Release Notes for the Industrial Ethernet 2000 Switch, Cisco IOS Release 15.2(2)E

Last Updated: January 10, 2017

Cisco IOS Release 15.2(2)E runs on all Cisco Industrial Ethernet IE 2000 switches.

Cisco IOS Software Release 15.2(2)E is part of the new software releases on Cisco IE 2000 Series Switches. This release delivers new software innovations in Industrial deployments that span across many technologies.

These release notes include important information about Cisco IOS Release15.2(2)E, and any limitations, restrictions, and caveats that apply to it.

Verify that these release notes are correct for your switch:

- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 6.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 7.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://software.cisco.com/download/navigator.html

Content

- System Requirements, page 2
- Upgrading the Switch License, page 6
- Installation Notes, page 9
- Software Features, page 9
- Important Notes, page 12
- Caveats, page 14
- Documentation Updates, page 17
- Related Documentation, page 17
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 18

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

System Requirements

- Hardware Supported, page 2
- Express Setup Requirements, page 5

Hardware Supported

Switch Models Supported

Table 1 Cisco IE 2000 Switches Supported

Switch Model	Description	Supported by Minimum Cisco IOS Release
Cisco IE-2000-4T-L	4 10/100BASE-T downlink ports 2 10/100BASE-T uplink ports	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-4T-B	4 10/100BASE-T downlink ports 2 10/100BASE-T uplink ports	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-4T-G-L	4 10/100BASE-T downlink ports 2 10/100/1000BASE-T uplink ports	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-4T-G-B	4 10/100BASE-T downlink ports 2 10/100/1000BASE-T uplink ports	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-4TS-L	4 10/100BASE-T downlink ports 2 100 Mb/s SFP (small form-factor pluggable) module uplink slots	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-4TS-B	4 10/100BASE-T Ethernet ports 2 100 Mb/s SFP module uplink slots	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-4TS-G-L	4 10/100BASE-T downlink ports 2 100/1000 Mb/s SFP module uplink slots	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-4TS-G-B	4 10/100BASE-T downlink ports 2 100/1000 Mb/s SFP module uplink slots	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-8TC-B	8 10/100BASE-T downlink ports 2 Fast Ethernet dual-purpose uplink ports	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-8TC-L	8 10/100BASE-T downlink ports 2 Fast Ethernet dual-purpose uplink ports	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-8TC-G-B	8 10/100BASE-T downlink ports 2 Gigabit Ethernet dual-purpose uplink ports	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-8TC-G-E	8 10/100BASE-T downlink ports 2 Gigabit Ethernet dual-purpose uplink ports Supports IEEE-1588 standard for synchronizing clocks. Can enable NAT by license upgrade.	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-8TC-G-L	8 10/100BASE-T downlink ports 2 Gigabit Ethernet dual-purpose uplink ports	Cisco IOS Release 15.0(2)EA1

Table 1 Cisco IE 2000 Switches Supported (continued)

