



Setup and Installation

Read this chapter to learn more about the switch setup and installation. This chapter also includes instructions on how to display the device manager in standard and in secure modes.

Before You Begin

Make sure that you have met the software and hardware requirements, as described in the [“System Requirements” section on page 1-10](#). Descriptions of the hardware features and benefits are in the [“Hardware Features” section on page 1-5](#).

Follow the setup and installation procedure described in the *Getting Started Guide for the Catalyst Express 500 Switches*.

Chapter Topics

- [Set Up the Switch for the First Time, page 2-2](#)
- [Install the Switch, page 2-5](#)
- [Display the Device Manager, page 2-13](#)
- [When You Are Done, page 2-14](#)

Set Up the Switch for the First Time

Prerequisite

To set up the switch for the first time, follow the procedure described in the *Getting Started Guide for the Catalyst Express 500 Switches*.

These are the configuration settings that you can set during initial setup:

- [Network Settings, page 2-2](#)
- [Optional Settings, page 2-5](#)

Network Settings

The network settings enable the switch to operate with its standard default settings and to be managed through the device manager. You must apply these settings to access and to take advantage of the monitoring, troubleshooting, and configuration features on the switch. Otherwise, the switch cannot be managed, and switch monitoring is limited to only its physical LEDs.

Management Interface (VLAN ID)

The ID of the management VLAN through which the switch will be managed.

The management VLAN ID can be from 1 to 1001. The default ID is 1. The default name for the management VLAN is *default*.

Note Make sure that the switch and your network management station are in the same VLAN. Otherwise, you cannot manage the switch from your management station. If they are in different VLANs, a router or Layer 3 switch is needed to communicate between VLANs.

The management VLAN is the broadcast domain where management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that should only be limited to a specific group of users (such as the administrators of your network). It also ensures secure, administrative access to all devices in the network at all times.

For more information about management VLANs and about VLANs in general, see the “VLAN Types” section on page 3-14.

| | |
|---------------------------|--|
| IP Assignment Mode | <p>The IP assignment mode determines if the switch IP information will be manually assigned (static) or be automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static.</p> <p>We recommend that you select Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the device manager.</p> <p>If you select DHCP, the DHCP server automatically assigns an IP address, subnet mask, and default gateway to the switch. As long as the switch is not restarted, the switch continues to use this information, and you can use the same IP address to access the device manager.</p> <p>Note If you manually assign the switch IP address and your network uses a DHCP server, make sure that the IP address that you give to the switch is not within the range of addresses that the DHCP server will automatically assign to other devices. This prevents IP address conflicts between the switch and another device.</p> |
| IP Address | <p>The IP address is a unique identifier for the switch in a network. The format is four numbers separated by periods. Each number can be from 0 to 255.</p> <p>This field is enabled only if the IP assignment mode is Static.</p> <p>Note Make sure that the IP address that you assign to the switch is not being used by another device in your network.</p> <p>The IP address and the default gateway cannot be the same.</p> <p>The IP addresses in the 10.0.0.0 network cannot be configured on the switch.</p> |
| Subnet Mask List | <p>The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets segment the devices in a network into smaller groups. The default is 255.255.255.0.</p> <p>This setting is enabled only if the IP assignment mode is Static.</p> |

| | |
|------------------------|--|
| Default Gateway | <p>The IP address for the default gateway. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The IP address should be part of the same subnet as the switch IP address.</p> <p>If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field.</p> <p>This setting is enabled only if the IP assignment mode is Static.</p> <p>Note You must specify a default gateway if your network management station and the switch are in different networks or subnetworks. Otherwise, the switch and your network management station will not be able to communicate with each other.</p> <p>The IP address and the default gateway cannot be the same.</p> |
| Username | <p>The name of a user who is authorized to access the device manager. The name can have up to 64 alphanumeric characters and is not case sensitive. The name cannot contain a ?, a space, or a tab.</p> <p>You must enter a username if you enter a password. We recommend that you provide a username-and-password pair to the switch to secure access to the device manager.</p> <p>After initial setup, you can add, delete, or modify username-and-password pairs from the Users and Passwords window on the device manager. To display this window, choose Configure > Users and Passwords from the device manager menu. For more information, see the “Control Access to the Switch” section on page 3-11.</p> |
| Password | <p>The password for the switch can have up to 25 alphanumeric characters, can start with a number, is case sensitive, and allows embedded spaces. The password cannot contain a ? or a tab and does not allow spaces at the beginning or end.</p> <p>We recommend that you provide a username-and-password pair to the switch to secure access to the device manager.</p> <p>After initial setup, you can add, delete, or modify username-and-password pairs from the Users and Passwords window on the device manager. To display this window, choose Configure > Users and Passwords from the device manager menu. For more information, see the “Control Access to the Switch” section on page 3-11.</p> |

