Cisco TelePresence MCU Series 4.4(3.57)

Software Maintenance Release Notes
September 2013

Contents

Product documentation

Version 4.4(3.57) is a maintenance release of software version 4.4 supported by the following MCU hardware platforms:

- Cisco TelePresence MCU 4200 Series
- Cisco TelePresence MCU 4500 Series
- Cisco TelePresence MCU 5300 Series
- Cisco TelePresence MCU MSE Series

The products are generically referred to as 'the MCU' in this document.

This document lists and describes the new features introduced by the point release 4.4(3.42), and issues resolved by this maintenance release.

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

- Cisco TelePresence MCU 4200 Series Getting started
- Cisco TelePresence MCU 4500 Series Getting started
- Cisco TelePresence MCU 5300 Series Getting started

- Cisco TelePresence MCU MSE 8420 Getting started
- Cisco TelePresence MCU MSE 8510 Getting started

New features in 4.4

Version 4.4 introduces a number of new security measures such as better password management, mutual authentication, certificate-based login, and optional Online Certificate Status Protocol (OCSP) validation of client certificates for HTTPS connections.

Several new features have been added to extend the conference experience, including call persistence, video to use by default, audio suppression during DTMF, adaptive gain control (AGC) on join, and initial muting of outgoing audio and video.

This version also introduces Quality of Service (QOS) tagging for all the different types of traffic originating from the MCU. The user interface has improved user cautions and features configurable headers and footers on the user interface pages.

The user interface and API have been updated as required to support these new features.

Security features

64 character User IDs

The MCU can now accept and store usernames that are 64 Unicode characters long. This applies anywhere that the MCU can accept a username, that is, from the web interface, an API call, FTP or serial console login, or a client certificate (common name).

Tighter password security

The MCU never stores passwords in plain text. They are always hashed using the SHA-2 algorithm before they are stored, even if an unhashed password is provided in a config file.

Changing passwords is also more secure now, irrespective of whether or not advanced security mode is enabled. When a user password changes, all session cookies associated with that username will immediately expire. Any users that are logged in when their passwords change will be logged out and may only log in with the new password.

Mutual authentication

The MCU can now perform mutual TLS authentication, which enables better security on a range of MCU interfaces.

The MCU now has a second trust store to provide for the different authentication requirements of this version. The original trust store authenticates the MCU's incoming and outgoing SIP calls (as in previous MCU versions), while the new trust store authenticates client and server certificates during web access, API calls, feedback receiver messages, and OCSP requests.

Whether mutual authentication occurs for these connections depends on the settings on the **Network > SSL certificates** page. The configuration options and accompanying certificate requirements are explained in Appendix: Mutual authentication connections and certificate identity requirements [p.23].

OCSP checks of client certificates

The MCU can now use OCSP to check client certificate revocation status (for HTTPS connections) against a pre-configured OCSP server. If the OCSP server responds that the certificate is 'good', the MCU allows

the client to authenticate with the certificate. In all other cases, the MCU will reject the certificate and prevent authentication.

The MCU always uses its known OCSP server and does not check any OCSP servers specified by the client certificate. The feature is configurable to include a nonce. Static Certificate Revocation Lists are not supported.

Certificate-based login

Users can now authenticate and log in using a client certificate, where previously they would always need to enter a username and password. The ability to log in with a username and password is retained, so the MCU can be configured to operate with or without certificate-based authentication.

CAUTION: When setting certificate-based authentication options for the MCU it is possible inadvertently to block *all* login access (including administrators) to the web interface. If you decide to implement certificate-based authentication we strongly recommend that you first review the appended topic Appendix: Transitioning to certificate-based security [p.25].

The MCU now supports four login modes, listed here from lowest to highest security level:

1	**Not required**	Certificate-based client authentication is not required (default) and client certificates are ignored. Password-based authentication is required for all client access, whether by users over HTTPS or applications making API calls.
2	**Verify certificate**	Incoming HTTPS connections are only permitted if the client certificate is signed by an authority that the MCU trusts, but password-based login is *still required* to authenticate the client, for HTTPS, API, and other client connections.
3	**Certificate-based authentication allowed**	Incoming HTTPS connections are only permitted if the client certificate is signed by an authority that the MCU trusts and, if the certificate's common name matches a stored username, the client logs in as that user. However, if the certificate is trusted and the common name does not match, the client may log in with username and password.
4	**Certificate-based authentication required**	Incoming HTTPS connections are only permitted if the client certificate is signed by an authority that the MCU trusts. The common name of the certificate must also match a stored username and password-based client authentication is not allowed. HTTP and FTP logins are blocked. If **Require administrator login** is checked (on **Settings > Security**), then console access is restricted to functions that do not require a login. **Note:** The MCU requires every user account to have a password, even if **Certificate-based authentication required** is selected and thus clients may not use their passwords. Furthermore, if the MCU is in advanced account security mode, passwords must be replaced every 60 days. Users are not prompted to change their passwords when they log in using certificate-based authentication, so the passwords will expire and generate security warnings. For the purpose of any timed access restrictions that exist on user accounts (typically password change intervals and inactive account expiry rules) any log in using a certificate is treated as a standard password-based login and will reset the timer accordingly.

Effect of certificate-based authentication on the API

If certificate-based authentication is allowed (option 3 above), the standard authentication parameters (**`authenticationUser`** and **`authenticationPassword`**) are required in API messages only if the client certificate is insufficient for login purposes.

If certificate-based authentication is required (option 4 above), the standard authentication parameters are ignored altogether and a client certificate must be used for login purposes, meaning that only HTTPS access is possible.

Persistent calls

The MCU's redial behavior has been extended to have greater scope and flexibility. You can now apply call persistence on a per participant basis. This feature is configurable to distinguish between a connection ending normally or failing, and for how persistent the MCU is in trying to restore the connection.

The persistence feature applies to participants and not to conferences or templates. Persistence can be applied to preconfigured endpoints, API-configured participants, or participants manually added to an active conference.

A call can only be made persistent before the MCU makes the call. Persistence cannot be applied to the call while the participant is connected or connecting, and cannot be applied to incoming calls. However, a preconfigured endpoint's persistence can be changed while a call is active, and the changes will be effective from the next call onwards.

The four levels of persistence are:

- **Never redial** - The MCU tries only once to connect to this participant.
- **Redial until connected** - The MCU only retries to connect to this participant when failing on first establishing a connection, and only then if the connection is not deliberately rejected; the MCU never retries if the connection fails after it is established.
- **Redial on unexpected disconnection** - The MCU retries on connection as in the previous option, but also retries if the connection fails after it is established. It does not retry if the connection is deliberately ended by either party.
- **Redial on any disconnection** - The MCU retries on first connection and also on subsequent connection failure, as in the previous two options, but also retries if the connection is deliberately ended by the endpoint.

