Release Notes for Cisco Edge 340 Series, Release 1.1 Patch 4

First Published: November 12, 2014
OL-31687-05

These release notes include important information about Cisco Edge 340 Series Software release 1.1 patch 4 and the limitations, restrictions, and caveats, if any, that apply to this release.

Contents

System Requirements

Hardware Supported

Table 1 Cisco Edge 340 Series Supported Hardware

Model No.	Description
CS-E340W	Cisco Edge 340 Series (Wireless)
CS-E340	Cisco Edge 340 Series (Non-wireless)

Software Images

Filename	Description
Cisco-Edge-1.1-i386-DVD.bin	Cisco Edge 340 Series OS

Upgrading to a New Software Release

The Cisco Edge 340 series supports the following installation and upgrade types:

- USB Mode Installation and Upgrade
- Remote Upgrade From the Web GUI
- BIOS Upgrade
- Patch Installation

USB Mode Installation and Upgrade

The Cisco Edge 340 Series software releases a self-extract installer. The file name is Cisco-Edge-*version*-i386-DVD.bin. It is an executive file that helps you to perform the installation automatically. When you execute the self-extract installer, the installation-related files are extracted to the hard drive of the Cisco Edge 340 Series, and a livecd is created in the internal USB. The system then boots from the internal USB (also known as the factory mode) and performs the installation automatically.

If the internal USB has already been created as a livecd, you can press the factory mode pinhole on the front panel of the Cisco Edge 340 Series to enter the factory mode and perform the installation procedure automatically.

Note Usually, the internal USB is created as a livecd in the factory. Executing the self-extract installer will overwrite the original livecd and create a new one.

Command Description

You can use the Cisco-Edge-*version*-i386-DVD.bin command with different parameters to implement installation or upgrade, print help, or create livecd only. In the command, *version* indicates the image version, which will be 1.1 for this release. For detailed instructions of installation and upgrade for this release, see *Cisco Edge 340 Series Software Configuration Guide, Release 1.1*.

For the installation and upgrade of the releases other than 1.1, refer to the software configuration guide of corresponding releases.

Note When you use this method to install or upgrade the system, make sure there is 1.5G free space at least.

1. To select the internal USB as a livecd disk and boot into factory mode to finish the installation automatically, use the following command:

   ```
   Cisco-Edge-1.1-i386-DVD.bin
   ```

2. To print help and then exit, use the following command:

```
Cisco-Edge-1.1-i386-DVD.bin --help|-h
```

3. To create livecd only, without entering factory mode nor executing the system installation program, use the following command:

   ```
   Cisco-Edge-1.1-i386-DVD.bin -t|--target <dev>
   ```

   <dev> is the full path of the target u-disk into which the livecd will be burned, for example, /dev/sdb1.

4. To wipe the home partition before the system is installed, use the following command:

   ```
   Cisco-Edge-1.1-i386-DVD.bin -w|--wipe
   ```

Note When the home partition is wiped, user data will be lost.

Remote Upgrade From the Web GUI

You can perform a remote upgrade for the Cisco Edge 340 Series using the web GUI if you have the address to download the self-extract installer. When you choose to perform the remove upgrade, the system will automatically download the self-extract-installer from the URL that you provide and execute the self-extract-installer to finish the installation.

BIOS Upgrade

BIOS upgrade can only be performed by manually installing the package and executing the commands in the Linux environment. BIOS is a critical part of the system, and there is no software recovery method if it crashes. To ensure successful BIOS upgrade, make sure that the external power supply is always connected, and do *not* perform any power cycle action during the upgrade process.

Patch Installation

Before installing a new software patch, you must already have the corresponding release image and all the patches released before this patch installed on your system.

Follow this procedure to install a new software patch:

Step 1 Log in to the Cisco Edge 340 Series system as root with terminal through SSH or Desktop.

Step 2 Copy or download the patch file to the Cisco Edge 340 Series release 1.1 filesystem.

