Installation and Boot

This section contains the following:

Configuring the Switch with the CLI-Based Setup Program

This section provides a command-line interface (CLI)-based setup procedure for a switch. You must be connected to the switch through the console port to use the CLI. The ESS3300 auto detects whether the console port is RJ-45 or USB.

If using an RJ-45 console connection, configure with these parameters:

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

If you are connecting the switch USB-mini console port to a Windows-based PC for the first time, install a USB driver. If your laptop or PC warns you that you do not have the proper drivers to communicate with the router, you can obtain them from your computers manufacturer, or go here: https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

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

Connect power to the device. The PC or terminal displays the bootloader sequence. Press **Enter** to display the setup prompt.

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 4.

IP 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 5 or Initial

Configuration - Type-7 Encryption, on page 8. To configure system security settings without running the initial setup, see Setting the Password Encryption Level, on page 11.

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 Configuring the Switch with the CLI-Based Setup Program, on page 1.

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 Configuring the Switch with the CLI-Based Setup Program, on page 1.

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.

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!
```

Upgrading the Switch Software

This section covers the various aspects of upgrading or downgrading the device software.

Finding the Software Version

The package files for the Cisco IOS XE software can be found on the system board flash device flash (flash:) or external SDFlash (sdflash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

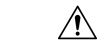
Software Images

The switch runs on Cisco IOS-XE, using an image named ess3x00-universalk9.<*release*>.SPA.bin.

Automatic Boot Loader Upgrade

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload.

For subsequent Cisco IOS XE releases, if there is a new bootloader in that release, it may be automatically upgraded based on the hardware version of the switch when you boot up your switch with the new image for the first time.



Caution Do not power cycle your switch during the upgrade.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE the first time	Boot loader may be upgraded to version "7.1.5" for ESS-3300.
	`Checking Bootloader upgrade...`
	`…`
	`Bootloader upgrade successful`

Software Installation Commands

Summary of Software Installation Commands	
To install and activate the specified file, and to commit changes to be persistent across reloads—**`install add file`** *`filename`* [**`activate commit`**]	
add file tftp: *filename*	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.
activate [**auto-abort-timer**]	Activates the file, and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes persistent over reloads.
remove	Deletes all unused and inactive software installation files.

Software Boot Modes

Your device supports two modes to boot the software packages. Installed mode and Bundle mode.

Installed Boot Mode

You can boot your device in installed mode by booting the software package provisioning file that resides in flash:

