MAX Communication Server
Release 8.0

New Features Guide

October 6, 2015

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

Contents

About This Guide

This guide describes the enhancements that have been added since the release of MaxCS 7.5.

- **Polycom Enhancements**

  The following enhancements are summarized in this guide; refer to the *MAXCS Polycom Configuration Guide* for full details and configuration instructions.

  - **Auto-Provisioning** (page 7)
  - **Global Extension Relocation** (page 7)
  - **User Password Consolidation** (page 8)
  - **Default Local Administrator password** (page 8)
  - **Secondary Proxy** (page 8)
  - **Auto-Generate Digit Map** (page 9)
  - **Mobile Fallback** (page 9)
  - **Firmware Auto-Upgrade** – VVX models (page 9)
  - **** Global BLF** (page 9)
  - **** Polycom VVS Expansion Module Support** (page 10)
  - **** Call Recording Button** – VVX models (page 10)
  - **** Transfer and Conference enhancements** (page 10)
  - **** Corporate Directory support** (page 10)
  - **** User Directory Dialin**g – VVX models (page 10)
  - **** Client Call Control** (page 11)
  - **Video Call support** – VVX models (page 11)
  - **Auto-Answer changes** – VVX models (page 11)
  - **Feature Code #33 changes** (page 11)
  - **Additional enhancements** (page 11)

  *** Feature requires a Polycom Advanced Features license*

- **Technology Enhancements**
  - **HMCP Load Balancing** -- The HMCP system has been optimized to perform load balancing on a multi-core system, to enhance performance. See page 12.
  - **Security Enhancement** --The new Java Service Manager can connect **only to the local system**. In addition, earlier versions of the MAXCS AltiGen Java Service Manager will not be able to connect to the MaxCS 8.0 AltiGen Java Service loader. This change makes the system more secure.
  - **SIP Groups** – This feature streamlines SIP registration configuration; SIP servers are now organized within SIP *groups*. You can include up to four SIP servers in each SIP group, and can prioritize their use within the group. See page 12 for details.
  - **Callback from Queue** – You can now offer callers the choice of receiving a return call instead of remaining in the call queue. This customizable feature lets you control various thresholds that can trigger the callback offer. For example, you can offer the callback option only to callers whose wait times exceed a set number of minutes. Or you can offer the callback option only to callers who are beyond a certain position in the call queue. See page 21 for details.
  - **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 35 for details.

- **Expanded 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 36 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 36 for a brief summary; refer to the configuration guide for your AudioCodes model 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 and connectivity to AudioCodes gateways. This feature is briefly described on page 39. 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 39 for details.
- **SIP Delayed Offer Support** – MaxCS now supports SIP Delay Offer on incoming SIP calls.

Requirements

This section lists the operating system requirements for the various types of MAXCS deployments.

Requirements: New Installations

This MAXCS 8.0 release supports Softswitch, hardware chassis, and MAXCS Private Cloud. The following operating systems are supported:

Max1000

- Windows 7 32-bit SP1

Max2000

- Windows 7 32-bit SP1
- Windows 2008 32-bit SP2

Office 3G/2G

- Windows 2008 32-bit SP2

The following Windows operation systems are supported for All-in-One Softswitch:

- Windows 8.1 Professional 64-bit (supported on Hyper-V version 6.0 and VMware ESX 5.5 and 6.0)
- Windows 7 Professional 64-bit SP1
- Windows Server 2008 R2 64-bit SP1
- Windows 2012 Server R2 64-bit (supported on VMware ESX 5.5 and 6.0)

MAXCS 8.0 uses internal network port 10072 to work with the client applications. Other applications on the users' system should not use this port. Since this is for internal use, no firewall setting should be configured for this port.

Requirements: Upgrades from Earlier Releases

If you are upgrading to MaxCS Release 8.0 from an earlier release of MaxCS, see the *MaxCS 8.0 Upgrade Guide* for system requirements and upgrade procedures. You can find this guide in the AltiGen Knowledgebase at https://know.altigen.com.

Polycom Enhancements in Release 8.0

This section provides an overview of the enhancements for Polycom IP Phone integration that have been added since the initial release of version 7.5. For full details and configuration instructions, refer to the *Polycom Configuration Guide*. You can find this guide in the AltiGen Knowledgebase at https://know.altigen.com.

Polycom Auto-Provisioning

This feature was added in Release 8.0.

In MaxCS 8.0, the process of provisioning Polycom IP phones has been significantly streamlined.

Administrators can now configure an option in the DHCP (Dynamic Host Configuration Protocol) server. The DHCP service, in conjunction with the AltiGen Polycom phone configuration service, will deploy configurations to Polycom phones automatically.

Polycom phones are preconfigured to use DHCP to receive an IP address and use DHCP Option (160) and then Option 66 to determine the location of a provisioning server.

AltiGen uses DHCP to configure the Polycom phones' "Provisioning Server Type" as "HTTP" and the "Provisioning Server Name" as the AltiGen Polycom phone configuration service IP or Hostname.

If a Polycom phone is used in a non-supported environment, then the Administrator is responsible for setting up a local provisioning server. In this case, the Administrator should configure the provisioning server's type and IP (Hostname) manually.

