cisco.



Software Configuration Guide, Cisco IOS XE 17.14.x (Catalyst 9400 Switches)

First Published: 2024-04-05

Americas Headquarters

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883 THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



Preface

This preface describes the conventions of this document and information on how to obtain other documentation. It also provides information on what's new in Cisco product documentation.

- Document Conventions, on page iii
- Related Documentation, on page v
- Obtaining Documentation and Submitting a Service Request, on page v

Document Conventions

This document uses the following conventions:

Convention	Description			
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)			
bold font	Commands and keywords and user-entered text appear in bold font.			
Italic font	Document titles, new or emphasized terms, and arguments for which you values are in <i>italic</i> font.			
Courier font	Terminal sessions and information the system displays appear in courier font.			
Bold Courier font	Bold Courier font indicates text that the user must enter.			
[x]	Elements in square brackets are optional.			
	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.			
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.			
$[x \mid y]$	Optional alternative keywords are grouped in brackets and separated by vertical bars.			

Convention	Description
$\{x \mid y\}$	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!,#	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Means the following information will help you solve a problem.

Ŵ

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Ð

Timesaver Means the described action saves time. You can save time by performing the action described in the paragraph.

Warning IN

ning IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number provided at the end of each warning statement to locate its translation in the translated safety warnings for this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

Ś

Note

Before installing or upgrading the , refer to the release notes.

Ŋ

Note Before installing or upgrading the switch, refer to the switch release notes.

Cisco Catalyst 9200 Series Switches documentation, located at:

https://www.cisco.com/c/en/us/products/switches/catalyst-9200-series-switches/index.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER

Contents

BGP EVPN VXLAN

Cisco DNA Service for Bonjour Cisco TrustSec High Availability Interface and Hardware Components **IP** Addressing Services IP Multicast Routing **IP** Routing Layer 2 Multiprotocol Label Switching Network Management Programmability Quality of Service Security System Management VLAN

Contents

I



Configuring the Switch Using the Web User Interface



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

- Introduction to Day 0 WebUI Configuration, on page 3
- Cisco DNA Center Cloud Onboarding Day 0 Wizard, on page 4
- Classic Day 0 Wizard, on page 7

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 This wizard would enable you to on-board this device to dnacentercloud.cisco.com. The wizard would give you step by		Classic Day 0 Wizard			
	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.		This wizard would enable you to configure the Switch with basic and advanced settings like User account, Management Interface IP address/LAN,STP mode selection etc. Once the wisard is successfully completed, user can access the Switch via WEBUI and command line using the Management Interface IP address provided.			
	NS BELOW BEFORE YOU BEGIN					
Ensure that you	a have all the required information from your service provide	er to complete the	e configuration.			
By default, the	wizard enables some recommended configurations. We re-	commend that yo	u keep these defaults unless you have a reason to change			
them.						
This wizard helps you to bring up your WAN/LAN connectivity quickly. You can change the configuration and configure advanced features after the						
wizard completes successfully.						
 As a best practice, when you use WebUI to configure a device, do not delete or modify the configuration directly by logging into the device. Changing 						

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

	BASIC SETTINGS			SUMMARY
create New Account			DEVICE INFO	HELP AND TIPS
Login Name*	testuser			
Login User Password*			Establish a new Usern Please remember it fo	ame and Password for the Device. r next Login.
Confirm Login User Password*			Establish a new passv level.	vord for the privileged command
evice ID Settings			Device name is an ide physical hardware dev	ntification that is given to the vice.
Device Name*	testdevice		clock synchronization	ol (NTP) is a networking protocol for between computer systems over able-latency data networks. Enter NTP server.
NTP Server	хххх			nen the difference in time will be f configuring the device.
Date & Time Mode	NTP Time	•	adjusted at the time o	comganing 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

	BASIC SETTINGS	SUMMARY
vice Management Settings		PHELP AND TIPS
P Address	Static DHCP	
/LAN ID* P Address* Subnet Mask* Default Gateway (optional) Associate VLAN Interface	2 x.x.xx x.x.xx x.x.xx (optional) GigabitEthernet1/0/2	Select this to enable access to the device using Teinet. Configur username and password to authenticate user access to the devi Select this to enable access to the device using Teinet. Configur username and password to authenticate user access to the devic 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 particip 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
DNS Server	X.X.X.X	forward VTP advertisements that they receive out their trunk por 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.