When you configure the MCU to persist a call, you can choose whether it will do so according to a limited or unlimited retry schedule. The limited schedule allows up to 10 reconnect attempts after which the MCU will stop trying. If you select the unlimited schedule, the MCU persists until the connection is made or until the participant's active state is destroyed (conference ends or participant is deleted).

If a persistent call using the limited retry schedule drops repeatedly, the MCU stops reconnecting after three successful reconnections. That is, the MCU will abandon a persistently failing call if it is configured to use the limited retry schedule.

Note: If an endpoint fails to use the correct signaling, and that participant is configured to be redialed on unexpected disconnection, then the MCU may interpret a deliberate rejection or disconnection as unexpected and redial the participant. Similarly, incorrect signaling may cause the MCU to not redial when the user may have expected call persistence. If you are experiencing this kind of issue, you can work around the incorrect behavior by changing that particular endpoint's redial setting.

Video to use by default

You can now configure a participant to display a different participant's video source by default.

The MCU shows the replacement video by default whenever the original participant's video would previously have been shown. For example, if the original participant becomes the active speaker, then by default the replacement video becomes the most prominent pane in the layout.

The original participant's video never shows in the conference while the replacement video is available, unless you explicitly choose to show the original participant's video in a specified pane in the layout.

This replacement is only effective when both participants are in the conference. If the video to use by default is not available, the MCU tries to use the original participant's video.

The configuration is applied only on the participant whose video will be replaced: no changes are required to the source participant's configuration. The source participant does not see the replacement video by default - that is, they won't see themself when their video is replacing another participant and they would otherwise have seen that participant. Multiple participants can use the same video to use by default setting.

Adaptive Gain Control (AGC) on join

You can now apply adaptive gain control (AGC) to templates, conferences or participants in advance so that the gain is automatically controlled when participants join conferences.

AGC means that the participant's audio levels are adjusted to a common reference level to ensure a consistent audio experience for all participants.

A participant's AGC setting always overrides a setting inherited from the conference settings, and automatic gain will be disabled for a connected participant when you manually change the gain.

Mute outgoing audio or stop outgoing video

The MCU can be configured to mute the audio or stop the video sent to a particular participant. The MCU now also signals all muting, with the exception of incoming audio. This exception is made by design, to ensure DTMF functionality which may otherwise have been impaired in some cases.

Suppress audio during DTMF

The MCU now has an option to suppress the audio coming from an endpoint when the MCU is sending the connection DTMF sequence to the endpoint, so that other participants do not hear the audio from the endpoint while it is connecting.

The audio suppression continues until the whole DTMF sequence is complete, even if the sequence contains leading or trailing commas - which create pauses of two seconds each.

This suppression is independent of other audio muting options and also persists during retries. This is necessary in combination with the persistence feature because, if the MCU needs to redial an endpoint in the middle of the conference, the other participants should not hear the audio from the endpoint while it is connecting.

The option can be applied to ad hoc participants and preconfigured endpoints.

Note: the maximum length of the DTMF sequence has been extended to 127 characters. In prior versions there was a 31 character limit.

Additional QoS (quality of service) functionality

The MCU can now tag all outgoing traffic with configurable QoS (quality of service) information. This applies to both Ethernet ports on the MCU, whether on IPv4 or IPv6 networks.

The MCU can tag these traffic types:

- **Video** - all main video and content video (RTP streams and RTCP information, ConferenceMe video over UDP, BFCP, and FECC) can be tagged with a single QoS value
- **Audio** - all audio (RTP streams and RTCP information, ConferenceMe audio over UDP) can be tagged with a single QoS value
- **Streaming** - all unicast and multicast RTP and RTSP streams can be tagged with a single QoS value
- **Signaling** - all H.225, H.245, Q.931 and SIP signaling (includes built-in gatekeeper and ConferenceMe signaling) can be tagged with a single QoS value
- **Operations, administration, and maintenance (OA&M)** - all HTTP, HTTPS, FTP, DNS, SNMP, ICMP, syslog, NTP, and OCSP traffic can be tagged with a single QoS value. ConferenceMe traffic that is tunneled through HTTP is tagged with the OA&M QoS value, as is any other category of traffic not listed here.

Interface changes

Configurable headers and footers

The MCU web interface now has configurable header and footer fields that, when set, will appear at the top and bottom of the web pages. Each field can accept up to 100 Unicode characters and will appear on all pages except the online help. In a cluster, the slaves and master can have different headers and footers.

Popup notices when downloading or uploading files

The MCU web interface now has additional user cautions for actions that may affect performance; for example, the user is cautioned when downloading audit logs to do so at times of low load.

Status pages no longer auto-refresh by default

Web status pages (such as **Status > General**) no longer auto-refresh by default. You can manually specify an auto-refresh interval on the **Settings > User interface** page.

Resolved issues

The following issues were found in previous releases and are resolved in 4.4(3.57).

Resolved since 4.4(3.54)

Identifier	Description
CSCuj28455	An error message such as the following may appear on a Cisco TelePresence MCU 5300 Series running 4.4(3.54) or older: `HEALTH_MONITOR Error sensor CC0 T0 core failed: reading 1127.000000 mV should be between 980 and 1120 mV`. In 4.4(3.54) and older, these messages may not be indicative of a genuine problem. An upgrade to the 4.4(3.57) Maintenance release is advised so that genuine voltage problems are not masked by spurious error messages.

Identifier	Description
CSCui47687	In previous releases an MCU would only ever send CIF to a Polycom RSS4000. This issue is now resolved.
CSCuj04596	In previous releases it was not possible to set a subnet mask of the form xxx.0.0.0 using the MCU's web interface. The error message **`Please fix errors and re-submit error: Invalid IP address`** was produced. This issue is now resolved.
CSCui72250	In previous releases if a localization package was uploaded to an MCU when the **Use localization package** setting was already checked, the localization package may not have taken immediate effect. This issue is now resolved.

Resolved since 4.4(3.49)

Identifier	Description
CSCug89505	In previous releases it was possible for an MCU to experience an unexpected restart if it received an API message including a **`displayNameOverrideValue`** that was longer than the maximum of 31 characters. This issue is now resolved.
CSCub28587	In some circumstances, an encrypted conference participant could be incorrectly reported as an unencrypted participant. This issue is now resolved.
CSCug56190	In previous releases, a customer MCU 4500 experienced an unexpected restart because it ran out of memory while trying to run many processes. This issue is further improved in this release.
CSCua00144	In previous releases a warning message was generated when the MCU received an unexpected SIP message. In this release, the message will now only appear at Trace level.
CSCuh78036	In previous 4.4 releases, under some circumstances it was possible for guests in an Automatic Lecture Mode type 2 conference to receive black video. This issue is now resolved.

