



# **MXP F9**

## **Software release notes**

**D14723.12**

**February 2016**

# Contents

<b>Contents</b>	<b>2</b>
<b>Document revision history</b>	<b>4</b>
<b>Introduction software version F9.3.4</b>	<b>5</b>
<b>Resolved issues and improvements since F9.3.3</b>	<b>6</b>
System	6
<b>Introduction software version F9.3.3</b>	<b>7</b>
<b>Resolved issues and improvements since F9.3.1</b>	<b>8</b>
System	8
<b>Introduction software version F9.3.1</b>	<b>9</b>
<b>Resolved issues and improvements since F9.3</b>	<b>10</b>
H323	10
System	10
<b>Introduction software version F9.3</b>	<b>11</b>
<b>Resolved issues and improvements since F9.1.2</b>	<b>12</b>
Video	12
Audio	12
SIP	13
H323	13
System	13
<b>Introduction software version F9.1.2</b>	<b>14</b>
<b>Resolved issues and improvements since F9.1.1</b>	<b>15</b>
Video	15
<b>Introduction software version F9.1.1</b>	<b>16</b>
<b>Resolved issues and improvements since F9.1</b>	<b>17</b>
Video	17
<b>Introduction software version F9.1</b>	<b>18</b>
<b>New features in F9.1</b>	<b>19</b>
New feature descriptions	19
OSD Call Flash	19
Serial Port Password Protection	19
Extended Support for alternate gatekeepers	19
<b>Resolved issues and improvements since F9.0.2</b>	<b>20</b>
H323	20

ISDN .....	20
SIP .....	20
System .....	21
User Interface .....	21
Video .....	21
Web interface .....	22
<b>Introduction software version F9.0.2 .....</b>	<b>23</b>
<b>Resolved issues and improvements since F9.0.1 .....</b>	<b>24</b>
Video .....	24
<b>Introduction software version F9.0.1 .....</b>	<b>25</b>
Changes and improvements since F9.0 .....	25
<b>Introduction .....</b>	<b>26</b>
<b>New features in F9.0 .....</b>	<b>27</b>
New feature descriptions .....	27
FECC over SIP .....	27
Web camera control .....	27
New languages .....	27
<b>Resolved issues and improvements since F8.2 .....</b>	<b>28</b>
User interface .....	28
Video .....	28
SIP .....	28
H323 .....	28
Network .....	29
Web interface .....	29
System .....	29
<b>Known Limitations .....</b>	<b>30</b>
Cisco .....	30
Polycom .....	31
Lifesize .....	31
Microsoft OCS .....	32
<b>Interoperability .....</b>	<b>33</b>
H.323 Gatekeepers/Traversal Servers .....	33
SIP Registrars/Proxies .....	33
SIP Client Applications .....	33
SIP PBX .....	33
Gateways .....	34
MCUs .....	34
Streaming servers .....	34
Endpoints .....	35
<b>Supplemental notes .....</b>	<b>36</b>
Software filenames .....	36
References .....	36
<b>Disclaimers and notices .....</b>	<b>37</b>

## Document revision history

Revision	Date	Description
12	26/02/2016	Release of F9.3.4 software
11	25/08/2014	Release of F9.3.3 software
10	14/06/2013	Minor update (Known Limitations)
9	21/01/2013	Release of F9.3.1 software, minor version.
8	23/11/2012	Release of F9.3 software.
7	23/01/2012	Release of F9.1.2 software, minor version.
6	03/10/2011	Release of F9.1.1 software, minor version.
5	09/06/2011	Release of F9.1 software.
4	12/01/2011	Release of F9.0.2 software, minor version.
3	22/09/2010	Release of F9.0.1 software, minor version.
2	16/09/2010	Release notes document change only. Added two resolved issues since F8.2
1	25/08/2010	Initial release of F9.0 software

## Introduction software version F9.3.4

These release notes describe the new features and capabilities included in the MXP Endpoint software version F9.3.4 released on the 26<sup>th</sup> February 2016.

