Cisco Catalyst IE3x00 Rugged Series Switches Hardware Installation Guide

First Published: 2018-01-03

Last Modified: 2023-12-14

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

CONTENTS

Preface

Audience

This guide is for the qualified installer responsible for installing Cisco Catalyst IE3x00 Rugged Series switches. We assume that you are familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

This guide documents the hardware features of the Cisco Catalyst IE3x00 Rugged Switches. It describes the physical and performance characteristics of each switch, explains how to install a switch, and provides troubleshooting information.

Conventions

This document uses the following conventions and symbols for notes, cautions, and warnings.

Note Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.

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

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

The safety warnings for this product are translated into several languages in the *Regulatory Compliance and Safety Information for the Regulatory Compliance and Safety Information for the Cisco Catalyst IE3400 Heavy Duty Series Switches* that ships with the product. The EMC regulatory statements are also included in that guide.

Note: The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Related Publications

Before installing, configuring, or upgrading the switch, see the release notes on Cisco.com for the latest information.

These documents provide complete information about the switch and are available on Cisco.com:

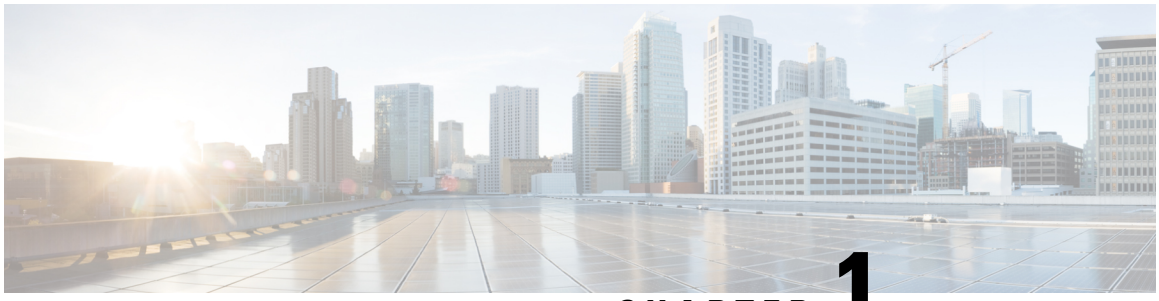
- *Regulatory Compliance and Safety Information for the Cisco IE 3X00 Switch*
- *Release Notes for the Cisco IE 3X00 Switch*
- *Cisco IE 3X00 Switch Software Configuration Guide*
- WebUI online help (available on the switch)

These compatibility matrix documents are available from this Cisco.com site:

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*

  (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*

  (not orderable but available on Cisco.com)



CHAPTER 1

Product Overview

Product Overview

The Cisco® Industrial Ethernet (IE) 3X00 Rugged Series Switch is the latest addition to our ruggedized switching platforms and provides superior high-bandwidth switching and proven Cisco IOS® Software-based routing capabilities for industrial environments. The Catalyst IE3x00 Rugged Series delivers highly secure access and industry-leading convergence using the Cisco Resilient Ethernet Protocol (REP) and is built to withstand extreme environments while adhering to overall IT network design, compliance, and performance requirements.

The Catalyst IE3x00 Rugged Series Switch is ideal for industrial Ethernet applications where hardened products are required, including factory automation, energy and process control, intelligent transportation systems (ITS), oil and gas field sites, city surveillance programs, and mining. With improved overall performance, greater bandwidth, a richer feature set, and enhanced hardware, the Cisco Catalyst IE3x00 Rugged Series Switch complements the current industrial Ethernet portfolio of related Cisco industrial switches.

The Cisco Catalyst IE3x00 Rugged Series Switch can easily be installed in your network. Through a user-friendly web Web UI, the Cisco Catalyst IE3x00 Rugged Series Switch provides easy out-of-the-box configuration and simplified operational manageability to deliver advanced security, data, video, and voice services over industrial networks.

Switch Models

	Default License Level[1]	Description
IE-3200-8T2S-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3200-8P2S-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 PoE/PoE+ ports, 2 fiber 100/1000 SFP-based ports; PoE power budget of 240W
IE-3300-8T2S-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE

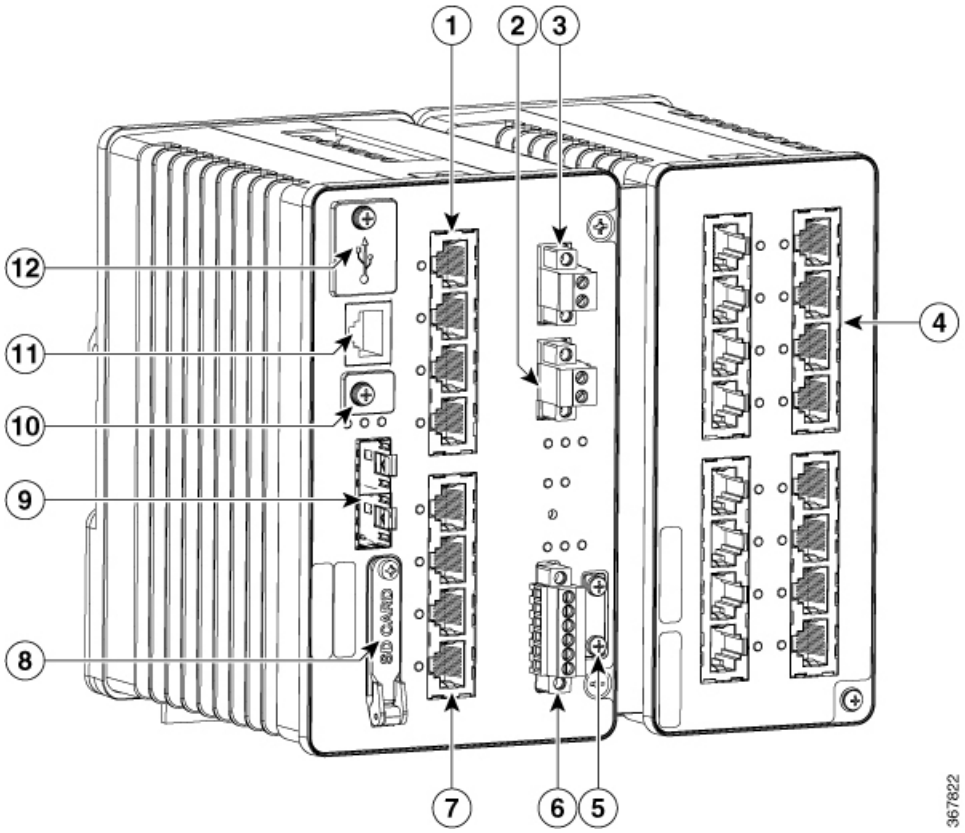
	Default License Level[1]	Description
IE-3300-8P2S-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 PoE/PoE+ ports, 2 fiber 100/1000 SFP-based ports; PoE power budget of 360W (including expansion module)
IE-3300-8T2S-A	Network Advantage	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3300-8P2S-A	Network Advantage	8 Gigabit Ethernet 10/100/1000 PoE/PoE+ ports, 2 fiber 100/1000 SFP-based ports; PoE power budget of 360W (including expansion module)
IE-3300-8T2X-A	Network Advantage	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 1/10 Gigabit Ethernet SFP-based ports, non-PoE
IE-3300-8T2X-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 1/10 Gigabit Ethernet SFP-based ports, non-PoE
IE-3300-8U2X-A	Network Advantage	8 GE Copper (4PPoE) & 2 10G SFP, Mod
IE-3300-8U2X-E	Network Essentials	8 GE Copper (4PPoE) & 2 10G SFP, Mod
IE-3400-8T2S-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3400-8T2S-A	Network Advantage	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3400-8P2S-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports with PoE
IE-3400-8P2S-A	Network Advantage	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports with PoE
IEM-3300-4MU=	N/A	Expansion Module with 4 2.5G Copper (4PPoE)

[1] See section *Licensing → Table: Permitted Combinations*, in this document for information about the add-on licenses that you can order.

Front Panel Overview

The illustrations in this section provide an overview of the variety of components available on the various switch models in this product family. Not all models are illustrated.

Figure 1: Cisco IE-3300-8T2S, and the IEM-3300-16T module shown



1	10/100/1000 Copper Ethernet ports (downlink ports)	7	10/100/1000 Copper Ethernet ports (downlink ports)
2	Power connector DC-B	8	Flash memory card slot
3	Power connector DC-A	9	SFP module slots (uplink ports)
4	10/100/1000 Copper Ethernet ports (downlink ports)	10	USB mini-Type B (console) port[2]
5	Protective ground connection	11	RJ-45 console port
6	Alarm connector	12	USB mini-Type A port[3]

[2] Use a screwdriver to remove the port cover and access the port.
[3] Use a screwdriver to remove the port cover and access the port.

Ports

Note: Different configurations are available. Not all ports or slots are present in all configurations.

1G SFP/ 10G SFP+ Ports (Uplinks)

Depending on the switch model, the uplink ports either support 1G/100M optics or 10G/1G optics. When using a 10G SFP, the port only operates at 1Gbps/10Gbps.

The IEEE 802.3u SFP module uplink slots provide full-duplex100/1000 Mb/s and 10Gb connectivity over multi-mode (MM) fiber cables or single-mode (SM) fiber cables. These ports use a SFP fiber-optic transceiver module that accepts a dual LC connector. Check the SFP specifications for the cable type and length.

For more information about SFP/SFP+ modules and cables, see SFP Module Connectors.

10/100/1000 BASE-T Downlink Ports

You can set the 10/100/1000 Base-T ports to operate in 10, 100 or 1000 Mb/s in full-duplex or half-duplex mode. You can also set these ports for speed and duplex autonegotiation in compliance with IEEE 802.3. (The default setting is autonegotiate.) When set for autonegotiation, the port senses the speed and duplex settings of the attached device and advertises its own capabilities. If the connected device also supports autonegotiation, the switch port negotiates the best connection (that is, the fastest line speed that both devices support, and full-duplex transmission if the attached device supports it) and configures itself accordingly. In all cases, the attached device must be within 328 feet (100 meters). 100BASE-TX traffic requires Category 5 cable. 10BASE-T traffic can use Category 3 or Category 4 cables.

You can use the **mdix auto** interface configuration command in the command-line interface (CLI) to enable the automatic medium-dependent interface crossover (auto-MDIX) feature. When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. For configuration information for this feature, see the switch software configuration guide or the switch command reference.

2500 BASE-T Downlink Ports

The 2500base-T ports operate in 100 Mb, 1000 Mb or 2500 Mb mode instead of 10,100, 1000. You can also set these ports for speed and duplex autonegotiation in compliance with IEEE 802.3. (The default setting is autonegotiate.) When set for autonegotiation, the port senses the speed and duplex settings of the attached device and advertises its own capabilities. If the connected device also supports autonegotiation, the switch port negotiates the best connection (that is, the fastest line speed that both devices support, and full-duplex transmission if the attached device supports it) and configures itself accordingly. In all cases, the attached device must be within 328 feet (100 meters). Multigig downlinks require Category 5e cables. 100BASE-TX traffic requires Category 5 cable. 10BASE-T traffic can use Category 3 or Category 4 cables.

You can use the **mdix auto** interface configuration command in the command-line interface (CLI) to enable the automatic medium-dependent interface crossover (auto-MDIX) feature. When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. For configuration information for this feature, see the switch software configuration guide or the switch command reference.

100/1000 Mb/s SFP Module Downlink Ports (on expansion modules only)

Expansion modules that support SFP interfaces support 100Mb and 1000Mb SFP speeds.

The 100/1000 Mb/s SFP module downlink slots provide full-duplex 100/1000 Mb/s connectivity over multi-mode (MM) fiber cables or single-mode (SM) fiber cables. These ports use a SFP fiber-optic transceiver module that accepts a dual LC connector. Check the SFP specifications for the cable type and length.

Management Ports

You can connect the switch to a PC running Microsoft Windows or to a terminal server through either the RJ-45 console port or the USB mini-Type B console port, also referred to as the USB-mini console port. These ports use the following connectors:

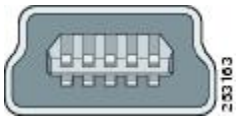
- RJ-45 console port uses an RJ-45-to-DB-9 female cable.
- USB-mini console port (5-pin connector) uses a USB Type A-to-5-pin mini-Type B cable.

The USB-mini console interface speeds are the same as the RJ-45 console interface speeds.

To use the USB-mini console port, you must install the Windows USB device driver on the device that is connected to the USB-mini console port and that is running Microsoft Windows.

With the Windows USB device driver, connecting and disconnecting the USB cable from the console port does not affect Windows HyperTerminal operations. Mac OS X or Linux require no special drivers.

Figure 2: USB Mini-Type B Port



The configurable inactivity timeout reactivates the RJ-45 console port if the USB-mini console port is activated, but no input activity occurs for a specified time period. When the USB-mini console port deactivates due to a timeout, you can restore its operation by disconnecting and reconnecting the USB cable. For information on using the CLI to configure the USB-mini console interface, see the switch software guide.

Power Connectors

DC Power Connector

You connect the DC power to the switch through the front panel connectors. The switch has a dual-feed DC power supply; two connectors provide primary and secondary DC power (DC-A and DC-B). The DC power connectors are near the top right of the Front Panel Overview, on page 2 on page 2 . Each power connector has an LED status indicator.

The switch power connectors are attached to the switch chassis. Each power connector has screw terminals for terminating the DC power. All connectors are attached to the switch front panel with the provided captive screws.

The power connector labeling is on the panel. The positive DC power connection is labeled “+” , and the return connection is labeled “–” .

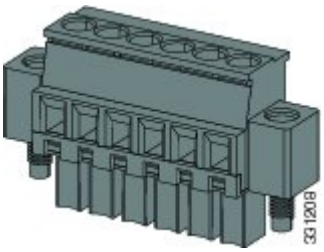
The switch can operate with a single power source or with dual power sources. When both power sources are operational, the switch draws power from the DC source with the higher voltage. If one of the two power sources fail, the other continues to power the switch.

Alarm Connector

You connect the alarm signals to the switch through the alarm connector. The switch supports two alarm inputs and one alarm output relay. The alarm connector is on the bottom right of the front panel. See Front Panel Overview, on page 2.

The alarm connector provides six alarm wire connections. The connector is attached to the switch front panel with the provided captive screws.

Figure 3: Alarm Connector



Both alarm input circuits can sense if the alarm input is open or closed. The alarm inputs can be activated for environmental, power supply, and port status alarm conditions. From the CLI, you can configure each alarm input as an open or closed contact.

The alarm output circuit is a relay with a normally open and a normally closed contact. The switch is configured to detect faults that are used to energize the relay coil and change the state on both of the relay contacts: normally open contacts close, and normally closed contacts open. The alarm output relay can be used to control an external alarm device, such as a bell or a light.

See the switch software configuration guide for instructions on configuring the alarm relays.

SFP Modules Supported

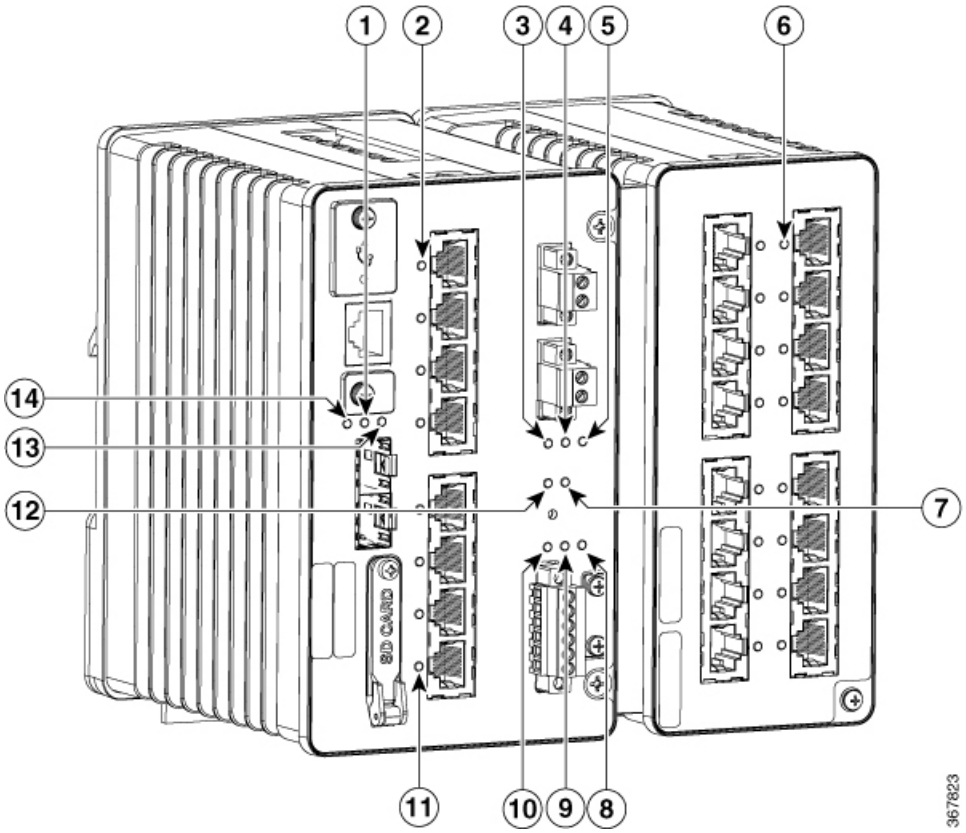
The SFP modules are switch Ethernet SFP modules that provide connections to other devices. Depending on the switch model, these field-replaceable transceiver modules provide uplink or downlink interfaces. The modules have LC connectors for fiber-optic connections.