Resolved since 4.4(3.42)

Identifier	Description
CSCue49344	In previous releases, some attribute fields could incorrectly appear before bandwidth information in the SDP of a SIP message. This issue is now resolved.
CSCuc09395	In the 4.3 release, a customer MCU 4500 experienced an unexpected restart because it ran out of memory while trying to run many processes. This issue is improved in this release.
CSCue03922	In previous releases, when the MCU received invalid RTCP messages, it would print error messages at a very high rate in the event/serial log which added extra load to the host processor. In this release, the error messages are rate limited so that the MCU host processor is not overwhelmed with printing hundreds of error messages.
CSCue08737	In previous releases, a customer MCU 4500 experienced an unexpected restart when encoding an H.263 bit-stream due to a misconfiguration of the encoder. This issue is now resolved.
CSCud48262	In previous releases, on the MCU 4220, 4520, and MSE 8420 models, the internal message queue could become saturated if a large number of participants simultaneously disconnected from the MCU. Repetition of these circumstances could lead to a reduction in the maximum number of participants that the MCU could support. This issue is now resolved.

Identifier	Description
CSCud53710	In previous releases, if the called party identification had been updated during the call, and the call subsequently failed, the MCU would use the updated information when attempting to reconnect the call instead of using the original information. This led to a reconnection failure. This issue is now resolved.
CSCue55707	In previous releases, the MCU chose to send H.263 over H.264 to new Polycom RealPresenceGroup series endpoints even though the endpoints advertise H.264 support. This issue is now resolved.
CSCue36290	In previous releases, the MCU on-line help pages (help_content_support.html and help_conference_add.html) had a misleading description for Hybrid content mode. This issue is now resolved.
CSCuf02861	In previous releases, the MCU host processor could become overloaded when holding conferences with a large number of participants with additional web and API usage. This could result in slow web and API responsiveness and in extreme conditions, the MCU could experience an unexpected restart. In this release, a number of performance related enhancements have been made to prevent the host processor from overloading.
CSCtx29996	In previous releases, when making SIP calls to Panasonic endpoints, the MCU sent incorrectly formed SIP UPDATE messages which resulted in the call being disconnected. This issue is now resolved.
CSCuc22159	In previous releases, a customer MCU 4500 experienced an unexpected restart due to a memory corruption resulting from a buffer overflow. This issue is now resolved.
CSCue00360	In previous releases, an MCU cascade with a Polycom RMX series could often result in the call being disconnected. This issue is now resolved for unencrypted calls. For encrypted calls, a workaround is necessary, where the audio codec G.722.1 Annex C should be disabled on the MCU. An RMX side fix is planned for the encrypted calls issue, tracked by Polycom as BRIDGE-4551, which will remove the need for this workaround.
CSCuf03032	In the previous 4.4 release, MCU in FullHD mode would incorrectly transcode an incoming 1080p content resolution to an outgoing resolution of 1600x1200, even when the endpoints in the conference had support for 1080p content. This issue is now resolved.
CSCuf20821	In the previous releases, an MCU could enter into an unresponsive state when an API application (e.g. TMS) tried to delete an ad-hoc conference while simultaneously creating an API-scheduled conference, while audit logging was enabled. This issue is now resolved.

Resolved since 4.3(2.32)

Identifier	Description
CSCud59266	In previous releases, in rare circumstances the MCU could experience an unexpected restart if invalid bitstream was sent to the DSP and the exit message would show an sse validate failure error. This is resolved in this release.
CSCtz69347	In previous releases, MCU 4200 Series models could experience an unexpected restart when the maximum MTU size was set to 400 bytes or lower. This is resolved in this release.
CSCua55120	In previous releases, the MCU could experience an unexpected restart when a participant's muted video was used as content source. This is resolved in this release.
CSCuc58773	In previous releases, when a space character was used for the displayNameOverrideValue string over the API, the MCU could not correctly overlay this character on the participant's video. This is resolved in this release.

Identifier	Description
CSCuc57928	In previous releases, the MCU 4200 Series models could experience an unexpected restart with an H.264 decoder marker check failure message when invalid bitstream was sent to the DSP. This is resolved in this release.
CSCuc46770	In previous releases, when content mode was set to passthrough, content transmission could fail from a C-series endpoint when an MXP endpoint was present in the same conference and the call bandwidth was less than 1Mbps. This is resolved in this release.
CSCub83253	In previous releases, when dialing a SIP participant by IP address, if the SIP registrar box was ticked, the MCU would incorrectly append its SIP domain name to the IP address. This is resolved in this release.
CSCub18876	In previous releases, MCU 4501 or 4505 models could take over a minute to establish H.245 connection to participants when there are several incomplete H.225 TCP connections open to powered-off endpoints. In this release, the behavior is improved for those models but it is still advised to ensure endpoints are turned on if they are preconfigured on the MCU as they will be automatically dialed out; alternatively use a gatekeeper.
CSCuc40088	In previous releases, the MCU could experience an unexpected restart due to a picture buffer overrun that could be triggered by a corrupt bit-stream. This is resolved in this release.
CSCtx81724	In previous releases, the RTCP PLI (picture loss indication) messages sent by the MCU were not part of a compound RTCP packet. This is resolved in this release.
CSCud59262	In previous releases, there was incorrect behavior of the conference's disconnect remaining guests feature and the participants' auto-disconnect feature. The MCU would ignore chairs that were configured to auto-disconnect when deciding if only guests remained in the conference. In this release, under the same circumstances, the MCU does not disconnect the remaining guests unless all the chairs have disconnected—irrespective of whether any chairs are configured to auto-disconnect.
CSCud48267	In previous releases, the MCU would attempt a registrar call for an endpoint that was configured to use a SIP registrar, even if SIP registrar usage was disabled for the whole MCU. This has been resolved in this release.
CSCtz42558	In previous releases, custom codec selections were not correctly applied to pre-configured SIP participants when they dialed in to the MCU. This is resolved in this release.
CSCuc40073	In previous releases, the MCU event log sometimes reported failure to send serial messages to the Supervisor even when the box is idle. This is resolved in this release.
CSCty83668	In previous releases, when a SIP participant was put on hold, it would appear either as a black pane or a frozen image to other participants. This is resolved in this release; when a participant is put on hold, that participant's video pane is not displayed.
CSCty77949	In previous releases, when attempts were made to overwrite a valid auto attendant banner image with an invalid image, the MCU might not subsequently have been able to delete the valid banner image when a user deleted the associated auto attendant. This led to a situation where all the auto attendant banner storage space was used, but the images could not be deleted – preventing further banner image uploads. This is resolved in this release.
CSCty98516	In previous releases, the display field in the FROM header of an MCU sip log did not correctly display Unicode characters. This is resolved in this release.
CSCua09538	In previous releases, the MCU 4500 series could experience a DSP watchdog trip restart due to exposure to corrupt H.264 bit stream. This is resolved in this release.

