# Introduction to Day 0 WebUI Configuration

This chapter contains the following sections:

# 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*.

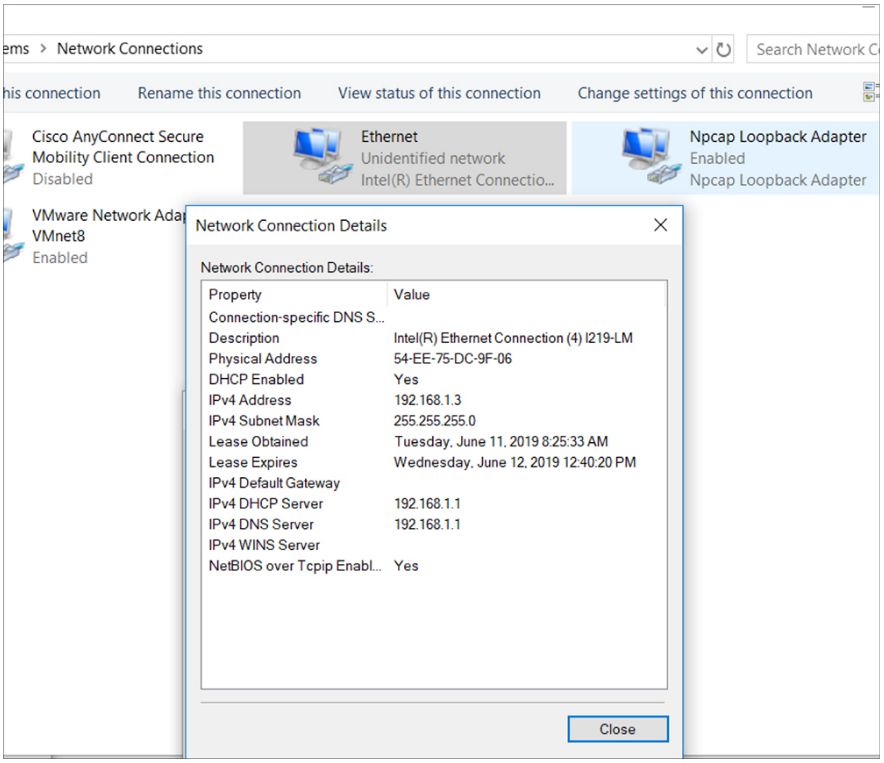
Verify that no devices are connected to the switch.

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*



ems > Network Connections
Search Network C
his connection
Rename this connection
View status of this connection
Change settings of this connection
Cisco AnyConnect Secure Mobility Client Connection
Disabled
Ethernet
Unidentified network
Intel(R) Ethernet Connectio...
Npcap Loopback Adapter
Enabled
Npcap Loopback Adapter
VMware Network Adap
VMnet8
Enabled
Network Connection Details
Close

Network Connection Details:

| Property | Value |
|---|---|
| Connection-specific DNS S... | |
| Description | Intel(R) Ethernet Connection (4) I219-LM |
| Physical Address | 54-EE-75-DC-9F-06 |
| DHCP Enabled | Yes |
| IPv4 Address | 192.168.1.3 |
| IPv4 Subnet Mask | 255.255.255.0 |
| Lease Obtained | Tuesday, June 11, 2019 8:25:33 AM |
| Lease Expires | Wednesday, June 12, 2019 12:40:20 PM |
| IPv4 Default Gateway | |
| IPv4 DHCP Server | 192.168.1.1 |
| IPv4 DNS Server | 192.168.1.1 |
| IPv4 WINS Server | |
| NetBIOS over Tcpip Enabl... | Yes |

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**.

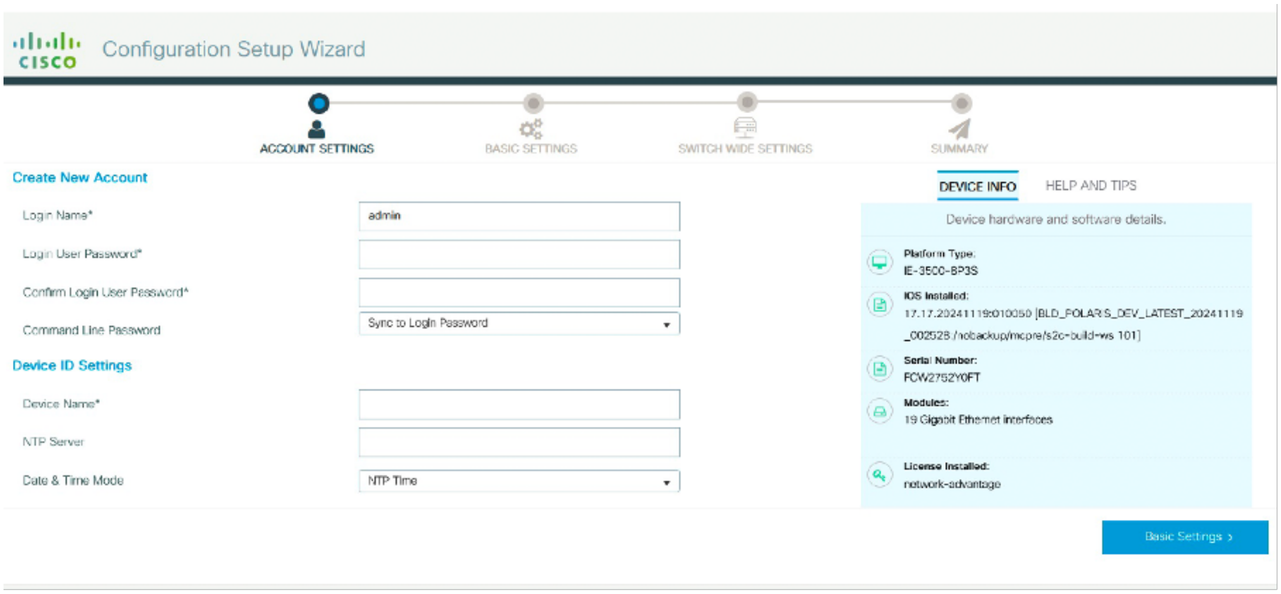
**Step 5** Use the **Command Line Password** drop-down list to choose where to synchronize the password.