Switch Model	Description	Supported by Minimum Cisco IOS Release
Cisco IE-2000-8TC-G-N	8 10/100BASE-T downlink ports, 2 Gigabit Ethernet dual-purpose uplink ports. Supports IEEE-1588 standard for synchronizing clocks and Network Address Translation (NAT).	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-16TC-B	16 10/100BASE-T downlink ports 2 Fast Ethernet dual-purpose uplink ports 2 100 Mb/s SFP module uplink slots	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-16TC-L	16 10/100BASE-T downlink ports 2 Fast Ethernet dual-purpose uplink ports 2 100 Mb/s SFP module uplink slots	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-16TC-G-E	16 10/100BASE-T downlink ports, 2 Gigabit Ethernet dual-purpose uplink ports 2 100 Mb/s SFP module uplink ports Supports IEEE-1588 standard for synchronizing clocks. Can enable NAT by license upgrade.	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-16TC-G-L	16 10/100BASE-T downlink ports 2 Gigabit Ethernet dual-purpose uplink ports 2 100 Mb/s SFP module uplink slots	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-16TC-G-N	16 10/100BASE-T downlink ports, 2 Gigabit Ethernet dual-purpose uplink ports, and 2 100Mb/s SFP module downlink slots. Supports IEEE-1588 standard for synchronizing clocks and Network Address Translation (NAT).	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-16TC-G-X[1]	16 10/100BASE-T downlink ports, 2 Gigabit Ethernet uplink ports 2 100 Mb/s SFP module uplink slots Supports IEEE-1588 standard for synchronizing clocks. Can enable NAT by license upgrade.	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-16PTC-G-L	16 10/100BASE-T downlink ports with 4 PoE/PoE+ and 2 Gigabit Ethernet dual-purpose uplink ports. Supports PoE/PoE+ on top of the LAN Lite image.	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-16PTC-G-E	16 10/100BASE-T downlink ports with 4 PoE/PoE+ 2 Gigabit Ethernet dual-purpose uplink ports Supports PoE/PoE+ and IEEE-1588 standard for synchronizing clocks on top of the LAN Base image. Supports Network Address Translation (NAT) on top of the Enhanced LAN Base license. NAT license should be ordered separately.	Cisco IOS Release 15.0(2)EA1

Table 1 Cisco IE 2000 Switches Supported (continued)

Switch Model	Description	Supported by Minimum Cisco IOS Release
Cisco IE-2000-16PTC-G-NX	16 10/100BASE-T downlink ports with 4 PoE/PoE+ 2 Gigabit Ethernet dual-purpose uplink ports Supports PoE/PoE+, IEEE-1588 standard for synchronizing clocks, and Network Address Translation (NAT) on top of Enhanced LAN Base image.	Cisco IOS Release 15.0(2)EA1
Cisco IE-2000-8T67-B	8 ports 10/100BASE T M12 connectors Layer 2 switch, all FE ports.	Cisco IOS Release 15.2(1)EY
Cisco IE-2000-16T67-B	16-port 10/100BASE-T M12 connectors Layer 2 switch, all FE ports.	Cisco IOS Release 15.2(1)EY
Cisco IE-2000-24T67-B	16 port 10/100BASE-T M12 connectors Layer 2 switch, all FE ports.	Cisco IOS Release 15.2(1)EY
Cisco IE-2000-8T67P-G-E	8-port 10/100BASE-T, 8-port POE/4-port POE+, 2-port 10/100/1000 uplink, Precision Time Protocol (PTP) support.	Cisco IOS Release 15.2(1)EY
Cisco IE-2000-16T67P-G-E	8-port 10/100BASE-T, 8-port POE/POE+, 2-port 10/100/1000 uplink, Precision Time Protocol (PTP) support.	Cisco IOS Release 15.2(1)EY
Cisco IE-2000-4S-TS-G-L	4 10/100BASE-TX SFP module downlink slots 2 Gigabit Ethernet SFP uplink slots	Cisco IOS Release 15.2(1)EY
Cisco IE-2000-4S-TS-G-B	4 10/100BASE-TX SFP module downlink slots 2 Gigabit Ethernet SFP uplink slots	Cisco IOS Release 15.2(1)EY

1. The Cisco IE-2000-16TC-G-X and IE-2000-16PTC-G-NX are the two models available with a conformal coating (Humiseal UB40).

SFP Modules Supported

The SFP modules are switch Ethernet SFP modules that provide connections to other devices. Depending on the switch model, these field-replaceable transceiver modules provide uplink or downlink interfaces. The modules have LC connectors for fiber-optic connections.

You can use any combination of the supported SFP modules.

