



Software Configuration Guide, Cisco IOS XE 17.13.x (Catalyst 9300 Switches)

First Published: 2023-12-30

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

SAMPLE

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.

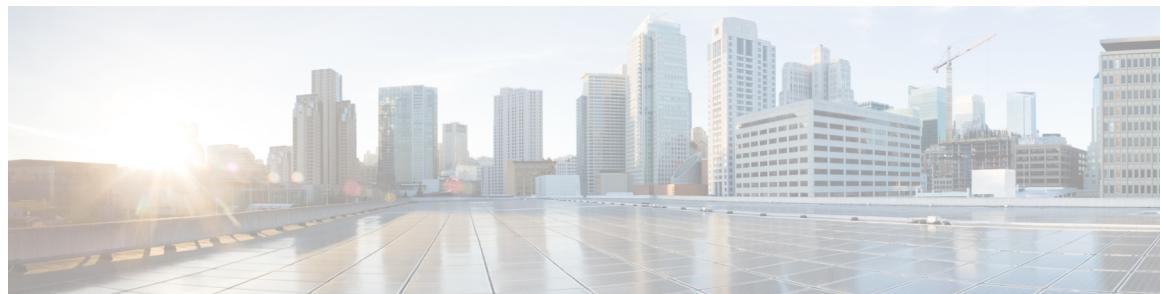
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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)

© 2023 Cisco Systems, Inc. All rights reserved.

SAMPLE



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
<code>^</code> or <code>Ctrl</code>	The <code>^</code> symbol and <code>Ctrl</code> represent the Control (Ctrl) key on a keyboard. For example, the key combination <code>^D</code> or <code>Ctrl-D</code> 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.
<i>Italic</i> font	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> font.
<code>Courier</code> font	Terminal sessions and information the system displays appear in <code>courier</code> font.
Codice 1 <code>Bold Courier</code> font	Bold Courier font indicates text that the user must enter.
<code>[x]</code>	Elements in square brackets are optional.
<code>...</code>	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
<code> </code>	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
<code>[x y]</code>	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Description
{x 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.



Tip Means *the following information will help you solve a problem*.



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



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



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

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.

SAMPLE

SAMPLE



CHAPTER 1

Contents

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

SAMPLE

SAMPLE



CHAPTER 2

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

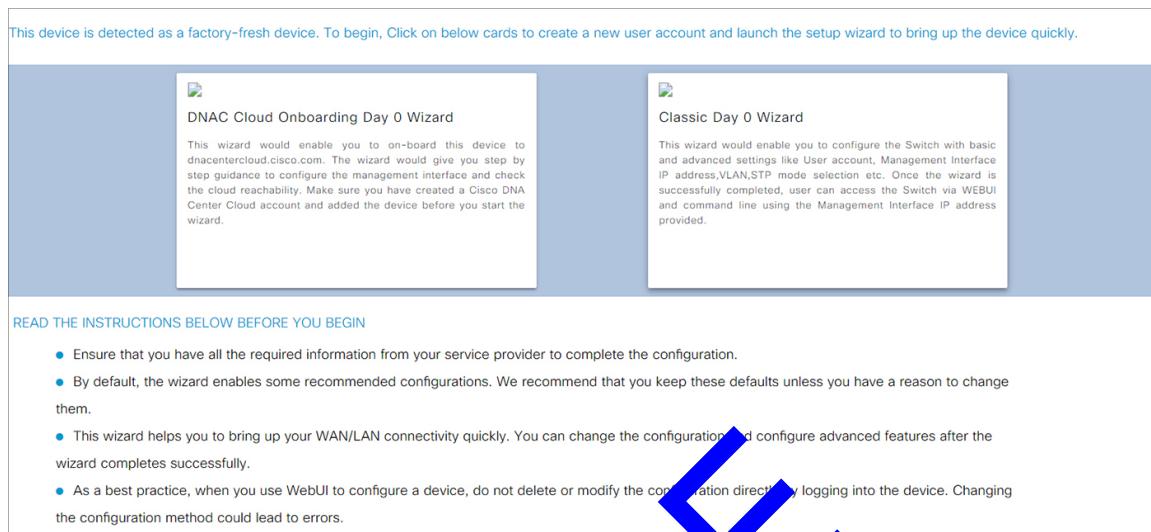
After you complete the hardware installation, you need to setup the switch with configuration required to enable traffic to pass through the network. On your first day with your new device, you can perform a number of tasks to ensure that your device is online, reachable and easily configured.