**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*



Create New Account

Login Name*: admin

Login User Password*:

Confirm Login User Password*:

Command Line Password: Sync to Login Password

Device ID Settings

Device Name*:

NTP Server:

Date & Time Mode: NTP Time

Device hardware and software details.

Platform Type:
IE-3500-8P3S

IOS Installed:
17.17.20241119:010050 [BLD_POLARIS_DEV_LATEST_20241119_002528 /nobackup/mcpre/s2c-build-ws 101]

Serial Number:
FCW2752Y0FT

Modules:
19 Gigabit Ethernet interfaces

License Installed:
network-advantage

# 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.

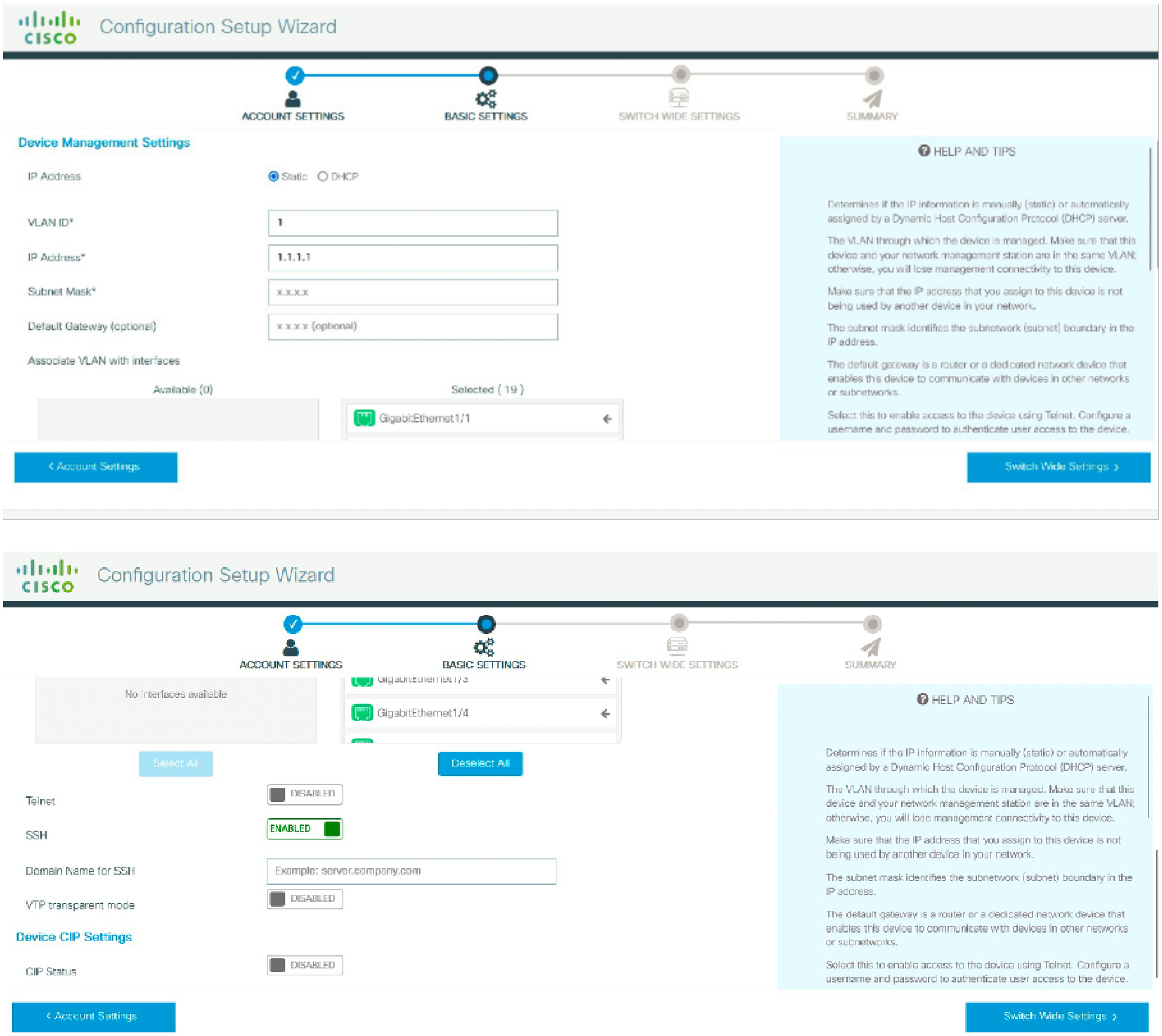
### Procedure

**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*



Configuration Setup Wizard

Device Management Settings

IP Address ● Static ○ DHCP

VLAN ID* 1

IP Address* 1.1.1.1

Subnet Mask* x.x.x.x

Default Gateway (optional) x.x.x.x (optional)

Associate VLAN with interfaces

Available (0)

Selected ( 19 )

GigabitEthernet1/1

HELP AND TIPS

Determines if the IP information is manually (static) or automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server.