Table 2 SFP Modules

Switch Model	Description
Rugged and industrial SFP modules[1]	GLC-FE-100LX-RGD
	GLC-FE-100FX-RGD
	GLC-SX-MM-RGD[2]
	GLC-LX-SM-RGD[2]
	GLC-ZX-SM-RGD[2]

Table 2 SFP Modules (continued)

Switch Model	Description
Commercial SFP modules	GLC-SX-MM
	GLC-LH-SM
	GLC-BX-U[2]
	GLC-BX-D[2]
	CWDM-SFP[2]
	DWDM-SFP[2]
	Gig GLC-T
Extended temperature SFP modules	SFP-GE-S[2]
	SFP-GE-L[2]
	SFP-GE-Z[2]
	GLC-EX-SMD
	GLC-LX-SMD
	GLC-FE-100FX
	GLC-FE-100LX
	GLC-FE-100EX
	GLC-FE-100ZX
	GLC-FE-100BX-U
	GLC-FE-100BX-D

1. The maximum operating temperature of the switch varies depending on the type of SFP module that you use. See the *Hardware Installation Guide* for more information.
2. These SFP modules have digital optical monitoring (DOM) support.

For the most up-to-date list of supported SFP models for Cisco Industrial Ethernet switches, see http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6981.html#wp138176

http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL632702.html

Express Setup Requirements

Hardware

- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
- 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- 16 GB available hard disk space (32-bit) or 20 GB (64-bit)

Software

- PC with Windows 7, or Mac OS 10.6.x
- Web browser (Internet Explorer 9.0, 10.0, and 11.0, or Firefox 25, 26) with JavaScript enabled
- Straight-through or crossover Category 5 or 6 cable

Express Setup verifies the browser version when starting a session, and it does not require a plug-in.

Upgrading the Switch License

Upgrade Cisco IOS software features through the Cisco Software Activation tool. It authorizes and enables the feature set on Cisco IE 2000 switch series based on the type of license. Enable features either through a licensing upgrade only, or both a licensing and software upgrade.

On Cisco IE 2000 switches, to upgrade from LAN Lite to LAN Base you do not require new software releases. However, the minimum software version required for Enhanced LAN Base is 15.0(2)EB. Running a release prior to 15.0(2)EB will require a software upgrade first before the license upgrade. See *Software Activation Licensing Upgrade* for detailed steps:

http://www.cisco.com/en/US/docs/switches/lan/cisco_ie2000/software/release/15_0_2_eb/upgrade/guide/ie2000_ug.html

Upgrading the Switch Software

- Finding the Software Version and Feature Set, page 6
- Deciding Which Files to Use, page 7
- Archiving Software Images, page 7
- Upgrading a Switch by Using the CLI, page 7
- Recovering from a Software Failure, page 8

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. On IE 2000, the image can be stored on the internal flash or external SD card.

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

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

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded Express Setup. You must use the combined tar file to upgrade the switch through Express Setup. To upgrade the switch through the CLI, use the tar file and the **archive download-sw** privileged EXEC command.

Table 3 Cisco IOS Software Image File

Filename	Description
ie2000-universalk9-tar.152-2.E.tar	Cisco IE 2000 cryptographic Cisco IOS image file

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

Note Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you take advantage of the available SD card memory by copying the extracted image directory and user configuration to SD card using the command [sync flash: sdflash:] to ensure a backup file is stored safely

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the *Cisco IOS Configuration Fundamentals Command Reference*:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

Note On IE2000, the image file can be downloaded to the internal flash or the SD card (if present).

To download software, follow these steps:

Step 1 Use Table 3 on page 7 to identify the file that you want to download.

Step 2 Download the software image file. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

http://www.cisco.com/cisco/web/download/index.html

To download the image for a Cisco IE 2000 switch, click **Switches > Industrial Ethernet Switches > Cisco IE 2000 Series Switches**, and then click on the Cisco IOS software for your specific switch model.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, see Appendix B of the software configuration guide for this release.

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Check that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, see the software configuration guide for this release.

Step 6 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# archive download-sw /overwrite /reload tftp:[[//location]/directory]/
image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For *//location*, specify the IP address of the TFTP server.

