



MAX Communication Server Release 8.5 Update 1

New Features Guide

May 16, 2018

Contents

About This Guide	3
Related Documentation.....	3
Requirements	3
Overview of MaxCS Enhancements.....	3
Enhancements in Release 8.5 Update 1	3
Enhancements in Release 8.5 QuickFix	5
Enhancements in Release 8.5.0.222	6
Enhancements in Release 8.5.0.215.....	7
Features No Longer Supported in Release 8.5 Update 1.....	7
Installation Procedures.....	7
MaxCS 8.5 Update 1 Enhancements.....	7
Multilingual Enhancements	8
Additional Fields for Extension Import/Export	10
System E-911 Caller ID.....	11
Monitoring Disk Capacity for Recording Files.....	12
Polycom VVX Firmware Auto-update Option	13
Polycom E911 Location ID from MAC Address	13
SightMax/ChatBeacon Support	14
MaxCS 8.5 QuickFix Enhancements.....	14
General Security Enhancements/TLS 1.2 Support	14
Public Certificate Support.....	15
Limit TLS to Version 1.2 Only.....	17
TLS 1.2 Support on Altigen Phones.....	17
Administrator Change Log	18
Polycom Enhancements	21
MaxCS 8.5.0.222 Enhancements	22
Plantronics Headset Support.....	22
Operational Limitations	24
Altigen Technical Support.....	24

About This Guide

This guide describes the enhancements that have been included in release MaxCS 8.5 Update 1.

Related Documentation

Additional information can be found in the following guides, which can be found on the *Support* tab of the Altigen web site: <https://www.altigen.com/support/>.

- *MaxCS 8.5 Update 1 Administration Manual*
- *MaxCS 8.5 Update 1 Upgrade Guide* (Follow the steps in that guide carefully to upgrade from MaxCS 8.0 or later.)
- *MaxCS VRManager Pro Manual*
- *MaxCS 8.5 Quality Management Guide*

Requirements

Refer to the MaxCS 8.5 Update 1 Administration Manual for the general requirements.

Note: Windows 2008 (which is the Operating System loaded on Office3G) **does not fully support TLS version 1.2**. Therefore, no version of Altigen MaxCS Server Software supports TLS 1.2 on Windows 2008 Server.

Overview of MaxCS Enhancements

Several updates have been prepared since the original release of MaxCS 8.5. Those builds are listed here, along with a summary of any new or updated features they included. Details for most features are included later in this guide or in other documentation where noted.

Enhancements in Release 8.5 Update 1

MaxCS 8.5. Update 1 Enhancements	
Quality Management application	<p>Assessment tools are typically used by Call Center operations to generate consistent independent evaluations of agent call-handling skills.</p> <p>In Altigen's <i>Quality Management</i> application, assessments are accomplished by listening to a recorded call while scoring the agent's performance on that call. Refer to the separate document, <i>MaxCS Quality Management Guide</i>.</p>
VRM Pro application	<p>A new application is introduced with this release; VRManager Pro. VRManager Pro offers many security features that were not available in VRManager:</p> <ul style="list-style-type: none"> • You can store voice recordings in encrypted format • You can now grant specific file record privileges to individual users (play, trim, and export)

MaxCS 8.5. Update 1 Enhancements	
	<ul style="list-style-type: none"> You can save VRM application data in an external database You can set password requirements ensure that users create more complex passwords You can implement policies such as password expiration periods, session timeout durations, and maximum number of login attempts allowed Users can trim voice recordings and export the trimmed recordings. The audio player display has been enhanced <p>Refer to the separate guide, <i>VRManager Pro Manual</i>.</p>
Multilingual enhancement	<p>MaxCS has a new option that expands your ability to assign or inherit language settings within AA branches. Each AA has two options in System > Multilingual Configuration on the AA tab:</p> <ul style="list-style-type: none"> Single Language - Specifies the language for that AA. All the prompts played to this trunk caller will be in this language. Multiple Languages - This option functions the same as the Multilingual option in previous releases. <p>See Multilingual Enhancements for details.</p>
Additional fields for importing and exporting extension data	<p>Several additional fields are available when import or export extension data. See Additional fields for Extension Import/Export for details.</p>
New options for automatic Polycom VVX firmware updates	<p>A new <i>Enable Polycom VVX firmware automatic upgrade</i> option in System > Polycom Configuration defaults to disabled (unchecked). This allows you to disable auto-upgrades to extensions during future MaxCS updates.</p> <p>In addition, MaxCS has a new algorithm for pushing firmware updates to Polycom phones. Staggering updates at 30-second intervals prevents the situation where all of your VVX phones try to update at the same time, which might cause problems.</p> <p>Refer to the <i>MaxCS Polycom Configuration Guide</i> and the <i>MaxCS Upgrade Guide</i> for full details.</p>
Polycom E911 Location ID updates	<p>You can now manage a Polycom phone's E911 Location ID (LID) just as you do Altigen IP Phone LIDs, in PBX > Location Based E911 Configuration. See Polycom E911 Location ID from MAX Address for details.</p>
Polycom phone support	<p>MaxCS now support Polycom models Trio 8500 and 8800.</p>
System E-911 CID	<ul style="list-style-type: none"> You can now configure a system E-911 Caller ID number for MaxCS, on the System Configuration > General tab. See E911 Number for MaxCS for details. When an emergency call is placed, the transmitted CID for the trunk call will be included in the call's Call Detail Record (CDR). In addition, the transmitted CID will be included in the SNMP

MaxCS 8.5. Update 1 Enhancements	
	trap that is automatically logged.
Disk capacity check for recordings	<p>This release monitors available disk space for four different drives, to ensure that there is sufficient space for voice recordings. In addition, there are new SNMP traps for low-capacity triggers.</p> <p>See Monitoring Disk Capacity for Recording Files for details.</p>
Voicemail message retention options	<p>You can now set a retention length for new, heard, and/or saved voicemail messages. This applies to extensions, workgroups, and huntgroups.</p> <p>Refer to the <i>MaxCS Administration Manual</i> for details.</p>
SightMax (ChatBeacon) updates	<p>The third-party application <i>SightMax</i> has been updated and renamed to <i>ChatBeacon</i>; MaxCS supports ChatBeacon version 2.0. For instructions, refer to the <i>MaxCS ChatBeacon Integration Guide</i>.</p>
RESTful CTI API Support	<p>MaxCS includes a Web Proxy, which includes a RESTful API. See the separate document, <i>Altigen Web API</i>.</p> <p>A RESTful API is an application program interface (API) that uses HTTP requests to GET, PUT, POST and DELETE data.</p> <p>This must be installed via a separate installation utility—it is not automatically installed via the main setup wizard.</p>

Enhancements in Release 8.5 QuickFix

MaxCS 8.5 QuickFix Enhancements	
Administrator Change Log	<p>The new <i>Change Log Report</i> (CLR) allows you to track configuration changes that have been made to MaxCS by administrators through the MaxAdministrator program. For details, see Administrator Change Log.</p>
General Security Enhancements	<p>For increased security, MaxCS now includes:</p> <ul style="list-style-type: none"> • Support for TLS version 1.2 • An option to use <i>only</i> version 1.2 when TLS is used; see Limit TLS to Version 1.2 Only • Support for public certificates; see Public Certificate Support for details • A new SNMP trap to alert you when your public certificate is close to expiring (if you let public certificates expire, your Polycom phones will no longer register)