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



Cisco DNA Center Cloud Onboarding Day 0 Wizard

Use this wizard to configure the management interface and check if it is reachable through the cloud.



Note

You must add the device to your Cisco DNA Center Cloud account before proceeding with this wizard.

Configuring Account Settings

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

Step 1

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

Step 2

Set a password of up to 25 alphanumeric characters.

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

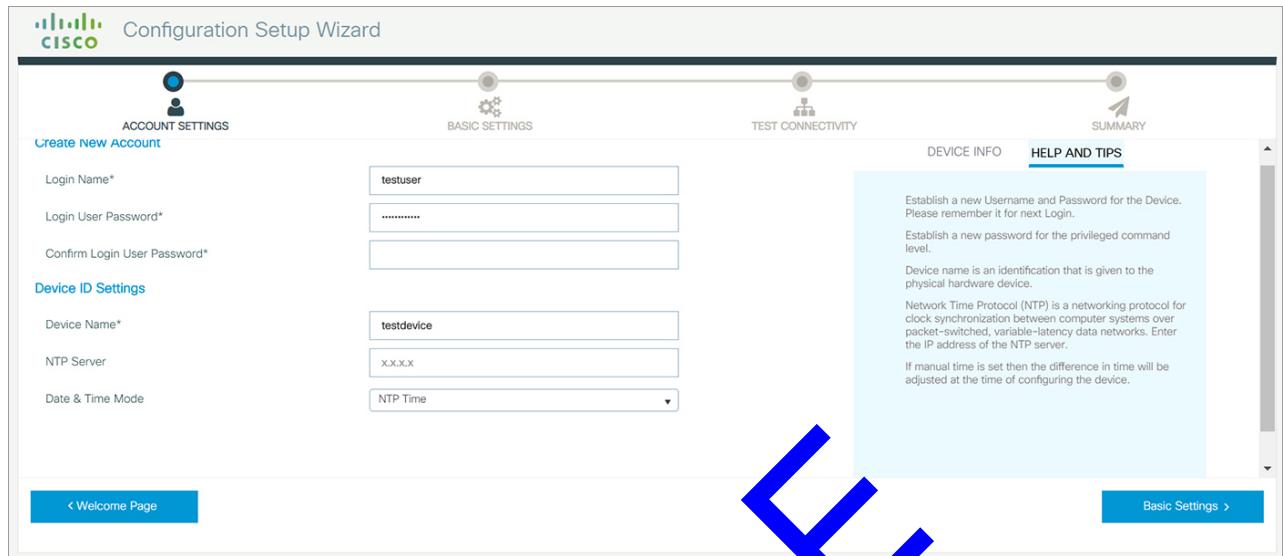
Step 3

In the **Device ID Settings** section, type a unique name in the **Device Name** field to identify your device in the network.

Step 4

Enter the date and time for your device manually in the **Time & Device Mode** field. To synchronize your device with an external timing mechanism such as a Network Time Protocol (NTP) clock source, enter the IP address in the **NTP Server** field.

