



Overview

- [Overview of the Cisco IE3500 Series Switch, on page 1](#)
- [Configuring the Switch Using the Web User Interface, on page 2](#)
- [Introduction to Day 0 WebUI Configuration, on page 2](#)
- [Device Configuration, on page 2](#)

Overview of the Cisco IE3500 Series Switch

Cisco IE3500 Rugged Series Switches

These are ruggedized switching platforms and provides superior high-bandwidth switching and proven Cisco IOS XE Software for industrial environments.

These DIN-rail Industrial Ethernet switches are designed to cater deployments where hardened products are required, including factory automation, smart cities, energy and process control, Intelligent Transportation Systems (ITS), energy production sites, smart city programs, and mining. They bring improved overall performance, greater bandwidth, a richer feature set, enhanced hardware, and class leading security

The switches include security features to provide secured networking environment

- Cisco Trusted Platform Module (TPM)—serves as a hardware root-of-trust for secure boot.
- Secure Boot—uses a public key to validate each subsequent booting stage.
- Chip guard—Cisco developed security feature that records unique ID of critical system to prevent hardware tampering.

Cisco IE3500H Heavy Duty Series Switches

These are the next-generation managed IP67 PoE switches powered by Cisco IOS XE and are ideal for deployment in the harshest environments. They are IP67-rated for water and dust resistance and are hardened to withstand temperatures ranging from freezing cold to extreme heat (-40 to 85°C), as well as severe shock and vibration.

The switches are available with up to 24 ports, offering either Fast Ethernet or all Gigabit Ethernet with M12 connectors. These switches can be wall-mounted and deployed without a housing cabinet, offering a power budget of 360W, and supporting Power over Ethernet (PoE), PoE+, and Universal Power over Ethernet (UPOE) at 60W.

The switches are equipped with advanced network-based security, segmentation, and visibility features for the most demanding industrial environments. They extend the power of intent-based networking to the harshest Internet of Things (IoT) edge, with use cases in industries such as mining, railways, and manufacturing.

Configuring the Switch Using the Web User Interface

This document walks you through the steps to access and configure your switch using the Web UI.



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

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.

Device Configuration

Use the procedures mentioned here 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



Note Before proceeding, ensure you have completed the Express Setup outlined in the hardware installation guide.

Procedure

- Step 1** Make sure that no devices are connected to the switch.
- Step 2** Connect one end of an ethernet cable to the switch and the other end of the ethernet cable to the host computer.
- Step 3** Set up your computer 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.

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** and **password**.

Note

By default, the login username is *admin*, and the password is the *system serial number*. You can change it as required.

Creating User Accounts

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

Procedure

Step 1 Launch a web browser on the computer and enter the device IP address (**https://192.168.1.1**) in the address bar.

Step 2 Enter the **username** in the **Login Name** field.

Step 3 Enter **password** in the **Login User Password** field.

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

Step 4 Reconfirm the password for the user in the **Confirm Login User Password** field.

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

Step 6 In the Device ID Settings section, enter a value in the **Device Name** field.

Step 7 (Optional) Enter NTP server details in the **NTP Server** field.

Step 8 Use the **Date & Time Mode** drop-down list to select NTP time.

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 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 value in the **VLAN ID** field to associate with the interface.
 - Enter a value in the **IP Address** field. Ensure that the IP address you assign is part of the subnet mask you enter.
 - Enter a value in the **Subnet Mask** field.
 - (Optional) Enter a value in the **Default Gateway** field.
 - Use the **Associated VLAN with Interface** section to select interfaces.
 - (Optional) Use the slider next to the **Telnet** field to enable access to the device using telnet.
 - (Optional) Use the slider next to the **SSH** field to enable secure remote access to the device using Secure Shell (SSH).
 - (Optional) Use the slider next to the **SSH** field to enable secure remote access to the device using Secure Shell (SSH).
 - (Optional) Use the slider next to the **VTP Transparent Mode** field to manage VLANs across a network of switches.
 - (Optional) In the Device CIP Settings section, use the slider next to the **CIP Status** field to enable CIP.
CIP is used for monitoring and diagnosing the health and functionality of industrial networks and devices.
- Step 3** If you chose *DHCP*, perform the following steps:
- Enter a value in the **VLAN ID** field to associate with the interface.
VLAN ID must be a value other than 1.
 - Enter a value in the **IP Address** field to specify the default gateway. Ensure that the IP address you assign is part of the subnet mask you enter.
 - Enter a value in the **Subnet Mask** field.
 - (Optional) Enter a value in the **Default Gateway** field.
 - (Optional) Use the slider next to the **Telnet** field to enable access to the device using telnet.
 - (Optional) Use the slider next to the **SSH** field to enable secure remote access to the device using SSH.
 - (Optional) Enter a value in the **Domain Name for SSH** field.
 - (Optional) Use the slider next to the **VTP Transparent Mode** field to manage VLANs across a network of switches.
 - (Optional) In the Device CIP Settings section, use the slider next to the **CIP Status** field to enable CIP.
CIP is used for monitoring and diagnosing the health and functionality of industrial networks and devices.
-

Configuring VLAN Settings

In the **VLAN Configuration** section, you can configure both data and voice VLANs.

Procedure

-
- Step 1** Use the slider next to the **Data VLAN** to enable data VLAN.
 - Step 2** Use the slider next to the **Voice VLAN** to enable voice VLAN.
-

Configuring 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 32768, 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** In the **DNS Server** field, type an IP address to identify the DNS server. This server is used for name and address resolution on your device.
 - Step 3** In the **DHCP Server** field, type the IP address of the DHCP 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** In the **Management Details** section, type an IP address to identify the SNMP server in the **SNMP Server** field.

SNMPv1, SNMPv2, and SNMPv3 are supported on your device.
 - Step 6** Specify the **SNMP community** string to permit access to the SNMP protocol.
 - Step 7** Click **Day 0 Config Summary** button to verify the configuration.
 - Step 8** Click **Submit**.
-

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 98 simultaneous sessions.

Procedure

-
- Step 1** From the WebUI, navigate through **Administration > Device > HTTP/HTTPS/Netconf/VTY**.
 - Step 2** In the **VTY Line** field, enter **0-xx**, depending on how many VTY lines you want to configure.
 - Step 3** Use the **VTY Transport Mode** drop-down list to select the VTY transport mode.
-