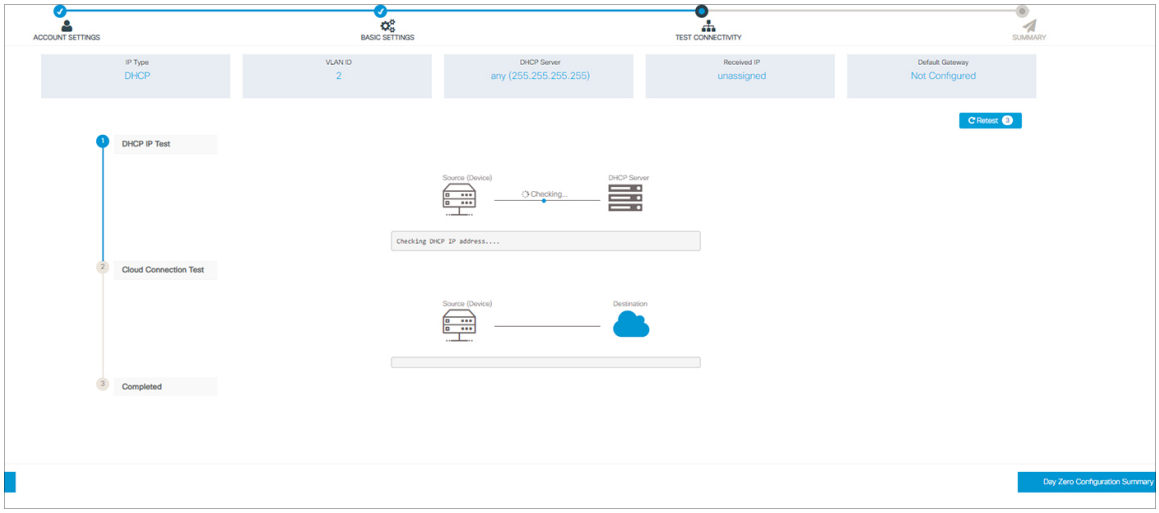
Step 1 Use the **Test Connectivity/Retest** button to ensure that connection is established between the device to the Cisco DNAC Cloud.

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

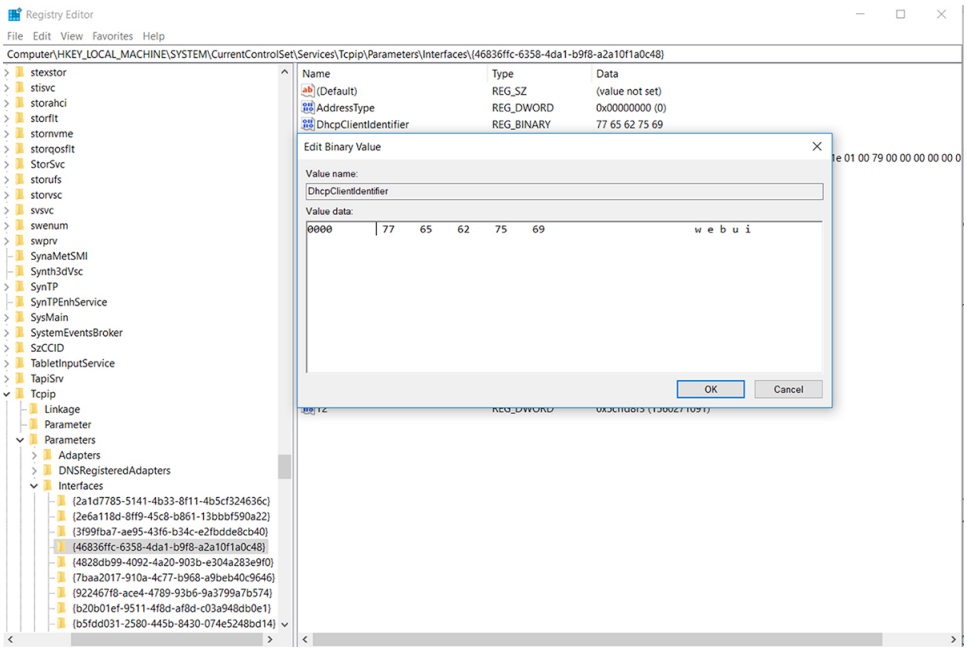
Set up the DHCP Client Identifier on the client to get the IP address from the switch, and to be able to authenticate with Day 0 login credentials.