Figure 2: Account Settings



Configuring Basic Device Settings

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

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

Configuring Basic Device Settings

Figure 3: Basic Settings - Static Configuration

The screenshot shows the 'Basic Settings' step of the Configuration Setup Wizard. The page title is 'Configuration Setup Wizard' with the Cisco logo. The navigation bar at the top includes 'ACCOUNT SETTINGS' (with a checkmark icon), 'BASIC SETTINGS' (with a gear icon), 'TEST CONNECTIVITY' (with a network icon), and 'SUMMARY' (with a document icon). Below the navigation bar, the section 'Device Management Settings' is displayed. It includes fields for IP Address (radio buttons for 'Static' and 'DHCP'), VLAN ID* (set to 2), IP Address* (x.x.x.x), Subnet Mask* (x.x.x.x), Default Gateway (optional) (x.x.x.x optional), Associate VLAN Interface (GigabitEthernet1/0/2), and DNS Server (x.x.x.x). A 'Create New Account' button is located at the bottom left, and a 'Test Connectivity >' button is at the bottom right. A 'HELP AND TIPS' panel on the right provides information about Telnet, SSH, and VTP.

Step 3

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

- Enter a value in the VLAN ID field.

VLAN ID must be a value other than 1.

- Ensure that the IP address you assign is part of the subnet mask you enter.
- Optionally, enter an IP address to specify the default gateway.
- Enter the address of the DNS Server.

Figure 4: Basic Settings - DHCP Configuration

The screenshot shows the 'Basic Settings' step of the Configuration Setup Wizard for DHCP configuration. The interface is identical to Figure 3, with the 'DHCP' radio button selected instead of 'Static'. The VLAN ID field is set to 2, and the other fields (IP Address*, Subnet Mask*, Default Gateway, and DNS Server) are empty or show placeholder values. The 'HELP AND TIPS' panel on the right provides information about Telnet, SSH, and VTP.

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 2** If connection is not established, click the **Retest** button.
If connection still fails, go to the previous **Basic Settings** page, make changes to the settings, and test connectivity again.
- Step 3** Once connectivity is established, go to the **Day Zero Configuration Summary** to save the configurations.

Figure 5: Test Connectivity



- Step 4** Verify that the configurations are applied successfully, and the device is redirected to Cisco DNAC Cloud.

What to do next

If redirection does not succeed, verify if the device is associated with a redirection controller profile on *Cisco PnP Connect (devicehelper)*.

Classic Day 0 Wizard

Use this wizard to configure the device with basic and advanced settings. Once complete, you can access the device through the WebUI using the management interface IP address.

