Release Notes for the Cisco Edge 300 Series Switch, Release 1.6

First Published: 2014-11-18

Last Modified: 2017-06-16

Release Notes for the Cisco Edge 300 Series Switch, Release 1.6

These release notes include important information about Cisco Edge 300 Software Release 1.6 and any limitations, restrictions, and caveats that apply to this release.

Supported Hardware

Table 1: Cisco Edge 300 Series Switch Supported Hardware

Switch	Description
CS-E300-AP-K9	Cisco Edge 300 series switch with WiFi and Bluetooth
CS-E300-K9	Cisco Edge 300 series switch
HS-E300-AP-K9[1]	HSJC/Cisco Edge 300 series switch with WiFi and Bluetooth
HS-E300-K9[2]	HSJC/Cisco Edge 300 series switch

1 This model is available only in China.

2 This model is available only in China.

Central Management and Configuration

The Cisco Edge 300 series switches function exclusively in a Smart Install network. Smart Install is a plug-and-play configuration and image-management feature, which means that once the Cisco Edge 300 series switch is placed in the network and powered on, it can work without a local configuration required.

Smart Install Network

A network using Smart Install includes a group of networking devices, including clients and a server. The server can be a common Layer 3 switch or a router that acts as a director.

All Cisco Edge 300 series switches function as Smart Install client switches in a Smart Install network. End users do not configure the client switches; all switches are centrally configured through a GUI that is installed on a TFTP server and managed by the director.

Note For more information, see the "Configuring the Smart Install Network" chapter in the software configuration guide for this release. For detailed information about Smart Install and the Smart Install director, see the http://www.cisco.com/en/US/docs/switches/lan/smart_install/release_12.2_58_se/configuration/guide/smart_install.html Smart Install Configuration Guide, Release 12.2(58)SE .

Applying and Upgrading Images and Configuration Files

Caution Before upgrading from software release 1.5RB1 to release 1.6, remove the Factory Mode OS Version and Fonts selections from the GUI and apply the changes. See the "Configuring the Smart Install Network" chapter in the software configuration guide for this release.

Caution If the device was originally installed with software release 1.5 and higher, do not downgrade the software release to 1.4 or lower via USB manual upgrading. Otherwise, the device may be seriously damaged.

Note When you are going to upgrade the system from release 1.x to release 1.6RB1_1 or release 1.6RB2, you can use only the Force Upgrade option. For more details, see the "Using the USB Smart Install on Cisco Edge OS Version 1.1.0 and Later" section in *Cisco Edge 300 Series Switch Software Configuration Guide, Release 1.6* , at the following URL: http://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_edge_300/software/release/1_6/configuration/guide/ce300cg/Trouble.html#pgfId-1000185

When the switch starts up, it connects to the director. If the switch detects any new images or configuration files, it automatically restarts in factory-default mode and then downloads and installs the new images or configuration files.

These are the supported types of image and configuration upgrades:

- Upgrade initiated by the user—For a single client switch that is in the network and connected to the director. The user turns the switch off and on, and then the switch will connect to the director and can detect and download any new image or configuration files. The user can also press and hold the Reset button down for 5 seconds and then release it. The system starts to download and program itself with the configured image and configurations on the TFTP server.
- Upgrade initiated by the administrator—For a single client switch that is in the network and connected to the director. The administrator initiates the upgrade by connecting to the switch, for example, over a Telnet connection.

For more information, see the "Configuring the Smart Install Network" chapter in the software configuration guide for this release.

Note On-demand upgrades and scheduled downloads are not supported. You cannot upgrade switches from the director by using the **write erase** and **reload**, **vstack download-image**, **vstack download-config**, or **archive download-sw** privileged EXEC commands.

