

Introduction to Day 0 WebUI Configuration

This chapter contains the following sections:

- Classic Day 0 Wizard, on page 1
- Connecting to the Switch, on page 1
- Creating User Accounts, on page 3
- Choosing Setup Options, on page 4
- Configuring Basic Device Settings, on page 4
- Configuring Your Device Based on a Site Profile, on page 7
- Configuring VLAN Settings, on page 12
- Configure STP Settings, on page 13
- Configuring DHCP, NTP, DNS and SNMP Settings, on page 13
- Configuring Port Settings, on page 14
- Configuring VTY Lines, on page 15

Classic Day 0 Wizard

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.

Connecting to the Switch

You can configure the device with both basic and advanced settings as outlined here. Once configured, access the device through the WebUI using the management interface's IP address

Before you begin

Verify that you have completed the Express Setup. For more details, see the *Cisco Catalyst IE9300 Rugged Series Switch Hardware Installation Guide*.

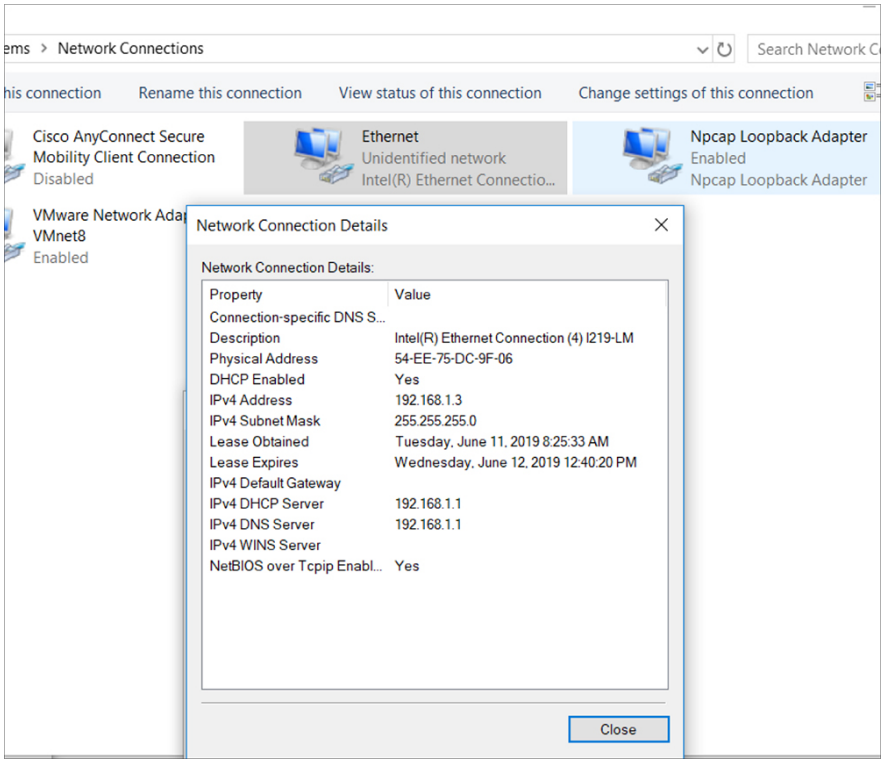
Verify that no devices are connected to the switch.

Connect one end of an ethernet cable to the switch and the other end of the ethernet cable to the host computer.

Procedure

Step 1 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 1: 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 2 Launch a web browser on the PC and enter the device IP address (`https://192.168.1.1`) in the address bar.

Step 3 Enter the Day 0 **username** `webui` and **password** `cisco`.

Note
By default, the login username is admin, and the password is the system serial number. You can change it as required.

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

Step 2 Enter the username in the **Login Name**.

Step 3 Enter **password** in the **Login User Password**.

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

Step 4 Reconfirm the password for the user in the **Confirm Login User Password**.