There are no new features in this release.

This document applies to all MXP endpoints that run F series software. The 150 MXP runs L series software. Statements and functionality in this document do not apply to the 150 MXP system.

## Resolved issues and improvements since F9.3.3

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to <http://www.cisco.com/cisco/psn/bssprt/bss>

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

The following issues were found in previous releases and are resolved in F9.3.4:

### System

Reference ID	Summary
CSCux88407	CVE-2015-2808 – Removed weak ciphers
CSCuw35427	SSL Server Diffie-Hellman passive listening attack Vulnerability
CSCuy48902	Weak ephemeral Diffie-Hellman public key warning in web browser
CSCuv85580	Fix for CVE-2015-3566 (Poodle) vulnerability

Please see Known Limitations on page 30 for all open issues with F9.3.4.

## Introduction software version F9.3.3

These release notes describe the new features and capabilities included in the MXP Endpoint software version F9.3.3 released on the 25<sup>th</sup> August 2014.

There are no new features in this release.

This document applies to all MXP endpoints that run F series software. The 150 MXP runs L series software. Statements and functionality in this document do not apply to the 150 MXP system.

**Note – Release F9.3.2 was an internal Cisco release only and never released officially externally.**

## Resolved issues and improvements since F9.3.1

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to <http://www.cisco.com/cisco/psn/bssprt/bss>

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

The following issues were found in previous releases and are resolved in F9.3.1:

### System

Reference ID	Summary
CSCup23989	Multiple Vulnerabilities in OpenSSL
CSCtw50411	Upgrade OpenSSL
CSCup67066	Multiple Vulnerabilities in Dropbear server

Please see Known Limitations on page 28 for all open issues with F9.3.3.

## Introduction software version F9.3.1

These release notes describe the new features and capabilities included in the MXP Endpoint software version F9.3.1 released on the 21st January 2013.

This document applies to all MXP endpoints that run F series software. The 150 MXP runs L series software. Statements and functionality in this document do not apply to the 150 MXP system.

## Resolved issues and improvements since F9.3

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to <http://www.cisco.com/cisco/psn/bssprt/bss>

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

The following issues were found in previous releases and are resolved in F9.3.1:

### H323

Reference ID	Summary
CSCua69939	MXP not working as expected when getting RRJ with alternate GK info

### System

Reference ID	Summary
CSCud43389	Not able to barge into welcome message on Audio bridge

## Introduction software version F9.3

These release notes describe the new features and capabilities included in the MXP Endpoint software version F9.3 released on the 23<sup>rd</sup> of November 2012.

This document applies to all MXP endpoints that run F series software. The 150 MXP runs L series software. Statements and functionality in this document do not apply to the 150 MXP system.

F9.2 was an internal release only.

## Resolved issues and improvements since F9.1.2

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to <http://www.cisco.com/cisco/psn/bssprt/bss>

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

The following issues were found in previous releases and are resolved in F9.3:

### Video

Reference ID	Summary
CSCtu23835	MPI (Minimum Picture Interval) for a custom-defined resolution invalid
CSCua44832	MXP can corrupt video data when NAL unit is large enough to cause IP fragmentation
CSCtx61200	System Reboot with Streaming enabled
CSCua92956	MXP 1700 can send heavily corrupted video – detect, change resolution and encoder restart on call complete

### Audio

Reference ID	Summary
CSCud35898	DNAM relay in wrong modus after upgrade
CSCud35892	Buzzing sound on MXP when muting the microphone on Jabber Video

## SIP

Reference ID	Summary
<i>CSCts02672</i>	Handle P-Asserted-Identity header field in incoming Sip Invite message

## H323

Reference ID	Summary
<i>CSCua69939</i>	MXP not working as expected when getting RRJ with alternate GK info