After installing the release 1.6RB1_1 software, you need to update the following patches as they are not included:

- Patch to Fix CSCur52554 (SSLv3 POODLE Patch Version 0.1), on page 3
- Patch to Fix CSCur02761 (Bash Vulnerability), on page 4

Recovering from a Software Failure

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

Software Images

Filename	Description
edge300-1.6RB4.tar	Cisco Edge 300 series operating system and Smart Install GUI installation package for release 1.6RB4
smi-usb-sunbird-1.6RB4-delivery.tar.gz	Cisco Edge USB Smart Install image for release 1.6RB4
edge300-1.6RB2.tar	Cisco Edge 300 series operating system and Smart Install GUI installation package for release 1.6RB2
smi-usb-sunbird-1.6RB2-delivery.tar.gz	Cisco Edge USB Smart Install image for release 1.6RB2
edge300-1.6RB1_1.tar	Cisco Edge 300 series operating system and Smart Install GUI installation package for release 1.6RB1_1
smi-usb-sunbird-1.6RB1_1-delivery.tar.gz	Cisco Edge USB Smart Install image for release 1.6RB1_1
edge300-1.6.0.tar	Cisco Edge 300 series operating system and Smart Install GUI installation package for release 1.6
md5.txt	md5 of edge300-1.6.0.tar and file in tar ball
smi-usb-sunbird-1.6.0-delivery.tar.gz	Cisco Edge USB Smart Install image for release 1.6

Patch to Fix CSCur52554 (SSLv3 POODLE Patch Version 0.1)

This is a generic patch for all the Cisco Edge 300 Series software releases, from release 1.1 to release 1.6.

Follow these steps to install the SSLv3 POODLE patch on your system:

SUMMARY STEPS

1. Log in as root to the Cisco Edge 300 with terminal through SSH or Desktop.
2. Copy or download the software package to the Cisco Edge 300 filesystem.
3. Manually install the patch, using **install.sh** contained in the package:
4. Reboot the system.
5. Follow the guidelines at the following URL to verify your installation:

DETAILED STEPS

Step 1 Log in as root to the Cisco Edge 300 with terminal through SSH or Desktop.

Step 2 Copy or download the software package to the Cisco Edge 300 filesystem.

Step 3 Manually install the patch, using **install.sh** contained in the package:

a) Use the following command to untar the patch, for example, to the /tmp folder:

Example:

```
# tar xvzf $folder/ce300-SSLv3-POODLE-patch-0.1.tar.gz -C /tmp/
```

b) (Optional) Back up the **/usr/local/cisco/nginx/conf/nginx.conf** binary file.

c) Go to the uncompressed folder of the patch and run **install.sh**:

Example:

```
# cd /tmp/ce300-SSLv3-POODLE-patch-0.1
# ./install.sh
```

After the patch is installed, the message "SSLv3 POODLE patch installed successfully" will be printed on the screen.

Step 4 Reboot the system.

Step 5 Follow the guidelines at the following URL to verify your installation:
https://access.redhat.com/articles/1232123

Note This patch can be installed repeatedly.

Patch to Fix CSCur02761 (Bash Vulnerability)

This is a generic patch for all the Cisco Edge 300 Series software releases, from release 1.1 to release 1.6, to fix the Bash vulnerability.

Follow these steps to install the patch on your system:

SUMMARY STEPS

1. Log in as root to the Cisco Edge 300 with terminal through SSH or Desktop.
2. Copy or download the software package to the Cisco Edge 300 filesystem.
3. Manually install the patch, using **install.sh** contained in the package:

DETAILED STEPS

Step 1 Log in as root to the Cisco Edge 300 with terminal through SSH or Desktop.

Step 2 Copy or download the software package to the Cisco Edge 300 filesystem.

Step 3 Manually install the patch, using **install.sh** contained in the package:

a) Use the following command to untar the patch, for example, to the /tmp folder:

Example:

```
# tar xvzf $folder/ce300-bash-vulnerability-patch-0.1.tar.gz -C /tmp/
```

b) (Optional) Back up the **/usr/local/cisco/bin/bash** binary file.

c) Go to the uncompressed folder of the patch and run **install.sh**:

Example:

```
# cd /tmp/ce300-bash-vulnerability-patch-0.1
# ./install.sh
```

If the patch has already been installed, the message "Bash already patched. Exit." will be printed on the screen. Otherwise, the message "Bash patch installed successfully" will be printed on the screen.