Refer to the **Cisco Optics-to-Device Compatibility Matrix** for details about the supported SFP Modules.

LEDs

You can use the LEDs to monitor the switch status, activity, and performance.

Figure 4: LEDs on the Cisco Catalyst IE3x00 Rugged Switch



1	SFP uplink 2 LED	8	Alarm Output LED
2	10/100/1000 Copper Ethernet Downlink Port LEDs on Base Chassis Ports 3-6	9	Alarm Input LED 2
3	DC Input A Status LED	10	Alarm Input LED 1
4	DC Input B Status LED	11	10/100/1000 Copper Ethernet Downlink Port LEDs on Base Chassis Ports 7-10
5	POE Operation LED (POE enabled versions)	12	Express Setup LED and Button

6	10/100/1000 Copper Ethernet Downlink Port LEDs on Expansion Module (If applicable)	13	Console LED
7	Operational Status LED	14	SFP Uplink 1 LED

Express Setup LED

The Express Setup LED displays the express setup mode for the initial configuration.

Color	Setup Status
Off (dark)	Switch is configured as a managed switch.
Solid green	Switch is operating normally.
Blinking green	Switch is in initial setup, in recovery, or initial setup is incomplete.
Solid red	Switch failed to start initial setup or recovery because there is no available switch port to which to connect the management station. Disconnect a device from a switch port, and then press the Express Setup button.

System LED

The System LED shows whether the system is receiving power and is functioning properly.

Color	System Status
Off	System is not powered on.
Blinking green	Boot is in progress.
Green	System is operating normally.
Red	Switch is not functioning properly.

USB-Mini Console LED

The USB-mini console LED shows which console port is in use. See LEDs, on page 6 for the LED location. If you connect a cable to a console port, the switch automatically uses that port for console communication. If you connect two console cables, the USB-mini console port has priority.

Color	Description
Green	USB-mini console port is active. RJ-45 console port LED is not active.
Off	Port is not active. RJ-45 console port is active.

Alarm LEDs

Alarm OUT

Alarm Output LED is set based on severity of input/facility Alarm

Color	System Status
Off	Alarm OUT is not configured, or the switch is off.
Green	Alarm OUT is configured, no Alarm detected or Input Alarm detected with severity NONE.
Blinking red	Input/Facility Alarm detected with severity Major.
Red	Input/Facility Alarm detected with severity Minor.

Alarm IN1 and IN2

Color	System Status
Off	Alarm IN1 or IN2 not configured.
Green	Alarm IN1 or IN2 configured, no alarm detected.
Blinking red	Major alarm detected.
Red	Minor alarm detected.

Power Status LEDs

The switch can operate with one or two DC power sources. Each DC input has an associated LED that shows the status of the corresponding DC input. If power is present on the circuit, the LED is green. If power is not present, the LED color depends on the alarm configuration. If alarms are configured, the LED is red when power is not present; otherwise, the LED is off.

If the switch has dual power sources, the switch draws power from the power source with the higher voltage. If one of the DC sources fails, the alternate DC source powers the switch, and the corresponding power status LED is green. The power status for the failed DC source is either off or red, depending on the alarm configuration.

Color	System Status
Green	Power is present on the associated circuit, system is operating normally.
Off	Power is not present on the circuit, or the system is not powered up.
Red	Power is not present on the associated circuit, and the power supply alarm is configured.

The Power A and Power B LEDs show that power is not present on the switch if the power input drops below the low valid level. The power status LEDs only show that power is present if the voltage at the switch input exceeds the valid level.

For information about the power LED colors during the boot fast sequence, see Verifying Switch Operation, on page 42.

Port Status LEDs

Each port and SFP uplink slot has a status LED, as shown in LEDs, on page 6 and described below.

Color	System Status
Off	No link.
Solid green	Link present.
Blinking green	Activity. Port is sending or receiving data.
Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
Solid amber	Port is not forwarding. The port was disabled by management, an address violation, or STP. After a port is reconfigured, the port LED can remain amber for up to 30 seconds while STP checks the switch for possible loops.

PoE Status LED

The PoE STATUS LEDs are located on the front panel, next to the PoE ports (models equipped with PoE ports).The LEDs display the functionality and status of the adjacent PoE ports.

Color	PoE Status
Off	PoE is off. If the powered device is receiving power from a non-PoE power source, the port LED is off even if the powered device is connected to the switch port.
Green	PoE is on. The port LED is green only when the PoE port is providing power.
Alternating green and amber	PoE is denied because providing power to the powered device will exceed the switch power capacity.

Color	PoE Status
Flashing amber	PoE is off due to a fault. **Caution** Non-compliant cabling or powered devices can cause a PoE port fault. Use only standard-compliant cabling to connect Cisco pre-standard IP Phones and wireless access points or IEEE 802.3af/at/bt-compliant devices. You must remove any cable or device that causes a PoE fault.
Amber	PoE for the port is disabled. (PoE is enabled by default.)

Flash Memory Card

The switch supports a flash memory card that makes it possible to replace a failed switch without reconfiguring the new switch. The slot for the flash memory card is on the front of the switch. A cover protects the flash card and holds the card firmly in place. The cover is hinged and closed with a captive screw. This prevents the card from coming loose and protects against shock and vibration.

Note: For more information on inserting and removing the flash memory card, see Installing or Removing the Flash Memory Card (Optional), on page 19.

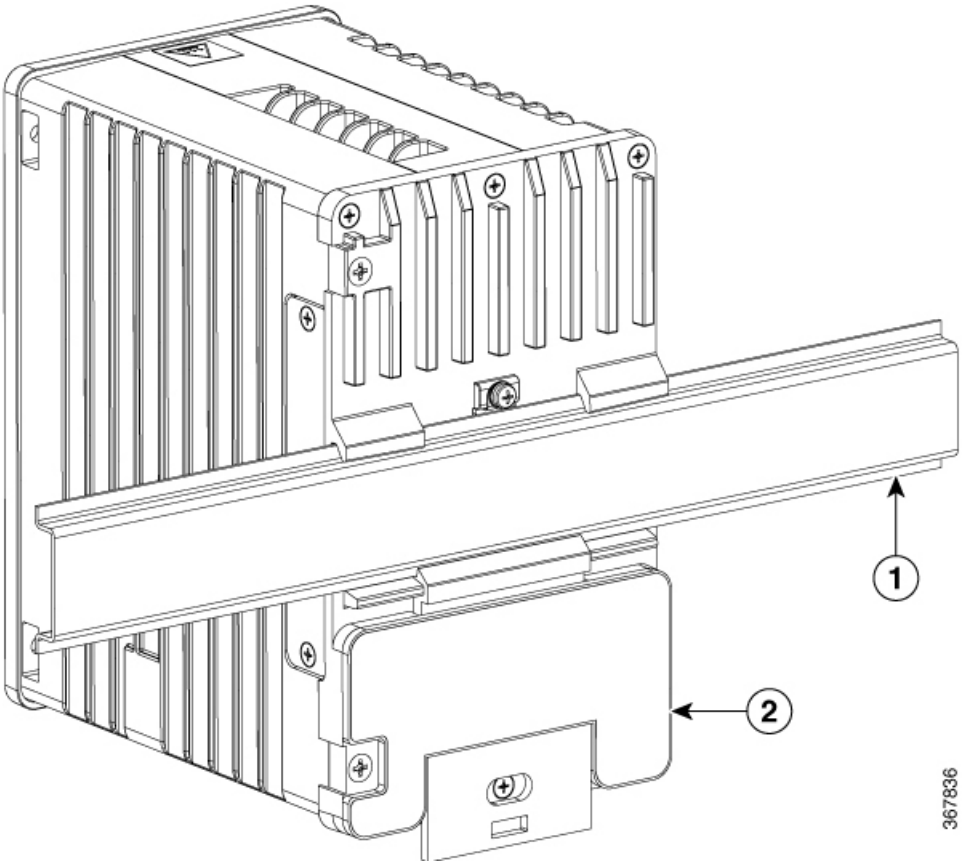
Note: The replacement SD card part number is SD-IE-4GB.

Rear Panel

The rear panel of the switch has a latch for installation on a DIN rail. The latch is spring-loaded to move down to position the switch over a DIN rail and return to the original position to secure the switch to a DIN rail.

Note The switch should only be installed in the vertical orientation shown in this document.

Figure 5: Cisco Catalyst IE3x00 Rugged Switch Rear Panel



Management Options

The switch supports these management options:

- Web UI

  You can use Web UI, which is in the switch memory, to manage individual and standalone switches. This web interface offers quick configuration and monitoring. You can access Web UI from anywhere in your network through a web browser. For more information, see the Web UI online help.
- Cisco IOS CLI

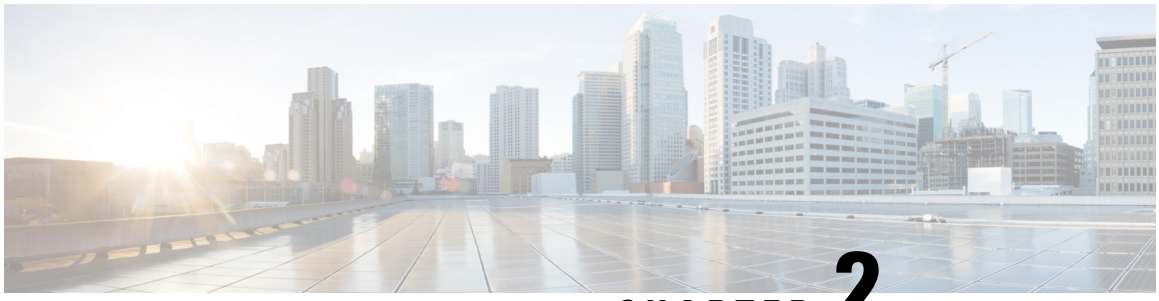
  The switch CLI is based on Cisco IOS software and is enhanced to support desktop-switching features. You can fully configure and monitor the switch. You can access the CLI either by connecting your management station directly to the switch management port, or a console port, or by using Telnet from a remote management station. See the switch command reference on Cisco.com for more information.
- SNMP network management

  You can manage switches from a SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager. The switch supports a comprehensive set of Management Information Base (MIB) extensions and four Remote Monitoring (RMON) groups. See the switch software configuration guide on Cisco.com and the documentation that came with your SNMP application for more information.

- Common Industrial Protocol

  The Common Industrial Protocol (CIP) management objects are supported. The Cisco IE 3X00 can be managed by CIP-based management tools, allowing the user to manage an entire industrial automation system with one tool.
- TIA Portal
  - TCP/IP and RT

    This switch supports PROFINET TCP/IP and RT and can be managed by Siemens' automation software such as STEP 7 and TIA Portal.



CHAPTER 2

Switch Installation

Switch Installation

This chapter describes how to install your switch, verify the boot fast, and connect the switch to other devices. It also includes information specifically for installations in hazardous environments.

Note Please refer to the Product Documentation of Compliance for certified installation procedures in Hazardous Locations.

Read these topics, and perform the procedures in this order:

Preparing for Installation

This section provides information about these topics:

Warnings

These warnings are translated into several languages in the Regulatory Compliance and Safety Information for this switch.

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals. Statement 43

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity. Statement 1001

Warning Before performing any of the following procedures, ensure that power is removed from the DCcircuit. Statement 1003

Warning Read the installation instructions before you connect the system to its power source. Statement 1004

Warning This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security. Statement1017

Warning This equipment is supplied as “open type” equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The interior of the enclosure must be accessible only by the use of a tool.

The enclosure must meet IP 54 or NEMA type 4 minimum enclosure rating standards. Statement 1063

Warning This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024

Warning This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028

Warning Only trained and qualified personnel should be allowed to install, replace, or service thisequipment. Statement 1030

Warning Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040

Warning For connections outside the building where the equipment is installed, the following ports must be connected through an approved network termination unit with integral circuit protection. 10/100/1000 Ethernet Statement 1044

Warning To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature, 60C/140F. Statement 1047

Warning Installation of the equipment must comply with local and national electrical codes. Statement 1074

Caution Airflow around the switch must be unrestricted. To prevent the switch from overheating, there must be the following

minimum clearances:

- Top and bottom: 2.0 in. (50.8 mm)
- Sides: 2.0 in. (50.8 mm)
- Front: 2.0 in. (50.8 mm)

Installation Guidelines

When determining where to place the switch, observe these guidelines.

Note The switch should only be installed in the vertical orientation shown in this document.

Environment and Enclosure Guidelines

Review these environmental and enclosure guidelines before installation:

- This equipment is intended for use in a Pollution Degree 2 industrial environment, in overvoltage Category II applications (as defined in IEC publication 60664-1), at altitudes up to 9842 ft (3 km) without derating.
- This equipment is considered Group 1, Class A industrial equipment, according to IEC/CISPR Publication 11. Without appropriate precautions, there may be potential difficulties ensuring electromagnetic compatibility in other environments due to conducted as well as radiated disturbance.
- This equipment is supplied as open-type equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The enclosure must have suitable flame-retardant properties to prevent or minimize the spread of flame, complying with a flame-spread rating of 5VA, V2, V1, V0 (or equivalent) if nonmetallic. The interior of the enclosure must be accessible only by the use of a tool. Subsequent sections of this publication might contain additional information regarding specific enclosure-type ratings that are required to comply with certain product safety certifications.

General Guidelines

Before installation, observe these general guidelines:

Caution Proper ESD protection is required whenever you handle Cisco equipment. Installation and maintenance personnel should be properly grounded by using ground straps to eliminate the risk of ESD damage to the switch.

Do not touch connectors or pins on component boards. Do not touch circuit components inside the switch. When not in use, store the equipment in appropriate static-safe packaging.

- The switch meets the voltage dips and interruptions requirements of IEC 61850-3 only when powered by a redundant power supply configuration.
- If you are responsible for the application of safety-related programmable electronic systems (PES), you need to be aware of the safety requirements in the application of the system and be trained in using the system.
- For better EMC performance, it is suggested to use S/UTP or SF/UTP cables for copper Ethernet ports. Refer ISO/IEC11801 standard for details on S/UTP and SF/UTP.

Caution THE DEVICE IS DESIGNED TO MOUNT ON A DIN RAIL THAT CONFORMS TO STANDARD IEC/EN60715, TOP HAT RAILS TH 35-7.5 OR TH 35-15.

Note In order to prevent excessive side to side movement of the unit it is advised to install DIN rail stop plates such as mouser part numbers 653-PFP-M, 651-1201662 or 845-CA402. These end stops can be installed on one or both sides or the unit to limit excessive side to side movement that typically occurs in high vibration environments.

When determining where to place the switch, observe these guidelines:

- Before installing the switch, first verify that the switch is operational by powering it on and observing boot fast. Follow the procedures in the Verifying Switch Operation, on page 42.
- For 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).
- Clearance to front and rear panels meets these conditions:
  - Front-panel LEDs can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Front-panel direct current (DC) power connectors and the alarm connector are within reach of the connection to the DC power source.
- Airflow around the switch must be unrestricted. To prevent the switch from overheating, you must have the following minimum clearances:
  - Top and bottom: 2.0 in. (50.8 mm)
  - Sides: 2.0 in. (50.8 mm)
  - Front: 2.0 in. (50.8 mm)

Caution When the switch is installed in an industrial enclosure, the temperature within the enclosure is greater than normal room temperature outside the enclosure.

Ensure temperatures inside the enclosure conform to device specifications detailed in the Data Sheet.

- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.

