Configuring the Switch

- Configuring the Switch Using the Web User Interface, on page 1
- Configuring the Switch Using the CLI, on page 15

Configuring the Switch Using the Web User Interface

Setting up the Switch

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. It comes with the default image, so there is no need to enable anything or install any license on the device. You can use WebUI to build configurations, and to monitor and troubleshoot the device without having CLI expertise.

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.
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.
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:

**Procedure**

**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.
Creating User Accounts

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

Procedure

**Step 1**  Log on using the default username and password provided with the device.
The default username is **cisco**; the default password is the serial number of the switch chassis. For Cisco Catalyst switches running software versions earlier than Cisco IOS XE Fuji 16.9.x, the default username is **webui**; the default password is the serial number of the switch chassis.

**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 4: 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:

**Procedure**

**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.
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**.

---

**Configuring Your Device Based on a Site Profile**

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Single Access Switch (Single Uplink)</th>
<th>Single Access Switch (Single Port Channel Uplink)</th>
<th>Single Access Switch (Redundant Port Channel Uplink)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The hostname or device name you provided as part of Quick Setup</td>
<td>The hostname or device name you provided as part of Quick Setup</td>
<td>The hostname or device name you provided as part of Quick Setup</td>
</tr>
<tr>
<td>Spanning Tree Mode</td>
<td>RPVST+</td>
<td>RPVST+</td>
<td>RPVST+</td>
</tr>
<tr>
<td>VTP</td>
<td>Mode Transparent</td>
<td>Mode Transparent</td>
<td>Mode Transparent</td>
</tr>
<tr>
<td>UDLD</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Error Disable Recovery</td>
<td>Recovery mode set to Auto</td>
<td>Recovery mode set to Auto</td>
<td>Recovery mode set to Auto</td>
</tr>
<tr>
<td>Port Channel Load Balance</td>
<td>Source Destination IP</td>
<td>Source Destination IP</td>
<td>Source Destination IP</td>
</tr>
<tr>
<td>SSH</td>
<td>Version 2</td>
<td>Version 2</td>
<td>Version 2</td>
</tr>
<tr>
<td>SCP</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>VTY Access to Switch</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Service Timestamp</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>VLAN</td>
<td>The following VLANs are created:</td>
<td>The following VLANs are created:</td>
<td>The following VLANs are created:</td>
</tr>
<tr>
<td></td>
<td>• Default VLAN</td>
<td>• Default VLAN</td>
<td>• Default VLAN</td>
</tr>
<tr>
<td></td>
<td>• Data VLAN</td>
<td>• Data VLAN</td>
<td>• Data VLAN</td>
</tr>
<tr>
<td></td>
<td>• Voice VLAN</td>
<td>• Voice VLAN</td>
<td>• Voice VLAN</td>
</tr>
<tr>
<td></td>
<td>• Management VLAN</td>
<td>• Management VLAN</td>
<td>• Management VLAN</td>
</tr>
<tr>
<td>Management Interface</td>
<td>Layer 3 settings configured on the management port, based on Quick Setup</td>
<td>Layer 3 settings configured on the management port, based on Quick Setup</td>
<td>Layer 3 settings configured on the management port, based on Quick Setup</td>
</tr>
<tr>
<td>IPv6 Host Policy</td>
<td>IPv6 host policy created</td>
<td>IPv6 host policy created</td>
<td>IPv6 host policy created</td>
</tr>
<tr>
<td>Setting</td>
<td>Single Access Switch (Single Uplink)</td>
<td>Single Access Switch (Single Port Channel Uplink)</td>
<td>Single Access Switch (Redundant Port Channel Uplink)</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>Uplink Interfaces</td>
<td>Selected uplink interfaces configured as trunk ports, set to allow all VLANs</td>
<td>Selected ports configured as Port-channel in trunk mode, set to allow all VLANs.</td>
<td>Selected ports configured as Port-channel in trunk mode, set to allow all VLANs.</td>
</tr>
<tr>
<td>Downlink Interfaces</td>
<td>Downlink ports configured in Access mode</td>
<td>Downlink ports configured in Access mode</td>
<td>Downlink ports configured in Access mode</td>
</tr>
<tr>
<td>Port-channel</td>
<td>Not configured</td>
<td>Port-channel to distribution created</td>
<td>Port-channel to distribution created</td>
</tr>
</tbody>
</table>