The VLAN through which the device is managed. Make sure that this device and your network management station are in the same VLAN; otherwise, you will lose management connectivity to this device.

Make sure that the IP address that you assign to this device is not being used by another device in your network.

The subnet mask identifies the subnetwork (subnet) boundary in the IP address.

The default gateway is a router or a dedicated network device that enables this device to communicate with devices in other networks or subnetworks.

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

Configuration Setup Wizard

No interfaces available

GigabitEthernet1/3

GigabitEthernet1/4

Telnet DISABLED

SSH ENABLED

Domain Name for SSH Example: server.company.com

VTP transparent mode DISABLED

Device CIP Settings

CIP Status DISABLED

HELP AND TIPS

Determines if the IP information is manually (static) or automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server.

The VLAN through which the device is managed. Make sure that this device and your network management station are in the same VLAN; otherwise, you will lose management connectivity to this device.

Make sure that the IP address that you assign to this device is not being used by another device in your network.

The subnet mask identifies the subnetwork (subnet) boundary in the IP address.

The default gateway is a router or a dedicated network device that enables this device to communicate with devices in other networks or subnetworks.

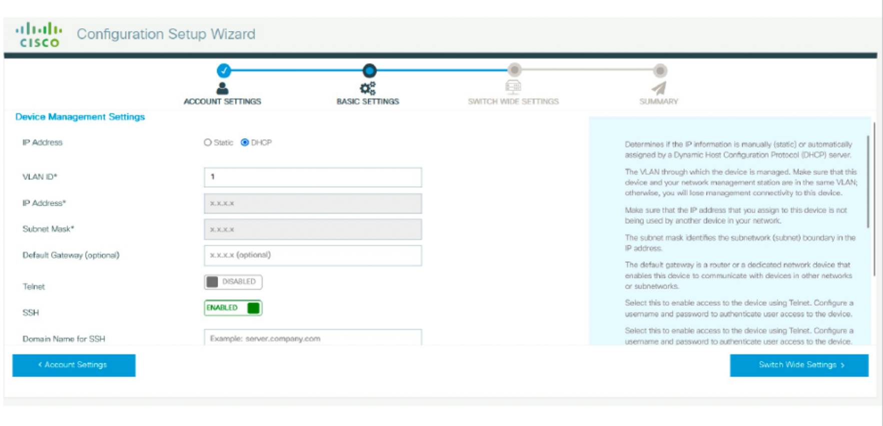
Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

**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*



Device Management Settings

IP Address ○ Static ● DHCP

VLAN ID* 1

IP Address* x.x.x.x

Subnet Mask* x.x.x.x

Default Gateway (optional) x.x.x.x (optional)

Telnet DISABLED

SSH ENABLED

Domain Name for SSH Example: server.company.com

Determines if the IP information is manually (static) or automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server.

The VLAN through which the device is managed. Make sure that this device and your network management station are in the same VLAN; otherwise, you will lose management connectivity to this device.

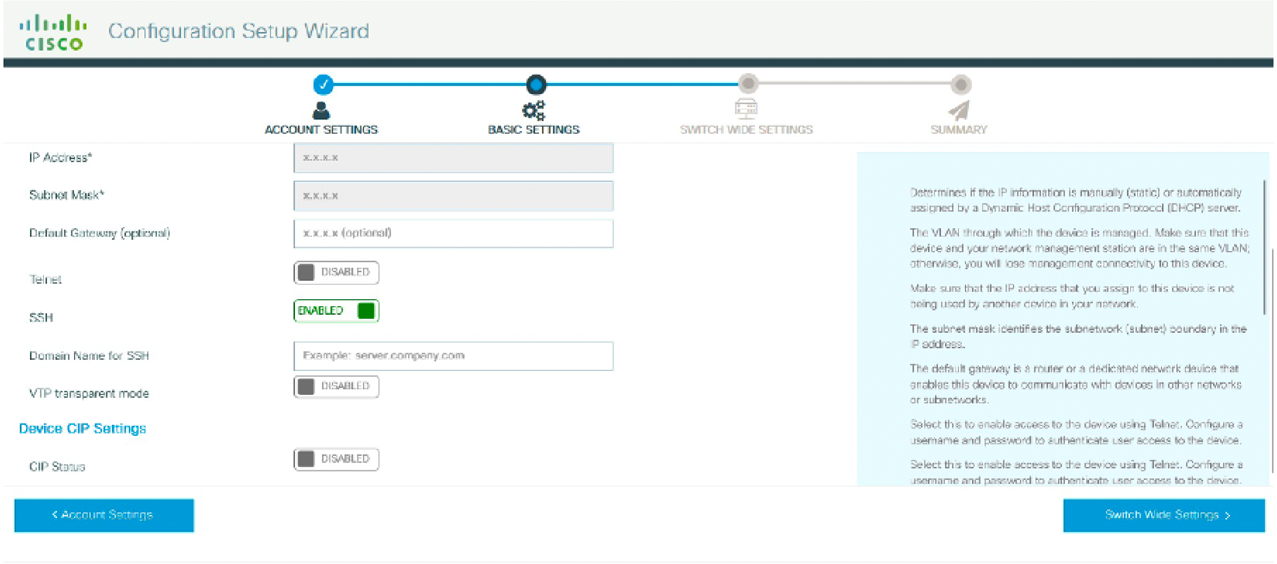
Make sure that the IP address that you assign to this device is not being used by another device in your network.

The subnet mask identifies the subnetwork (subnet) boundary in the IP address.

The default gateway is a router or a dedicated network device that enables this device to communicate with devices in other networks or subnetworks.

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.