Step 3 Use the following command to check if there is a patch management tool installed:

```
# which cpg_patch_ctl
```

To check the version of cpg_patch_ctl, use the following command:

```
# rpm -aq | grep cpg_patch_tool
```

In the output of the above command, 1.1.0-1 means release 1.1.0.1, while 1.1.0-2 means release 1.1.0.2.

Step 4 If the cpg_patch_ctl tool is not installed, use the following steps to manually install the patch:

a. Use the following command to uncompress the patch, for example, to the /tmp folder:

   ```
   # tar xvzf $folder/ce340-1.1-patch-0.4.tar.gz -C /tmp/
   ```

b. Go to the target folder where you uncompressed the patch and run the install.sh file to install the patch management tool:

```
# cd /tmp/ce340-1.1-patch-0.4
# ./install.sh
```

You can use the following parameters with the **install.sh** command for different functionalities:

- **-d** or **--debug**—Enable the debug information output.
- **-f** or **--force**— Force to install all system RPMs of the patch.
- **-V** or **--version**—Print the version of the patch.
- **-h** or **--help**—Print the usage information.

Note If an old patch is installed, the system will only upgrade new or changed RPM packages in the current patch.

Step 5 If the cpg_patch_ctl tool is already installed and the version is 1.1.0.2, use it to install the patch by using the following command:

```
# cpg_patch_ctl --install $folder/ce340-1.1-patch-0.4.tar.gz
```

If the cpg_patch_ctl tool version is 1.1.0.1, use the **install.sh** command in Step 4 to install the patch.

Note From cpg_patch_ctl version 1.1.0.2, the tool will check for the new version when installing the patch TAR package. If there is a new version available, the tool will be upgraded, and then you will be prompted to run the command again.

If the patch is installed successfully, the following message will be displayed:

```
'INFO: Patch installed successfully.'
```

Otherwise, an error message will be displayed:

```
'ERROR: <ERROR Message>'
```

If the patch is already installed, or the patch that you are going to install is older than the patch that is already installed on the system, the installation will be aborted and the following warning will be displayed:

```
'WARNING: Patch already installed. Abort.' or 'WARNING: Patch is elder than current
installed one. Abort.'
'WARNING: If you want to re-install, please add "--force" option to "cpg_patch_ctl" tool'
```

If you want to reinstall the patch, use the **install.sh --force** command to install the patch in force mode, or add the **--force** option when using the **cpg_patch_ctl** command.

Note To check persistency, you can run the preinstall script, *ce340-1.1-patch-0.x/system/pre-install.sh* before installing the patch, and run the post-install script *ce340-1.1-patch-0.x/system/post-install.sh* after installing the patch file RPMs.
End users are recommended to use the default version of both scripts. Partners can modify the scripts to meet your requirement.

Step 6 After the patch is installed successfully, run the following command to check the version:

```
# cpg_patch_ctl --get version
```

You can get more information by using the following command:

```
# cpg_patch_ctl --help
```

Step 7 Execute the **reboot** command manually if necessary.

Note The patch cannot be uninstalled or rolled back.

Note From release 1.1.0.3, a new nginx SSL certificate based on new OpenSSL is imported. If you have already changed nginx SSL certificate before "/usr/share/nginx/conf/*", you must reinstall them after you finished installing the patch. Or you need to delete the "systems//system/nginx-ssl-crt-1.4.4-1.fc16.edge340.i686.rpm" before installing the patch.

Recovering from a Software Failure

For recovery procedures, see the “Troubleshooting” chapter in the *Cisco Edge 340 Series Software Configuration Guide*.

New and Changed Information

This section contains new and changed information for this release.

New Software Features in Release 1.1 Patch 4

There is no new software feature in release 1.1 patch 4.

New Software Features in Release 1.1 Patch 3

Release 1.1 patch 3introduces the following new software features:

- OpenSSL upgrade—Supports OpenSSL 1.0.1i.
- Log rotation for Nginx—Supports to compact the obsolete logs automatically and delete them on the next day.

New Software Features in Release 1.1 Patch 2

Release 1.1 patch 2 introduces the following new software features:

- Patch Management Tool—Supports to install or upgrade a new RPM, and ignore the same version. Supports debug options to enable debug information output. When installing the patch TAR package, the tool will check and try to upgrade itself if there is a new version of the tool.
- VLC HLS—Supports to enable the VLC HLS plugin.