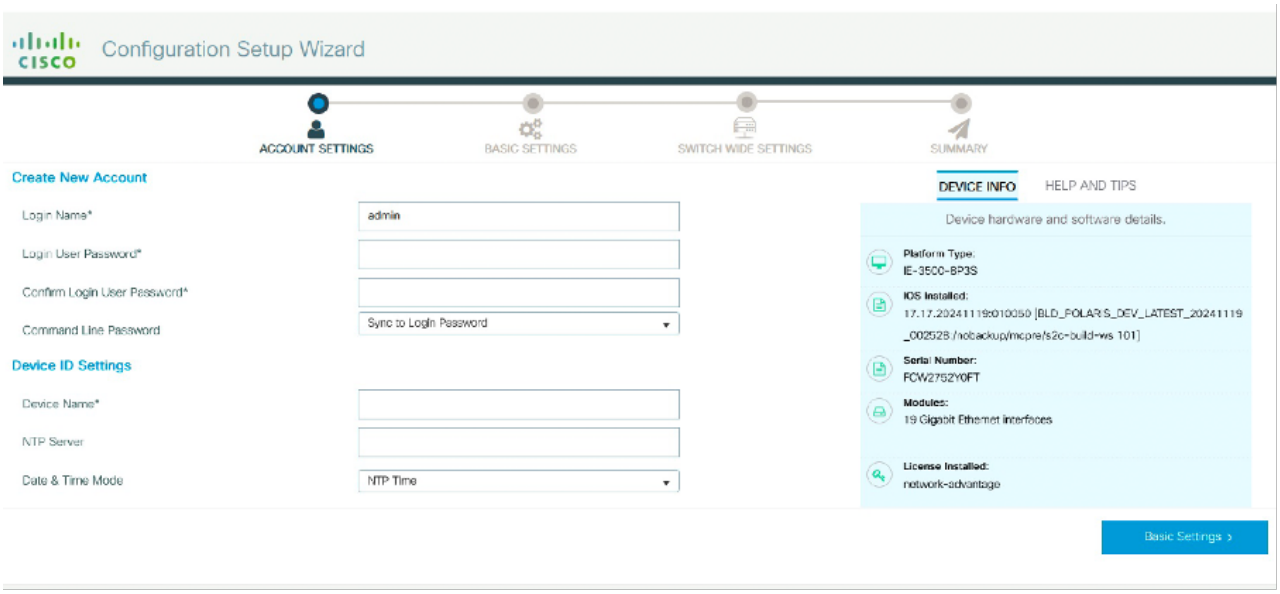
Step 5 Use the **Command Line Password** drop-down list to choose where to synchronize the password.

Step 6 In the Device ID Settings section, enter a value in the **Device Name**.

Step 7 (Optional) Enter NTP server details in the **NTP Server**.

Step 8 Use the **Date & Time Mode** drop-down list to select NTP time.

Figure 2: 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** configure this information.