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

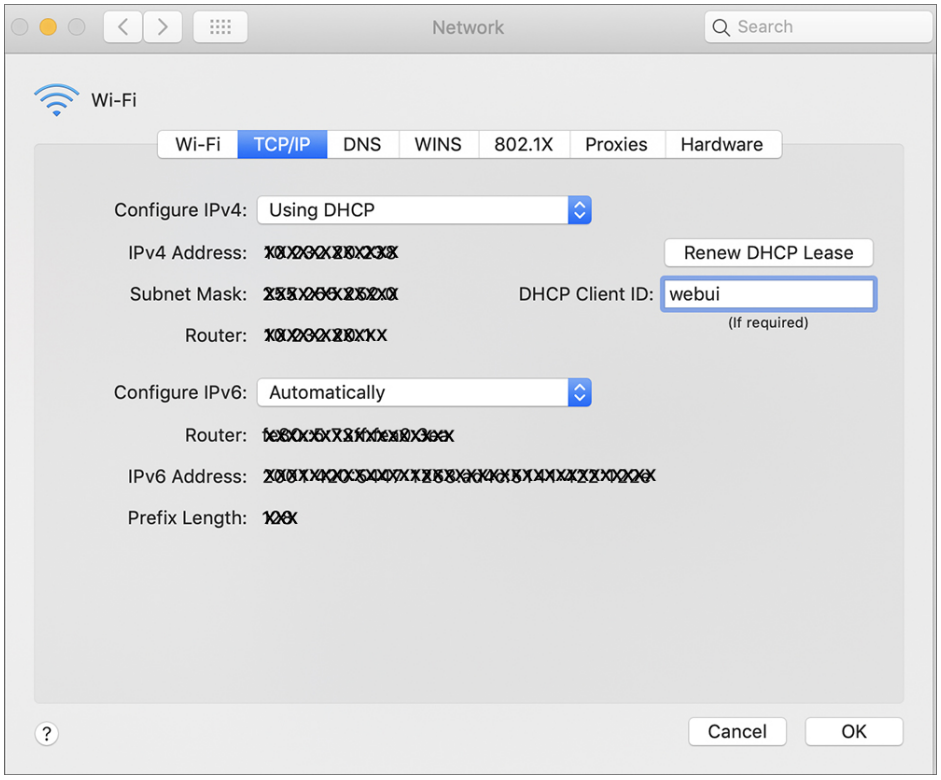


5. Restart the PC for the configuration to take effect.

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:

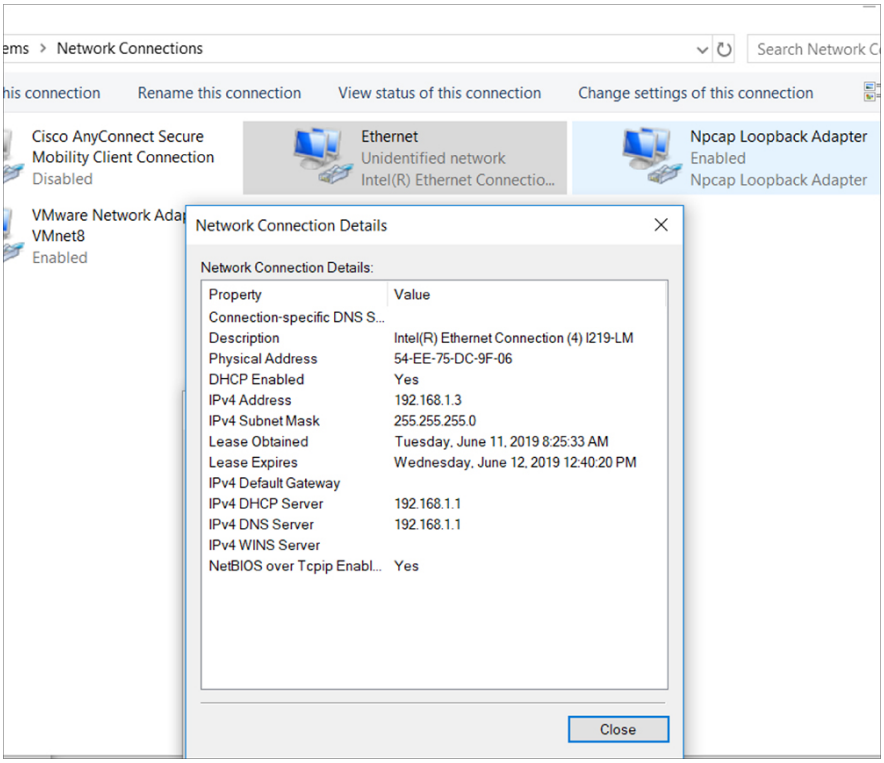
Procedure

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.

