

Configuring the Switch Using the Web User Interface



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

| | DNAC Cloud Onboarding Day 0 Wizard | Clas | ssic Day 0 Wizard | | | |
|--|--|--------------------------|--|--|--|--|
| | This wizard would enable you to on-board this device to dnacentarcloud.cisco.com. The wizard would give you step by step guidance to configure the management interface and check the cloud reachability. Make sure you have created a Cisco DNA Center Cloud account and added the device before you start the wizard. | and a IP ad succe | wizard would enable you to configure the Switch with basic dvanced settings like User account. Management Interface dirdes.VLANS?P mode selection etc. Once the wizard is sesfully completed, user can access the Switch via WEBU command line using the Management Interface IP address ded. | | | |
| | IS BELOW BEFORE YOU BEGIN | | | | | |
| Ensure that you | have all the required information from your service provide | r to complete the config | guration. | | | |
| • By default, the wizard enables some recommended configurations. We recommend that you keep these defaults unless you have a reason to change | | | | | | |
| By default, the | them. | | | | | |
| | | | | | | |
| | ps you to bring up your WAN/LAN connectivity quickly. You | can change the configu | ration and configure advanced features after the | | | |

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.



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

| • | | | |
|--|----------------|-------------------|--|
| ACCOUNT SETTINGS Create New Account | BASIC SETTINGS | TEST CONNECTIVITY | DEVICE INFO HELP AND TIPS |
| Login Name* | testuser | | |
| Login User Password* | | | Establish a new Username and Password for the Device. Please remember it for next Login. |
| Confirm Login User Password* | | | Establish a new password for the privileged command level, |
| | | | Device name is an identification that is given to the physical hardware device. |
| evice ID Settings | | | Network Time Protocol (NTP) is a networking protocol for |
| Device Name* | testdevice | | clock synchronization between computer systems over packet-switched, variable-latency data networks. Enter the IP address of the NTP server. |
| NTP Server | XXXX | | If manual time is set then the difference in time will be |
| Date & Time Mode | NTP Time | • | adjusted at the time of configuring the device. |
| | | | |
| | | | |
| < Welcome Page | | | Basic Settings ➤ |

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:
 - 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

| VLAN ID* | atic © DHCP | | HELP AND TIPS Select this to enable access to the device using Teinet. Configure a username and password to authenticate user access to the device. |
|----------------------------|---------------------------------------|-------------|---|
| VLAN ID* | atic OHCP | 7 | |
| Default Gateway (optional) | ccx (optional) abliEthernet1/0/2 v |]]] | Select this to enable access to the device using Teinet. 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 participat 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 ports in VTP Version 2. |

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

| | BASIC SETTINGS | TEST CONNECTIVITY | SUMMARY |
|---|--|-------------------|---|
| Device Management Settings | | | HELP AND TIPS |
| IP Address VLAN ID* IP Address* Subnet Mask* Default Gateway (optional) DNS Server | © Static @ DHCP 2 XXXX XXXX XXXX XXXX XXXX XXXX | | Select this to enable access to the device using Teinet. Configure a username and password to authenticate user access to the device. Select this to enable access to the device using Teinet. 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 switchkes do forward VTP advertisements that they receive out their trunk ports in VTP Version 2. |
| < Create New Account | | | Test Connectivity > |

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 2If 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

| | C BASIC SETTINGS | | TEST CONNECTIVITY | SUMMARY |
|-------------------------|---------------------|--------------------------------------|---------------------------|--------------------------------|
| IP Type DHCP | VLAN ID 2 | DHCP Server any (255.255.255,255) | Received IP unassigned | Default Gateway Not Configured |
| DHCP IP Test | Checking I | Since Durice) Output | | C hatest |
| 2 Cloud Connection Test | | Source (Device) Destinuit | n | |
| 3 Completed | | | | Bay Zero Configuration Summe |

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).

Add a new REG_BINARY DhcpClientIdentifier with Data 77 65 62 75 69 for webui. You need to manually type in the value.

Registry Editor File Edit View Favori Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\/46836ffc-6358-4da1-b9f8-a2a10f1a0c48} stexstor stisvc storahci storflt Name Data REG_SZ (value not set) (Default) R AddressType REG DWORD 0x00000000 (0 77 65 62 75 69 28 DhcpClientIdentifie REG_BINARY stornvme storqosfit StorSvc storufs storvsc Edit Binary Value \times le 01 00 79 00 00 00 00 00 00 DhcpClientIdentifier SVSVC Value data: swenum 77 65 62 75 webu swenum swprv SynaMetSMI Synth3dVsc SynTP SynTPEnhService SysMain SystemEventsBroker SzCCID TabletInputService TapiSrv OK Cancel Tcpip Linkage Parameter Parameters Adapters DNSRegisteredAdapters Interfaces {2a1d7785-5141-4b33-8f11-4b5cf324636c (2e6a118d-8ff9-45c8-b861-13bbbf590a22) (3f99fba7-ae95-43f6-b34c-e2fbdde8cb40) (46836ffc-6358-4da1-b9f8-a2a10f1a0c48) {4828db99-4092-4a20-903b-e304a283e9f0} {7baa2017-910a-4c77-b968-a9beb40c9646} {922467f8-ace4-4789-93b6-9a3799a7b574} {b20b01ef-9511-4f8d-af8d-c03a948db0e1} {b5fdd031-2580-445b-8430-074e5248bd14