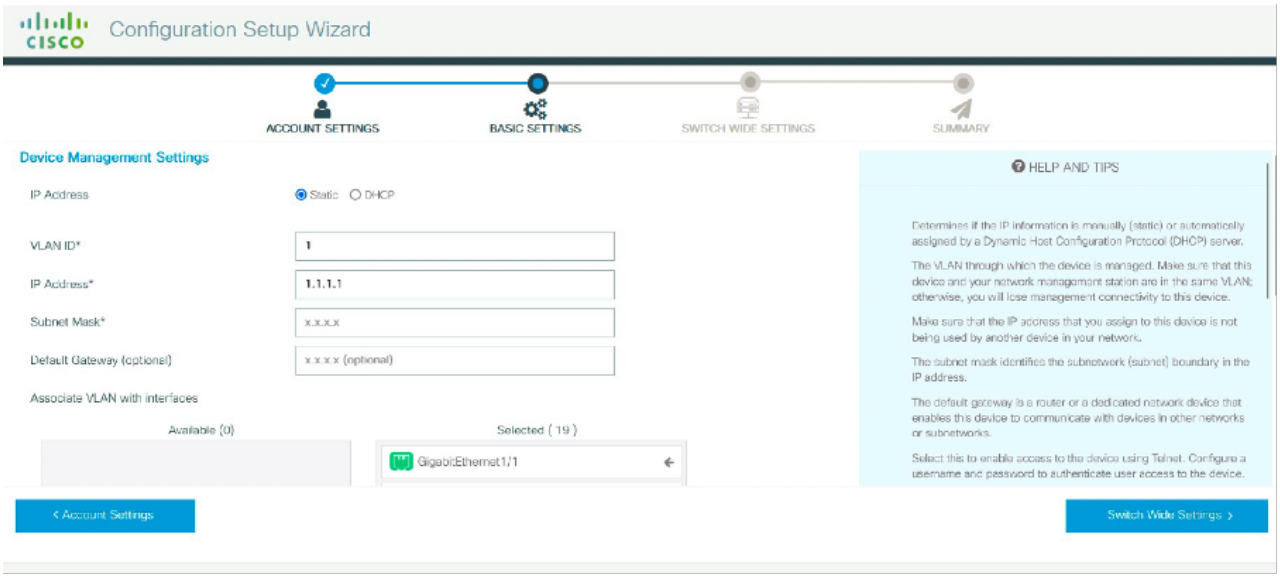
Procedure

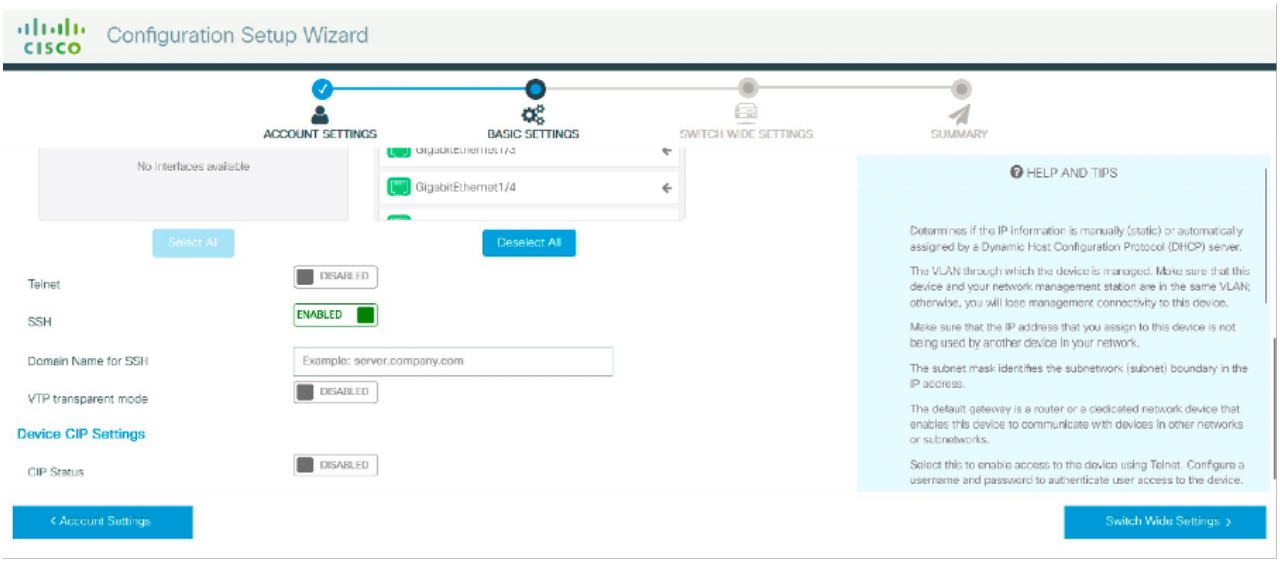
Step 1 In the **Device Management Settings** assign an IP address to the management interface using either Static or DHCP address.

Step 2 If you choose **Static**, perform these steps.

- Enter a value in **VLAN ID** to associate with the interface.
- Enter a value in **IP Address** . Ensure that the IP address you assign is part of the subnet mask you enter.
- Enter a value in **Subnet Mask**.
- (Optional) Enter a value in **Default Gateway**.
- Use the **Associated VLAN with Interface** section to select interfaces.
- (Optional) Use the slider next to **Telnet** to enable access to the device using telnet.
- (Optional) Use the slider next to **SSH** to enable secure remote access to the device using Secure Shell (SSH).
- (Optional) Use the slider next to **SSH** to enable secure remote access to the device using Secure Shell (SSH).
- (Optional) Use the slider next to **VTP Transparent Mode** to manage VLANs across a network of switches.
- (Optional) In the Device CIP Settings section, use the slider next to **CIP Status** to enable CIP. CIP is used for monitoring and diagnosing the health and functionality of industrial networks and devices.