IP Address* x.x.x.x

Subnet Mask* x.x.x.x

Default Gateway (optional) x.x.x.x (optional)

Telnet DISABLED

SSH ENABLED

Domain Name for SSH Example: server.company.com

VTP transparent mode DISABLED

Device CIP Settings

CIP Status DISABLED

Determines if the IP information is manually (static) or automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server.

The VLAN through which the device is managed. Make sure that this device and your network management station are in the same VLAN; otherwise, you will lose management connectivity to this device.

Make sure that the IP address that you assign to this device is not being used by another device in your network.

The subnet mask identifies the subnetwork (subnet) boundary in the IP address.

The default gateway is a router or a dedicated network device that enables this device to communicate with devices in other networks or subnetworks.

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

**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.

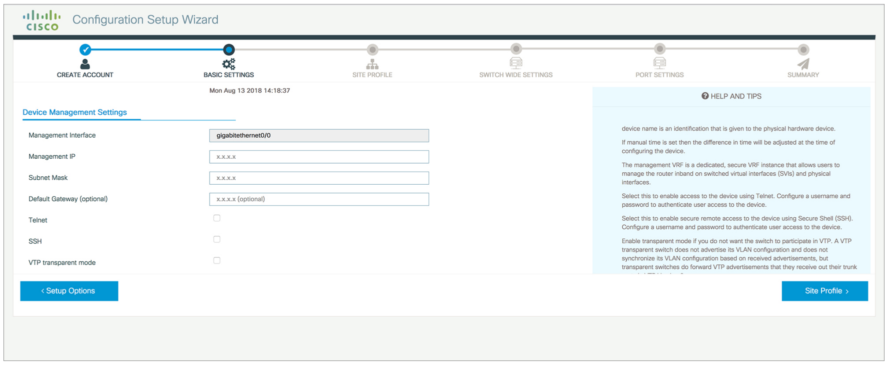
**Step 6** To enable access to the device using telnet, check the **Telnet** check box.

**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***



Mon Aug 13 2018 14:18:37

Device Management Settings

| | |
|---|---|
| Management Interface | gigabitethernet0/0 |
| Management IP | x.x.x.x |
| Subnet Mask | x.x.x.x |
| Default Gateway (optional) | x.x.x.x (optional) |
| Telnet | □ |
| SSH | □ |
| VTP transparent mode | □ |

HELP AND TIPS

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

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

The management VRF is a dedicated, secure VRF instance that allows users to manage the router inband on switched virtual interfaces (SVIs) and physical interfaces.

Select this to enable access to the device using Telnet. Configure a username and password to authenticate user access to the device.

Select this to enable secure remote access to the device using Secure Shell (SSH). Configure a username and password to authenticate user access to the device.

Enable transparent mode if you do not want the switch to participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements, but transparent switches do forward VTP advertisements that they receive out their trunk

# 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.

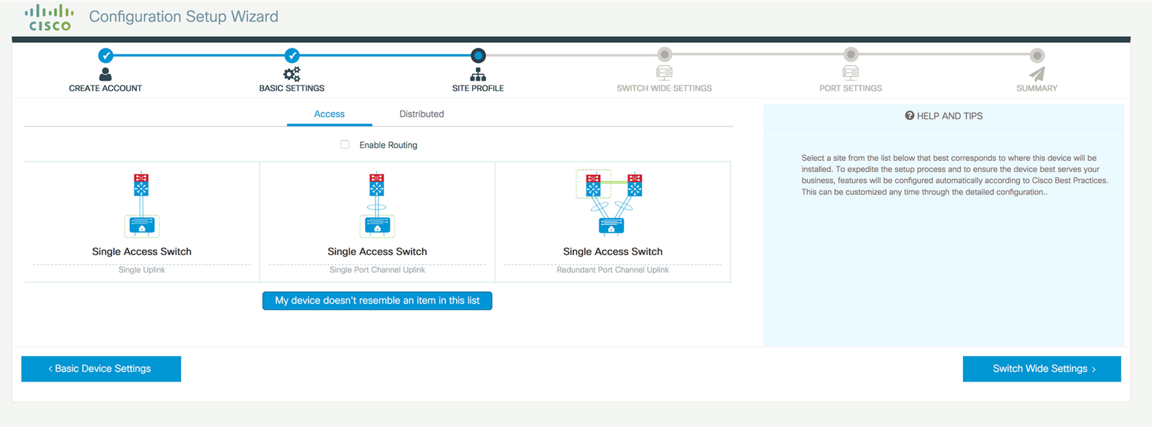
Choosing a site profile as part of Quick Setup allows you to configure your device based on the business needs of your enterprise. For example, you could use your device as an access switch, to connect client nodes and endpoints on your network, or as a distribution switch, to route packets between subnets 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:<br>• Default VLAN<br>• Data VLAN<br>• Voice VLAN<br>• Management VLAN | The following VLANs are created:<br>• Default VLAN<br>• Data VLAN<br>• Voice VLAN<br>• Management VLAN | The following VLANs are created:<br>• Default VLAN<br>• Data VLAN<br>• Voice VLAN<br>• 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 |