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.

| | | Network | | | Q Search |
|-----------------|------------------------|----------|--------|------------|------------------|
| Wi-Fi | | | | | |
| Wi-Fi | TCP/IP DNS V | WINS 8 | 802.1X | Proxies | Hardware |
| | | | | | |
| Configure IPv4: | Using DHCP | | | O | |
| IPv4 Address: | *8.2002.2022 | | | | Renew DHCP Lease |
| Subnet Mask: | 2222000225220 | | DHCP | Client ID: | webui |
| Router: | XXX2002X200XXX | | | | (If required) |
| Configure IPv6: | Automatically | | | 0 | |
| Router: | TERSOLVEX X & MXDEXIXX | GKBAK | | | |
| IPv6 Address: | 2008.8.24200.524497.8 | 25822000 | квхахх | **** | |
| Prefix Length: | 1028X | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | Cancel |
| | | | | | Cancel |

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

| ems > Network Connectio | ons | | | ~ Ū | Search Network (|
|---|---|---|-----------------|-----------|---|
| his connection Rename | e this connection View s | tatus of this connection | Change settings | of this o | connection |
| Cisco AnyConnect Secu Mobility Client Connec Disabled | tion 🧏 Un | ernet identified network eI(R) Ethernet Connectio | | Enabled | Loopback Adapter I Loopback Adapter |
| VMware Network Ada VMnet8 Enabled | Network Connection Detail | s | × | | |
| | Property Connection-specific DNS S. Description Physical Address DHCP Enabled IPv4 Address IPv4 Subnet Mask Lease Obtained Lease Expires IPv4 Default Gateway IPv4 DHCP Server IPv4 DHCP Server IPv4 UNS Server NetBIOS over Tcpip Enabl | Intel(R) Ethernet Connection 54-EE-75-DC-9F-06 Yes 192.168.1.3 255.255.255.0 Tuesday, June 11, 2019 8.25 Wednesday, June 12, 2019 192.168.1.1 192.168.1.1 | 533 AM | | |

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

| Configuration Se | BASIC SETTINGS | SITE PROFILE | SWITCH WIDE SETTINGS | PORT SETTINGS | SUMMARY |
|------------------|----------------|--------------------|----------------------|-----------------------------------|-------------------------|
| Login Name | | | | Hardware and Software | details of the device. |
| Password | | | | Platform Type: IOS Installed: | |
| Confirm password | | | | Serial Number: | |
| | | | | Modules: | |
| | | | | Cee License Installed: | |
| | | Create New Account | | | Basic Device Settings > |
| | | | | | |
| | | | | | |

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

| CREATE ACCOUNT | BASIC SETTINGS | SITE PROFILE | SWITCH WIDE SETTINGS | PORT SETTINGS | SUMMARY |
|--------------------------------|--------------------------|---------------------------------------|--------------------------|--|--|
| evice ID and Location Settings | | | | HELP A | ND TIPS |
| Device Name | | · · · · · · · · · · · · · · · · · · · | Device name is mandatory | | |
| Date & Time Mode | Automatic | • | | device name is an identification that is g | iven to the physical hardware device. |
| | | | | If manual time is set then the difference configuring the device. | in time will be adjusted at the time of |
| evice Management Settings | Mon Aug 13 2018 14:18:06 | | | The management VRF is a dedicated, se manage the router inband on switched v interfaces. | |
| Management Interface | gigabitethemet0/0 | | | Select this to enable access to the devic password to authenticate user access to | e using Telnet. Configure a username and the device. |
| Management IP | x.x.x.x | | | Select this to enable secure remote acc Configure a username and password to | ess to the device using Secure Shell (SSH). authenticate user access to the device. |
| Subnet Mask | X.X.X.X | | | Enable transparent mode if you do not w transparent switch does not advertise its | ant the switch to participate in VTP. A VTP |
| Default Gateway (optional) | x.x.x.x (optional) | | | synchronize its VLAN configuration base | |
| < Setup Options | | | | | Site Profile > |