Figure 3: Basic Settings - Device ID and Location Settings



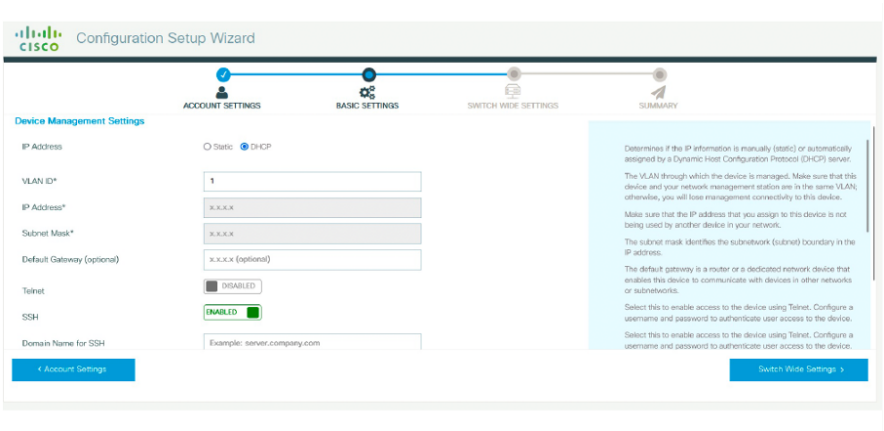


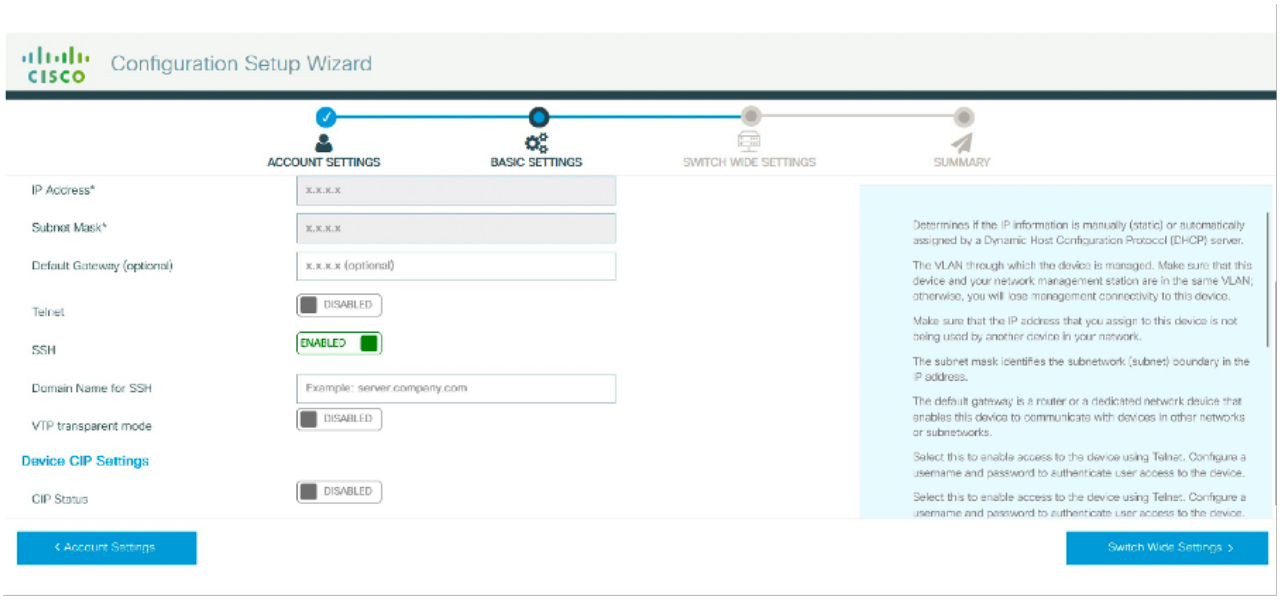
Step 3 If you choose **DHCP**, perform these steps.

- Enter a value in the **VLAN ID** to associate with the interface. **VLAN ID** must be a value other than 1.
- Enter a value in **IP Address** to specify the default gateway. Ensure that the IP address you assign is part of the subnet mask you enter.
- Enter a value in **Subnet Mask**.
- (Optional) Enter a value in **Default Gateway**.
- (Optional) Use the slider next to **Telnet** to enable access to the device using telnet.
- (Optional) Use the slider next to **SSH** to to enable secure remote access to the device using SSH.

- (Optional) Enter a value in **Domain Name for SSH**
- (Optional) Use the slider next to **VTP Transparent Mode** to manage VLANs across a network of switches.
- (Optional) In the Device CIP Settings section, use the slider next to **CIP Status** to enable CIP. CIP is used for monitoring and diagnosing the health and functionality of industrial networks and devices.

Figure 4: Basic Settings - Device ID and Location Settings





Step 4 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 5 Optionally, enter an **`IP address`** to specify the default gateway.

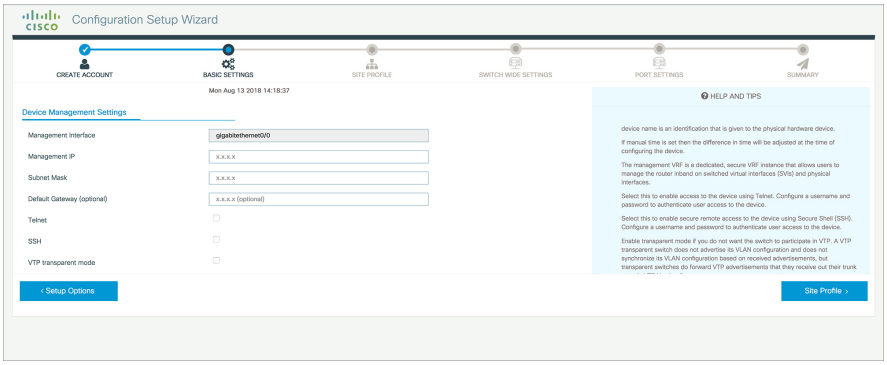
Step 6 To enable access to the device using telnet, check the **Telnet** check box.

Step 7 To enable secure remote access to the device using Secure Shell (SSH), check the **SSH** check box.