## System

Reference ID	Summary
<i>CSCtw70688</i>	RFC2833 not spec compliant (DTMF)
<i>CSCtx21724</i>	SNMP Authentication Bypass
<i>CSCtx21725</i>	Hard-coded Password Disables Protect Mode
<i>CSCts13420</i>	SNMP Community strings should be treated as credentials
<i>CSCtx21713</i>	MXP FTP Denial of Service Vulnerability
<i>CSCtx21719</i>	Improper Validation of SNMP Community String
<i>CSCts58181</i>	Add robots.txt to Prevent Web Crawlers
<i>CSCtt44621</i>	Add Image Signing to MXP Software Packages
<i>CSCty45728</i>	Randomize H.225 Request Sequence Numbers on Boot
<i>CSCty45761</i>	MXP Web Interface Vulnerable to Clickjacking
<i>CSCty45724</i>	Inconsistent Validation of H.225 Request Sequence Numbers

## Introduction software version F9.1.2

These release notes describe the new features and capabilities included in the TANDBERG MXP Endpoints software version F9.1.2 released on the 23<sup>th</sup> of January 2012.

This document applies to all MXP endpoints that run F series software. The TANDBERG 150 MXP runs L series software. Statements and functionality in this document does not apply to the TANDBERG 150 MXP system

## Resolved issues and improvements since F9.1.1

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

### Procedure

**Step 1** To access the Bug Search Tool, go to <http://www.cisco.com/cisco/psn/bssprt/bss>

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

The following issue was found in previous releases and is resolved in F9.1.2

### Video

Reference ID	Summary
<i>CSCtt41567</i>	Video intermittently freezes for calls with H.264 video resolutions between CIF and 768x448. After disconnecting call, all subsequent calls will freeze and codec must be rebooted to revert to normal.

## Introduction software version F9.1.1

These release notes describe the new features and capabilities included in the TANDBERG MXP Endpoints software version F9.1.1 released on the 3<sup>rd</sup> of October 2011.

This document applies to all MXP endpoints that run F series software. The TANDBERG 150 MXP runs L series software. Statements and functionality in this document does not apply to the TANDBERG 150 MXP system.

## Resolved issues and improvements since F9.1

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

### Procedure

**Step 1** To access the Bug Search Tool, go to <http://www.cisco.com/cisco/psn/bssprt/bss>

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

The following issues were found in previous releases and are resolved in F9.1.1

### Video

Reference ID	Summary
<i>CSCts79092</i>	Intermittently the far end site will get no video or half a screen on video on MXP platform with F9.1
<i>CSCtr90106</i>	Video freezes in back to back ISDN GW calls to MCU.

## Introduction software version F9.1

These release notes describe the new features and capabilities included in the TANDBERG MXP Endpoints software version F9.1 released on the 9<sup>th</sup> of June 2011.

This document applies to all MXP endpoints that run F series software. The TANDBERG 150 MXP runs L series software. Statements and functionality in this document does not apply to the TANDBERG 150 MXP system.

## New features in F9.1

The TANDBERG MXP F9.1 software contains the following new features:

- ▶ OSD Call Flash.
- ▶ Serial Port Password Protection.
- ▶ H.323: Extended support for alternate gatekeepers in reject message from gatekeeper.

### New feature descriptions

#### OSD Call Flash

It is now possible to configure the On Screen Display (OSD) to flash for incoming calls. This can be done using the following command:

xConfiguration OSD CallFlash Mode: <Off/On>

#### Serial Port Password Protection

It is now possible to password protect the serial port using the following command:

xConfiguration SerialPort [1..2] Control Password: <S: 0, 16>

#### Extended Support for alternate gatekeepers

Support for alternate gatekeepers in H.323 RAS RRJ message from gatekeeper if registration is rejected.