Refer to the *MAXCS Polycom Configuration Guide* for full instructions.

Polycom Global Extension Relocation

This feature was added in MaxCS 7.5 Patch 1.

Users can now relocate their Polycom phones within the Enterprise domain by using #17.

Requirements

- A Third-party IP Device license must be assigned 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 Features* 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*.

After upgrading to Release 8.0, the user must pick up the handset and then press #17. Then they must the extension number and voicemail password to bind that Polycom phone to that extension number.

Refer to the *MAXCS Polycom Configuration Guide* for full instructions.

Polycom User Password Consolidation

This feature was added in MaxCS 7.5 Patch 1.

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*

After the upgrade to Release 8.0 has been completed, some Polycom users may need to pick up the handset and press #17 to log into their extensions, entering their voicemail password.

Refer to the *MAXCS Polycom Configuration Guide* for full instructions.

Polycom Default Local Administrator Password

This feature was added in MaxCS Release 8.0.

You can change the default Polycom administrator password (which is currently 456) via a new field on the **System** > **Number Plan** tab. This is the password for the Polycom phone itself; users must enter this password to access menus on the phone to change its configuration.

In addition, you can enable a Polycom phone so that it downloads this default password; select **PBX** > **AltiGen IP Phone Configuration**, select the extension, and switch to the *Polycom* tab. Check the *Enable Password Control* option; the password from the **System** > **Number** tab will be copied over.

Refer to the *MAXCS Polycom Configuration Guide* for full instructions.

Polycom Secondary Proxy Support

This feature was added in MaxCS 7.5 Patch 1.

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. You can select which extensions will register to the survivable gateway.

The supported emergency gateways are the following devices:

- AudioCodes MP11x
- MultiTech MVP 410 – (for this device, only emergency dialing is supported and outbound DTMF is not supported)

For details on configuring the gateways, refer to the appropriate configuration guide in the AltiGen Knowledgebase.

Polycom Auto-Generate Digit Map

This feature was added in Release 8.0.

You can now have MaxCS Administrator automatically generate a digit map, which will be based upon your current dialing plan. You do this via a button on the **System** > **System Configuration** > **Number** tab.

We recommend that you review the auto-generated digit map, to make sure that it meets your system requirements. Modify the map as needed.

After you make any change to the system dial plan, click the **Generate Polycom Digit Map** button and a new digit map will be created base on the current dialing plan. The new Digit Map will overwrite the previous version.

Polycom phones must be rebooted in order to receive the updated configuration.

Refer to the *MAXCS Polycom Configuration Guide* for full instructions.

Polycom Mobile Fallback

This feature was added in Release 8.0.

You can now enable mobile fallback on Polycom phones, just as you can with AltiGen IP Phones. When enabled for an extension, if a Polycom phone loses its network connection, MAXCS will automatically fall back to a Mobile Extension for this extension.

To enable this for an extension, open the **PBX** > **Extension Configuration** > **General** tab, check the *Enable Fallback to Mobile Extension* option, and specify the appropriate mobile extension channel from the list.

Refer to the *MAXCS Polycom Configuration Guide* for full instructions.

Polycom Firmware Auto-Upgrade

This feature was added in Release 8.0.

MaxCS now supports an automatic firmware upgrade on the following Polycom VVX phones:

- VVX 300/310
- VVX 400/410
- VVX 500
- VVX 600

The Auto-upgrade feature is not supported on VVX 1500 model phones.

There are two separate options that you can use to upgrade VVX firmware. One is for new phones that you have recently acquired and are starting to configure (it can also be used on existing phones that are not associated with an extension on this server, such as when an extension number is changed). The other option is for existing phones that are already associated with an extension.

Refer to the *MAXCS Polycom Configuration Guide* for full instructions.

Polycom Global BLF

This feature was added in Release 8.0.

You can now set a Global extension as a BLF softkey for Polycom phones, just as you can with AltiGen IP phones.

This feature requires a *Polycom Advanced Features* license.

Polycom VVX Expansion Module Support

This feature was added in Release 8.0.

MaxCS now supports the Polycom VVX Expansion Module, which is a third-party device that is sold by Polycom to work with their model VVX IP phones. The Expansion model is supported on the following Polycom phones:

- VVX 300/310
- VVX 400/410
- VVX 500
- VVX 600

The BLF slots that you configure will overflow from the VVX phone onto the expansion module. In other words, the BLF slots will fill up all available slots on the Polycom phone's LCD display first, then will begin filling up the expansion module.

This feature requires a *Polycom Advanced Features* license.

Refer to the *MAXCS Polycom Configuration Guide* for details.

Polycom VVX Call Recording Button

This feature was added in Release 8.0.

You can enable a *Record* softkey for Polycom VVX models. This option is found on the **PBX** > **AltiGen IP Phone** > **Configuration** Polycom tab.

Once this feature has been enabled, the VVX extension user can tap a **Record** softkey on their Polycom phone to choose to record the call in progress. A new page opens, with a **Record** button for users to click.

This feature requires a *Polycom Advanced Features* license.

Refer to the *MAXCS Polycom Configuration Guide* for full instructions.