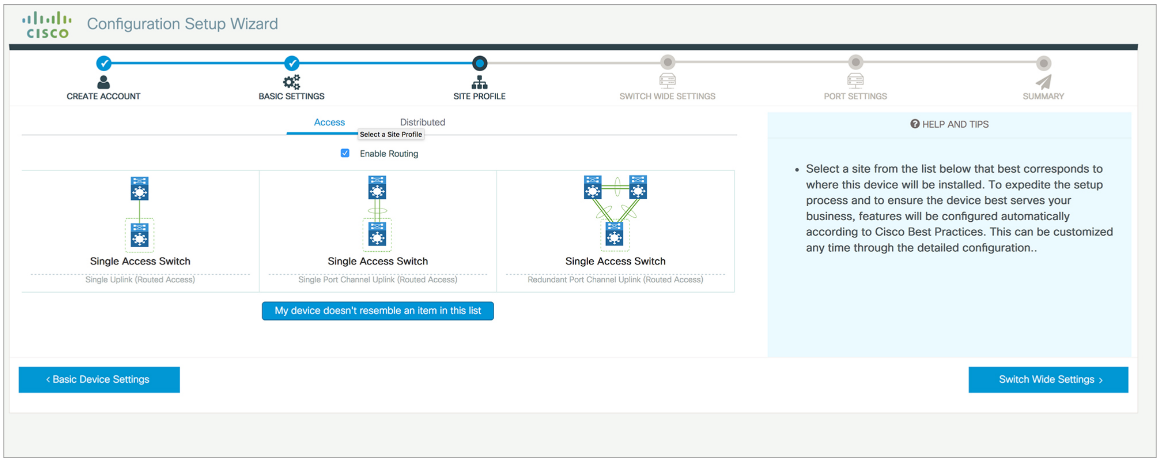
*Figure 6: Site Profile - Access Switches*



☐ Enable Routing

Select a site from the list below that best corresponds to where this device will be installed. To expedite the setup process and to ensure the device best serves your business, features will be configured automatically according to Cisco Best Practices. This can be customized any time through the detailed configuration..

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



☑ Enable Routing

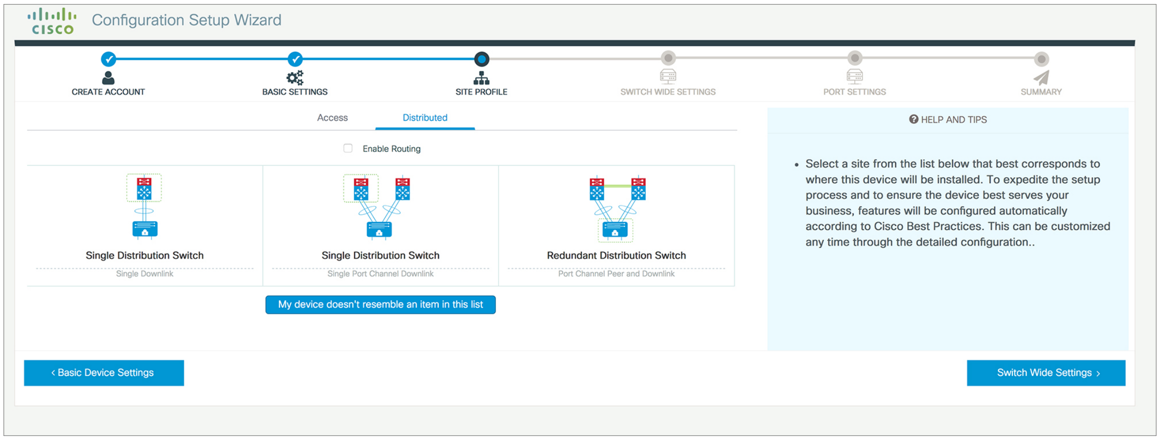
- Select a site from the list below that best corresponds to where this device will be installed. To expedite the setup process and to ensure the device best serves your business, features will be configured automatically according to Cisco Best Practices. This can be customized any time through the detailed configuration..

*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 |

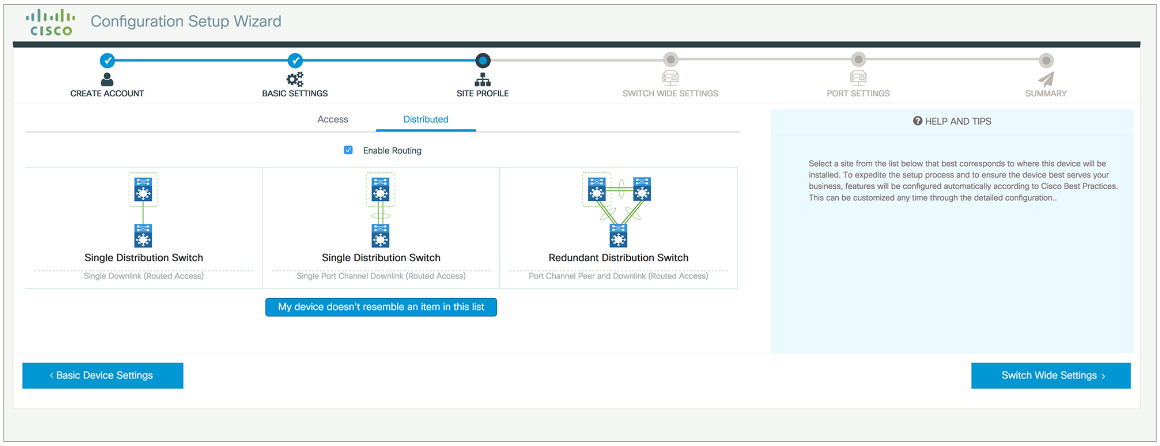
| Setting | Single Distribution Switch (Single Downlink) | Single Distribution Switch (Single Port Channel Downlink) | Redundant Distribution Switch (Port Channel Peer and Downlink) |
|---|---|---|---|
| SCP | Enabled | Enabled | Enabled |
| VTY Access to Switch | Enabled | Enabled | Enabled |
| Service Timestamp | Enabled | Enabled | Enabled |
| VLAN | The following VLANs are created:<br>• Default VLAN<br>• Data VLAN<br>• Voice VLAN<br>• Management VLAN | The following VLANs are created:<br>• Default VLAN<br>• Data VLAN<br>• Voice VLAN<br>• Management VLAN | The following VLANs are created:<br>• Default VLAN<br>• Data VLAN<br>• Voice VLAN<br>• 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*