```
Switch: boot flash:packages.conf
```

Note The packages.conf file for particular release is created on following the install workflow described in the section, *Installing a Software Package*.

The provisioning file contains a list of software packages to boot, mount, and run. The ISO file system in each installed package is mounted to the root file system directly from flash.

Note The packages and provisioning file used to boot in installed mode must reside in flash. Booting in installed mode from usbflash0: or tftp: is not supported.

Installing a Software Package

You can install, activate, and commit a software package using a single command or using separate commands. This task shows how to use the **install add file activate commit** command for installing a software package.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**install add file tftp:** *filename* [**activate commit**]
	Example:
	`Device# install add file tftp://192.168.0.1//tftpboot/folder1/ess9300_iosxe.17.04.01.SPA.bin activate commit`
	`Device# install add file flash:ess9300_iosxe.17.04.01.SPA.bin activate commit`
		Copies the software install package from a remote location (via FTP, HTTP, HTTPs, TFTP) to the device, performs a compatibility check for the platform and image versions, activates the software package, and makes the package persistent across reloads.
		• This command extracts the individual components of the .bin file into sub-packages and packages.conf file.
		• The device reloads after executing this command.

Step 3	**exit** **Example:** `Device# exit`	Exits privileged EXEC mode and returns to user EXEC mode.

Managing the Update Package

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**install add file tftp:** *filename* **Example:** `Device# install add file tftp://172.16.0.1//tftpboot/folder1/ess9300_iosxe.17.04.01.SPA.bin`	Copies the software install package from a remote location (via FTP, HTTP, HTTPs, TFTP) to the device, and performs a compatibility check for the platform and image versions. • This command extracts the individual components of the .bin file into sub-packages and packages.conf file.
Step 3	**install activate** [**auto-abort-timer**] **Example:** `Device# install activate`	Activates the added software install package, and reloads the device. • When doing a full software install, do not provide a package filename. • The **auto-abort-timer** keyword, automatically rolls back the software image activation. The automatic timer is triggered after the new image is activated. If the timer expires prior to the issuing of the **install commit** command, then the install process is automatically terminated. The device reloads, and boots up with a previous version of the software image.
Step 4	**install abort** **Example:** `Device# install abort`	(Optional) Terminates the software install activation, and rolls back to the version that was running before current installation procedure. • You can use this command only when the image is in an activated state; and not when the image is in a committed state.
Step 5	**install commit** **Example:** `Device# install commit`	Makes the changes persistent over reload. • The **install commit** command completes the new image installation. Changes are persistent across reloads until the auto-abort timer expires.
Step 6	**install rollback to committed** **Example:** `Device# install rollback to committed`	(Optional) Rolls back the update to the last committed version.

	Command or Action	Purpose
Step 7	**install remove** {**file** *filesystem: filename* | **inactive**} **Example:** `Device# install remove inactive`	(Optional) Deletes all unused and inactive software installation files.
Step 8	**show install summary** **Example:** `Device# show install summary`	Displays information about the active package. • The output of this command varies according to the **install** commands that are configured.

Bundle Mode Upgrade

To upgrade the Cisco IOS XE software when the switch is running in bundle mode, follow these steps:

Step 1 Download the bundle file to local storage media.

Step 2 Configure the **boot system** global configuration command to point to the bundle file.

Step 3 Reload the switch.

Example

Upgrading Cisco IOS XE Software Bundle Mode

This example shows the steps to upgrade the Cisco IOS XE software on a switch that is running in bundle mode. It shows using the **copy** command to copy the bundle file to flash:, configuring the boot system variable to point to the bundle file, saving a copy of the running configuration, and finally, reloading the switch.

```
Switch#copy scp: sdflash:
Address or name of remote host [10.106.224.22]?Enter
Source username [xxxxx]?Enter
Source filename []? sdflash/ess3x00-universalk9.17.04.01.SPA.bin
Destination filename [ess3x00-universalk9.17.04.01.SPA.bin]?Enter
This is a Cisco managed device to be used only for authorized purposes.
Your use is monitored for security, asset protection, and policy compliance.


Password:
 Sending file modes: C0644 344345038 ess3x00-universalk9.17.04.01.SPA.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
344345038 bytes copied in 637.684 secs (539993 bytes/sec)
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no boot system
Switch(config)#boot system sdflash:ess3x00-universalk9.17.04.01.SPA.bin
Switch(config)#end
Switch#write memory
*May 27 14:49:55.121: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...
[OK]
Switch#
*May 27 14:50:01.341: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
```

```
 file
Switch#sh boot
Current Boot Variables:
BOOT variable = sdflash:ess3x00-universalk9.17.04.01.SPA.bin;

Boot Variables on next reload:
BOOT variable = sdflash:ess3x00-universalk9.17.04.01.SPA.bin;
Config file = flash:/nvram_config
ENABLE_FLASH_PRIMARY_BOOT = no
MANUAL_BOOT variable = no
ENABLE_BREAK variable = yes

