Cisco Catalyst IE3100H Heavy Duty Series Switch Hardware Installation Guide

First Published: 2025-08-08

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS

Preface

Audience

This guide is for the networking or computer technician responsible for installing Cisco Catalyst IE3100H 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

For additional documentation, see the Cisco Catalyst IE3100 Heavy Duty Series documentation at

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

Attention If the equipment is used in a manner not follow this installation guide, the protection provided by the equipment may be impaired.

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 **Statement 1071—**Warning Definition

IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number at the beginning of each warning statement to locate its translation in the translated safety warnings for this device.

SAVE THESE INSTRUCTIONS

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 IE3100H 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.

Communications, services, and additional information

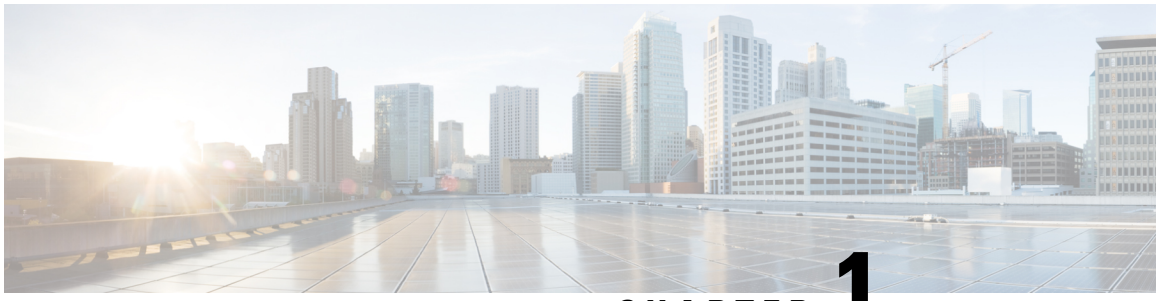
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



CHAPTER 1

Product Overview

Product Overview

Cisco Catalyst IE3100H Heavy Duty Series Switch is a IP66/IP67 rated compact entry-level managed L2 switch. The switch is specifically designed as an I/O Network Switch for PLC-level connectivity, available in 8 Gigabit Ethernet (X-coded) or 2 Gigabit Ethernet (X-coded) + 6 Fast Ethernet (D-coded) M12 interface models. These switches cater to deployments including of automotive manufacturing, food and beverage, clean rooms or other industrial environments that are required to be cleaned regularly with harsh-chemicals and support a 24x7 production process.

The switch is an enclosed type equipment, it can be wall mounted and deployed without a housing cabinet, under either indoor or outdoor environment with Pollution Degree 2.

Switch Models

Table 1: Cisco Catalyst IE3100H Heavy Duty Series Switch Model Features

Hardware Specifications	IE-3100H-8T-E	IE-3100H-6FT2T-E
100-Mbps D-coded ports	0	6
1-Gbps X-coded ports	8	2
Removable storage	SD card[1]	
Console ports	1x A-code M12	
Power input (Marked Rating)	12–48 VDC, 1.5 A	
Power Connector	1xL-Code M12	

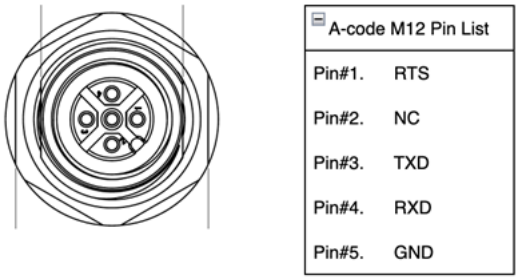
[1] The SD card is optional and is not shipped by default with the switch.

Console Management Port

You can connect the switch to a PC running Microsoft Windows or to a terminal server through the A-code M12 connector 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 1: Console Connector



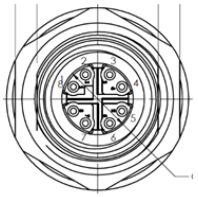
Note For specified cable, use Cisco Product CAB-CONSOLE-M12=

Ethernet Ports

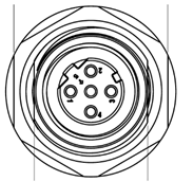
The Catalyst IE-3100H-8T-E switch has 8x Ethernet ports supporting 1000Base-T, 100Base-TX and 10Base-T with autonegotiation, auto-MDIX, and cable diagnostics on X-code M12 connectors.