## Resolved issues and improvements since F9.0.2

The following issues were found in previous releases and are resolved in F9.1

### H323

Reference ID	Summary
<i>CSCtr25591</i>	Fixed an issue where DTMF tones does not work for 2nd call in MultiSite
<i>CSCtq80408</i>	Fixed an issue where H.323 registration fails after resetting all H.323 and name settings.
<i>CSCtq80404</i>	Fixed an issue with H.460.18 SCR messaging.
<i>CSCtq80779</i>	Fixed an issue with H.245 ECS message handling.

### ISDN

Reference ID	Summary
<i>CSCtq80764</i>	Fixed an issue with FECC in H.320 leg in a MPS GW call.
<i>CSCtq80774</i>	Fixed an issue with ISDN restricted call scheduling in TMS

### SIP

Reference ID	Summary
<i>CSCtq80783</i>	Port 4444 is now closed when SIP ICE is set to on.
<i>CSCtq80771</i>	Added SIP QoS tagging.
<i>CSCtq83185</i>	Fixed an issue where call would disconnect after a double hold and resume.
<i>CSCtq83224</i>	Fixed an issue with no video from OCS R2 MOC.
<i>CSCtq83232</i>	Fixed an issue where the call drops when DNS query at time of registration renewal returns different IP address
<i>CSCtq83199</i>	Fixed some issues with FECC
<i>CSCtq83229</i>	Fixed an issue with BFCP when reconnecting a disconnected call.
<i>62537</i>	Added parsing of proprietary extensions to RFC5168 to respond to SIP INFO messages
<i>55212</i>	Fixed the content labels for main and dual media lines with Mirial SoftPhone PC client.

## System

Reference ID	Summary
<i>CSCtq83215</i>	Fixed a stability issue when OSD is disabled on DVI 1 upon boot.
<i>83686</i>	Fixed an issue where a call to a system configured with multisite is not resumed when transferred call is rejected
<i>CSCtq83207</i>	Fixed a stability issue after multisite is disconnected and new participant is dialed.
<i>CSCtq83221</i>	Fixed a stability issue with long SIP viaURI with alpha lower a's
<i>CSCtq83202</i>	Fixed a stability issue with incoming calls from IBM Lotus Sametime and other Daviko SIP based clients.
<i>CSCtq83189</i>	Fixed a stability issue when system in Kiosk mode

## User Interface

Reference ID	Summary
<i>CSCtq83211</i>	Fixed an issue where the Multisite banner would not time out. Fixed Multisite banner off mode.
<i>89606</i>	Fixed an issue where the search in phonebook is off by one and highlights wrong entry
<i>88068</i>	Fixed an issue where the dialing message shows old entry if contact was renamed in TMS.
<i>87402, 76754</i>	Fixed a Phonebook issue with missing contact entry when scrolling down past the bottom of the page.
<i>87400</i>	Fixed an issue where the corporate directory would display an empty entry at bottom of the list.
<i>81830, 81561</i>	Fixed several issues when searching and scrolling in phonebooks.
<i>80267, 77408</i>	Fixed an issue with the corporate directory when network connection is lost in Kiosk mode.

## Video

Reference ID	Summary
<i>87456</i>	Fixed a stability issue when going from 5+1 split to vs in multisite with duo video
<i>CSCts02687, CSCtr80192</i>	Fixed an issue where video could freeze when changing main video source
<i>85225</i>	Fixed an issue where MXP would send 448p instead of w448p to SD limited systems.
<i>83545</i>	Fixed an issue with no video after calling a MCU at 1472 kbps.
<i>77417</i>	Fixed an issue with no duo video when having another participant on hold.

## Web interface

Reference ID	Summary
83697	Fixed an issue with Microsoft IE8 and system login when system name consists of UTF-8 Unicode characters.
83631	Fixed an issue with web interface limiting the numbers of phonebook folders to 10.
79708	Fixed an issue with web camera control and auto camera detection when connected to a TVS.
72471	Fixed an issue where it was possible to see previous caller in Web snapshots when making a new call

## Introduction software version F9.0.2

These release notes describe the new features and capabilities included in the TANDBERG MXP Endpoints software version F9.0.2 released on the 12<sup>nd</sup> of January 2011.