Switch#reload
Proceed with reload? [confirm]Enter

*May 27 14:50:08.989: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.
watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system
```

Licensing

This section provides information about the licensing packages for features available on Cisco ESS3300 series switches.

License Levels - Usage Guidelines

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- Evaluation licenses cannot be ordered. They are not tracked via Cisco Smart Software Manager and expire after a 90-day period. Evaluation licenses can be used only once on the switch and cannot be regenerated. Warning system messages about an evaluation license expiry are generated only 275 days after expiration and every week thereafter. An expired evaluation license cannot be reactivated after reload.

Note Network Essentials license is the default license. It is permanent. A connection to the Smart Licensing server is not required if the switch will be deployed with a Network Essentials license.

Note Entering the command **license smart reservation** after the initial configuration will prevent an erroneous message "Smart Licensing Status: UNREGISTERED/EVAL MODE" from appearing on your device.

ESS3300 Model Numbers and Licensing

The following table lists the supported hardware models and the default license levels they are delivered with.

	Default License Level	Description
ESS-3300-NCP-E	Network Essentials	Main Board without a cooling plate. 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports. Terminal Power: 16W
ESS-3300-NCP-A	Network Advantage	Main Board without a cooling plate. 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports. Terminal Power: 16W
ESS-3300-CON-E	Network Essentials	Main Board conduction cooled 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports Terminal Power: 16W
ESS-3300-CON-A	Network Advantage	Main Board conduction cooled 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports Terminal Power: 16W
ESS-3300-24T-NCP-E	Network Essentials	Main Board with a 16p Expansion Board without a cooling plate 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W
ESS-3300-24T-NCP-A	Network Advantage	Main Board with a 16p Expansion Board without a cooling plate 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W

	Default License Level	Description
ESS-3300-24T-CON-E	Network Essentials	Main Board with a 16p Expansion Board conduction cooled 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W
ESS-3300-24T-CON-A	Network Advantage	Main Board with a 16p Expansion Board conduction cooled 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W

Upgrading the License Level

The following commands show how to upgrade from Network Essentials to Network Advantage.

The following shows the switch running Network Essentials:

```
switch#show version
Cisco IOS XE Software, Version BLD_V174_1_THROTTLE_LATEST_20201207_031930_V17_4_0_193
Cisco IOS Software [Bengaluru], ESS3x00 Switch Software (ESS3x00-UNIVERSALK9-M), Experimental
 Version 17.4.20201207:040001
[S2C-build-v174_1_throttle-208-/nobackup/mcpre/BLD-BLD_V174_1_THROTTLE_LATEST_20201207_031930
 156]
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Mon 07-Dec-20 00:33 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON
BOOTLDR: Version 7.0.6 [DEVELOPMENT SOFTWARE] crashkernel=64M
switch uptime is 7 weeks, 5 days, 5 hours, 7 minutes
Uptime for this control processor is 7 weeks, 5 days, 5 hours, 8 minutes
System returned to ROM by Reload Command
System image file is "flash:packages.conf"
Last reload reason: Reload Command
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                      Technology-package
Current                       Type                         Next reboot
------------------------------------------------------------------------------
network-essentials   Smart License                  network-essentials


Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco ESS-3300-CON (ARM) processor (revision V01) with 890141K/6147K bytes of memory.
Processor board ID 32
1 Virtual Ethernet interface
24 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
3952748K bytes of physical memory.
523264K bytes of crashinfo at crashinfo:.
1684480K bytes of Flash at flash:.
3883008K bytes of sdflash at sdflash:.

Base Ethernet MAC Address          : 40:ce:24:b7:75:20
Motherboard Assembly Number        : 73-101439-03
Motherboard Serial Number          : FJZ22150D34
Model Revision Number              : V01
Motherboard Revision Number        : 3
Model Number                       : ESS-3300-CON
System Serial Number               : 32
Top Assembly Part Number           : 68-101690-01
Top Assembly Revision Number       : 17P
System FPGA version                : 0.88.0
SKU Brand Name                     : Cisco


Configuration register is 0x102

switch#
```

The following shows the licenses in use:

```
switch#show license summary
License Usage:
  License                Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  No licenses in use
switch#
```

The following shows a protocol not found in Network Essentials:

```
switch(config)#router ospf 10
Protocol not in this image
switch(config)#
```

Upgrade the switch to Network Advantage:

```
switch(config)#license boot level network-advantage
% use 'write' command to make license boot config take effect on next boot
switch(config)#end
switch(config)#write memory
Building configuration...
[OK]
switch#
```

Reload the switch:

```
switch#reload
Proceed with reload? [confirm]<Enter>

watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system

Initializing disk drivers...
Initializing file systems...

