New Features Guide

MAXCS 7.5 Patch 1

May 13, 2015

Contents

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

Introduction

This guide describes the enhancements that have been added since the original release of MaxCS Release 7.5. Enhancements included in this build include:

- **Free Format** – This feature lets you insert delays and/or to send out additional DTMF digits when forwarding calls to an extension, a hunt group, a workgroup, or an outside number. This option is located on the **PBX** > **Extension Configuration** Answering tab. See page 5 for details.
- **Verizon SIP trunk support** – Two new SIP Trunk options, *Custom P-Asserted Identity* and *Diversion*, have been added to the SIP Trunk Profile parameters to support Verizon Caller ID. *Custom P-Asserted Identity* allows you to insert a header into the SIP packet. See page 6 for details.
- **SIP Trunk Release Link Tie** (SIP Refer) - This feature is implemented to support various AudioCodes devices. It instructs the SIP Trunk provider to release both the inbound and the outbound legs of a transferred call once the transfer has been completed. See page 6 for a brief summary; refer to the configuration guide for your specific AudioCodes device for full instructions.

  Note: Not all PBX or services providers support SIP Refer or release link tie.
- **SIP Trunk TLS Support** – This feature is implemented to support SIPTrunk.com SIP Trunks. This feature is briefly described on page 9. For full details, refer to the appropriate SIP Trunk Configuration guide in the AltiGen Knowledgebase.
- **IPTalk Redirect** – This feature allows users to redirect a client application to the alternate server if the client loses its connection to the main server. See page 9 for details.
- **SIP Delayed Offer Support** – MaxCS now supports SIP Delay Offer on incoming SIP calls.
- **Polycom Global Relocation** – Users can now relocate their Polycom phones within the Enterprise domain. See page 14 for details.
- **Polycom Password Consolidation** – AltiGen has merged the various passwords for Polycom phones, to make maintenance an easier process. See page 14 for details.
- **Polycom Secondary Proxy** – You can now assign a secondary proxy server that Polycom phones will connect to when the main MaxCS server becomes unavailable, for limited inbound and outbound calls. When the main MaxCS server is back up, the phones will automatically reconnect to the main server. See page 16 for details.

Requirements

In order to apply this update, your environment must meet the following minimum requirements:

- The server must be running MaxCS Release 7.5.0.502
- Polycom VVX model phones must have firmware version 5.2.2.0501. You can either upgrade phone firmware before you upgrade to MaxCS 7.5 Patch 1, or wait and upgrade the firmware after you have completed the MaxCS update (see the *Polycom Configuration Guide* for full configuration details).

Applying MaxCS 7.5 Patch 1

You can also find these instructions in the Readme file.

Server Update

This update can be applied only onto a MaxCS server that is running Release 7.5, including Release 7.5.502.

On the AltiWare server system:

1. Read the readme file carefully; you should be aware of the various bug fixes and other updates that have been included in this update.
2. Run *UpdateServer.exe*. Follow the instructions in the installation wizard.
3. A message, "AltiGen Service Utility," will appear during the installation. Please shut down all AltiGen services.

Client Update

MaxAgent, MaxCommunicator, and MaxOutlook clients must be upgraded. This can be done through the auto-upgrade process as the applications are launched. There is no need to install files from the MaxClientAndOtherApp folder. However, for convenience, the full installation is still included in the folder.

Update Notes

If you installed a stand-alone version of MaxAdministrator, upgrade MaxAdministrator by running the full MaxAdministrator installation in the folder *MaxClientAndOtherApp\MaxAdministrator*.

When MaxCS is installed, a built-in program, MaxAdministrator UpdateServer.exe, will also update the MaxAdministrator.

When you copy the installation files to other location, also remember to copy the "Shared Components" folder.

Rollback Instructions

The following procedure can only be used to roll back to the previous state. For example, if you are running version 7.5.0.502 and update to 7.5 Patch 1, you can rollback **only** to version 7.5.0.502.

To roll back to the previous update on the server,

1. Run *UpdateServer.exe*.
2. Select **Rollback to previous update** and choose **Next**.

Enhancements Included in MaxCS 7.5 Patch 1

This section describes the new features included in this update.

Free Format Forwarding Support for SIP Trunk and SIP Extensions

You can configure an extension to send out additional DTMF digits to an extension, hunt group/workgroup, or outside number after the call is forwarded to an outside line.

There are various uses for this virtual-forwarding feature. For example, you can configure an extension to forward fax calls to the first available fax hunt group. Another example would be to forward calls to a FaxFinder extension. You can embed several commas to add a delay before MAXCS releases the Centrex line to complete a call transfer.

Free format is supported on SIP trunks, PRI trunks, T1 trunks, analog trunks, SIP extensions, and analog extensions.

Example: Forwarding to a FaxFinder Extension

Suppose that you want an extension to forward incoming calls to a FaxFinder extension 2002 which is behind an AudioCodes MP202 or MP118 device. This configuration is illustrated in the next figure.

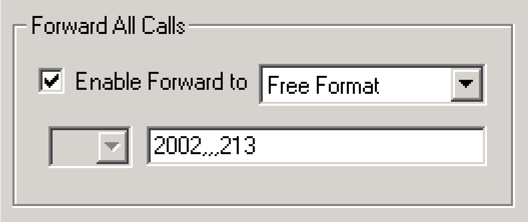


Figure 1: Example of call forwarding with a 3-second delay and DTMF digits to send

The string in Figure 1 indicates that the call should be forwarded to extension 2002 (for FaxFinder). The next three commas each insert a one-second delay. The last three digits indicate to send DTMF digits 213.

After the DTMF digits are received, FaxFinder will use "213" as the destination number to receive the Fax.

Example: Forwarding to an Outside Number

Suppose you have a virtual extension 2001 and you want to set call forwarding to an outside number "4085979000" through the SIP trunk.

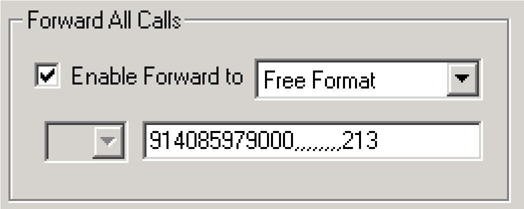


Figure 2: Example of call forwarding to a specific extension at an external phone number

In Figure 2, the string indicates to forward the call to that outside phone number (our example is AltiGen's corporate phone number) and then wait for 8 seconds (this is the 8 commas). After that delay, three more DTMF digits will be sent out through the SIP trunk. The result is that the call will be sent to extension 213.

Format Guidelines

- Each comma inserts a one-second delay after the call is forwarded. We recommend that you use at least five commas (for five seconds). Longer numbers may require additional commas. However, too many commas will impact the cut through time.
- You can enter up to 40 digits.
- You can include the digits 0-9, *, #, and ",".

Configure Forwarding

To configure this forwarding,

1. Select **PBX** > **Extension Configuration**.
2. Select the extension and switch to the *Answering* tab.
3. Check *Enable Forward to* and set it to **Free Format**.
4. Enter the appropriate string in the next field.

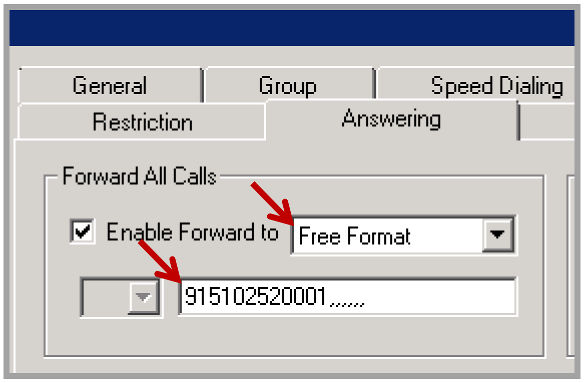


Figure 3: Example of call forwarding to an outside phone number with a long delay

Expanded Caller ID Support

This feature is designed for support of Caller ID on Verizon SIP Trunks. Unless you are instructed by your service provider to set these values, you should only use these fields when you connect to Verizon SIP Trunks.

Two new SIP Trunk options, *Custom P-Asserted Identity* and *Diversion*, have been added to the SIP Trunk Profile parameters.

- *Custom P-Asserted Identity* allows you to insert a header into the SIP packet. When this field is not empty, the specified header will be included in the SIP packet.

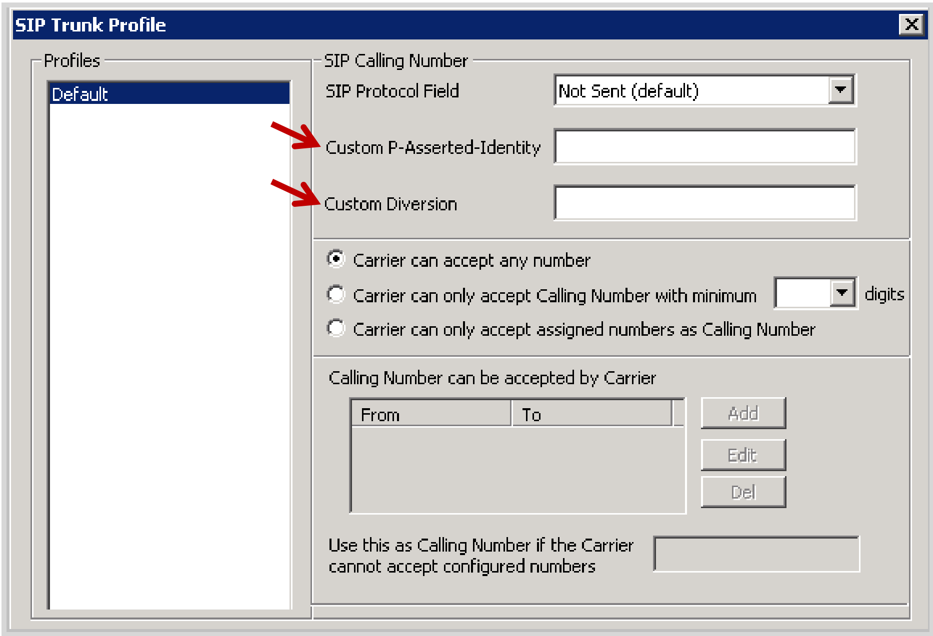


Figure 4: Two new SIP Trunk Profile parameters

- *Custom Diversion*. When this field is not empty, its content will be included in the SIP packet.

  If the field does not contain a semicolon, a suffix will be attached, as shown in red in the following line:

  Diversion: Custom diversion text;reason=unknown;privacy="off"

- if there is a semicolon in the text, the suffix will not be attached, as depicted in the following line:

  Diversion: Custom diversion text

Release SIP Tie-Link Trunk

This feature has been implemented to support various AudioCodes devices. We are providing a short overview here, for your convenience. For full AudioCodes configuration instructions, refer to the appropriate article for your AudioCodes model. Third-party configuration guides are stored in the AltiGen Knowledgebase (https://know.altigen.com).

Note: Not all PBX or services providers support SIP Refer or release link tie.

This feature instructs the SIP Trunk provider to release both the inbound and the outbound legs of a transferred call once the transfer has been completed.

The parameters for this feature, *Enable SIP REFER* and *Enable Centrex Transfer*, are located on the SIP Trunk Profile page. The extension-specific parameter for this feature, *Enable SIP Tie-Link Trunk*, is located on the **PBX** > **Extension Configuration** page, on the **General** tab.

To enable the feature within MaxCS Administrator, open the SIP Trunk profile and check the options *Enable SIP REFER* and *Enable Centrex Transfer*.

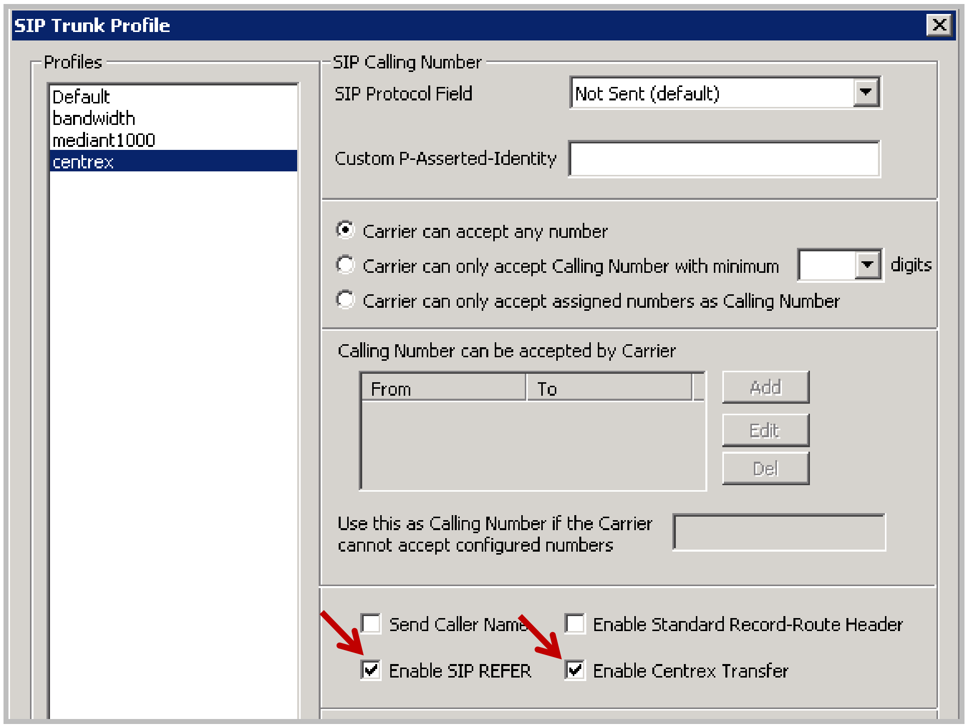


Figure 5: The "Enable SIP REFER" parameter for the SIP Trunk Profile

To configure the SIP Trunk, open the SIP Trunk Configuration panel and Set *SIP Trunk Profile* to the profile you just modified. Apply this setting to the other SIP trunks as appropriate.

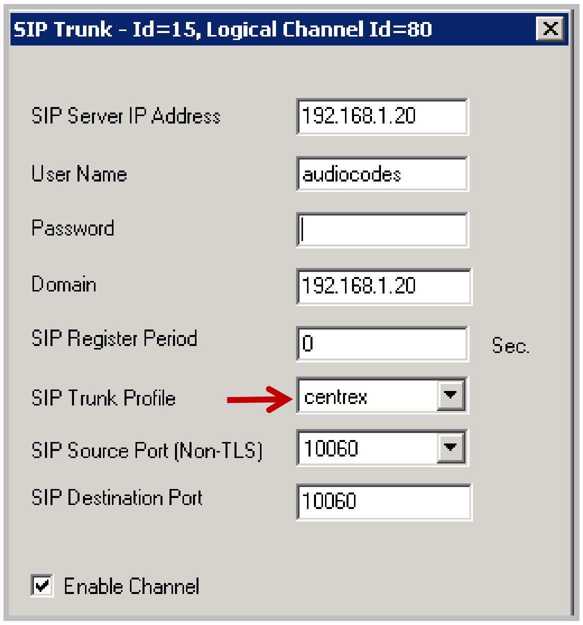


Figure 6: Assign the SIP Trunk Profile

To configure an individual extension, open its *General* tab and check the option *Release SIP Tie-Link Trunk*. This setting is supported for only virtual extension forwarding.

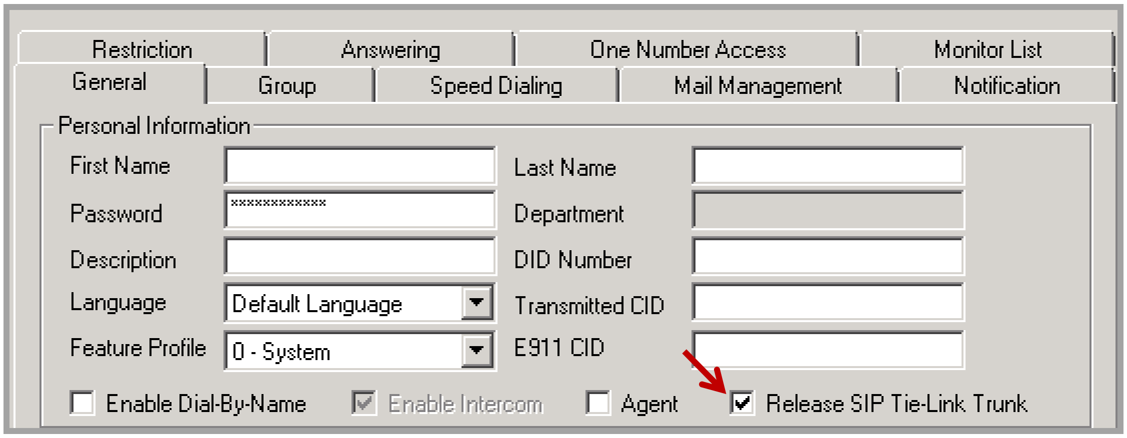


Figure 7: Check the "Release SIP Tie-Link Trunk" option

SIP Trunk TLS Support

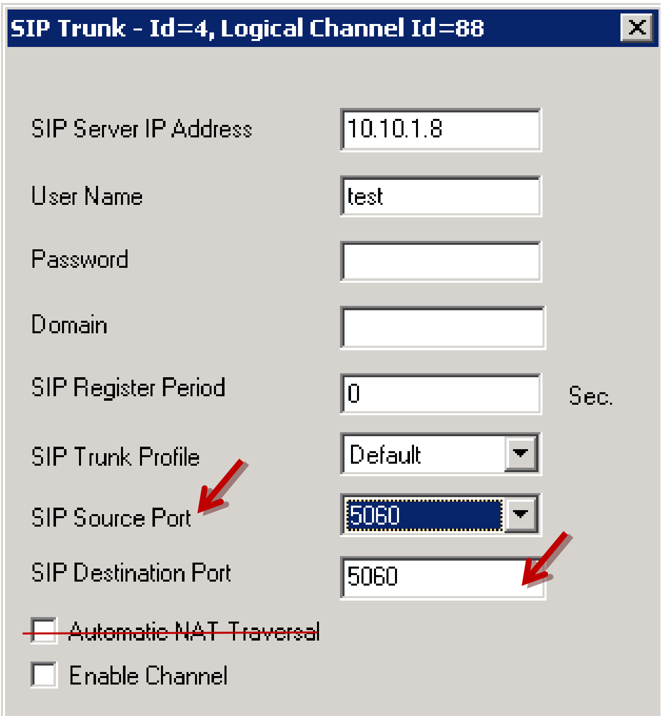
This release of MaxCS supports TLS/SRTP on SIP Trunks.

MaxCS SIP trunks will not verify a TLS far-end certificate. A self-signed certificate public key is provided under http://maxcs_ip_addr/altigen.crt, if the SIP trunk provider needs to verify the certificate. TLS/SRTP secures the SIP signal and voice between MaxCS and SIP trunk service provider.

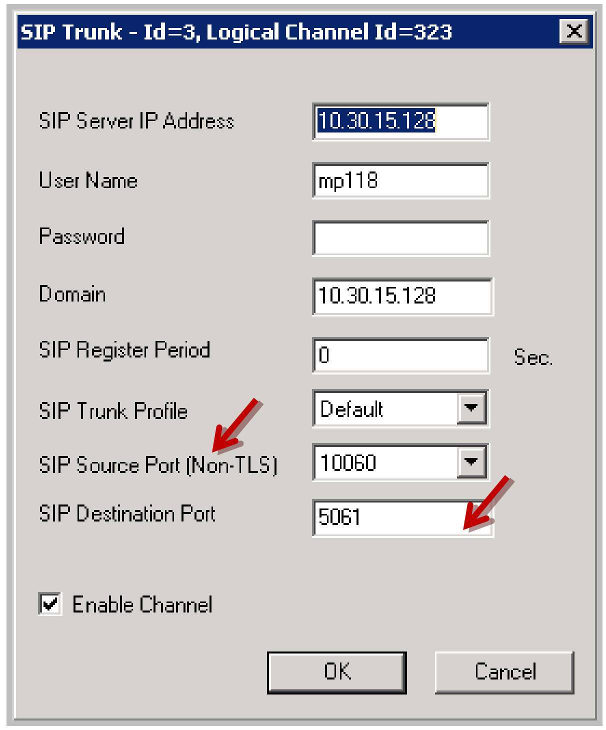
Supported devices:

- AudioCodes MP-11x
- AudioCodes Mediant 1000-B PRI / T1
- SIPTrunk.com SIP Trunks

When configuring SIP Trunks, you no longer see the option *Automatic NAT Traversal*. After you upgrade to this release, your SIP Trunks will no longer have this parameter. The option *SIP Source Port* has been changed to *SIP Source Port (Non-TLS).* The *SIP Destination Port* field in our example is set to **5061**. For SIPTrunk.com SIP Trunks, this field should be set to port 5067.



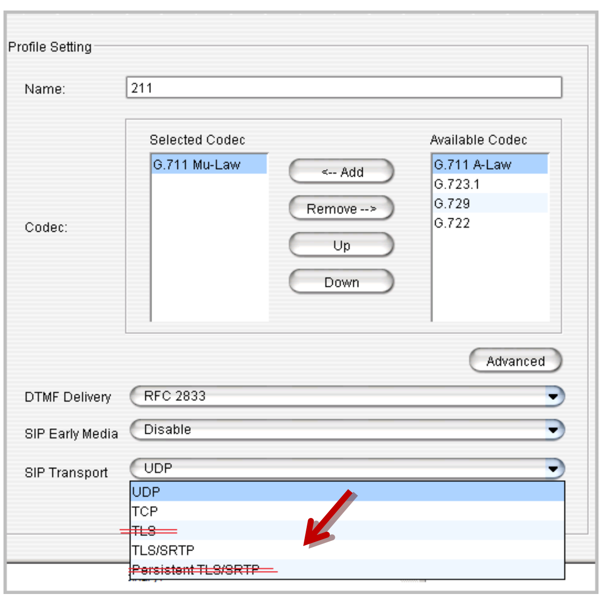
SIP Trunk parameters: Release 7.5



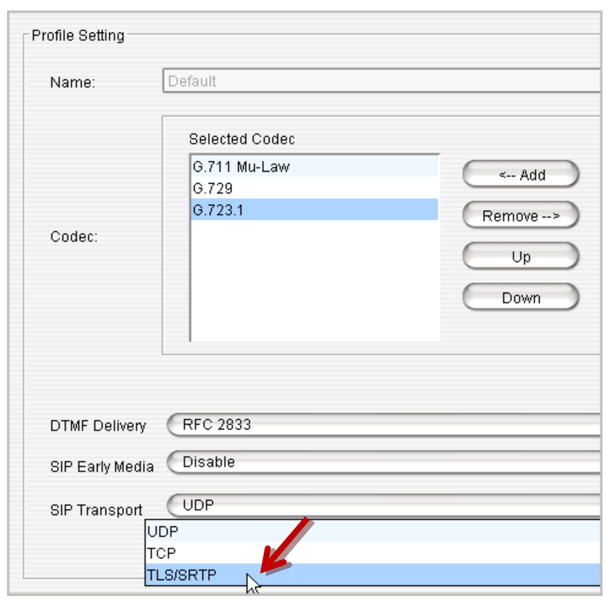
SIP Trunk parameters: Release 7.5 Patch 1

Figure 8: Changes to SIP Trunk parameters

Another enhancement is found in Enterprise Manager. The options “TLS” and “Persistent TLS/SRTP” in the codec settings are no longer available. All of the customer’s codec profiles that had the *SIP Transport* option set to **TLS** or **Persistent TLS/SRTP** will be updated to the new option **TLS/SRTP** automatically during the upgrade process.



SIP Transport options: Release 7.5



SIP Transport options: Release 7.5 Patch 1

Figure 9: Changes to the Codec Profile SIP Transport option

To configure a SIP Trunk for TLS/SRTP,

1. Make sure your SIP gateway or SIP trunk has TLS/SRTP enabled.
2. In MaxAdministrator, open Trunk view. Select **Trunk** > **Trunk Properties** > **SIP Trunk Configuration.**
3. Select a channel and click **Edit**. Enter the following parameters:
    - Fill in the SIP trunk server IP address, username, and password for the SIP trunk.
    - If the trunk needs to register to the MaxCS server, fill in the period. Otherwise, fill "0".
    - For the *SIP Destination Port*, use port 5067 for SIPTrunk.com SIP trunks. *SIP Source Port* is not used here. The SIP source port will be always 5061 if TLS/SRTP is used.
    - Check the Enable Channel checkbox.
4. Save the changes.

SIP Option over TLS is not supported.

IPTalk Redirect

The Redirect feature, if enabled by the Administrator, will prompt users to connect to a backup server if their client application loses its connection with the primary server.

This feature has been implemented in a similar fashion in the following MaxCS client applications:

- MaxAgent
- MaxCommunicator
- MaxOutlook

To enable this feature, Administrators will perform two steps:

1. Enable the Redirect feature for MaxCS.
2. Enable the Redirect ability for specific users.

How Administrators Enable the Redirect Feature

To enable the Redirect feature,

1. Apply the MaxCS 7.5 Patch 1 update.
2. Log into MaxCS Administrator.
3. First, enable the Redirect feature for MaxCS. Select **VoIP** > **Enterprise Network Management** to open Enterprise Manager.

4. Click the *Servers* button on the Toolbar. Select the **Information** subtab.
5. Check the option *Enable Redirection to Alternate Server*.
6. For *Alternate Server*, select the server that you want to use as the alternate server. Click **Apply**.

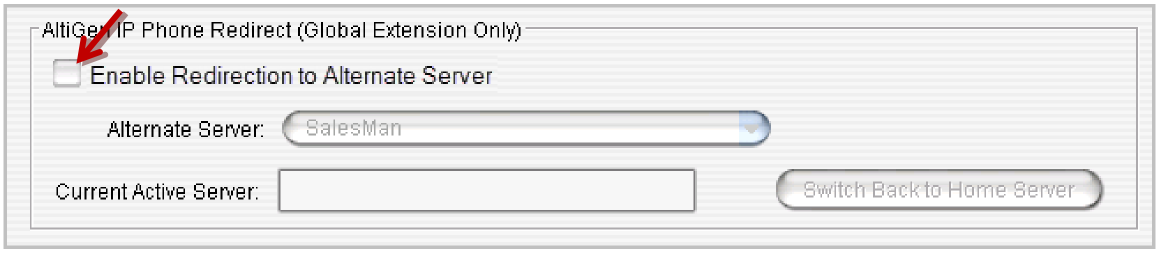


Figure 10: Enable the Redirect feature in Enterprise Manager

7. Next, enable the Redirect feature for specific users. In Enterprise Manager, click the *User* button on the Toolbar.
8. Select the *Resolve* subtab.
9. Select the users who will be able to use this switchover ability.
10. Select *Enable Switchover to Alternate Server*. Click **Apply**.

Figure 11: Enable Redirect individual users

11. Assign the IPTalk seat license to the remote extension to enable the IPTalk Redirect feature. You do this in the *Client Seat License Management* window.

How to Switch Users Back to the Main Server

In the event that the main server goes down or is otherwise unavailable, you can ask users to switch client applications from the alternate server back to the main server by following these steps:

1. Open Enterprise Manager, select *Servers* on the Toolbar, and select the *Information* subtab.
2. Click **Switch Back to Home Server**.

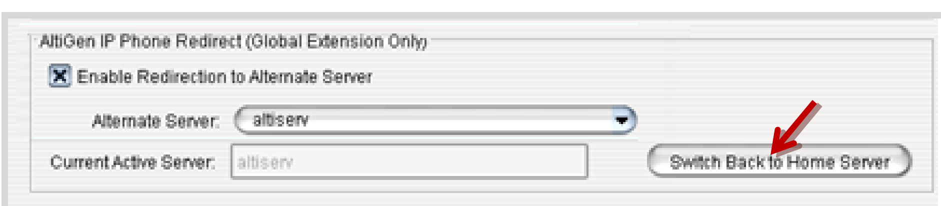


Figure 12: How to switch client applications back to the main server

The Redirect Feature from the User's Perspective

For MaxCommunicator and MaxAgent, when you enable this feature for MaxCS, those users to whom you have enabled the switchover ability will experience the following behavior if their client loses its connection with the MaxCS server:

1. When the MaxCS client application detects that its connection with the MaxCS server has been lost, the client will present a pop-up message to the user. The message will inform the user that the connection has been lost, and will offer the user several options.

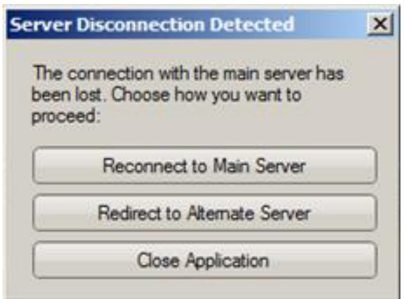


Figure 13: The client application prompts the user to reconnect or switch

2. If the user chooses **Reconnect to Main Server**, then the client will try to re-establish its connection with the main server. If it cannot reconnect, it will prompt the user to redirect the connection to the alternate server.

   If the user chooses **Redirect to Alternate Server**, then the client will establish a connection with the alternate server.

3. Once the Administrator has brought the main server back up and clicked *Switch Back to Home Server* within Enterprise Manager, the user will be prompted to switch the client's connection back to the main server.

MaxOutlook Reconnection

For MaxOutlook, when the connection with the main server is lost, this message opens:

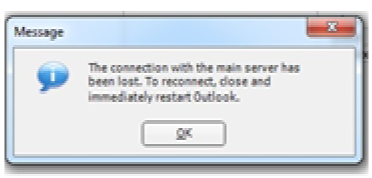


Figure 14: MaxOutlook user prompt

After the user closes Outlook and restarts it (within 5 minutes), MaxOutlook prompts the user to either reconnect or redirect.

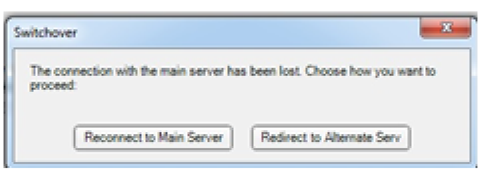


Figure 15: MaxOutlook prompt to reconnect

If the user does not restart MaxOutlook within 5 minutes, MaxOutlook will not redirect, and the user will see the login page showing the login server address as the main server.

Once the Administrator has brought the main server back up and clicked *Switch Back to Home Server* within Enterprise Manager, the user will be prompted to switch the client's connection back to the main server.

Operational Notes for IPTalk Redirect

- SCR 40560 - Occasionally, MaxAgent will not automatically restart and reconnect when the main LAN is lost for a few minutes.
- SCR 40559 - Under heavy load (4000 per hour), when you redirect IPTalk, you will see a message "Server is not available currently."
- SCR 40515 - IP extension status displays conflict in Enterprise\User after redirection.
- SCR 40820 - The IP phone redirect feature and the #27 global relocation feature are mutually exclusive. If the IP phone redirect feature is enabled, then the #27 global relocation feature cannot be enabled, and vice versa. If both features are enabled from a previous version, the redirect feature will be disabled automatically after this patch is installed.

Polycom Enhancements

There are two primary enhancements to Polycom phone handling; these changes are summarized here. Refer to the most recent *Polycom IP Phone Configuration Guide* for full details. You can find this guide in the AltiGen Knowledgebase at https://know.altigen.com.

Polycom Phone Firmware and BootROM Requirements

Polycom Series	Models	MaxCS Version	Firmware
VVX	300, 310, 400, 410, 500, 600	Release 7.5.0.502	4.1.6.4835
VVX	300, 310, 400, 410, 500, 600	Release 7.5 Patch 1	5.2.2.0501
SoundPoint	IP 335, 550, 560, 650, 670	All	4.0.4.2906 (BootROM 5.0.4.x, 5.0.5.x, or later)
SoundStation	IP 6000, 7000		4.0.4.x

Polycom Global Extension Relocation

Users can now relocate their Polycom phones within the Enterprise domain.

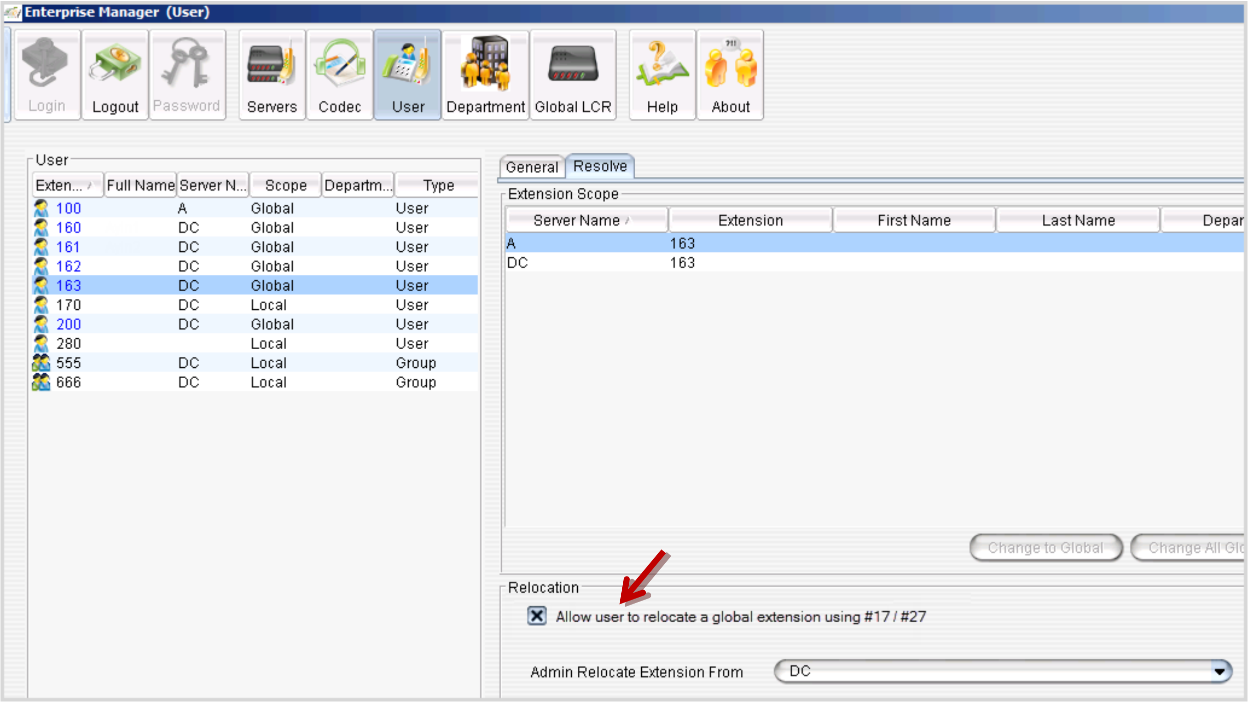
Note: If you have enabled the *IP Phone Redirect* feature, the *Polycom Global Relocation* feature will be disabled. You can implement one of these features, but not both.

Requirements

In order to use this feature, your environment must meet the following requirements:

- There must be a third-party IP Device license applied to the extension.
- A Polycom Advanced Features license must be assigned to the extension.
- A Polycom Advanced Features license is required on the server to which the extension is being relocated. For example, assume active global extension 200 is on server A. A Polycom phone on server B enters #17, and then enters extension number 200 and the password. When the server B extension is activated, MaxCS automatically checks for a Polycom Advanced license. If no Polycom Advanced license is available on server B, then this relocation request would fail.

To enable this feature, a checkbox on the Enterprise Manager > **User** > **Resolve** tab has been renamed to *Allow user to relocate a global extension using #17/#27*.



To relocate the phone, users follow these steps:

1. Connect the phone.
2. Enter the extension number and the voicemail password.

Operational Notes

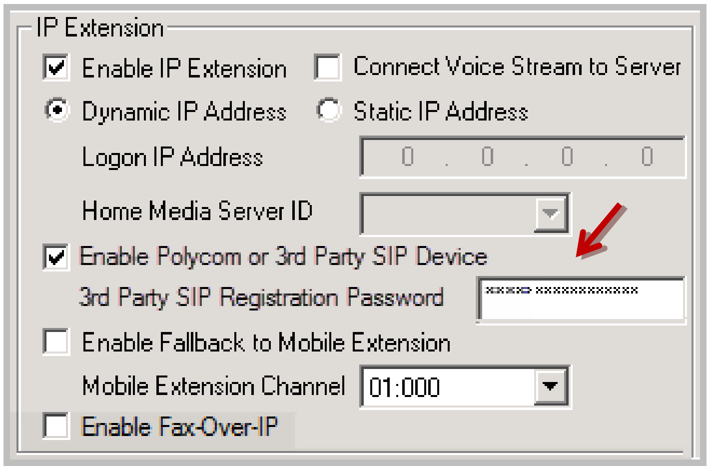
- After upgrading to 7.5 Patch 1, press the speaker and/or pick up the handset, and then press #17. Enter an extension number and its voicemail password to bind that Polycom phone to that extension number.

Polycom Password Consolidation

To simplify Polycom phone management, AltiGen has merged the various passwords in MaxCS into a single password. Specifically, the provisioning password, the voicemail password, and the SIP Registration have been combined into a single password, which is set to the voicemail password.

This has resulted in changes to two options on the *Extension Configuration* page, found on the *General* tab. Both renamed options are in the *IP Extension* group:

- *Enable Polycom or 3rd Party SIP Device*
- *3rd Party SIP Registration Password*



Important: After the upgrade to 7.5 Patch 1 has been completed, some Polycom users may need to press the Speaker button or pick up the handset and press #17 to log into their extensions, entering their voicemail password.

Polycom Secondary Proxy Support

You can now assign a secondary proxy server that Polycom phones will connect to when the main MaxCS server becomes unavailable. On this proxy server, some limited inbound and outbound calls can be performed; only SIP/UDP is supported. When the main MaxCS server is back up, the phones will automatically reconnect to the main server, restoring all functionality.

The supported emergency gateways are AudioCodes MP11x and MultiTech MVP 410. For the MVP, only emergency dialing is supported and outbound DTMF is not supported. For configuration details, refer to those configuration guides in the AltiGen Knowledgebase.

To set a proxy server for an extension, for times when the main server is unavailable,

1. In MaxCS, select **PBX** > **AltiGen IP Phone Configuration**.
2. Switch to the **Polycom** tab.
3. Select the extension.
4. Check the option **Enable Secondary Proxy**.

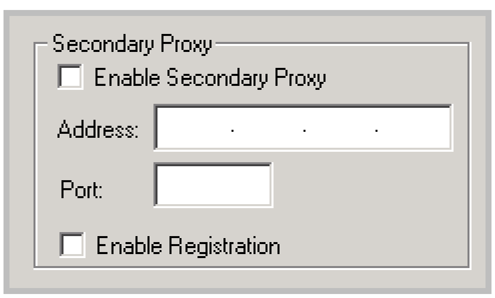


Figure 16: The Secondary Proxy options

5. For the *Address* field, enter the emergency gateway's IP address and port number.
6. You can enable SIP Registration to the secondary proxy by checking that option. Refer to your gateway's configuration guide to determine whether to enable SIP registration.

Notes

- If the deployment supports both Polycom and AltiGen IP phones, the port number on the gateway must be 5060.
- You can enable TLS/SRTP for the extension; however, when the phone switches to the secondary proxy, it will use only SIP/UDP without encryption to avoid conflicts with the TLS certificate configuration.

  Be aware that when you enable TLS/SRTP for an extension, if the phone switches to the secondary proxy, it will use only SIP/UDP without encryption. The extension will switch back to TLS/SRTP when the phone reverts to the main proxy.
- If the user has multiple phones with the same extension number, then all of these phones will have the same secondary proxy. Because of this configuration, remote phones may not work correctly when they cannot reach the main MaxCS server.
- If you use AudioCodes MP-11x as the secondary proxy, SAS (Standalone Survivability) will be used. The MP-11x supports up to 25 registered users when SAS is enabled. To work around this limitation, disable SIP registration on additional Polycom phones. When the phone is not registered to the MP-11x, it cannot receive calls from other extensions. When a PSTN call comes in to the MP-11x, the call cannot be forwarded to a Polycom phone that is not registered to that MP-11x. However, an unregistered Polycom phone can still make PSTN calls. So the approach is to enable SIP registration ONLY on those Polycom phones that need to receive incoming calls while MaxCS is not reachable. For other SIP extensions, disable the SIP registration.

Limitations

- The secondary proxy/gateway must support digit manipulation. Polycom phones have a pre-loaded digitmap, and the number sent to the gateway from the phones starts with a trunk access code (usually this is the digit 9). The proxy/gateway will need to remove (strip out) this digit before sending the number to PSTN.
- With an AudioCodes gateway SAS, the Polycom phones with SIP registration enabled will be able to dial extension-to-extension and receive inbound calls. Polycom phones with *Enable Registration* unchecked will only be able to place outbound calls while it cannot reach the main MaxCS server.
- If a Polycom phone must support the #17 feature, disable the SIP registration option. The phone will only be able to place outbound calls while it cannot reach the main MaxCS server.

AltiGen Technical Support

AltiGen does not provide general configuration support for AudioCodes products. For general configuration information, refer to your AudioCodes documentation.

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