Installing or Removing the Flash Memory Card (Optional)

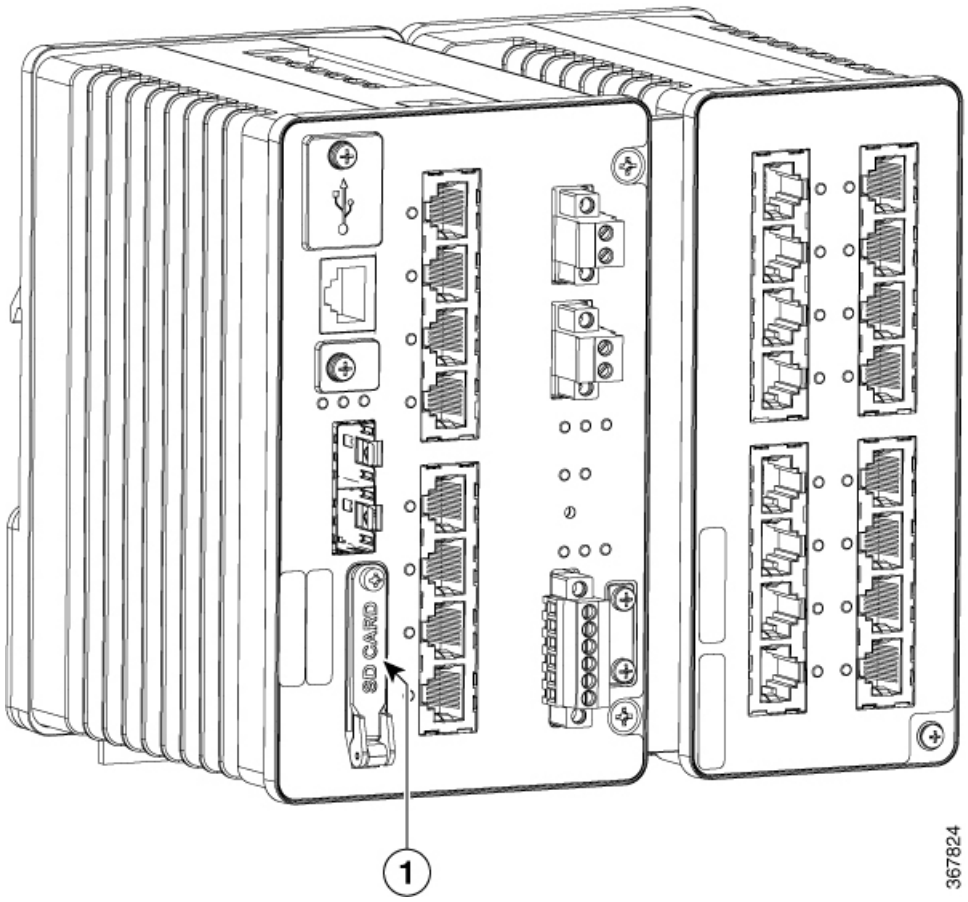
Optionally, you can execute the sync command to copy Flash to SDFlash: and make SDFlash: the primary storage, then remove the SD card.

It is strongly recommended that you use the SD card to boot or store the config for future easy replacement, in case of a hardware failure.

To install or replace the flash memory card, follow these steps:

1. On the front of the switch, locate the door that protects the flash memory card slot. Loosen the captive screw at the top of the door using a Phillips screwdriver to open the door.

Figure 6: Installing the Flash Memory Card in the Switch



2. Install or remove the card:
   a. To install a card, slide it into the slot, and press it in until it clicks in place. The card is keyed so that you cannot insert it the wrong way.
   b. To remove the card, push it in until it releases for it to pop out. Place it in an antistatic bag to protect it from static discharge.
3. After the card is installed, close the guard door and fasten the captive screw using a Phillips screwdriver to keep the door in place.

Connecting to a Console Port (Optional)

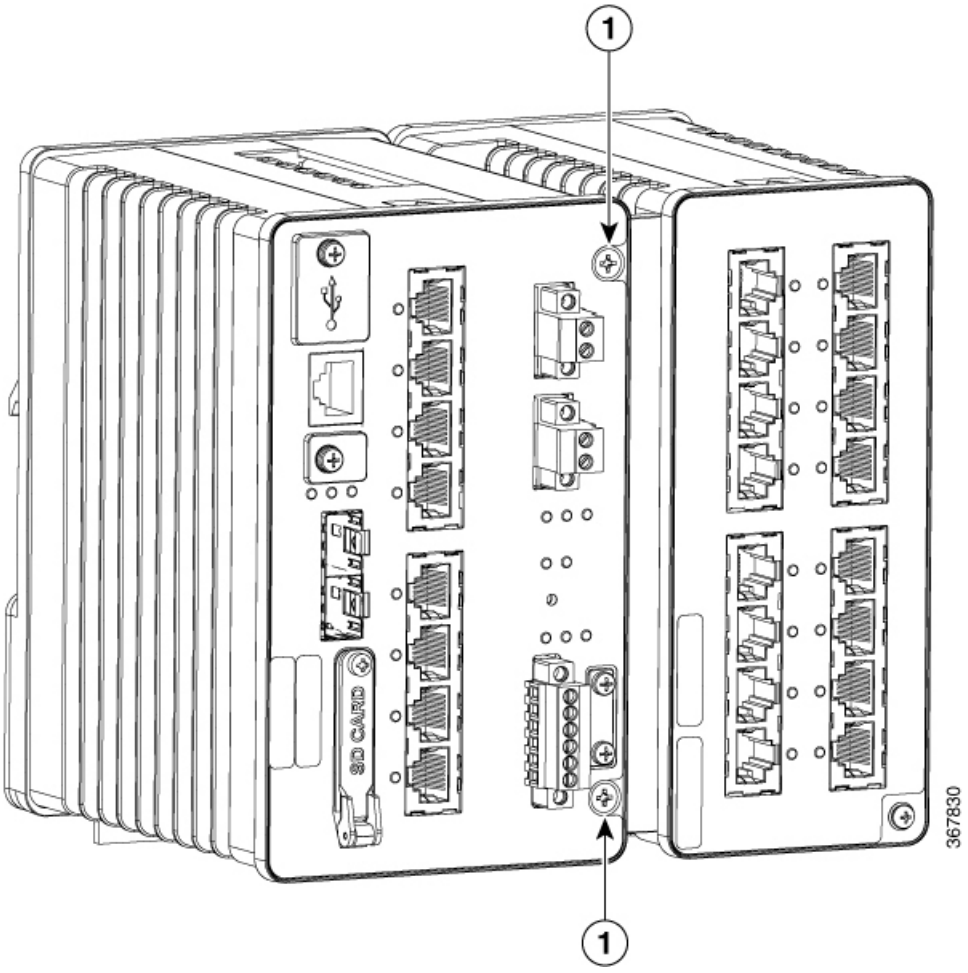
You can also enter CLI commands through the console port. For more information about this process see Accessing the CLI Through the Console Port.

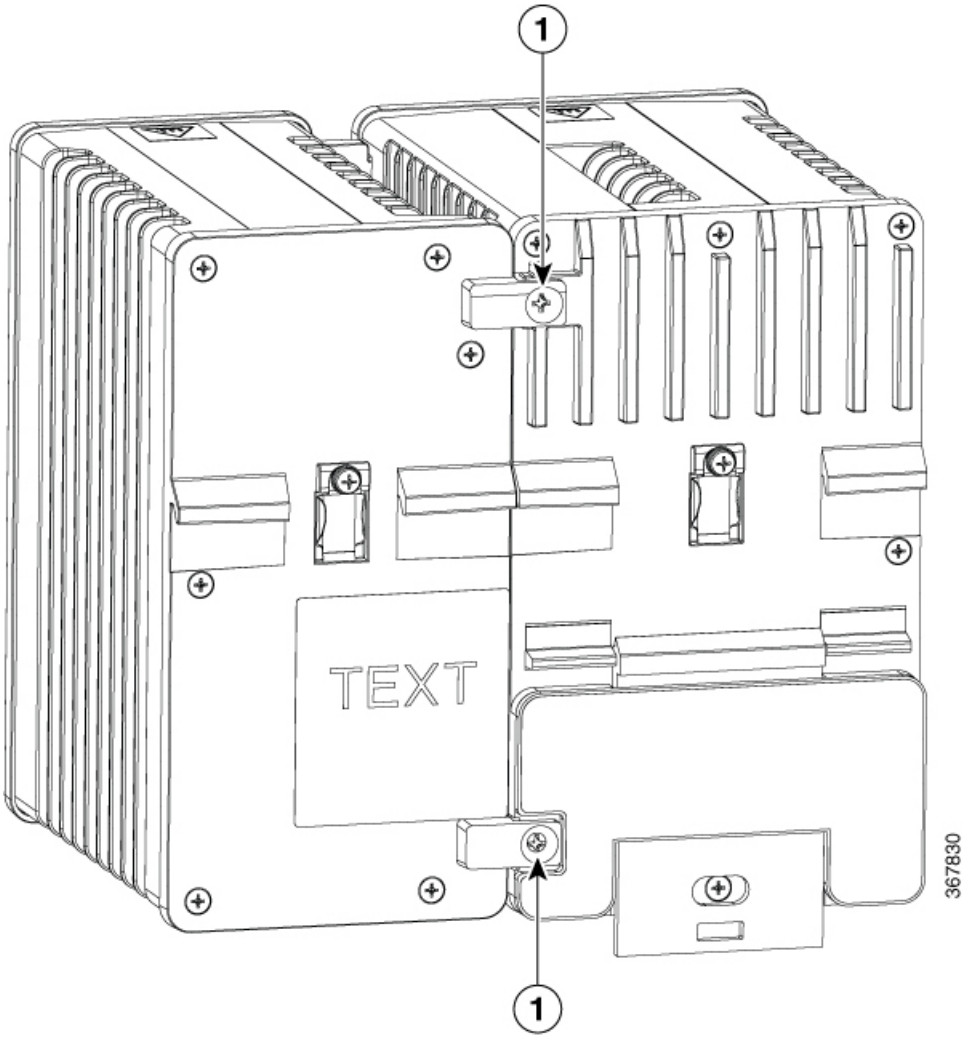
Attaching an Expansion Module (Optional)

If you're installation calls for use of one of the expansion modules listed in Switch Models, use the following procedure to attach the module to the switch:

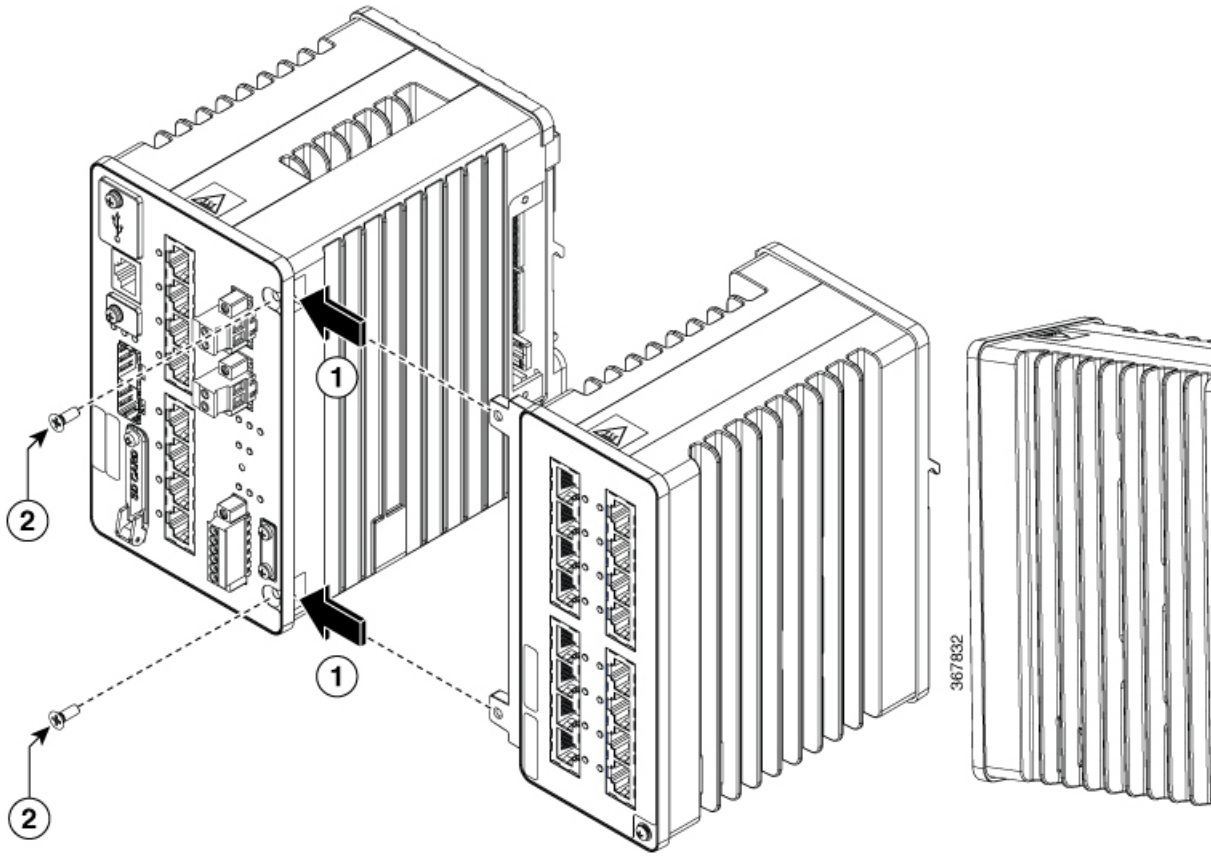
Danger Do not attach any expansion module to a switch while the switch is energized.

1. Remove the 2 screws securing the side cover plate to the switch.
2. Remove the two screws from the front of the Expansion chassis, and the two screws from the rear of the base.


1
SD CARD
367830
1



3. Align tabs on top and bottom left front of expansion module with slots on top and bottom right side of switch along with tabs on top and bottom left rear of module and holes at top and bottom right rear of switch, and press module and switch together so that theelectrical connections engage and the screw holes



4. Secure the 4 flathead phillips screws with 5-6 in-lbs torque

Connecting to Power

Tools and Equipment

Obtain these necessary tools and equipment:

- Ratcheting torque flathead screwdriver that exerts up to 18 in-lb (2.03 N-m) of pressure.
- For the protective ground connector, obtain a single or pair of stu size 6 ring terminals (such as Hollingsworth part number R3456B or equivalent).
- Crimping tool (such as Thomas & Bett part number WT4000, ERG-2001, or equivalent).
- 10-gauge copper ground wire.
- For DC power connections, use UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.
- Wire-stripping tools for stripping 10- and 14-gauge wires.
- A number-2 Phillips screwdriver.
- A flat-blade screwdriver.

Supported Power Supplies

Cisco is constantly updating the IoT Power Supply portfolio. Please refer to the Cisco Catalyst IE3x00 Rugged Switch Data Sheet for a comprehensive list of supported power supplies and their capabilities.

Installing the Power Converter on a DIN Rail, Wall, or Rack Adapter

You install the power converter on a DIN rail, wall, or rack as you would a switch module.

Warning This equipment is supplied as “open type” equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The interior of the enclosure must be accessible only by the use of a tool.

The enclosure must meet IP 54 or NEMA type 4 minimum enclosure rating standards. Statement 1063

Caution To prevent the switch assemble from overheating, there must be sufficient spacings as explained under Installation Guidelines, between any other switch assembly.

Grounding the Switch

Make sure to follow any grounding requirements at your site.

Warning This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024

Warning When installing or replacing the unit, the ground connection must always be made first and disconnected last. Statement 1046

Warning This equipment is intended to be grounded to comply with emission and immunity requirements. Ensure that the switch functional ground lug is connected to earth ground during normal use. Statement 1064

Caution To make sure that the equipment is reliably connected to earth ground, follow the grounding procedure instructions, and use a UL-listed ring terminal lug suitable for number 10 AWG wire, such as Hollingsworth part number R3456B or equivalent)

Note Use at least an 10 AWG (5.26 mm2) conductor to connect to the external grounding screw.

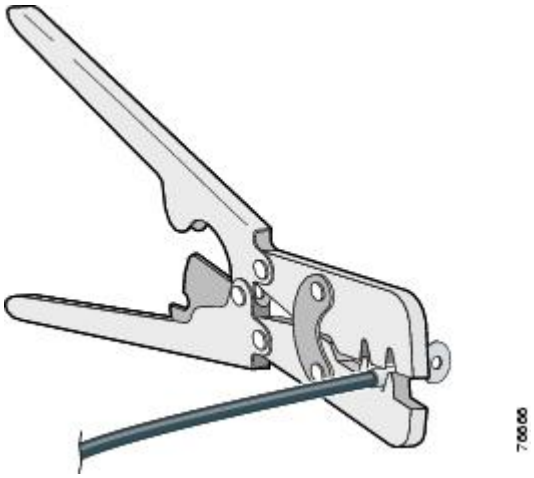
The ground lug is not supplied with the switch. You can use one of the these options:

- Single ring terminal
- Two single ring terminals

To ground the switch to earth ground by using the ground screw, follow these steps:

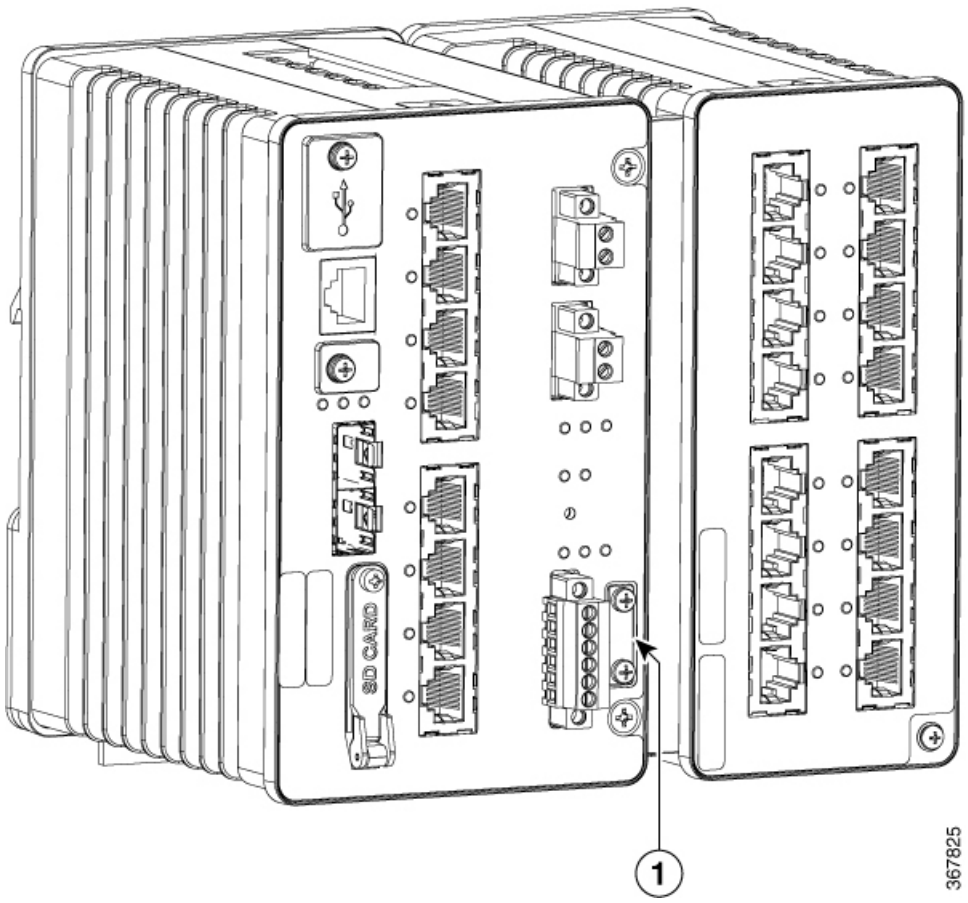
1. Use a standard Phillips screwdriver or a ratcheting torque screwdriver with a Phillips head to remove the ground screw from the front panel of the switch. Store the ground screw for later use.
2. Use the manufacturer's guidelines to determine the wire length to be stripped.
3. Insert the ground wire into the ring terminal lug, and using a crimping tool, crimp the terminal to the wire. If two ring terminals are being used, repeat this action for a second ring terminal.