Connecting to the Switch

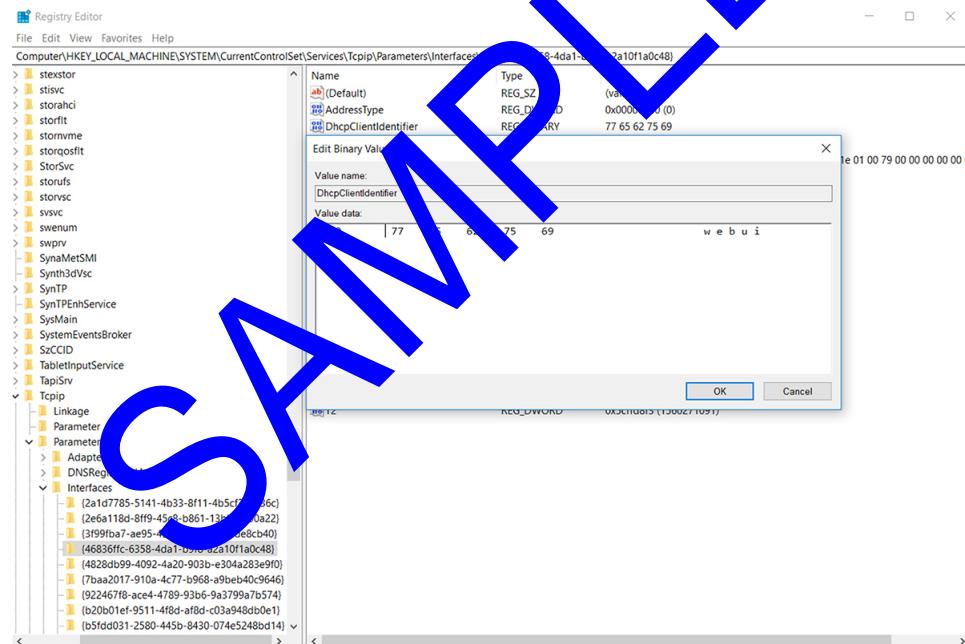
Before you begin

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

Setting up the DHCP Client Identifier on the client for Windows

1. Type **regedit** in the Windows search box on the taskbar and press *enter*.
2. If prompted by User Account Control, click **Yes** to open the Registry Editor.
3. Navigate to
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces and locate the **Ethernet Interface** Global Unique Identifier (GUID).
4. Add a new REG_BINARY **DhcpClientIdentifier** with Data **77 65 62 75 69** for **webui**. You need to manually type in the value.

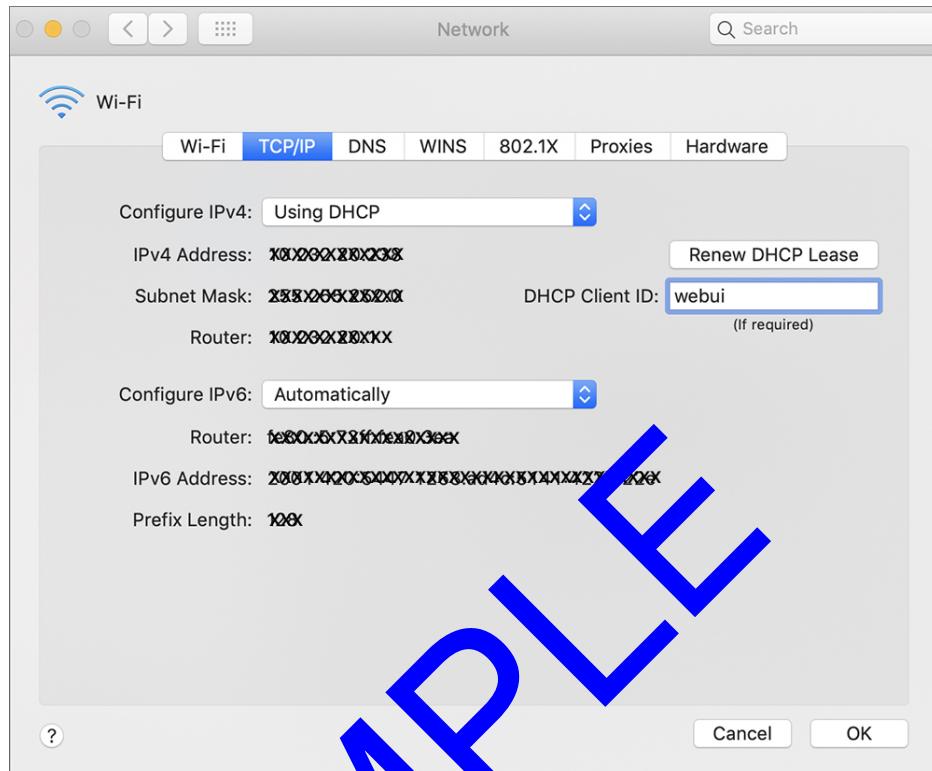
Figure 6: Setting up DHCP Client Identifier on Windows