Polycom Transfer and Conference on MaxCS Clients

These enhancements were included in Release 8.0.

In this release, Polycom users now have additional ways to transfer calls and to join or initiate conferences, using the client applications MaxAgent, MaxOutlook, MaxCommunicator, and AltiConsole. Refer to the *MAXCS Polycom Configuration Guide* for details.

- Users must enabled the *Use Polycom Phone to make or answer calls* option in their MAXCS client in order to use this feature.
- Users must have a *Polycom Advanced Features* license in order to perform these operations.

Polycom VVX Directory Dialing

This feature was added in Release 8.0. Directory Dialing requires a MAXCS *Polycom Advanced Features* license, and is only supported on the following VVX model IP phones.

- VVX 300/310
- VVX 400/410
- VVX 500
- VVX 600

Polycom users can now choose contact from a corporate directory to place calls, transfer calls, and perform other basic functions.

A default Directory Profile, named *System,* is provided by default. It includes all extensions. You can configure additional Directory Profiles as needed.

To configure this feature, you will create corporate directories and then enable directory use for appropriate extensions.

Refer to the *MAXCS Polycom Configuration Guide* for full instructions.

Polycom Client Call Control

This feature was added in Release 8.0.

The MaxCS Clients are now synchronized with Polycom phones; regardless whether you used the client or the Polycom phone to place a call on hold, you can retrieve the call from either the client or the phone.

Polycom-to-Polycom Video Call Support

This feature was added in Release 8.0.

MAXCS supports video calls on Polycom IP phones for Softswitch deployments. Video calls are not supported on Max1000 or Office systems.

Supported devices include:

- VVX500 and VVX600 (these models require a separate Polycom VVX USB camera)
- VVX1500 (this model has a built-in camera)

Considerations:

- Video conferences are not supported; only direct peer-to-peer calls are supported.
- Video calls are supported in Softswitch Deployments only.

Refer to the *MAXCS Polycom Configuration Guide* for configuration instructions.

Polycom Device Auto-Answer Changes

In previous releases, agents with Polycom VVX phones could both enable the Auto-Answer feature as well as set the default voice path (speaker or handset) in a single setting the client's **Configuration** > **Extension** page.

Due to the specific way that Polycom handles voice paths, AltiGen has changed how users configure this feature. Configuration now requires two separate steps.

To enable or disable the client Auto-Answer feature, users still open the MaxAgent *Configuration* page. The choices now are **Enable** and **Disable**. (The choice in earlier releases was *Speaker* or *Headset*).

This feature requires an *Advanced Features license*.

Refer to the *MAXCS Polycom Configuration Guide* for full instructions.

Polycom #33 Do Not Disturb Feature Profile

When you clear Call Management feature #33 – do not disturb (in **System Configuration** > **Feature Profiles**), both the DND button and the DND softkey will be disabled in Polycom phones that have been assigned to that profile. However, users will still see the disabled DND softkey until the phone is rebooted.

Similarly, when you *enable* feature #33, some Polycom models will enable the DND button right away; other models may need to be rebooted before the change will take effect.

Polycom Miscellaneous Updates

The Caller ID will now show correctly while the call is ringing; in the previous release, the Caller ID updated only after the call connected.

Polycom Known Issues and Considerations

For a list of known issues, refer to the *Polycom Configuration Guide*.

Technology Enhancements in Release 8.0

This section describes new features included in this release.

HMCP Load Balancing

This feature was added in MaxCS 8.0.

The HMCP system has been enhanced to perform load balancing on a multi-core system, in a round-robin method. This results in a more even distribution of work across all channels, resulting in performance that is more consistent.

Security Enhancement

This feature was added in MaxCS 8.0.

A security enhancement has been added for the AltiGen Java Service Loader.

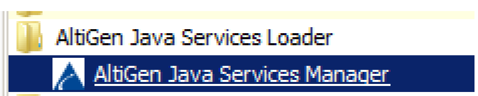


Figure 1: AltiGen Java Services Manager

Prior to Release 8.0, you could use AltiGen Java Service Manager to connect a remote machine's Java Service Loader with the default password, if the remote server's administrator had not changed the password.

In MaxCS 8.0, however, the new Java Service Manager can connect **only to the local system**. In addition, earlier versions of the MAXCS AltiGen Java Service Manager will not be able to connect to the MaxCS 8.0 AltiGen Java Service loader.

This change will prevent you from running Java Service Loader Manager from a LAN or WAN connection. The only way to access Java Service Loader Manager now will be from the server itself, via Remote Desktop.

SIP Group Configuration

This feature was added in MaxCS 8.0.

In previous releases of MaxCS, SIP registration was configured by individual channels. This configuration approach had several disadvantages. For example, configuring multiple channels with the same authentication credentials was inefficient. Setting multiple channels to register to the same server and having to configure only one of them with a registration period required configuring that channel twice. Moreover, for some scenarios, such as configuring an AltiGen SIP Trunk fax server, one trunk had to be reserved for fax even if faxes were seldom sent or received.