Figure 7: Crimping the Ring Terminal



4. Slide the ground screw through the terminal.
5. Insert the ground screw into the functional ground screw opening on the front panel.
6. Use a ratcheting torque screwdriver to tighten the ground screws and ring terminal to the switch front panel. The torque should not exceed 4.5 in-lb (0.51 N-m).

Figure 8: Ground-Lug Screw



7. Attach the other end of the ground wire to a grounded bare metal surface, such as a ground bus, a grounded DIN rail, or a grounded bare rack.

Caution The expansion module must be grounded separately. Note that this is an EMC ground not a safety ground, unlike the one on the main chassis.

Connecting the Power Converter to an AC Power Source

These sections describe the steps required to connect the power converter to an AC power source:

Preparing the AC Power Connection

To connect the power converter to an AC power source, you need an AC power cord. Power cord connector types and standards vary by country. Power-cord wiring color codes also vary by country. You must to have a qualified electrician select, prepare, and install the appropriate power cord to the power supply.

Note Use copper conductors only, rated at a minimum temperature of 167°F (75°C).

Note This section does not apply to PWR-IE50W-AC-IEC, which has pluggable IEC connector.

Connecting the AC Power Source to the Power Converter

Caution AC power sources must be dedicated AC branch circuits. Each branch circuit must be protected by a dedicated two-pole circuit breaker.

Note Do not turn on AC power until the wiring is secured.

1. Remove the plastic cover from the input power terminals and set it aside.
2. Insert the exposed ground wire lead (10-to-12 AWG cable) into the power converter ground wire connection. Ensure that only wire *with insulation* extends from the connector. Note that the position of the power converter may vary on different switch models.
3. Tighten the ground wire terminal block screw.

Note Torque to 10 in-lb (1.13Nm).

4. Insert the line and neutral wire leads into the terminal block line and neutral connections. Make sure that you cannot see any wire lead. Ensure that only wire *with insulation* extends from the connectors.
5. Tighten the line and neutral terminal block screws.

Note Torque to 10 in-lb (1.13Nm).

6. Replace the plastic cover over the terminal block.
7. Connect the other end of the wiring to your AC power source.

Connecting the Power Converter to a DC Power Source

You can also connect the power converter to a DC power source. Several power supplies can be used. Refer to the data sheet for the appropriate DC input ratings.

Note Use copper conductors only, rated at a minimum temperature of 167°F (75°C).

1. Measure a single length of stranded copper wire long enough to connect the power converter to the earth ground. The wire color might differ depending on the country that you are using it in.

For connections from the power converter to earth ground, use shielded 14-AWG stranded copper wire.

2. Measure a length of twisted-pair copper wire long enough to connect the power converter to the DC power source.

   For DC connections from the power converter to the DC source, use 10-AWG twisted-pair copper wire.

3. Using a wire-stripping tool, strip the ground wire and both ends of the twisted pair wires to 0.25 inch (6.3 mm) ± 0.02 inch (0.5 mm). Do not strip more than 0.27 inch (6.8 mm) of insulation from the wires. Stripping more than the recommended amount of wire can leave exposed wire from the power and relay connector after installation.
4. Connect one end of the stranded copper wire to a grounded bare metal surface, such as a ground bus, a grounded DIN rail, or a grounded bare rack.
5. Insert the other end of the exposed ground wire lead into the earth-ground wire connection on the power converter terminal block. Note that the position of the power converter may vary on different switch models.
6. Tighten the earth-ground wire connection terminal block screw.

Note Torque to 8 in.-lb, not to exceed 10 in-lb.

Warning An exposed wire lead from a DC-input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC-input power source wire extends from the power and relay connector. Statement 122

7. Insert the twisted-pair wire leads into the terminal block line and neutral connections. Insert the wire lead into the neutral wire connection and the wire\ lead into the line wire connection. Ensure that only wire *with insulation* extends from the connectors.
8. Tighten the line and neutral terminal block screws.

Note Torque to 8 in.-lb, not to exceed 10 in-lb.

9. Connect the red wire to the positive pole of the DC power source, and connect the black wire to the return pole. Ensure that each pole has a current-limiting-type fuse rated to 30 Amp.

Wiring the DC Power Source

Read these cautions and warnings before wiring the switch the DC power source.

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 15A. Statement 1005**

Warning **Before performing any of the following procedures, ensure that power is removed from the DCcircuit. Statement 1003**

Warning **A readily accessible two-poled disconnect device must be incorporated in the fixed wiring. Statement 1022**

Warning **Warning: Only trained and qualified personnel should be allowed to install, replace, or service thisequipment. Statement 1030**

Warning **Warning: Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC60950 based safety standards. Statement 1033**

Warning **Installation of the equipment must comply with local and national electrical codes. Statement 1074**

Caution **PoE output power is not isolated from the switch's power input. Connecting PoE ports between two IE3x00 systems may create a power loop. The energy from an external surge can pass through the switch and among the PoE ports.**

Caution **If an internal fault occurs, switches with PoE-capable Ethernet ports may apply PoE power to a port even when it is not connected to a PoE powered device.**

You must use appropriate protection to ensure that such events do not create a hazard.

Caution **On switches that support PoE, do not connect any terminal of the DC power source to earth ground.**

Caution **For wire connections to the power and alarm connectors, you must use UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.**

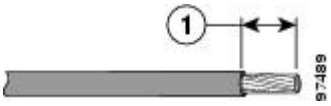
To wire the switch to a DC power source, follow these steps:

1. Locate the two power connectors on the switch front panel labeled DC-A and DC-B.
2. Identify the connector positive and return DC power connections. The labels for power connectors DC-A and DC-B are on the switch panel as displayed below.

Label	Connection
+	Positive DC power connection
–	Return DC power connection

3. Measure two strands of twisted-pair copper wire (14 AWG) long enough to connect to the DC power source.
4. Using a wire-stripping tool, strip each of the two twisted pair wires coming from each DC-input power source to 0.25 inch (6.3 mm) ± 0.02 inch (0.5 mm). Do not strip more than 0.27 inch (6.8 mm) of insulation from the wire. Stripping more than the recommended amount of wire can leave exposed wire from the power connector after installation.

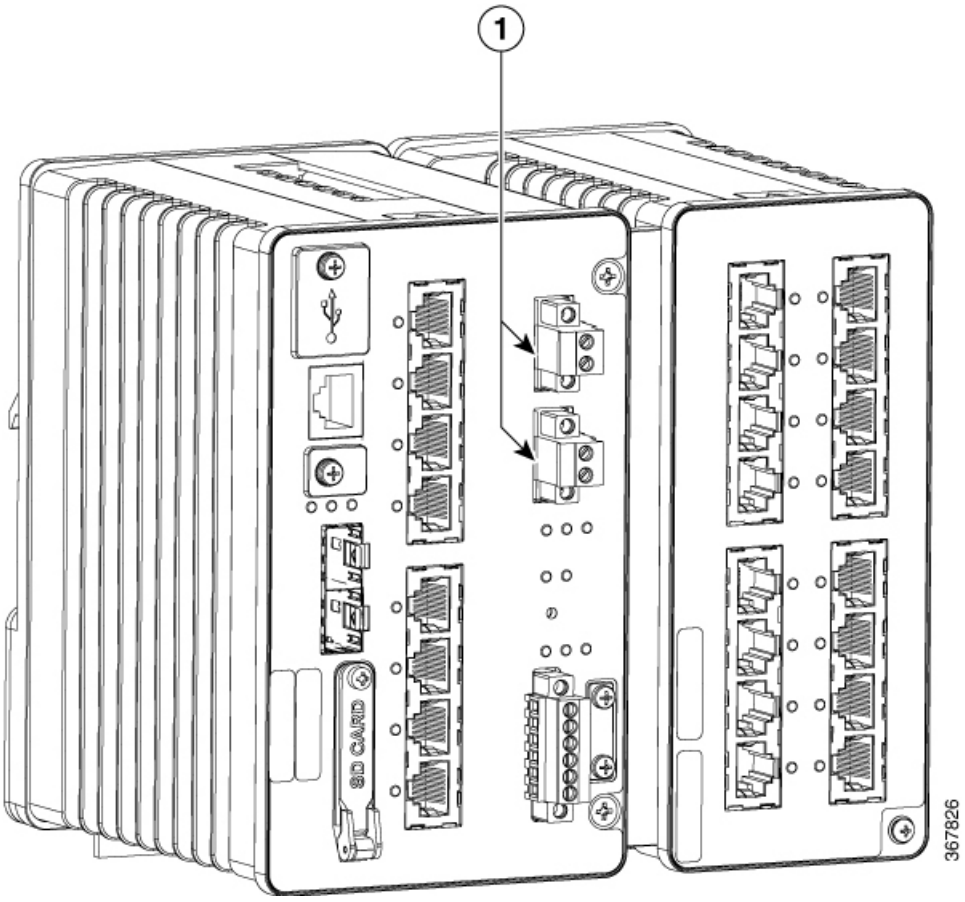
Figure 9: Stripping the Power Connection Wire



1	0.25 in. (6.3 mm) ± 0.02 in. (0.5 mm)

5. Remove the two captive screws that attach the power connector to the switch, and remove the power connector. Remove both connectors if you are connecting to two power sources.

Figure 10: Removing the Power Connectors from the Switch



1	Power Connectors

6. On the power connector, insert the exposed part of the positive wire into the connection labeled "+" and the exposed part of the return wire into the connection labeled "–". Make sure that you cannot see any wire lead. Only wire *with insulation* should extend from the connector.

Warning An exposed wire lead from a DC-input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC-input power source wire extends from the connector(s) or terminal block(s). Statement 122

7. Use a ratcheting torque flathead screwdriver to torque the power connector captive screws (above the installed wire leads) to 5in-lb (0.565 Nm).

Caution Do not over-torque the power connector's captive screws. The torque should not exceed 5in-lb (0.565 Nm).

8. Connect the other end of the positive wire to the positive terminal on the DC power source, and connect the other end of the return wire to the return terminal on the DC power source.

When you are testing the switch, one power connection is sufficient. If you are installing the switch and are using a second power source, repeat Step 4 through Step 8 using the second power connector.

Attaching the Power Connectors to the Switch

To attach the power connectors to the front panel of the switch, follow these steps:

1. Insert one power connector into the DC-A receptacle on the switch front panel, and the other into the DC-B receptacle.

Warning Failure to securely tighten the captive screws can result in an electrical arc if the connector is accidentally removed. Statement 397

Warning Use twisted-pair supply wires suitable for 86°F (30°C) above surrounding ambient temperature outside the enclosure. Statement 1067

Warning Installation of the equipment must comply with local and national electrical codes. Statement 1074

2. Use a ratcheting torque flathead screwdriver to tighten the captive screws on the sides of the power connectors.

   When you are testing the switch, one power source is sufficient. If you are installing the switch and are using a second power source, repeat this procedure for the second power connector (DC-B), which installs just below the primary power connector (DC-A).

   When you are installing the switch, secure the wires coming from the power connector so that they cannot be disturbed by casual contact. For example, use tie wraps to secure the wires to the rack.

Applying Power to the Power Converter

Move the circuit breaker for the AC outlet or the DC control circuit to the *on* position.

The LED on the power converter front panel is green when the unit is operating normally. The LED is off when the unit is not powered or is not operating normally. After the power is connected, the switch automatically begins the power-on self- test (POST), a series of tests that verifies that the switch functions properly.

Installing the Switch

This section describes how to install the switch:

Warning This equipment is supplied as “open type” equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The interior of the enclosure must be accessible only by the use of a tool.

The enclosure must meet IP 54 or NEMA type 4 minimum enclosure rating standards. Statement 1063

Caution To prevent the switch from overheating, ensure these minimum clearances:

- Top and bottom: 2.0 in. (50.8 mm)
- Exposed side (not connected to the module): 2.0 in. (50.8 mm)
- Front: 2.0 in. (50.8 mm)

Installing the Switch on a DIN Rail

The switch ships with a spring-loaded latch on the rear panel for a mounting on a DIN rail.

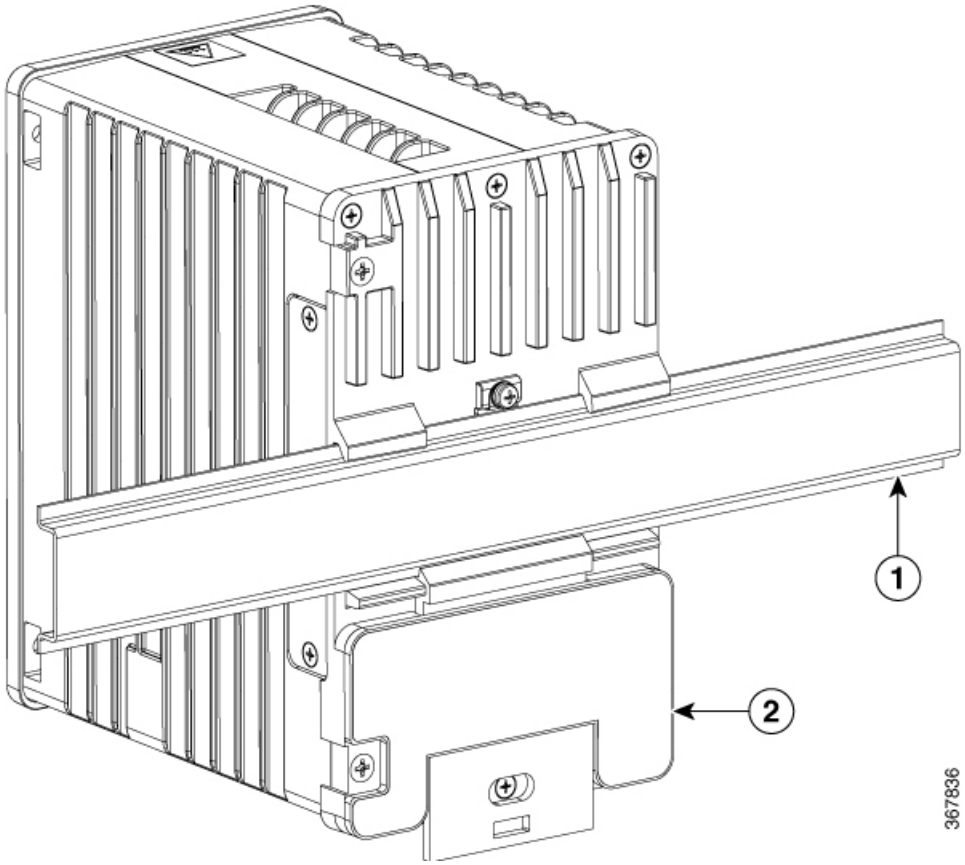
You can install the switch as a standalone device on the DIN rail or with the expansion modules already connected. You must connect expansion modules to the switch before installing the switch on the DIN rail.

To attach the switch to a DIN rail, follow these steps:

1. Position the rear panel of the switch directly in front of the DIN rail, making sure that the DIN rail fits in the space between the two hooks near the top of the switch and the spring-loaded latch near the bottom.
2. Holding the bottom of the switch away from the DIN rail, place the two hooks on the back of the switch over the top of the DIN rail.

Caution Do not stack any equipment on the switch.

Figure 11: Position the Hooks Over the DIN Rail



1	DIN Rail
2	Switch

3. Push the switch toward the DIN rail to cause the spring-loaded latch at the bottom rear of the switch to move down, and snap into place.