The Catalyst IE-3100H-6FT2T-E switch has 2x 1Gigabit M12 X-code uplink Ethernet ports and 6x 10/100Mpbs M12 D-code downlink Ethernet ports.

Figure 2: M12 Ethernet Ports



X-code M12 Pin List	
Pin#1.	MDI1_P
Pin#2.	MDI1_N
Pin#3.	MDI0_P
Pin#4.	MDI0_N
Pin#5.	MDI2_P
Pin#6.	MDI2_N
Pin#7.	MDI3_N
Pin#8.	MDI3_P



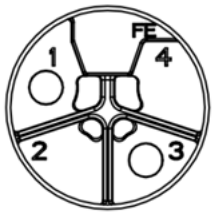
D-code M12 Pin List	
Pin#1.	TX+
Pin#2.	RX+
Pin#3.	TX-
Pin#4.	RX-

Power Connector

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

A Micro-Change (M12) Single-Ended Cordset, 4 Poles, L-Coded, Female power cord must be used to power the switch.

Figure 3: Power Connector



L-code M12 Pin List	
Pin#1.	DC+
Pin#2.	NC
Pin#3.	DC-
Pin#4.	NC

1	DC+	3	DC–
2	NC	4	NC

Note

- To meet UL 61010-2-201 UL Listing requirement, Amphenol ADAD-DLFS0400152 connectors must be used with the Cisco Catalyst IE3100H switch.
- CSA 61010-2-201 certification allow IE3100H use any CSA/UL approved M12 L-Code Female Plug

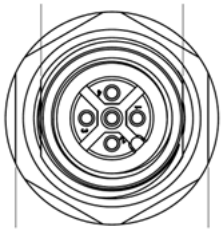
Console Management Port

You can connect the switch to a PC running Microsoft Windows or to a terminal server through the A-code M12 connector 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 4: Console Connector

