Cisco TelePresence Serial Gateway Series 1.0(1.38)

Software Maintenance Release Notes
May 2014

Contents

Introduction

These release notes accompany maintenance software Version 1.0(1.38) for the Cisco TelePresence Serial Gateway Series. The software applies to the following devices:

- Cisco TelePresence Serial GW 3340 unit
- Cisco TelePresence Serial GW MSE 8330 blade

For clarity in this document, the term “serial gateway” is used in references that include both the Serial GW 3340 unit and the Serial GW MSE 8330 blade.

The serial gateway allows video calls to be made between IP-based networks and synchronous, serial-based networks. It supports V.35, RS-530, and RS-449 serial interfaces (with RS-366 dialing). The serial gateway also supports independent clocking on individual ports, and resynchronization via LOS.

CAUTION: Supervisor blade software version (Serial GW MSE 8330 only)
In the case of the Serial GW MSE 8330, it is a prerequisite for this software release that the Cisco TelePresence Supervisor MSE 8050 (Supervisor) blade is running software Version 2.1(1.18) or later.

Product documentation

The following documents provide guidance on product installation, configuration, and operation:

- *Cisco TelePresence Serial GW 3340 Getting Started*
- *Cisco TelePresence Serial GW MSE 8330 Getting Started*
- *Cisco TelePresence Serial Gateway Series Remote Management API Reference Guide*
- *Cisco TelePresence Serial Gateway Series 1.0 Online Help (printable format)*

All product documentation can be found on Cisco.com.

Resolved issues

The following issues were found in previous releases and are resolved in 1.0(1.38).

Resolved since Version 1.0(1.37)

Identifier	Description
CSCuo21535	**Symptom:** Cisco TelePresence Serial Gateway Series 8330 and 3340 include a version of openssl that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160. This bug has been opened to address the potential impact on this product. **Conditions:** Device with default configuration and running software release 1.0(1.37). Devices running software release 1.0(1.34) are not affected by this vulnerability. **Workaround:** Not currently available. Customers that do not require the new functionality nor the bug fixes on release 1.0(1.37) may evaluate downgrading affecting devices to software version 1.0(1.34). **Further Problem Description:** Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/5: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved since Version 1.0(1.34)

Identifier	Description
CSCua26057	In previous releases, long term use of the Microsoft Internet Explorer web browser could result in the serial gateway gradually running out of memory, which could cause an unexpected restart.

Resolved since Version 1.0(1.23)

Identifier	Description
CSCtx77443	Incorrect LED behavior was exhibited for Port 8 and Port 16.
CSCtx77438	The Default Codecs link in the dial plan was broken and directed users to a non-existent

Identifier	Description
	/settings_isdn.html page instead of to the correct */settings_serial.html* page.

Open issues

The following issues apply to this version of the serial gateway.

Identifier	Summary
CSCtr37711	If you configure a static IP route, when you reboot the gateway a spurious warning message about the default gateway is written to the event log: "*<unknown> Warning No default gateway on [port A][port B]*". In reality, in this situation the default gateway is set successfully during the boot process and you can ignore the message.

Updating the software

Software dependencies

In the case of the Serial GW MSE 8330, the Supervisor blade must be running software Version 2.1(1.18) or later before you install this release on the Serial GW MSE 8330 blade.

Prerequisites

CAUTION: You **must** back up your configuration **before** you upgrade the software.

You must remember the administrator user name and password for the backup file in case you ever need to use it.

CAUTION: If you use CDR data for any purpose (such as billing and auditing) you **must** also download and **save** the CDR data.

The software upgrade process requires a hardware restart. Make sure that the serial gateway is not in use, or warn any active users who may be affected by the loss of service.

Backup instructions

You can back up the serial gateway configuration via the web interface or via FTP.

To back up the configuration through the web interface, follow the instructions in the online help accessible from the interface. To back up the gateway through FTP, follow these steps:

1. Make sure that the FTP service is enabled on the **Network > Services** page.
2. Connect to the gateway using an FTP client.
3. Log in as an administrator. You will see a file called *configuration.xml*. This contains the complete configuration of your unit.
4. Copy this file and store it somewhere safe.

CAUTION: You must remember the administrator user name and password for the configuration backup file in case you ever need to use the backup.

Before you start

Have the following items available before you start:

- The new software image file.
- The current software image file (in case you need to reverse the upgrade).
- Your configuration backup XML file.
- The administrator user name and password for the backup file (you will need these if you have to use the backup).
- If applicable, make sure that the CDR data has been downloaded and saved.

Upgrade instructions

Note: The upgrade may take some time to complete (you can monitor progress through the serial port).

Process using the web interface

1. Unzip the image file to a local folder.
2. In a web browser, navigate to the web interface of the serial gateway.
3. Sign in as an administrator. On a new device the default user name is *admin* with no password.
4. Go to **Settings > Upgrade**.
5. In the **Main software image** area, specify the location of the software image file.
6. Click **Upload software image**.

   A progress bar displays while the web browser uploads the file to the serial gateway. This takes some time depending on your network connection. Do not navigate away from the upgrade page or refresh the page during the upload.

   When the upload completes, the browser refreshes automatically and displays an upload completed message.
7. Close the success message.
8. In the changed Upgrade page, click **Shutdown N-port Serial-IP gateway**.
9. When prompted, confirm the shutdown.
10. When the shutdown completes, click **Restart N-port Serial-IP gateway and upgrade**.

    The device reboots and upgrades as it restarts. This may take a while to complete.

Note: If you are logged out due to inactivity, sign in again as an administrator and click **Restart N-port Serial-IP gateway and upgrade**.

Process using FTP

1. Connect to the serial gateway via FTP.
   For example, from a command prompt type **`ftp <gateway IP address>`**.
2. Sign in as an administrator. On a new device, the default user name is *admin* with no password.
3. Upload the upgrade file.
   For example, from the FTP prompt type **`put <image filename>`**.
4. When the upload completes, reboot the device. You can reboot from the **Upgrade** page on the web interface.
5. The device upgrades as it restarts.

Downgrade instructions

If you need to reverse your upgrade, you can re-install the former version of the software. The downgrade procedure is the same as for the upgrade except that it uses the earlier software image.

CAUTION: If you use CDR data for any purpose you **must** download and **save** the CDR data before you downgrade to an earlier version. The gateway will delete all existing CDRs.

Process using the web interface

1. Go to **Settings > Upgrade**.
2. In the **Restore configuration** area, navigate to and select the appropriate *configuration.xml* backup file.
3. Check the *User settings* check box.
4. If required, check the *Network settings* check box.
5. Click **Restore backup file**.
6. When the configuration is restored, you need to re-install the required former software version.

Accessing Bug Toolkit

Bug Toolkit contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds.

1. Using a web browser, go to http://tools.cisco.com/Support/BugToolKit/.
2. Sign in with a Cisco.com username and password.

The identifiers listed in these release notes will take you directly to a description of each issue.

Getting help

If you experience any problems when configuring or using Cisco TelePresence Serial Gateway Series products, see the Product documentation section of these release notes. If you cannot find the answer you need in the documentation, check the web site at http://www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

Document revision history

Date	Revision	Description
May 2014	06	Third maintenance release
Jul 2012	05	Maintenance release for Serial GW 3340 and Serial GW MSE 8330
Apr 2012	04	First release for Serial GW 3340 and maintenance release for Serial GW MSE 8330
Aug 2011	03	First release for Serial GW MSE 8330
Jun 2011	02	EFT for Serial GW MSE 8330

Date	Revision	Description
Apr 2011	01	Limited circulation issue

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 SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND 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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.