New Software Features in Release 1.1 Patch 1

Release 1.1 patch 1 introduces the following new software features:

- Multiple language support—Supports to change system language or input language to French, Spanish, and Portuguese. Supports to browse web pages in French, Spanish, and Portuguese.

New Software Features in Release 1.1

Release 1.1 introduces the following new software features:

- SIP video call plug-in (for Chrome and Firefox)[1]
  - Support HD video call with up to 720p resolution, compatible with CUCM (v9.1.0), interoperable with EX90, Cisco IP Phone 9971 and 9951.
  - Supports device registration and unregistration.
  - Supports to set up, end, pick up, and mute a call; supports echo cancellation, call waiting splash screen, and volume adjustment; supports Logitech C920 HD camera.
  - Screen sharing—Supports to accept shared screen from Cisco TelePresence C20 and TP EX90.
- Zero-touch Deployment—Supports DHCP Option 43. Support to download scripts from the URL provided in this field. Supports to connect the server with the provided IP address in this field.
- NTP server backup—Supports at least two NTP server IP addresses for backup. To configure backup servers, separate the server names with comma.
- HD video:
  - VLC JS API—Supports basic function and API to adjust stream latency. The default value of latency is 300 ms.
  - Streaming support—Supports H.264, MPEG2, MPEG4 part2, and WVC-1 codec for HTTP with video frame-rate up to 30fps (Apache server is recommended); supports MPEG2 codec for UDP and RTP with video frame-rate up to 30fps (VLC server is recommended).
  - Supports up to 20 Mbps data rate, GOP length 15.
  - Supports 1080p,1080i@30fps, and 720p@30fps.
- DMP support:
  - Boots into DMP mode—Supports auto-login, and re-auto-login; supports to change the username and password for the user account of auto-login; supports to skip desktop.
  - Supports to report the current status of the VLC by JS API, such as whether it is in playback or paused, and the time position of playback.
- New system monitoring dashboard—All system status can be monitored on a single web page with graphic statistics.
- Updated log settings on web GUI—Supports to set size and level of local log, and upgrade log to remote server by assigning server IP, port, level, etc.
- Resolution support:
  - Supports HDMI auto detection—Supports to detect all fields in HDMI EDID, and set it according to both normal section and extended section.

1. The SIP video call plug-in has a better performance in Chrome than Firefox.

  - Resolution override—Supports to disable the EDID detection, and set any resolution values from the default resolution value list to a monitor.

Note For a complete list of available resolution values, see *Cisco Edge 340 Series Software Configuration Guide*.

Note If the monitor does support enforced setting, the preferred resolution in EDID will be chosen.

  - Resolution enforcement setting—Supports to set up default resolution and enforce the settings to all connected monitors.

- Show IP—Supports to show wired and wireless IPv4 address on GDM and desktop.
- Supports IR remote controller of model number DMP-RM-K9=. Supports system default key mapping and API for customization.
- Touch screen—Supports both single touch screen and multi touch screen.

Caveats

This section displays open and resolved caveats for this release.

Open Caveats in Release 1.1 Patch 4

There is no open caveat in release 1.1 patch 4.

Resolved Caveats in Release 1.1 Patch 4

- CSCur05619

  Edge 340 Digital Media Player eval for the security issue of CVE-2014-6271 and CVE-2014-7169.
- CSCur30222

  TLS/SSL server supports SSL version 3 to solve the security issue of POODLE/CVE-2014-3566.
- CSCur43343

  VLC plugin in Chrome will crash when transiting from one video to another.
- CSCur26934

  Edge 340 Chrome browser crashes when opening web page with mp3.
- CSCup41424

  When there is no space left in the root partition on the Cisco Edge 340, it will not be able to log in or not be able to run some applications.

Open Caveats in Release 1.1 Patch 3

There is no open caveat in release 1.1 patch 3.