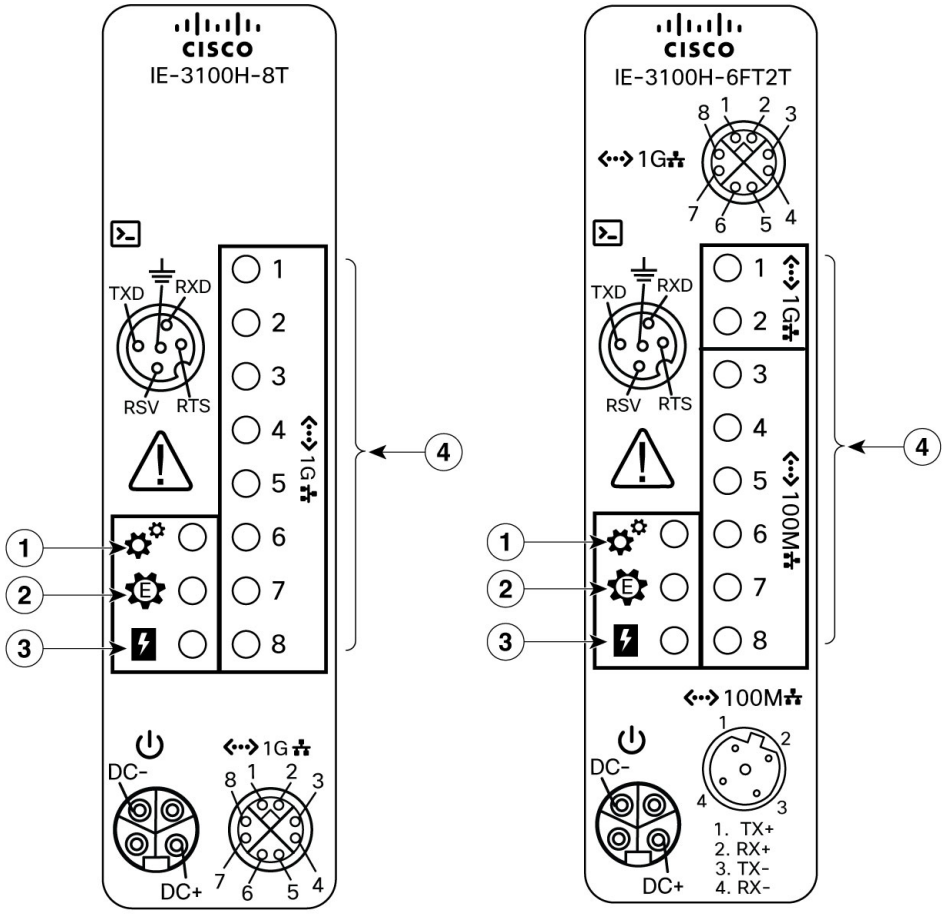


A-code M12 Pin List	
Pin#1.	RTS
Pin#2.	NC
Pin#3.	TXD
Pin#4.	RXD
Pin#5.	GND

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

LEDs

The LEDs display the overall system, power supply, and Ethernet port status.



1	System LED	3	Power LED
2	Express Setup LED	4	Ethernet Ports 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 Button

Express Setup is a web-based procedure to configure initial IP address information to the new switch. It provides a simple way to manage the switch and connect it to an existing network of local routers and the internet.

The Cisco Catalyst IE3100H Heavy Duty Series Switch front panel has an Express Setup button and a setup LED. The button is recessed to prevent accidental activation; you need a paper clip or similar object to press it. You trigger different Express Setup features by varying the amount of time that you press the button.

Table 3: Express Setup Modes

Mode	Seconds Required to Trigger Mode	Description
Short Press	1 to 5	Places the switch into Express Setup mode
Medium Press	6 to 10	Causes the switch to start DHCP discovery phase on the VLAN1 interface
Long Press	16 to 20	Causes the switch to erase its startup configuration and reload. This in turn causes the switch to revert to its Day 1 default configuration.

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

For more information, see Running Express Setup, on page 21.

Table 4: Express Setup LED Status

Color	Status
Black	System is UP
Blinking Green	Short Press
Blinking GREEN and RED Alternatively	Medium Press
Blinking GREEN(for 5 second), Blinking RED(for 5 more seconds), and OFF(BLACK for 10 to 15 seconds) then Blinking GREEN and RED	Long Press

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 5: 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.

Port status LEDs

Each 10/100BASE-T or 10/100/1000Base-T port (identified by numbers 1-8, depnding upon the the model) has a port status led.

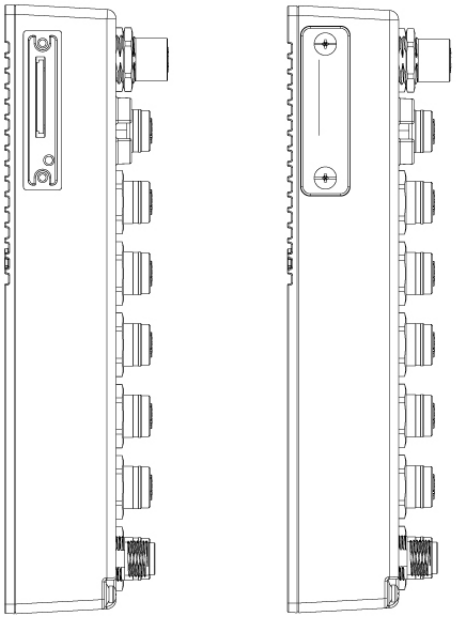
Table 6: Port status LEDs

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.

