Configuring the Switch with the CLI Setup Program

• Configure the Switch with the CLI-Based Setup Program, on page 1

Configure the Switch with the CLI-Based Setup Program

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

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

Accessing the CLI Through the Console Port

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

RJ-45 Console Port

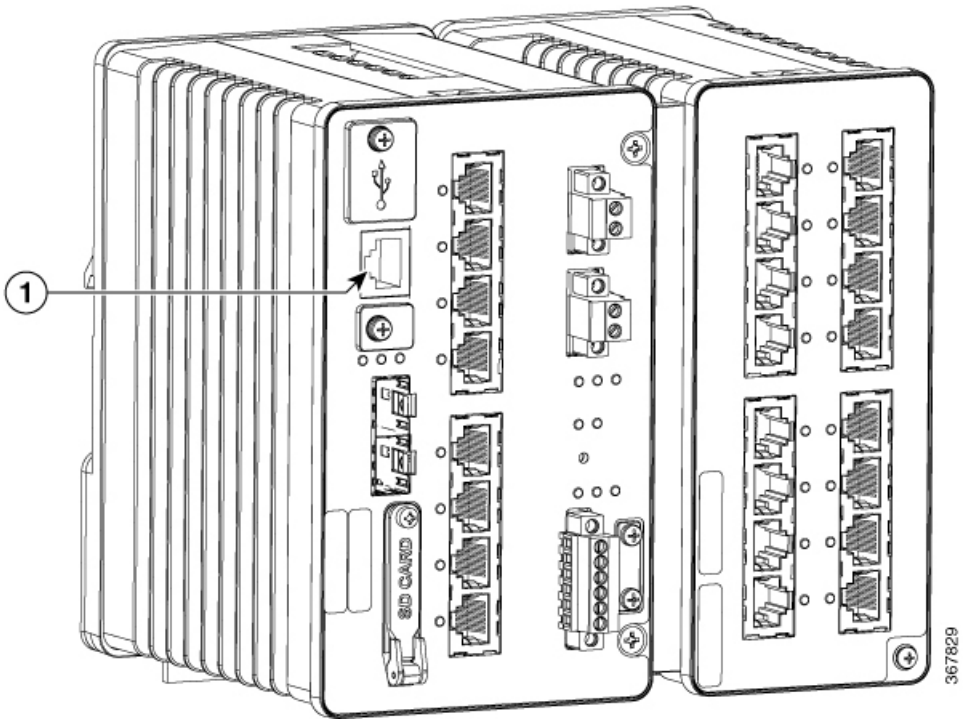
1. Connect one end of the console cable to your PC.

   Doing so may require an adapter for USB to RJ45.