Some benefits of the new approach:

- The number of SIP trunk channels is now configurable, as opposed to the license-based model in earlier releases.
- SIP trunk configuration is accessed through single entry point “SIP Group Configuration” screen as opposed through SIP Profile and multiple entry points in the previous release. This design improves usability for SIP trunk provisioning.
- Each SIP Trunk group may be configured with one or more SIP servers, and the server’s status is displayed. When at least one SIP server’s status is up, this SIP Trunk Group is considered active.

  The priority of the SIP server is from top to bottom. For example, when two SIP servers are configured in a group, MaxCS sets up SIP calls with the first SIP server if its status is up. Otherwise, if the second server is up then MaxCS will set up the calls with second SIP server instead.
- The configuration for SIP.US SIP trunk can now be achieved by configuring a single SIP Trunk Group with two servers, gw1.sip.us and gw2.sip.us where gw1 is used as primary server and gw2 as backup server.
- The Register tab in SIP Group Configuration displays SIP Registration parameters for the highlighted SIP Server entry. One SIP Registration session is established for each SIP server. This registration status defines the SIP server up/down status. When all the servers in a group are down, all the SIP trunk channels associated with this SIP trunk group are considered inactive.

  This design eliminates the problem in the previous release where when the SIP registration to a server failed, only those channels with SIP registration enabled are down but other channels connect to the same server are still active.
- Allows a SIP server in multiple SIP groups – In the case where the system connects to a SIP carrier through multiple SIP trunks, the administrator may configure this carrier’s SIP server in multiple SIP Groups, and each SIP Server entry has the same domain, IP address but different User Name.

  This configuration should be used for outbound call ONLY as Out Call Routing may select the trunk channels associated with a particular SIP trunk group. Inbound calls, in this case, are routed in a first-available fashion to all of the SIP trunk channels of these SIP Groups that have this SIP server address configured.

  Settings and SIP OPTION parameters are re-organized and supported for each SIP Server entry.

  Best effort configuration conversion is performed when MAXCS is upgraded from a previous release. The administrator should verify the SIP Group and SIP Trunk channel assignment after upgrading.

To streamline SIP registration, AltiGen has implemented SIP Group configuration. The following three panels in the earlier releases have been consolidated:

- The SIP Trunk Configuration dialog box
- The Trunk Group Configuration dialog box
- The SIP Trunk Profile dialog box

In addition, the Trunk Configuration dialog box has been updated to show the SIP Trunk group, in the *Type* column.

The SIP Signaling Channel Configuration dialog box is the main starting point for all SIP channel configuration. (Double-click a **SIPSP** board in *Boards* view and then click **Board Configuration** to reach this panel.)

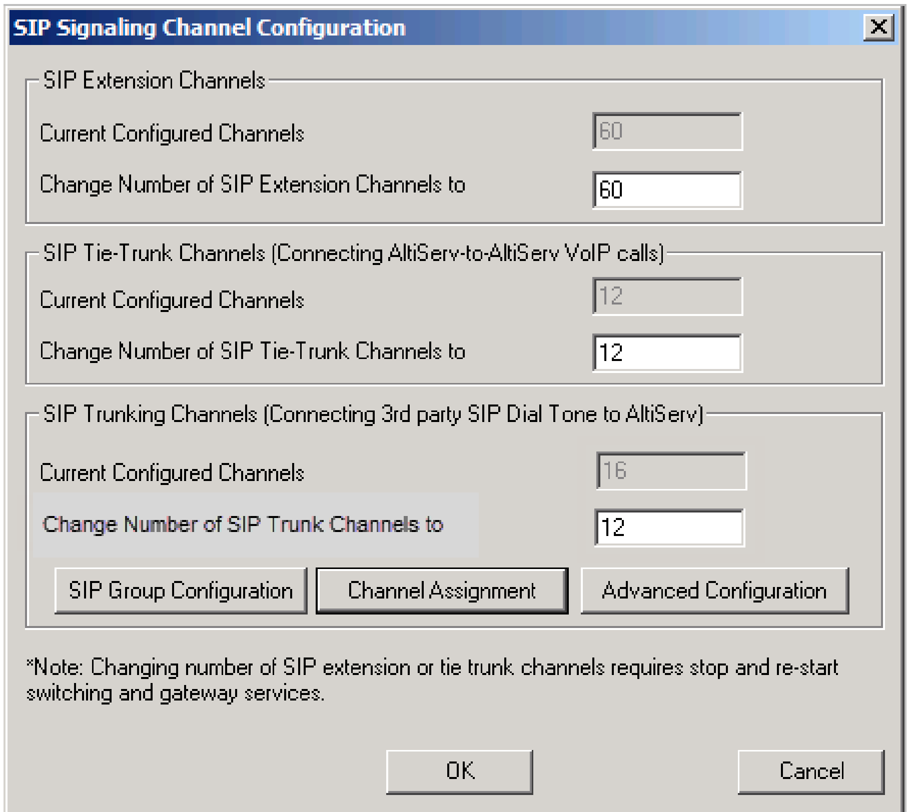


Figure 2: The new buttons on the updated SIP Signaling Channel Configuration panel

Two of the buttons in the earlier releases have been replaced with two new buttons:

- **SIP Group Configuration** – This is where you now configure SIP Groups, adding SIP servers and configuring various options for each server.
- **Channel Assignment** – This is where you now enable and disable channels, and move channels from one SIP group to another.