************************************************************
* Rom Monitor for ESS3300                                  *
* Copyright (c) 2017-2020 by Cisco Systems, Inc.           *
* All rights reserved.                                     *
************************************************************

* Version:  7.0.6
* Compiled: Sun 08-Nov-20 22:38 [DEVELOPMENT SOFTWARE]
* Boot Partition: qspi-upgrade-bootloader
* Reset Reason: Soft Reset
* REL and DEV keys installed

Loading "flash:packages.conf" to memory...
Loading "flash:/ess3x00-rp_iot.BLD_V174_1_THROTTLE_LATEST_20201207_031930_V17_4_0_193.SSA.pkg"
 to memory...
Verifying image
"flash:/ess3x00-rp_iot.BLD_V174_1_THROTTLE_LATEST_20201207_031930_V17_4_0_193.SSA.pkg"...
Image passed digital signature verification
Loading "flash:/ess3x00-rpboot.BLD_V174_1_THROTTLE_LATEST_20201207_031930_V17_4_0_193.SSA.pkg"
 to memory...
Verifying image
"flash:/ess3x00-rpboot.BLD_V174_1_THROTTLE_LATEST_20201207_031930_V17_4_0_193.SSA.pkg"...
Image passed digital signature verification

Booting ss-rommon...
Version:  7.0.6
Compiled: Sun 08-Nov-20 22:38 [DEVELOPMENT SOFTWARE]

Address Map    : Total: 7884608 bytes
 IOT Pkg Header: 0x00000000 size: 1396
 SS-Rommon     : 0x00000574 size: 628960
 Sup PL[01]    : 0x001836c4 size: 5568668
 Rtos[01]      : 0x0009a3ec size: 953668
 BL[1835014]   : 0x006d3500 size: 727616

Address Map    : Total: 56306701 bytes
 RP_Boot Header: 0x00000000 size: 1396
```

```
 Kernel        : 0x00000574 size: 32541248
 Dtb           : 0x01f08fb4 size: 45144
 InitRamFs     : 0x01f1400c size: 23718913

Checking for Bootloader upgrade...
Bootloader upgrade not required
SUP PL (profile: 1) configuration done successfully
RTOS (profile: 1) boot successful

Taking BP out of reset
Taking LC1 out of reset
Taking LC2 out of reset
Taking LC3 out of reset

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software [Bengaluru], ESS3x00 Switch Software (ESS3x00-UNIVERSALK9-M), Experimental
 Version 17.4.20201207:040001
[S2C-build-v174_1_throttle-208-/nobackup/mcpre/BLD-BLD_V174_1_THROTTLE_LATEST_20201207_031930
 156]
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Mon 07-Dec-20 00:33 by mcpre


This software version supports only Smart Licensing as the software licensing mechanism.


PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE,
AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE
"SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL
ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU
ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement
(EULA) and any relevant supplemental terms (SEULA) found at
http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

You hereby acknowledge and agree that certain Software and/or features are
licensed for a particular term, that the license to such Software and/or
features is valid only for the applicable term and that such Software and/or
features may be shut down or otherwise terminated by Cisco after expiration
of the applicable license term (e.g., 90-day trial period). Cisco reserves
the right to terminate any such Software feature electronically or by any
other means available. While Cisco may provide alerts, it is your sole
responsibility to monitor your usage of any such term Software feature to
ensure that your systems and networks are prepared for a shutdown of the
Software feature.


All TCP AO KDF Tests Pass
```

```
cisco ESS-3300-CON (ARM) processor (revision V01) with 890141K/6147K bytes of memory.
Processor board ID 32
1 Virtual Ethernet interface
24 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
3952748K bytes of physical memory.
523264K bytes of crashinfo at crashinfo:.
1684480K bytes of Flash at flash:.
3883008K bytes of sdflash at sdflash:.

Base Ethernet MAC Address          : 40:ce:24:b7:75:20
Motherboard Assembly Number        : 73-101439-03
Motherboard Serial Number          : FJZ22150D34
Model Revision Number              : V01
Motherboard Revision Number        : 3
Model Number                       : ESS-3300-CON
System Serial Number               : 32
Top Assembly Part Number           : 68-101690-01
Top Assembly Revision Number       : 17P
System FPGA version                : 0.88.0
SKU Brand Name                     : Cisco


Press RETURN to get started!


switch>
```

Once the above step is completed, the switch will have the EVAL license. The customer needs to purchase the Network Advantage license so that it reflects in the corresponding smart account. For Smart licensing, the license from the smart account is consumed once the device establishes communication to the CSSM server. For the SLR model below, these are the steps to apply the license in the switch from smart account.