d) Follow the guidelines at the following URLs to verify your installation:
https://access.redhat.com/articles/1200223

https://shellshocker.net/

New Software Features in Release 1.6

Release 1.6 introduces the following new software features:

- Firmware upgrades enhancement—Provides HTTP-based API for firmware upgrade.
- Font adding—Supports to easily add custom fonts to the Cisco Edge 300 so that it can work at both desktop and application level. The change takes effect without rebooting. You can add fonts either by Clish with local file, or by SMI with remote file.
- Audio control—Supports both HTTP API and shell command.
- Daylight saving time auto adjustment—Supports automatic adjustment between daylight saving time and standard time by supporting NTPD.
- Location time support—Supports to set location-based time rather than time zone-based time via HTTP API and Clish.

- Low time tolerance—Supports to keep time tolerance less than 30 seconds after running one month by supporting NTPD.
- NTP sync-up interval configuration—Supports to configure the sync interval through GUI, API, and CLI. You can setup NTP server via GUI.
- Terminal GUI in factory and USB SMI image—Supports a Terminal GUI output to HDMI if you boot up to the Linux OS of factory mode or USB SMI image. You can:
  - View the process of factory system booting up or OS upgrading.
  - Access shell terminal after logging in as root to do debug or diagnosis.

Note Release 1.5RB1 and previous versions do not support any HDMI output in factory or USB SMI Linux OS.

- Terminal GUI when failing to mount internal USB Storage—Supports a Terminal GUI output to HDMI when the system fails to mount internal USB storage, so that you can debug with shell command in the terminal.

Note Release 1.5RB1 and previous versions will hang without any HDMI output when failing to mount internal USB storage.

- System files backup and restore—Supports to back up important boot-up scripts and configurations in the /backup folder when the first-time booting up after OS upgrading. You can also back up other files as needed.
- System log and cache file clean—Supports to do smooth clean of application logs or cache files.
- Logrotate service—Supports the open source tool Logrotate to rotate log to control the log file size. System will rotate log files every 1 hour at first minute: xx h 01 min. You can also add your own Logrotate configuration to the /etc/logrotate.d/ folder.
- Health monitor—Supports to monitor the status of CPU, memory, process, hard drive, NTP, and VLC, and record the error messages if there is any problem.
- USB console by USB-RS232 cable—Supports USB console by USB-RS232 cable.
- Disable 3G and Bluetooth by default—Supports to disable unnecessary TCP ports to reduce work load.

Limitations and Restrictions

- If CE300 needs to be downgraded to a lower version from release 1.6, 1.6RB1_1, or 1.6RB2, it should first be downgraded to release 1.5, then downgraded to release 1.3. The correct downgrade path is release 1.6/1.6RB1/ 1.6RB2 -> release 1.5 -> release 1.3.
- If you apply the 1.6RB2_2 or 1.6RB2_3 patch to your switch before you upgrade the switch from release 1.5, 1.5rb1, 1.6, or 1.6RB1_1 to 1.6RB2,
  - the Edge 300 switch will boot in Desktop mode and appsapce need to be re-registered;

- the NTP server settings will be wiped out and need to be reconfigured.
- Auto login and resolution of the Edge 300 switch will not be retained.

- The Cisco Edge 300 Series switches only support the following 3G dongle models:
  - Huawei EC1270, for CDMA2000
  - Huawei E261, for WCDMA
- Due to hardware limitation, Cisco Edge 300 Series switches do not support dual videos in one screen.
- The Cisco Edge 300 Series switches do not support stretching video streams played via VLC plugin, because:
  - The version of the VLC plugin used in Cisco Edge 300 Series does not support aspect ratio.
  - The PVR driver (third party code licensed to Intel) does not support stretching.
- Pressing the **Reset** button for 10 seconds will trigger an installation from the server or USB, but will not remove the local configuration from the device. The only way to remove the local configuration is to log in to the device via SSH or log in through the local console by connecting a keyboard and mouse, and then execute the following commands:

```
rm /etc/startup-config
rm -rf /apps/localconfig/*
```

Open Caveats in Release 1.6

- CSCun09221

HTTP API SET "api/1.0/sys/gateway" returns wrong status.