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

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

Figure 1: Connecting the Console Cable



1
RJ-45 Console Port

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

USB Mini-Type B Console Port

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

Figure 2: USB Mini-Type B Console Port Cover

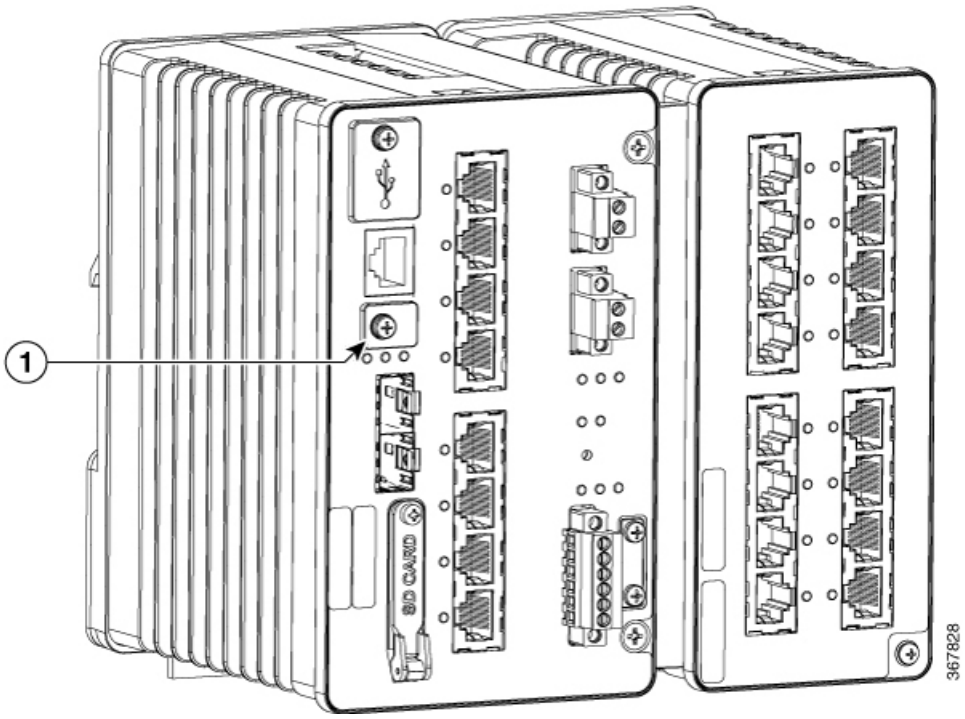


Table 1:

1	USB Mini-Type B Console Port Cover

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

9. The PC or terminal displays the bootloader sequence. Press **Enter** to display the setup prompt. See Entering the Initial Configuration Information, on page 4 to configure the switch using the Setup program.

Entering the Initial Configuration Information

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

In Cisco IOS XE 17.10.1 and later, you can set a password encryption level so that user passwords are not stored in plain text. See System Security Configuration (Cisco IOS XE 17.10.1 and later), on page 6.

IP and Password Settings

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

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

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

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

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

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

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

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

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

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

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

```
Enter enable secret: secret_password
```

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

```
Enter enable password: enable_password
```

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

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

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

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

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

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

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

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

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

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

9. This summary appears:

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

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

- Command-line interface (CLI)

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

System Security Configuration (Cisco IOS XE 17.10.1 and later)

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

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

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

You can use the setup program to set the password encryption level on both a new switch and a switch that is already configured. For a new switch, see Initial Configuration - Type-6 Encryption, on page 7 or Initial Configuration - Type-7 Encryption, on page 10. To configure system security settings without running the initial setup, see Setting the Password Encryption Level, on page 13.

Initial Configuration - Type-6 Encryption

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

Before you begin

Access the CLI as described in Accessing the CLI Through the Console Port, on page 1.

Procedure

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

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

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

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

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

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

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

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

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

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

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

Step 4 Enter the master key again to confirm it:

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

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
```

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

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

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

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

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

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

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


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

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

Step 7 Enter a hostname for the switch:

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

Step 8 Enter an enable secret password:

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

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

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

Step 10 Enter an enable password:

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

Step 11 Enter a virtual terminal password.

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

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

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

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

```
Current interface summary

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

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

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

The following configuration command script was created:

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

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

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

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



Press RETURN to get started!
```

What to do next

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

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

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

To use WebUI, see the online help for WebUI.

Initial Configuration - Type-7 Encryption

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

Before you begin

Access the CLI as described in Accessing the CLI Through the Console Port, on page 1.

Procedure

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

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

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

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

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

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

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

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

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

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

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

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

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


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

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

Step 5 Enter a hostname for the switch:

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

Step 6 Enter an enable secret password:

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

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

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

Step 8 Enter an enable password:

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

Step 9 Enter a virtual terminal password.

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

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

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

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

```
Current interface summary

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

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

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

The following configuration command script was created:

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

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

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

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



Press RETURN to get started!
```

What to do next

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

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

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

To use WebUI, see the online help for WebUI.

Setting the Password Encryption Level

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

Procedure

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

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

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

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

Step 2 Enter the enable secret at the prompt:

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

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

The following configuration command script was created:

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

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

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

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

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

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

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

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

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

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

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

Step 6 Enter the master key again to confirm it:

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

The following configuration command script was created:

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

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

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

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

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


Press RETURN to get started!


Switch>
```

CLI Setup Examples

Initial Configuration Example

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

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


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

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

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

 Enter your encryption selection [2]: 0

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

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

The following configuration command script was created:

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


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

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

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


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

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

  Enter host name [Switch]: Switch123

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

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

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

Current interface summary

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

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

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

The following configuration command script was created:

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

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


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

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



Press RETURN to get started!
```

System Security Configuration Example

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

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


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

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

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

 Enter your encryption selection [2]: 0

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

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

The following configuration command script was created:
```

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


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

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


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


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

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

  Enter host name [Switch]: Switch123

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

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

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

Current interface summary

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

```
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

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

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

The following configuration command script was created:

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


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

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



Press RETURN to get started!
```