



Release Notes for Cisco IOS Release 15.2(4)EA9a

First Published: February 7, 2020

Last Updated: February 11, 2020

Cisco IOS Release 15.2(4)EA9a runs on these platforms:

- Cisco Industrial Ethernet 2000 Series Switches
- Cisco Industrial Ethernet 2000U Series Switches
- Cisco Industrial Ethernet 3000 Series Switches
- Cisco Industrial Ethernet 3010 Series Switches
- Cisco Industrial Ethernet 4000 Series Switches
- Cisco Industrial Ethernet 5000 Series Switches
- Cisco 2500 Series Connect Grid Switches
- Cisco Embedded Service 2020 Series Switches
- Cisco Ethernet Switch Module (ESM) for Cisco 2000 Series Connected Grid Routers

These release notes include important information about Cisco IOS Release 15.2(4)EA9a and any limitations, restrictions, and caveats that apply to the release. Verify that these release notes are correct for your switch.

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** command. See [Finding the Software Version and Feature Set, page 6](#).
- If you are upgrading to a new release, see the software upgrade filename for the software version. See [Deciding Which Files to Use, page 7](#).

For a complete list of documentation for the platforms associated with this release, see [Related Documentation, page 15](#).

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

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

Organization

This document includes the following sections:

Conventions, page 2	Conventions used in this document.
Feature Support in Cisco IOS Release 15.2(4)EA9a, page 4	Lists all features supported in Release 15.2(4)EA9a.
System Requirements, page 6	System requirements for Release 15.2(4)EA9a.
Upgrading the Switch Software, page 6	Procedures for downloading software.
Limitations and Restrictions, page 9	Known limitations in this release.
Caveats, page 11	Open and resolved caveats in Release 15.2(4)EA9a.
Documentation Updates, page 11	Updates to the IE switch product documentation.
Related Documentation, page 15	Links to the documentation for the hardware platforms associated with this release.

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Conventions

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning: IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Feature Support in Cisco IOS Release 15.2(4)EA9a

Cisco IOS Release 15.2(4)EA9a is a *bug fix only* release; however, it supports all the features first introduced by Cisco IOS 15.2(4)EA1 as listed in [Table 1](#).

This release also supports the [IE 5000 features introduced in Cisco IOS Release 15.2\(2\)EB and EB1](#).

Table 1 New Feature Summary for Cisco IOS Release 15.2(4)EA1

Feature	Platform	Description	Related Documentation
NTP to PTP Translation (Time Services)	IE 5000	This time service enhancement allows the IE switches to act as Grandmaster clocks to the PTP hierarchy with NTP as the time source. The NTP time source ties the PTP working clock to the everyday “wall clock.” This allows the customer to use PTP and NTP generated timestamps together during troubleshooting and analysis. In addition, NTP is more cost effective and robust than GPS for applications that only need 1 second precision for wide-area synchronization.	<ul style="list-style-type: none"> ■ Precision Time Protocol Software Configuration Guide for IE 4000 and IE 5000 Switches ■ Device Manager Online Help
Media Redundancy Protocol (MRP) and PROFINET Enhancements	IE 4000	<p>MRP (Media Redundancy Protocol), an open standard industrial protocol, can support up to 50 nodes with maximum recovery time up to 200ms.</p> <p>MRP operates at the MAC layer and is commonly used in conjunction with the PROFINET standard for industrial networking in manufacturing.</p> <p>This release supports MRP manager and client and includes the following enhancements to PROFINET:</p> <ul style="list-style-type: none"> ■ PROFINET stack upgrade to version 2.31. ■ PROFINET support for MRP Manager (MRM) and Client (MRC) functionality. PROFINET (PNIO) Certification with v2.3 	<ul style="list-style-type: none"> ■ Media Redundancy Protocol Configuration Guide for IE 2000 and IE 4000 Switches ■ Device Manager Online Help
Hardware Watchdog Reset	IE 4000 IE 5000	The Hardware Watchdog Reset feature causes the switch to reload if IOS software is unresponsive for a certain period of time (5 minutes). The CPU Hardware Watchdog ensures that the switch reloads if software is hung for whatever reason.	Hardware Watchdog Reset, page 12