For */directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/image-name.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

For additional recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- Express Setup program, as described in the switch getting started guide.
- CLI-based setup program, as described in the switch hardware installation guide.
- DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manual assignment of an IP address, as described in the switch software configuration guide.

Software Features

For more information about the following new features for this release, please see the associated Configuration Guide here: http://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie2000/software/release/15_2_2_e/configuration/guide/scg-ie2000.html

Open Plug-N-Play Agent

Cisco Open Plug-n-Play agent is a software application that is running on a Cisco IOS or IOS-XE device and provides zero-touch deployment of all new devices. The application facilitates the acquisition and loading of pertinent images, configuration files, and other required files to the device along with notifications for various events. (Cisco IE 2000 only supports Cisco IOS).

Cisco EnergyWise

Cisco EnergyWise includes software and services that help you measure and manage the energy use of all the connected devices across your networks. IE 2000 supports Cisco EnergyWise version 2.8. For more information, see the Cisco EnergyWise software release notes and the configuration guide here: http://www.cisco.com/c/en/us/td/docs/switches/lan/energywise/version2_8/ios/release/notes/ol23554.html

Smart Install

Smart Install is a plug-and-play configuration and software upgrade feature that provides zero-touch deployment for new switches. You can ship a switch to a location, place it in the network and power it on with no configuration required on the device. For more information, see *Smart Install Configuration Guide* here: http://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install.html

Note IE2000 can be a Smart Installation Director

Device Sensor

Device Sensor is supported from Cisco IOS Release 15.2(2)E1.

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

Cisco IOS Limitations

- Ethernet
- IP
- QoS
- RADIUS
- SPAN and RSPAN
- Spanning Tree Protocol
- Trunking
- VLAN

Ethernet

- Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to same member ports based on hashing results calculated by the ASIC.

  If this happens, uneven traffic distribution will happen on EtherChannel ports.

  Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:

  – for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**

  – for incrementing source-ip traffic, configure load balance method as **src-ip**

  – for incrementing dest-ip traffic, configure load balance method as **dst-ip**

  – Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (i.e. 2, 4, or 8)

  For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal.(CSCeh81991)

IP

- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console.

  The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

QoS

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue.

  The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)

- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)

RADIUS

- RADIUS change of authorization (COA) reauthorization is not supported on the critical auth VLAN.

  There is no workaround. (CSCta05071)

SPAN and RSPAN

- When the RSPAN feature is configured on a switch, Cisco Discovery Protocol (CDP) packets received from the RSPAN source ports are tagged with the RSPAN VLAN ID and forwarded to trunk ports carrying the RSPAN VLAN. When this happens a switch that is more than one hop away incorrectly lists the switch that is connected to the RSPAN source port as a CDP neighbor.

  This is a hardware limitation. The workaround is to disable CDP on all interfaces carrying the RSPAN VLAN on the device connected to the switch. (CSCeb32326)

- CDP, VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Spanning Tree Protocol

- CSCtl60247

  When a switch or switch stack running Multiple Spanning Tree (MST) is connected to a switch running Rapid Spanning Tree Protocol (RSTP), the MST switch acts as the root bridge and runs per-VLAN spanning tree (PVST) simulation mode on boundary ports connected to the RST switch. If the allowed VLAN on all trunk ports connecting these switches is changed to a VLAN other than VLAN 1 and the root port of the RSTP switch is shut down and then enabled, the boundary ports connected to the root port move immediately to the forward state without going through the PVST+ slow transition.

  There is no workaround.

Trunking

- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in

VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y.

There is no workaround. (CSCdz42909).

- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics.

  There is no workaround. (CSCec35100).

VLAN

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)
- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

  The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port. (CSCsi26392)
- When many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time.

  The workaround is to remove unnecessary VLANs to reduce CPU utilization when many links are flapping. (CSCtl04815)

Important Notes

- IPv4 Static Routing Notes, page 12
- 61000-4-3 Standard Notes, page 12
- Express Setup Notes, page 13

IPv4 Static Routing Notes

Cisco IE 2000 supports IPv4 static routing in the LAN Base image. To access static routing commands, you need to change the SDM template from the default template to lanbase-routing, followed by a switch reload sequence.