**Figure 7: Site Profile - Access Switches**
**Figure 8: Site Profile - Access Switches (with Routed Access)**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Single Distribution Switch (Single Downlink)</th>
<th>Single Distribution Switch (Single Port Channel Downlink)</th>
<th>Redundant Distribution Switch (Port Channel Peer and Downlink)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The hostname or device name you provided as part of Quick Setup</td>
<td>The hostname or device name you provided as part of Quick Setup</td>
<td>The hostname or device name you provided as part of Quick Setup</td>
</tr>
<tr>
<td>Spanning Tree Mode</td>
<td>RPVST+</td>
<td>RPVST+</td>
<td>RPVST+</td>
</tr>
<tr>
<td>VTP</td>
<td>Mode Transparent</td>
<td>Mode Transparent</td>
<td>Mode Transparent</td>
</tr>
<tr>
<td>UDLGD</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Error Disable Recovery</td>
<td>Recovery mode set to Auto</td>
<td>Recovery mode set to Auto</td>
<td>Recovery mode set to Auto</td>
</tr>
<tr>
<td>Port Channel Load Balance</td>
<td>Source Destination IP</td>
<td>Source Destination IP</td>
<td>Source Destination IP</td>
</tr>
<tr>
<td>SSH</td>
<td>Version 2</td>
<td>Version 2</td>
<td>Version 2</td>
</tr>
<tr>
<td>SCP</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>VTY Access to Switch</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Service Timestamp</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
### Setting | Single Distribution Switch (Single Downlink) | Single Distribution Switch (Single Port Channel Downlink) | Redundant Distribution Switch (Port Channel Peer and Downlink)
--- | --- | --- | ---
VLAN | The following VLANs are created:  
• Default VLAN  
• Data VLAN  
• Voice VLAN  
• Management VLAN | The following VLANs are created:  
• Default VLAN  
• Data VLAN  
• Voice VLAN  
• Management VLAN | The following VLANs are created:  
• Default VLAN  
• Data VLAN  
• Voice VLAN  
• Management VLAN
Management Interface | Layer 3 settings configured on the management port, based on Quick Setup | Layer 3 settings configured on the management port, based on Quick Setup | Layer 3 settings configured on the management port, based on Quick Setup
Uplink Interfaces | Selected uplink ports connect to other distribution or core switches | Selected uplink ports connect to other distribution or core switches | Selected uplink ports connect to other distribution or core switches
Downlink Interfaces | Downlink connections to access switches configured in Trunk mode | Downlink connections to access switches configured in Trunk mode | Downlink connections to access switches configured in Trunk mode
Port-channel | Port-channel to core created | Port-channel to core or access created | Port-channel to core or distribution created

*Figure 9: Site Profile - Distribution Switches*
### Table 3: Default Configuration Loaded with Each Site Profile (Core Switches)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Standalone Core Switch (with ECMP Peers)</th>
<th>Standalone Collapsed Core Switch (with ECMP Peer and Port Channel Downlink)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The hostname or device name you provided as part of Quick Setup</td>
<td>The hostname or device name you provided as part of Quick Setup</td>
</tr>
<tr>
<td>UDLD</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Error Disable Recovery</td>
<td>Recovery mode set to Auto</td>
<td>Recovery mode set to Auto</td>
</tr>
<tr>
<td>Port Channel Load Balance</td>
<td>Source Destination IP</td>
<td>Source Destination IP</td>
</tr>
<tr>
<td>SSH</td>
<td>Version 2</td>
<td>Version 2</td>
</tr>
<tr>
<td>SCP</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>VTY Access to Switch</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Mitigate Address Spoofing</td>
<td>Unicast RPF (uRPF) in strict mode</td>
<td>Unicast RPF (uRPF) in strict mode</td>
</tr>
<tr>
<td>Service Timestamp</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Management Interface</td>
<td>Layer 3 settings configured on the management port, based on Quick Setup</td>
<td>Layer 3 settings configured on the management port, based on Quick Setup</td>
</tr>
<tr>
<td>QoS Policy</td>
<td>QoS Policy for Distribution/Core defined</td>
<td>QoS Policy for Distribution/Core defined</td>
</tr>
<tr>
<td>Uplink Interfaces</td>
<td>Selected uplink ports connect to MAN/WAN device</td>
<td>Selected uplink ports connect to MAN/WAN device</td>
</tr>
<tr>
<td>Downlink Interfaces</td>
<td>Downlink connections to access switches</td>
<td>Downlink connections to distribution switches</td>
</tr>
</tbody>
</table>
### Configuring Switch Wide Settings

#### Configuring VLAN Settings

**Procedure**

**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

**Procedure**

**Step 1**
RPVST is the default STP mode configured on your device. You can change it to PVST from the **STP Mode** drop-down list.