MaxCS 8.5 QuickFix Enhancements	
Altigen Phone Security Enhancements	The Altigen IP705, IP710, IP720, and IP720a phones support TLS 1.2 via the new firmware version 2XB3. For details, see TLS 1.2 Support on Altigen Phones
Polycom Security Enhancements	<p>This release includes several Polycom security enhancements:</p> <ul style="list-style-type: none"> • VVX — 300/310/311, 400/410/411, 500/501, 600/601 phones support firmware version 5.6.0.17325 (VVX 1500 is not supported). This version is required in order to use a public certificate and to use TLS 1.2 • SoundStation — IP6000/IP7000 phones support firmware version 4.0.13.1445, which supports the use of public certificates, but does not support TLS 1.2 • SoundPoint — SoundPoint models do not support TLS 1.2 or public certificates <p>This release also includes a field for you to specify the location of the Polycom Directory server when you have a wildcard or SAN public certificate. See the section Polycom Enhancements for full details.</p>
MaxCS Client Security Enhancements	TLS 1.2 is now supported on IPTalk on MaxAgent, MaxCommunicator, and MaxOutlook.
AudioCodes Security Enhancements	<p>For enhanced security, MaxCS now supports firmware release F6.6.0A.336.004 on the AudioCodes MP1xx and Mediant devices.</p> <p>SIP UDP and SIP TLS 1.0 and 1.2 are supported.</p> <p>Both Altigen Enterprise certificates and public certificates are supported.</p> <p>For configuration steps, refer to the separate MaxCS AudioCodes configuration guides.</p>
Java Update	MaxCS now supports Java SE Runtime Environment JRE 8u171.

Enhancements in Release 8.5.0.222

MaxCS 8.5.0.222 Enhancements	
Exchange Server 2016 support	MaxCS now supports Exchange Server 2016 for Exchange Integration. Refer to the <i>MaxCS 8.5 Administration Manual</i> chapter for details.
Outlook 2016 support	MaxOutlook now supports Outlook 2016.
Windows Server 2016	MaxCS now supports Windows Server 2016.
Plantronics Headset Support	MaxAgent and MaxCommunicator now support several Plantronics headsets; for details, see Plantronics Headset Support .

Enhancements in Release 8.5.0.215

MaxCS 8.5.0.215 Enhancements	
Secured MaxAdministrator Connectivity	Communication between the MaxCS server and MaxAdministrator have been encrypted, for higher security.

Features No Longer Supported in Release 8.5 Update 1

The VRManager application is no longer supported starting with MaxCS 8.5 Update 1. Customers who used VRManager with previous releases can upgrade to VRM Pro (refer to the separate guide, *VRManager Pro Manual*).

Installation Procedures

This release supports:

- A new installation; follow the steps in the *MaxCS SoftSwitch Deployment Guide*.
- An upgrade from MaxCS Release 8.0 or later (refer to the *MaxCS 8.5 Update 1 Upgrade Guide* for detailed instructions, to ensure that you retain your existing configuration)

Note that TCP port 10078 is used for secured MaxAdministrator connection. Therefore, make sure that TCP port 10078 is opened on the server-side firewall for remote MaxAdministrator connection.

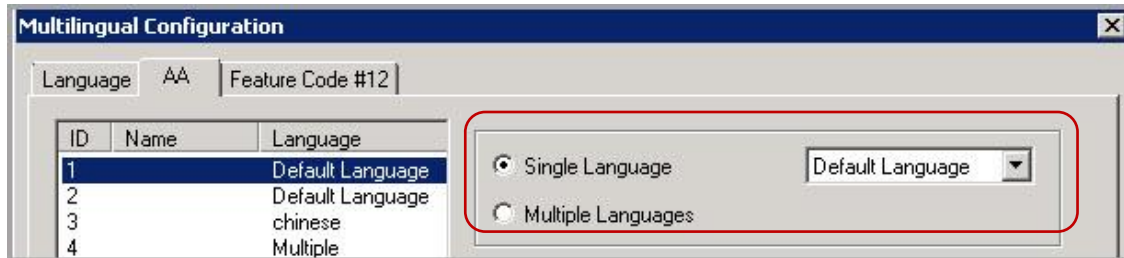
MaxCS 8.5 Update 1 Enhancements

Enhancements in Release 8.5 Update 1 include:

- A new *Quality Management* application; refer to the separate manual for details
- A new version of VRManager, VRM Pro, is offered with this release; see the separate manual for details
- [Multilingual Enhancements](#)
- [Additional Fields for Extension Import/Export](#)
- [System E-911 Caller ID](#)
- [Monitoring Disk Capacity for Recording Files](#)
- [Polycom VVX Firmware Auto-update Option](#)
- [Polycom E911 Location ID from MAC Address](#)
- [SightMax/ChatBeacon Support](#)

Multilingual Enhancements

Altigen has enhanced the multilingual feature for AA.



MaxCS has a new option that expands your ability to assign or inherit language settings within AA branches. Each AA has two options in **System > Multilingual Configuration** on the AA tab:

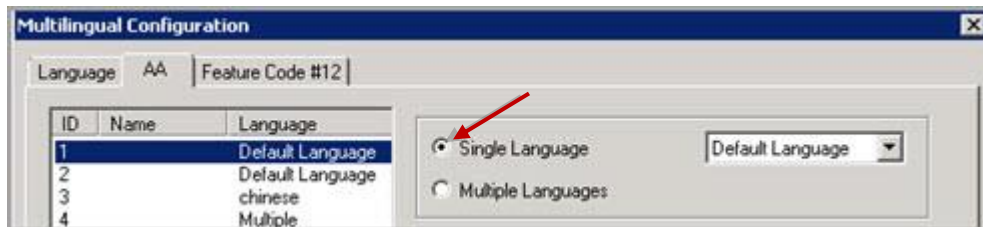
- **Single Language** - Specifies the language for that AA. All the prompts played to this trunk caller will be in this language.
- **Multiple Languages** - This option functions the same as the Multilingual option in previous releases.

Single Language AA Configuration

- If the AA routes the trunk caller to another a "Single Language" AA with a different language setting, then the new language setting will be used from that point on.
- If the AA routes the trunk caller to an AA set to "Multiple Languages," then no language selection prompt will be played; the original language setting remains.

To configure an AA for Single Language,

1. In the *Multilingual Configuration* panel AA tab, select the AA ID number in the list on the left.
2. On the right, select the **Single Language** option and then choose the language from the pull-down list.



All calls routed to this AA will now use the selected language in AA branches., including all system phrases and all custom phrases.

Note that calls routed to a workgroup to target an agent for a selected language must use the *Single Language* option.

Following are two common scenarios for configuring language options in AAs using the *Single Language* AA feature.

Multilingual Example 1: DNIS Routing

In this example, AA1 is configured as Single Language and set to Chinese. AA2 is configured for Single Language and set for Spanish.