Identifier	Description
CSCub18878	In previous releases, there were a number of areas within the H.264 decoder code where invalid (non-H.264) data could potentially cause an error and as a consequence the DSP could crash or timeout. The H.264 decoder resiliency has been vastly improved in this release.
CSCub15957	In previous releases, the MCU would not refresh its registration to a SIP registrar if the contact header field of the 200 OK message from the registrar exceeded 256 characters. This issue has been resolved in this release.
CSCub15970	In some circumstances, the MCU stopped responding to HTTP(S) requests on both the web interface and API calls. This recent problem has been attributed to Firefox browser version 14.0.1 (the first release code of Firefox 14; release date: 17th July 2012) and is improved in this release. This version of Firefox is still not recommended; Firefox 15 or later should be used instead. See also the limitations section of these release notes.
CSCty91132	In previous releases, when multiple names were received in the SIP header field, the MCU often did not prioritize the 'display field' among other names. This is resolved in this release.

Open issues

The following issues apply to this version of the Cisco TelePresence MCU Series software.

Identifier	Description
CSCug62534	In a call between an MCU 4500 and a TX9000, if the TX9000 switches the camera used to supply video, then the video stream from the MCU showing that participant will become blurry for one or two seconds.
CSCuc58400	When the MCU shuts down due to high ambient temperature, the diagnostic log correctly reports this event as a thermal override shutdown. However, the MCU status page incorrectly logs this restart as a 'user requested shutdown'.
CSCue35267	In certain scenarios, the MCU participant disconnect CDR log may leave the disconnection cause field empty instead of reporting the event as 'unknown'. The possible conditions that may trigger this are: the participant has been disconnected through in-call menu; the participant has been disconnected by the participant.disconnect API call; the unit has shut down; port allocation has exceeded when the participant was already in the conference and then disconnected; ConferenceMe participant disconnected as ConferenceMe has been disabled mid-call etc.
CSCtr53874	Slot 10 of the Cisco TelePresence MSE 8000 chassis does not support clustering in this MCU software release. However, slot 10 in the same chassis as a cluster can be used for a standalone blade of any type.
CSCts46406	If the MCU Ethernet interfaces are configured to have the same IP address and then you attempt to disable a service on one of the interfaces the service is still allowed, even though the web interface shows it set to disabled.
CSCuc41494	RealPlayer multicast for IPv6 is not currently supported.
CSCuc41501	MCU 4500 Series and MCU 4200 Series models are unable to register with their internal gatekeepers using their global IPv6 addresses. The workaround for this issue is to use an IPv6 loopback address [::1] rather than the global IPv6 address.

Limitations

Downgrade without restore causes username inconsistency after upgrade

When you downgrade from MCU 4.4 to MCU 4.3 or earlier, change a username, then upgrade to 4.4 again, that username's original 4.4 value is retained and is not changed. The reason for this is that the 4.4 software introduced a new field in configuration.xml to hold a longer username than was previously possible, but the previous field was also retained (the previous field was retained to ensure you could log in to restore your configuration). After you downgrade, the new field remains in the configuration file until you overwrite it with your 4.3 (or earlier) configuration file. If you fail to restore your 4.3 (or earlier) configuration, the upgrade process does not subsequently recreate the configuration file (which already has the new field) and so the usernames can become inconsistent.

To work around this limitation, follow the recommended backup and restore procedures when downgrading or upgrading. When you downgrade, you must also restore your configuration to ensure that the configuration file matches the software version.

Google Chrome on Microsoft Windows 7 fails to provide client certificate

Certificate-based authentication and login will fail if the user attempts to access the MCU web interface using Google Chrome on Microsoft Windows 7. This issue only occurs when the client certificate is generated by the Microsoft Certification Authority. To work around the issue, use a different browser, operating system, or certification authority.

Transferring a persistent call can result in both endpoints joining the conference

When you transfer a persistent call from the active endpoint to another endpoint, the MCU redials the original endpoint, maintaining the persistence on that call, and also joins the target endpoint to the conference without call persistence. The transfer use case is not officially supported in this version.

Firefox 14

Firefox 14 is not supported for use with the MCU. We strongly recommend that you refrain from using Firefox 14 to access the MCU web interface. This version of the browser causes an issue that was not present in previous browser versions and which has been fixed in the following version (Firefox 15).

Dynamic IP address assignment

This limitation applies to MCU 4200 Series and MCU 4500 Series only. When you configure dynamic IP address assignment for IPv4 or IPv6 on one of the unit's Ethernet ports, the other IP interface on that port temporarily loses network connectivity.

Issues when removing the CompactFlash™ during operation

Removing the CompactFlash card while the MCU is in operation has been known to cause a restart.

Windows Media Player

Streaming a conference with Windows Media Player in multiple windows or tabs on the same browser will crash the browser. This is a known issue with Windows Media Player. If you need to stream more than one conference simultaneously, use a different player such as QuickTime or Real Player.

In addition, Windows Media Player 11 can display streams incorrectly when used as an embedded player with browsers other than Internet Explorer. This is a known incompatibility. In some cases, setting the video size of the main streaming video window (the Video size field in the Streaming page) to Large will correct the problem. To work around this issue, you can use QuickTime or RealPlayer instead of WMP, or use Internet Explorer instead of your normal browser.

The MCU does not support 64-bit versions of Windows Media Player. To work around this limitation, use a 32-bit version of Windows Media Player.

Streaming to QuickTime 7 causes problems with some browsers

Streaming to an embedded QuickTime player using the QuickTime 7.0 plus later option for the Player format on the MCU can cause certain browsers to crash or remain in the 'negotiating' state indefinitely. Affected browsers include: IE6; Firefox 1.5 (Mac and PC); Safari 2.0.3 and earlier, and Camino. IE7 and Safari 2.0.4 do not appear to be affected by this. Using the QuickTime 6.5 plus later option for the Player format on the MCU will allow streaming to QuickTime using any browser that supports a QuickTime plug-in.

Clustering limitations

Cisco TelePresence MCU Conference Director will only work with the master blade in a cluster.

If you are using Cisco Telepresence Management Server Version 12.6 or earlier to schedule conferences on clustered blades, only add the master blade to TMS. Do not add slave blades to TMS and remove from TMS any blade that you subsequently configure as a slave blade: you will need to reconfigure any scheduled conferences that were previously configured on slave blades as new conferences running on the master blade.

Uploading and downloading large files while heavily loaded

We recommend that you do not upload or download large files from the MCU while it is hosting active calls. Files such as CDRs, audit logs and code images should be transferred when there are few or no calls on the MCU.

Binary Floor Control Protocol on encrypted calls

The transmission of SIP content from the MCU using Binary Floor Control Protocol (BFCP) is not supported on encrypted calls. To allow content to be transmitted over SIP calls in a separate channel from main video, you should disable encryption on the MCU or on the target endpoint.

Raw IPv6 addresses in Firefox 4.0 and later

It is not possible to access an MCU HTTPS web interface in Mozilla Firefox Version 4.0 using a raw IPv6 address. It is possible with IPv4 addresses and in earlier versions of Firefox, or if a hostname is used instead of the raw IPv6 address. This issue is being tracked by Mozilla as bug 633001.

Automatic link-local IPv6 assignment on disabled interface

When you enable IPv6 on any of the device's Ethernet ports (**Network > Port A** or **Network > Port B**), the device automatically assigns a link-local IPv6 address to each Ethernet port, even if the port is disabled. An IP address that is assigned to a disabled Ethernet port may not be apparent on the web interface.

Link-local addresses

Link-local IPv6 addresses are generated using the MAC address of each physical interface, and are thus unique per physical interface. No restrictions are imposed on link-local IPv6 addresses and all services enabled on their corresponding global IPv6 addresses are available on the link-local address. They support basic configuration and administration services (such as the web interface) but may not support full functionality such as making and receiving calls. Full functionality is only guaranteed for the main global IPv6 address on each interface.

We recommend using a PC with a single network interface connected to the local subnet when trying to access the MCU web UI using its link-local IPv6 address. Otherwise, login may fail since web browsers do not support URL redirection for an address with a scope ID.

Interoperability

We endeavor to make the MCU interoperable with all relevant standards-based equipment. While it is not possible to test all scenarios, the testing that the data below is based on covers all the most common functions of the listed endpoints and infrastructure.

Version 4.4 of the MCU software was used for this interoperability testing.

Note: Unless otherwise stated, Cisco Unified Communications Manager (CUCM) version 9.0.1 and Cisco TelePresence Video Communication Server (VCS) version X7.2 were used in the interoperability tests.

About the interoperability section

The interoperability section describes the equipment and software revisions that were tested for interoperability with this release. The absence of a device or revision from this section does not imply a lack of interoperability.

Interoperability testing often requires interworking from one signaling/call control protocol to another. The following table lists phrases that are used to briefly describe the call paths that were tested for each interoperability scenario. The call paths in the table place the endpoint first and the MCU last as a general convention.

Call scenario	Call path description
SIP	Endpoint <--SIP--> MCU. A registrar is used but not shown here.
H.323	Endpoint <--H.323--> MCU. A gatekeeper is used but not shown here.
H.323 to SIP interworking	Endpoint <--H.323--> VCS <--SIP--> MCU.
SIP to H.323 interworking	Endpoint <--SIP--> VCS <--H.323--> MCU.
CUCM to VCS	Endpoint <--SIP--> CUCM <--SIP--> VCS <--H.323--> MCU.
CUCM to MCU	Endpoint <--SIP--> CUCM <--SIP--> MCU.

Endpoints

This section lists interoperability issues with endpoints, by manufacturer. Where an endpoint has limitations, such as a lack of support for encryption or content, the interoperability tests omitted the limitations and they are not listed here.

An infrastructure issue may manifest itself as an issue with a particular endpoint or series of endpoints; issues of this nature are listed separately under 'Infrastructure'.

Cisco endpoints

Equipment	Software revision	Comments
Cisco TelePresence System 3000	1.9.2(19)	Tested CUCM to VCS and CUCM to MCU. ■ Video to CTS 3000 is periodically corrupted (CSCtx91858). ■ This endpoint does not respond properly to commands to mute/unmute audio/video from MCU. Using this feature with this endpoint may lead to unexpected behavior (CSCud21801).

Cisco TelePresence System 1300 Series	1.9.2(19)	Tested CUCM to VCS and CUCM to MCU. ■ The CTS 1300-47 endpoint does not respond properly to commands to mute/unmute audio/video from MCU. Using this feature with this endpoint may lead to unexpected behavior (CSCud21801).
Cisco TelePresence System 500-37	1.9.2(19)	Tested CUCM to VCS and CUCM to MCU. ■ Calls on the CUCM to VCS path between this endpoint and the MCU 5300 Series show video corruption on the endpoint (CSCtz98039). ■ Video corruption is present on the PIN entry screen when this endpoint connects to an MCU in HD mode on the CUCM to VCS call path (CSCud21804). ■ Video on the endpoint appears with a distorted aspect ratio and a black border when the MCU is configured to allow only 4:3 outgoing aspect ratios. Work around this issue by not restricting the MCU to 4:3 only (CSCud34601). ■ This endpoint does not respond properly to commands to mute/unmute audio/video from MCU. Using this feature with this endpoint may lead to unexpected behavior (CSCud21801).
Cisco TelePresence System 500-32	1.9.2(19)	Tested CUCM to VCS and CUCM to MCU. ■ The endpoint does not respond properly to commands to mute/unmute audio/video from MCU. Using this feature with this endpoint may lead to unexpected behavior (CSCud21801). ■ Video appears with a black border when the MCU is configured to allow only 4:3 outgoing aspect ratios. Work around this issue by not restricting the MCU to 4:3 only (CSCud34601).
Cisco Unified Video Advantage	2.2(2)	Tested CUCM to VCS and CUCM to MCU. ■ The endpoint does not respond properly to commands to mute/unmute audio/video from MCU. Using this feature with this endpoint may lead to unexpected behavior (CSCud45901).
Cisco Jabber Video for TelePresence (Windows)	4.5(16582)	Tested SIP and SIP to H.323 interworking. ■ Video from some MCU models to this endpoint is displayed in the wrong aspect ratio when the MCU is in SD media port mode. This affects MCU MSE Series, MCU 4200 Series, and MCU 4500 Series (CSCud33382).
Cisco Jabber Video for TelePresence (Mac OSX)	4.5(16582)	Tested SIP and SIP to H.323 interworking. ■ Jabber Video will display the video from the MCU in the wrong aspect ratio when using the H.263 codec. Under normal circumstances H.264 or H.263+ is used in preference to H.263 (CSCtx91864). ■ Video from some MCU models to this endpoint is displayed in the wrong aspect ratio when the MCU is in SD media port mode. This affects MCU MSE Series, MCU 4200 Series, and MCU 4500 Series (CSCud33382).

Cisco UC Integration (TM) for Microsoft Lync	8.5 (229.20137)	Tested CUCM to VCS and CUCM to MCU. ■ Pressing hold resume on the endpoint may result in lower resolution video transmission from the MCU.
Cisco Unified Personal Communicator	8.6.3.20802-1.2.148	Tested CUCM to VCS and CUCM to MCU. ■ Pressing hold resume on the endpoint may result in lower resolution video transmission from the MCU.
Cisco Jabber for Windows	9.0.5 (11368)	Tested CUCM to VCS and CUCM to MCU.
Cisco Jabber for iPad	9.1 (20014)	Tested SIP and SIP to H.323 interworking.
Cisco Unified IP Phone 9971	9-3-1-33	Tested CUCM to VCS and CUCM to MCU. ■ Calls from Cisco Unified IP Phone 9971 to the MCU on the CUCM to MCU path result in no audio/video from the endpoint (CSCub97604). ■ Video to Unified IP Phone 9971 may appear cropped by the screen boundary. As a result, presentation (that goes in main video with this endpoint) may also appear cropped (CSCto96806).
Cisco TelePresence System 1700 MXP	F9.1.2	Tested H.323 and SIP. ■ FECC negotiation can take several seconds on SIP calls (CSCty04059).
Tandberg 150 MXP	L6.1.0	Tested H.323 and SIP.
Cisco TelePresence SX20 Quick Set	TC5.1.4	Tested H.323 and SIP.
Cisco TelePresence System EX90	TC5.1.4	Tested H.323, SIP, CUCM to VCS, and CUCM to MCU. ■ Video from EX90 endpoint to MCU may be displayed in wrong aspect ratio when using H.263+ (CSCud33351).
Cisco TelePresence Codec C90	TC5.1.4	Tested H.323, SIP, CUCM to VCS, and CUCM to MCU.
Cisco IP Video Phone E20	TE4.1.1	Tested H.323, SIP, CUCM to VCS, and CUCM to MCU. ■ The endpoint does not correctly signal a deliberate disconnection, so the MCU treats it as an unexpected disconnection and may redial if configured to redial on unexpected disconnections (CSCud34448).

Sony endpoints

Equipment	Software revision	Comments

PCS-G50	2.72	Tested H.323 and H.323 to SIP interworking. ■ At low bandwidths this endpoint may not handle audio properly. You can mitigate this by disabling AAC codec for this endpoint. ■ The endpoint does not correctly signal a deliberate disconnection, so the MCU treats it as an unexpected disconnection and may redial if configured to redial on unexpected disconnections.
PCS-XG80	2.36	Tested H.323 and SIP. ■ An H.323 call to an encryption-required conference may result in no video or delay in starting video. ■ The MCU 5300 Series cannot use AAC-LC with this endpoint. ■ When calling over SIP, this endpoint only supports the first audio and video codecs that it advertises. If the MCU chooses a different audio or video codec from the advertised set, the endpoint may not be able to decode the audio or video from the MCU. ■ On H.323 calls the endpoint does not correctly signal a deliberate disconnection, so the MCU treats it as an unexpected disconnection and may redial if configured to redial on unexpected disconnections.

Polycom endpoints

Equipment	Software revision	Comments
HDX 4500	3.0.3.1-19040	Tested H.323 and SIP. ■ The Polycom HDX 4500 is unable to decode video or content sent by the MCU in the aspect ratio 1600x1200. (CSCts46398 / Polycom reference: VIDEO-90136) ■ Using only Siren 14 audio codec with this endpoint is not supported. However, if the MCU does not apply this restriction, the parties will successfully interoperate using a different audio codec. ■ The endpoint is not capable of simultaneously sending H.263+ main video and H.264 content. All other codec combinations work. ■ H.261 video between MCU and this endpoint does not work over SIP. ■ The endpoint does not respond properly to commands to mute/unmute audio/video from MCU. Using this feature with this endpoint may lead to unexpected behavior.

VVX 1500	4.0.2.11307	Tested H.323 and SIP. ■ Due to inaccurate timestamps sent by this endpoint, lip synchronization cannot be guaranteed. ■ When calling over SIP, this endpoint only supports the first audio and video codecs that it advertises. If the MCU chooses a different audio or video codec from the advertised set, the endpoint may not be able to decode the audio or video from the MCU. ■ The endpoint does not respond properly to commands to mute/unmute audio/video from MCU. Using this feature with this endpoint may lead to unexpected behavior.

Other endpoints

Equipment	Software revision	Comments
Microsoft Lync through Cisco TelePresence Advanced Media Gateway	4.0.7577.4103	Tested H.323 and SIP. Tested with Cisco TelePresence Advanced Media Gateway version 1.1(1.34). ■ The endpoint does not respond properly to commands to mute/unmute audio/video from MCU. Using this feature with this endpoint may lead to unexpected behavior.
Radvision Scopia XT1000	2.5.406	Tested H.323 and SIP. ■ BFCP is only supported on inbound calls to the MCU. (CSCtz21165) ■ The endpoint does not respond properly to commands to mute/unmute audio/video from MCU. Using this feature with this endpoint may lead to unexpected behavior.
LifeSize Room 200	4.7.21	Tested H.323 and SIP. ■ Encrypted SIP calls are not supported between the MCU and this endpoint. ■ G.722.1 Annex C is not supported on SIP calls between the MCU and this endpoint.
LifeSize Team	LS_TM1_4.1.1(17)	Tested H.323 and SIP. ■ Encrypted SIP calls are not supported between the MCU and this endpoint. ■ G.722.1 Annex C is not supported on SIP calls between the MCU and this endpoint.

Infrastructure

Equipment	Software revision	Comments
Cisco TelePresence Video Communication Server	X7.2	■ An encrypted H.323 to SIP call on the CUCM to VCS path to a CTS endpoint may fail to show video on the CTS if the conference is set to encryption optional (CSCud43073).

Cisco Unified Communications Manager	9.0.1	■ Calls from Cisco Unified IP Phone 9971 via the CUCM to VCS path result in no audio/video from the endpoint. (CSCub97604). ■ 60fps capable endpoints may not be able to negotiate 60fps with the MCU when the call is made via the CUCM to VCS path. ■ CUCM may not correctly respond to mid-call renegotiation from the MXP on a call to the MCU via the CUCM to MCU path (CSCtx16122).
Cisco TelePresence Content Server	S5.3	Tested H.323 and SIP. ■ On some MCU models, audio may be distorted or fail to decode if G722.1 codec is negotiated with this endpoint (CSCty01044). This affects MCU MSE Series, MCU 4200 Series, and MCU 4500 Series. ■ H.323 audio only calls to a TCS will not be recorded (CSCud41359).
TANDBERG Gatekeeper	N5.2	Tested H.323.
GNU Gatekeeper (GnuGk)	2.3.1	Tested H.323.
Polycom MGC-50	9.0.3.1	Tested H.323. ■ H.264 video between the MGC and the MCU is not supported if the call bandwidth is 384 kbps or less. To avoid this, either use a higher bandwidth or disable H.264 when dialing the MGC using custom codec selection (CSCts46389).
Polycom PathNavigator	7.00.03	Tested H.323.

Updating to 4.4

Prerequisites

The software upgrade process requires a hardware restart. Schedule a downtime window and notify users of when the service will be unavailable. The duration of an upgrade can be up to 25 minutes.

Have the following available and complete the backup processes described before you proceed to upgrade the software:

- New software package.
- Current software image file (in case you need to reverse the upgrade).
- Back up of the configuration (the configuration.xml file).
- You will require the administrator user name and password for the configuration backup file if you ever need to use the backup. If you attempt to downgrade / restore the software and you cannot load an appropriate configuration file, you may be unable to log in to the device.
- If using Call Detail Records (CDRs), or any other logs, for billing, auditing or other purposes, you must download and save your logged data. When the device reboots as part of the upgrade, all existing CDRs will be deleted.
- Administrative access to all units to be upgraded.

- The model numbers and serial numbers of your devices in case you need to contact Cisco Technical Support.

CAUTION: Make sure that all the backup processes described in this section have been completed before you start the upgrade. Failure to do so could result in data loss.

CAUTION: If you are upgrading a cluster you must upgrade all blades in the cluster to the same software version.

Backup configuration instructions

Using a web browser

1. In a web browser, navigate to the web interface of the device.
2. Sign in as an administrator.
3. Go to **Settings > Upgrade.**
4. In the **Backup and restore** area, click **Save backup file**.
5. Copy the resulting *configuration.xml* file to a secure location.

Using FTP

Note: The Cisco TelePresence MCU 5300 Series does not support FTP.

1. Check that the device supports FTP and that the FTP service is enabled on the **Network > Services** page.
2. Connect to the device using an FTP client.
3. Log in as an administrator (use the administrator credentials that you would use to connect to the web interface).
4. Copy *configuration.xml* to a secure location.

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

Upgrade instructions

Using a web browser

1. Unzip the image file locally.
2. In a web browser, navigate to the web interface of the device.
3. Sign in as an administrator.
   The username is *admin* and there is no password on a new unit.
4. Go to **Settings > Upgrade**.
5. In the **Main software image** section, locate the **New image file** field. Browse to and select the unzipped new image file.
6. Click **Upload software image**.
   The web browser uploads the file to the device, which may take a few minutes.

Note: Do not browse away from the **Upgrade** page, or refresh the page, during the upload process – this will cause the upload to fail.

A pop-up window displays to show upload progress. When complete, close the message. The web browser refreshes automatically and displays the message *Main image upload completed*.

7. Click **Shut down MCU**. This option will now change to **Confirm MCU shutdown**. Click to confirm.
8. Click **Restart MCU and upgrade**.
   The unit will reboot and upgrade itself; this can take up to 25 minutes.

Note: You may be logged out due to inactivity. If this happens, log in again, go to **Settings > Shutdown** and click **Restart MCU and upgrade**.

9. Go to the **Status** page to verify that your device is using the new version.
10. If necessary, restore your configuration; refer to the online help for details.

Using FTP

Note: The Cisco TelePresence MCU 5300 Series does not support FTP.

1. Check that the device supports FTP and that the FTP service is enabled on the **Network > Services** page.
2. Unzip the image file locally.
3. Connect to the device using an FTP client.
4. Log in as an administrator (use the administrator credentials that you would use to connect to the web interface).
5. Upload the image file.
6. Reboot the hardware after the upload.
   You can reboot via the upgrade page on the web interface.
   The unit upgrades itself when it restarts.
7. Log in to the web interface and go to the **Status** page to verify that your device is using the new version..
8. If necessary, restore your configuration; refer to the online help for details.

Note: You can monitor the upgrade progress via the serial port.

Downgrade instructions

Note: This release contains a system management update for the Cisco TelePresence MCU Series. This update is included by default on all Cisco TelePresence MCU 5300 Series appliances manufactured after September 2013. Do not downgrade an appliance that is manufactured after September 2013 to a software version earlier than 4.4; this downgrade is not supported. Please consult Cisco Technical Assistance Center if you require further assistance.

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

CAUTION: Make sure that all relevant backup processes described in Prerequisites have been completed before you start the downgrade. Failure to do so could result in data loss.

Downgrade procedure

You need the correct version of the software and your corresponding saved configuration before you proceed.

1. Follow the upgrade procedure using the earlier software image.
2. Restart the hardware and check the status via the web interface.
   The status report indicates the software version.
3. Restore your configuration from the saved XML file; refer to the online help for details.

Using the Bug Search Tool

The Bug Search Tool contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

To look for information about a specific problem mentioned in this document:

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a cisco.com username and password.
3. Enter the bug identifier in the Search field and click **Search**.

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**.
2. From the list of bugs that appears, use the **Filter** drop-down list to filter on either *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology*.

Use **Advanced Search** on the Bug Search Tool home page to search on a specific software version.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

Getting help

If you experience any problems when configuring or using Cisco TelePresence MCU Series, 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.

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit http://www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

Appendix: Mutual authentication connections and certificate identity requirements

Local certificate

The MCU can only have one local certificate. In all cases where the MCU needs to present a certificate to another party, the MCU uses the certificate listed in the Local certificate section of the **Network > SSL certificates** page. The MCU ships with a default certificate which you should replace if you want to use the certificate for security purposes.

Your local certificate must be configured in such a way that it can be correctly identified by the remote party, whether the remote party is an HTTPS client of the MCU, an HTTPS server to which the MCU connects, or a SIP entity that either calls the MCU or is called by the MCU.

Connections that may involve certificate exchange

Connection type	Settings on **Network > SSL certificates** page
Incoming SIP call (to MCU)	**Verification settings**: *Outgoing and incoming calls*
Outgoing SIP call (from MCU)	**Verification settings**: *Outgoing calls only* or *Outgoing and incoming calls*
Web interface user (to MCU)	**Client certificate security**: *Verify certificate*, *Certificate-based authentication allowed*, or *Certificate-based authentication required*.
API user (to MCU)	**Client certificate security**: *Verify certificate*, *Certificate-based authentication allowed*, or *Certificate-based authentication required*.
OCSP server (from MCU)	**Server certificate security**: *Verify certificate*
Feedback receiver (from MCU)	**Server certificate security**: *Verify certificate*

SIP TLS connections and certificate identity requirements

For the following secure SIP connection types, you should ensure that the MCU's local certificate, and any certificates presented to the MCU, can be identified and verified according to the following guidelines.

Outgoing SIP calls (MCU acting as a client)

The MCU performs a SIP TLS handshake with the called party, and the parties must be able to verify each other's certificates.

The MCU verifies that the received certificate is trusted by checking against its SIP trust store. The certificate must be signed by an authority that is in the MCU's SIP trust store.

The MCU identifies the owner of the certificate in the following way:

- The MCU looks for either an IP address or a domain identifier for the remote party in the **`URI`** and **`DNS`** fields of the certificate's subject alternative name (**`subjectAltName`**) extension.
- If the **`subjectAltName`** is not present, the MCU looks for either an IP address or a domain identifier in the certificate's Common Name (**`CN`**) field.

Note: If you require TLS on non-proxied SIP calls from the MCU, the MCU's local certificate **must** identify the MCU by its IP address. This requirement arises because the remote endpoint will be establishing TLS connections directly to the MCU, which provides its IP address as its identity.

Incoming SIP calls (MCU acting as a server)

The MCU performs a SIP TLS handshake with the calling party, and the parties must be able to verify each other's certificates.

The MCU verifies that the received certificate is trusted by checking against its SIP trust store. The certificate must be signed by an authority that is in the MCU's SIP trust store.

HTTPS connections and certificate identity requirements

For the following secure HTTP connection types, you should ensure that the MCU's local certificate, and any certificates presented to the MCU, can be identified and verified according to the following guidelines.

Client connections (MCU acting as a server)

This applies when API users and web interface users connect to the MCU if those clients are required, by the MCU's configuration, to present certificates.

The MCU verifies that the received certificate is trusted by checking against its HTTPS trust store. The certificate must be signed by an authority that is in the MCU's HTTPS trust store.

If certificate-based login is allowed or required, the MCU also checks the received certificate's common name. If it matches with a stored username, then the client logs in as that user.

Server connections (MCU acting as a client)

This applies when the MCU connects to a feedback receiver or an OCSP server if those servers are required, by the MCU's configuration, to present certificates.

The MCU verifies that the received certificate is trusted by checking against its HTTPS trust store. The certificate must be signed by an authority that is in the MCU's HTTPS trust store.

The MCU identifies the owner of the certificate in the following way:

- The MCU checks the **`DNS`** field of the certificate's subject alternative name (**`subjectAltName`**) extension for a domain identifier.
- If the **`DNS`** field is absent (or if the whole **`subjectAltName`** extension is absent), then the MCU will look at the common name for a domain identifier (IP address is not allowed in common name).
- The MCU also checks the **`IP address`** field of the certificate's subject alternative name (**`subjectAltName`**) extension, if present.

Appendix: Transitioning to certificate-based security

Certificate-based security methods carry a risk of inadvertently blocking all login access to the MCU. (If problems occur with the client certificate or the trust store, you will need to fall back to HTTP. If you cannot fall back—because HTTP is disabled or because HTTP to HTTPS redirection is set—then all access methods will be blocked.) To avoid this we strongly recommend that you follow the corresponding procedure below when implementing certificate-based security options:

Enabling client certificates and certificate login (HTTPS connections)

To transition access handling for HTTPS connections from standard, password-based access to required client certificate validation and optionally to allow certificate-based login, do the following:

1. Ensure that an appropriate HTTPS trust store is installed on the MCU (**Network > SSL certificates**) and that the web browser(s) to be used to access the MCU are configured with a valid client certificate.
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and disable **Redirect HTTP requests to HTTPS** (uncheck the check box). This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**.
   a. Scroll to the **HTTPS trust store** section.
   b. Set **Client certificate security** to *Verify certificate* (to have client certificate validation but no certificate login) or *Certificate-based authentication allowed* (to have client certificate validation and to allow certificate-based login).
   c. Click **Apply changes**.
5. Now test that you are able to log in to the MCU over an HTTPS connection.
   a. First verify that you can log in using the standard password login mechanism.
   b. If you specified *Certificate-based authentication allowed* in the previous step, also verify that certificate-based login is working as expected. This step is recommended, although strictly not essential as *Certificate-based authentication allowed* mode still allows password login if certificate login fails.

Note: Provided that this procedure is successful, you can now disable HTTP (**Network > Services**) or enable redirection from HTTP to HTTPS (**Settings > Security**) if either are required by your configuration.

Enabling OCSP checking

CAUTION: The MCU will only perform OCSP checking if client certificate security mode is enabled. To do this go to **Network > SSL certificates** and set the **Client certificate security** option. When you first enable OCSP checking, set **Client certificate security** to one of the 'lesser' modes (*Verify certificate* or *Certificate-based authentication allowed*). If you want to set it to *Certificate-based authentication required*, only do so after you have completed the procedure for Requiring certificate-only login (all connections) [p.26] and you are certain that OCSP checking is working correctly.

To enable OCSP checking for the MCU, do the following:

1. Ensure that an appropriate HTTPS trust store has been installed on the MCU (**Network > SSL certificates**).
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and *disable* **Redirect HTTP requests to HTTPS**. This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**.
   a. Scroll to the **Online certificate status protocol (OCSP)** section.
   b. Set **Certificate to check** to *HTTPS client certificates*.
   c. Enter the URL of the external OCSP server and set any options you require.
   d. Click **Apply changes**.
5. Now test that you are able to log in to the MCU over an HTTPS connection. Only proceed to the next step if you can successfully log in.
6. Do one of the following, as appropriate for your configuration:
   - Go to **Network > Services** and disable HTTP.
   - Go to **Settings > Security** and enable **Redirect HTTP requests to HTTPS**.

Requiring certificate-only login (all connections)

To transition from password-based authentication to required certificate-based authentication for *all* connection types, do the following:

1. Ensure that an appropriate HTTPS trust store is installed on the MCU (**Network > SSL certificates**) and that the web browser(s) to be used to access the MCU are configured with a valid client certificate.
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and *disable* **Redirect HTTP requests to HTTPS** (uncheck the check box). This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**:
   a. Scroll to the **HTTPS trust store** section.
   b. Set **Client certificate security** to *Certificate-based authentication allowed*.
   Do NOT set **Client certificate security** to *Certificate-based authentication required* yet.
   c. Click **Apply changes**.
5. Now test that you are able to log in to the MCU over an HTTPS connection *using a certificate*. Only proceed to the next step if you can successfully log in with a certificate.
6. Assuming the previous step succeeded, go to the **Client certificate security** option again and this time set it to *Certificate-based authentication required*.
7. Click **Apply changes** and confirm at the prompt.
   It is now not possible to log in over HTTP. To log in over HTTPS requires a valid client certificate signed by a certificate authority, which matches the HTTPS trust store on the MCU.
8. Do one of the following, as appropriate for your configuration:
   - Go to **Network > Services** and disable HTTP.
   - Go to **Settings > Security** and enable **Redirect HTTP requests to HTTPS**.

Document revision history

Date	Revision	Description
December 2012	16	Release version.

Date	Revision	Description
April 2013	17	Maintenance release version.
July 2013	18	Maintenance release version.
September 2013	19	Maintenance release version.

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.

© 2013 Cisco Systems, Inc. All rights reserved.