This document applies to all MXP endpoints that run F series software. The TANDBERG 150 MXP runs L series software. Statements and functionality in this document does not apply to the TANDBERG 150 MXP system.

## Resolved issues and improvements since F9.0.1

The following issues were found in previous releases and are resolved in F9.0.2

### Video

Reference ID	Summary
82826	Fixed an issue with video freezing when presentation stops.

# Introduction software version F9.0.1

These release notes describe the new features and capabilities included in the TANDBERG MXP Endpoints software version F9.0.1 released on the 22<sup>nd</sup> of October 2010.

This document applies to all MXP endpoints that run F series software. The TANDBERG 150 MXP runs L series software. Statements and functionality in this document does not apply to the TANDBERG 150 MXP system.

## Changes and improvements since F9.0

Software version F9.0.1 is a production release only. No changes to functionality in this release.

# Introduction

These release notes describe the new features and capabilities included in the TANDBERG MXP Endpoints software version F9.0 released on the 25<sup>th</sup> of August 2010.

This document applies to all MXP endpoints that run F series software. The TANDBERG 150 MXP runs L series software. Statements and functionality in this document does not apply to the TANDBERG 150 MXP system.

## New features in F9.0

The TANDBERG MXP F9.0 software contains the following new features:

- ▶ Far end camera control (FECC) over SIP.
- ▶ Camera control in web interface.
- ▶ Welsh, Polish and Czech languages support.

### New feature descriptions

#### FECC over SIP

Far End Camera Control (FECC) is now supported over SIP by using Binary Floor Control Protocol (BFCP).

#### Web camera control

It is now possible to control the camera position and zoom from the web interface.

#### New languages

The following additional standard languages support has been added:

Welsh, Polish and Czech.

# Resolved issues and improvements since F8.2

The following issues were found in previous releases and are resolved in F9.0.

## User interface

Reference ID	Summary
69730	Picture layout entry in Japanese language menu corrected from PIP to POP

## Video

Reference ID	Summary
71931	Video freezing periodically from Classic, using H.264.
73297	Improved behavior when disconnecting 1st participant from MS call.
73329	Missing 1336x768@60 in VGA output table.
78896	Improved duo video behavior for incoming call when active call placed on hold.

## SIP

Reference ID	Summary
51077	Fixed behavior for blind transfer when transferring back and forth.
58204	Fixed issue when transferring call on a E20.
69555	Fixed duo video initiation for interworked call involving ICE.
72803	Standardized DNS SRV lookups.
73357	Fixed authentication-info parsing.
74779	Fixed SIP call rate limit to Polycom HDX
75193	Fixed issue with incoming video hold from Cisco CUCM
75680	Fixed issue with not sending Hello being FCS on receiving FCC.
75942	Added xAPI feedback information when IP connection lost.
77407	MXP via CUCM will only transmit 512kbps.

## H323

Reference ID	Summary
62854	Endpoint does not deregister aliases after multiple alias is turned off.
69298	Telephone call fails via Cisco GW over CCM.
72905	Missing one alternate gatekeeper entry in xStatus h323gatekeeper feedback.

## Network

Reference ID	Summary
73386	Improved alternate Gatekeepers functionality.
78248	Resolved NAT issues introduced in F8.x

## Web interface

Reference ID	Summary
70797	Fixed limit for TMS phonebooks displayed in webpage.