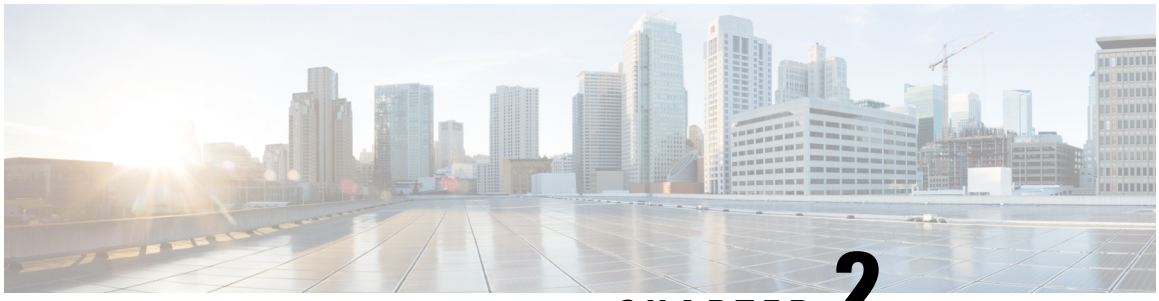
SD Card Connector

The switch supports an SD card that makes it possible to replace a failed switch without configuring the replacement switch. You can also use the SD card to copy files on and off the system.

Figure 5: SD Card slot and its cover



The connector is on the side of the switch, behind a cover that protects the SD card and holds it in place. The switch supports SD card of upto 16 GB storage capacity.



CHAPTER 2

Switch Installation

This chapter describes how to install your switch, verify the boot fast, and connect the switch to other devices.

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 **Statement 1003**—DC Power Disconnection

To reduce risk of electric shock or personal injury, disconnect DC power before removing or replacing components or performing upgrades.

Warning **Statement 1017**—Restricted Area

This unit is intended for installation in restricted access areas. Only skilled, instructed, or qualified personnel can access a restricted access area.

Warning **Statement 1033—**Safety Extra-Low Voltage (SELV)—IEC 60950/ES1–IEC 62368 DC Power Supply

To reduce the risk of electric shock, connect the unit *only* to a DC power source that complies with the SELV requirements in the IEC 60950-based safety standards or the ES1 requirements in the IEC 62368-based safety standards.

Warning **Statement 1074—**Comply with Local and National Electrical Codes

To reduce risk of electric shock or fire, installation of the equipment must comply with local and national electrical codes.

Warning **Statement 1079—**Hot Surface

This icon is a hot surface warning. To avoid personal injury, do not touch without proper protection.

Note **Statement 1089—**Instructed and Skilled Person Definitions

An instructed person is someone who has been instructed and trained by a skilled person and takes the necessary precautions when working with equipment.

A skilled person or qualified personnel is someone who has training or experience in the equipment technology and understands potential hazards when working with equipment.

Warning **Statement 1091—**Installation by an Instructed Person

Only an instructed person or skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of an instructed or skilled person.

Warning **Statement 9001—**Product Disposal

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

Note **Statement 407**—Japanese Safety Instruction

You are strongly advised to read the safety instruction before using the product.

https://www.cisco.com/web/JP/techdoc/pldoc/pldoc.html

When installing the product, use the provided or designated connection cables/power cables/AC adapters.

〈製品使用における安全上の注意〉

www.cisco.com/web/JP/techdoc/index.html

接続ケーブル、電源コードセット、**AC**アダプタ、バッテリなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外をご使用になると故障や動作不良、火災の原因となります。また、電源コードセットは弊社が指定する製品以外の電気機器には使用できないためご注意ください。

Caution Airflow around the switch must be unrestricted. To prevent the switch from overheating, there must be the following minimum clearances:– Top and bottom: 1.0 in. (25 mm)– Sides: 1.0 in. (25 mm)– Front: 1.0 in. (25 mm)

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

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:

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.
- 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 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: 1.0 in. (25 mm)
  - Sides: 1.0 in. (25 mm)

- Front: 1.0 in. (25 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.
- 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 firmware and the startup configuration are stored, making it possible to replace a failed switch without reconfiguring the replacement switch.