   After the switch is mounted on the DIN rail, connect the power and alarm wires, as described in Connecting Alarm Circuits, on page 35.

Note For instructions on how to remove the switch from a DIN rail, see Removing the Switch from a DIN Rail , on page 34.

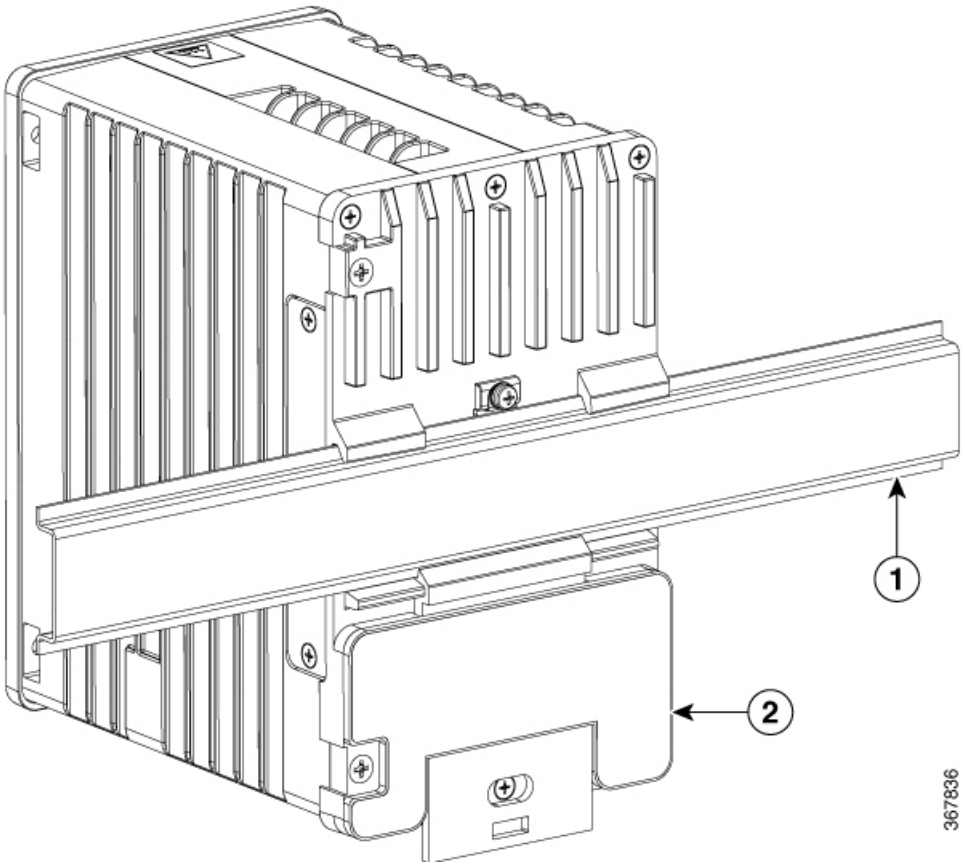
Removing the Switch from a DIN Rail

To remove the switch from a DIN rail, follow these steps:

1. Ensure that power is removed from the switch, and disconnect all cables and connectors from the front panel of the switch.

2. Insert a tool such as a flathead screwdriver in the slot at the bottom of the spring-loaded latch and use it to release the latch from the DIN rail.
3. Pull the bottom of the switch away from the DIN rail, and lift the hooks off the top of the DIN rail.

Figure 12: Releasing the Spring-Loaded Latch from the DIN Rail



4. Remove the switch from the DIN rail.

Connecting Alarm Circuits

After the switch is installed, you are ready to connect the DC power and alarm connections.

Wiring the External Alarms

The switch has two alarm input and one alarm output relay circuits for external alarms. The alarm input circuits are designed to sense if the alarm input is open or closed relative to the alarm input reference pin. Each alarm input can be configured as an open or closed contact. The alarm output relay circuit has a normally open and a normally closed contact.

Alarm signals are connected to the switch through the six-pin alarm connector. Three connections are dedicated to the two alarm input circuits: alarm input 1, alarm input 2, and a reference ground. An alarm input and the reference ground wiring connection are required to complete a single alarm input circuit. The three remaining connections are for the alarm output circuit: a normally open output, a normally closed output, and a common

signal. An alarm output and the common wiring connection are required to complete a single alarm output circuit.

The labels for the alarm connector are on the switch panel and are displayed below.

Label	Connection
NO	Alarm Output Normally Open (NO) connection
COM	Alarm Output Common connection
NC	Alarm Output Normally Closed (NC) connection
IN2	Alarm Input 2
REF	Alarm Input Reference Ground connection
IN1	Alarm Input 1

Caution The input voltage source of the alarm output relay circuit must be an isolated source and limited to less than or equal to 24 VDC, 1.0A or 48VDC, 0.5A.

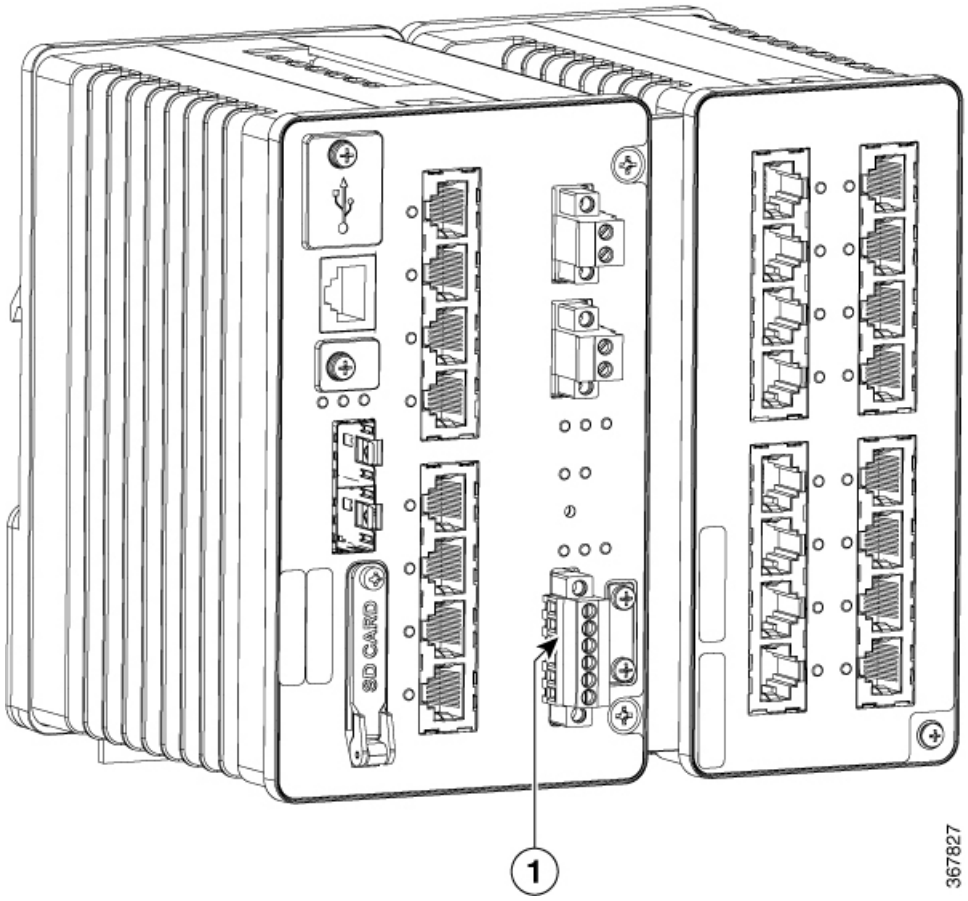
Caution To reduce risk of electric shock and fire, the alarm ports must be connected to an IEC60950/IEC 62368 compliant limited power source.

Note Wire connections to the power and alarm connectors must be UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire.

To wire the switch to an external alarm device, follow these steps:

1. Remove the captive screws that hold the alarm connector on the switch, and remove the connector from the switch chassis.

Figure 13: Alarm Connector



2. Measure two strands of twisted-pair wire (16-to-18 AWG) long enough to connect to the external alarm device. Choose between setting up an external alarm input or output circuit.
3. Use a wire stripper to remove the casing from both ends of each wire to 0.25 inch (6.3 mm) ± 0.02 inch (0.5 mm). Do not strip more than 0.27 inch (6.8 mm) of insulation from the wires. Stripping more than the recommended amount of wire can leave exposed wire from the alarm connector after installation.
4. Insert the exposed wires for the external alarm device into the connections based on an alarm input or output circuit setup. For example, to wire an alarm input circuit, complete the IN1 and REF connections.
5. Use a ratcheting torque flathead screwdriver to tighten the alarm connector captive screw (above the installed wire leads) to 2 in-lb (0.23 N-m).

Figure 14: Securing the Alarm Connector Captive Screws

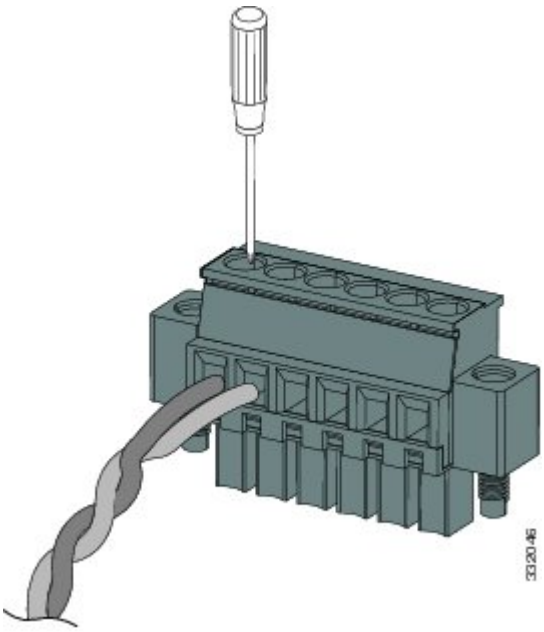


Figure 15: Securing the Alarm Connector Captive Screws

Caution Do not over-torque the power and alarm connectors' captive screws. The torque should not exceed 2in-lb (0.23N-m).

6. Repeat Step 2 through Step 5 to insert the input and output wires of one additional external alarm device into the alarm connector.

The first alarm device circuit is wired as an alarm input circuit; the IN1 and REF connections complete the circuit. The second alarm device circuit is wired as an alarm output circuit that works on a normally open contact basis; the NO and COM connections complete the circuit.

Attaching the Alarm Connector to the Switch

Warning Failure to securely tighten the captive screws can result in an electrical arc if the connector is accidentally removed. Statement 397

To attach the alarm connector to the front panel of the switch, follow these steps:

1. Insert the alarm connector into the receptacle on the switch front panel.
2. Use a ratcheting torque flathead screwdriver to tighten the captive screws on the sides of the alarm connector.

Connecting Destination Ports

These section provide more information about connecting to the destination ports:

Connecting to 10/100/1000 Ports

The switch 10/100/1000 ports automatically configure themselves to operate at the speed of attached devices. If the attached ports do not support autonegotiation, you can explicitly set the speed and duplex parameters. Connecting devices that do not autonegotiate or that have their speed and duplex parameters manually set can reduce performance or result in no communication.

Note For Rail and Smart Grid compliance, SF/UTP cables were used for Ethernet ports.

To maximize performance, choose one of these methods for configuring the Ethernet ports:

- Let the ports autonegotiate both speed and duplex.
- Set the port speed and duplex parameters on both ends of the connection.

The IE3300 all Gigabit series (with expansion module) supports power budget of up to 360W for PoE/PoE+, shared across up to 24 ports.

The IE3300 10G series (with expansion module) supports power budget of up to 480W (pending safety & compliance approval) for IEEE® 802.3af / 802.3at / 802.3bt (type 3 & type 4), shared across up to 24 ports.

Caution To prevent electrostatic-discharge (ESD) damage, follow your normal board and component handling procedures.

To connect to 10BASE-T, 100BASE-TX or 1000BASE-T devices, follow these steps:

1. When connecting to workstations, servers, routers, and Cisco IP phones, connect a straight-through cable to an RJ-45 connector on the front panel.

   When connecting to 1000BASE-T-compatible devices, use a twisted four-pair, Category 5 or higher cable.

   The auto-MDIX feature is enabled by default. For configuration information for this feature, see the Cisco IE 3x00 Switch Software Configuration Guide for the appropreate software release.

2. Connect the other end of the cable to an RJ-45 connector on the other device. The port LED turns on when both the switch and the connected device have established a link.

   The port LED is amber while Spanning Tree Protocol (STP) discovers the topology and searches for loops. This can take up to 30 seconds, and then the port LED turns green.

If the port LED does not turn on:

- The device at the other end might not be turned on.
- There might be a cable problem or a problem with the adapter installed in the attached device. See Troubleshooting for solutions to cabling problems.
- Reconfigure and reboot the connected device if necessary.

- Repeat Steps 1 through 3 to connect each device.

Installing and Removing SFP Modules

These sections describe how to install and remove SFP modules. SFP modules are inserted into SFP module slots on the front of the switch. These field-replaceable modules provide the uplink optical interfaces, send (TX) and receive (RX).

You can use any combination of rugged SFP modules. See the release notes on Cisco.com for the list of supported modules. Each SFP module must be of the same type as the SFP module on the other end of the cable, and the cable must not exceed the stipulated cable length for reliable communications.

Caution When you use commercial SFP modules such as CWDM and 1000BX-U/D, reduce the maximum operating temperature by 27° F. The minimum operating temperature is 32°F (0°C).

For detailed instructions on installing, removing, and cabling the SFP module, see your SFP module documentation.

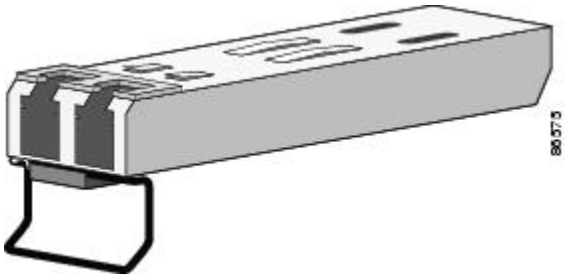
Installing SFP Modules into SFP Module Ports

Caution Do not install or remove the SFP module with fiber-optic cables attached to it because of the potential damage to the cables, the cable connector, or the optical interfaces in the SFP module. Disconnect all cables before removing or installing an SFP module.

Removing and installing an SFP module can shorten its useful life. Do not remove and insert SFP modules more often than is absolutely necessary.

The following illustration shows an SFP module that has a bale-clasp latch.

Figure 16: SFP Module with a Bale-Clasp Latch



To insert an SFP module into the SFP module slot:

1. Attach an ESD-preventive wrist strap to your wrist and to a grounded bare metal surface.
2. Find the send (TX) and receive (RX) markings that identify the correct side of the SFP module.

   On some SFP modules, the send and receive (TX and RX) markings might be replaced by arrows that show the direction of the connection, either send or receive (TX or RX).
3. Align the SFP module sideways in front of the slot opening.

4. Insert the SFP module into the slot until you feel the connector on the module snap into place in the rear of the slot.
5. Remove the dust plugs from the SFP module optical ports and store them for later use.

Caution Do not remove the dust plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

6. Insert the LC cable connector into the SFP module.

Removing SFP Modules from SFP Module Slots

To remove an SFP module from a module receptacle:

1. Attach an ESD-preventive wrist strap to your wrist and to a grounded bare metal surface.
2. Disconnect the LC from the SFP module.
3. Insert a dust plug into the optical ports of the SFP module to keep the optical interfaces clean.
4. Unlock and remove the SFP module.

   If the module has a bale-clasp latch, pull the bale out and down to eject the module. If the bale-clasp latch is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the bale-clasp latch.
5. Grasp the SFP module between your thumb and index finger, and carefully remove it from the module slot.
6. Place the removed SFP module in an antistatic bag or other protective environment.

Connecting to SFP Modules

This section describes how to connect to a fiber-optic SFP port. For instructions on how to install or remove an SFP module, see Installing and Removing SFP Modules, on page 40.

Warning Class 1 laser product. Statement 1008

Caution Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light. Before connecting to the SFP module, be sure that you understand the port and cabling guidelines in Preparing for Installation, on page 15.

To connect a fiber-optic cable to an SFP module, follow these steps:

1. Insert one end of the fiber-optic cable into the SFP module port.
2. Insert the other cable end into a fiber-optic receptacle on a target device.

3. Observe the port status LED:
   - The LED turns green when the switch and the target device have an established link.
   - The LED turns amber while the STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.
   - If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Troubleshooting for solutions to cabling problems.
4. If necessary, reconfigure and restart the switch or the target device.