## System

Reference ID	Summary
70978, 71137	Stability issues when language set to Japanese or Simplified Chinese
74284	Stability issue when receiving too much data from camera.
77367	Fixed SNMP DoS attack issue
73548	Improved behavior under DoS attack

# Known Limitations

## Cisco

Reference ID	Equipment	Summary
CSCUh38093	MXP F9.3.4 / VCS / CUCM	MXP stops sending video after SIP session refresh re-invite in VCS-CUCM trunked call
CSCtx88327	MXP F9.3.4	FECC from Cisco Jabber Video to MXP results in MXP switching to VNC input causing Jabber to receive black video.  <b>Will be fixed in Cisco Jabber Video 4.6</b> - Upgrade JV to 4.6 and provision the JV client to use the new FECC method. JV will then be able to do FECC towards MXP without switching the main video input.
CSCty51581	MXP F9.3.4	Jabber Video calls MXP and BFCP fails
CSCud35814	MXP F9.3.4	No Presentation to Jabber Video when added to ongoing MultiSite with active presentation
CSCud34699	MXP F9.3.4	Duo not opened as expected in multisite scenario (sip only)
CSCud34703	MXP F9.3.4	System reboots when content server returns 486 busy
CSCts60532	MXP F9.3.4	Self view in audio call switches to remote view after 10-30 seconds
CSCtw49862	MXP F9.3.4	Remote view banner reappears periodically when in a telephone call
CSCts90640	MXP F9.3.4	When making an audio-only call from an MXP device if you set the device to self-view, it switches back to far end view after a few minutes.
CSCtu14067	MXP F9.3.4	EDGE95 VCR Audio ports are linked despite documentation saying otherwise
CSCts66671	MXP F9.3.4	Quick search only works for phonebooks with less than 8000 contacts
CSCtx86536	MXP F9.3.4	Unable to view corporate phone book that has an entry with name that includes apostrophe
CSCtt36832	MXP F9.3.4	MXP is not making calls at the correct call speed when the contact search is performed.
CSCts03240	MXP F9.3.4	MXP does not respect capset reduction from C40 in multisite call with sharpness
CSCua28053	MXP F9.3.4	Multisite site call with dual stream - Video layout Changes after rejecting call
CSCtx67907	MXP F9.3.4	MXP codec reboot when setting PC as main source when PC image contains continuous alphabets/numbers

<i>CSCud35869</i>	MXP F9.3.4	System might not support more than 25 web browser windows connected at the same time.
<i>CSCts13423</i>	MXP F9.3.4	The system has well known default password to the admin account (TANDBERG) and the SNMP community string is set to 'public'. We recommend these be changed to something other than their default values for security reasons. The device owner should configure these passwords when setting up the device for the first time. SNMP can also be completely disabled on the device.
<i>CSCud35907</i>	MXP F9.3.4	SIP dual stream (BFCP) over TCP is no longer possible. BFCP over UDP only.
<i>CSCud35882</i>	MXP F9.3.4	Multiway call not possible through Web Interface.
<i>CSCty45767</i>	MXP F9.3.4	Require Current Password at Password Change
<i>CSCts58144</i>	MXP F9.3.4	MXP XML API Crash With Sufficiently Long XML Tags
<i>CSCts58148</i>	MXP F9.3.4	MXP XML API Crash With Sufficiently Long XML Values
<i>CSCts58150</i>	MXP F9.3.4	CSRF Vulnerabilities in Web Interface
<i>CSCts58207</i>	MXP F9.3.4	XSS in Login Banner
<i>CSCtx21726</i>	MXP F9.3.4	Clear Text Storage of Sensitive Credentials
<i>CSCtq78796</i>	MXP F9.3.4	MXP 1700 Sends Invalid Terminal Type in Multisite Calls
<i>CSCtq78824</i>	MXP F9.3.4	Unauthenticated Diffie Hellman Key Exchange in Peer to Peer Calls
<i>CSCts58177</i>	MXP F9.3.4	DHCP Transaction ID Needs Randomization

## Polycom

Reference ID	Equipment	Summary
<i>CSCud34721</i>	Polycom DMA 2.0.0	When the MXP has SIP transport set for Auto call into Polycom DMA

## Lifesize

Reference ID	Equipment	Summary
<i>CSCud35877</i>	Lifesize RM 220 SW LS_RM2_4.7.0 (19)	Bad Video on MXP from LifeSizeRM

## Microsoft OCS

Reference ID	Equipment	Summary
CSCtw62553	OCS 2007R2	One-way Video when interworking between a Cisco TelePresence MXP series codec and OCS MOC.