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

Setting up the DHCP Client Identifier on the client for MAC

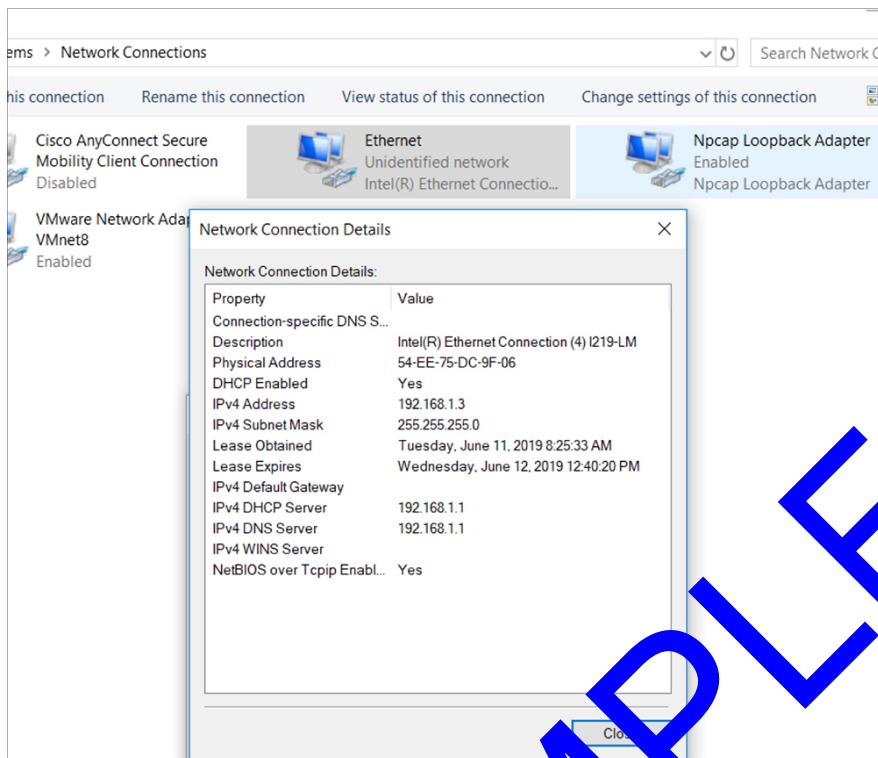
1. Go to **System Preferences > Network > Advanced > TCP > DHCP Client ID:** and enter **webui**.

Figure 7: Setting up DHCP Client Identifier on MAC

2. Click **OK** to save the changes.

The bootup script runs the configuration wizard, which prompts you for basic configuration input: (**Would you like to enter the initial configuration dialog? [yes/no]:**). To configure Day 0 settings using the web UI, do not enter a response; perform the following tasks instead:

-
- 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.
- A large blue watermark reading 'SAMPLE' is diagonally across the bottom of the page.

Creating User Accounts**Figure 8: Obtaining the IP Address**

It may take up to three mins. You must complete the Day 0 setup through the web UI before using the device terminal.

Step 4

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

Step 5

Enter the Day 0 **username webui** and **password cisco**.

What to do next

Create a user account.

Creating User Accounts

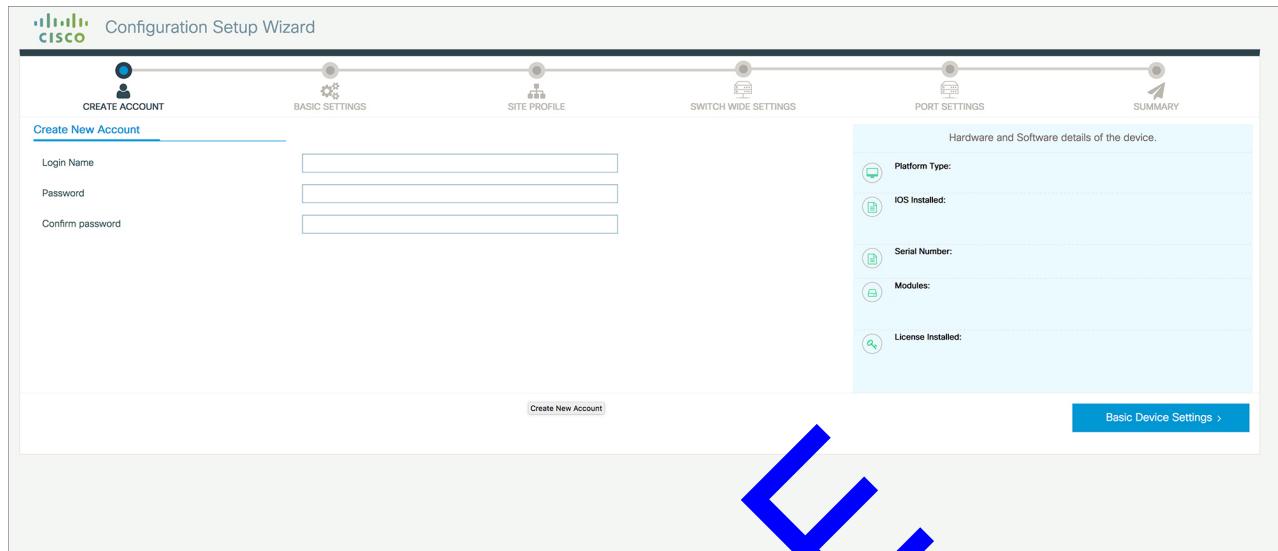
Setting a username and password is the first task you will perform on your device. Typically, as a network administrator, you will want to control access to your device and prevent unauthorized users from seeing your network configuration or manipulating your settings.