There is no workaround.

- CSCun20348

WiFi client cannot get IP address while using authentication of cisco PEAP (PEAPv1/EAP-GTC).

There is no workaround.

- CSCun20409

Mplayer cannot work properly with cache for certain video.

There is no workaround.

- CSCue17433

WiFi device may get lost with small possibility.

The workaround is to unplug the power line and reboot the DUT.

- CSCue39412

Video conference under WiFi client mode may cause the DSP buffer allocation to fail.

The workaround is the power cycle of the DUT.

- CSCtq80334

Ethernet LAN to 11n wireless performance cannot reach 80 mbps.
There is no workaround.

- CSCtr05376

Video overlays on mosaic function if there are more than two videos.
There is no workaround.

- CSCtr31770

No audio output after switching to the next page of Mosaic in the full screen mode.
There is no workaround.

- CSCue32448

Playing video in the full screen mode with flash plug-in may cause screen black.
The workaround is the power cycle of the DUT.

- CSCtr69972

System runs into DSP host buffer allocate failed state.
The workaround is the power cycle of the DUT.

- CSCtr77794

Mouse cursor gets stuck in busy state after accessing some apps.
There is no workaround.

- CSCtz90980

Tool bar functions and full screen mode of Flash Player does not work properly.
There is no workaround.

- CSCuc34169

DUT runs into DSP buffer allocate fail stat while running Mosaic.
The workaround is the power cycle of the DUT.

- CSCua22437

It takes long to access web when video conference is activate.
There is no workaround.

- CSCue27085

When playing two video with VLC plug-in, there may be broken noises.
There is no workaround.

- CSCtz55647

On-line media (YouTube) gets stuck on desktop after the browser is minimized.

The workaround is to stop playing the on-line media.

- CSCuc75379

Radius server configuration failed with Smart Install GUI.

The workaround is to configure the Radius server by web GUI or Clish.

- CSCum17707

Backup radius server does not work.

There is no workaround.

- CSCup25128

CE300 cannot play MPEG4 video in MKV well.

There is no workaround.

- CSCup06882

Codec MPEG2 can not playback smoothly with VLC plugin.

There is no workaround.

- CSCup04482

1024x768 resolution of ViewSonic VS14864 is not supported.

There is no workaround.

- CSCup09306

VC1 video cannot be played smoothly.

There is no workaround.

- CSCup14711

Security mode WPA/WPA2 Enterprise does not work after reboot.

The workaround is as following:

1. Plug Ethernet cable to GE port, and make sure it can get IP address.
2. Reboot the device.
3. When the device finish rebooting, log in to Web GUI, and click Apply button on the Wi-Fi page.

- CSCup14325

CE300 NAND flash issue.

There is no workaround.

- CSCup09410

Text tracker flicking at H.264 video in MP4.

There is no workaround.

- CSCup09370

One MPEG4 Video file cannot be played.

There is no workaround.

- CSCup28451

CE300 has mosaic when playing stream video.

There is no workaround.

Resolved Caveats in Release 1.6RB5_3

Table 2: Resolved Caveats

Caveat Number	Description
CSCvc94710	Evaluation of ce300 for OpenSSL Jan 2017
CSCvd72231	Evaluation of ce300 for NTP March 2017

Resolved Caveats in Release 1.6RB5_2

- CSCva52251

Importing SHA2 certificate for CE300.

Resolved Caveats in Release 1.6RB5_1

- CSCvc23555

Evaluation of CE300 for NTP November 2016.

- CSCvc08726

Evaluation of CE300 for OpenSSL November 2016.

Resolved Caveats in Release 1.6RB5

- CSCvb48672

Evaluation of CE300 for Openssl September 2016.

- CSCvb85669

Evaluation of CE300 for CVE-2016-5195 (DIRTY CoW).