```
switch#license smart reservation request all
```

Using the Reservation code generated from the above command, a Reservation Authorization code should be generated from the smart account and used in the following command:

```
switch#license smart reservation install <Reservation Auth code>
```

Verify the change by showing the license summary:

```
switch#show license summary
License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (ESS3300_Network_Advantage)       1 IN USE

switch#
```

The following shows that the protocol displayed earlier is now available in Network Advantage:

```
switch(config)#router ospf 10
switch(config-router)#
```

The following commands show the license usage:

```
switch#show license tech support
Smart Licensing Tech Support info

Smart Licensing Status
======================

Smart Licensing is ENABLED
```

```
Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Address: <empty>
    Port: <empty>
    Username: <empty>
    Password: <empty>
  Server Identity Check: False

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)

switch#show license usage
License Authorization:
  Status: Not Applicable

network-advantage (ESS3300_Network_Advantage):
  Description: network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual

switch#
```

The following displays the switch inventory:

```
switch#show inventory
NAME: "Chassis", DESCR: "Cisco ESS-3300-CON"
PID: ESS-3300-CON      , VID: V01  , SN: 32

NAME: "Supervisor", DESCR: "ESS3x00-M 2 uplink SFP's, 8x1GE Copper PoE ports Conduction
```

```
cooled"
PID: ESS-3300-CON      , VID: V01  , SN: 32

NAME: "TenGigabitEthernet1/2", DESCR: "SFP-10GBase-SR"
PID: SFP-10G-SR          , VID: V03  , SN: FNS21300STA

NAME: "GigabitEthernet1/3", DESCR: "1000BaseSX SFP"
PID: GLC-SX-MMD          , VID: V02  , SN: OPM24030S4U

NAME: "GigabitEthernet1/4", DESCR: "100BaseLX-FE SFP"
PID: GLC-FE-100LX-RGD    , VID: V02  , SN: ACW23390FY4

NAME: "GigabitEthernet1/5", DESCR: "10/100/1000BaseTX SFP"
PID: GLC-TE              , VID: V01  , SN: AVC233122E1

NAME: "Expansion Module", DESCR: "ESS3x00-Ex Expansion Module 16x1GE Copper PoE Conduction
 cooled"
PID: ESS-3300-16T-CON  , VID: V01  , SN: 16

switch#
```

Boot from the USB

The switch can be booted from configuration files located on the pluggable USB. Customized startup configuration files can be booted from IOS or from ROMMON.

Booting from IOS

The following configuration steps need to be taken in order to boot from the USB.

To display the boot options:

```
switch(config)#boot config ?
  bootflash:  URL of the config file
  flash:      URL of the config file
  msata:      URL of the config file
  nvram:      URL of the config file
  usbflash0:  URL of the config file
  webui:      URL of the config file
```

The syntax for the boot command is:

boot config usbflash0:<*file name*>

For example:

```
switch(config)#boot config usbflash0:startup-config
switch(config)#
switch#write memory
Building configuration...
[OK]
*Feb 10 10:20:11.990: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
```

The environment variable CONFIG_FILE in the following example confirms that the startup-config is set to boot from usbflash0.

```
switch#show boot
BOOT variable =
```

```
CONFIG_FILE variable = usbflash0:startup-config
BOOTLDR variable does not exist
Configuration register is 0x1820
Standby not ready to show bootvar
```

Booting from ROMMON

The following configuration steps need to be taken in order to boot from the USB.

From the ROMMON prompt, execute **set CONFIG_FILE=usbflash0:** <*filename*>

For example:

```
rommon 2 > set CONFIG_FILE=usbflash0:my_startupcfg
rommon 3 > sync
rommon 4 > set
PS1=rommon ! >
MCU_UPGRADE=SKIP
THRPUT=
LICENSE_BOOT_LEVEL=
RET_2_RTS=
MCP_STARTUP_TRACEFLAGS=00000000:00000000
BSI=0
RANDOM_NUM=1275114933
BOOT=flash:Jun5_1.SSA,12
RET_2_RCALTS=951454376
CONFIG_FILE=usbflash0:my_startupcfg
```

Continue booting the IOS image as usual from the ROMMON prompt.

Booting from the USB Feature Summary

- Once the CONFIG_FILE is set to a non-default value, the **nvram:startup-config** command is aliased to this new location.
- Any change made to the config file in usbflash will be reflected in nvram:startup-config as well.
- The EXEC command **erase nvram:startup-config** erases the contents of NVRAM, and deletes the file referenced by CONFIG_FILE variable.
- If the USB is unplugged after setting the **boot config usbflash0:** <*filename*> variable, then the day 0 default configuration will take effect.
- When the configuration is saved using the **copy system:running-config nvram:startup-config** command, the device saves a complete version of the configuration file to the location specified by the CONFIG_FILE environment variable, and a distilled version to NVRAM. A distilled version is one that does not contain access list information.

Clearing the Startup Configuration

You can clear the configuration information from the startup configuration. If you reboot the device with no startup configuration, the device enters the Setup command facility so that you can configure the device from scratch. To clear the contents of your startup configuration, complete the task in this section:

Important The IOS command parser may show a **factory-reset all** command. For embedded platforms this command is **NOT** supported as it leads to an ambiguity of which factory does it reference. A partner or integrator may install value add features that could be wiped out and not restored when such a command is executed. The system is obviously not in the state when it left the patrner or integrator's factory. If the desire is to perform a deep wipe of the on-board flash file system, the user should use the zeroization function and be completely familiar with the recovery features of the platform.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**erase nvram** **Example:** `Device# erase nvram`	Clears the contents of your startup configuration. **Note** For all platforms except the Class A Flash file system platforms, this command erases NVRAM. The startup configuration file cannot be restored once it has been deleted. On Class A Flash file system platforms, when you use the **erase startup-config** EXEC command, the device erases or deletes the configuration pointed to by the CONFIG_FILE environment variable. If this variable points to NVRAM, the device erases NVRAM. If the CONFIG_FILE environment variable specifies a flash memory device and configuration filename, the device deletes the configuration file. That is, the device marks the file as “deleted,” rather than erasing it. This feature allows you to recover a deleted file.

Emergency Recovery Installation

The following procedure supports the Cisco ESS3300 and the Cisco ESS9300.

Note There is different terminology used when referring to the push button depending on the product. The IE3x00 switches call this the Express Setup switch. Other products may refer to this as the Factory Default Switch. In either case, the functionality is the same.

If the other recovery methods fail, the switch has a trap door method that you can use in order to recover the system. You must have a terminal that is connected to port Gi1/3 of the switch that runs a TFTP server. Download a valid image file from CCO and store it in the root of the TFTP server.

It is likely that the switch is stuck at the **switch**: prompt. However, if you are in a boot loop, you can use the push button functionality in order to break the cycle: hold the button for approximately 5 seconds, and the switch breaks the cycle and stops at the **switch**: prompt.

Complete these steps in order to perform an emergency recovery:

Step 1: Boot the emergency install image.

```
switch: boot emgy0:<image-name>.SPA.bin
Booting golden bootloader...
Initializing disk drivers...
Initializing file systems...
**********************************************************
* Rom Monitor for ESS3300                                *
* Copyright (c) 2017-2018 by Cisco Systems, Inc.         *
* All rights reserved.                                   *
**********************************************************
* Version:  1.1.1
* Compiled: Sun 01-Jul-18 22:17 [RELEASE SOFTWARE]
* Boot Partition: qspi-golden-bootloader
* Reset Reason: Soft Reset
Loading "emgy0:ess3x00-universalk9.17.04.01.SPA.bin" to memory...
Verifying image "emgy0:ess3x00-universalk9.17.04.01.SPA.bin"...
Image passed digital signature verification
Checking for Bootloader upgrade...
Bootloader upgrade not required
SUP PL (profile: 1) configuration done successfully
<...>
Press RETURN to get started!
Switch>
```

Step 2: Configure an IP address on the switch. Additional details on IP configuration can be found here

```
switch(config-if)# ip address <ip-address> <subnet-mask>
```

Step 3: Ping the terminal that contains the TFTP server in order to test the connectivity:

```
switch> ping 192.0.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.0.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Step 4: Copy the image via tftp

```
switch> copy tftp://location/directory/bundle_name flash:

<...>
```

Step 5: Restart the system.