Step 1

Log on using the default username and password provided with the device.

Step 2

Set a password of up to 25 alphanumeric characters. The username password combination you set gives you privilege 15 access. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Figure 9: Create Account

Choosing Setup Options

Select **Wired Network** to configure your device based on a site profile, and continue to configure switch wide settings. Otherwise, continue to the next step and configure only basic settings for your device.

Configuring Basic Device Settings

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

Step 1

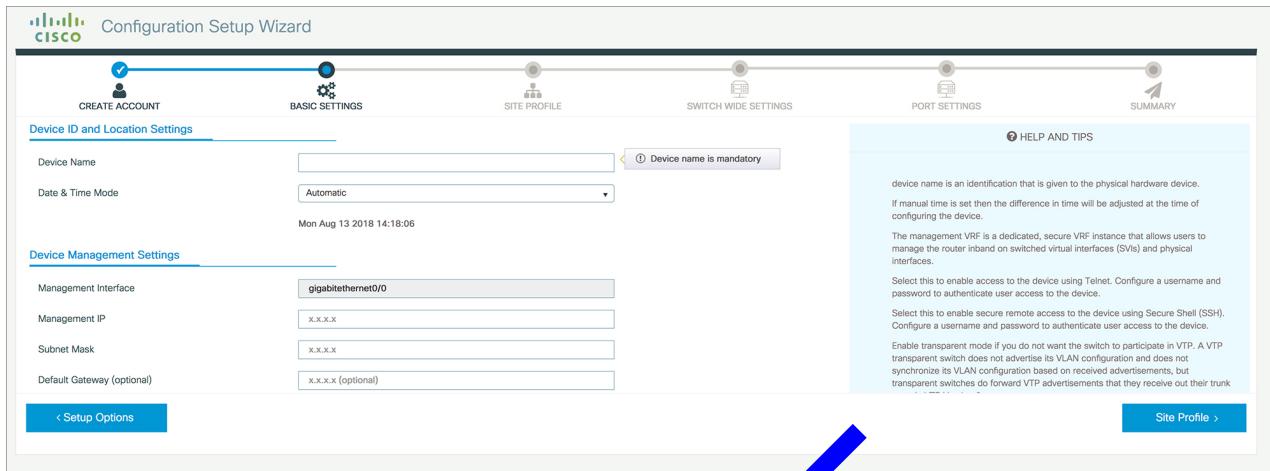
In the **Device ID and Location** settings section, type a unique name to identify your device in the network.

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.