Step 8 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 5: 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

Setting	Single Access Switch (Single Uplink)	Single Access Switch (Single Port Channel Uplink)	Single Access Switch (Redundant Port Channel Uplink)
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
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 6: Site Profile - Access Switches

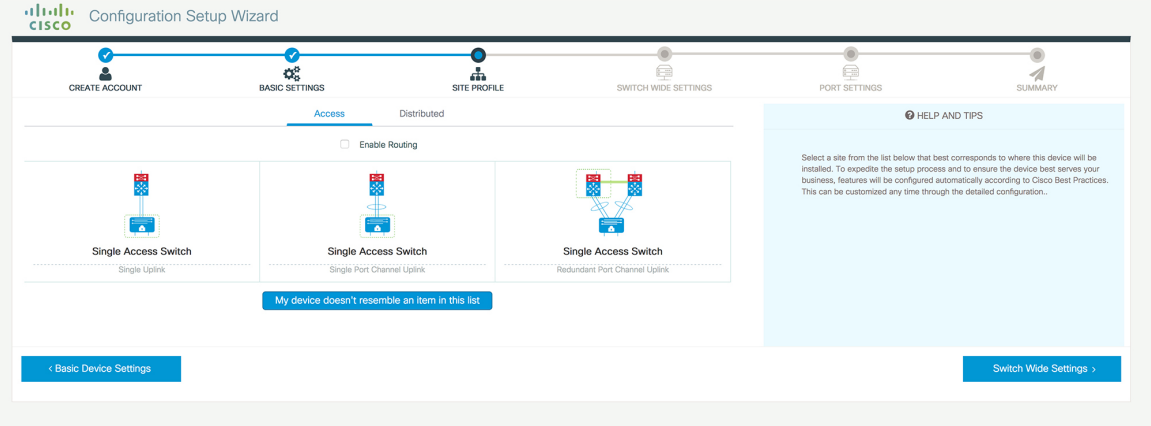


Figure 7: Site Profile - Access Switches (with Routed Access)

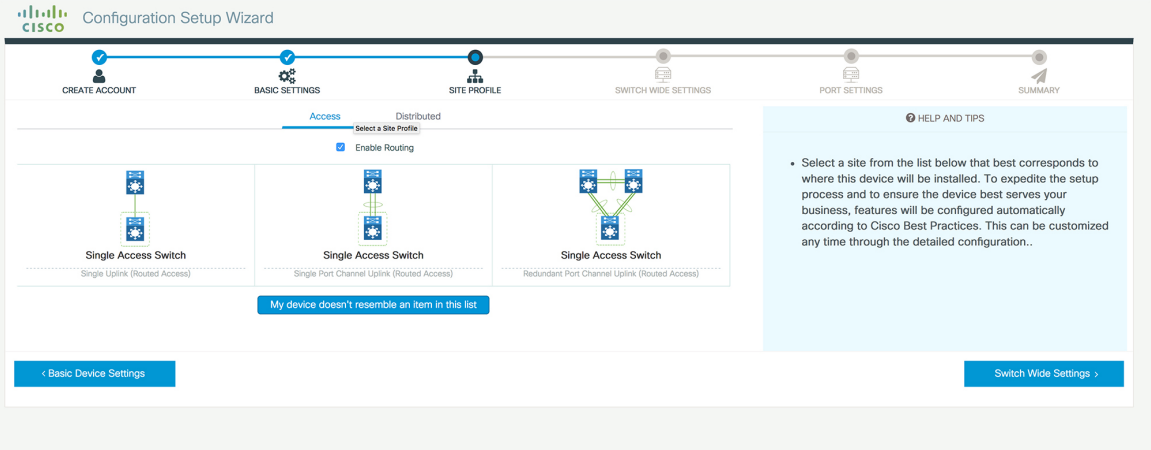


Table 2: Default Configuration Loaded with Each Site Profile (Distribution Switches)

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
SSH	Version 2	Version 2	Version 2

Setting	Single Distribution Switch (Single Downlink)	Single Distribution Switch (Single Port Channel Downlink)	Redundant Distribution Switch (Port Channel Peer and Downlink)
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
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 8: Site Profile - Distribution Switches

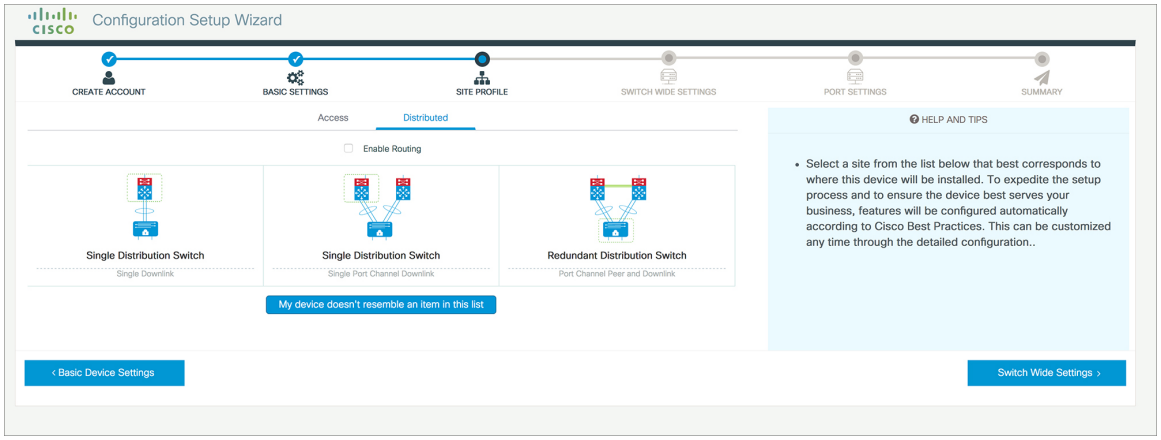


Figure 9: Site Profile - Distribution Switches (with Routed Access)

