



Cisco TelePresence Advanced Media Gateway 3610 Version 1.1(1.34)

Software release notes

D14839.04

November 2011

Contents

Document revision history	3
Introduction	4
New features and functionality.....	5
Support for Microsoft Lync Server 2010	5
Support for Microsoft Communicator for Mac 2011	5
Support for media encryption	5
Widescreen video cropping control	5
Changes to proxy definitions	5
HD video restriction control (Communicator for Mac clients)	5
Open caveats.....	6
Updating the software.....	7
Prerequisites.....	7
Backup instructions	7
Upgrade instructions.....	8
Before you begin	8
Procedure using the web interface.....	9
Procedure using FTP	9
Downgrade instructions	10
Procedure	10
Checking for updates and getting help.....	11
References and related documents	11

Document revision history

Revision	Date	Description
D14839.01	August 2011	EFT release.
D14839.02	October 2011	Release candidate (1).
D14839.03	October 2011	Release candidate (2).
D14839.04	November 2011	Final release.

Introduction

These release notes accompany software version 1.1(1.34), which is a new feature release for the Cisco TelePresence Advanced Media Gateway 3610 (Cisco AM GW 3610). The release notes describe the features available in the new software and how to install the software.

New features and functionality

Support for Microsoft Lync Server 2010

Version 1.1 of the Cisco AM GW 3610 provides interoperability with the Microsoft Lync Server 2010 and Microsoft Lync 2010 client software (formerly Microsoft Office Communicator Server (OCS) and Microsoft Office Communicator (MOC)).

Support for Microsoft Communicator for Mac 2011

Version 1.1 also provides interoperability with the Microsoft Communicator for Mac 2011 client.

Support for media encryption

The Cisco AM GW 3610 already supports TLS (Transport Layer Security) encryption, including encryption of the signaling path between the Cisco AM GW 3610 and Microsoft Lync / MOC and Communicator for Mac clients.

Version 1.1 extends encryption support to SRTP (Secure Real-Time Transport Protocol). For configurations running Cisco TelePresence Video Communication Server (Cisco VCS) version X5.2 or later, SRTP support includes encryption of the media path between the Cisco AM GW 3610 and Microsoft Lync / MOC and Communicator for Mac clients.

Important! By default, encryption support is disabled on the Cisco AM GW 3610. To switch on encryption you must install the *Encryption* feature key and then enable TLS (go to the **Network > Services** page and select *Incoming Encrypted SIP (TLS)*). The online help describes how to install feature keys.

Widescreen video cropping control

In the previous release, incoming widescreen video for standard 4:3 output configurations was always cropped. In Version 1.1 the image will still be cropped by default, but you can optionally specify that the image should be letterboxed instead.

Changes to proxy definitions

Version 1.1 introduces the following changes to proxy definition settings in the web user interface:

- You no longer need to specify an outgoing transport protocol. The outgoing transport for a proxy is now automatically set to match that of the incoming call.
- You can now optionally specify a port number for the Cisco VCS, using standard *IP:port* address notation (for example, *x.x.x.x:y*). If a port is specified, the Cisco AM GW 3610 uses that port for signaling toward the Cisco VCS.

HD video restriction control (Communicator for Mac clients)

In some Mac-based scenarios HD video can consume too much CPU on the Mac, which may lead to poor quality audio to and from the Communicator for Mac client.

Version 1.1 provides a new system setting that you can optionally use to restrict Communicator for Mac clients to sending VGA video only (they can still receive HD). By reducing the CPU load on the Mac this option minimizes the chances of degraded audio quality to and from the client.

Open caveats

The following issues currently apply to this version of the Cisco AM GW 3610.

Identifier	Summary
CSCtu04824	Support for Call transfer and Multiway to join a Lync / MOC client as a conference participant is only available with VCS proxies that are running software version X7 or later and are configured to use the Microsoft OCS / Lync B2BUA (back-to-back user agent).
CSCtu04829	Call hold requests are not fully supported and a call hold request may result in the far-end user experiencing frozen video. Video will return to normal when the call is resumed.