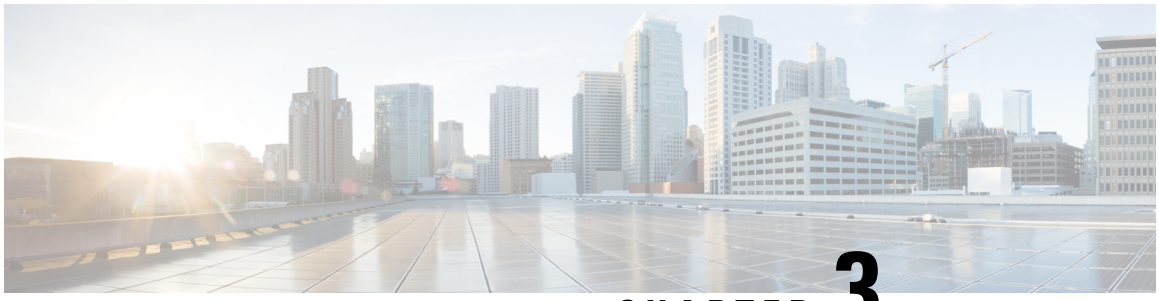
Verifying Switch Operation

Before installing the switch in its final location, power on the switch, and verify that the switch powers up in boot fast style. The boot fast sequence allows the switch to boot up in less than 90 seconds.

Where to Go Next

If the default configuration is satisfactory, the switch does not need further configuration. You can use any of these management options to change the default configuration:

- Start the Web UI, which is in the switch memory, to manage individual and standalone switches. This is an easy-to-use web interface that offers quick configuration and monitoring. You can access the Web UI from anywhere in your network through a web browser. For more information, see the Software Configuration Guide and the Web UI online help.
- Use the CLI to configure the switch as an individual switch from the console.
- Start an SNMP application such as the CiscoView application.
- Start the Common Industrial Protocol (CIP) management tool. You can manage an entire industrial automation system with the CIP-based tools.



CHAPTER 3

Express Setup

When you first set up the switch, you should use Express Setup to enter the initial IP information. This process enables the switch to connect to local routers and the Internet. You can then access the switch through the IP address for additional configuration.

Required Equipment

You need this equipment to set up the switch:

- Computer running Windows or a Mac.
- A Web browser (IE or Firefox) with JavaScript enabled.
- A straight-through or crossover Category 5 Ethernet cable to connect your computer to the switch port.

Note Do not use the RS232 serial console port for Express Setup.

- A small paper clip to reach the button.

Note Before running Express Setup, disable any pop-up blockers or proxy settings on your browser and any wireless client running on your computer.

Run Express Setup

Complete the steps in this section to use Express Setup to enter the initial IP information.

Before you begin

Perform the following checks before you use Express Setup.

- Make sure that the switch is in default factory mode.
- Make sure that nothing is connected to the switch.

  During Express Setup, the switch acts as a DHCP server.

Note Exception: You can add a serial console cable to monitor the booting sequence. *Do not press [return key] on the console screen*. Make sure that the computer that is connected to the switch is configured with DHCP.

Procedure

Step 1 Complete one of the following actions:

If the switch...	Then...
Is fresh out of the box	Go to the next step.
Is not fresh out of the box	Use a paper clip to reset the switch for 15 seconds until the System LED turns red, then release the paper clip. The switch automatically reboots once the System LED goes red.

Note The Express setup long press (press the button for 15 seconds to reset the switch to use factory default settings) deletes the configurations (nvram_config and vlan.dat) from the flash and removable media (SD card or USB flash drive). Remove any removable media if you do not want any files to be deleted from the SD card or USB flash drive.

Step 2 On the computer that is connected to the switch, disable web browser pop-up blockers and proxy settings.

Step 3 Connect power to the switch.

See the wiring instructions in Grounding the Switch and Wiring the DC Power Source.

Step 4 Power on or reset the switch.

Use LEDs to monitor boot progress:

- Blinking System LED: bootloader
- Off System LED: POST
- Solid Green System LED: POST exit, initializing IOS
- Green System and Alarm LEDs green: IOS initialization done
- Blinking Express Setup LED: Ready for express setup process

Step 5 Insert paper clip into Express Setup button for 1 to 2 seconds.

When released, port Gig1/3 LED starts flashing green.

Step 6 Connect the computer to port Gig1/3.

The LED continues to blink.

Step 7 After the computer has the IP Address 192.168.1.1, point the browser to http://192.168.1.254.

Step 8 Enter the username and password.

The username is admin, and the password is the system serial number.

The **Account Settings** window appears.

Step 9 In the **Account Settings** window, complete the following tasks:

a) Fill out the fields in the **Account Settings** window as follows:

- *Login Name:* admin

  You can change the login name here, if you like.

- *Login User Password*: By default, the login user password is the serial number of the switch.

  You can change the login user password here if you like.

- *Confirm Login User Password*: Retype the password that you used earlier.

- *Command-Line Password* (Optional): This defaults to Sync to Login Password.

  You can change the command login password here by using the drop-down menu.

- *Device Name*: Create an identifier for the device in the network.

- *NTP Server* (Optional): You may identify an NTP server for the device here.

- *Date & Time Mode* (Optional): Identify the mode here, through the drop-down.

Trouble If the account settings window does not appear, make sure that any pop-up blockers or proxy settings on your browser are disabled. Also make sure that any wireless client is disabled on your computer.

b) After you finish filling in the fields in the **Account Settings** window, click **Basic Settings**.

Step 10 In the **Basic Settings** window, complete the following tasks:

a) Fill out the fields as follows, using English letters and Arabic numbers:

- *IP Address*: Choose Static or DHCP.

- *VLAN ID*: Enter a valid VLAN ID.

  This is the management VLAN for the switch.

- *IP Address*: Enter a valid IP Address.

- *Subnet Mask*: Enter a valid subnet mask.

- *Default Gateway*: Enter the IP address of the router (not optional if IP is static).

  You must enter the router IP address if the IP address is static.

(Optional) On this screen you can also enable or disable Telnet and SSH and configure CIP settings.

The CIP VLAN can be the same as the management VLAN, or you can isolate CIP traffic on another VLAN that is already configured on the switch. The default CIP VLAN is VLAN 1. Only one VLAN on a switch can have CIP enabled. If the CIP VLAN is different from the management VLAN, you must specify an IP address for the CIP VLAN. Make sure that the IP address that you assign to the switch is not being used by another device in your network.

For more information about the CIP VLAN settings, click Help on the toolbar.

b) After you finish filling in the fields in the **Basic Settings** window, click **Switch Wide Settings**.

Step 11 In the **Switch Wide Settings** window, complete the following tasks:

a) Fill out the fields as follows:

- *Data VLAN*: You can enable or disable the data VLAN with the button here.
- *Voice VLAN*: You can enable/disable Voice VLAN here.
- *STP Mode* (Optional): Select an STP Mode from the drop-down
- *Bridge Priority*: You can update, enable, or disable Bridge Priority here.
- *Domain Name* (Optional): Enter a valid Domain Name.

b) After you finish filling in the fields in the **Switch Wide Settings** window, click **Day 0 Config Summary**.

The **Summary** window displays the configuration settings that you made.

Step 12 In the **Summary**window, confirm that the settings are accurate and complete one of the following actions:

If the settings...	Then...
Are correct	Click **Submit** to complete the initial setup.
Are not correct	**a.** Click the back button and make the required changes. **b.** Navigate back to the **Summary** window. **c.** Click **Submit** to complete the initial setup.

After you click **Submit**, the following events occur:

a. The switch is configured and exits Express Setup mode.

b. The browser displays a warning message and tries to connect with the earlier switch IP address.

c. Success dialogue appears. Click **OK**.

Typically, connectivity between the computer and the switch is lost because the configured switch IP address is in a different subnet from the IP address on the computer.

Step 13 Turn off DC power at the source, disconnect all cables to the switch, and install the switch in your network.

Step 14 If you changed the static IP address on your computer, change it to the previously configured static IP address.

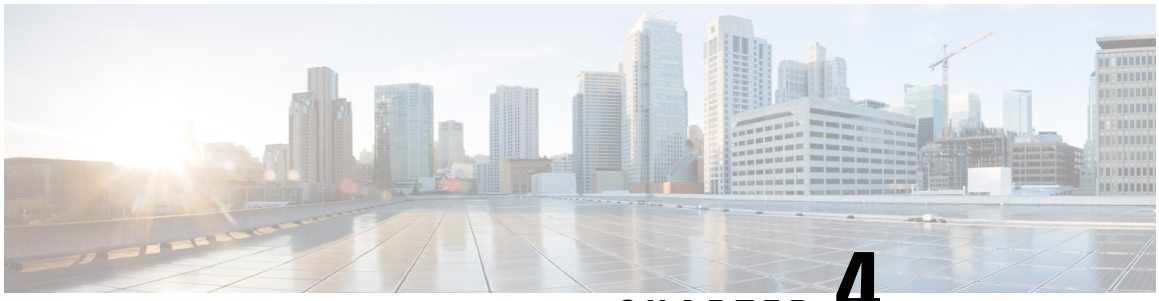
What to do next

You can display Web UI by following these steps:

1. Start a web browser on your computer.
2. Enter the switch IP address, username, and password in the web browser, and press Enter. The WebUI page appears.

Trouble If the WebUI page does not appear:

- Confirm that the port LED for the switch port connected to your network is green.
- Confirm that the computer that you are using to access the switch has network connectivity by connecting it to a well-known web server in your network. If there is no network connection, troubleshoot the network settings on the computer.
- Make sure that the switch IP address in the browser is correct.
- Ping the Switch IP Address and confirm IP reachability.
- If the switch IP address in the browser is correct, the switch port LED is green, and the computer has network connectivity, continue troubleshooting by reconnecting the computer to the switch. Configure a static IP address on the computer that is in the same subnet as the switch IP address.
- When the LED on the switch port that is connected to the computer is green, reenter the switch IP address in a web browser to display the Web UI. When Web UI appears, you can continue with the switch configuration.



CHAPTER 4

Configuring the Switch with the CLI Setup Program

Configure the Switch with the CLI-Based Setup Program

This chapter provides a command-line interface (CLI)-based setup procedure for the switch.

Before connecting the switch to a power source, review the safety warnings in Warnings section of the Switch Installation, on page 15 chapter.

Accessing the CLI Through the Console Port

You can enter Cisco IOS commands and parameters through the CLI. The IE3x00 has two console options: RJ45 8 pin, or USB Mini-type B. Use one of these options to access the CLI:

RJ-45 Console Port

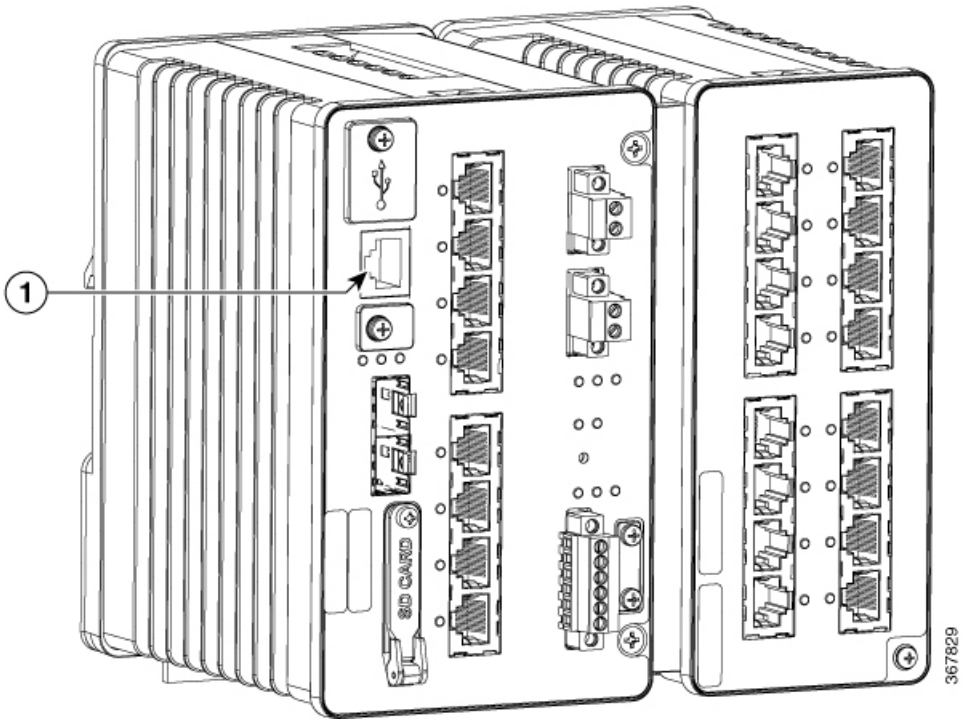
1. Connect one end of the console cable to your PC.

   Doing so may require an adapter for USB to RJ45.

2. Connect the other end of the cable or adapter to the switch console port.

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

Figure 17: Connecting the Console Cable



1
RJ-45 Console Port

4. Configure the baud rate and character format of the PC or terminal to match the console port characteristics:
   - 9600 baud
   - 8 data bits
   - 1 stop bit
   - No parity
   - None (flow control)
5. Connect power to the switch as described in Connecting to Power.
6. The PC or terminal displays the bootloader sequence. Press **Enter** to display the setup prompt. See Entering the Initial Configuration Information, on page 52 to configure the switch using the Setup program.

USB Mini-Type B Console Port

1. If you are connecting the switch USB-mini console port to a Windows-based PC for the first time, install a USB driver.
2. Use a Phillips screwdriver to loosen the screw on the USB mini-type B console port cover. Remove the screw and take off the cover.

Figure 18: USB Mini-Type B Console Port Cover

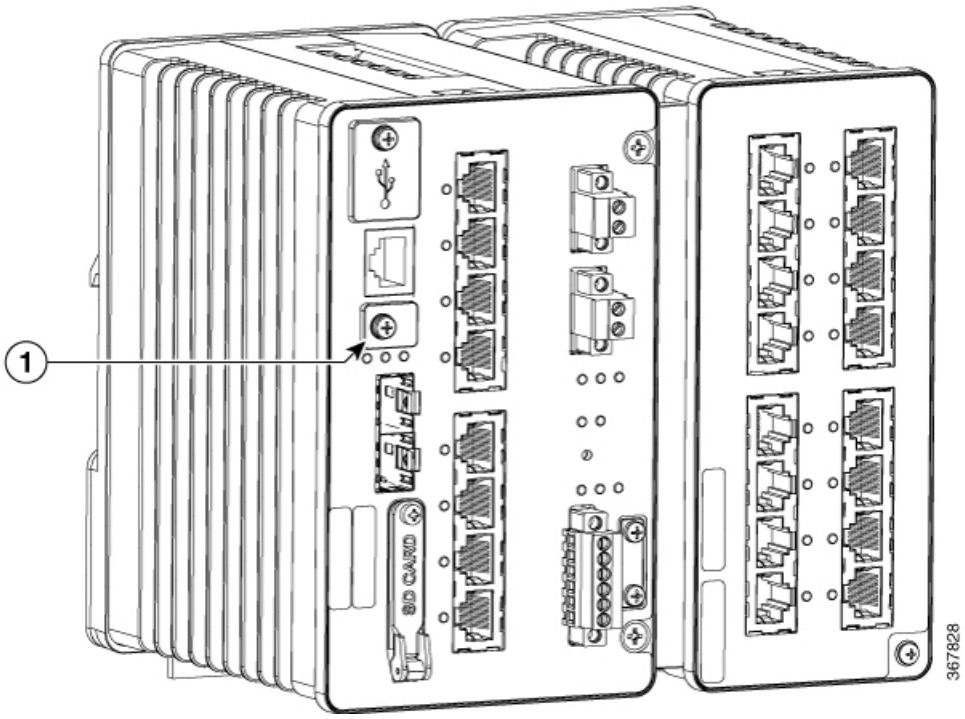


Table 1:

1	USB Mini-Type B Console Port Cover

3. 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-mini console port.
4. Identify the COM port assigned to the USB-mini console port
5. Start the terminal-emulation program on the PC or the terminal. The program, frequently a PC application such as PuTTY, HyperTerminal, or ProcommPlus, makes communication possible between the switch and your PC or terminal.
6. Configure the COM port.
7. Configure the baud rate and character format of the PC or terminal to match the console port characteristics:
   a. 9600 baud
   b. 8 data bits
   c. 1 stop bit
   d. No parity
   e. None (flow control)
8. Connect power to the switch as described in Connecting to Power.

9. The PC or terminal displays the bootloader sequence. Press **Enter** to display the setup prompt. See Entering the Initial Configuration Information, on page 52 to configure the switch using the Setup program.

Entering the Initial Configuration Information

To set up the switch, you need to complete the setup program, which runs automatically after the switch is powered on. You must assign an IP address and other configuration information necessary for the switch to communicate with the local routers and the Internet. This information is also required if you plan to use WebUI to configure and manage the switch.

In Cisco IOS XE 17.10.1 and later, you can set a password encryption level so that user passwords are not stored in plain text. See System Security Configuration (Cisco IOS XE 17.10.1 and later), on page 54.