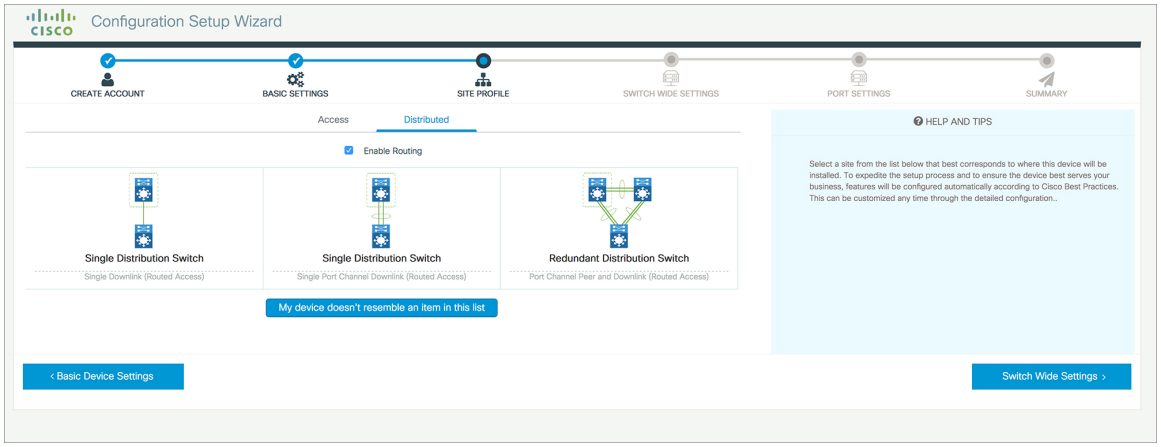
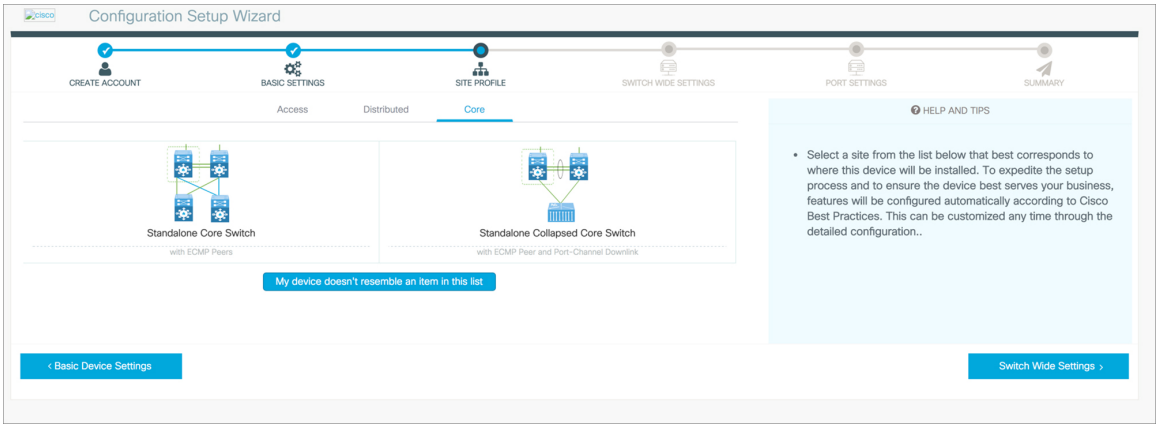


Table 3: Default Configuration Loaded with Each Site Profile (Core Switches)

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

Setting	Standalone Core Switch (with ECMP Peers)	Standalone Collapsed Core Switch (with ECMP Peer and Port Channel Downlink)
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 10: Site Profile - Core Switches



Configuring VLAN Settings

In the **VLAN Configuration**, you can configure both data and voice VLANs.

Procedure

Step 1 Use the slider next to **Data VLAN** to enable data VLAN.

Step 2 Use the slider next to **Voice VLAN** to enable voice VLAN.