Updating the software

Prerequisites



CAUTION: You **must** back up the Cisco AM GW 3610 configuration **before** you upgrade the software (see below for instructions).



CAUTION: If you use Call Detail Records (CDR) for billing, auditing or any other purpose, you **must** also download and **save** your current CDR data before you upgrade the software.

Backup instructions

To back up the Cisco AM GW 3610 configuration through the web interface, follow the instructions in the online help.

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. Use an FTP client to connect to the Cisco AM GW 3610.
 3. Log in as 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 backup configuration. You will need these if you ever need to use the backup file.

Upgrade instructions

You can use either of the following methods to perform the upgrade:

- [Using the web interface](#)
- [Using FTP](#)

Note: The upgrade may take up to 25 minutes to complete (you can monitor progress through the serial port).

Before you begin

Make sure that the Cisco AM GW 3610 is not in use. The software upgrade process requires a hardware restart and anyone using the Cisco AM GW 3610 during the upgrade may experience poor performance and loss of connectivity.

Have the following items available before you start the upgrade:

- ▶ 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.

Procedure using the web interface

1. Unzip the image file.
2. In a web browser, navigate to the IP address of the Cisco AM GW 3610.
3. Sign in as administrator.
4. Go to the **Maintenance > Upgrade** page.
5. In the Main software image section, 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 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 - if you do the upload will abort.

The browser refreshes automatically after the upload completes and displays an upload completed message.

7. Close the completion message.
8. Click **Shut down AM GW**.
9. When prompted, confirm the shutdown.
10. When the shutdown completes, click **Restart AM GW and upgrade**.

The device reboots and upgrades as it restarts. This may take some time to complete.

Note: If you are logged out due to inactivity, sign in again as administrator and on the **Shutdown** page click **Restart AM GW and upgrade** to complete the upgrade.

Procedure using FTP

1. From the command prompt, use an FTP client to connect to the Cisco AM GW 3610. For example:
ftp <AM_GW IP Address>
2. Sign in as administrator.
3. Upload the upgrade file. For example, from the FTP prompt type:
put cisco_amgw3600_1.1.(1.34)
4. When the upload completes, reboot the device from the **Shutdown** page in the application web interface.

The device reboots and upgrades as it restarts. This may take some time to complete.

Note: If you are logged out due to inactivity, sign in again as administrator and on the **Shutdown** page click **Restart AM GW and upgrade** to complete the upgrade.

Downgrade instructions

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



CAUTION: If you use CDR data for any purpose you **must** download and **save** the CDR data before you downgrade the software. The Cisco AM GW 3610 will delete all existing CDRs during the downgrade.

Procedure

1. Log in as administrator.
2. Go to **Maintenance > Upgrade**.
3. In the **Restore configuration** area, navigate to and select an appropriate *configuration.xml* backup file that is compatible with the release to which you want to downgrade.
4. Check the *User settings* check box.
5. If required, check the *Network settings* check box.
6. Click **Restore backup file**.
7. When the configuration restore is complete, follow the upgrade instructions in [Updating the software](#).

Checking for updates and getting help

If you experience any problems when configuring or using the product, consult the online help available from the user interface. The online help explains how the individual features and settings work.

If you cannot find the answer you need, 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.
- ▶ Find further relevant documentation, for example product user guides, printable versions of the online help, reference guides, and articles that cover many frequently asked questions.
- ▶ Get help from the Cisco Technical Support team. Make sure you have the following information ready before raising a case:
 - The serial number and product model number of the unit (if applicable).
 - The software build number which can be found on the product user interface (if applicable).
 - Your contact email address or telephone number.
 - A full description of the problem.

References and related documents

All documentation for the latest version of the Cisco AM GW 3610 can be found at http://www.cisco.com/en/US/products/ps11449/tsd_products_support_series_home.html.

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.

© 2011 Cisco Systems, Inc. All rights reserved.