In the SIP Signaling Channel Configuration panel, you can do the following:

- Create new SIP groups
- Add servers to SIP groups (and remove servers from SIP groups)
- Change the relative priority of servers in a SIP group
- Configure various registration and SIP Options for a server

Create a New SIP Group

To create a new SIP Group,

1. Double-click a **SIPSP** board in *Boards* view and then click **Board Configuration** > **SIP Group Configuration**.
2. Below the *Groups* list, click **Add**.

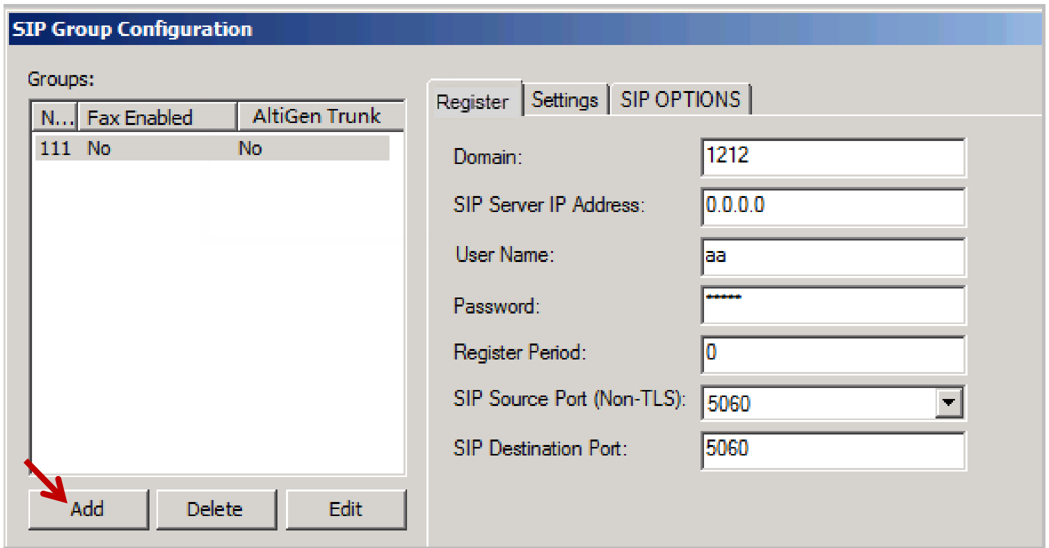


Figure 3: Click Add to creating a new SIP Group

3. Provide a name for the group and indicate whether this is an AltiGen SIP Trunk.

   Note: Release 8.0 includes license checking for AltiGen SIP trunks. Be aware that trunks will show as not registered if you start MAXCS Administrator before MAXCS is fully up, because license information will not be ready until then. However, after 30 to 90 seconds, the trunk should be show as ready.

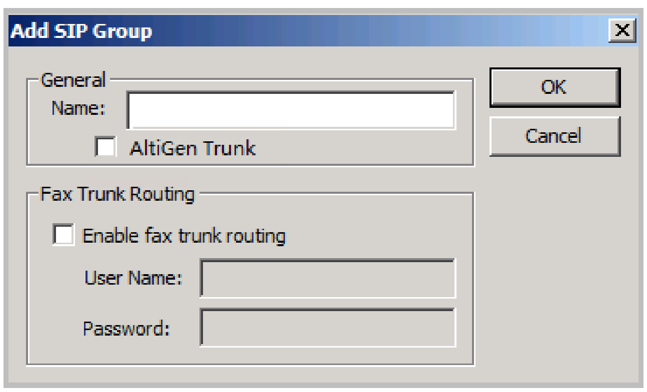


Figure 4: The parameters for the new SIP Group

4. If appropriate, select **Enable fax trunk routing** and provide the fax user name and fax password. These fields are for use only with AltiGen SIP Trunks.

Add SIP Servers to a SIP Group

You can add up to four servers to each SIP group. To add a SIP server to a SIP group,

1. Double-click a **SIPSP** board in *Boards* view and then click **Board Configuration** > **SIP Group Configuration**.
2. Select the appropriate SIP group in the *Groups* list.
3. Below the *SIP Servers* list, click **Add**.

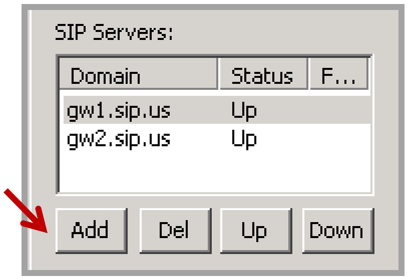


Figure 5: Click Add to add SIP servers to a SIP Group

4. Enter the Domain name.
5. (Optional) If you want to copy the settings from another server, choose the group and the server from those two pulldown menus.

