Cisco Catalyst IE3400 Heavy Duty Series Hardware Installation Guide

First Published: 2019-09-03

Last Modified: 2023-03-07

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

© 2019–2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Audience

This guide is for the networking or computer technician responsible for installing Cisco Catalyst IE3400 Heavy Duty Series switches. We assume that you are familiar with the concepts and terminology of local area networking (LAN).

Purpose

This guide describes the physical and performance characteristics of each switch, explains how to install a switch, and provides troubleshooting information.

Additional product information is available at http://www.cisco.com/en/US/products/ps12451/index.html

For additional documentation, see the Cisco Catalyst IE3400 Heavy Duty Series documentation at http://www.cisco.com/en/US/products/ps12451/tsd_products_support_series_home.html

For information about the Cisco IOS commands, see http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=268438303

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.

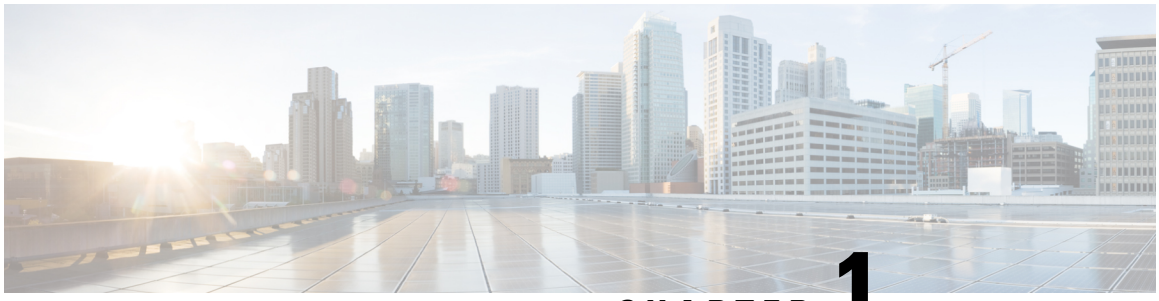
Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end 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.

Related Publications

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

See www.cisco.com/en/US/products/ps12451/tsd_products_support_series_home.html.



CHAPTER 1

Product Overview

Product Overview

The Cisco® Catalyst® IE3400 Heavy Duty Series is Cisco's next-generation, IP66 and IP67-rated switching platform designed to provide enhanced network-based security, segmentation, and visibility in the most demanding industrial environments. The Cisco® Catalyst® IE3400 Heavy Duty Series switches extend the power of intent-based networking to the harshest Internet of Things (IoT) edge.

The Cisco Catalyst IE3400 Heavy Duty Series switches deliver the advanced capabilities similar to the Cisco Catalyst IE3400 Rugged Series in environments that have heavy exposure to dust and water. These switches are available with 8, 16, or 24 Fast Ethernet (D-coded) or Gigabit Ethernet (X-coded) M12 interfaces. The switches can be wall mounted and deployed without a housing cabinet.

Note Installation details are provided in the Switch Installation section.

The IE3400 Heavy Duty Series switches are powered by Cisco IOS® XE, a next-generation operating system with built-in security and trust, featuring Secure Boot, image signing, and the Cisco Trust Anchor module. Cisco IOS XE also provides API-driven configuration with open APIs and data models.

The IE3400 Heavy Duty Series can be managed with powerful tools such as Cisco DNA Center and Industrial Network Director, and can be easily set up with a completely redesigned, user-friendly, modern GUI tool called WebUI. The platform also supports Flexible NetFlow for real-time visibility into traffic patterns and threat analysis with Cisco Stealthwatch®.

Most of the documentation related to this product can be found at
http://www.cisco.com/en/US/products/ps12451/tsd_products_support_series_home.html

Switch Models and Power Supply

Figure 1: Cisco Catalyst IE3400 Heavy Duty Series

The following table lists and describes the switches and power supply. All IP66 and IP67 switches run Cisco IOS XE firmware.

Table 1: Switch and Power Supply Descriptions

Hardware Specifications	IE-3400H-8FT	IE-3400H-8T	IE-3400H-16FT	IE-3400H-16T	IE-3400H-24FT	IE-3400H-24T
Total 100-Mbps D-coded ports	8	N/A	16	N/A	24	N/A
Total 1-Gbps X-coded ports	N/A	8	N/A	16	N/A	24
Removable storage	SD card See Note 1.	SD card See Note 1.	SD card See Note 1.	SD card See Note 1.	SD card See Note 1.	SD card See Note 1.
Alarm outputs See Note 2 and 3.	1 alarm output relay	1 alarm output relay	1 alarm output relay	1 alarm output relay	1 alarm output relay	1 alarm output relay
Alarm inputs See Note 2.	1 alarm input	1 alarm input	1 alarm input	1 alarm input	1 alarm input	1 alarm input
Console ports See Note 2.	1	1	1	1	1	1
Power input	Mini-change, (single power source)	Mini-change, (single power source)	Mini-change, (single power source)	Mini-change, (single power source)	Mini-change, (single power source)	Mini-change, (single power source)

Note 1. The SD card is optional and is not shipped by default with the switch.

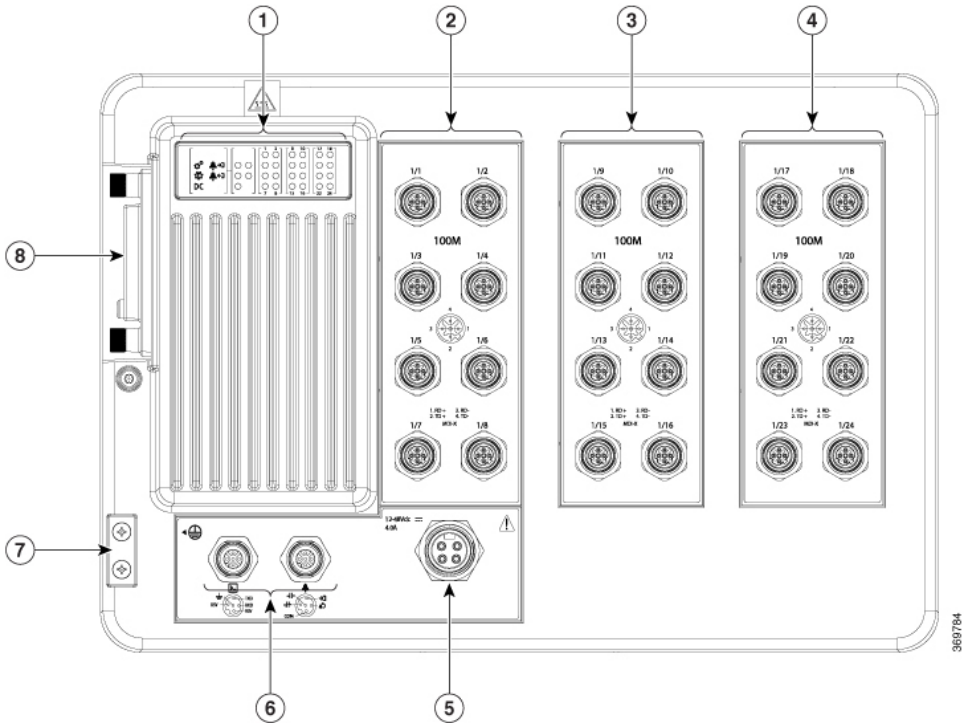
Note 2. Using an M12 A-coded 5-pin connector.