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

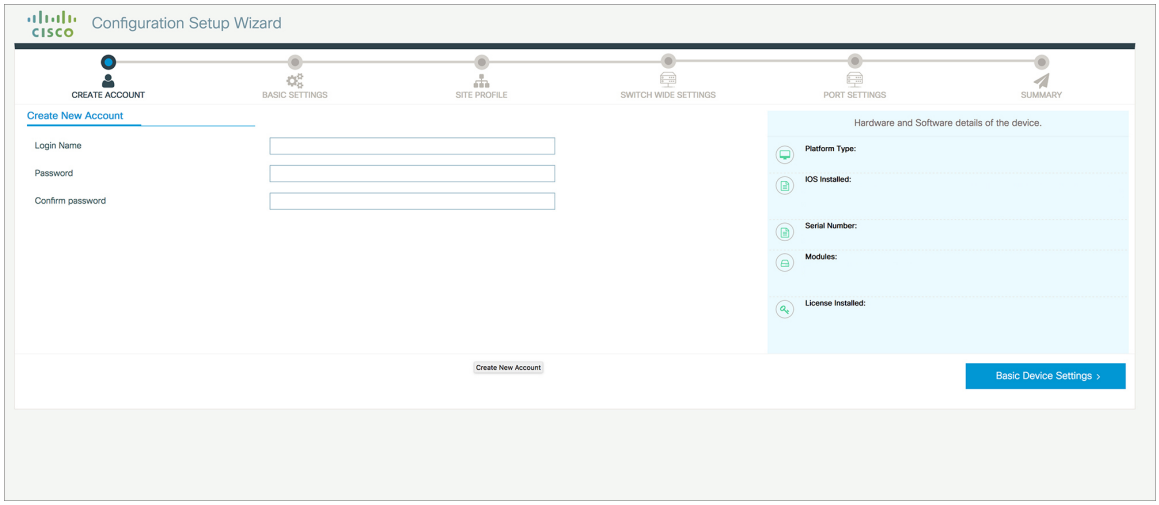
Setting a username and password is the first task you will perform on your device. Typically, as a network administrator, you will want to control access to your device and prevent unauthorized users from seeing your network configuration or manipulating your settings.

Procedure

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



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

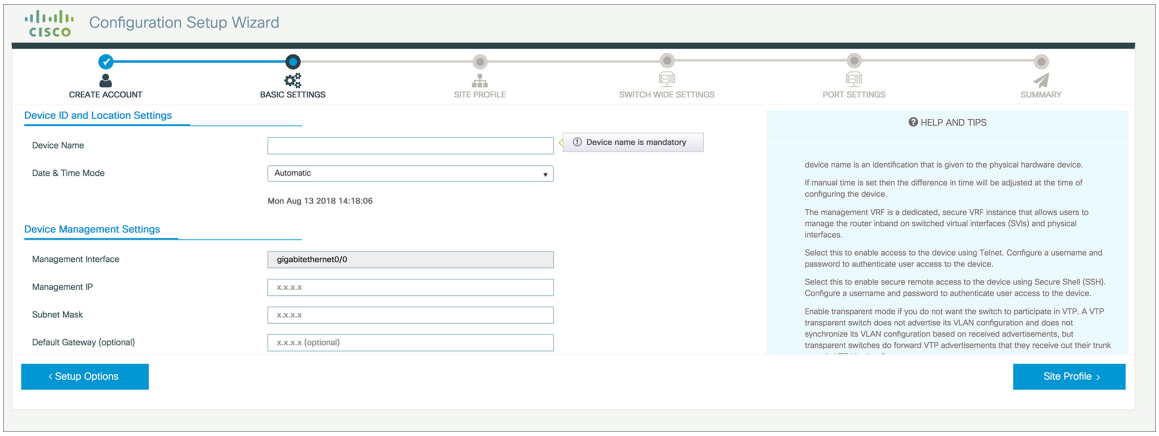
On the **Basic Device Settings** page configure the following information:

Procedure

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.