- CSCuz92769

Evaluation of CE300 for NTP June 2016.

Resolved Caveats in Release 1.6RB4_3

- CSCus37394

Edge 300 does not support TLS 1.1 or 1.2, only TLS 1.0.

- CSCuv35027

Edge 300 returns incorrect/static serial number in sysDescr via SNMP.

- CSCux41425

Evaluation of CE300 for OpenSSL December 2015 vulnerabilities.

- CSCux95193

Evaluation of CE300 for NTP_January_2016.

- CSCuy07442

Evaluation of CE300 for OpenSSL January 2016.

- CSCuy35298

Evaluation of CE300 for glibc_Feb_2016.

- CSCuy54698

Evaluation of CE300 for OpenSSL March 2016.

- CSCuz44337

Evaluation of CE300 for NTP_April_2016.

- CSCuz52514

Evaluation of CE300 for OpenSSL May 2016.

Resolved Caveats in Release 1.6RB4_2

- CSCux18603

Device request for proxy credentials.

- CSCuw84983

Evaluation of CE300 for NTP_October_2015.

Resolved Caveats in Release 1.6RB4_1

- CSCuu82504

Evaluation of CE300 for OpenSSL June 2015.

Resolved Caveats in Release 1.6RB4

- CSCut46086

MARCH 2015 OpenSSL Vulnerabilities.

- CSCuu16999

Failed to upgrade with smi_local due to version check error.

Resolved Caveats in Release 1.6RB2_3

- CSCuu08669

Same version of image cannot be upgraded using SMI network upgrade.

Resolved Caveats in Release 1.6RB2_2

- CSCuu16999

Failed to upgrade with smi_local due to version check error.

This patch is applicable on release 1.5, 1.5RB1, 1.6, 1.6RB1_1 and 1.6RB2. which enables SMI local upgrade with version check. Once the patch is installed and upgraded to any of the above versions, the patch will no longer be available on the upgraded version. If you want to upgrade later, you will have to install this patch again to enable SMI local upgrade with version check.

Note To use smi_local to upgrade to release 1.6RB1_1 or 1.6RB2, the **upgrade-fm** option should be **on**. For more information on upgrading an image using smi_local, see the *Cisco Edge 300 Series Switch Software Configuration Guide, Release 1.6* at http://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_edge_300/software/release/1_6/configuration/guide/ce300cg/HttpAPI.html#pgfId-1056923

Resolved Caveats in Release 1.6RB2

- CSCur52554

TLS/SSL Server supports SSL version 3: POODLE/CVE-2014-3566.

- CSCur02761

Edge 300 evaluation for CVE-2014-6271 and CVE-2014-7169.

- CSCus69651

Evaluation of glibc GHOST vulnerability - CVE-2015-0235.

- CSCus27239

NTPd.org vulnerabilities.

- CSCus42801

OpenSSL vulnerabilities.

Resolved Caveats in Release 1.6RB1_1

- CSCul76460

CE300 corrupt file system after reboot and remains in hang status.

Resolved Caveats in Release 1.6

- CSCun20340

Need to double reboot when using the old-version SMI to upgrade OS.
The workaround is to reboot the DUT again.

- CSCun20365

USB SMI failed by the front USB port.
There is no workaround.

- CSCun20391

OS upgrade from remote https server failed.
There is no workaround.

- CSCue39436

Reboot or halt of the DUT may be failed unexpectedly.
The workaround is the power cycle of the DUT.

- CSCud99595

Power outage may cause the usb-disk to be read only, and then the upgrade will not go on.
There is no workaround.

- CSCup24260

Multiple Vulnerabilities in OpenSSL - June 2014.

Related Documentation

These documents provide complete information about the switch and are available from these Cisco.com sites:

http://www.cisco.com/go/cisco_edge_300

- *Cisco Edge 300 Series Switch Software Configuration Guide*
- *Cisco Edge 300 Series Switch Installation Guide*
- *Release Notes for the Cisco Edge 300 Series Switch*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation .

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed . The RSS feeds are a free service.