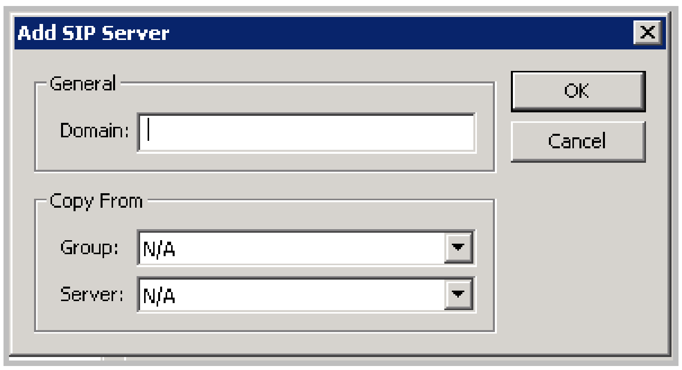


Figure 6: The parameters for the SIP Server

Note: Click **Refresh** to retrieve the latest registration status.

To remove a server from a SIP group,

1. Double-click a **SIPSP** board in *Boards* view and then click **Board Configuration**.
2. Select the appropriate SIP group in the *Groups* list.
3. Select the server that you want to remove from the SIP group.
4. Click **Del** (Delete).

Change the Order of SIP Servers in a SIP Group

The order of the servers in the Servers list determines how the servers are accessed. The first server is always used; when that server is not available, the next server in the list is used, and so on.

To change the priority order of servers within a group,

1. Double-click a **SIPSP** board in *Boards* view and then click **Board Configuration**.
2. Select the appropriate SIP group in the *Groups* list.
3. In the Servers list, select the server to move, and then click **Up** or **Down** as appropriate.

Configure SIP Server Registration Parameters

The *Register* tab contains all registration-related settings for a SIP server. All of the settings on the SIP Trunk Configuration dialog box from earlier releases of MaxCS are found on this tab.

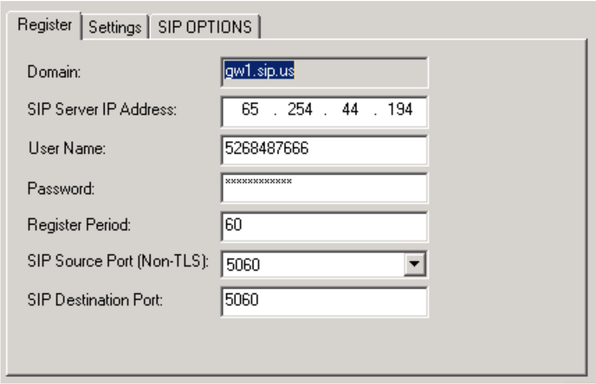


Figure 7: The SIP Server registration parameters

The lone exception is the *Enable Channel* option, which is now handled in the *Channel Assignment* panel.

Note: SIP Server registration status depends upon both the registration results and the SIP OPTIONS results. If either of those two processes fails, the server's status will be set to DOWN. SIP Groups and member channels share the same registration status. As long as at least one SIP server is UP, all of the enabled member channels will show as status Idle.

Configure General SIP Server Parameters

The *Settings* tab contains the parameters from the SIP Trunk Profile tab in earlier releases of MaxCS.

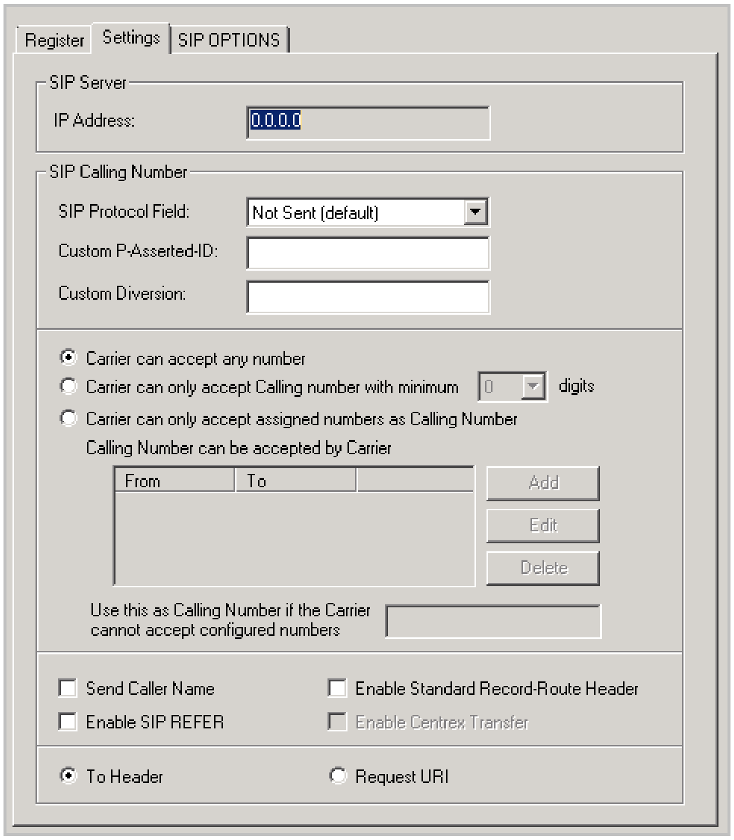


Figure 8: The SIP Server general parameters

Configure Server SIP Options

The SIP OPTIONS tab includes the SIP OPTIONS parameters from the previous release of MaxCS. The SIP Server Name parameter is essentially the new Domain field.