Table 1 New Feature Summary for Cisco IOS Release 15.2(4)EA1

Feature	Platform	Description	Related Documentation
MACsec (IEEE 802.1AE)	IE 5000	<p>MACsec is the IEEE 802.1AE standard for providing strong cryptographic protection at Layer 2. MACsec provides secure (encryption and authentication) MAC Service on a frame-by-frame basis. MACsec provides secure communications between stations that are attached to the same LAN.</p> <p>MACsec is only supported on 1G uplinks.</p> <p>Note You must have the IP Service license installed to support the MACsec feature.</p>	Configuring MACsec Encryption
Express Setup enhancements with CIP support for IE Switches	IE 5000	<p>This feature enhances Express Startup to limit manual switch intervention. There are three options for using Express Setup:</p> <ul style="list-style-type: none"> ■ You must configure a new in the box (NIB) switch that has no configuration file loaded (config.text / vlan.dat) directly via a console cable. ■ You can configure the switch with the existing Express Setup method. <p>The existing Express Setup behavior is enhanced to improve the failure LED indication behavior.</p> <ul style="list-style-type: none"> ■ You can have an IP address assigned to the switch without using Device Manager if you installed the switch in an already running environment with certain services available (DHCP). 	<ul style="list-style-type: none"> ■ Device Manager Online Help ■ Express Setup Enhancements, page 12 ■ For details on Express Setup documentation for all IE switches, see the Express Setup Program entry in Table 3Methods for Assigning IP Information, page 9
Locate Switch	IE 5000	<p>When enabled, Locate Switch causes all possible LED to glow in ALT_RED and GREEN once the locate switch is enabled with a specific time. This performance varies from previous releases. (CSCux75707)</p> <p>The Locate Switch time setting has been changed from <9-255> to <0-255> time in seconds: 0: Stop Blink 9-255: Blink LED</p> <p>Enter the following show command to verify your settings:</p> <pre>Switch# sh locate-switch Locate Switch enabled!! time left: 249 sec</pre>	<ul style="list-style-type: none"> ■ Device Manager Online Help

System Requirements

Table 1 New Feature Summary for Cisco IOS Release 15.2(4)EA1

Feature	Platform	Description	Related Documentation
Device Manager (DM) Enhancements	IE 4000, IE 5000	<ul style="list-style-type: none"> Ability to launch Device Manager in Express Setup medium press mode (as well as previously supported short press mode). 	<ul style="list-style-type: none"> Device Manager Online Help

System Requirements

This section describes the following system requirements for Cisco IOS Release 15.2(4)EA9a

- [Express Setup Requirements, page 6](#)

Express Setup Requirements

This section summarizes the hardware and software requirements for the Windows platform.

For a listing of Express Setup documentation, see [Table 1 New Feature Summary for Cisco IOS Release 15.2\(4\)EA1, page 4](#).

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 32) 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 Software

These are the procedures for downloading software. Before downloading software, read these sections for important information:

- [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 8](#)
- [Installation Notes, page 9](#)

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. The image is stored on the compact flash memory card.

Upgrading the Switch Software

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 can also use the **dir filesystem:** privileged EXEC command to see the directory names of other software images stored in flash memory. For example, use the **dir flash:** command to display the images in the flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform an upgrade by using a combined tar file which contains the Cisco IOS image and the files needed for PROFINET GSD, CIP EDS and the Web Device Manager; and, in some cases, the FPGA upgrade files.

To upgrade the switch through the CLI, use the combined tar file and the **archive download-sw** privileged EXEC command to overwrite the older image completely.

Table 2 lists the filenames for this software release.

Table 2 Cisco IOS Software Image Files

File Name	Description
cgs2520-ipserviceslmk9-tar.152-4.EA9a.tar	CGS 2520 IP services image file
cgs2520-lanbaselmk9-tar.152-4.EA9a.tar	CGS 2520 LAN base image file
grwicdes-ipserviceslmk9-tar.152-4.EA9a.tar	ESM IP services image file
grwicdes-lanbaselmk9-tar.152-4.EA9a.tar	ESM LAN base image file
c2020-universalk9-tar.152-4.EA9a.tar	ESS 2020 universal image file
ie2000-universalk9-tar.152-4.EA9a.tar	IE 2000 Universal image file
ie2000u-ipserviceslmk9-tar.152-4.EA9a.tar	IE 2000U Universal image file
ie2000u-lanbaselmk9-tar.152-4.EA9a.tar	IE 2000U LAN base image file
ies-ipservicesk9-tar.152-4.EA9a.tar	IE 3000 Universal image file
ies-lanbasek9-tar.152-4.EA9a.tar	IE 3000 LAN base image file
ie3010-ipservicesk9-tar.152-4.EA9a.tar	IE 3010 IP services image file
ie3010-lanbasek9-tar.152-4.EA9a.tar	IE 3010 LAN base image file
ie4000-universalk9-tar.152-4.EA9a.tar	IE 4000 Universal image file
ie5000-universalk9-tar.152-4.EA9a.tar	IE 5000 Universal image file

Archiving Software Images

Before upgrading your switch software, make sure that you archive copies of both your current Cisco IOS release and the Cisco IOS release to which you are upgrading. Keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and 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 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 download the tar file from Cisco.com and archive it on an internal host in your network.

Upgrading the Switch Software

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.

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: Make sure that the compact flash card is in the switch before downloading the software.

To download software, follow these steps:

1. Use [Table 2 on page 7](#) to identify the file that you want to download.
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://software.cisco.com/download/navigator.html>

For example, to download the image for an IE 4000 switch, select Products > Switches > Industrial Ethernet Switches > Cisco Industrial Ethernet 4000 Series Switches, then select your switch model. Select IOS Software for Software Type, then select the image you want to download.

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 the “Assigning the Switch IP Address and Default Gateway” chapter in the applicable document for your switch as listed in [Table 3](#).

4. Log into the switch through the console port or a Telnet session.
5. (Optional) Ensure 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 [Table 3](#).

6. Download the image file from the TFTP server to the switch.

If you are installing the same version of software that currently exists 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 command above untars/unzips the file. The system prompts you when it completes successfully.

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

If you specify the command without the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch Flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message displays.

- 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. or hostname.
- For **/directory/image-name.tar**, specify the directory and the image to download. Directory and image names are case sensitive. The directory is for file organization and it is generally a *tftpboot/user-ID* path.

Limitations and Restrictions

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. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message displays.

Installation Notes

You can assign IP information to your switch using the methods shown in [Table 3](#).

Table 3 Methods for Assigning IP Information

Method	Platform	Document
Express setup program	IE 2000	Cisco IE 2000 Switch Hardware Installation Guide , Device Manager Online Help
	IE 3000	Cisco IE 3000 Switch Getting Started Guide , Device Manager Online Help
	IE 3010	Cisco IE 3000 Switch Getting Started Guide , Device Manager Online Help Note: The Cisco IE 3000 Switch Getting Started Guide serves as Express Setup reference for the IE 3010.
	IE 4000	Cisco IE 4000 Switch Hardware Installation Guide
	IE 5000	Cisco IE 5000 Hardened Aggregator Hardware Installation Guide
CLI-based setup program	IE 4000	Cisco IE 4000 Switch Hardware Installation Guide
	IE 5000	Cisco IE 5000 Hardened Aggregator Hardware Installation Guide
DHCP-based autoconfiguration	IE 4000	Cisco Industrial Ethernet 4000 Series Switch Software Configuration Guide
	IE 5000	Cisco IE 5000 Hardened Aggregator Hardware Installation Guide
Manually assigning an IP address	IE 4000	Cisco Industrial Ethernet 4000 Series Switch Software Configuration Guide
	IE 5000	Cisco IE 5000 Hardened Aggregator Hardware Installation Guide

Limitations and Restrictions

We recommend that you 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 for these issues. Some features might not work as documented, and some features might be affected by recent changes to the switch hardware or software. These caveats have a status of Closed.

■ CSCuo83410

Symptom When a port gets congested, classes with a larger queue-limit size are not receiving more frames per second than the classes with a smaller queue-limit size.

Limitations and Restrictions

Conditions This issue occurs on the IE 4000 when queue-limit sizes are configured unequally in classes. Classes with a larger queue-limit size are not receiving more frames per second than the classes with a smaller queue-limit sizes.

Workaround There is no workaround for this issue.

■ CSCuq21005

Symptom In-line editing becomes unresponsive on the Device Manager Port Thresholds page on IE 2000, IE 3000 and IE 4000 switches.

Conditions Editing a field too quickly can cause in-line editing to become unresponsive.

Workaround Editing the box repeatedly works if the user waits one or two seconds for Device Manager to push the update to the device.

■ CSCur09517

Symptom The PRP LED did not light up correctly. Observed anomalies in PRP LED in the events below:

Conditions Impacted platform: IE4K

1. Issue a **shut/no shut** on logical PRP interface (interface prp-channel 1|2).
2. Unplug and plug in cables for uplink ports.
3. Certain sequence issues observed with issuing **shut/no shut** on logical interface PRP-channel 1 followed by logical interface PRP-channel 2 and vice versa.

Workaround There is no workaround for this issue.

■ CSCus02105

Symptom **show cip object v4router 0** does not display correct routes in some scenarios. Issue was first seen on an IE 2000; however, it applies to all IE and CG switches that support VLAN configuration and CIP features.

Conditions If you configure a cip unsupported route, for example, ip route 0.0.0.0 0.0.0.0 fa 1/1 172.27.168.129. the route will not be displayed properly in the **sh cip object v4router** command output. All following routes (including supported routes such as ip route 0.0.0.0 0.0.0.0 fa 1/1 or ip route 172.27.168.129 vln 1) also will not be displayed properly.

Workaround Reload the switch.

■ CSCut31523

Symptom Switch running Parallel Redundancy Protocol (PRP) disables PRP1 interface at least twice at random periods.

Conditions IE 4000 running release 15.2(2) with Parallel Redundancy Protocol (PRP) configured.

Workaround To re-enable PRP on the switch, connect to the switch via a console port and enter **shut** and then **no shut** commands on the PRP1 interface.

■ CSCuv46039

Symptom Interface link flaps occurred on the IE 4000 with use of aggressive **lsl-age** timer under REP port configuration.

Conditions This issue occurs in a REP Ring with three or more nodes with **lsl-age** timer set to 120 msecs and after a period of a few minutes to a couple of hours.

Another side affect could be a malloc failure (CAM flush) with repeated link flaps which may cause the switch to crash.

Workaround Increase **rep lsl-age** timer to a value greater then 120 msec. Recommended value is 3000 msec.

Caveats

- **CSCuw28503**

Symptom On IE platforms, Flex-Link failover time could be around 700msec when using Gigabit Ethernet ports.

Conditions Steps to reproduce:

1. Configure two Gig links on the IE switch as flex links.
2. Shut a member link and wait for the traffic to switch over to the other link. Failover time of around 700 msec is seen.

Workaround Use Fast Ethernet ports to implement Flex-Link.

Caveats

This section addresses the open and resolved caveats in this release and provides information on how to use the Bug Search Tool to find further details on those caveats. This section includes the following topics:

- [Table 4 Resolved Caveats, page 11](#)
- [Cisco Bug Search Tool, page 11](#)

Table 4 Resolved Caveats

Bud ID	Headline
CSCvs39599	Modify Reload Reason: When switch reloads due to Profinet DCP reset request (all IE platforms)
CSCvs46080	Self-signed certificates expire on 00:00 1 Jan 2020 UT (IE2000, IE3000, IE4000, IE4010, IE5000)

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat listed in this document:

1. Access the BST (use your Cisco user ID and password) at <https://tools.cisco.com/bugsearch/>
2. Enter the bug ID in the Search For: field.

Documentation Updates

This section includes the following late updates to documentation for IE switches:

- [No Support for MAB + NEAT, page 12](#)
- [Enabling Logging Alarms for Syslog Messages, page 12](#)
- [Hardware Watchdog Reset, page 12](#)
- [Express Setup Enhancements, page 12](#)
- [Locate Switch, page 14](#)

No Support for MAB + NEAT

Please note that MAB + NEAT **is not** supported on CGS2520s in the Cisco 15.2(4)EA Releases (15.2(4)EA1 through 15.2(4)EA9a). MAB + NEAT may be incorrectly noted as supported in the “802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)” sections of 15.2(4)EA User Documentation.

Enabling Logging Alarms for Syslog Messages

The following information is relevant to all IE Switches software releases from Release 12.2(58)SE onward (CSCvg26502).

On IE switches, there is an option to configure temperature alarm levels as noted in the “[Configuring the Switch Alarms: Associating the Temperature Alarms to a Relay](#)” section within IE Switch Software Configuration Guides.

However, configured alarms do not generate any syslogs until you set Major alarm **logging alarm 2** and Minor alarm **logging alarm 3** for temperature threshold alarms.

IMPORTANT: The logging alarm **must be enabled** to generate syslog messages.

Hardware Watchdog Reset

The expected behavior on the switch when there is an IOS software problem is for the switch to crash, save the information that helps software engineers debug the crash, and then reload. However, there can be rare occurrences of the switch hanging without crashing. Hangs are very hard to reproduce and even harder to fix because there is no trace of what caused the hang. Following are some of the symptoms when the switch hangs:

- Switch becomes totally unresponsive to the CLI
- Traffic forwarding stops
- LEDs stop blinking
- Switch does not save any crash information
- Switch does not reload

The switch not reloading is a very serious issue, especially for IoT deployments in remote and sometimes hard to reach locations where sending personnel to reload the box is expensive, time consuming, and leads to the system being rendered unusable for that time.

The Hardware Watchdog Reset feature causes the switch to reload if IOS software is unresponsive for a certain period of time (5 minutes). The CPU Hardware Watchdog ensures that the switch reloads if software is hung for whatever reason.

Configuring Hardware Watchdog Reset

This feature is enabled by default. The following CLI command disables and re-enables this feature:

```
(config)# boot hardware-watchdog disable
(config)# no boot hardware-watchdog disable
```

This command requires a reboot to take effect.

The scheduler process-watchdog (software) remains in effect even after this feature is disabled.

Express Setup Enhancements

Express Setup has three options to meet the needs of different installer roles. You select an option based on how long you press the Express Setup button.

Documentation Updates

- **Short press mode**—You want to use the existing Express Setup method.
The existing Express Setup behavior has improved failure LED indication.
- **Medium press mode**—You are installing a switch into an already running environment with certain services available (DHCP) or you want to have the device receive an IP address without using Device Manager.
- **Long press mode**—You are confident and knowledgeable in the use of Cisco IOS CLI and can configure the switch directly using a console cable.

Table 5 summarizes Express Setup for each mode.

Table 5 Express Setup Modes

	Short Press Mode	Medium Press Mode	Long Press Mode
Press duration	1-4 seconds.	5-10 seconds.	15-20 seconds.
LED blinking pattern (start and end of Express Setup)	Blinks green from 1-4 seconds.	Blinks red from 4-10 seconds.	Blinks alternating green and red from 15-20 seconds.
Abort Express Setup	Express Setup button released between 10-15 seconds (Express Setup Indicator LED is off).	Express Setup button released between 10-15 seconds (Express Setup Indicator LED is off).	Express Setup button released after 20 seconds (Express Setup Indicator LED is off).

Table 5 Express Setup Modes (continued)

	Short Press Mode	Medium Press Mode	Long Press Mode
Description	<ul style="list-style-type: none"> ■ Express Setup management interface is selected. ■ DHCP Server is set up on VLAN 1000 with an address of 192.168.1.254. ■ The port LED changes from blinking green to solid green once the PC - Switch link comes up. ■ Once DHCP session is successfully established, the PC is assigned an IP address of 192.168.1.1 on VLAN 1 and the Express Setup indicator LED changes from blinking green to solid green. ■ The user starts a browser session and Device Manager (DM) Express Setup page opens with default username and password set to "no username" / cisco. ■ The user configures the Switch from DM Express Setup page. 	<ul style="list-style-type: none"> ■ DHCP request is sent out of all ports on VLAN 1. ■ Express Setup indicator LED blinks alternating green and red while waiting for DHCP response. ■ Upon DHCP response, Express Setup indicator LED blinks green for 5 seconds and is then turned off. ■ VLAN 1 is configured for the IP address returned, and default password is set to "no username"/cisco ■ CIP is enabled on VLAN 1 with CIP security password set to "switch". ■ If non-default switch configuration is detected or If no DHCP response is received for 5 minutes from when the DHCP request was transmitted, Express Setup is aborted and the EXP/Setup indicator LED turns solid red (for 10 seconds). 	<ul style="list-style-type: none"> ■ All configuration and settings (config.text, vlan.dat, and private-config.text files) on-board and SD Flash are reset to factory defaults. ■ Switch reloads and comes up with factory default settings.

Locate Switch

You can configure Locate Switch using CLI and the Device Manager.

When enabled, **Locate Switch** causes all possible LEDs to glow ALT_RED and GREEN (LEDs that are in one color blink) once the switch is enabled with a specific time. This performance varies from previous releases (CSCux75707).

The Locate Switch time setting has been changed from <9-255> to <0-255> time in seconds:

```
switch# locate-switch?
<0-255> time in seconds
0      : Stop Blink
9-255: Blink LED
```

Enter the following **show** command to verify your settings:

```
Switch# sh locate-switch
Locate Switch enabled!!
time left: 249 sec
```

The **locate-switch** command is a volatile command and will not be saved or displayed in running or startup configuration.

Related Documentation

Table 6 Related Documentation

Device or Feature	Related Documents
Cisco Industrial Ethernet 2000 Series Switches	http://www.cisco.com/go/ie2000
Cisco Industrial Ethernet 2000U Series Switches	http://www.cisco.com/go/ie2000U
Cisco Industrial Ethernet 3000 Series Switches	http://www.cisco.com/go/ie3000
Cisco Industrial Ethernet 3010 Series Switches	http://www.cisco.com/go/ie3010
Cisco Industrial Ethernet 4000 Series Switches	http://www.cisco.com/go/ie4000
Cisco Industrial Ethernet 5000 Series Switches	http://www.cisco.com/go/ie5000

© 2020 Cisco Systems, Inc. All rights reserved.

Related Documentation