Resolved Caveats in Release 1.1 Patch 3

- CSCuq53899

  User space will be fully occupied by Nginx logs.
- CSCun99096

  Autologin may not work if registering a new CE340, which is not compatible with release 1.0.5.
- CSCun67800

  Kernel error being printed continuously after player or plugin is closed abnormally, which will cause the system hanging for a while.

Open Caveats in Release 1.1 Patch 2

There is no open caveat in release 1.1 patch 2.

Resolved Caveats in Release 1.1 Patch 2

- CSCup59010

  HLS stream pauses and delays.
- CSCup87707

  CE340 GUI will not accept IP with 255 in the third octet for a DNS server.
- CSCuo77756

  The mouse is not moving smoothly after being plugged out and plugged in again.

Open Caveats in Release 1.1 Patch 1

- CSCup68251

  VLC has no response and cannot be closed.

  The workaround is not to do fast forwarding when in pause.
- CSCup94518

  EAP method: FAST,inner auth: EAP-GTC does not work.

  The workaround is not to use GTC inner authentication with Anonymous automatic PAC provisioning in the FAST authentication mode.
- CSCup94410

  GE port has serious packet loss after 1 Gbps stream test for 12 hours.

  The workaround is not to adapt heavy data stream.
- CSCup94289

Error message: Could not switch the monitor configuration.

There is no workaround. Reboot to recover.

- CSCup92018

  HDMI display edge got cut off on some resolution on some monitors.

  The workaround is to adjust the scan mode of the monitor.

- CSCup91423

  Coordinates are not correct in portrait mode.

  The workaround is to change to landscape mode.

- CSCup89152

  The second to forth octet cannot accept 255 during IPv4 configuration.

  There is no workaround.

Resolved Caveats in Release 1.1 Patch 1

- CSCuo84574

  The login page is in Chinese after the language is set to Spanish.

- CSCuo34203

  Cannot get resolution list on Web GUI with Cisco 42’ LCD.

- CSCuo21086

  The coordinates are not correct on the test web page when the touch mode is set to multi-touch.

- CSCup48500

  There is black background flickering between video transitions in VLC plugin.

- CSCuo23755

  OpenSSL heartbeat issue. A missing bound check was found in the way OpenSSL handled TLS heartbeat extension packets.

- CSCup24248

  Multiple vulnerabilities in OpenSSL - June 2014.

  - CVE-2010-5298—SSL_MODE_RELEASE_BUFFERS session injection or denial of service.
  - CVE-2014-0076—Fix for the attack described in the paper "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack".
  - CVE-2014-0195—DTLS invalid fragment vulnerability.
  - CVE-2014-0198—SSL_MODE_RELEASE_BUFFERS NULL pointer dereference.
  - CVE-2014-0221—DTLS recursion flaw.
  - CVE-2014-0224—SSL/TLS MITM vulnerability.
  - CVE-2014-3470—Anonymous ECDH denial of service.

Open Caveats in Release 1.1

- CSCuj03737

Intel graphic driver-related issues.

- When the system wakes from S3 mode, the Timesys Fedora 14 system runs slower.
- The extend screen does not work properly.
- Nothing is displayed after switching the monitor from VGA to HDMI.
- The HDMI monitor displays instability.
- Screen displays a different layout after the HDMI monitor is turned off and then unplugged and plugged in again.
- Disconnecting VGA or HDMI in the extend display mode causes a display error.
- When the VGA resolution is adjusted, HDMI has no output.
- Display errors accrue in the extend display mode.
- When the system is booted up with VGA connected and then the HDMI is plugged in, there is no HDMI output.
- In the duplicated mode, setting HDMI rotation causes the VGA display to crash.
- In the extend mode, rotating HDMI display causes error.
- In the extend mode, the second screen overlaps with the main screen.
- Login panel layout is not displayed correctly after reboot with dual-portrait setting.
- When the resolution rotation is changed from duplicated to extend mode (dual-portrait), the display shows wrong layout.
- When the resolution rotation is changed from right to normal (dual-portrait), the display shows wrong layout.
- When the resolution rotation is changed from landscape-portrait to dual-landscape mode, the display shows wrong layout.
- When the resolution rotation is changed from extend to duplicated (landscape-portrait), the display shows wrong layout.
- When the resolution rotation is changed from dual-landscape to landscape-portrait, the display shows wrong layout.