Optional Settings

The optional settings identify and synchronize the switch so that it can be managed properly. The switch clock is automatically synchronized with the system clock on your network management station. You can manually set the system clock settings if the switch should have different time settings.

| | |
|-----------------------------|---|
| Host Name | A name for the switch. The name can have up to 31 alphanumeric characters. The name cannot contain a ?, a space, or a tab. The default is Switch. We recommend entering either the name, location, or IP address of the switch to help identify the switch during monitoring or troubleshooting. |
| System Date | The date that the switch automatically reads from the network management station. You can also manually set the date. |
| System Time | The time that the switch automatically reads from the network management station. You can also manually set the time. |
| Time Zone | The time zone that the switch automatically reads from the network management station. You can also manually set the time zone. |
| Daylight Saving Time | The check box is automatically enabled only when the selected time zone is in U.S., Europe, or Australia. |

Install the Switch

This section includes these topics:

- [Warnings, page 2-6](#)
- [Installation Guidelines, page 2-9](#)
- [Rack-Mounting, page 2-10](#)
- [Desktop-Mounting, page 2-11](#)
- [Wall-Mounting, page 2-12](#)

Warnings

These warnings are translated into several languages in the *Regulatory Compliance and Safety Information for the Catalyst Express 500 Switches* document that shipped with the switch. Review these warnings before you power or install the switch.

**Warning**

To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 113°F (45°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings. Statement 17B

**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 stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage. Statement 48

**Warning**

Attach only the Cisco RPS (model PWR675-AC-RPS-N1=) to the RPS receptacle. Statement 100C

**Warning**

Ethernet cables must be shielded when used in a central office environment. Statement 171

**Warning**

If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch. Statement 265

**Warning**

To comply with safety regulations, mount switches on a wall with the front panel facing up. Statement 266

**Warning**

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

**Warning**

Read the installation instructions before connecting the system to the power source. Statement 1004

**Warning**

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

**Warning**

Class 1 laser product. Statement 1008

**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**

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device. Statement 1019

**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**

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

**Warning**

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

**Warning**

Voltages that present a shock hazard may exist on Power over Ethernet (PoE) circuits if interconnections are made using uninsulated exposed metal contacts, conductors, or terminals. Avoid using such interconnection methods, unless the exposed metal parts are located within a restricted access location and users and service people who are authorized within the restricted access location are made aware of the hazard. A restricted access area can be accessed only through the use of a special tool, lock and key or other means of security. Statement 1072

**Warning**

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

Installation Guidelines

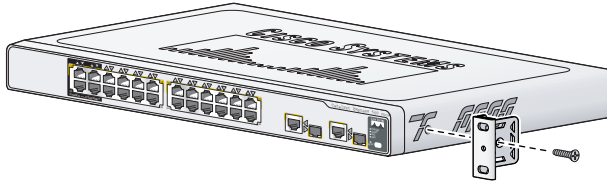
When deciding where to place the switch, be sure to observe these requirements:

- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.
- Clearance to front and rear panels is such that
 - Airflow around the switch and through the vents is unrestricted.
 - Front-panel LEDs can be easily read.
 - Access to ports is sufficient for unrestricted cabling.
 - AC power cord can reach from the AC power outlet to the connector on the switch rear panel.
- Temperature does not exceed 113°F (45°C), humidity does not exceed 85 percent, and altitude at the installation site is not greater than 10,000 feet (3049 m).

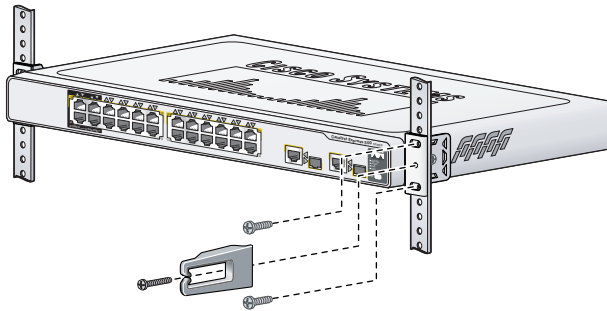
If the switch is installed in a closed or multirack assembly, the temperature around it might be greater than normal room temperature.

- For copper Ethernet ports, cable lengths from the switch to connected devices can be up to 328 feet (100 meters).
- For SFP module cable lengths, see [Table A-2](#) and the documentation that shipped with the module.