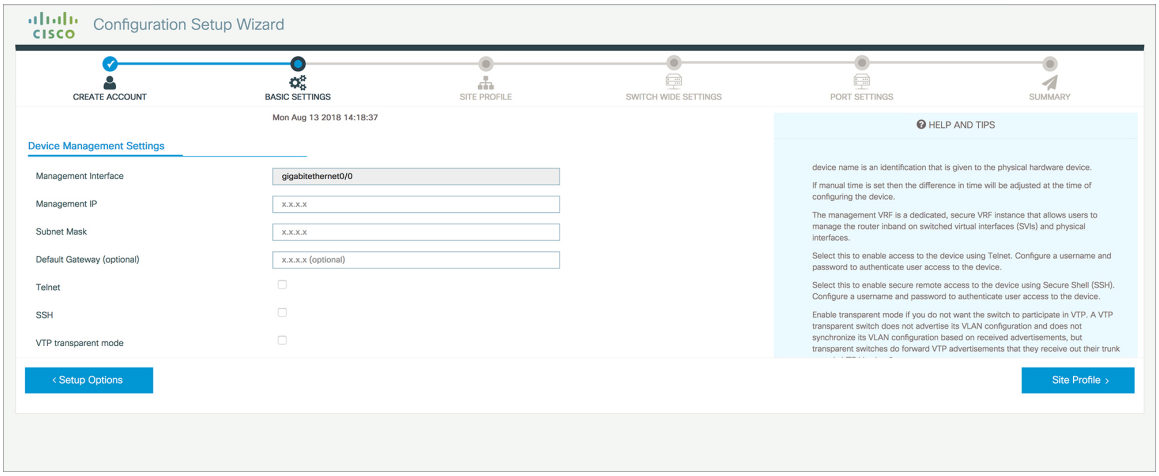
Step 5 To enable access to the device using telnet, check the **Telnet** check box.

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 (Distribution Switches)

Setting	Single Distribution Switch (Single Downlink)	Single Distribution Switch (Single Port Channel Downlink)	Redundant Distribution Switch (Port Channel Peer and Downlink)
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: • Default VLAN • Data VLAN • Voice VLAN • Management VLAN	The following VLANs are created: • Default VLAN • Data VLAN • Voice VLAN • Management VLAN	The following VLANs are created: • Default VLAN • Data VLAN • Voice VLAN • Management VLAN
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
QoS Policy	QoS Policy for Distribution defined	QoS Policy for Distribution defined	QoS Policy for Distribution defined

Setting	Single Distribution Switch (Single Downlink)	Single Distribution Switch (Single Port Channel Downlink)	Redundant Distribution Switch (Port Channel Peer and Downlink)
Uplink Interfaces	Selected uplink ports connect to other distribution or core switches	Selected uplink ports connect to other distribution or core switches	Selected uplink ports connect to other distribution or core switches
Downlink Interfaces	Downlink connections to access switches configured in Trunk mode	Downlink connections to access switches configured in Trunk mode	Downlink connections to access switches configured in Trunk mode
Port-channel	Port-channel to core created	Port-channel to core or access created	Port-channel to core or distribution created