Configuring Basic Device Settings

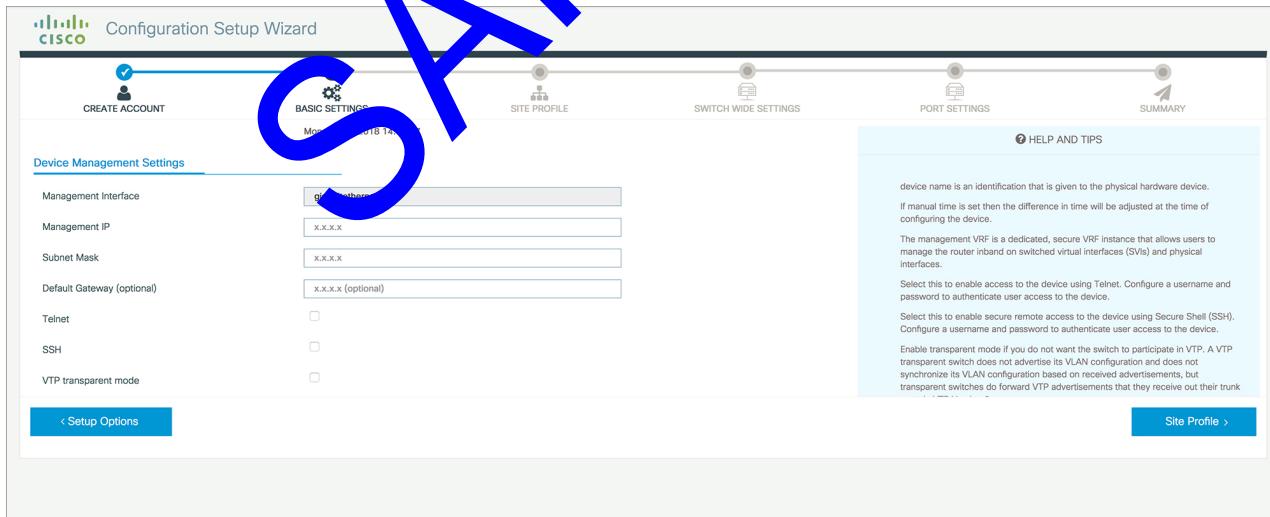
Figure 10: Basic Settings - Device ID and Location Settings



- 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), click the **SSH** check box.
- Step 7** Check the **VTP transparent mode** check box to disable the device from participating in VTP.

If you did not select **Wired Network**, in the earlier step, continue to the next screen to verify your configuration on the **Day 0 Config Summary** screen, and click **Finish**. To automatically configure your device based on a site profile, click **Setup Options**, and select **Wired Network**.

Figure 11: Basic Settings - Device Management Settings



Configuring Your Device Based on a Site Profile

To ease your configuration tasks and save time, choose a site profile based on where your device may be installed and managed in your network. Based on the site profile you choose, your device is automatically configured according to Cisco best practices. You can easily modify this default configuration, from the corresponding detailed configuration screens.

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

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 12: VLAN and STP Settings

The screenshot shows the 'Configuration Setup Wizard' interface. At the top, there are tabs: CREATE ACCOUNT, BASIC SETTING, SITE PROFILE, SWITCH WIDE SETTINGS, PORT SETTINGS, and SUMMARY. The 'SITE PROFILE' tab is selected. On the left, there are sections for 'VLAN Configuration' (Data VLAN, Voice VLAN, Management VLAN), 'STP Configuration' (STP Mode dropdown set to RPVST, Bridge Priority checked, Bridge Priority Number dropdown set to 32768), and 'General Configuration' (Site Profile button). On the right, there is a 'HELP AND TIPS' panel with information about Data VLANs, STP, and Syslog. At the bottom right is a 'Port Settings >' button.

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 13: DHCP, NTP, DNS and SNMP Settings