61000-4-3 Standard Notes

The following note is an update to the *Regulatory Compliance and Safety Information* (RCSI) guide. This note applies to the 61000-4-3 standard listed in the “EMC Interface Immunity” section of Table 1 of the guide.

Note To meet 10V/m or 20V/m Radiated Immunity levels, shielded cables must be used on the uplink ports, G1/1 and G1/2.

This note applies to these SKUs:
– IE-2000-4T-G-L
– IE-2000-4T-G-B
– IE-2000-8TC-G-L
– IE-2000-8TC-G-B
– IE-2000-8TC-G-E
– IE-2000-16TC-G-L
– IE-2000-16TC-G-E
– IE-2000-16TC-G-X

Express Setup Notes

- This browser setting is recommended for speeding up the time required to display Express Setup from Microsoft Internet Explorer:
  1. Choose **Tools** > **Internet Options**.
  2. Click **Settings** in the Temporary Internet files area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display Express Setup. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip http authentication** {**aaa** | **enable** | **local**}	Configures the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enables the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enables the password, which is the default method of HTTP server user authentication. • **local**—Specifies the local user database, as defined on the Cisco router or access server.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entries.

- Express Setup uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

  If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, http://10.1.126.45:184 where 184 is the new HTTP port number). Write down the port number through which you are connected. Use care when changing the switch IP information.

  If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip http authentication** {**enable** | **local** | **tacacs**}	Configures the HTTP server interface for the type of authentication that you want to use. • **enable**—Enables the password, which is the default method of HTTP server user authentication. • **local**—Specifies the local user database, as defined on the Cisco router or access server. • **tacacs**—Specifies the TACACS server.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entries.

Note

- IE-2000-4S-TS-G do not have copper ports for PC, a Gigabit GLC-T copper SFP is required to perform express setup.
- If the Express Setup failed in the Web Browser, use the reset button to reset the switch to factor default

Caveats

The following sections provide information about caveats. You can click the issue number to view more information in the Cisco Bug Search tool (login required):

- Open Caveats, page 15
- Caveats Resolved in Cisco IOS Release 15.2(2)E6, page 15
- Caveats Resolved in Cisco IOS Release 15.2(2)E5, page 15
- Caveats Resolved in Cisco IOS Release 15.2(2)E4, page 15
- Caveats Resolved in Cisco IOS Release 15.2(2)E3, page 15
- Caveats Resolved in Cisco IOS Release 15.2(2)E2, page 16
- Caveats Resolved in Cisco IOS Release 15.2(2)E1, page 16
- Caveats Resolved in Cisco IOS Release 15.2(2)E, page 17

Open Caveats

No Open Caveats.

Caveats Resolved in Cisco IOS Release 15.2(2)E6

Bug ID	Headline
CSCuz56319	PDs do not reliably auto back UP if power inline auto max 15400

Caveats Resolved in Cisco IOS Release 15.2(2)E5a

Bug ID	Headline
CSCvb19326	NTP leap second addition is not working during leap second event
CSCvb29204	BenignCertain on IOS and IOS-XE
CSCuv87976	CLI Knob for handling Leap second add/delete ignore/handle

Caveats Resolved in Cisco IOS Release 15.2(2)E5

Issue	Description
CSCux09996	CIPNAT Att 3 to attach NAT instance not working properly
CSCuv42560	Trustpool bundle fails to deploy on devices with smaller nvram space

Caveats Resolved in Cisco IOS Release 15.2(2)E4

Issue	Description
CSCuv37518	PoE ports report fault when shut and/or PoE is disabled

Caveats Resolved in Cisco IOS Release 15.2(2)E3

Issue	Description
CSCul73513	Server-client clock not in sync after leap configuration
CSCum17258	EPM_SESS_ERR: Error in activating feature (EPM ACL PLUG-IN)
CSCup81878	Line by Line Sync fails while deleting dynamic NTP peer