Figure 12: Site Profile - Distribution Switches

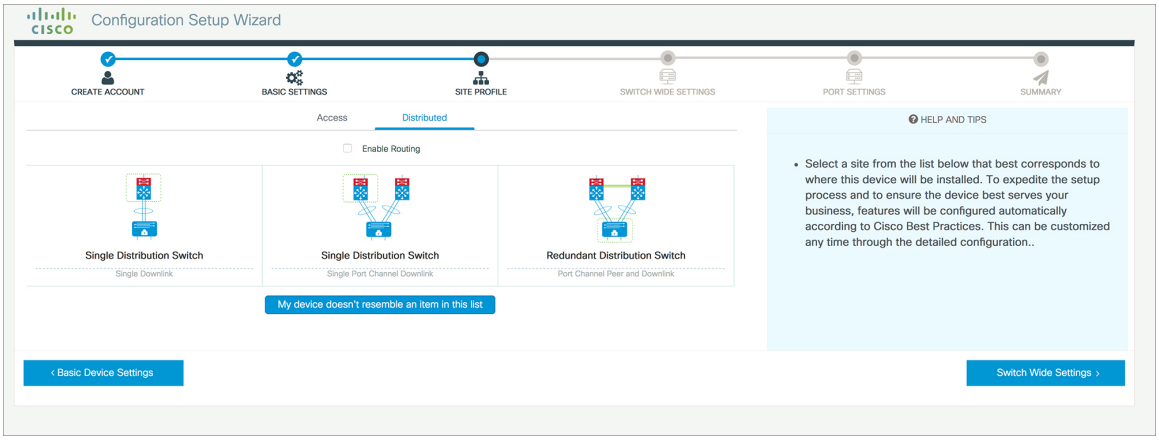


Figure 13: Site Profile - Distribution Switches (with Routed Access)

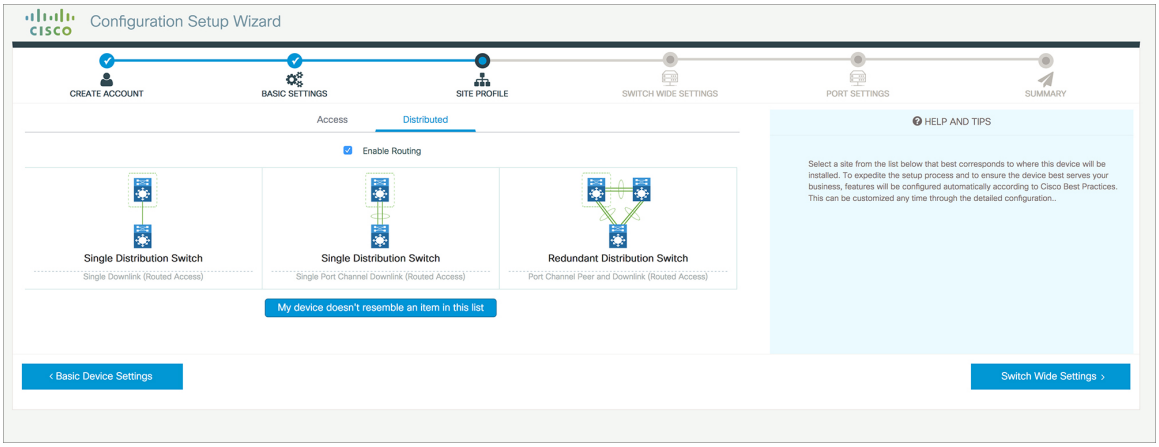
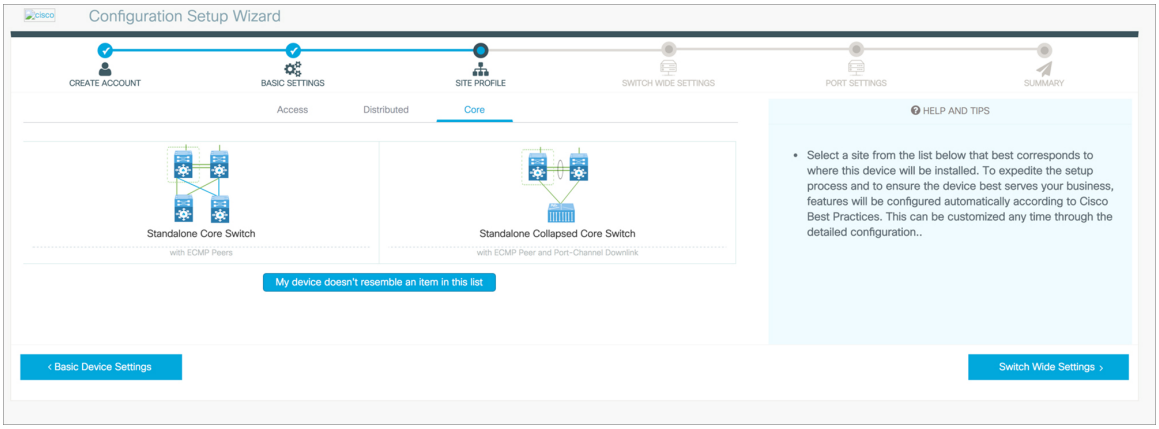


Table 2: Default Configuration Loaded with Each Site Profile (Core Switches)