What to do next

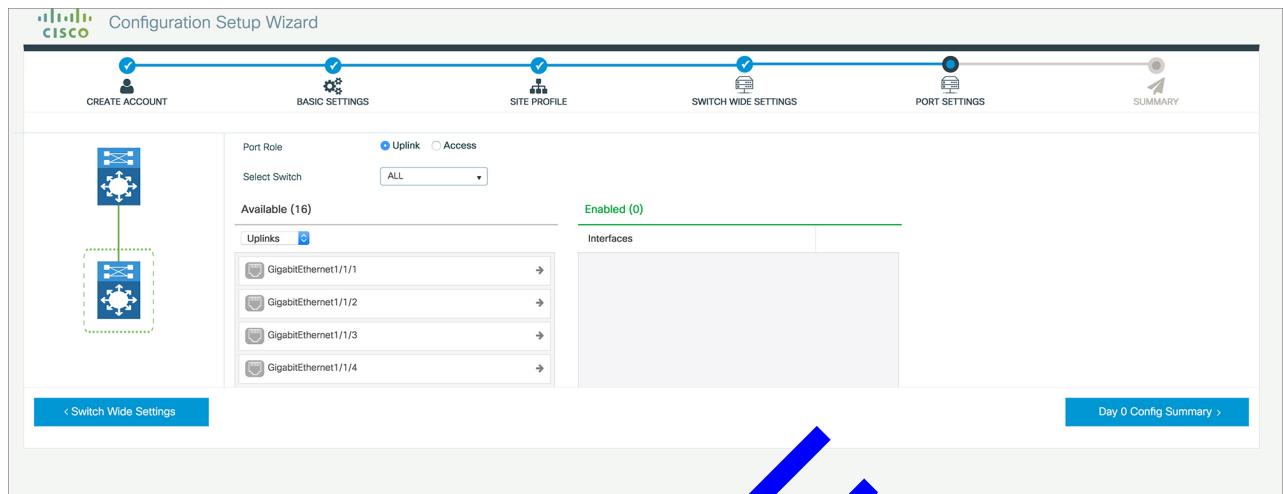
Configure port settings

Configuring Port Settings

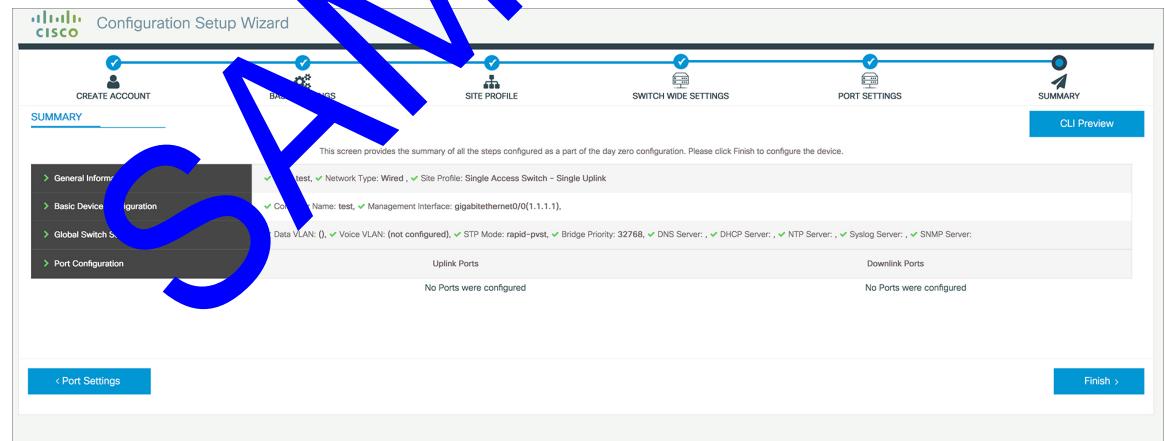
- Step 1** Based on the site profile chosen in the earlier step which is displayed in the left-pane, select the **Port Role** from among the following options:
- Uplink – For connecting to devices towards the core of the network.
 - Downlink – For connecting to devices further down in the network topology.
 - 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 14: Port Settings**What to do next**

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

Figure 15: Day 0 Config Summary

Configuring VTY Lines

For connecting to the device through Telnet or SSH, the Virtual Terminal Lines or Virtual TeleType (VTY) is used. The number of VTY lines is the maximum number of simultaneous access to the device remotely. If the device is not configured with sufficient number of VTY lines, users might face issues with connecting to the WebUI. The default value for VTY Line is . The device allows up to simultaneous sessions.

Configuring VTY Lines

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 16: Configuring VTY Line