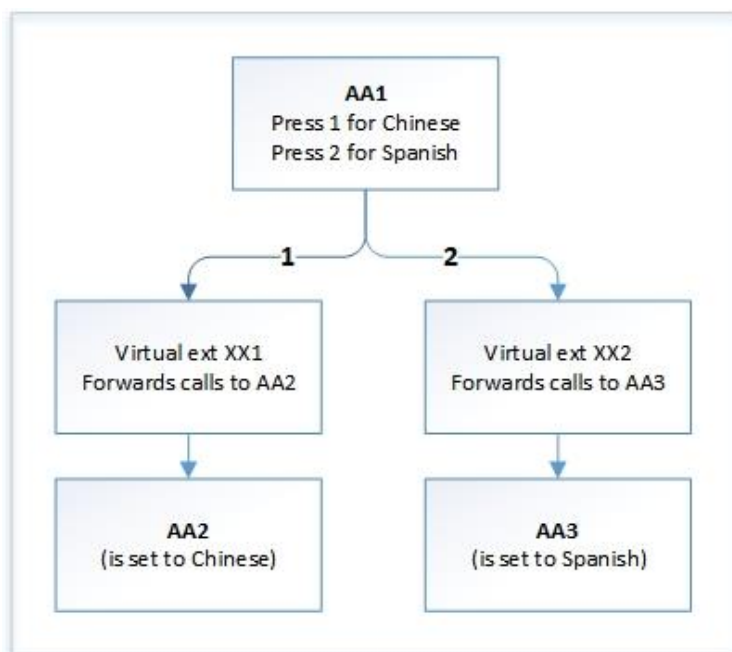
DNIS1 can route to AA1 so that those customers can hear the phrases in Chinese. DNIS2 can route to AA2, which has been configured to play the phrases in Spanish.

Multilingual Example 2: Virtual Extension Forwarding

In this example, configure AA1 to ask the caller which language they want to hear. The options could be "Press 1 to hear prompts in Chinese; press 2 to hear prompts in Spanish."

Configure the routing such that if the caller presses 1, the call is transferred to virtual extension xxx1; if the caller presses 2, then the call is transferred to virtual extension xxx2.

Set virtual extension xxx1 to forward calls to AA2, which has been configured as Single Language and set to Chinese. Set virtual extension xxx2 to forward calls to AA3, which is configured as Single Language and set to Spanish.

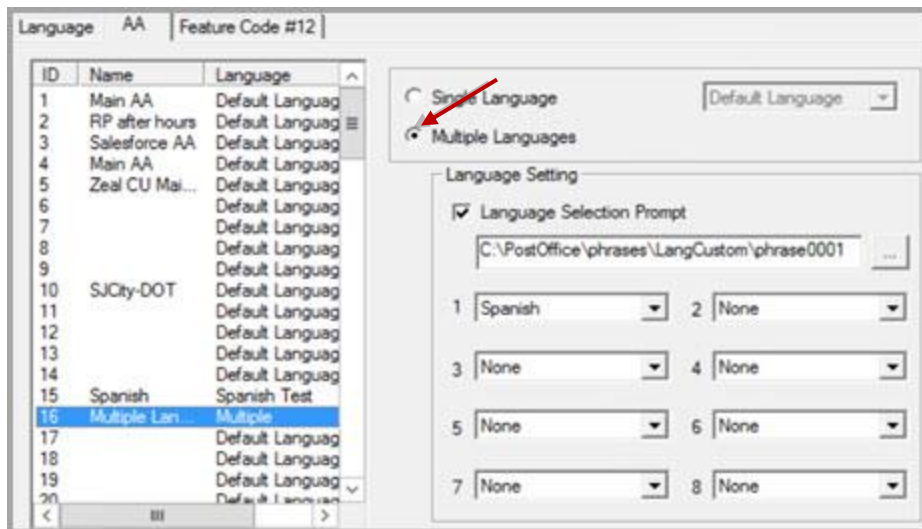


Multiple Language AA Configuration

To configure an AA for Multiple Languages,

1. In the *Multilingual Configuration* panel AA tab, select the AA ID number in the list on the left.
2. On the right, select the **Multiple Language** option.
3. Check the option **Language Selection Prompt** and choose the desired prompt phrase. We recommend that you use whatever prompt you have that defines the digits assigned each language.
4. For fields 1-8, assign a language to each digit based upon the prompt phrase you assigned.

In the example figure below, if the caller presses the digit 1, then the system will use that language (1 is assigned to Spanish) from that point forward, for all system phrases and custom phrases.



Note that you can use the In-Call Routing Table to manage inbound calls to a Multiple Language AA.

Operational Notes for Multilingual Configuration

There is one scenario to be aware of when configuring multilingual AAs. This scenario is when a user receives a direct DID call and then transfers the call to a workgroup or huntgroup.

Because the call originated as a direct DID call, it did not go through an AA that offered the caller a language preference. Therefore, if the user transfers the call to a workgroup/huntgroup with foreign language agents, the caller will hear prompts in the system default language.

To handle this scenario, the call must first be transferred to an AA that is configured as *Single Language* for that specific language first, and then routed on.

1. Configure a new AA. The first line of this AA should be to transfer the call to the desired workgroup/Huntgroup; for example, to workgroup 520.
2. Open the *AA tab of Multilingual Configuration*. Assign a language to the AA that you created in the previous step.
3. Create a virtual extension; for example, extension 521. Configure this virtual extension to forward all calls to the AA that you configured in step 1.
4. In *Dialed Digit Translator*, add an *Extension Dialed Digit Translator* entry for workgroup 520 and translate to 521.

Additional Fields for Extension Import/Export

Many additional fields are now available when importing or exporting extension data. The following table describes the fields and the location of their respective options within MaxAdministrator.

Field Name	Location in MaxCS Administrator	Option in GUI
Allow to transfer to an outsider	Extension Configuration > Restriction	Allow Calls to be Transferred or Conferenced to an Outside Number

Allow to configure an outsider	Extension Configuration > Restriction	Allow Extension User to Configure Forwarding, Notification and Reminder Call to an Outside Number
Allow an outsider to call in VM	Extension Configuration > Restriction	Allow Outside Caller to Make or Return Calls from within VM System
Allow an outsider to call international in VM	Extension Configuration > Restriction	Allow Outside Caller to Make or Forward International Calls from within VM System
Enable Polycom or 3rd Party	Extension Configuration > General	Enable Polycom or 3 rd Party SIP Device
Enable Forward	Extension Configuration > Forward All Calls	Enable Forward to
Forward Type	Extension Configuration > Forward All Calls	Target Type
Forward Prefix	Extension Configuration > Forward All Calls	Target Prefix
Forward Number	Extension Configuration > Forward All Calls	Target Number

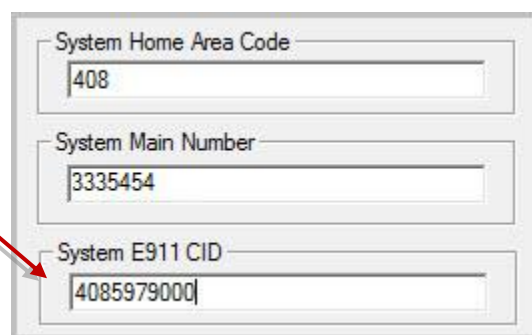
System E-911 Caller ID

With this release, you can configure a default E911 CID for MaxCS. Extensions that have no E911 CID configured will use this new System E911 CID.