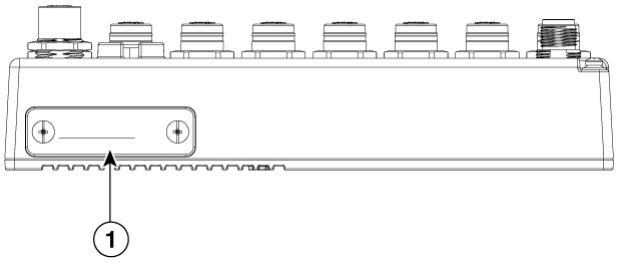
The SD memory card cover protects the flash card against shock and vibration by holding the card in place. The cover is attached via lanyard, and secured with captive screws. The slot for the SD memory card is located on the side of the switch.

Note The switch supports upto 16 GB capacity SD-card.

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.



1	SD card slot cover with captive screws (2x)

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 3.5 to 4.5 in-lbs (0.40 to 0.51 Nm) 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 console 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.

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.

Connecting to Power

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

If a custom power supply is used, use the power cable with pig tail ends. Connect the female end of the M12 Power L-code cable to the power connector on the switch (torque—0.60 Nm/5.3 in-lbs) and connect the pigtail to the non-standard power supply.

Grounding the Switch

Follow any grounding requirements at your site.

Warning **Statement 2004—**Grounded Equipment

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.

Note A ground lug is not supplied with the switch. Use a single ring terminal lug.

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

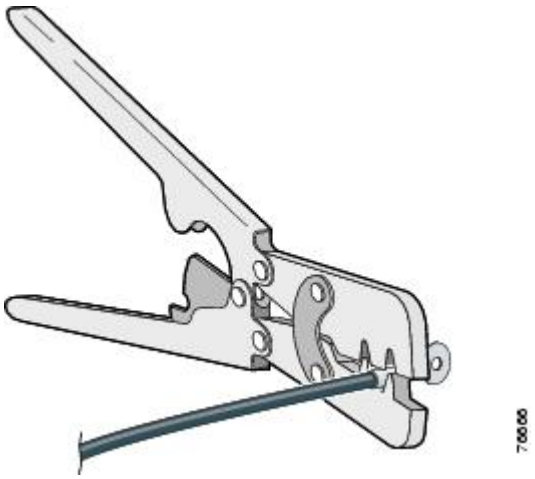
Procedure

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.

Figure 6: 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.

Connecting Destination Ports

These section provides information about connecting to the destination ports.

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.

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.

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.

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.

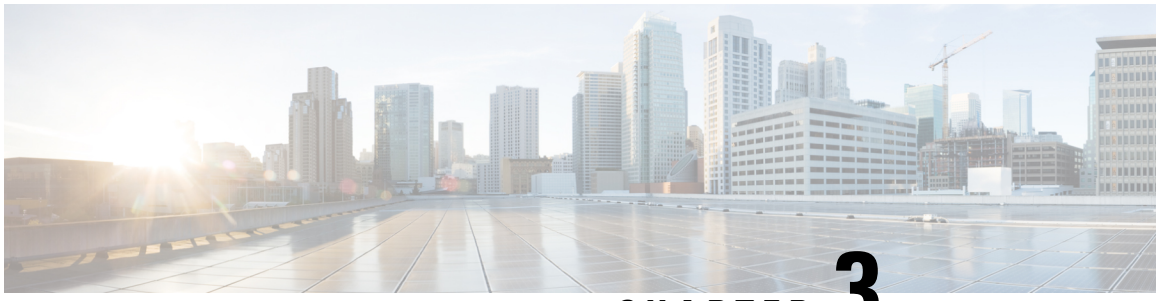
- Cisco Catalyst Center that can be found at: https://www.cisco.com/site/us/en/products/networking/catalyst-center/index.html

- 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: 1.0 in. (25 mm)– Exposed side (not connected to the module): 1.0 in. (25 mm) – Front: 1.0 in. (25 mm)