# Interoperability

The systems below have been tested and verified with this software release.

## H.323 Gatekeepers/Traversal Servers

Equipment	Software revision	Comments
Cisco Video Communication Server (VCS)	X4.2, X5, X5.1, X6, X7.2.1	Both Assent and H.460.18/.19 traversal technologies supported.

## SIP Registrars/Proxies

Equipment	Software revision	Comments
Cisco Video Communication Server (VCS)	X7.2.1	
Microsoft OCS 2007 R2	3.5.6907.0	

## SIP Client Applications

Equipment	Software revision	Comments
Microsoft Office Communicator 2007 R2	3.5.6907.0	

## SIP PBX

Equipment	Software revision	Comments
Alcatel OXE	9.0	
Cisco UCM	7.0	

## Gateways

Equipment	Software revision	Comments
TANDBERG MPS Gateway	J4.5	
TANDBERG Gateway	G3.2	
Cisco ISDN Gateway	2.1	

## MCUs

Equipment	Software revision	Protocol	Comments
TANDBERG MPS	J4.5	H323 and SIP	
TANDBERG MCU	D3.10	H323 and SIP	
Cisco 4210	4.3	H323 and SIP	
Cisco 4520	4.3	H323 and SIP	
Polycom MGC50	9.0.3.1	H323 and H320	
Polycom RMX 2000	6.0.0.105	H323 and H320	Audio only when resolution forced to 720p on RMX

## Streaming servers

Equipment	Software revision	Protocol	Comments
Cisco Content Server	S4.0	H323 and SIP	

## Endpoints

Equipment	Software revision	Protocol	Comments
Cisco C-Series and EX90	TC5.1.6, TC6.0.0	H323 and SIP	
Cisco E20	TE4.1.1	SIP	
Cisco MXP	F8.2	H323 and SIP	
Cisco Jabber Video Telepresence	4.5	SIP	Far end camera control towards MXP will result in no video – see Known Issues. <b>Will be fixed in JV 4.6.</b>
TANDBERG Personal series	L6.1	H323 and SIP	
Lifesize Room 200	4.5.6	H323	
Polycom VS MP512	7.5.4	H323	
Polycom VS FX	6.0.5	H323 and H320	FX does not support H239
Polycom QDX6000	4.0.1-3040	H323	
Polycom HDX 8000 HD	2.5.0.5	H323	
Polycom HDX 8000	2.0.2	H323	
Polycom HDX 8006	2.6.0.4740	H323	HDX unable to receive 720p.
Polycom VSX 7000	9.0.6	H323 and H320	
Polycom PVX	8.0.16.0003	H323	
Sony TL50	2.42	H323	
Sony PCS-XG80	2.04.00	H323	

# Supplemental notes

## Software filenames

The correct software filenames are listed in the following table

TANDBERG MXP Systems	Software
All systems that support AES encryption	s50000f9_3_4.pkg
All systems that do not support AES encryption	s50001f9_3_4.pkg

## References

Cisco TelePresence Software	<a href="http://www.cisco.com/cisco/software/navigator.html">http://www.cisco.com/cisco/software/navigator.html</a>
Cisco TelePresence Docs	<a href="http://www.cisco.com/go/telepresence/docs">http://www.cisco.com/go/telepresence/docs</a>
Cisco Website	<a href="http://www.cisco.com">http://www.cisco.com</a>
TANDBERG FTP site	<a href="http://ftp.tandberg.com">http://ftp.tandberg.com</a>

## Disclaimers and notices

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](http://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.