Configuration Setup Wizard
CREATE ACCOUNT
BASIC SETTINGS
SITE PROFILE
SWITCH WIDE SETTINGS
PORT SETTINGS
SUMMARY
Access
Distributed
□ Enable Routing
Single Distribution Switch
Single Downlink
Single Distribution Switch
Single Port Channel Downlink
Redundant Distribution Switch
Port Channel Peer and Downlink
My device doesn't resemble an item in this list
‹ Basic Device Settings
Switch Wide Settings ›
HELP AND TIPS

- Select a site from the list below that best corresponds to where this device will be installed. To expedite the setup process and to ensure the device best serves your business, features will be configured automatically according to Cisco Best Practices. This can be customized any time through the detailed configuration..

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


Configuration Setup Wizard
CREATE ACCOUNT
BASIC SETTINGS
SITE PROFILE
SWITCH WIDE SETTINGS
PORT SETTINGS
SUMMARY
Access
Distributed
☑ Enable Routing
Single Distribution Switch
Single Downlink (Routed Access)
Single Distribution Switch
Single Port Channel Downlink (Routed Access)
Redundant Distribution Switch
Port Channel Peer and Downlink (Routed Access)
My device doesn't resemble an item in this list
‹ Basic Device Settings
Switch Wide Settings ›
HELP AND TIPS

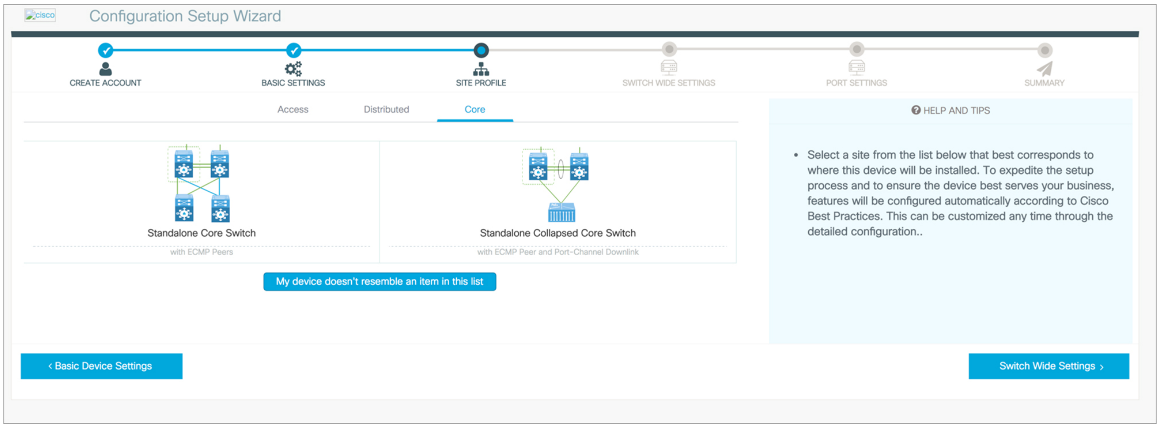
Select a site from the list below that best corresponds to where this device will be installed. To expedite the setup process and to ensure the device best serves your business, features will be configured automatically according to Cisco Best Practices. This can be customized any time through the detailed configuration..

*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*



- Select a site from the list below that best corresponds to where this device will be installed. To expedite the setup process and to ensure the device best serves your business, features will be configured automatically according to Cisco Best Practices. This can be customized any time through the detailed configuration..

# 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.

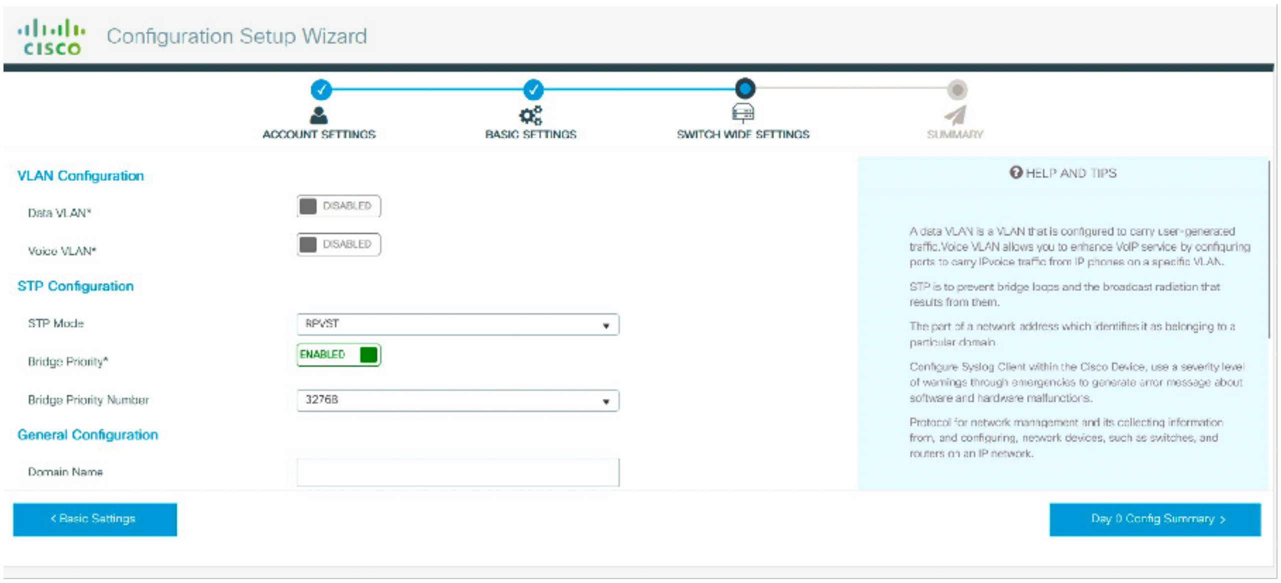
# Configure STP Settings

### 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*



VLAN Configuration

Data VLAN* DISABLED

Voice VLAN* DISABLED

STP Configuration

STP Mode RPVST

Bridge Priority* ENABLED

Bridge Priority Number 32768

General Configuration

Domain Name

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.