You can overwrite this default to assign different E911 CIDs for individual extensions.

Note: Phones that are managed through the *Location-Based E911* table will use the configured Location ID instead of the System E911 CID.

This CID is set on the System **Configuration > General** tab. **Make sure that you include the area code in your entry.**



There are several different E911 options within MaxCS. The new logic regarding which E911 CID is used during a 911 call is as follows:

1. If a Location ID has been assigned to the extension (**PBX > Location Based E911 Configuration > View E911 Assignments**), then the E911 CID associated with the assigned LID will be sent during an E911 call from the extension.
2. If no Location Based E911 LID has been configured, then the extension's configured E911 CID will be sent.
3. If there is no extension E911 CID configured for the extension, then this new System E911 CID will be sent.

4. If no System E911 CID has been configured, then the extension's Transmitted CID will be sent.
5. If the extension does not have a Transmitted CID configured, then the extension's DID number will be sent (if it is 10 digits or longer)
6. If there is no DID number associated with the extension, then the trunk's Transmitted CID will be sent.
7. If the area code and phone number have not been configured for the trunk, then the System Main number will be sent.

Monitoring Disk Capacity for Recording Files

MaxCS now regularly checks the available disk space of four drives, to make sure that there is enough space for voice recordings:

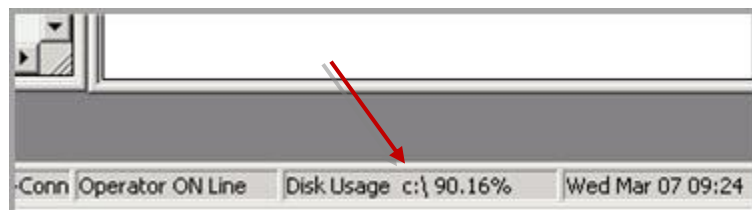
- The Windows system drive
- The MaxCS server drive
- The postoffice system drive
- The Voice Recording drive (this drive is monitored only if recording is enabled and the recording folder is set to the local drive)

MaxCS also includes 4 new SNMP traps for this disk space monitoring. You can specify the threshold for these traps in MaxAdministrator: **Report > SNMP Configuration**. The trap will be triggered every 30 minutes while the usage remains above the specified threshold.

OID	Description
1.3.6.1.4.1.13679.17.1	Alerts if the System drive is low on disk space
1.3.6.1.4.1.13679.17.2	Alerts if the MaxCS drive is low on disk space
1.3.6.1.4.1.13679.17.3	Alerts if the post office server drive is low on disk space
1.3.6.1.4.1.13679.17.4	Alerts if the recording drive is low on disk space

Note that the earlier trap 1.3.6.1.4.1.13679.17 is no longer used.

Within MaxAdministrator, the status bar shows you the state of the disk that is closest to being full:



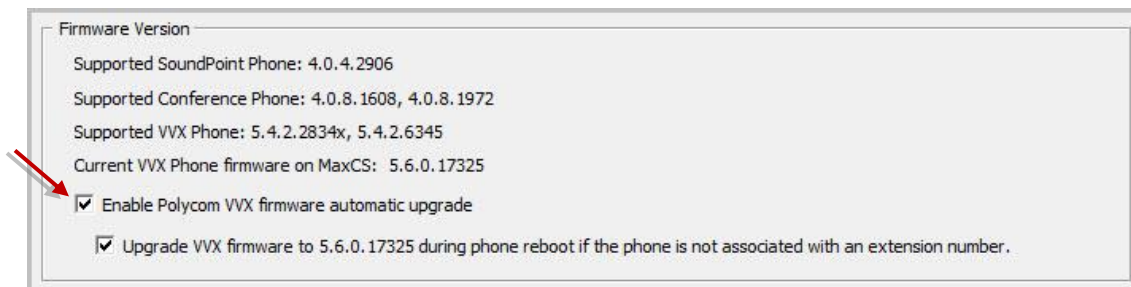
If MaxCS detects that one of those drives has exceeded the capacity of the registry value that you configured, you will see an alert when you open MaxAdministrator, to warn you. The alert will list the state of each drive. The registry entry where you assign this threshold is:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AltiGen Communications, Inc.\AltiWare\DiskSpace

Polycom VVX Firmware Auto-update Options

This release includes a new *Enable Polycom VVX firmware automatic upgrade* option in **System > Polycom Configuration**. It defaults to disabled (unchecked).

While this option is unchecked, VVX phone firmware will **not** be updated.



Refer to the *Polycom Configuration Guide* for full details on how to enable/disable firmware updates for VVX phones.

Polycom E911 Location ID from MAC Address

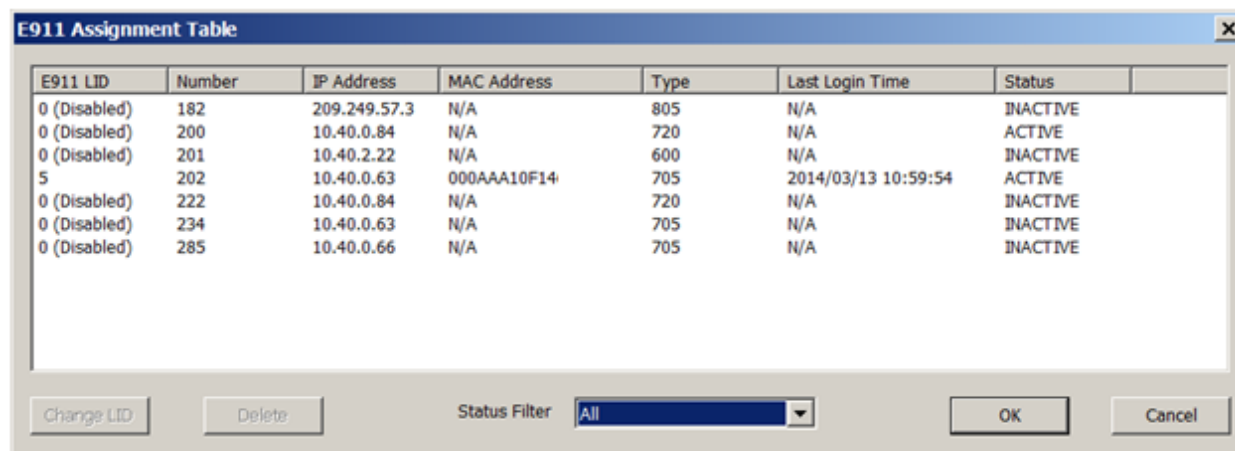
Beginning with Release 8.5 Update 1, you have a new way to assign E911 Location IDs (LIDs) to Polycom phones.

Note that you can still use the old method (updating each phone's .cfg file), if necessary. The new method fully supports roaming users.

During the Polycom SIP registration process, MaxCS retrieves each Polycom phone's MAC address and assigns an E911 LID based upon that MAC address. Initially, the system assigns the default LID number 0.

You can change the phone's E911 LID assignment from the default 0 to an appropriate LID, the same way that you would update LIDs for Altigen IP phones.

To change a Polycom phone's assigned E911 LID, select **PBX > Location Based E911 Configuration**, then choose **View E911 Assignments**. You will see Polycom phones listed along with Altigen IP phones. Select the extension and click **Change LID**.



E911 LID	Number	IP Address	MAC Address	Type	Last Login Time	Status
0 (Disabled)	182	209.249.57.3	N/A	805	N/A	INACTIVE
0 (Disabled)	200	10.40.0.84	N/A	720	N/A	ACTIVE
0 (Disabled)	201	10.40.2.22	N/A	600	N/A	INACTIVE
5	202	10.40.0.63	000AAA10F14	705	2014/03/13 10:59:54	ACTIVE
0 (Disabled)	222	10.40.0.84	N/A	720	N/A	INACTIVE
0 (Disabled)	234	10.40.0.63	N/A	705	N/A	INACTIVE
0 (Disabled)	285	10.40.0.66	N/A	705	N/A	INACTIVE

When you change the LID for a Polycom phone, you are essentially mapping the phone's MAC address to the new LID on the MaxCS server.

With this new design, the E911 CID stays with the physical phone instead of being associated with the extension.

Updating Previous E911 Entries in Polycom Configuration Files

This section applies only if you are upgrading from an earlier version of MaxCS and you had edited Polycom configuration files to include an E911 Location ID (LID).

In earlier releases, you set a Polycom phone's E911 LID by editing the phone's .cfg file.

Starting with Release 8.5 Update 1, you have two options:

- if you do not want to manage Polycom phone LIDs within MaxAdministrator, you can leave these custom entries intact. The custom entry in the configuration file overrides any MAC address/LID setting in MaxAdministrator for that extension. Note that this method does not fully support roaming users; therefore, we recommend that you switch to the new method.
- If you prefer to use the E911 LID table to configure Polycom LIDs, then you must edit the custom entries in those extension .cfg files.

Here is an example of how to edit those configuration files. In this example, we use extension 286; substitute the actual extension number in each file.

1. On the MaxCS server, open the ..\altiserv\PolycomCFG\Extension_286.cfg file.
2. Modify the line `reg.1.auth.userid="286xatgnemx2"` to:

```
reg.1.auth.userid="286"
```

3. Save the file.
4. In MaxAdministrator, select PBX > AltiGen IP Phone Configuration and switch to the Polycom tab. Select the extension (286) and click Save and Reboot Polycom Extension.

Note that in some cases, you may need to reboot the phone twice in order for the change to take effect.

SightMax/ChatBeacon Support

The third-party application *SightMax* has been updated and renamed to *ChatBeacon*; MaxCS supports ChatBeacon version 2.0.

For instructions, refer to the *MaxCS ChatBeacon Integration Guide*.

MaxCS 8.5 QuickFix Enhancements

This section describes enhancements that were included in the 8.5 QuickFix Release.

General Security Enhancements/TLS 1.2 Support

This release of MaxCS includes several security enhancements:

- MaxCS now supports TLS 1.2; there is an option to use *only* version 1.2 when TLS is used
- MaxCS now supports public certificates; there is also a new SNMP trap, to alert admins when a public certificate is approaching its expiration date (OID 1.3.6.1.4.1.13679.38.1)

The next few sections describes these enhancements.

Public Certificate Support

Public certificates are **optional** in MaxCS.

MaxCS supports the following types of public certificates:

- Common Subject certificates
- Wildcard certificates
- Certificates with Subject Alternative Names (SANs)

To obtain a public certificate, businesses need to own a public DNS domain and assign MaxCS a FQDN in that DNS domain. Then you can purchase a public certificate.

Altigen recommends obtaining a certificate from GoDaddy. We recommend these certificates because their CA certificate will not expire until the year 2031, which is much later than many other provider's certificate expiration dates. See <https://www.godaddy.com/web-security/ssl-certificate>. If you let your public certificate expire, **your Polycom phones will no longer register**.



Certificate Details

Please note the following when you are implementing a public certificate:

- When you are creating a certificate request in Windows and must choose a Cryptographic Service Provider, select *Microsoft RSASChannel*, 2048 bit). The steps on this web page may be helpful to you: <https://www.digicert.com/csr-ssl-installation/iis-7.htm>
- Complete the certificate signing on the IIS server where you initially generated the Certificate Signing Request (CSR).
- Use Windows MMC (Microsoft Management Console) to export the file to a .pfx file. You may find the instructions in this web page helpful: <https://www.ssldesk.com/export-ssl-certificate-private-key-pfx-using-mmc-windows/>
- You must enable TLS 1.2 on the server in order to use a public certificate.

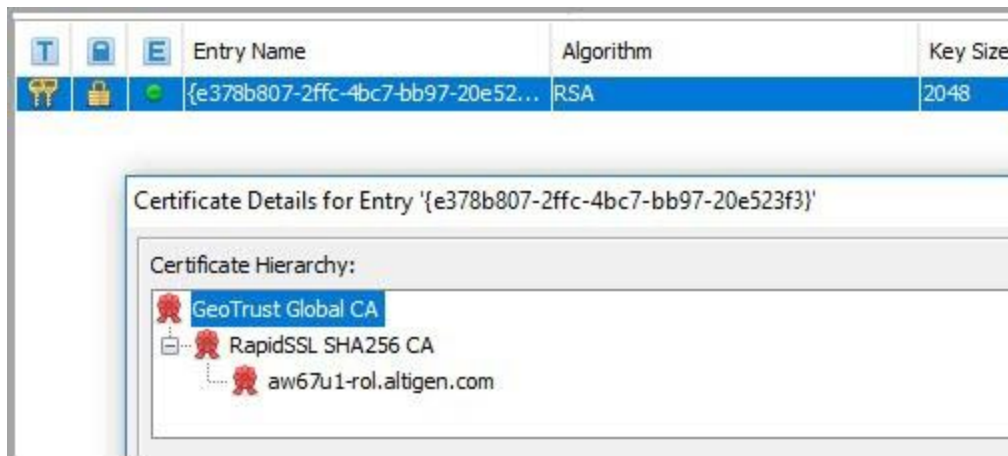
Certificate Format

The certificate format that MaxCS supports is the .pfx format, which is used by Microsoft IIS.

The key pairs in the .pfx file must contain the full certificate chain; otherwise, Polycom phones may reject it. To confirm that a .pfx file contains a full certificate chain:

1. Download the Keystore Explorer tool from the internet (<http://keystore-explorer.org/>).
2. Open the .pfx file in Keystore Explorer and double-click the key pair entry.

The full certificate chain should appear, similar to the following figure.



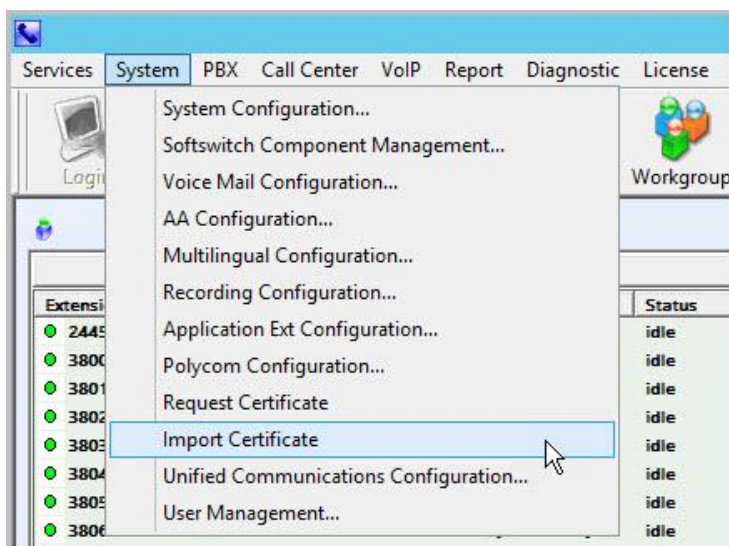
In this example, GeoTrust Global CA is supported by Polycom phone, so the full certificate chain/certificate hierarchy should be “GeoTrust Global CA>RapidSSL SHA256 CA>aw67u1-rol.altigen.com.”

The Polycom phone already has “Geo Trust Global CA” in its firmware, so “GeoTrust Global CA” is optional in this certificate hierarchy. In other words, whether you see “GeoTrust Global CA” in this certificate hierarchy or not, the Polycom phone will accept the certificate. However, if you only see “aw67u1-rol.altigen.com” in this hierarchy, then the .pfx file does not contain the sufficient certificate hierarchy information, and the Polycom phone will reject it.

Import a Public Certificate

To import a public certificate into MaxAdministrator:

1. In MaxAdministrator, select **System > Import Certificate**.



2. Browse to the .pfx certificate file.
3. Enter the private key password for this certificate, if required, into the *Private Key Password* field. Click **OK**.

4. You will see a notification that a server restart is required. The certificate will take effect after you restart all Altigen services.

Note that a new SNMP trap will alert you when a public certificate is close to its expiration date.

Limit TLS to Version 1.2 Only

Note that Windows 2008 does not fully support TLS version 1.2. Therefore, no version of Altigen MaxCS Server Software supports TLS 1.2 on Windows 2008 Server.

Some organization have policies that all systems on TLS must use TLS version 1.2 only, for enhanced security. To offer this service, MaxCS has a new option on the **System Configuration > General** tab: *Use TLS 1.2 only when TLS is used*.

Before you check this TLS option, confirm that all of the following entities support TLS 1.2:

- Polycom phones
- The current firmware on all Altigen phones
- Third-party SIP clients

In addition, if you are using TLS on SIP trunks, all of the following entities must also support TLS 1.2:

- Third-party gateways
- SIP trunk service providers (Note that Altigen SIP trunks support TLS1.2; if you require TLS/SRTP on Altigen SIP trunks, contact Altigen Support to coordinate that configuration change)

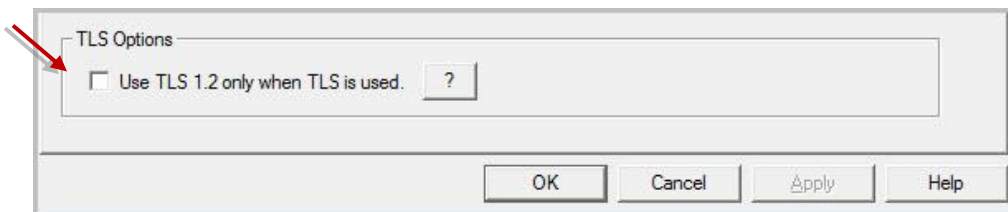
Any SIP TLS end point (SIP Trunk, SIP client, etc.) that does not support TLS 1.2 will not work with MaxCS if you enable this option. If you have phones that do not support TLS 1.2 and you enable TLS to version 1.2 only, then those phones may not work properly. For example, they may not be able to place or receive calls, or other errors may occur.

Important

Note: You must manually reboot the MaxCS system in order for this option to take effect.

To enable this feature,

1. Select **System > System Configuration**.



2. On the *General* tab, check the option **Use TLS 1.2 only when TLS is used**. (Click the “?” button for full details on this option.) Save your changes.
3. At an appropriate time, stop the Altigen services and reboot the MaxCS server. Your change will not take effect until after you reboot the service.

TLS 1.2 Support on Altigen Phones

Altigen has new firmware, version 2xB3, which will work with MaxCS regardless whether TLS 1.2 is used/enforced in your environment. Note that this new firmware only accepts the SIP TLS connection from the MaxCS server to which it is registered; it will reject any other attempted connections.

This firmware can be applied to the following Altigen phones:

- IP 705
- IP710
- IP 720
- IP 720a

Altigen IP phones do not need to use public certificates.

Configure IP-805 Phones in a TLS 1.2 Environment

The Altigen IP-805 does not support TLS 1.2. Therefore, when you are using IP-805 phones in a TLS 1.2-only environment, those phones must use SIP UDP/RTP mode.

To configure this, disable TLS/SRTP on each IP-805 phone extension:

1. In MaxAdministrator, select **PBX > Altigen IP Phone Configuration**.
2. On the *General* tab, clear the two *SIP Transport* checkboxes.

Administrator Change Log

The MaxCS 8.5 Administrator Change Log Report (CLR) allows administrators and auditors to track configuration changes that have been made to MaxCS 8.5 by administrators through the MaxAdministrator program.

Note that changes that have been made through applications other than MaxAdministrator, such as any changes made through Enterprise Manager or any board configuration changes performed at the Service Provider level, will not appear in Change Log Reports.

This document describes how to generate MaxCS 8.5 Administrator Change Log Reports.

Requirements

In order to generate reports of changes logged through MaxCS 8.5 Administrator, your system must be running MaxCS release 8.5 QuickFix or later.

Configuration changes made within MaxAdministrator are logged into the CDR database via the Internal/External Logger service. Therefore, the External Logger Service and an external SQL server (to host the CDR database) are required.

No direct SQL database connection between MaxAdministrator and the CDR database is required.

Overview

When an administrator makes a configuration change within MaxAdministrator, the details of that change are logged into the CDR database.

The record contains information such as the following:

- The date and time of the change
- A description of the change
- The user who made the change

Administrators generate Change Log Reports by clicking a button within MaxAdministrator and specifying criteria such as a date range, a user, or an action pattern match. The query request is sent to Altiserv; Altiserv queries the

logs through the Log Service and returns the matching results to the administrator. From there, the report can be exported to a PDF file as needed.

About the Change Records

When an administrator submits configuration changes, change records are saved to the *AdminLog* table in the CDR database.

This table consists of the following columns.

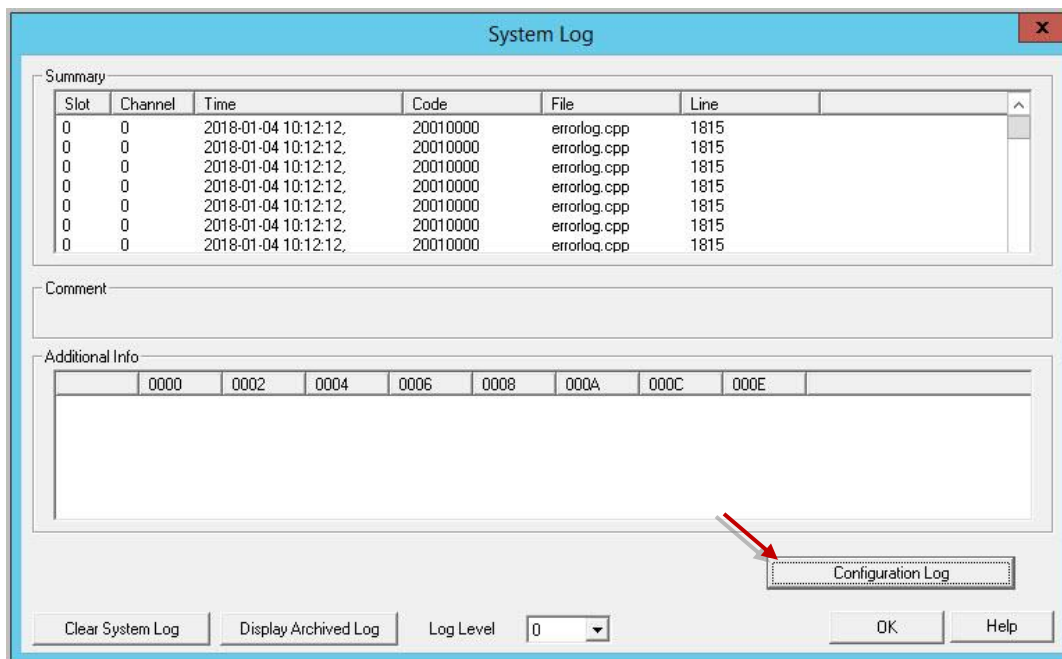
Column	Description
[GUID]	The GUID of the transaction; all records generated by this user's change will share the same GUID
[SeqId]	The sequence number of the record
[date]	The date and time that the change was made
[user]	The login name of the admin user who made the change
[description]	A description of the change that was made

More than one record may be written, depending upon the actual changes that the admin user makes. If so, each record for the event will share the same GUID. *Only the first record in the sequence* will show the date and the user.

Generating a Change Log Report

To generate a Change Log Report,

1. Log into MaxAdministrator and select **Diagnostic > System Log**.
2. Click the **Configuration Log** button. The Query panel opens.



3. Specify a Report Header; the text you enter here will appear at the top of the report. The Report Header is retained; when you next run a report, this text will be prepopulated for you. This field has a maximum character length of 1024.
4. The Data Source options will include the log services that are configured in the system. Choose a source.
5. Optional fields:
 - Specify a date range, if appropriate.
 - Specify a user, if appropriate, by entering some of the user's name. Wildcards are supported. If you leave this field blank, all users will be included in the report.
 - Enter a description for the report (maximum characters 1023).
6. Click **Query**. A panel shows you the configuration changes that meet your report criteria.

No.	LogDate	LogUser	Description
1	1/3/2018 07:33:31	admin	Replace ext 2445, rc 0
2	1/3/2018 07:36:09	admin	Offset of OEXT=449, len=1, OldValue=44, NewValue=04 .
3	1/3/2018 07:36:14	admin	Replace ext 2448, rc 0
4	1/3/2018 07:37:44	admin	Offset of OEXT=449, len=1, OldValue=44, NewValue=04 .
5	1/3/2018 07:39:23	admin	Replace ext 2448, rc 0
6	1/3/2018 07:39:23	admin	Offset of OEXT=449, len=1, OldValue=04, NewValue=00 .
7	1/3/2018 07:39:23	admin	Replace ext 2448, rc 0
8	1/3/2018 07:39:29	admin	Offset of OEXT=449, len=1, OldValue=00, NewValue=04 .
9	1/3/2018 07:39:30	admin	Update ext 2447 monitor list
10	1/3/2018 07:49:20	admin	Set monitor list of ext 2447
11	1/3/2018 08:36:08	admin	Add ext 2447, rc 0
12	1/3/2018 08:49:28	admin	Replace ext 2447, rc 0
13	1/3/2018 08:50:13	admin	Offset of OEXT=446, len=1, OldValue=0C, NewValue=4C .
14	1/3/2018 08:50:13	admin	Offset of OEXT=2228, len=1, OldValue=00, NewValue=01 .
15	1/3/2018 08:50:13	admin	Offset of OEXT=2232, len=4, OldValue=FF FF FF FF, NewValue=00 00 00 00 .
16	1/3/2018 08:50:38	admin	Replace ext 2447, rc 0

7. Click **Export to PDF** if you want to save the report as a PDF file; specify the filename and location.

Polycom Enhancements

This release includes several Polycom security enhancements.

Firmware Updates in Release 8.5 QuickFix

The VVX phones and the SoundStation phones have new firmware in this release.

Supported Polycom Firmware		
VVX Models	IP300/310/311 IP400/410/411 IP500/501 IP600/601	Firmware version 5.6.0.17325 This firmware version is required in order to use a public certificate and to use TLS 1.2
	Note that the IP1500 is not supported.	
SoundStation Models	IP6000 IP7000	Firmware version 4.0.13.1445 This firmware supports the use of public certificates, but does not support TLS 1.2
SoundPoint Models	IP331 IP450 IP550 IP560 IP650 IP670	4.0.4.2906 (BootROM 5.0.4.x, 5.0.5.x, or later) – this is the ‘4.0.4 Split’ download from the Polycom download site SoundPoint models do not support TLS 1.2 or public certificates.

Retrieving Altigen Enterprise Certificates for Polycom Phones

To request an Altigen certificate for your Polycom phones,

1. In MaxAdministrator, select **System > Request Certificate**.
2. Enter the either IP address or the FQDN of your MaxCS server.

The system will prompt you to reboot the server once the certificate is requested.

Polycom Support for Public Certificates

MaxCS supports the following types of public certificates:

- Common Subject certificates
- Wildcard certificates
- Certificates with Subject Alternative Names (SANs)

Polycom supports certificates from a few specific Certificate Authorities, including GoDaddy, Verisign, and Comodo. The list is too long to reproduce here, and is also subject to change after this guide goes to publication. Therefore, we recommend that you perform a web search for “Certificate Updates for Polycom UC Software” and obtain a complete and up-to-date list of accepted CA’s.

Note that if a public certificate expires, the Polycom phones will no longer register. Therefore, make sure not to let public certificates expire.

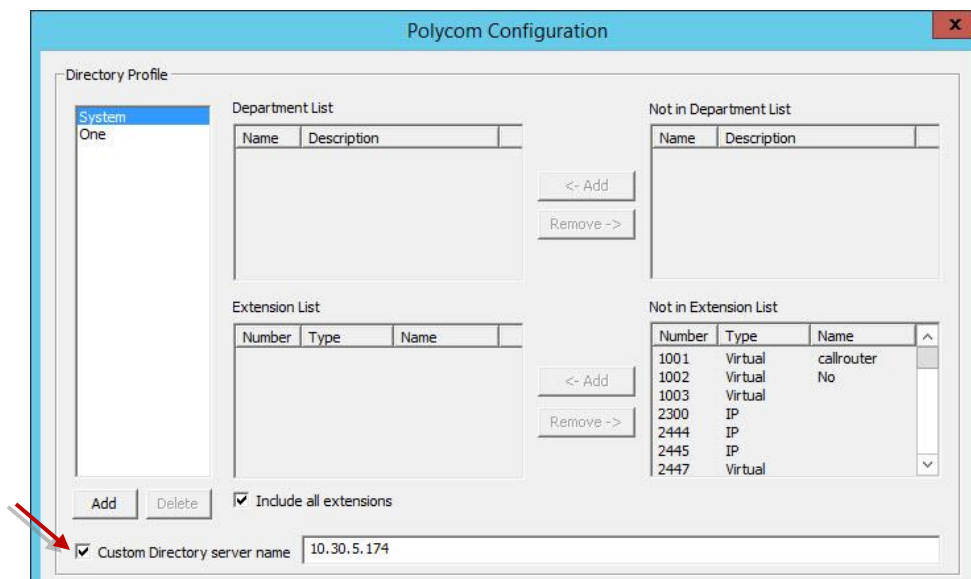
For details on the required format of the certificate, and how to import a certificate, see the section [Public Certificate Support](#).

Specify the Polycom Custom Directory When Using Public Certificates

This release includes a new field, where you can specify the location of the Polycom Directory server.

By default, that directory server is the certificate's host name or an IP address.

If you are using a wildcard or SAN public certificate, you will need to enter FQDN for the MaxCS Server in this field.



To reach this field, select **System** > **Polycom Configuration**.

MaxCS 8.5.0.222 Enhancements

This section describes enhancements that were included in Release 8.5.0.222.

Plantronics Headset Support

The following headsets have been tested and certified for this release:

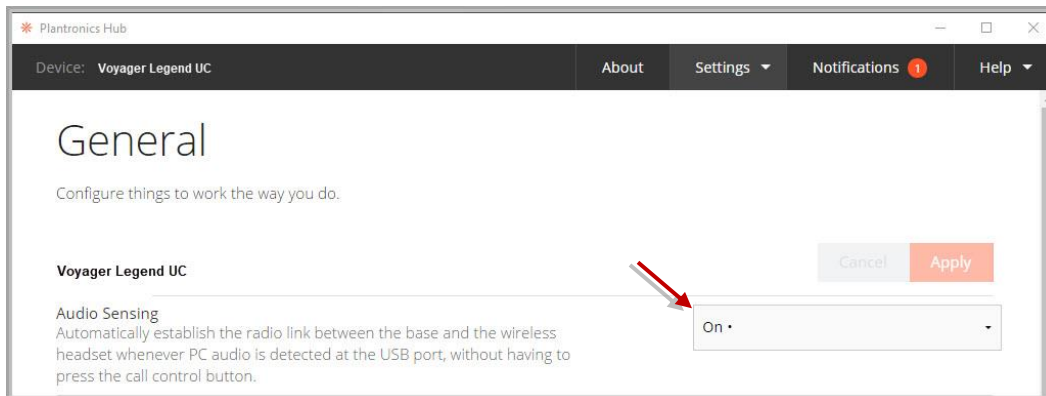
- W740-M
- W420
- Voyager Legend UC

Plantronics headsets are supported on these clients:

- MaxAgent
- MaxCommunicator

Plantronics Installation and Configuration

1. Follow the Plantronics Headset *Quick Start Guide* to set up the headset and load the *Plantronics Spokes* software.
2. Open the Plantronics Hub application and set *Audio Sensing* to **On**. Save the change.



3. Run the MaxCS client (MaxAgent or MaxCommunicator) *setup.exe* file and follow the instructions to complete the installation.
4. In the client's *Settings* section:
 - a) Set the *IPTalk Voice Through* and optionally the *Ring Through* options to your Plantronics device.
 - b) Check the option *Plantronics Headset Integration*.
 - c) Save your changes.

Using Plantronics Headsets with MaxCS Client Applications

Use the Call Answer / End button to:

- Answer a call
- End a call
- Resume a call that was placed on hold

Note that you cannot place calls on hold via the Plantronics headset.

Known Issues with Plantronics Headset

Following are known issues with Plantronics headset support in this release.

- When you press the flash button in MaxAgent to transfer a call, you cannot press the Plantronics button to disconnect.
- When the 'Plantronics Headset Integration' option is enabled and multiple calls are active, intermittently only one ring tone is played when call comes out of personal queue. The user can still see the incoming call popup.
- When the 'Plantronics Headset Integration' option is not enabled on the MaxCS client, incoming ring tones may be cut off in some headsets.

Operational Notes

- While your Plantronics headset is integrated with a MaxCS client, you must close your Lync/Skype client; you cannot enable the headset with a MaxCS client and with Lync/Skype at the same time.
- The #81 and #82 features are not supported on Plantronics headsets

Operational Limitations

Refer to the Readme files on your installation media for any know limitations with this release.

Altigen Technical Support

Altigen provides technical support to Authorized Altigen Partners and distributors only. End user customers, please contact your Authorized Altigen Partner for technical support.

Authorized Altigen Partners and distributors may contact Altigen technical support by the following methods:

- You may request technical support on Altigen's Partner web site, at <https://partner.altigen.com>. Open a case on this site; a Technical Support representative will respond within one business day.
- Call 888-ALTIGEN, option 5, or 408-597-9000, option 5, and follow the prompts. Your call will be answered by one of Altigen's Technical Support Representatives or routed to the Technical Support Message Center if no one is available to answer your call.

Technical support hours are 5:00 a.m. to 5:00 p.m., PT, Monday through Friday, except holidays.

If all representatives are busy, your call will be returned in the order it was received, within four hours under normal circumstances. Outside Altigen business hours, only urgent calls will be returned on the same day (within one hour). Non-urgent calls will be returned on the next business day.

Please be ready to supply the following information:

- Partner ID
- Altigen Certified Engineer ID
- Product serial number
- AltiWare or MaxCS version number
- Number and types of boards in the system
- Server model
- The telephone number where you can be reached



NOTICE: While every effort has been made to ensure accuracy, Altigen Communications, Inc., will not be liable for technical or editorial errors or omissions contained within the documentation. The information contained in this documentation is subject to change without notice.

This documentation may be used only in accordance with the terms of the Altigen Communications, Inc., License Agreement.

Altigen Communications, Inc.

679 River Oaks Parkway, San Jose, CA 95134

Telephone: 888-Altigen (258-4436) | Fax: 408-597-9020

E-mail: info@altigen.com Web site: www.altigen.com

All product and company names herein may be trademarks of their registered owners. Copyright © Altigen Communications, Inc. 2018. All rights reserved.