**Step 2**
To change a bridge priority number from the default value 32748, change **Bridge Priority** to Yes and choose a priority number from the drop-down list.
Configuring DHCP, NTP, DNS and SNMP Settings

Procedure

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

Procedure

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

- Uplink – For connecting to devices towards the core of the network.
- Downlink – For connecting to devices further down in the network topology.
- Access – For connecting guest devices that are VLAN-unaware.

**Step 2**
Choose an option from the Select Switch drop-down list.

**Step 3**
Make selections from the Available list of interfaces based on how you want to enable them and move them to the Enabled list.
What to do next

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

Figure 15: Day 0 Config Summary

Configuring the Switch Using the CLI

Accessing the CLI Through the Console Port

You can access the CLI on a configured or unconfigured switch by connecting the RJ-45 console port or USB console port of the switch to your PC or workstation and accessing the switch through a terminal emulation program.
Connecting the RJ-45 Console Port

Procedure

Step 1 Connect the RJ-45-to-DB-9 adapter cable to the 9-pin serial port on the PC. Connect the other end of the cable to the switch console port.

Step 2 Start the terminal-emulation program on the PC or the terminal. The program, frequently a PC application such as HyperTerminal or ProcommPlus, makes communication between the switch and your PC or terminal possible.

Step 3 Configure the baud rate and character format of the PC or terminal to match the console port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Step 4 Power on the switch as described in the switch getting started guide.

Step 5 The PC or terminal displays the bootloader sequence. Press Enter to display the setup prompt.

Connecting the USB Console Port

Procedure

Step 1 If you are connecting the switch USB console port to a Windows-based PC for the first time, install the USB driver. See Installing the Cisco Microsoft Windows USB Device Driver, on page 17.

Note USB Type A port on the switch provides file system support and is NOT a console port. See USB Type A Port section.

Step 2 Connect a USB cable to the PC USB port. Connect the other end of the cable to the switch mini-B (5-pin-connector) USB console port.

Step 3 Start the terminal-emulation program on the PC or the terminal. The program, frequently a PC application such as HyperTerminal or ProcommPlus, makes communication between the switch and your PC or terminal possible.
Step 4 Configure the baud rate and character format of the PC or terminal to match the console port default characteristics:

• 9600 baud
• 8 data bits
• 1 stop bit
• No parity
• None (flow control)

Step 5 Power on the switch as described in the switch getting started guide.

Step 6 The PC or terminal displays the bootloader sequence. Press Enter to display the setup prompt. Follow the steps in the Setup program.

Installing the Cisco Microsoft Windows USB Device Driver

A USB device driver must be installed the first time a Microsoft Windows-based PC is connected to the USB console port on the switch.

Installing the Cisco Microsoft Windows 7 USB Driver

Procedure

Step 1 Obtain the Cisco USB console driver file from the Cisco.com web site and unzip it.

Note You can download the driver file from the Cisco.com site for downloading the switch software.

Step 2 If using 32-bit Windows 7, double-click the setup.exe file in the Windows_32 folder. If using 64-bit Windows 7, double-click the setup(x64).exe file in the Windows_64 folder.

Step 3 The Cisco Virtual Com InstallShield Wizard begins. Click Next.

Step 4 The Ready to Install the Program window appears. Click Install.

Note If a User Account Control warning appears, click Allow - I trust this program to proceed.

Step 5 The InstallShield Wizard Completed window appears. Click Finish.

Step 6 Connect the USB cable to the PC and the switch console port. The USB console port LED turns green, and the Found New Hardware Wizard appears. Follow the instructions to complete the driver installation.
Uninstalling the Cisco Microsoft Windows USB Driver

Uninstalling the Cisco Microsoft Windows 7 USB Driver

**Before you begin**

Disconnect the switch console terminal before uninstalling the driver.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Run setup.exe for Windows 32-bit or setup(x64).exe for Windows-64bit. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>The InstallShield Wizard for Cisco Virtual Com appears. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>When the Program Maintenance window appears, select the Remove radio button. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>When the Remove the Program window appears, click <strong>Remove</strong>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If a User Account Control warning appears, click <strong>Allow - I trust this program to proceed</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>When the InstallShield Wizard Completed window appears, click <strong>Finish</strong>.</td>
</tr>
</tbody>
</table>