# 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.

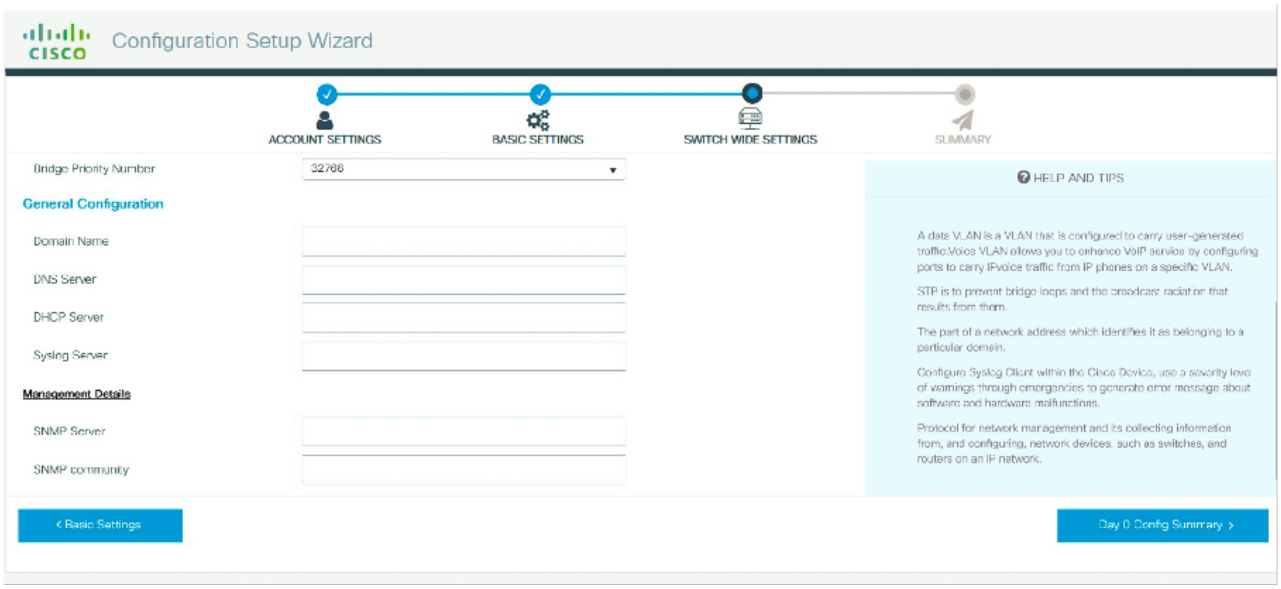
**Step 4** In the **Syslog Server**, type the IP address of the server to which you want to send syslog messages.

**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***



Bridge Priority Number: 32768

General Configuration

Domain Name:

DNS Server:

DHCP Server:

Syslog Server:

Management Details

SNMP Server:

SNMP community:

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

### Procedure

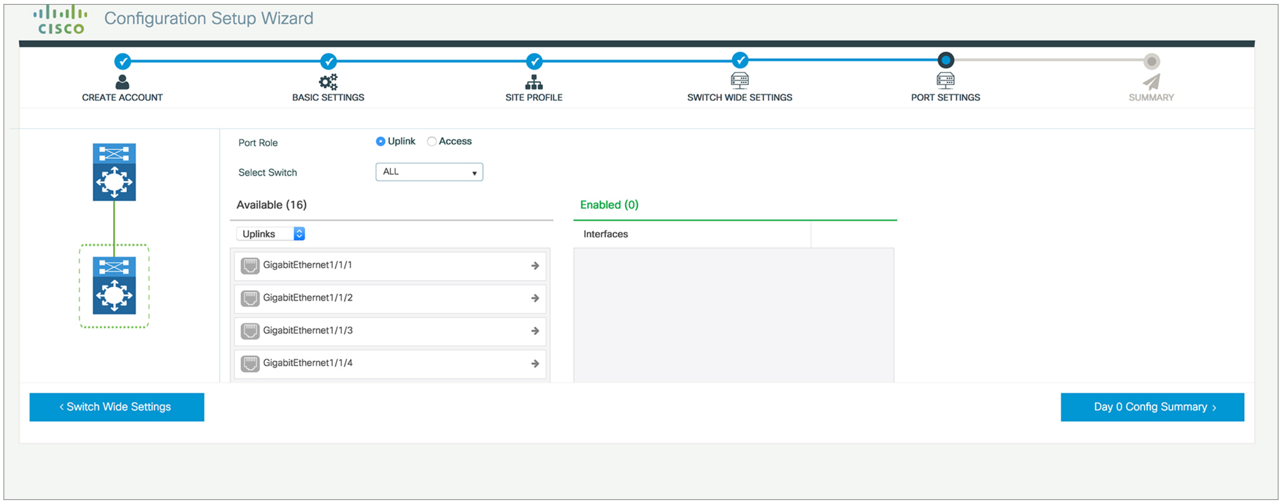
**Step 1** Based on the site profile chosen in the earlier step which is displayed in the left-pane, select the **Port Role** from among the following options:

- 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*



Port Role ● Uplink ○ Access

Select Switch ALL

Available (16)

Uplinks

- GigabitEthernet1/1/1
- GigabitEthernet1/1/2
- GigabitEthernet1/1/3
- GigabitEthernet1/1/4

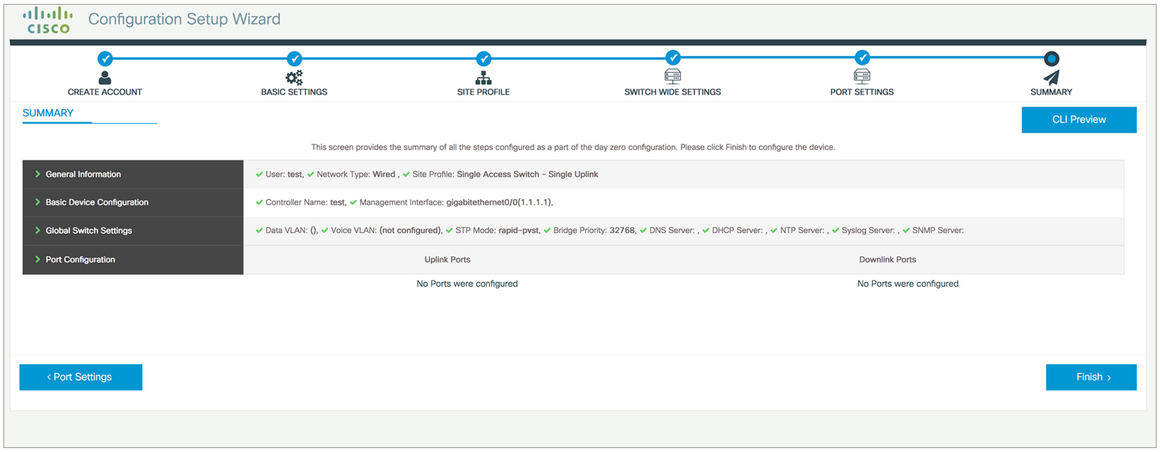
Enabled (0)

Interfaces

## What to do next

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

*Figure 14: Day 0 Config 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: (), ✓ Voice VLAN: (not configured), ✓ STP Mode: rapid-pvst, ✓ Bridge Priority: 32768, ✓ DNS Server: , ✓ DHCP Server: , ✓ NTP Server: , ✓ Syslog Server: , ✓ SNMP Server: | |
| › Port Configuration | Uplink Ports | Downlink Ports |
| | No Ports were configured | No Ports were configured |

# 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.

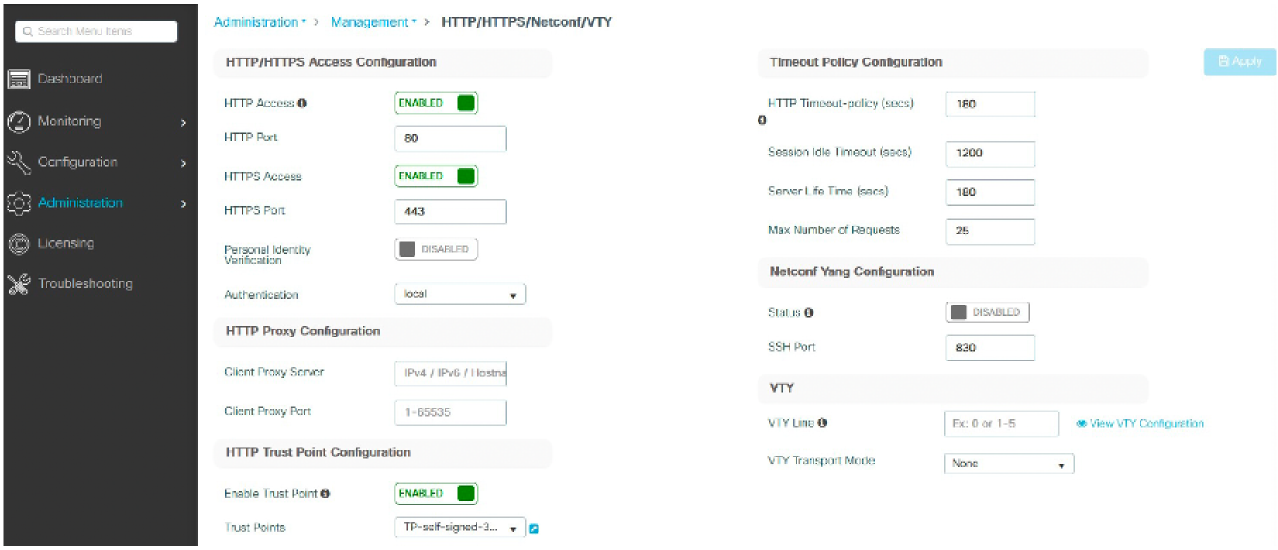
### Procedure

**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*



**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 / Hostna
Client Proxy Port: 1-65535

**HTTP Trust Point Configuration**

Enable Trust Point: ENABLED
Trust Points: TP-self-signed-3...

**Timeout Policy Configuration**

HTTP Timeout-policy (secs): 180
Session Idle Timeout (secs): 1200
Server Life Time (secs): 180
Max Number of Requests: 25

**Netconf Yang Configuration**

Status: DISABLED
SSH Port: 830

**VTY**

VTY Line: Ex: 0 or 1-5 View VTY Configuration
VTY Transport Mode: None