Issue	Description
CSCur11439	Energywise Activitycheck powers off phone during an active call
CSCur58372	"snmp-server enable traps syslog" shows in "show run all" output after removal
CSCur59242	Crash due to tplus_client_stop_timer
CSCus09761	IOS-Phone not placed in critical voice VLAN when AAA server is unreached
CSCus13924	Device crashes while configuring 'Identity' commands
CSCus47009	Switch does not increment the "Received on untrusted ports" DHCP counter
CSCus79132	Dot1x authentication legacy behavior broken
CSCut10251	Some commands are not in running-config after AUTOINSTALL finishes
CSCut13064	BPDU filter does not work on output port when STP is disabled
CSCut20271	C3560X responds to ARP request from management port
CSCut27272	CPUHOG and crash due to Auth Manager process
CSCut79680	ip default-gateway is not seen in running-config after AUTOINSTALL
CSCut87425	CPU hog in "EEM TCL Proc" after TCL script termination with long runtime
CSCuu50392	Auth Manager memory leak with ISE authentication
CSCuu97116	Acct messages should include Class attribute from authentication
CSCuv06451	IOSd crash in eap_auth_terminal_state calling free_internal

Caveats Resolved in Cisco IOS Release 15.2(2)E2

No caveats were resolved in this release

Caveats Resolved in Cisco IOS Release 15.2(2)E1

Issue	Description
CSCun80959	Desg port on the RootBridge experienced block forward for 30 sec
CSCup96299	IPv6 Multicast RIB entry refer to wrong distance
CSCuq10827	C3560X cHsrpGrpStandbyState is incorrect
CSCur00722	Hard Reset of the Active Sup cause switch to power cycle

Caveats Resolved in Cisco IOS Release 15.2(2)E

Issue	Description
CSCtn27420	The switch maintains an IP device tracking table to store information about detected hosts. In 15.2(1)EY, IP Device Tracking (IPDT) is globally enabled. To avoid the ARP probing caused by race conditions or duplicate ip addresses (CSCui55905) the IPDT has been disabled at the interface level by default. This includes IE2000 with command [ip device tracking maximum 0]. In 15.2(2)E, a new global command is added to allow a user-defined ARP request source IP instead of using the default source IP 0.0.0.0. The new global command “ip device tracking probe auto-source fallback 0.0.0.x 255.255.255.0 override” allows the user to use the host address of 0.0.0.x in the subnet to avoid any duplicate IP address problems.
CSCun95906	On Cisco IE 2000, you can use an SD card as the boot device and to store a configuration file. (For information about how to use SD card, see *Using an SD Card with the Cisco IE 2000 Switch, Cisco IOS Release 15.0(2)EA1* here: http://www.cisco.com/c/dam/en/us/td/docs/switches/lan/cisco_ie2000/hardware/sd-card/sd_card.pdf.) However, because crypto keys are not stored on an SD card for security reasons, you could be locked out from accessing a new switch when you use an SD card to boot up the switch. An enhancement in 15.2(2)E provides for automatic regeneration of the key if SSH is properly configured. This enhancement ensures seamless zero touch replacement of a switch.

Documentation Updates

- Related Documentation, page 17

Related Documentation

Installation, Configuration, Maintenance, and Operation Guides

http://www.cisco.com/en/US/products/ps11245/tsd_products_support_series_home.html

Online Help (available on the switch)

- Express Setup online help
- Device Manager online help

SFP Information

- Compatibility Information: www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html
- Installation Notes: www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

MIBs

- MIBs for this product are listed in the datasheet: www.cisco.com/en/US/prod/collateral/switches/ps9876/ps12451/data_sheet_c78-705523.html
- MIBs can be located with this MIB tool by using the IOS version number: tools.cisco.com/ITDIT/MIBS/

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.