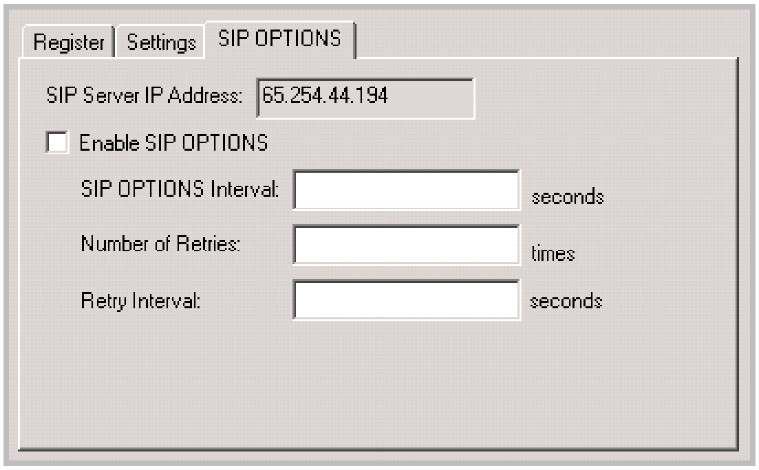


Figure 9: The SIP Server SIP Options

Enable or Disable Channels

To view a list of channels and determine the SIP Group to which each channel belongs,

1. Double-click a **SIPSP** board in *Boards* view and then click **Board Configuration**.
2. Click **Channel Assignment**.

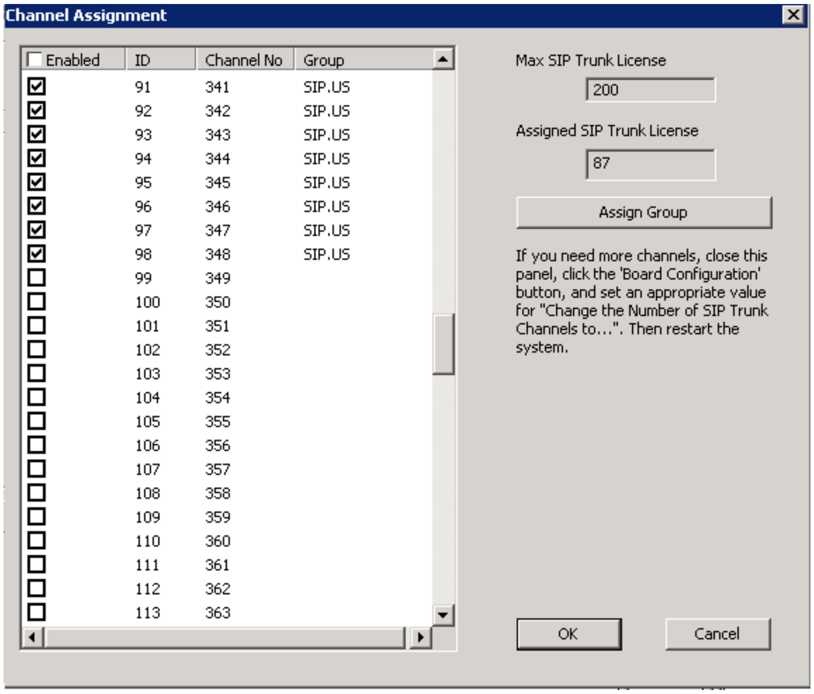


Figure 10: Channel Assignment view

A checkbox indicates whether a channel is currently enabled.

To disable a channel, clear its checkbox. To enable a channel, check its checkbox. To enable or disable all channels, check or clear the checkbox in the column heading at the top of the list.

If you discover that you need to add more channels, close this panel, click the **Board Configuration**, and set an appropriate value for the *Change Number of SIP Trunk Channels to*… option (see Figure 2). Then restart the system.

Assign Channels to a SIP Group

To assign a channel to a SIP Group, or reassign it to a different SIP Group,

1. Double-click a **SIPSP** board in *Boards* view and then click **Board Configuration**.
2. Click **Channel Assignment**.
3. Select one or more channels in the list. Use **Ctrl-Click** to select multiple channels.

4. Click **Assign Group**.

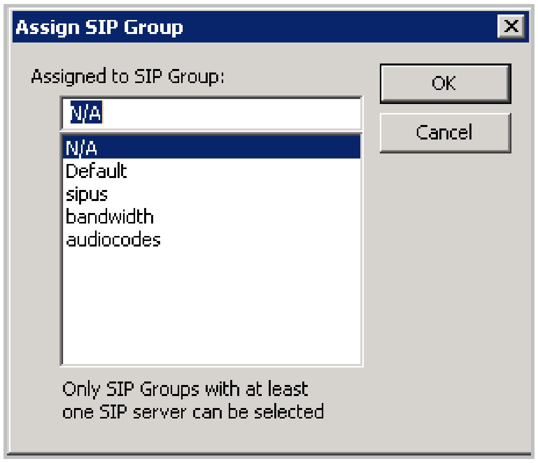


Figure 11: The list of available SIP Groups

5. Choose a SIP Group from the list and click **OK**.

Considerations:

- A channel is not enabled if it is not assigned to any SIP group.
- If you assign a disabled channel to a SIP group, doing so does not automatically enable it – you must manually enable the channel (see the previous section).
- In order to assign channels to a SIP group, the SIP group must have at least one SIP Server assigned to it.
- If you remove all SIP Servers from a SIP Group, all channels previously assigned to that SIP group automatically will show as 'Not Ready.'