Setting	Standalone Core Switch (with ECMP Peers)	Standalone Collapsed Core Switch (with ECMP Peer and Port Channel Downlink)
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
UDLD	Enabled	Enabled
Error Disable Recovery	Recovery mode set to Auto	Recovery mode set to Auto
Port Channel Load Balance	Source Destination IP	Source Destination IP
SSH	Version 2	Version 2
SCP	Enabled	Enabled
VTY Access to Switch	Enabled	Enabled
Mitigate Address Spoofing	Unicast RPF (uRPF) in strict mode	Unicast RPF (uRPF) in strict mode
Service Timestamp	Enabled	Enabled
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
QoS Policy	QoS Policy for Distribution/Core defined	QoS Policy for Distribution/Core defined
Uplink Interfaces	Selected uplink ports connect to MAN/WAN device	Selected uplink ports connect to MAN/WAN device
Downlink Interfaces	Downlink connections to access switches	Downlink connections to distribution switches
Cross-connect Interfaces	Selected ports connect to other core switches	Selected ports connect to other core switches

Figure 14: Site Profile - Core Switches



Configuring VLAN Settings

Procedure

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.

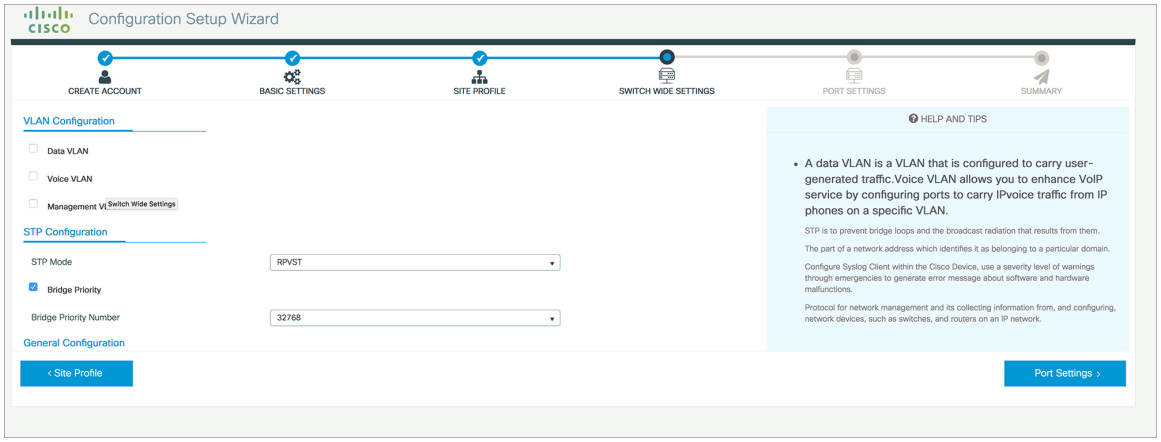
Configure STP Settings

Procedure

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 15: VLAN and STP Settings



Configuring DHCP, NTP, DNS and SNMP Settings

Procedure

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.

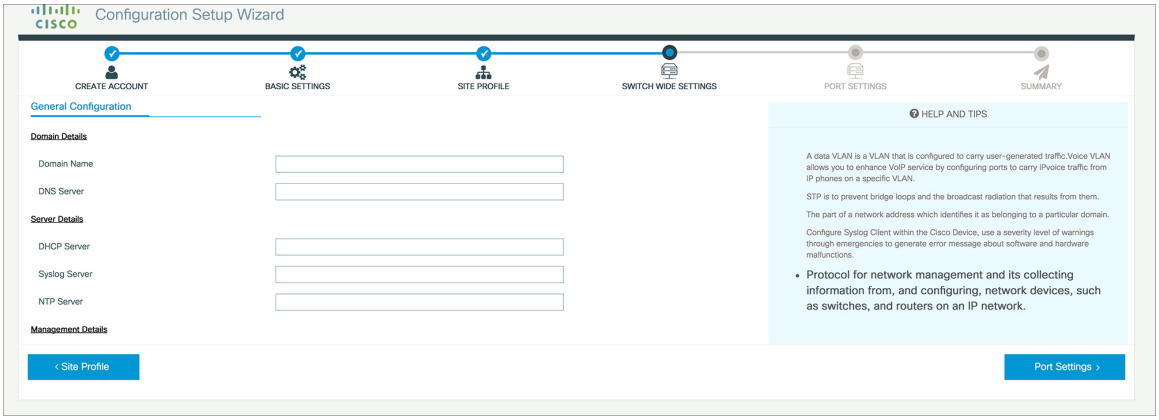
Step 4 In the **Syslog Server** field, type the IP address of the server to which you want to send syslog messages.