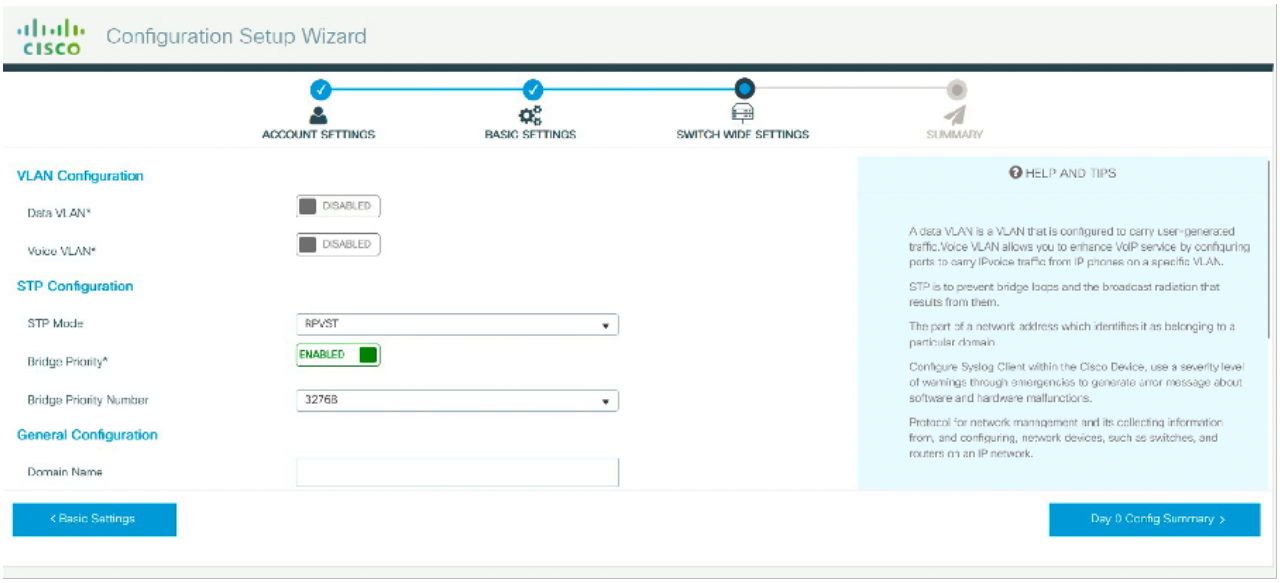
Configure STP Settings

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 11: VLAN and STP Settings



Configuring DHCP, NTP, DNS and SNMP Settings

Procedure

Step 1 In the **Domain Details**, enter a domain name that the software uses to complete unqualified hostnames.

Step 2 In the **DNS Server**, 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 **DHCP Server**, type the IP address of the DNS server that you want to make available to DHCP clients.

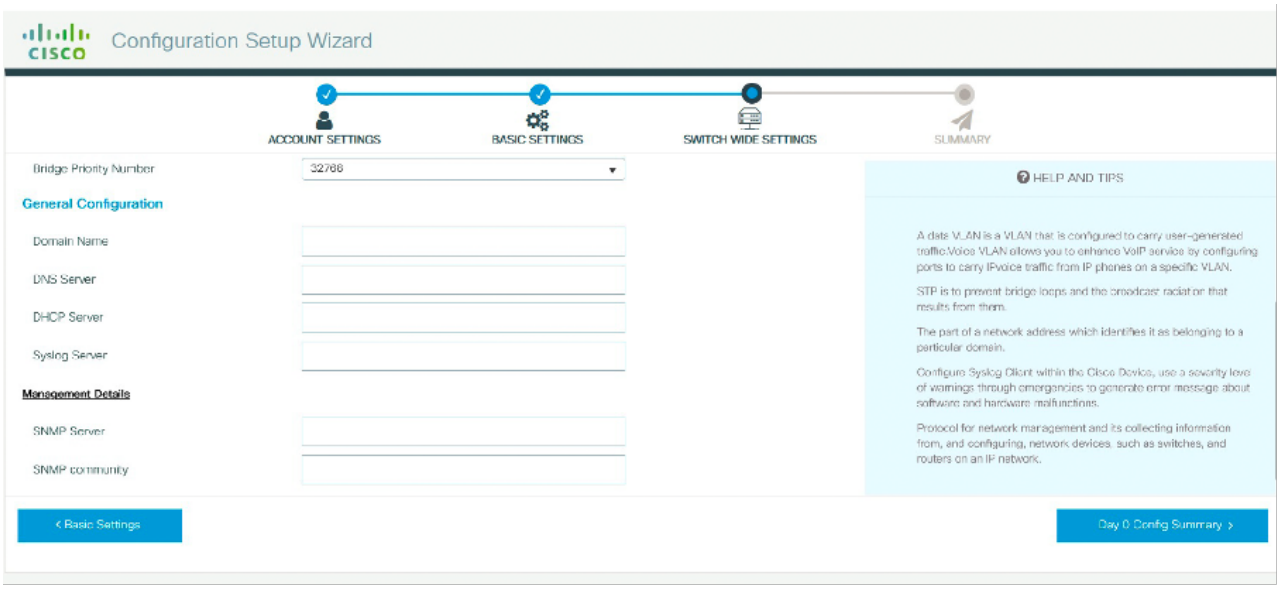
Step 4 In the **Syslog Server**, type the IP address of the server to which you want to send syslog messages.

Step 5 In the **Management Details**, type an IP address to identify the SNMP server in the **SNMP Server**.