- 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 |
|------------------|-------------------|---------------------|
| | | |

| CREATE ACCOUNT | BASIC SETTINGS | SITE PROFILE | SWITCH WIDE SETTINGS | PORT SETTINGS | SUMMARY | | |
|----------------------------|--------------------------|--------------------|----------------------|--|--|--|--|
| | Mon Aug 13 2018 14:18:37 | | | HELP / | AND TIPS | | |
| Device Management Settings | | | | | | | |
| Management Interface | gigabitethernet0/0 | | | device name is an identification that is g If manual time is set then the difference | | | |
| Management IP | x.x.x.x | | | configuring the device. | | | |
| Subnet Mask | X.X.X.X | | | The management VRF is a dedicated, se manage the router inband on switched v interfaces. | | | |
| Default Gateway (optional) | x.x.x.x (optional) | x.x.x.x (optional) | | | | Select this to enable access to the devi password to authenticate user access t | te using Telnet. Configure a username and the device. |
| Telnet | | | | Select this to enable secure remote acc Configure a username and password to | ess to the device using Secure Shell (SSH). authenticate user access to the device. | | |
| SSH | | | | Enable transparent mode if you do not v transparent switch does not advertise its | vant the switch to participate in VTP. A VTP | | |
| VTP transparent mode | | | | synchronize its VLAN configuration base | | | |
| < Setup Options | | | | | Site Profile > | | |
| | | | | | | | |
| | | | | | | | |

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.

| 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: | The following VLANs are created: | The following VLANs are created: |
| | Default VLAN | • Default VLAN | • Default VLAN |
| | • Data VLAN | • Data VLAN | • Data VLAN |
| | • Voice VLAN | • Voice VLAN | • Voice VLAN |
| | Management VLAN | Management VLAN | Management VLAN |

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) |
|----------------------|---|---|--|
| Management Interface | Layer 3 settings | Layer 3 settings | Layer 3 settings |
| | configured on the | configured on the | configured on the |
| | management port, based | management port, based | management port, based |
| | on Quick Setup | on Quick Setup | 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 | Selected uplink ports | Selected uplink ports |
| | connect to other | connect to other | connect to other |
| | distribution or core | distribution or core | distribution or core |
| | switches | switches | switches |
| Downlink Interfaces | Downlink connections to | Downlink connections to | Downlink connections to |
| | access switches | access switches | access switches |
| | configured in Trunk mode | configured in Trunk mode | 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



| CREATE ACCOUNT | | PROFILE SWITCH WIDE SETTINGS | PORT SETTINGS | SUMMARY |
|----------------------------|---|---|--|--|
| | Access Distributed | | HELP / | ND TIPS |
| Single Distribution Switch | Enable Routing Single Distribution Switch Single PortFaure Downlink (Routed Access) My device doesn't resemble an Item in this II | Redundant Distribution Switch Port Channel Peer and Downlink (Routed Access) | Select a site from the flat below that been installed. To expected the setup processor bosines, external weak to exclusion with an exclusion that can be externized any time throug | and to ensure the device best serves omatically according to Cisco Best Pra |
| < Basic Device Settings | | | | Switch Wide Settings |

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 |

| Setting | Standalone Core Switch (with ECMP Peers) | Standalone Collapsed Core Switch (with ECMP Peer and Port Channel Downlink) |
|--------------------------|---|---|
| Cross-connect Interfaces | Selected ports connect to other core switches | Selected ports connect to other core switches |

Figure 14: Site Profile - Core Switches

| CREATE ACCOUNT | BASIC SETTINGS | SITE PROFILE | SWITCH WIDE SETTINGS | PORT SETTINGS | SUMMARY |
|----------------|------------------------|--|----------------------|---|--|
| | Access Distributed | Core | | HELP / | AND TIPS |
| | Core Switch WP Pers | Standalone Collar with ECMP Peer and 9 m item in this list | | Select a site from the list behavior will be ins where this device will be ins process and to ensure the d features will be configured a Best Practices. This can be detailed configuration | talled. To expedite the setu evice best serves your busi utomatically according to C |

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 15: VLAN and STP Settings

| 0 | ⊘ | ⊘ | 0 | | | |
|------------------------------------|----------------|--------------|----------------------|---|---|--|
| CREATE ACCOUNT | BASIC SETTINGS | SITE PROFILE | SWITCH WIDE SETTINGS | PORT SETTINGS | SUMMARY | |
| VLAN Configuration | | | | HELP A | ND TIPS | |
| Data VLAN | | | | | a configured to computer | |
| Voice VLAN | | | | A data VLAN is a VLAN that is configured to carry user- generated traffic.Voice VLAN allows you to enhance VoIF | | |
| Management VL Switch Wide Settings | | | | service by configuring ports phones on a specific VLAN. | to carry IPvoice traffic from IP | |
| STP Configuration | | | | STP is to prevent bridge loops and the b | oadcast radiation that results from them. | |
| | | | | The part of a network address which ide | tifies it as belonging to a particular domain. | |
| STP Mode Bridge Priority | RPVST | • | | Configure Syslog Client within the Cisco through emergencies to generate error n malfunctions. | | |
| Bridge Priority Number | 32768 | • | | | collecting information from, and configuring, outers on an IP network. | |
| General Configuration | | | | | | |
| < Site Profile | | | | | Port Settings > | |
| | | | | | | |