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 16: DHCP, NTP, DNS and SNMP Settings



What to do next

Configure port settings.

Configuring Port Settings

Procedure

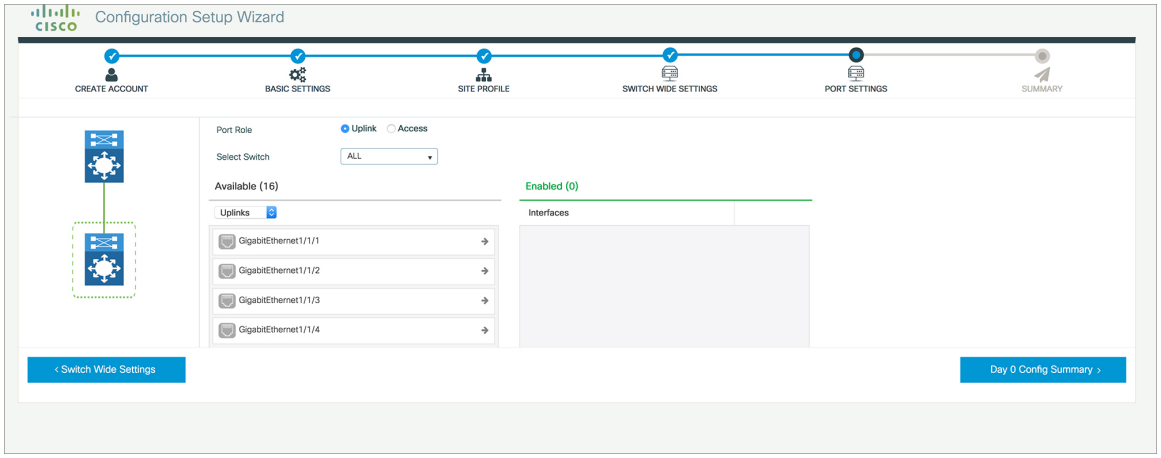
Step 1 Based on the site profile chosen in the earlier step which is displayed in the left-pane, select the **Port Role** from among the following options:

- 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.

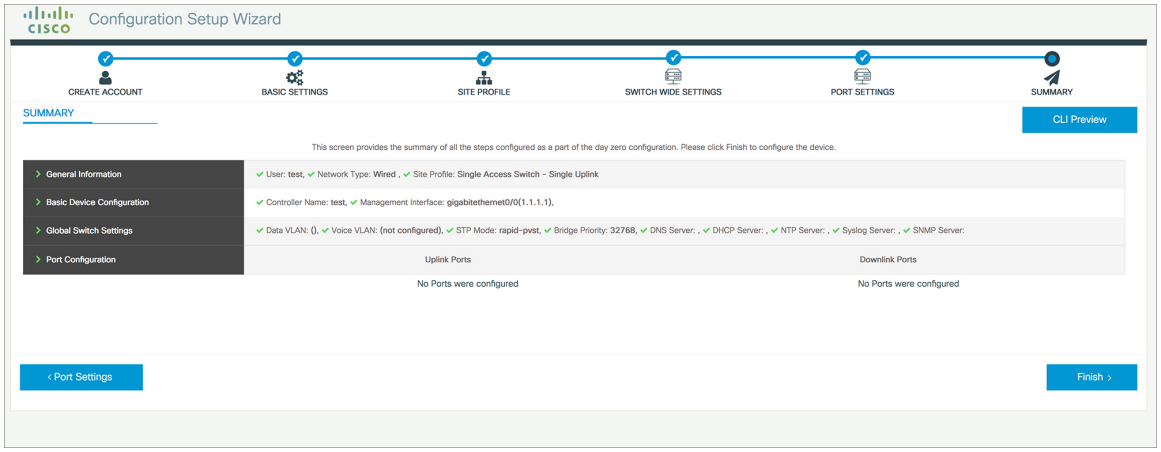
Figure 17: Port Settings



What to do next

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

Figure 18: Day 0 Config Summary



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 99 simultaneous sessions.

Procedure

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 19: Configuring VTY Line