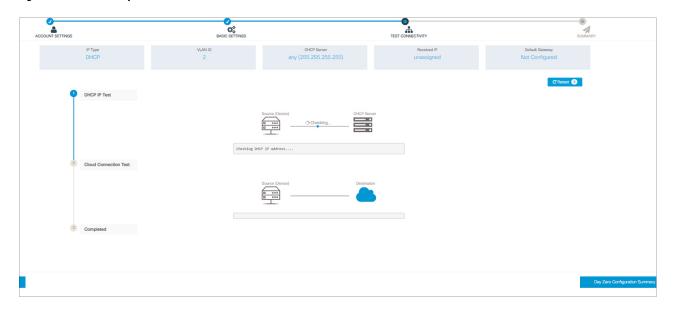
Figure 4: Basic Settings - DHCP Configuration

ACCOUNT SETTINGS	BASIC SETTINGS	TEST CONNECTIVITY	SUMMARY
evice Management Settings			HELP AND TIPS
IP Address	Static DHCP		
VLAN ID*	2		Select this to enable access to the device using Telnet. Configure username and password to authenticate user access to the devic
IP Address*	x.x.x		Select this to enable access to the device using Telnet. Configure username and password to authenticate user access to the device
Subnet Mask*	X.X.X		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.
Default Gateway (optional)	x.x.x.x (optional)		Enable transparent mode if you do not want the switch to particip
DNS Server	XXXX		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 port VTP Version 2.

L

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 3Once 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

B	F	Registry Editor											-		×
Fi	le	Edit View Favorites Help													
C	om	puter\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS	et\	Services\Tcpip\	Paramete	rs\Inter	faces\{4	6836ffc-	5358-4da1	-b9f8-a2a10f1a0c48}					
>	1	stexstor	^	Name				Туре		Data					
>	1	stisvc		(Default)				REG_S	7	(value not set)					
>	1	storahci		38 AddressTyp	e				WORD	0x00000000 (0)					
>	L	storfit		38 DhcpClient				REG_B		77 65 62 75 69					
>	1	stornvme						NEO_D		11 05 02 15 05					
>		storqosfit		Edit Binary Va	lue							>		79 00 00 0	
>		StorSvc		Value name:									100100	79 00 00 0	00000
>		storufs		DhcpClientIde											
>		storvsc			nther										
2		SVSVC		Value data:											
>		swenum		0000	77	65	62	75	69		webu	i			1
>		swprv													
		SynaMetSMI													
F		Synth3dVsc													
>		SynTP													
		SynTPEnhService SysMain													ł
>.>		SystemEventsBroker													
~		SZCCID													
ŝ		TabletInputService													
- (TapiSrv		1											
÷		Tcpip									ОК	Cancel			
	Ŀ	Linkage		10 12				NEQ L	WORD	000000000000000000000000000000000000000	02710911		-		
	-	Parameter													
	÷	Parameters													
		> Adapters													
		> DNSRegisteredAdapters													
		V] Interfaces													
		- 2a1d7785-5141-4b33-8f11-4b5cf324636c}													
		-2 {2e6a118d-8ff9-45c8-b861-13bbbf590a22}													
		-3199fba7-ae95-43f6-b34c-e2fbdde8cb40													
		46836ffc-6358-4da1-b9f8-a2a10f1a0c48													
		-1 {4828db99-4092-4a20-903b-e304a283e9f0}													
		-] {7baa2017-910a-4c77-b968-a9beb40c9646}													
		- [] {922467f8-ace4-4789-93b6-9a3799a7b574}													
		- [{b20b01ef-9511-4f8d-af8d-c03a948db0e1}													
		- [65fdd031-2580-445b-8430-074e5248bd14] <	-												
<		>		<											>

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.

L

				Netw	ork		Q Search
📄 Wi-Fi							
•	Wi-Fi	TCP/IP	DNS	WINS	802.1X	Proxies	Hardware
Config	jure IPv4:	Using DI	HCP			\$	
IPv4	Address:	XXXXXXXXXXX	16X XX 8				Renew DHCP Lease
Subr	net Mask:	2222/000	(12)55/2X(3)		DHCP	Client ID:	
	Router:	100000000	10XXXX				(If required)
Config	jure IPv6:	Automat	ically			\$	
	Router:	texexxxexx	S MXDexi	8X3495X			
IPv6	Address:	20087742	0050000	*****	KKK BXXXX	****	
Prefi	x Length:	162 8 X					
							Cancel
							Cancer

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	ins		~ Ū	Search Network C
his connection Rename	e this connection View s	tatus of this connection	Change settings of this	connection 🖷
Cisco AnyConnect Secu Mobility Client Connec Disabled	tion 🦰 🌄 Uni	ernet dentified network el(R) Ethernet Connectio	Enable	Loopback Adapter d Loopback Adapter
VMware Network Ada VMnet8	Network Connection Details	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 DNS Server IPv4 WINS 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	:33 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 S	etup Wizard						
	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY		
Create New Account				Hardware and Software	details of the device.		
Login Name				Platform Type:			
Password				IOS Installed:			
Confirm password							
				Serial Number:			
				Modules:			
				License Installed:			
Oreste 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.