IP and Password Settings

You need this information from your network administrator before you complete the setup program:

- Encryption level and Master key (Cisco IOS XE 17.10.1 and later)
- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)
- Enable secret password
- Enable password

Initial Configuration (Cisco IOS XE 17.9.x and earlier)

Complete the following steps to create an initial configuration for the switch with the setup program:

1. Enter **Yes** at these two prompts:

```
Would you like to enter the initial configuration dialog? [yes/no]: yes
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.
Would you like to enter basic management setup? [yes/no]: yes
```

2. Enter a hostname for the switch, and press **Return**.

   On a command switch, the hostname is limited to 28 characters; on a member switch, it is limited to 31 characters. Do not use *-n* , where n is a number, as the last character in a hostname for any switch.

```
Enter host name [Switch]: host_name
```

3. Enter an enable secret password, and press **Return**.

   The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces. The secret password is encrypted, and the enable password is in plain text.

```
Enter enable secret: secret_password
```

4. Enter an enable password, and press **Return**.

```
Enter enable password: enable_password
```

5. Enter a virtual terminal password, and press **Return**.

   The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

```
Enter virtual terminal password: terminal-password
```

6. (Optional) Configure Simple Network Management Protocol (SNMP) by responding to the prompts. You can also configure SNMP later through the CLI, Device Manager, or the Cisco Network Assistant application. To configure SNMP later, enter **no**.

```
Configure SNMP Network Management? [no]: no
```

7. Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network, and press **Return**. For this release, always use **vlan1** as that interface.

Note The switch will transmit a DHCP discover message on the **vlan1** interface. If the switch is connected to the network before the CLI initial setup process is started, the interface may have been assigned a dynamic IP address. It is all right if you do not see an IP address on the **vlan1** interface. This process allows you set a static IP address for management, which will over write the dynamically assigned IP address.

```
Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration
Interface IP-Address OK? Method Status Protocol
Vlan1 unassigned NO unset up down
GigabitEthernet1/1 unassigned YES unset down down
GigabitEthernet1/2 unassigned YES unset down down
GigabitEthernet1/3 unassigned YES unset down down
GigabitEthernet1/4 unassigned YES unset down down
GigabitEthernet1/5 unassigned YES unset down down
GigabitEthernet1/6 unassigned YES unset down down
GigabitEthernet1/7 unassigned YES unset down down
GigabitEthernet1/8 unassigned YES unset down down
GigabitEthernet1/9 unassigned YES unset down down
GigabitEthernet1/10 unassigned YES unset down down
Enter interface name used to connect to the
management network from the above interface summary: vlan1
Enter interface name used to connect to the
management network from the above interface summary: vlan1
```

8. Configure the interface by entering the switch IP address and subnet mask and pressing Return. The IP address and subnet masks shown here are examples.

```
Configuring interface Vlan1:
Configure IP on this interface? [yes]:
IP address for this interface: 10.1.1.2
Subnet mask for this interface [255.255.255.0] :
Class A network is 10.0.0.0, 8 subnet bits; mask is /24
```

9. This summary appears:

```
The following configuration command script was created:
hostname ie3300
enable secret 9 $9$rkqtjJhIkZyANU$Ib4nfuxrpHBi.lixF.0Ir94k9XWYsW3nyF7Glmc6lkc
enable password cisco
line vty 0 15
password cisco
no snmp-server
!!
interface Vlan1
no shutdown
ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
!
end
```

After you complete the setup program, the switch can run the default configuration that you created. If you want to change this configuration or want to perform other management tasks, use one of these tools:

- Command-line interface (CLI)

To use the CLI, enter commands at the Switch> prompt through the console port by using a terminal emulation program. For configuration information, see the switch Cisco Catalyst IE3x00 Rugged Switch software configuration guides.

System Security Configuration (Cisco IOS XE 17.10.1 and later)

For enchanced security, sensitive information such as passwords needs to be encrypted. The configuration dialog includes a System Security Configuration Dialog that allows you to set the password encryption level. Encryption levels include type-6 and type-7 encryption. It is recommended that you enable both types.

- Type-6 uses Advanced Encryption Standard (AES) for encrypting the passwords. Type-6 password encryption and decryption is coupled with a master-key that you enter. You must remember the master key because it cannot be recovered.
- The master key is the password/key used to encrypt all other keys in the switch configuration with the use of an AES symmetric cipher. The master key is not stored in the switch configuration and cannot be seen or obtained in any way while connected to the switch. Once configured, the master key is used to encrypt any existing or new keys in the switch configuration. Keys are not encrypted until you issue the **password encryption aes** command.

- Type-7 passwords are an obfuscation of the original plain text password. It is based on Vigenere Cipher and prevents someone seeing the real passwords in a configuration.

You can use the setup program to set the password encryption level on both a new switch and a switch that is already configured. For a new switch, see Initial Configuration - Type-6 Encryption, on page 55 or Initial Configuration - Type-7 Encryption, on page 58. To configure system security settings without running the initial setup, see Setting the Password Encryption Level, on page 61.

Initial Configuration - Type-6 Encryption

To create an initial configuration for the switch with the setup program with type-6 encryption, complete the following steps:

Before you begin

Access the CLI as described in Accessing the CLI Through the Console Port, on page 49.

Procedure

Step 1 Enter **Yes** at the following prompt:

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes
```

Step 2 At the prompt, enter the password encryption level that you want to apply:

```
  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered

 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0
```

Note In Cisco IOS XE 17.10.1, if you select both type 6 & type 7 encryption [0], only the username is automatically converted to type 6, and the enable password and the line vty password are automatically converted to type 7 instead of type 6.

Step 3 Enter the master key to be used to encrypt all other keys in the switch:

```
Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!, #,
 ;' : ************
```

Step 4 Enter the master key again to confirm it:

```
Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
```

```
password encryption aes
service password-encryption
!
!
end
```

Note You should save the Master Key, because you will need it if this device is replaced.

Step 5 Enter **2** at the prompt to save the System Security Configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

Step 6 Enter **yes** at the prompt to configure basic management settings:

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

Step 7 Enter a hostname for the switch:

```
Enter host name [Switch]: Switch123
```

Step 8 Enter an enable secret password:

```
 The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
```

Step 9 Enter the enable secret password again to confirm it:

```
 Confirm enable secret: **********
```

Step 10 Enter an enable password:

```
 The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********
```

Step 11 Enter a virtual terminal password.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

```
The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: ********
```

Step 12 Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network. For this release, always use **vlan1** as that interface.

Note The switch will transmit a DHCP discover message on the **vlan1** interface. If the switch is connected to the network before the CLI initial setup process is started, the interface may have been assigned a dynamic IP address. It is all right if you do not see an IP address on the **vlan1** interface. This process allows you set a static IP address for management, which will over write the dynamically assigned IP address.

```
Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [10.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 10.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 10.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
```

Step 13 Enter **2** to save the configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

What to do next

After you complete the setup program, the switch can run the default configuration that you created. If you want to change this configuration or want to perform other management tasks, use one of these tools:

- Command-line interface (CLI)
- Web User Interface (WebUI)

To use the CLI, enter commands at the *Switch* > prompt through the console port by using a terminal emulation program or through the network by using Telnet. For configuration information, see the configuration guides for the Cisco IE3x00 switches.

To use WebUI, see the online help for WebUI.

Initial Configuration - Type-7 Encryption

To create an initial configuration for the switch with the setup program with only type-7 encryption, complete the following steps:

Before you begin

Access the CLI as described in Accessing the CLI Through the Console Port, on page 49.

Procedure

Step 1 Enter **Yes** at the following prompt:

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes
```

Step 2 At the prompt, enter **1** to apply only type-7 password encryption:

```
  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered
```

```
 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 1
```

Step 3 Enter **2** at the prompt to save the System Security Configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

Step 4 Enter **yes** at the prompt to configure basic management settings:

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

Step 5 Enter a hostname for the switch:

```
Enter host name [Switch]: Switch123
```

Step 6 Enter an enable secret password:

```
 The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
```

Step 7 Enter the enable secret password again to confirm it:

```
 Confirm enable secret: **********
```

Step 8 Enter an enable password:

```
 The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********
```

Step 9 Enter a virtual terminal password.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

```
The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: ********
```

Step 10 Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network. For this release, always use **vlan1** as that interface.

Note The switch will transmit a DHCP discover message on the **vlan1** interface. If the switch is connected to the network before the CLI initial setup process is started, the interface may have been assigned a dynamic IP address. It is all right if you do not see an IP address on the **vlan1** interface. This process allows you set a static IP address for management, which will over write the dynamically assigned IP address.

```
Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [10.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 10.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 10.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
```

Step 11 Enter **2** to save the configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

What to do next

After you complete the setup program, the switch can run the default configuration that you created. If you want to change this configuration or want to perform other management tasks, use one of these tools:

- Command-line interface (CLI)
- Web User Interface (WebUI)

To use the CLI, enter commands at the *Switch* > prompt through the console port by using a terminal emulation program or through the network by using Telnet. For configuration information, see the configuration guides for the Cisco IE3x00 switches.

To use WebUI, see the online help for WebUI.

Setting the Password Encryption Level

Follow this procedure to configure system security settings (type-6 and type-7 encryption) without running the initial setup.

Procedure

Step 1 Enter **No** at the following prompt:

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
Autoinstall trying DHCPv6 on Vlan1

Would you like to enter the initial configuration dialog? [yes/no]: no
```

Step 2 Enter the enable secret at the prompt:

```
  The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
```

```
  Enter enable secret: **********
  Confirm enable secret: **********

The following configuration command script was created:

enable secret 9 $9$YMkVvPLbxKn4bE$OAOX/akBBsukkRV1L.Tk7p2KaM0BXLQI.HbyGbXB8/g
!
end
```

Step 3 Enter **2** to save the configuration and go to the System Security Configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

Step 4 At the prompt, enter the password encryption level that you want to apply:

```
  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered

 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0
```

Step 5 Enter the master key to be used to encrypt all other keys in the switch:

```
Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!, #,
 ;' : ************
```

Step 6 Enter the master key again to confirm it:

```
Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end
```

Note You should save the Master Key, because you will need it if this device is replaced.

Step 7 Enter **2** at the prompt to save the System Security Configuration:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
```

```
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.


Press RETURN to get started!


Switch>
```

CLI Setup Examples

Initial Configuration Example

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes


  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered

 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0

 Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!,
#, ;' : ************

 Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Switch]: Switch123

  The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
  Confirm enable secret: **********

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: ********

Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  12.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [12.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 12.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
```

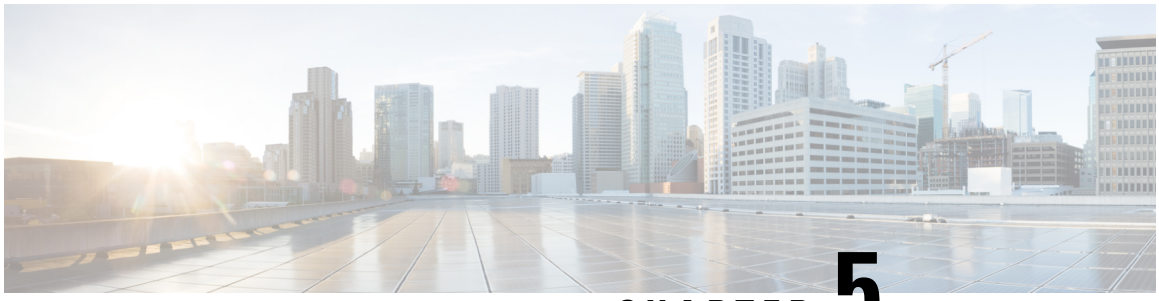
```
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 12.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

System Security Configuration Example

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
Autoinstall trying DHCPv6 on Vlan1   yes


  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered

 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0

 Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!,
#, ;' : ************

 Confirm the master key: ************

The following configuration command script was created:
```

```
key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.


At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Switch]: Switch123

  The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
  Confirm enable secret: **********

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: ********

Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  12.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
```

```
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [12.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 12.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 12.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```



CHAPTER 5

Troubleshooting

Diagnosing Problems

The switch LEDs provide troubleshooting information about the switch. They show boot fast failures, port-connectivity problems, and overall switch performance. You can also get statistics from Web UI, the CLI, or an SNMP workstation. See the Cisco Catalyst IE3x00 Rugged Switch Software Configuration Guide, or the documentation that came with your SNMP application for details.

Switch Boot Fast

See Verifying Switch Operation for information on boot fast.

Note Boot fast failures are usually fatal. Contact your Cisco TAC representative if your switch does not successfully complete boot fast.

Note You can disable the boot fast and run POST by using the Cisco IOS CLI, see the Cisco IE 3X00 Switch Software Configuration Guide for more information.

Switch LEDs

Look at the port LEDs information when troubleshooting the switch. See LEDs for a description of the LED colors and their meanings.

Switch Connections

Bad or Damaged Cable

Always examine the cable for marginal damage or failure. A cable might be just good enough to connect at the physical layer, but it could corrupt packets as a result of subtle damage to the wiring or connectors. You can identify this problem because the port has many packet errors or it constantly flaps (loses and regains link).

- Exchange the copper or fiber-optic cable with a known good cable.
- Look for broken or missing pins on cable connectors.
- Rule out any bad patch panel connections or media convertors between the source and the destination. If possible, bypass the patch panel, or eliminate media convertors (fiber-optic-to-copper).
- Try the cable in another port to see if the problem follows the cable.

Ethernet and Fiber-Optic Cables

Make sure that you have the correct cable:

- For Ethernet, use Category 3 copper cable for 10 Mb/s UTP connections. Use either Category 5, Category 5e, or Category 6 UTP for 10/100, 10/100/1000 Mb/s, and PoE connections.
- Verify that you have the correct fiber-optic cable for the distance and port type. Make sure that the connected device ports match and use the same type encoding, optical frequency, and fiber type.
- Determine if a copper crossover cable was used when a straight-through was required or the reverse. Enable auto-MDIX on the switch, or replace the cable.

Link Status

Verify that both sides have a link. A broken wire or a shutdown port can cause one side to show a link even though the other side does not have a link.

A port LED that is on does not guarantee that the cable is functional. It might have encountered physical stress, causing it to function at a marginal level. If the port LED does not turn on:

- Connect the cable from the switch to a known good device.
- Make sure that both ends of the cable are connected to the correct ports.
- Verify that both devices have power.
- Verify that you are using the correct cable type. See Cable and Connectors for information.
- Look for loose connections. Sometimes a cable appears to be seated but is not. Disconnect the cable, and then reconnect it.

10/100/1000 Port Connections

If a port appears to malfunction:

- Verify the status of all ports by checking the LEDs. For more information, see Switch LEDs, on page 69.

- Use the **show interfaces** privileged EXEC command to see if the port is error-disabled, disabled, or shut down. Reenable the port if necessary.
- Verify the cable type.

SFP Module

Use only Cisco SFP modules. Each Cisco module has an internal serial EEPROM that is encoded with security information. This encoding verifies that the module meets the requirements for the switch.

- Inspect the SFP module. Exchange the suspect module with a known good module.
- Verify that the module is supported on this platform. (The switch release notes on Cisco.com list the SFP modules that the switch supports.)
- Use the **show interfaces** privileged EXEC command to see if the port or module is error-disabled, disabled, or shutdown. Reenable the port if needed.
- Make sure that all fiber-optic connections are clean and securely connected.

Interface Settings

Verify that the interface is not disabled or powered off. If an interface is manually shut down on either side of the link, it does not come up until you reenable the interface. Use the **show interfaces** privileged EXEC command to see if the interface is error-disabled, disabled, or shut down on either side of the connection. If needed, reenable the interface.

Ping End Device

Ping from the directly connected switch first, and then work your way back port by port, interface by interface, trunk by trunk, until you find the source of the connectivity issue. Make sure that each switch can identify the end device MAC address in its Content-Addressable Memory (CAM) table.

Spanning Tree Loops

STP loops can cause serious performance issues that look like port or interface problems.

A unidirectional link can cause loops. It occurs when the traffic sent by the switch is received by the neighbor, but the traffic from the neighbor is not received by the switch. A broken cable, other cabling problems, or a port issue can cause this one-way communication.

You can enable UniDirectional Link Detection (UDLD) on the switch to help identify unidirectional link problems. For information about enabling UDLD on the switch, see the “Understanding UDLD” section in the switch software configuration guide on Cisco.com.

Switch Performance

Speed, Duplex, and Autonegotiation

Port statistics that show a large amount of alignment errors, frame check sequence (FCS), or late-collisions errors, might mean a speed or duplex mismatch.

A common issue occurs when duplex and speed settings are mismatched between two switches, between a switch and a router, or between the switch and a workstation or server. Mismatches can happen when manually setting the speed and duplex or from autonegotiation issues between the two devices.

To maximize switch performance and to ensure a link, follow one of these guidelines when changing the duplex or the speed settings.

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the interfaces on both ends of the connection.
- If a remote device does not autonegotiate, use the same duplex settings on the two ports. The speed parameter adjusts itself even if the connected port does not autonegotiate.

Autonegotiation and Network Interface Cards

Problems sometimes occur between the switch and third-party network interface cards (NICs). By default, the switch ports and interfaces autonegotiate. Laptops or other devices are commonly set to autonegotiate, yet sometimes issues occur.

To troubleshoot autonegotiation problems, try manually setting both sides of the connection. If this does not solve the problem, there could be a problem with the firmware or software on the NIC. You can resolve this by upgrading the NIC driver to the latest version.

Cabling Distance

If the port statistics show excessive FCS, late-collision, or alignment errors, verify that the cable distance from the switch to the connected device meets the recommended guidelines. See Cable and Connectors.