There is no workaround.

- CSCuj49538

  HTTP stream playback is not smooth and easy to block in 2 channels mode.

  There is no workaround.

- CSCuj78740

  VLC plugin-related issues.

  - RTSP display has limited support for VLC plugin.
  - When the VLC plugin plays two channels of 1080p 24fps videos with one browser on a 1080P screen for 48 hours, the videos stop unexpectedly after 12 or 48 hours. And the system may crash if the bit rates of the two channels of videos are too high.
  - Only the videos with the same codec can play smoothly in the same time with one browser.
  - The web page with other contents in addition to VLC plugin got high xorg CPU usage.

  There is no workaround.

- CSCun23000

PPTP reconnecting automatically does not work in AP mode.

The workaround is to reboot the device or reconnect the VPN manually.

- CSCun47114

  VLC streaming play back related issues.

  - UDP unicast video cannot play smoothly in Wi-Fi mode.
  - UDP multicast video begin with 6s of green frames.
  - Long time delay and heavy mosaic on video stream.
  - Big mosaic on MPEG2 video stream.
  - VLC media player cannot play HTTP network stream (YouTube).
  - VLC crashed in long-term live stream test.

  There is no workaround.

- CSCun70198

  Network manager crashed occasionally after switching the Wi-Fi mode.

  The workaround is to reboot the device.

- CSCun80404

  Connection will be lost in high-density Extended Service Set (ESS) network.

  The workaround is to reconnect to the ESS network manually.

- CSCun96138

  DUT cannot reconnect to the ASUS AP RT-N56U after disconnected.

  The workaround is to reboot the DUT.

- CSCuo10636

  DNS server got from VPN still presents when connection is unestablished.

  The workaound is to reboot the device.

- CSCuo23986

  The rescue mode can only be displayed by VGA.

  There is no workaround.

- CSCuo26650

  Playing 1080P-H264-MP4 video in portrait mode joggled.

  There is no workaround.

- CSCuo29278

  Edge 340 screen frozen at MPEG2 video stream in Wi-Fi station mode.

  There is no workaround.

- CSCuo35575

  Extend mode related issues:

  - Dual display in the extend mode in not supported.
  - When playing 2 videos in 1080P extend mode, unexpected flicker appears.
  - When playing 2 videos in 1080P extend mode, the entire frame cannot be displayed.
  - Frame loss happened when playing 2 videos in extend mode.

– VGA screen has abnormal appearance in 2 channels extend mode.

There is no workaround.

Resolved Caveats in Release 1.1

- CSCuh50737

  Switching Wi-Fi modes has less than 1% probability to get core dump.

- CSCui11621

  Tray icon state of Wi-Fi client is connected even disassociated. The status change will be presented in no longer than 30s.

- CSCui12047

  RA-link driver related issues.

- CSCui16498

  IPv6 DHCP client cannot work when router advertisement is disabled on the connected router.

- CSCui21592

  Video conference lasting for more than 10 hours may cause system halted.

- CSCui52915

  Failed to boot up and stuck unexpectedly after SW reboot.

- CSCuj05758

  Wrong operation of USB hot plug makes system abnormal.

- CSCuj21736

  Configuration is not able to display after AP is enabled.

- CSCuj79962

  GDM window appears twice after booting up.

- CSCuj84575

  Stuck to boot up after changing the HDMI signal to VGA.

- CSCul21534

  AP configuration does not take effect after reload.

- CSCul21580

  The br0 interface cannot obtain IP address after the configuration is reloaded.

- CSCul49523

  EAP method option is missing on the Web GUI.

Related Documentation

These documents provide detailed information about the Cisco Edge 340 Series device and are available at:

http://www.cisco.com/go/cisco_edge_340

http://www.cisco.com/go/cisco_edge_340_s

- *Cisco Edge 340 Series Software Configuration Guide*
- *Cisco Edge 340 Series Installation Guide*

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* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.