Note 3. Relay max. rating: 24VDC at 1A, 48VDC at 0.5A.

Front Panel of the Switch

This section describes the front panel components. The following figures depict the components available on the various models in this product family. Not all models are illustrated.

Figure 2: Catalyst IE3400H Front Panel



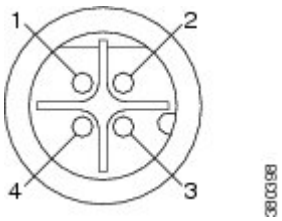
1	Switch Status LEDs	6	Console Port (left) Alarm Port (right)
2, 3, 4	Ethernet ports	7	Ground Lug
5	Power Input Port	8	SD Card Cover

10/100BASE-T Ports

You can set the 10/100BASE-T ports to operate at 10 or 100 Mb/s over IP standard M12 cabling. The ports can operate in full-duplex, half-duplex, autonegotiate (default), or never half-duplex mode.

A **Never Half Duplex** option for a port functions as the name implies, the link is never established at half duplex; it is either full-duplex or no link. Never Half Duplex avoids the unpredictable response times that in a CSMA/CD network can cause safety features to trip or interruptions that require restarting the process flow.

Figure 3: FE Ports

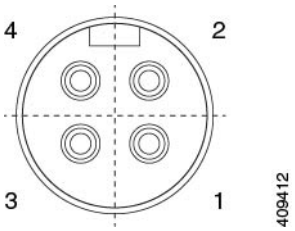


1	RD +	3	RD –
2	TD +	4	TD –

Power Connector

You connect the DC power to the switch through the front panel connector. The power connector labeling is on the panel. Torque power connection to 10in/lbs.

Figure 4: Power Connector



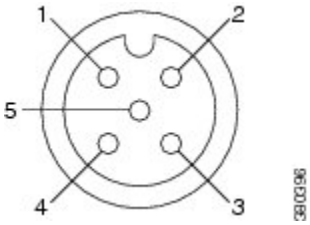
1	NC	3	DC–
2	DC+	4	NC

Alarm Connector

You connect the alarm signals to the switch through the alarm connector. The switch supports one alarm output relay.

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. The alarm output is rated at 24Vdc/1A, 48Vdc/0.5A maximum.

Figure 5: Alarm Connector



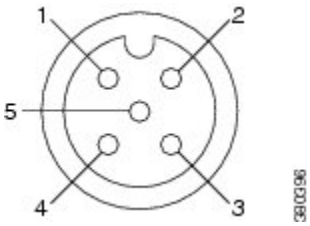
1	NO Alarm Output Normally Open (NO) connection	4	Alarm In Reference
2	NC Alarm Output Normally Closed (NC) connection	5	COMMON Alarm Common connection
3	Alarm In		

Console Management Port

You can connect the switch to a PC running Microsoft Windows or to a terminal server through the 5-pole A-coded console port and configure it by using the CLI. The baud rate and format of the console port is:

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

Figure 6: Console Connector



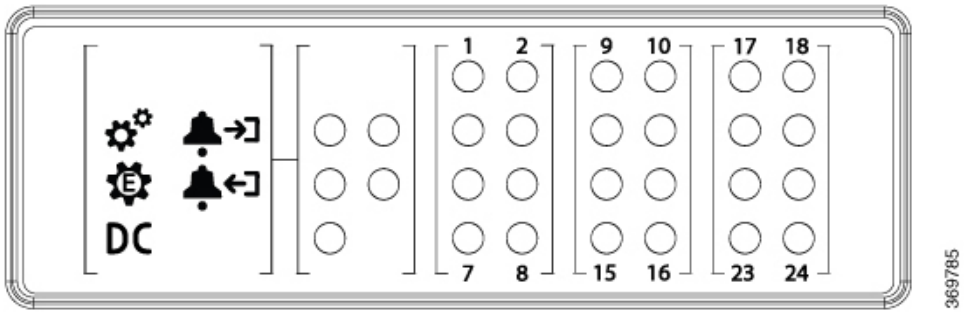
1	RTS	4	RXD
2	CTS	5	GND
3	TXD		

Note For specified cable, use Cisco Product CAB-CONSOLE-M12=

LEDs

You can use the LEDs to monitor overall system status and power supply input and output status as well as port and alarm status.

Figure 7: Switch LEDs



System LED

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

Table 2: System LED

Color	Status
Off	Switch is not powered on.
Blinking green	Boot fast (power-on self test) is in progress.
Green	Switch is operating normally.
Red	Switch is not functioning properly.

Express Setup LED

The Express Setup LED displays the status of the initial setup for the initial configuration.

Table 3: Setup LED

Color	Status
Off (dark)	Configured as a managed switch.
Solid green	Operating normally running the initial setup configuration.
Blinking green	Performing the initial setup, in recovery, or the initial setup is incomplete.
Solid red	Failed to start initial setup or recovery because there is no available port to link the switch to the management station. Disconnect a device from a switch port, and then press the Express Setup button.

Power Status LEDs

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.

Table 4: Power Status LEDs

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	An alarm has been configured to indicate that power is not present on the associated circuit or the power input dropped below the lowest valid level.

For information about the power LED colors and behaviors during the boot fast sequence, see the "LEDs" section.

Alarm LEDs

The following table list the alarm LED colors and their meanings.

Table 5: Alarm Out Status LEDs

Color	System Status
Off	Alarm out is not configured or the Switch is off.
Green	Alarm out is configured, no alarms detected.
Blinking red	Major alarm detected.
Red	Minor alarm detected.

Port Status LEDs

Each 10/100BASE-T or 10/100/1000Base-T port (identified by numbers 1-23, depnding upon the the model) has a port status led.

Table 6: Port Status LEDs

Color	Status
Off	No link.
Solid green	Link present. No activity.
Blinking green	Port is actively sending or receiving data.
Alternating green-amber	Link fault. Errors that affect connectivity and throughput, such as excessive collisions, CRC errors, and alignment and jabber errors, are monitored.

Solid amber	Port is not forwarding. The port was disabled by management, an address violation, or STP. **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds while STP checks the switch for loops.

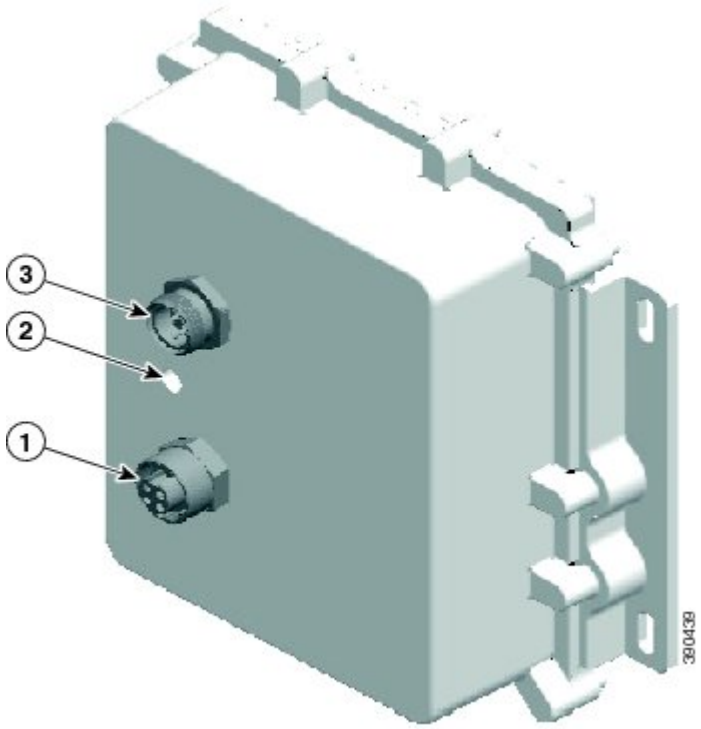
IP67 Power Supply

The switch is offered with optional IP67 power supplies, (PWR-IE160W-67-DC=) and (PWR-IE180W-67-AC=). The IP67 DC power supply can take 18 to 60Vdc input and provide a 54V, 160W DC output. The IP67 AC power supply can take 85-264VAC/ input and provide a 54V, 180W DC output. There are also non-IP67 power supplies compatible with the switch.

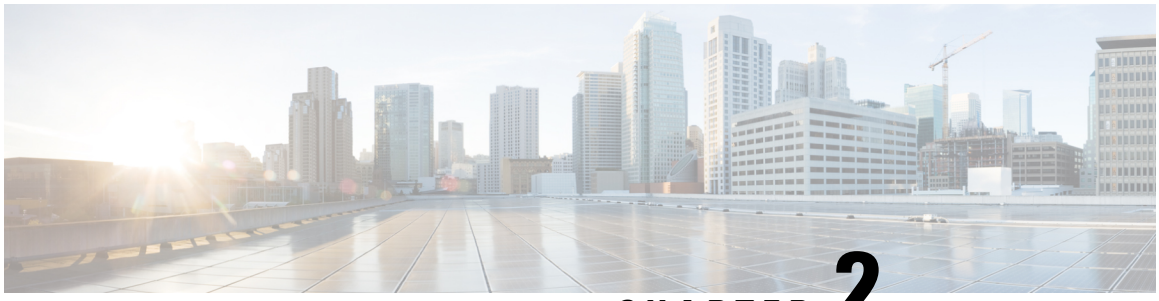
Note The power supplies are sold separately.

The following figure displays the IP67 Power Supply.

Figure 8: Cisco IP67 Power Supply



1	DC output connector	3	DC input power connector
2	Status LED		



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.

We recommend performing a preliminary configuration of the switch before it is installed in a permanent location.

Preparing for Installation

Warnings

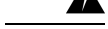
These warnings are translated into several languages in the Regulatory Compliance and Safety Information for this switch.

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 DC circuit. 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. Statement 1017

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

Warning Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950 based safety standards. Statement 1033

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, Console, and Alarm Statement 1044

Warning To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 140°F (60°C) 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)

Caution If installer is providing cabling for an IP66/IP67 and Type 4X rated environment, the cables must be suitably rated for IP66/IP67 and Type 4X requirements

EMC Environmental Conditions for Products Installed in the European Union

This section applies to products to be installed in the European Union.

The equipment is intended to operate under the following environmental conditions with respect to EMC:

- A separate defined location under the user's control.
- Earthing and bonding shall meet the requirements of ETS 300 253 or CCITT K27.
- AC-power distribution shall be one of the following types, where applicable: TN-S and TN-C as defined in IEC 364-3.

In addition, if equipment is operated in a domestic environment, interference could occur.

Installation Guidelines

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

Environment and Enclosure Guidelines

Review these environmental and enclosure guidelines before installation:

- 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.

Caution To meet IP67 Compliance, all cables, dust caps, or the captive screws on the SD card cover must be torqued to the recommended spec before operating the unit. For torque specs see "Cisco IE 2000 IP67 Series Switches Technical Specifications"

Caution Use caution when removing dust caps. Dust caps in an over-tightened state may adhere to the connector O-ring seal. Ensure that the O-ring remains in place when dust caps are removed and follow all torque specs here: "Cisco IE 2000 IP67 Series Switches Technical Specifications"

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.

- 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.

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 "Where to Go Next" section on page 14 .
- For 10/100 ports and 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).
- Operating environment is within the ranges listed in Appendix F, "Technical Specifications."
- 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)
- Ambient temperature does not exceed 140°F (60°C).
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.

Verifying Package Contents

Included in the box is the switch itself and it's installation documentation. If any item is missing or damaged, contact your representative or reseller for support.

Tools and Equipment

Obtain these necessary tools and equipment:

- A single or a pair of stud size 6 ring terminals (Hollingsworth part number R3456B or equivalent) for use as a protective ground connector.
- Crimping tool (Thomas & Bett part number WT2000, ERG-2001 or equivalent).
- 10-gauge copper ground wire.
- UL- and CSA-rated, style 1007 or 1569 twisted-pair copper appliance wiring material (AWM) wire for DC power connections.
- Wire-stripping tools for stripping 10-, 16-, and 18-gauge wires.
- Number-2 Phillips screwdriver.
- Flat-blade screwdriver.
- 15mm 12pt socket for IP67 dust caps

- Torque Driver (Such as a Torqueleader TT500 or equivalent)

Installing or Removing the Memory Card (Optional)

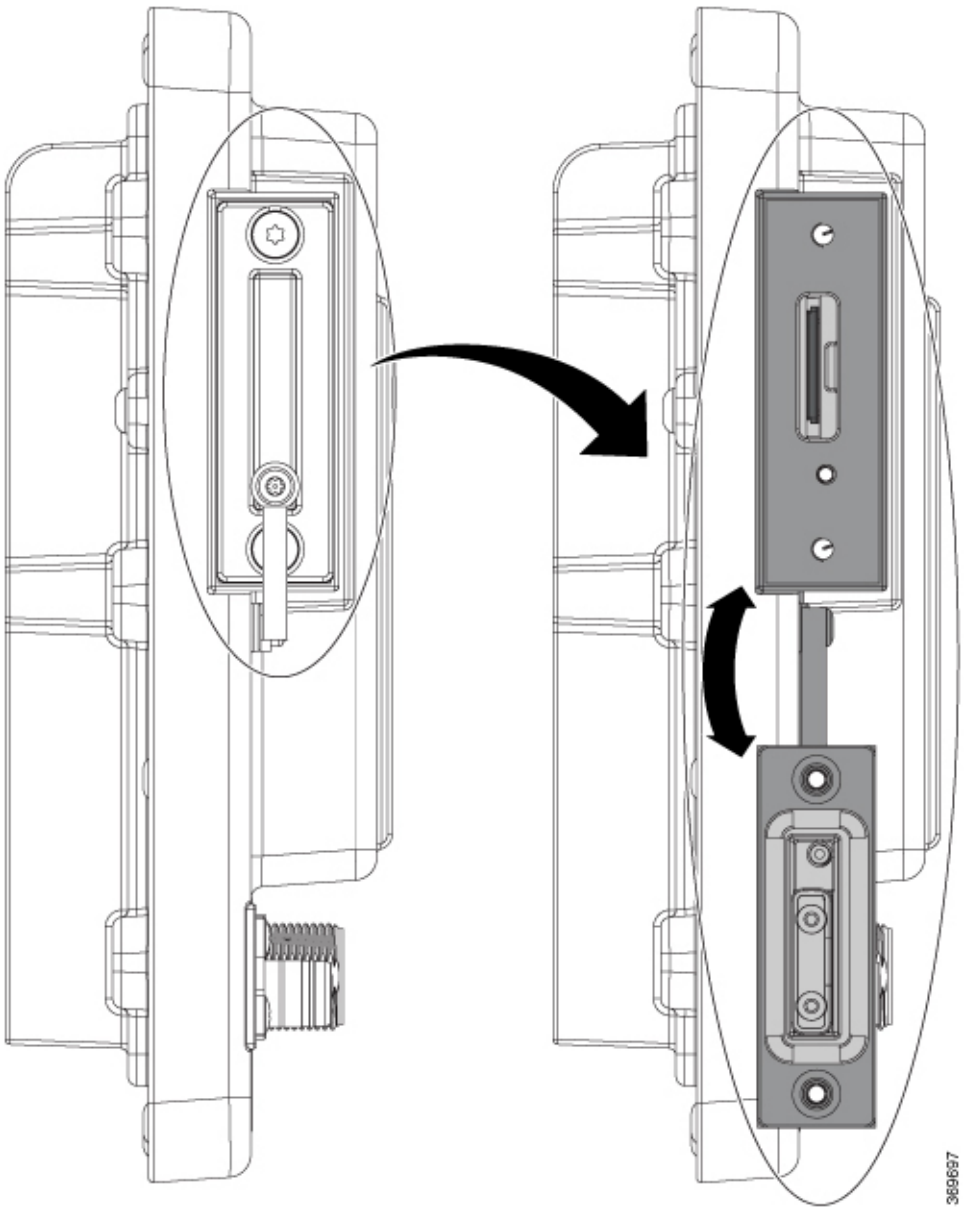
The switch supports a hot-swappable SD memory card (SD-IE-4GB) firmware and the startup configuration are stored, making it possible to replace a failed switch without reconfiguring the replacement switch.

The SD memory card cover protects the flash card against shock and vibration by holding the card in place. The cover is attached via lanyard, and secured with captive screws. The slot for the SD memory card is located on the side of the switch.

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

Procedure

Step 1 On the side of the switch, loosen the captive screws until they are free of the chassis. See the following figure.



Step 2 Install or remove the card:

- 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.
- To install a card, slide it into the slot, and press on it until it clicks in place. The card is keyed so that you cannot insert it the wrong way.

Step 3 Close the guard door and fasten the captive screws to 15.93 to 19.47 in/lbs (1.8 -2.2Nm) to maintain IP67 compliance.

Connecting a PC or Terminal to the Console Port

To configure the device, you can connect a PC or terminal to the console port and enter Cisco IOS commands through the CLI. This section describes the procedure for connecting a PC to the console port and using a terminal emulator application, such as PuTTy or Hyperterminal, to configure the device.

Procedure

Step 1 Connect the 5-pole-to-DB-9 adapter cable (Cisco PID CAB-CONSOLE-M12=) to a 9-pin serial port on a PC. Connect the other end of the cable to the switch console port.

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

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

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

Step 4 Connect power to the switch as described in Connecting to Power, on page 15.

Step 5 The PC or terminal shows the status of the bootup sequence. The switch will auto boot. When the IOS XE software has completed the bootup process the words "Press RETURN to get started!".

Note If you plan to use the Plug N Play (PNP) agent for automating day 1 install, then do not press return. this stops the automated install of PNP. Press return only to use the CLI to complete the Day 1 install process.

Step 6 To ensure IP67 compliance, make sure all console dust caps and cables are in place and torqued to 4.43 to 7.08 in/lbs (0.5 to 0.8 Nm).

Connecting to Power

You must supply a power solution for the device. The input voltage should be between 9.6V and 60Vdc

If a custom power supply is used, use the power cable with pig tail ends. Connect the female end of the circular mini-change cable to the power connector on the switch (torque = 10in/lbs) and connect the pigtail to the non-standard power supply.

Warning This product relies on the building’s installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 10 A Statement 1005

The recommended torque to achieve IP67 compliance is 10 in-lbs (1.13 Nm) for the power input connector on the switch, power output and input connector on the Cisco IP67 power supply.

Grounding the Switch

Follow any grounding requirements at your site.

Danger 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 10AWG wire (Hollingsworth part number R3456B or equivalent).

Caution Use at least a 4 mm 2 conductor to connect to the external grounding screw.

A ground lug is not supplied with the switch. You can select from these options:

- Single ring terminal
- Two single ring terminals

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

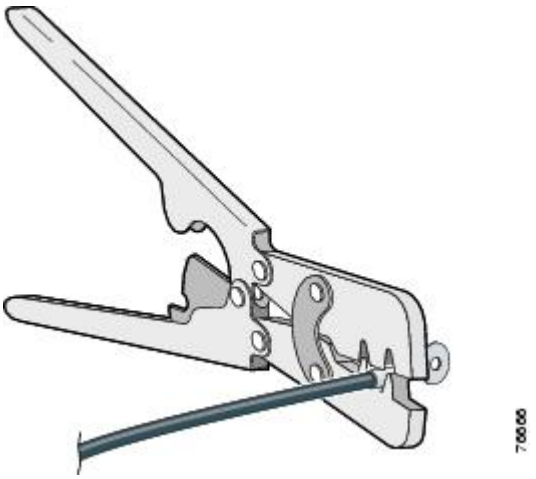
Procedure

Step 1 Use a standard Phillips screwdriver or a ratcheting torque screwdriver with a Phillips head to remove the ground screw from the switch. Store the ground screw for later use.

Step 2 Use the manufacturer guidelines to determine the wire length to be stripped.

Step 3 Insert the ground wire into the ring terminal lug, and using a crimping tool, crimp the terminal to the wire. See the following figure. If two ring terminals are being used, repeat this action for a second ring terminal.

Figure 9: Crimping the Ring Terminal



Step 4 Slide the ground screw through the terminal.

Step 5 Insert the ground screw into the ground screw opening.

Step 6 Use a ratcheting torque screwdriver to tighten the ground screws and ring terminal to the switch front panel to 3.5 in-lb (0.4 N-m). The torque must not exceed 3.5 in-lb (0.4 N-m).

Step 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.

Connecting the earth ground wire

Procedure

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

Note For connections from the power supply to earth ground, use 10 to 12-AWG stranded copper wire.

Step 2 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.

Connect the other end of the wire to the grounding screw on the power supply. Only wire with insulation should extend from the connection.

Note The position of the power supply may vary on different switch models.

Step 3 Tighten the earth-ground wire connection screw.

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

Running Express Setup

Use Express Setup to enter the initial IP management information. You can then access WebUI on the switch by pointing your broswer to the switch IP address to complete the Day 1 configuration.

You need this equipment to set up the switch:

- Computer running Windows or a Mac.
- A web browser with JavaScript enabled.

  Google Chrome 38 or later, Mozilla Firefox 35 or later, or Apple Safari 7 or later.
- Straight-through or crossover Category 5 or 6 cable
- A small paper clip to reach the button.

Note The cable should have M12 Xcode or Dcode connector on one end and RJ45 on the other. Xcode cable is for Models IE-3400H-8T, IE-3400H-16T, and IE-3400H-24T. The Dcode cable is for models IE-3400H-8FT, IE-3400H-16FT, and IE-3400H-24FT.

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

To run Express Setup:

Procedure

Step 1 Make sure that nothing is connected to the switch, and the cover for the SD card has been removed (see Installing or Removing the Memory Card (Optional), on page 13).

During Express Setup, the switch acts as a DHCP server. If your PC has a static IP address, write down the PC static IP address and temporarily configure your PC settings to use DHCP before going to the next step.

Step 2 Connect power to the switch.

See the instructions in the Connecting to Power, on page 15.

The boot sequence begins. This process can take up to 90 seconds. During boot fast, the SYS LED blinks green, and the other LEDs turn steady green. When boot fast is complete, the SYS LED turns steady green, and the Express Setup LED starts to blink green.

If the SYS LED is off (system not powered on), continues to blink green (POST in progress), or is solid red (Fault), contact the Cisco Technical Assistance Center (TAC).

Step 3 Press the Express Setup button (located next to the SD Card slot, under the cover) for 2 to 3 seconds. This button is recessed behind the panel, so you can use a simple tool, such as a paper clip.

When you press the Express Setup button, switch port 1/1 begins blinking green.

Step 4 Connect a Category 5 Ethernet cable (not provided) to the top left port on the switch to the Ethernet port on your PC. on the switch its always the top left port regardless of model.

The port LEDs on your PC and on the switch blink green while the switch configures the connection. The steady green port LEDs indicate a successful connection.

If the port LEDs do not turn green after about 30 seconds, make sure that:

- You connected the Ethernet cable to the top left port labeled 1/1.
- You are using an undamaged Category 5 or 6 Ethernet cable.
- The other device is turned on.

Step 5 Start a browser session on the PC. A login prompt appears.

Step 6 Enter IP address 192.168.1.254 into the browser URL bar. If a security warning appears, click to accept the risk and proceed. A login prompt appears.

Step 7 Username is 'admin', and password is the system serial number found on the side of the switch next to the SD card cover.

The Configuration Setup Wizard Setup web page appears.

If it does not appear, make sure that any pop-up blockers or proxy settings on your browser are disabled and that any wireless client is disabled on your PC.

Step 8 The first of four web pages appears. You need to navigate through all four web pages to complete express setup. In the Account Settings page, provide values for all fields with "*" .

- Enter a Login Name.
- Command Line Password should be set to **Sync to Login Password** from the dropdown menu.
- Date & Time is optionally set to **NTP Time** from the dropdown menu.

Step 9 Click **Basic Settings** once the settings are correct.

The **Basic Settings** window is displayed.

- Enter an IP address. (This field is mandatory).
- SSH: click the enable box.
- *(Scroll down using right side scroll bar to address all mandatory fields)*

Step 10 Click **Switch Wide Settings**.

The **Switch Wide Settings** window is displayed *(No required fields on this page)*.

Step 11 Click **Summary**.

The **Summary** window is displayed.

Step 12 Verify the information displayed in the summary is correct, and when ready click **Submit**.

In case of an error do the following:

- Verify connectivity:
  - Open a command prompt, type ping 192.168.1.254, all replies should be received.
  - Do not unplug PC from the switch
- In case of error or to return IE switch to Manufacturing defaults:
  - The IE Switch can be returned to mfg defaults by inserting paper clip (or equivalent) into Express Setup recess for 15-20 seconds, observe the Express Setup LED, remove the paper clip when it flashes alternating orange/green.
  - After 15 seconds release paper clip, IE switch will auto reload.
  - After reboot, IE switch will be in factory defaults. Wait approximately 120 seconds.
  - Express Setup LED blinks orange, which means reloading factory defaults.
  - When Express Setup LED blinks green, restart the Express Setup procedure.

Note The Express setup long press (pressing 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). Remove any removable media if you do not want any files to be deleted from the SD card.

- Reset procedure
- Screen naming vs power page naming
- PC disconnect, start over

What to do next

You can now manage the switch by using WebUI, or CLI.

Launching WebUI

Display WebUI by following these steps:

Procedure

Step 1 Start a web browser on your PC or laptop.

Step 2 Enter the switch IP address, username, and password (assigned previously in Step 8) in the web browser, and press **Enter**. The WebUI page appears.

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 PC 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 PC.
- Make sure that the switch IP address in the browser is correct.
- Configure a static IP address on the PC that is in the same subnetwork as the switch IP address.
- When the LED on the switch port connected to the PC or laptop is green, reenter the switch IP address in a web browser to display the WebUI.

Connecting Alarm Circuits

After the switch is installed, you can connect the alarm.

For instructions on grounding the switch and connecting it to power, see the Connecting to Power, on page 15.

Wiring the External Alarms

Use M12 A-coded cable to connect to the alarm connector on the switch. Recommended torque is 4.43 to 7.08 in/lbs (0.5 to 0.8 Nm).

The recommended cable part number from Molex is 1200650523. One end of the cable has M12 A-coded connector and the other end is open.

The labels for the alarm connector are on the switch panel and are displayed in the following table.

Table 7: Alarm Connector Labels (Top to Bottom)

Pin	Label	Connection
1	NO	Alarm Output Normally Open (NO) connection
2	NC	Alarm Output Normally Closed (NC) connection
3	UNCONNECTED	Unused
4	UNCONNECTED	Unused
5	COMMON	Alarm Common connection

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, 1.0 A or 48 VDC, 0.5 A.

Connecting Destination Ports

These section provides information about connecting to the destination ports.

Caution IP66/IP67 UL50E Type 4X compliant only when all cables are mated and torqued appropriately or with the supplied dust caps attached.

Connecting to 10/100 and 10/100/1000 Ports

The 10/100 and 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 linkage.

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.
- For connecting Ethernet cables to models IE-3400H-8FT, 16FT, & 24FT use cables with D-code M12 connectors.
- To connect Ethernet cables to Models IE-3400H-8T, 16T, & 24T use cables with X-code M12 connectors.

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:

Procedure

Step 1 When connecting to workstations, servers, routers, and Cisco IP phones, connect a straight-through cable to a M12 connector (IP67 Torque: 4.43 to 7.08 in/lbs or 0.5 to 0.8 Nm) on the front panel. See Figure 1-2 .

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.

Step 2 Connect the other end of the cable to a M12 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 Chapter 4, “Troubleshooting,” for solutions to cabling problems.

Step 3 Reconfigure and reboot the connected device if necessary.

Step 4 Repeat Steps 1 through 3 to connect each device.

Step 5 To ensure IP67 compliance, make sure all alarm dust caps and cables are in place and torqued to 4.43 to 7.08 in/lbs (0.5 to 0.8 Nm).

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:

- WebUI

  You can use WebUI web interface to manage and monitor individual switches. Device Manager can be accessed from anywhere in your network through a web browser by using the management IP address of the switch. For more information, see the Device Manager online help.

- Cisco IOS-XE CLI

  The switch CLI is a version of Cisco iOS firmware that can be used to configure and monitor the switch. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station.

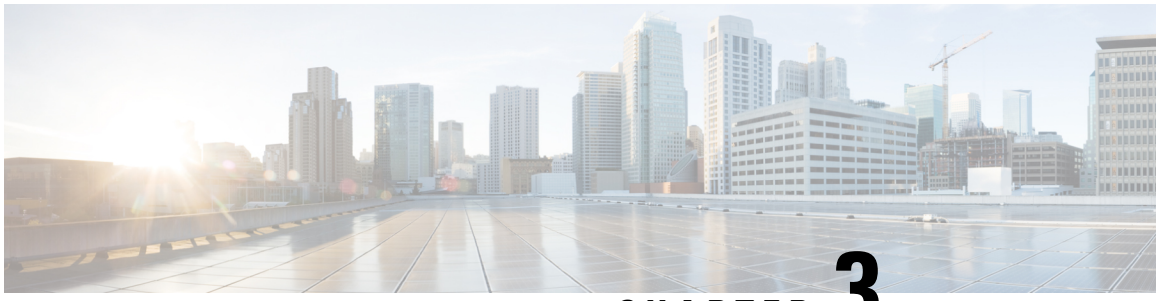
- Cisco DNA Center that can be found at: https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html

- SNMP

  Switches can be managed by using a SNMP-compatible management station 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.

- Common Industrial Protocol

Common Industrial Protocol (CIP) management objects are supported by the switch, allowing you to manage an entire industrial automation system with one tool.



CHAPTER 3

Switch Mounting

Switch Mounting

This chapter describes how to mount the switch.

Mounting the Switch

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 the Wall

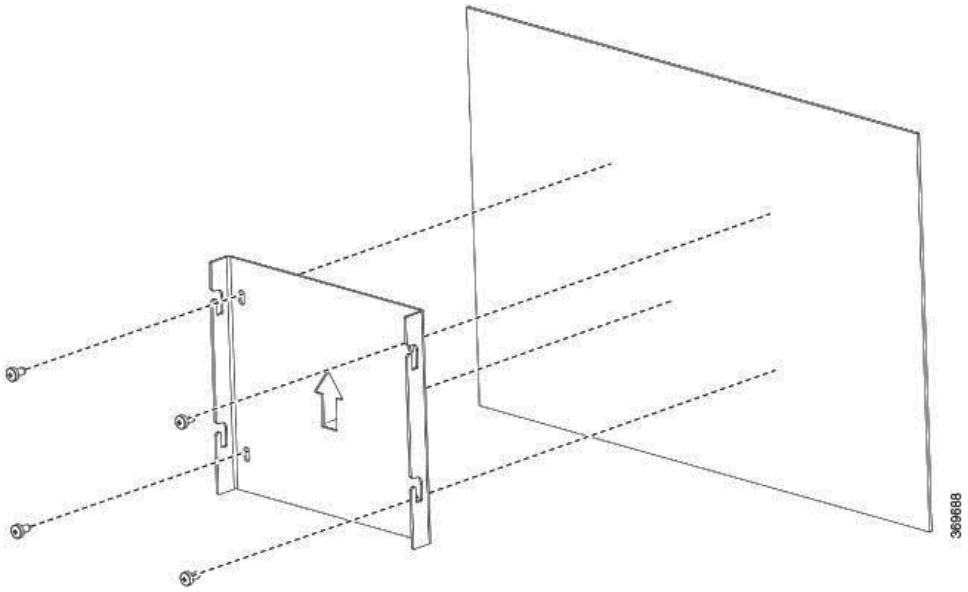
To attach the switch to a wall or a panel, follow these steps.

Warning Read the wall-mounting instructions carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system. Statement 378

Procedure

Step 1 Position the switch mounting bracket against the wall or a panel in the desired location, with the arrow pointing up. See the following figure. Attach the bracket to the wall with the 4 enclosed Philips screws.

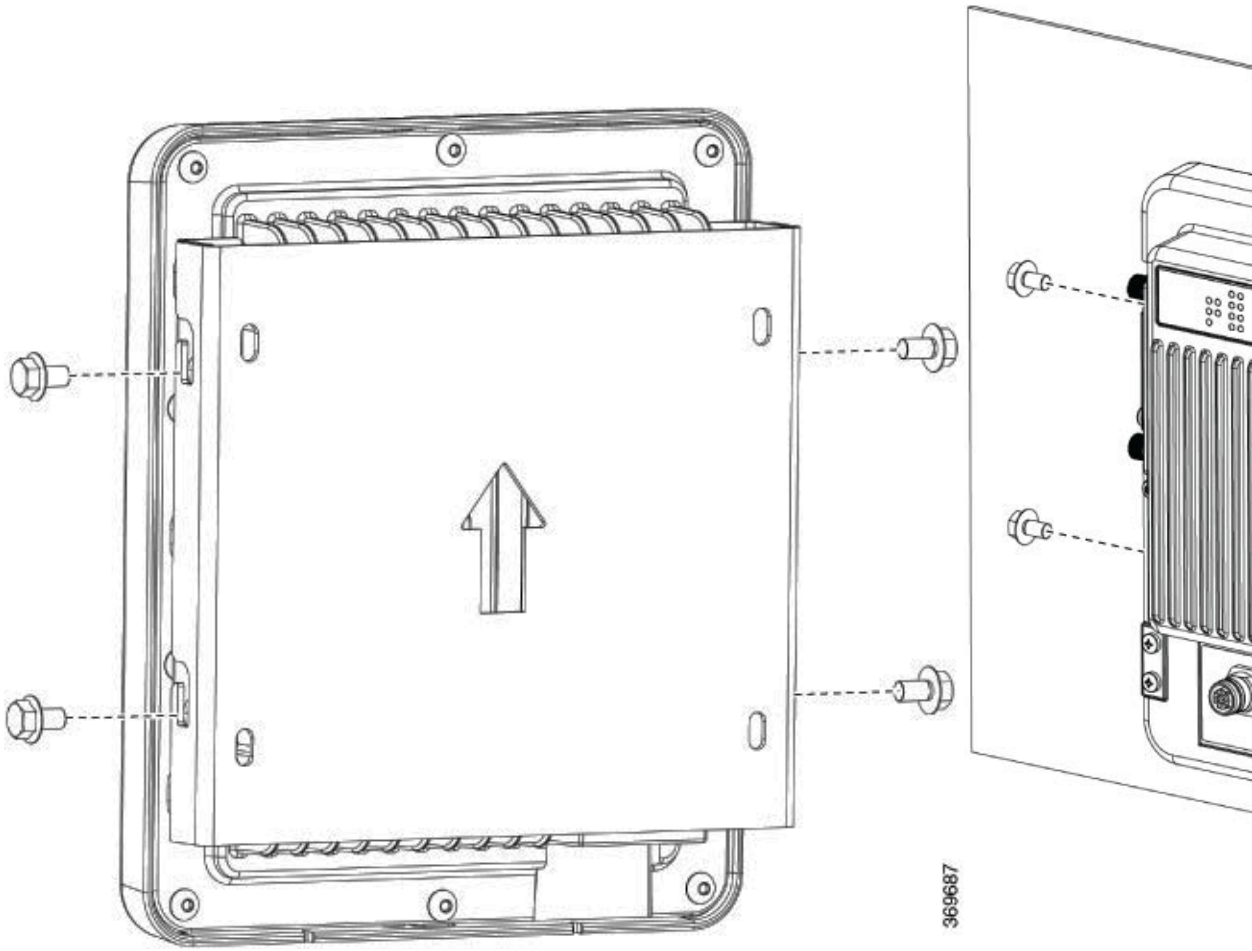
Figure 10: Mounting Wall Bracket to Wall



Note When attaching the bracket to the wall or pannel, ensure that the screws engage a stud or support structure capable of supporting the weight of the bracket and the switch.

Step 2 Loosly attach the 4 mounting screws to the switch and slide it into the bracket and down. See the following figure.

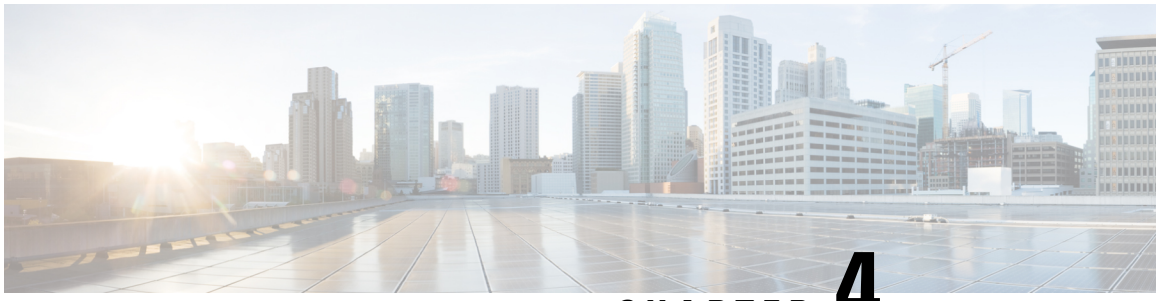
Figure 11: Attaching the Switch to the Mounting Bracket



Step 3 To remove the switch, loosen the 4 mounting screws and slide the switch up and forward, out of the mounting bracket. Then the bracket itself can be unscrewed from the wall, if necessary.

What to do next

After the switch is mounted on the wall or panel, connect the power and alarm wires, as described in the "Connecting Alarm Circuits" section on page -12 .



CHAPTER 4

Configuring the Switch with the CLI Setup Program

Entering the Initial Configuration Information

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

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 32.

Before connecting the switch to a power source, review the safety warnings in Warnings.

To connect a PC to the console port of the switch, see Connecting a PC or Terminal to the Console Port, on page 15.

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
- SSH 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 32 or Initial Configuration - Type-7 Encryption, on page 36. To configure system security settings without running the initial setup, see Setting the Password Encryption Level, on page 39.

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 Connecting a PC or Terminal to the Console Port, on page 15.

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 Connecting a PC or Terminal to the Console Port, on page 15.

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
!
```

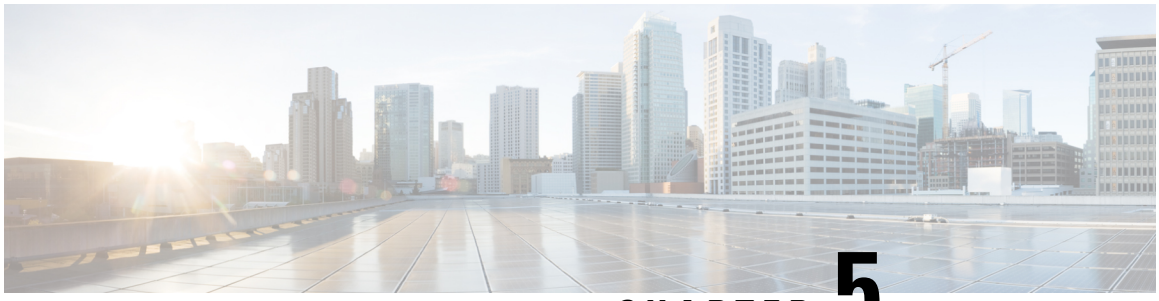
```
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4


[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

Troubleshooting

This chapter provides troubleshooting recommendations.

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 Device Manager, the CLI, or an SNMP workstation.

Switch Connections

Bad or Damaged Cable

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 cable with a known good cable.
- Look for broken or missing pins on cable connectors.
- Rule out any bad patch panel connections or media converters between the source and the destination. If possible, bypass the patch panel.
- Try the cable in another port to see if the problem follows 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.
- Look for loose connections. Sometimes a cable appears to be seated but is not. Disconnect the cable, and then reconnect it.

10/100 and 10/100/1000 Port Connections

If a port appears to malfunction:

- Verify the status of all ports. See Table 1-1 for descriptions of the LEDs and their meanings.
- 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.

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 notification that the traffic was received 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 “Information About UDLD” section in the IOS-XE Software Configuration guide for the Cisco Catalyst IE 3x00 Switches, 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, a common issue when duplex and speed settings are mismatched between 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 to the same speed and duplex mode. If this does not solve the problem, there could be a problem with the firmware or software on the NIC. You might 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.

Resetting the Switch

Resetting the switch deletes the configuration and reboots the switch.

Reasons why you might want to reset the switch to the factory default settings include:

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

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:

Procedure

Step 1 Press and hold the Express Setup button for 15 seconds or more. The switch reboots. The system led turns green and the expres setup led starts to blink green.

Step 2 Press the Express Setup button again for 1-3 seconds. LED for port 1/1 blinks green.

The switch now behaves like a factory-default configured switch. Go to section above on Express Setup to complete re-install.

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.
```

How to Recover Passwords

Password recovery is a feature that a system administrator can enable or disable. If password recovery is disabled, the only way to recover from a lost or forgotten password is to clear the switch configuration entirely. For this procedure, see the "Resetting the Switch" section.

Troubleshooting Express Setup

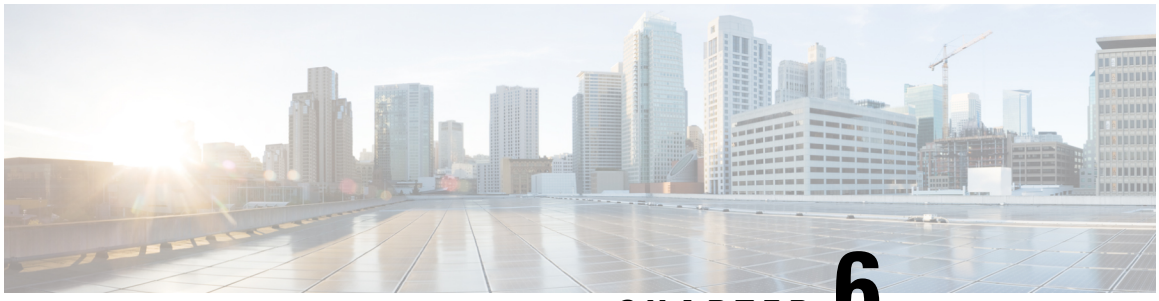
This section provides troubleshooting tips for the initial switch configuration.

Checklist	Recommendation
Was the SETUP LED blinking when you pressed the Express Setup button?	If no, or you are not sure, restart the switch. Make sure that the SETUP LED is blinking when you press the Express Setup button.
Did you connect your PC to the wrong switch port?	Verify that you are connected to the switch port with the blinking LED.
Did you start a browser session on your PC before the SETUP LED was solid green?	If yes, or you are not sure, restart the switch, and repeat the Express Setup procedure.
Did you start a browser session on your PC and the setup page did not appear?	If the window does not appear, enter a URL in your browser, such as *Cisco.com* or another well known website.
Did you have a pop-up blocker running on your PC when you connected to the switch port?	If yes, disconnect the cable from the switch port, disable the pop-up blocker, press the Express Setup button, and reconnect the cable to the blinking Ethernet port.

Checklist	Recommendation
Did you have proxy settings enabled in your browser software when you connected to the switch port?	If yes, disconnect the cable from the switch port, disable the proxy settings, press the Express Setup button, and reconnect the cable to the blinking Ethernet port.
Did you have a wireless client running on your PC when you connected to the switch port?	If yes, disconnect the cable from the switch port, disable the wireless client, press the Express Setup button, and reconnect the cable to the blinking Ethernet port.
Do you need to change the switch IP address after you have already completed the initial setup?	Go to the **Configure > Express Setup** Device Manager screen to change the switch IP address. For more information about changing the switch IP address, see the Cisco IE 2000 Switch Software Configuration Guide at Cisco.com.

Finding the Switch Serial Number

If you contact Cisco Technical Assistance, you need to know the serial number of your switch. The serial number is on the compliance label on left hand side under the removeable door. You can also use the **show version** privileged EXEC command to obtain the switch serial number.



CHAPTER 6

Technical Specifications

Technical Specifications

This appendix provides the technical specification for the Cisco Catalyst IE3400 Heavy Duty Series switches.

Operating Temperature Specifications

The following table lists the operating temperatures for the Cisco Catalyst IE3400 Heavy Duty Series switches in three different environments.

Table 8: Operating Temperature for the Cisco Catalyst IE3400 Heavy Duty Series switches

	Industrial Automation and Other Locations Requiring Enclosures	Substation	Traffic Signal
Enclosure types	Sealed enclosures For example: NEMA4, NEMA4X, NEMA12, NEMA13, IP54, and IP66.	Vented enclosures For example: NEMA1, IP66, and IP67.	Fan or blower-equipped enclosures For example: NEMA TS-2. **Note** The minimum airflow is 200 lfm[1].

[1] lfm = linear feet per minute.

Note The safety certifications apply only to ambient temperatures under 140°F (60°C). However, the Cisco Catalyst IE3400 Heavy Duty Series switches can function in the substation and traffic signal installations under the environmental conditions shown in the following table.

Technical Specifications

The technical specifications for the Cisco Catalyst IE3400 Heavy Duty Series switches are as follows:

Table 9: Cisco Catalyst IE3400 Heavy Duty Series Technical Specifications

Environmental Ranges	
Storage temperature	–40 to 185°F (–40 to 85°C)
Operating temperature (measured inside enclosure, 1” below the bottom surface of the switch)	–40 to 167°F (–40 to 75°C) **Caution** Operating temperatures exceeding 60C are not covered by the product safety certifications and approvals. • -40C to +70C (Vented Enclosure Operating) • -40C to +60C (Sealed Enclosure Operating) • -34C to +75C (200 LFM or more Fan or Blower equipped Enclosure Operating) • -40C to +85C (Type Tested to +85C for 16 hours)
Operating humidity	5 to 95% (noncondensing)
Ingress Protection/Type Ratings	IP66 and IP67 Rated for protection against dust and submersion in water NEMA type 4x **Caution** IP66 and IP67, NEMA type 4x compliant only when all IP67 cables are mated and torqued appropriately or with the supplied dust caps attached.
Operating altitude	Up to 15,000 feet (4570 meters)
Storage altitude	Up to 40,000 feet (4570 meters)

Table 10: Power Specifications

Power Specifications	**IE-3400H-8FT**	**IE-3400H16FT**	**IE-3400H-24FT**	**IE-3400H-8T**	**IE-3400H-16T**	**IE-3400H-24T**
Marked Input voltage range	12 to 48VDC	12 to 48VDC	12 to 48VDC	12 to 48VDC	12 to 48VDC	12 to 48VDC
Input voltage range (Absolute)	9.6 to 60VDC	9.6 to 60VDC	9.6 to 60VDC	9.6 to 60VDC	9.6 to 60VDC	9.6 to 60VDC
Input current @ (9.6V / 60V)	3.0A/0.51A	4.0A/0.65A	4.6A/0.75A	3.2A/0.54A	4.4A/0.71A	5.1A/0.83A
Power consumption @ (9.6V / 60V)	28.8W/30.6W	38.4W/39.0W	44.2W/45.0W	30.4W/32.2W	41.6W/42.3W	49.0W/49.8W

Table 11: Physical Configurations

Physical Specifications	IE-3400H-8FT	IE-3400H-8T	IE-3400H16FT	IE-3400H-16T	IE-3400H-24FT	IE-3400H-24T
Dimensions (H x W x D)	9.58 x 7.90 x 3.15 in. 24.33 x 20.07 x 8.00 cm	9.58 x 7.90 x 3.15 in. 24.33 x 20.07 x 8.00 cm	9.58 x 10.90 x 3.15 in. 24.33 x 27.69 x 8.00 cm	9.58 x 10.90 x 3.15 in. 24.33 x 27.69 x 8.00 cm	9.58 x 13.90 x 3.15 in. 24.33 x 35.31 x 8.00 cm	9.58 x 13.90 x 3.15 in. 24.33 x 35.31 x 8.00 cm
Weight (including mounting bracket)	8.45 lb 4.35 kg	8.45 lb 4.35 kg	11.25 lb 5.10 kg	11.25 lb 5.10 kg	13.90 lb 6.30 kg	13.90 lb 6.30 kg
Mounting	Wall mount	Wall mount	Wall mount	Wall mount	Wall mount	Wall mount

Connectors and Cabling

The connectors and cabling for the Cisco Catalyst IE3400 Heavy Duty Series switches are below.

Table 12: Cisco Catalyst IE3400 Heavy Duty Series Cables and Connectors

Data Ports	• Copper 100 Base-T M12 D coded 4 pole (pin) cable: M12 Male and/or M12/RJ-45 connector • Copper GE M12 X coded 8 pole (pin) shielded cable: M12 Male and/or M12/RJ-45 connector
Alarm Port	• Copper M12 A-Coded 5 Pin connector
Power Input	• Mini Style 4-pin connector for power input
Console Cable: CAB-CONSOLE-M12=	• Console Cable 6ft with M12 and DB9F for IE3400H Switch

Torque Specifications

The torque specifications for the Cisco Catalyst IE3400 Heavy Duty Series switches are below.

Table 13: Cisco Catalyst IE3400 Heavy Duty Series Torque Specs

Alarm, Console, Ethernet ports (M12 Connectors)	• 4.43 to 7.08 in-lbs (0.5 to 0.8 Nm)
M12 Connector Dust Cap (Alarm, Console, Ethernet ports)	• 3.5 in-lbs (0.4 Nm)
Power Supply Connector (Mini-Change)	• 10 in-lbs (1.13 Nm)

SD Card Access Door Captive Screws	• 15.93 to 19.47 in/lbs (1.8 -2.2Nm)

Alarm Ratings

The alarm ratings for the Cisco Catalyst IE3400 Heavy Duty Series switches are below.

Table 14: Cisco Catalyst IE3400 Heavy Duty Series Alarm Ratings

Alarm Ratings	Specification
Alarm	One alarm output relay using an M12 A Coded 5 Pin connector (Max. rated: 24VDC @ 1A / 48VDC @ 0.5A)