Resetting the Switch

These are reasons why you might want to reset the switch startup configuration to factory defaults:

- You installed the switch in your network and cannot connect to it because you assigned the wrong IP address.
- You want to reset the password on the switch.

Note Resetting the switch deletes the configuration and reboots the switch. To securely erase all data, see Enabling Secure Data Wipe, on page 73.

Caution If you press the Express Setup button when you power on, the automatic boot sequence stops, and the switch enters bootloader mode.

To reset the switch:

1. Press and hold the Express Setup button (recessed behind a small hole in the faceplate) for about 15 seconds with a paper clip or similar object. The Express Setup LED will blink red/green when its recessed button has been held down long enough.

2. The switch reboots. The system LED turns green after the switch completes rebooting.
3. Press the Express Setup button again for 3 seconds. A switch Ethernet port blinks green.

The switch now behaves like an unconfigured switch. You can configure the switch by using the CLI setup procedure described in Configure the Switch with the CLI-Based Setup Program.

Emergency Recovery Installation

To recover Cisco Catalyst IE3x00 Rugged and IE3400 Heavy Duty switches that are stuck at the switch prompt, see Emergency Recovery Installation.

If other recovery methods—such as using a different valid image on the flash or a USB drive—fail, completing the emergency recovery procedure enables you to download a valid released image.

Enabling Secure Data Wipe

Secure data wipe is a Cisco wide initiative to ensure storage devices on all IOS XE based platforms are properly purged using NIST SP 800-88r1 compliant secure erase commands.

This feature is supported in Cisco IOS XE 17.10.1 and later on the following IoT switches for all license levels:

- IE3200
- IE3300
- IE3400
- IE3400H
- ESS3300

When secure data wipe is enabled, everything in internal flash memory is erased, including:

- User configuration and passwords
- Cisco IOS XE image
- Embedded MultiMediaCard (eMMC)
- rommon variables
- ACT2 Secure Storage

Note Secure erase does not clear the SD card or USB device contents. You must manually erase or reformat external storage devices.

The switch will be in rommon prompt with default factory settings (baud rate 9600) after the command is executed. The internal flash memory will not get formatted until the IOS image is rebooted.

Note If an sdflash/usbflash with a valid image inserted, the device will boot with the image in the external media based on the boot precedence. The device will be in rommon only if no external media with an image is inserted in the device.

Performing a Secure Data Wipe

To enable secure data wipe, enter the **factory-reset all secure** command in priviledged exec mode, as shown in the following example:

```
Switch#factory-reset ?
  all                 All factory reset operations
  keep-licensing-info  Keep license usage info
Switch#factory-reset all ?
secure  Securely reset all
Switch#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]Y
```

factory-reset command options:

- **factory-reset all**—Remove everything from flash
- **factory-reset keep-licensing-info**—Keep the licensing information after factory reset and remove everything else from flash.
- **factory-reset all secure** —Remove everything from flash, and also unmount and sanitize the partitions before mounting back. This ensures that the data from those partitions cannot be recovered.

Important The **factory-reset all secure** operation may take hours. Please do not power cycle.

To check the log after the switch executes the command, boot up IOS XE and enter the following **show** command:

```
Switch#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IE3200
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```

Finding the Switch Serial Number

If you contact Cisco Technical Assistance, you must know the serial number of your switch. You can also use the **show version** privileged EXEC command to obtain the switch serial number.

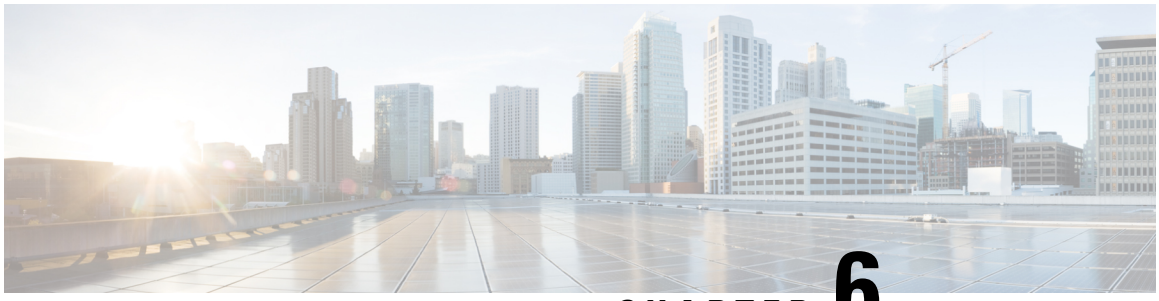
Also, the Serial Number for the switch is printed on the device label, on the device itself.

How to Recover Passwords

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

Note On these devices, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message reminds you to return to the default configuration during the recovery process.

See Resetting the Switch, on page 72 for the procedure to reset the switch and enter a new password.



CHAPTER 6

Technical Specifications

Technical Specifications

The most current technical specifications for the IE 3x00 series switches can be found in the data sheets:

- Cisco Catalyst IE3200 Rugged Series Data Sheet
- Cisco Catalyst IE3300 Rugged Series Data Sheet
- Cisco Catalyst IE3400 Rugged Series Data Sheet

Additional specifications and details not in the data sheets are in this section.

Enclosure Specifications

Table 2: Enclosure specifications for the Cisco IE 3X00 Switches

	Industrial Automation and Hazardous Locations	**Substation**	**Traffic Signal**
Enclosure types	Sealed enclosures For example: NEMA4, NEMA4X, NEMA12, NEMA13, IP54, and IP66.	Vented enclosures For example: NEMA1, IP20, and IP21.	Fan or blower-equipped enclosures For example: NEMA TS-2. **Note:** The minimum airflow is 150 lfm[4].

[4] lfm = linear feet per minute.

Current and Input Voltage Ratings

Table 3: Current and Input Voltage Rating

Model	Voltage Range	@Max Amps	PoE / PoE (+) budget
IE-3200-8T2S	12-48Vdc	2.2A	N/A
IE-3200-8P2S	12-54Vdc	5.5A	240W
IE-3300-8T2S	12-48Vdc	4.0A	N/A
IE-3300-8T2X	12-48Vdc	4.0A	N/A
IE-3300-8U2X	12-54Vdc	10.6A	480W
IE-3300-8P2S	12-54Vdc	10.6A	240W (base), 360W (with module)
IE-3400-8T2S	12-48Vdc	4.4A	N/A
IE-3400-8P2S	12-54Vdc	10.7A	240W (base), 480W (with expansion module)

Alarm Ratings

Table 4: Cisco IE3x00 Alarm Ratings

Alarm Ratings	Specification
Alarm input electrical specification	Senses an external dry contact. The open circuit voltage between any alarm input (1 to 4) and alarm input common is 3.3 VDC. The loop current is 3 mA max per input. The alarm input's low-level input voltage threshold is 0.4V. Do not apply external power to the alarm input.
Alarm output electrical specification	1.0 A @ 24 VDC or 0.5 A @ 48 VDC

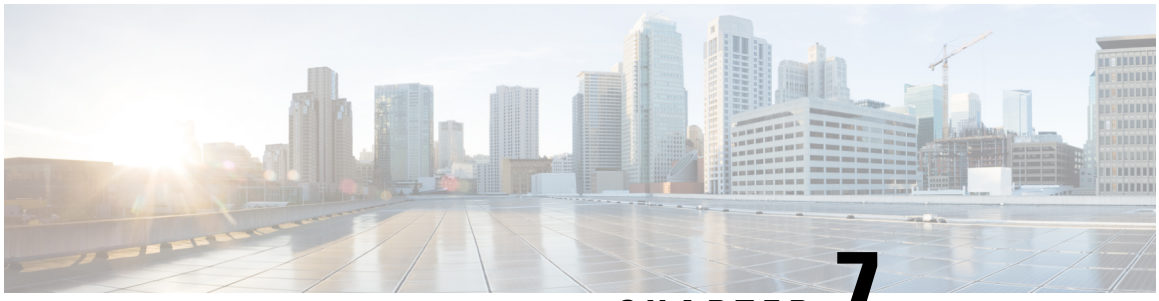
Installation Guidelines for Utility, Railway, and Marine Environments

Follow the guidelines in this section when installing the switch in utility, railway, and marine environments,

- Use shielded Ethernet cables to comply with the EMC requirements for power utility, power stations, railways, and marine environments. These installations refer to DNVGL CG-0339, IACS UR E10, IEC 60945.

- Use industrial grade SFP modules rated for -40C to +85C operation.
- For marine installations, you must install the product inside a metal enclosure, preferably IP54 or better.
- Use DNVGL "Type Approved" power supply for marine installations that use DNVGL CG-0339 guidelines.

  Cisco IE3x00 series switches require 54V (typical) for PoE operation. Refer to the Current and Input Voltage Ratings, on page 78 section for more details on the power input.
- IE3x00 products are approved for the marine installation category “All locations except bridge and open deck.”
- The IE3200 series complies with specific requirements of EN50155, exclusions clauses apply.



CHAPTER 7

Cable and Connectors

Cable and Connectors

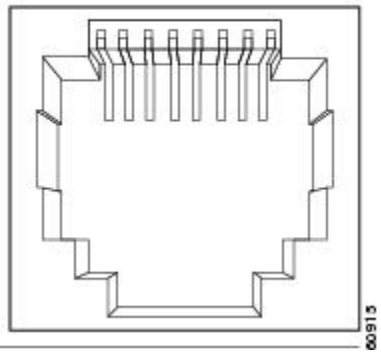
Connector Specifications

10/100/1000 Ports

The 10/100/1000 Ethernet ports on the switches use RJ-45 connectors.

Figure 19: 10/100/1000 Port Pinouts

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-

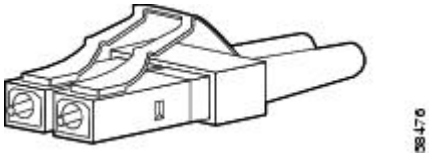


Note Connector pins 1, 2, 3, and 6 are used for PoE.

SFP Module Connectors

The illustration below shows an LC style connector that is used with the SFP Module slots. It is a fiber-optic cable connector.

Figure 20: Fiber-Optic SFP Module LC Connector

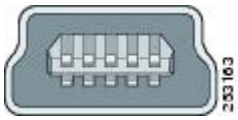


Warning Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments. Statement 1051

Console Port

The switch has two console ports: a USB 5-pin mini-Type B port on the front panel (see image below) and an RJ-45 console port on the rear panel.

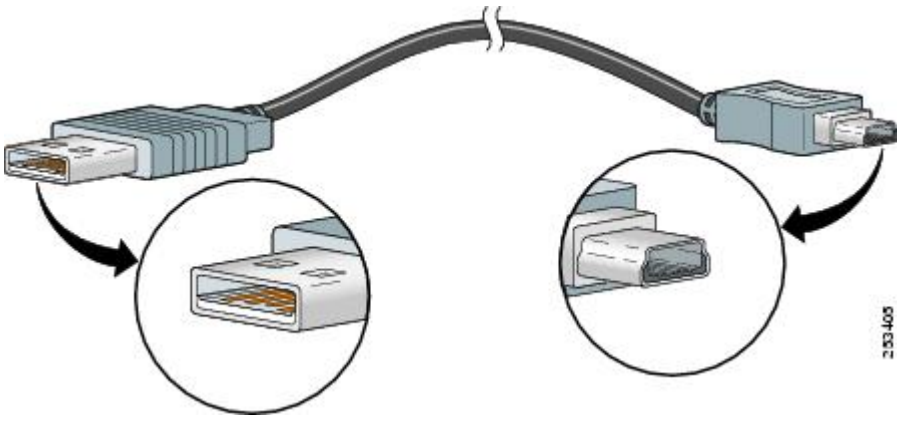
Figure 21: USB Mini-Type B Port



The USB console port uses a USB Type A to 5-pin mini-Type B cable, shown in the illustration below. The USB Type A-to-USB mini-Type B cable is not supplied.

Note When running Linux, access the USB Console using **Minicom** instead of **Screen**.

Figure 22: USB Type A-to-USB 5-Pin Mini-Type B Cable



The RJ-45 console port uses an 8-pin RJ-45 connector The supplied RJ-45-to-DB-9 adapter cable is used to connect the console port of the switch to a console PC. You need to provide a RJ-45-to-DB-25 female DTE adapter if you want to connect the switch console port to a terminal. You can order a kit (part number ACS-DSBUASYN=) containing that adapter.

Alarm Port

The labels for the alarm connector pin-outs are on the switch panel and are displayed below.

Label	Connection
NO	Alarm Output Normally Open (NO) connection
COM	Alarm Output Common connection
NC	Alarm Output Normally Closed (NC) connection
IN2	Alarm Input 2
REF	Alarm Input Reference Ground connection
IN1	Alarm Input 1

Cables and Adapters

SFP Module Cables

Each port must match the wave-length specifications on each end of the cable, and for reliable communications, the cable must not exceed the allowable length. Refer to the Data Sheets for the complete list of supported SFP Modules and cables.

Note

- The maximum operating temperature of the switch varies depending on the type of SFP module that you use.

  Note When using modules SFP-10G-ER-I & ONS-SI+-10G-ER, we require 5°C temperature derating.

- Modal bandwidth applies only to multimode fiber.
- A mode-field diameter/cladding diameter = 9 micrometers/125 micrometers.
- A mode-conditioning patch cord is required when using 1000BASE-LX/LH SFP modules, MMF, and a short link distance . Using an ordinary patch cord can cause transceiver saturation, resulting in an elevated bit error rate (BER). When using the LX/LH SFP module with 62.5-micron diameter MMF, you must also install a mode-conditioning patch cord between the SFP module and the MMF cable on both the sending and receiving ends of the link. The mode-conditioning patch cord is required for link distances greater than 984 feet (300 m).
- 1000BASE-ZX SFP modules can send data up to 62 miles (100 km) by using dispersion-shifted SMF or low-attenuation SMF. The distance depends on the fiber quality, the number of splices, and the connectors.
- When the fiber-optic cable span is less than 15.43 miles (25 km), insert a 5-decibel (dB) or 10-dB inline optical attenuator between the fiber-optic cable plant and the receiving port on the 1000BASE-ZX SFP module.

Cable Pinouts

Figure 23: Four Twisted-Pair Straight-Through Cable Schematic for 1000BASE-T Ports

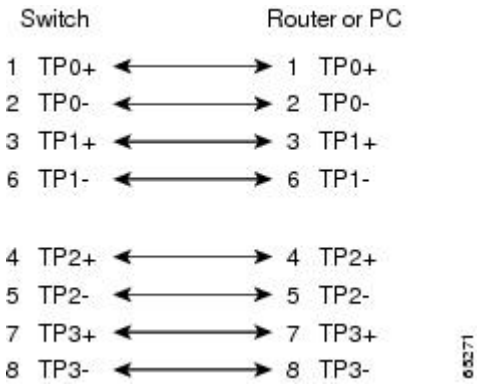
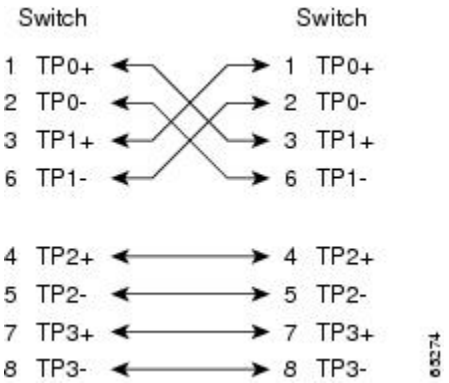
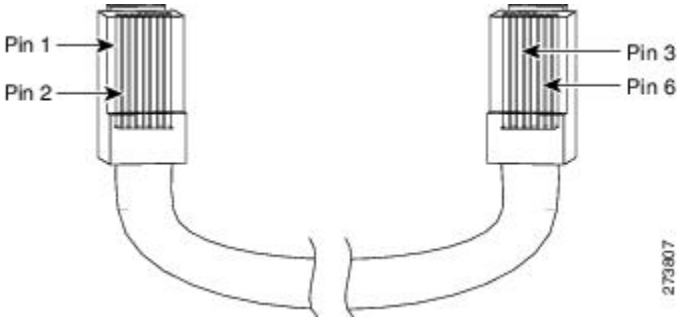


Figure 24: Four Twisted-Pair Crossover Cable Schematics for 1000BASE-T Ports



To identify a crossover cable, hold the cable ends side-by-side, with the tab at the back. The wire connected to pin 1 on the left end should be the same color as the wire connected to pin 3 on the right end. The wire connected to pin 2 on the left end should be the same color as the wire connected to pin 6 on the right end.

Figure 25: Identifying a Crossover Cable



Console Port Adapter Pinouts

The console port uses an 8-pin RJ-45 connector. If you did not order a console cable, you need to provide an RJ-45-to-DB-9 adapter cable to connect the switch console port to a PC console port. You need to provide an RJ-45-to-DB-25 female DTE adapter if you want to connect the switch console port to a terminal.

Switch ConsolePort (DTE)	RJ-45-to-DB-9Terminal Adapter	ConsoleDevice
Signal	DB-9 Pin	Signal
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

Note The RJ-45-to-DB-25 female DTE adapter is not supplied with the switch.

SwitchConsolePort (DTE)	RJ-45-to-DB-25Adapter	ConsoleDevice
Signal	DB-25 Pin	Signal
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS