Release Notes for Cisco IOS Release 15.2(5a)E1 for the IE 4010

Last Updated: February 27, 2018

First Published: December 23, 2016

Cisco IOS Release 15.2(5a)E1 runs on the following platform:

- Cisco Industrial Ethernet 4010 Series Switches (IE 4010)

Note: Cisco IOS Release 15.2(5a)E1 is a bug fix only release. There are no new features introduced in this release.

These release notes include important information about Cisco IOS Release 15.2(5a)E1 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 4.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See Deciding Which Files to Use, page 4.

For a complete list of documentation for the platforms associated with this release, see Related Documentation, page 11.

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.
System Requirements, page 3	System requirements for Releases 15.2(5a)E1.
Upgrading the Switch Software, page 3	Procedures for downloading software.
Limitations and Restrictions, page 6	Known limitations in this release.
Caveats, page 6	Open caveats in Release15.2(5a)E1.
Documentation Updates, page 10	Updates to the IE switch product documentation.
Related Documentation, page 11	Links to the documentation for the hardware platforms associated with this release.
Obtain Documentation and Submit a Service Request, page 11	Link to information about Cisco documentation.

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	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 `courier` font.
< >	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.

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.

System Requirements

This section describes the following system requirements for Cisco IOS Release 15.2(5a)E1:

- Express Setup Requirements, page 3

Express Setup Requirements

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

For a listing of Express Setup documentation, see Table 2Methods for Assigning IP Information, page 6.

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 4
- Deciding Which Files to Use, page 4
- Archiving Software Images, page 4
- Upgrading a Switch by Using the CLI, page 5

■ Installation Notes, page 6

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.

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 the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through Express Setup. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 1 lists the filenames for this software release.

Note: If you download the IP services image and plan to use Layer 3 functionality, you must use the Switch Database Management (SDM) routing template. To determine the currently active template, enter the **show sdm prefer** privileged EXEC command. If necessary, enter the **sdm prefer** global configuration command to change the SDM template to a specific template. For example, if the switch uses Layer 3 routing, change the SDM template from the default to the routing template. You must reload the switch for the new template to take effect.

Note: Beginning with Cisco IOS Release 15.2(5)E, we **no longer release** the IE 3000 IP services image. The latest release for the IP services image on the IE 3000 is 15.2(4)EA1.

Table 1 Cisco IOS Software Image Files

File Name	Description
ie4010-universalk9-tar.152-5a.E1.tar	IE 4010 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.

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 1 on page 4 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 4010 switch, select Products > Switches > Industrial Ethernet Switches > Cisco Industrial Ethernet 4010 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 2.
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 2.
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.

   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 2.

Table 2 Methods for Assigning IP Information

Method	Platform	Document
Express setup program	IE 4010	*Cisco IE 4010 Switch Hardware Installation Guide*
CLI-based setup program	IE 4010	*Cisco Industrial Ethernet 4000, 4010 and 5000 Switch Software Configuration Guide*
DHCP-based autoconfiguration	IE 4010	*Cisco Industrial Ethernet 4000, 4010 and 5000 Switch Software Configuration Guide*
Manually assigning an IP address	IE 4010	*Cisco Industrial Ethernet 4000, 4010 and 5000 Switch Software Configuration 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.

- **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.

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.

- **CSCut57413**

Symptom The PRP channel should not be in connected state when one of the ports is in suspended/not connected state.

Condition Any port configuration mismatch will put the port in a suspended state, and if that port is part of the PRP channel, the channel is still connected. This issue was seen on IE 4000.

Workaround Remove the conflicts in the port configurations. Entering **shut/no shut** will bring the port UP.

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:

- Open Caveats, page 7
- Resolved Caveats, page 7
- Accessing Bug Search Tool, page 10

Open Caveats

- **CSCvb17036**

Symptom By using GSD files, unable to configure media type as 'fiber'. Only "Copper" as a media type can be configurable.

Conditions Problem seen on IE2K and IE4K. Working fine on IE5000.

Workaround Use CLI to configure media type.

Resolved Caveats

- **CSCvc28935**

Symptom IE4010 reloads unexpectedly after configuring NTP server on the switch.

Conditions The following procedure is available to prevent the reboot cycle from occurring.

Make sure this command is issued within 5 minutes to prevent the reboot cycle from occurring.

Disable OBFL on the switch:

1. Power cycle the IE-4010 unit and wait for it to come to the IOS prompt.

2. At the IOS prompt disable OBFL by entering the following:

switch#config t

switch(config)#no hw-module module logging onboard

switch(config)#end

switch#wr memory

Workaround This issue is resolved in Cisco IOS Release 15.2(5a)E1.

- **CSCur35236**

Symptom RJ45 Link comes up on combo port with different Media Type on both sides.

Conditions Configure different Media Type on both sides for Combo ports.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCuv84571**

Symptom On the IE 4000 in Device Manager, changing between IP assignment modes deletes the static IP address.

Conditions Steps to reproduce:

1. Launch the device in a browser.
2. Select Configure > Network > VLAN Management.
3. Add a VLAN with a static IP address and save it.
4. Edit the same VLAN and switch between IP assignment modes (No IP Address, Static, and DHCP).
5. The created static IP address is deleted.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCux59845**

Symptom Boundary Clock does not forward PTP Management packets across VLANs on IE4000 and IE5000. This issue also affects IE2000 and IE3000.

Conditions Previous design had PTP Management packets forwarded within the same vlan. Design changes have PTP packets forwarded across different VLANs and routed ports.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCuy81921**

Symptom Traffic on Gig 1/4 ceases as soon as prp channel is added on IE 4000 and IE 5000. Observed the ping traffic did not go through.

Conditions When the SVI is created on both ends, assigned the IP address on both ends. Once the PRP channel is created, cannot ping the address of the other end.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCuz48728**

Symptom Encounter crash occurred on an IE-4000-4T4P4G-E running 15.2(4)EA or 15.2(4)EA1 with an uplink to a Catalyst 2000 switch.

Conditions IE-4000-4T4P4G-E running 15.2(4)EA or EA1 with an uplink port-channel to Catalyst 2000.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCuz65513**

Symptom The default ACL is not editable from DM but is editable from CLI.

Conditions This issue is seen when attempting to edit default ACL CISCO-CWA-URL-REDIRECT-ACL in Device Manager.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCva80784**

Symptom Any RJ-45 interface (G1/1 THROUGH G1/12), if configured with speed auto 1000 / duplex full, permits a switch or other device configured for auto-negotiation on a Fast Ethernet only-capable adapter to connect and operate at 100/full.

Conditions

SKU: IE-4010-16S12P, IOS: 15.2(4.5.12)EC IE4010-UNIVERSALK9-M

SKU: IE-5000-16S12P, IOS: 15.2(5)E IE5000-UNIVERSALK9-M

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCva85646**

Symptom Alarm setting for SD card not present on the IE 4010.

Conditions This issue is seen on the IE-4010-4S24P running Cisco IOS 15.2(4.5.14)EC.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCva96583**

Symptom PRP duplication removes weakness against introduced delay/jitter.

Conditions PRP duplication failure to remove percentage is reaching 100 percent when introduced delay is 3 ms for two flows; also PRP duplication failure to remove percentage is 32.9 percent when introduced jitter is 3 ms even for single flow.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb04864**

Symptom Profinet check box is not enabled by default.

Conditions

1. Perform a short press or medium press.
2. Open the DM Express Setup page from PC.
3. The second Express Setup page should show the Profinet check box enabled by default, but it is not enabled.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb11859**

Symptom In Device Manager on the IE 4010, Port Settings-Auto mdix options should not be grayed out.

Conditions Steps to reproduce the issue:

1. Launch the device manager using Firefox.
2. Go to Configure-->Network--Port Settings.
3. Click on Edit interface option by selecting any of the one interface.
4. Auto MDIX option is grayed out and cannot be enabled or disabled.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb32407**

Symptom Device Manager login page displays “undefined” instead of “Confirm password”.

Conditions Steps to reproduce:

1. Perform a short press on the device.
2. Connect to the PC to open the DM Express Setup page.
3. Enter the first login password.
4. The second login configuration should show the login name and password and “Confirm password”.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb40748**

Symptom A timed-out CIP connection class 1 connection that is missing its associated session crashes CIP connection manager when it tries to close its UDP socket.

Conditions A session may be missing for a variety of reasons, such as switch IP address removed/updated, UCMM unregister, ENIP encap timeout or error, or UDP socket block or send error.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

- **CSCvb45849**

Symptom Device Manager Port Settings page on the IE 4010 did not show port type in edit window.

Conditions Steps to reproduce:

1. Go to Configure -->Port Settings.
2. Select the port and click edit window.
3. Check for the port type in the edit window. The port type is mentioned in online help and seen in the console but this is not available in the port setting page on DM page.

Workaround This issue is resolved in Cisco IOS Release 15.2(5)E1.

Accessing Bug Search Tool

You can use the Bug Search Tool to find information about caveats for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To access the Bug Search Tool, enter the following URL:

bst.cloudapps.cisco.com/bugsearch

Documentation Updates

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

- Enabling Logging Alarms for Syslog Messages, page 10
- Resilient Ethernet Protocol (REP), page 10
- Related Documentation, page 11

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 l**ogging alarm 3** for temperature threshold alarms.

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

Resilient Ethernet Protocol (REP)

See the revised configuration recommendations for the **lsl-age-timer** *timer-value* command (CSCux92117) in the "Configuring REP Configurable Timers" section in the REP chapter of the LAN Switching Configuration Guide, Cisco IOS XE Release 3S.

Related Documentation

Table 3 Related Documentation

Device or Feature	Related Documents
Cisco Industrial Ethernet 4010 Series Switches	http://www.cisco.com/go/ie4010

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

No combinations are authorized or intended under this document.

© 2016–2018 Cisco Systems, Inc. All rights reserved.