Installing the Switch on the Wall

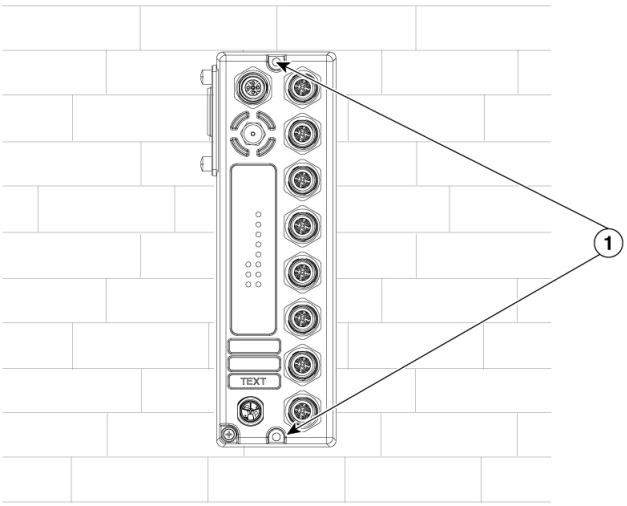
Warning **Statement 1094—**Read Wall-Mounting Instructions Before Installation

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.

Procedure

Step 1 Position the switch against the wall or a panel in the desired location. See the following figure. Attach the device to the wall with the Philips screws.

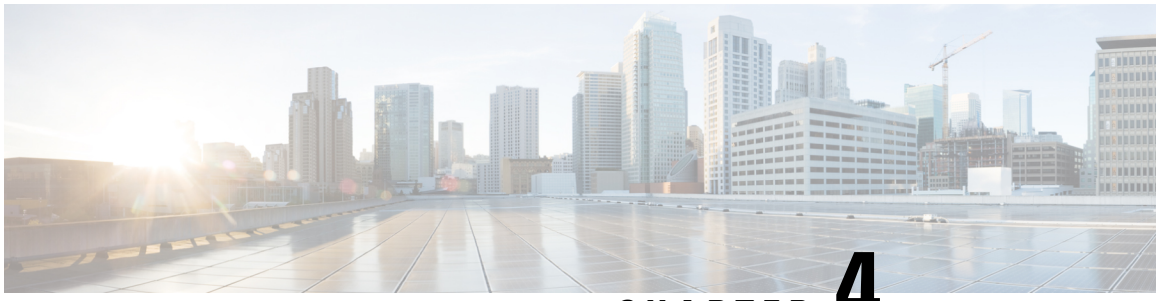
Figure 7: Mounting Wall Bracket to Wall



1	Wall mounting holes

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

Step 2 After the switch is mounted on the wall or panel, connect the power and Ethernet cables.



CHAPTER 4

Express Setup

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 X-code cable for Catalyst IE-3100H-8T-E and the D-code, X-code cable for Catalyst IE-3100H-6FT2T-E on one end and RJ45 on the other end.

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 Ensure that nothing is connected to the switch, and the cover for the SD card has been removed.

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.

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 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 the switch to the Ethernet port on your PC.

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, ensure that:

- You are using an undamaged cable.
- The other device is turned on.

Step 5 Start a browser session on the PC.

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 6 Enter the Username and Password.

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

Alternately, If the user connects via console, they can see the system serial number in the boot log.

The Configuration Setup Wizard Setup web page appears.

Note
Disable any pop-up blockers or proxy settings on your browser, and ensure that the wireless client on your PC is turned off if the setup web page does not appear.

Step 7 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 8 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 9 Click **Switch Wide Settings**.

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

Step 10 Click **Summary**.

The **Summary** window is displayed.

Step 11 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 red/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.
  - 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:

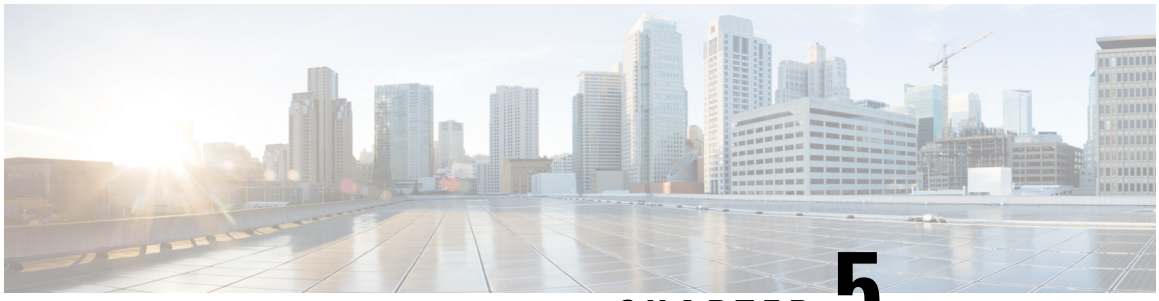
Procedure

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.