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 16: DHCP, NTP, DNS and SNMP Settings

| CREATE ACCOUNT | BASIC SETTINGS | SITE PROFILE | SWITCH WIDE SETTINGS | PORT SETTINGS | SUMMARY |
|---|----------------|--------------|----------------------|--|---|
| General Configuration | | | | HELP A | ND TIPS |
| Domain Details Domain Name DNS Server Server Details | | | | allows you to enhance VoIP service by c IP phones on a specific VLAN. STP is to prevent bridge loops and the b | d to carry user~generated traffic.Voice VLAN onfiguring ports to carry IPvoice traffic from readcast radiation that results from them. ntifies it as belonging to a particular domain. |
| DHCP Server | | | | Configure Syslog Client within the Cisco through emergencies to generate error n malfunctions. | |
| Syslog Server NTP Server | | | | Protocol for network manage information from, and confige as switches, and routers on | uring, network devices, such |
| Management Details | | | | | |
| < Site Profile | | | | | Port Settings > |

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 17: Port Settings

| CREATE ACCOUNT | BASIC SETTINGS | SITE PROFILE | SWITCH WIDE SETTINGS | SUMMARY |
|----------------------|----------------------|--------------|----------------------|----------------------|
| | Port Role OUplink | Access | | |
| | Select Switch ALL | ¥ | | |
| | Available (16) | Enabled (| 0) | |
| | Uplinks 😒 | Interfaces | | |
| | GigabitEthernet1/1/1 | ÷ | | |
| € ∰- | GigabitEthernet1/1/2 | ÷ | | |
| () | GigabitEthernet1/1/3 | > | | |
| | GigabitEthernet1/1/4 | <i>></i> | | |
| Switch Wide Settings | | | | Day 0 Config Summary |
| | - | | | |

What to do next

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

Figure 18: Day 0 Config Summary

| 0 | O | <u> </u> | <u> </u> | <u> </u> | • | | |
|----------------------------|------------------------------------|--|---|--------------------------|-------------|--|--|
| CREATE ACCOUNT | BASIC SETTINGS | SITE PROFILE | SWITCH WIDE SETTINGS | PORT SETTINGS | SUMMARY | | |
| MMARY | | | | | CLI Preview | | |
| | This screen provides | the summary of all the steps configured as a pa | rt of the day zero configuration. Please click Finish to conf | igure the device. | | | |
| General Information | 🗸 User: test, 🖌 Network Type: Wire | ✓ User: test, ✓ Network Type: Wired, ✓ Site Profile: Single Access Switch - Single Uplink | | | | | |
| Basic Device Configuration | ✓ Controller Name: test, ✓ Manager | ✓ Controller Name: test, ✓ Management Interface: gigabitethernet0/0(1.1.1.1), | | | | | |
| Global Switch Settings | ✓ Data VLAN: (), ✓ Voice VLAN: (no | ✓ Data VLAN: (), ✓ Voice VLAN: (not configured), ✓ STP Mode: rapid-pvst, ✓ Bridge Priority: 32768, ✓ DNS Server: , ✓ DHCP Server: , ✓ NTP Server: , ✓ Syslog Server: , ✓ Syslog Server: , ✓ SNMP Server: | | | | | |
| > Port Configuration | | Uplink Ports | | Downlink Ports | | | |
| | | No Ports were configured | | No Ports were configured | | | |
| | | | | | | | |
| | | | | | | | |
| < Port Settings | | | | | Finish | | |

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.

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

| Q Search Menu Items | Administration * > Device | | |
|---------------------|---------------------------|----------------------------|------------------------|
| Dashboard | General | IP Routing | DISABLED |
| Monitoring > | FTP/SFTP/TFTP | Host Name* | SW-9200 |
| Configuration > | Bluetooth | Banner | |
| Administration | | | |
| C Licensing | | Management Interface | GigabitEthernet0/0 |
| Troubleshooting | | IP Address* 0 | |
| | | Subnet Mask* | |
| | | System MTU(Bytes) 1 | 1500 |
| | | VTY Line 0 | 0-30 @View VTY options |
| | | VTY Transport Mode | Select a value |