Configuration Set	up Wizard				
CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
Device ID and Location Settings				O HELP /	AND TIPS
Device Name		<	① Device name is mandatory		
Date & Time Mode	Automatic	•		device name is an identification that is g	
				If manual time is set then the difference configuring the device.	in time will be adjusted at the time of
Device 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	gigabitethernet0/0			Select this to enable access to the devic password to authenticate user access to	ce 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 v transparent switch does not advertise it:	vant the switch to participate in VTP. A VTP s VLAN configuration and does not
Default Gateway (optional)	x.x.x.x (optional)			synchronize its VLAN configuration base transparent switches do forward VTP ad	d on received advertisements, but lvertisements that they receive out their trunk
< Setup Options					Site Profile >

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
------------------------------------	---------------------

CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
	Mon Aug 13 2018 14:18:37			HELP A	ND TIPS
vice Management Settings					
lanagement Interface	gigabitethernet0/0			device name is an identification that is g If manual time is set then the difference	
fanagement 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)			Select this to enable access to the devic password to authenticate user access to	
elnet				Select this to enable secure remote acc Configure a username and password to	
SSH				Enable transparent mode if you do not w transparent switch does not advertise its	
/TP transparent mode				synchronize its VLAN configuration base transparent switches do forward VTP ad	d on received advertisements, but
< 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.

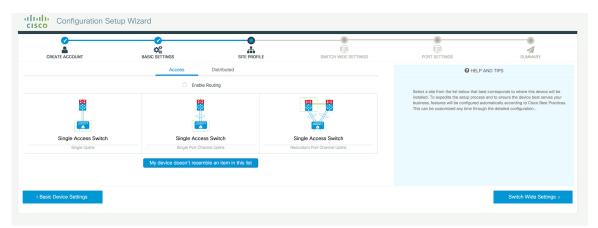
Choosing a site profile as part of Quick Setup allows you to configure your device based on the business needs of your enterprise. For example, you could use your device as an access switch, to connect client nodes and endpoints on your network, or as a distribution switch, to route packets between subnets and VLANs.

Setting	Single 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	name you provided as part name you provided as part n	
Spanning Tree Mode	RPVST+ RPVST+ H		RPVST+
VTP	Mode Transparent	Mode Transparent	Mode Transparent
UDLD	Enabled Enabled H		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	n 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 (Access Switches)

(Single Uplink) (Single Access Switch (Single Port Channel Uplink)	Single Access Switch (Redundant Port Channel Uplink)	
Management Interface	Layer 3 settings configured on the management port, based on Quick Setup	Layer 3 settings configured on the management port, based on Quick Setup	Layer 3 settings configured on the management port, based on Quick Setup	
IPv6 Host Policy	IPv6 host policy created	IPv6 host policy created	IPv6 host policy created	
QoS Policy for DownlinkAuto 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	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.	
Downlink Interfaces Downlink ports configured in Access mode		Downlink ports configured in Access mode	Downlink ports configured in Access mode	
Port-channel	Not configured	Port-channel to distribution created	Port-channel to distribution created	

Figure 12: Site Profile - Access Switches



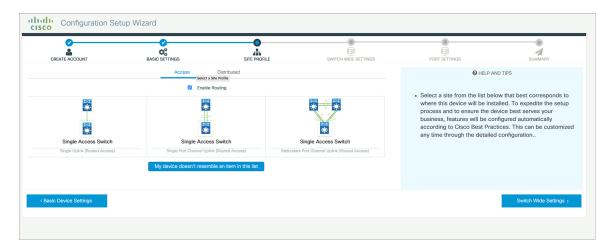
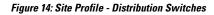


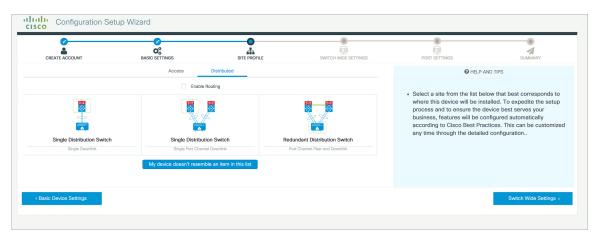
Figure 13: Site Profile - Access Switches (with Routed Access)

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	P 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	
SSH Version 2		Version 2	Version 2	
SCP	Enabled	Enabled	Enabled	
VTY Access to Switch	Enabled	Enabled	Enabled	
Service Timestamp	Enabled	Enabled	Enabled	

Switch (Single Downlink)		Single Distribution Switch (Single Port Channel Downlink)	Redundant Distribution Switch (Port Channel Peer and Downlink)	
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	
Management Interface	gement 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 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	nlink Interfaces 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	





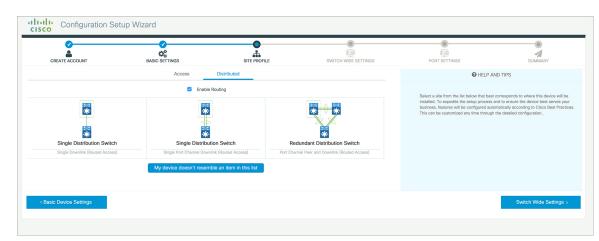


Figure 15: Site Profile - Distribution Switches (with Routed Access)

Configuring VLAN Settings

Step 1 In the **VLAN Configuration** section, you can configure both data and voice VLANs. Type a name for your data VLAN.

Step 2 To configure a data VLAN, ensure that the **Data VLAN** check box is checked, type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range.

Step 3 To configure a voice VLAN, ensure that the **Voice VLAN** check box is checked, type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate a VLAN range.

Configuring 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 16: VLAN and STP Settings

CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
AN Configuration				HELP A	ND TIPS
Data VLAN Voice VLAN Management Vi ^{Switch Wide Settings TP Configuration STP Mode Bridge Priority Bridge Priority Number}	RPVST 32768	•		service by configuring ports phones on a specific VLAN. STP is to prevent bridge loops and the t The part of a network address which lid Configure Syslog Client within the Claso through emergencies to generate error millifuctors.	N allows you to enhance VoIP to carry IPvoice traffic from IP readcast radiation that results from them. entlies it as belonging to a particular domain Device, use a severity level of warnings masque about Solver and hardware masque about Solver and hardware as collecting information from, and configurin
eneral 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 17: DHCP, NTP, DNS and SNMP Settings

CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
General Configuration				HELP A	ND TIPS
bomain Details Domain Name DNS Server Server, Details DHCP Server Systog Server				allows you to enhance Vol zervice by o IP phones on a specific VLAN. STP is to prevent bridge loops and the b The part of a network address which ide Configure Systep Gleen which the Calco through emergencies to generate error malfunctions. • Protocol for network manage	ntifies it as belonging to a particular domain. Device, use a severity level of warnings nessage about software and hardware ement and its collecting
NTP Server				information from, and config as switches, and routers on	uring, network devices, such an IP network.
< 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 18: Port Settings

CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
	Port Role OUplink	Access			
	Select Switch ALL	•			
23 S	Available (16)	Enabled	(0)		
	Uplinks ᅌ	Interfaces	\$		
	GigabitEthernet1/1/1	>			
٠	GigabitEthernet1/1/2	<i>></i>			
S	GigabitEthernet1/1/3	*			
	GigabitEthernet1/1/4	>			
witch Wide Settings					Day 0 Config Summar

What to do next

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

Figure 19: Day 0 Config Summary

Configuration Se	tup Wizard							
CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY			
SUMMARY					CLI Preview			
	This screen provides	the summary of all the steps configured as a par	t of the day zero configuration. Please click Finish to conf	gure 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, ✓ Manage	✓ Controller Name: test, ✓ Management Interface: gigabitethemet0/0(1.1.1.1),						
> Global Switch Settings	✓ Data VLAN: (), ✓ Voice VLAN: (no	V Data VLAN: (), V Voice VLAN: (not configured), V STP Mode: rapid-pvet, V Bridge Priority: 32768, V DNS Server:, V DHCP Server:, V NTP Server:, V Syslog Se						
> 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 20: 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	
(O) Administration >			
C Licensing		Management Interface	GigabitEthernet0/0
		IP Address* 0	
X Troubleshooting		Subnet Mask*	
		System MTU(Bytes) 0	1500
		VTY Line 1	0-30 Wiew VTY options
		VTY Transport Mode	Select a value