Supported SNMP versions areare SNMPv1, SNMPv2, and SNMPv3.

Step 6 Specify the **SNMP community** string to permit access to the SNMP protocol.

Figure 12: DHCP, NTP, DNS and SNMP Settings



What to do next

Configure port settings.

Configuring Port Settings

Procedure

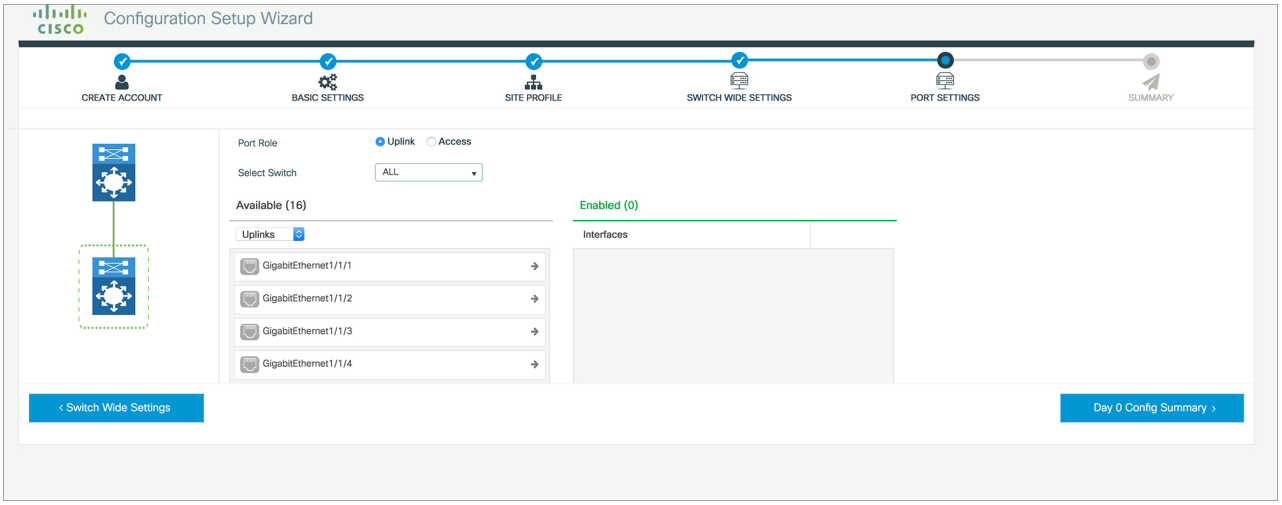
Step 1 Based on the site profile chosen in the earlier step which is displayed in the left-pane, select the **Port Role** from among the following options:

- 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.

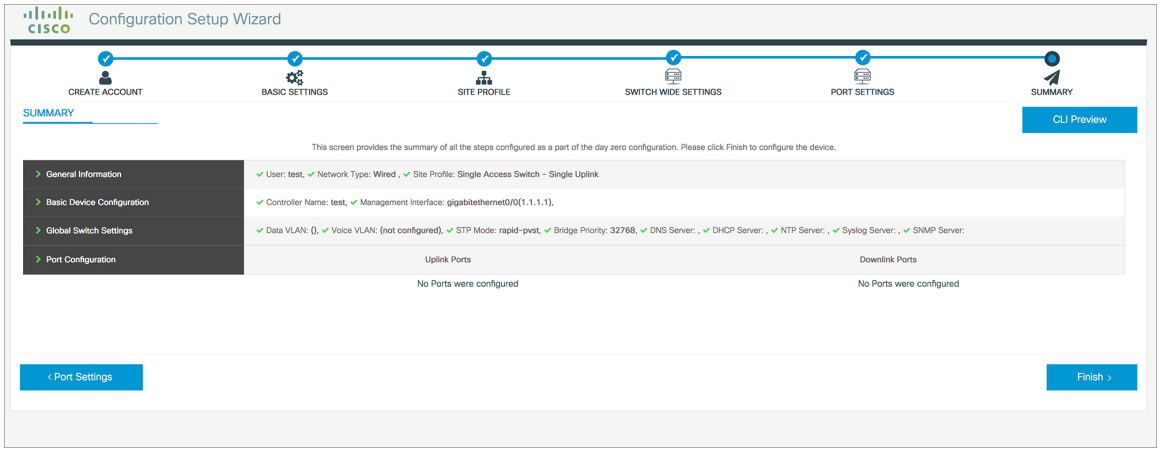
Figure 13: Port Settings



What to do next

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

Figure 14: 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. You must change the default value for VTY Line, 0-15 (or 0-4 in some models), to 0-30 to allow up to thirty simultaneous sessions.

Procedure

Step 1 From the WebUI, navigate through **Administration > Management > HTTP/HTTPS/Netconf/VTY**

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

Step 3 Use the **VTY Transport Mode** drop-down list to select the VTY transport mode.

Figure 15: Configuring VTY Line