CHAPTER 5

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 17.17.1 and later, you can set a password encryption level so that user passwords are not stored in plain text. See .

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 14.

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 17.17.1 and later)
- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)
- Enable secret password
- Enable password
- SSH password

System Security Configuration

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 26 or Initial Configuration - Type-7 Encryption, on page 29. To configure system security settings without running the initial setup, see Setting the Password Encryption Level, on page 32.

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:

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 17.17.1, 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

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 14.

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 .

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!
```

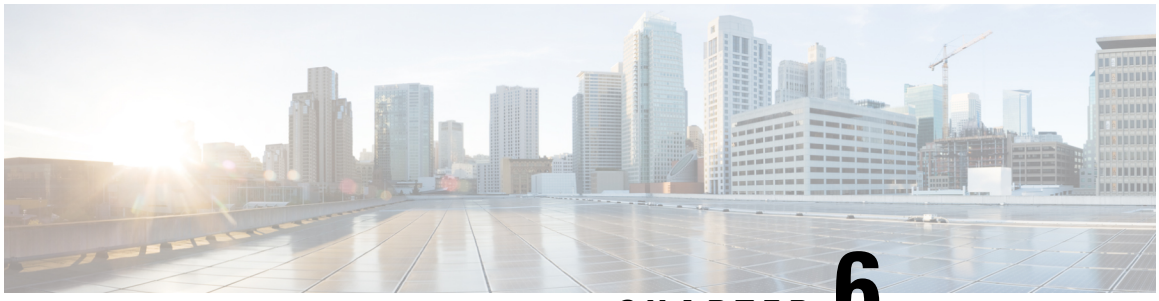
System Security Configuration Example

```
         --- 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 6

Troubleshooting

Connectivity issues may cause the switch to malfunction, arising from physical faults such as damaged cables, loose connections, or software issues such as incorrect port configurations.

Physical connectivity issues

The switch may not function properly due to connectivity issues arising due to physical faults such as damaged cables, loose connections.

The switch LEDs help diagnose the issue. 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.

A port LED that is lights up 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:

- Check for loose connections. Sometimes a cable appears to be seated but is not. Disconnect the cable, and then reconnect it.
- Check for broken or missing pins on cable connectors..
- Ensure correct cable type is used.
- Ensure that both devices have power.
- Ensure that both ends of the cable are connected to the correct ports.
- Connect the cable from the switch to a known good device.

Software configuration issues

If a 10/100 and 10/100/1G port appears to malfunction:

- Verify the status of all ports. See Port status LEDs, on page 7 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.

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 , 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 17.17.1 and later on the following IoT switches for all license levels:

- IE3100H

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:# IE3100h
Purge ACT2 chip at 12-08-2024, 15:17:28
ACT2 chip Purge done at 12-08-2024, 15:17:29
mtd and backup flash wipe start at 12-08-2024, 15:17:29
mtd and backup flash wipe done at 12-08-2024, 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 Resetting the Switch, on page 43.

Troubleshooting Express Setup

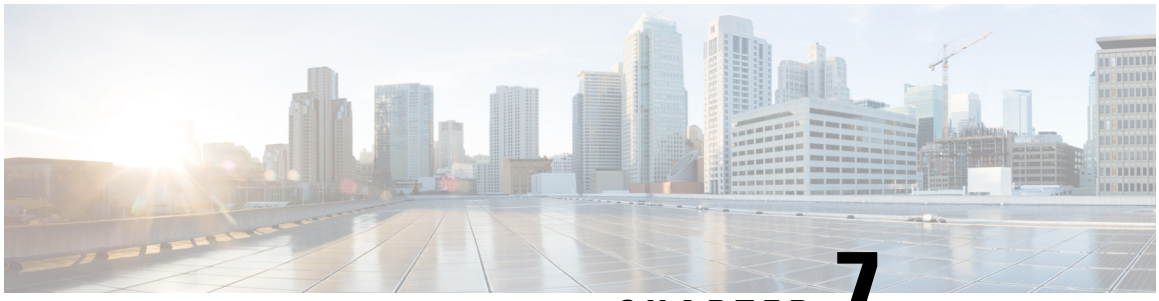
This section provides troubleshooting tips for the initial switch configuration.

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.
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.

Checklist	Recommendation
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 the bottom of the device or on the small label adjacent to the Power Connector.. You can also use the **show version** privileged EXEC command to obtain the switch serial number.



CHAPTER 7

Technical Specifications

Technical Specifications

Table 7: Physical Configurations

Physical Specifications	IE-3100H-6FT2T-E	IE-3100H-8T-E
Dimensions (H x W x D)	7.90 x 2.71 x 2.10 in 20.07 x 6.88 x 5.33 cm	7.90 x 2.71 x 2.10 in 20.07 x 6.88 x 5.33 cm
Weight (including the supplied dust caps installed)	0.754 Kg	0.738 Kg
Mounting	Wall	Wall
Environmental Ranges		
Storage temperature	–40 to 85°C (–40 to 185°F)	
Operating temperature (measured inside enclosure, 1 inch below the bottom surface of the switch)	–40 to 75°C (–40 to 167°F) **Caution** Operating temperatures exceeding 60°C are not covered by the product safety certifications and approvals. • Fan Cooled Enclosure Operating: -40°C to +75°C (-40°F to 167°F) • Vented Enclosure Operating: -40°C to +70°C (-40°F to 158°F) with minimum 40 lfm on unit • Sealed Enclosure Operating: -40°C to +60°C (-40°F to 140°F) • Short Term Operating: +85°C (185°F) for 16 hours	
Operating humidity	5 to 95% (non condensing)	

Physical Specifications	IE-3100H-6FT2T-E	IE-3100H-8T-E
Ingress Protection/Type Ratings	IP66 and IP67 Rated for protection against dust and submersion in water. NEMA Type 4 **Caution** IP66 and IP67, NEMA Type 4 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 (4572 meters) with no derating; Up to 40,000 feet (12,192 meters) derated to 25°C ambient	
Storage altitude	Up to 40,000 feet (12192 meters)	

Table 8: Power Specifications

Power Specifications	IE-3100H-6FT2T-E	IE-3100H-8T-E
Marked Input voltage range	12 to 48 VDC	12 to 48 VDC
Input voltage range (Absolute)	9.6 to 60VDC	9.6 to 60VDC
Marked Input current rating	1.5 A	1.5 A
Input current @ (9.6V / 60V)	0.998 A/0.174 A	1.265 A/ 0.210 A
Power consumption @ (9.6V / 60V)	9.58 W / 10.44 W	12.14 W/ 12.60 W

Connectors and Cabling

Table 9: Cisco Catalyst IE3100H Heavy Duty Series Switches 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
Power Input	M12 L-code female plug
Console Cable:	Console Cable with RS-232 with A-code M12 connector CAB-CONSOLE-M12=

Torque Specifications

Table 10: Cisco Catalyst IE3100H Heavy Duty Series Switch Torque Specs

Console, Ethernet ports (M12 Connectors)	4.43 to 7.08 in-lbs (0.5 to 0.8 Nm)
M12 Connector Dust Cap (Console, Ethernet ports)	4.5 to 5.5 in-lbs (0.51 to 0.62 Nm)
Power Supply Connector (M12 L-code)	5.3 in-lbs (0.60 Nm)
SD Card Access Door Captive Screws	4.43 to 7.08 in-lbs (0.5 to 0.8 Nm)