Rack-Mounting

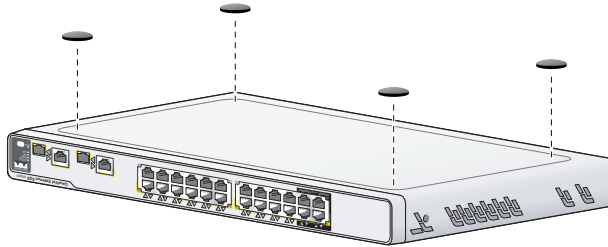


Position the mounting bracket and screw on the side of the switch. Tighten the screw with a screwdriver. Repeat on the opposite side.



Insert the switch into the 19-inch rack, and align the bracket in the rack. Use either the 10-32 pan-head screws or the 12-24 pan-slotted screws to secure the switch in the rack. Use the supplied black Phillips machine screw to attach the cable guide to either bracket.

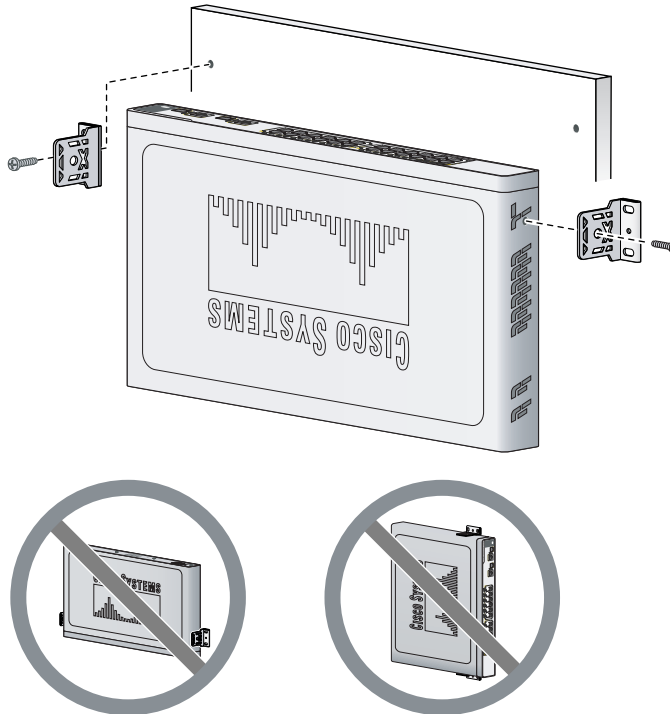
Desktop-Mounting



Place the switch upside-down on a flat surface. Attach the four rubber pads to the recessed areas on the bottom of the switch. Place the switch on a desktop near an AC power source.

If you are stacking switches, make sure that the mounting feet of the upper switch align with the recesses of the lower switch. Do not stack more than four units high.

Wall-Mounting



Position the mounting bracket and screw on the side of the switch, rotated 90-degrees from the view shown in the rack-mounting illustration. Tighten the screw with a screwdriver. Repeat on the opposite side.

Mount the switch on the wall with the front panel facing up. For the best support of the switch and cables, make sure that the switch is attached securely to wall studs or to a firmly attached plywood mounting backboard. Screws for wall-mounting are not provided.

Display the Device Manager

Prerequisite

Make sure that you meet the requirements described in the [“System Requirements”](#) section on page 1-10.

You can display the device manager ([Figure 1-3](#)) from anywhere in your network through a web browser such as Microsoft Internet Explorer or Netscape Navigator.

Follow these steps to display the device manager:

1. Open a web browser session on your PC or workstation.
2. Enter the switch IP address in the web browser, and press **Enter**. The device manager page appears.
3. Use the device manager to perform basic switch configuration and monitoring. See the device manager online help for information.

For more advanced configuration, download and run the Cisco Network Assistant (see the [“Cisco Network Assistant”](#) section on page 1-12) application.

We recommend running the cryptographic software image on the switch and using the option to run a secured session with the switch. See the [“Secured Sessions with the Switch”](#) section on page 2-13 for information on how to ensure that your device manager session is protected from unauthorized access.

Secured Sessions with the Switch

The switch uses the Secure Sockets Layer (SSL) protocol to secure the HTTP communications between the switch and your network management station. When you attempt to display the device manager, this protocol:

- Authenticates the web-based connection between the switch and your network management station
- Encrypts and decrypts the information exchanged between the switch and your network management station to protect the information from unauthorized access over the Internet

SSL is enabled by default on the switch. It is available only on the cryptographic version of the switch software image.

More information about secured sessions is available from the device manager online help.

When You Are Done

Use the features that are described in [Chapter 3, “Customization”](#) and [Chapter 4, “Monitoring”](#) to configure and to monitor the switch in your network.