Trunk View Enhancements

As a result of adding SIP Groups to MaxCS, the *Type* column in Trunk view will now shows each SIP Trunk's group name (if it is part of a group).

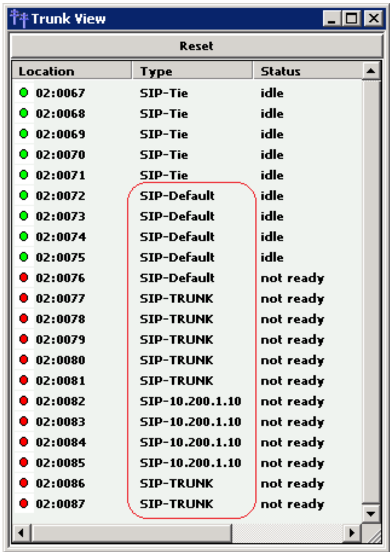


Figure 12: Trunk View, showing the Group names

Trunk Configuration Enhancements

The Trunk Configuration dialog box now shows the SIP trunk's Group information in the *Type* column.

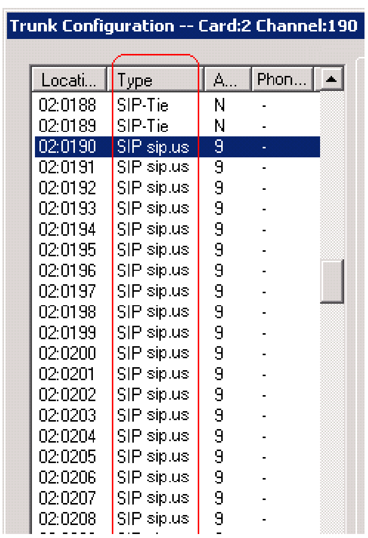


Figure 13: The Trunk Configuration panel, showing the Group name

Callback from Queue

This feature was added in MaxCS Release 8.0.

A new feature enables organizations to offer callers the option of receiving a return call instead of waiting on hold in a call queue.

You can customize the specific queue conditions under which a caller is offered the callback option. For example, you can specify that only calls with an anticipated wait time of longer than 25 minutes should be offered the callback option. You could also specify that only calls that have at least 9 calls ahead of them should be offered the callback option.

You can also indicate a daily cutoff time for callbacks, so that returned calls can be completed before that workgroup's business day ends.

For return calls, you can specify how many attempted calls to place, how long to wait between those attempted return calls, and a caller ID to transmit with the returned calls.

The Caller's Perspective

Once you enable and configure the Callback options, callers who reach the threshold for receiving a return call hear various prompts. For example:

> "All of our representatives are busy. Rather than remain on hold, you can press 3 to receive a return call.
>
> The wait time for your return call will be approximately <xx> minutes. Press 1 to set up a return call. Press 2 to remain on hold.
>
> Please say your name. When you have finished speaking, press the # key.
>
> Your name was recorded as <caller name>. To re-record, press 1, or to continue, press the # key.
>
> You will be called at <incoming phone number>. Press 1 to confirm this number, or press 2 to be called at a different phone number.
>
> Please enter the 10-digit phone number. When you have finished, press the # key.
>
> You will be called at <phone number> in approximately <xx> minutes. Thank you. Goodbye."

Callers who receive a return call hear various phrases and prompts before they are connected. Following is an example of a successful return call:

> "Hello, this is a call back from <company name>. We are returning a call from <caller name>. If we have reached <caller name>, please press 1. To decline this call, press 3.
>
> One moment while we connect you with a representative."

An unsuccessful call back can be the result of a timeout or a declined call. Following is an example of a call that timed out, with no response from the other party:

> "Hello, this is a return call that was requested by <caller name>. If this is you, please press 1. To decline this call, press 3.
>
> We are sorry that we are unable to reach <caller name>. We will try again later. Goodbye."

Processing Logic

When Callback from Queue is enabled and configured, callers will be offered the option of a return call if the call meets all of the following conditions:

- The call is in a workgroup queue and it is not a callback call.
- The workgroup is using Advanced Queue Management and has the Callback feature enabled and configured.
- The estimated callback time is within the business hours boundary that you have configured for the target workgroup (from page 26).
- Either or both of the following conditions must be met:

- The call's expected wait time is longer than the value that you have set for the *Expected Wait Time is longer than xx minutes* option.
- The call's position in the queue is greater than the value you have set for the *Queue position is greater than xx* option.

Here is an overview of how Expected Wait-time (EWT) is calculated, to help you understand the Callback feature:

- if total calls(incalls + outcalls) < 10, EWT(expected wait time) = 2.
- if available agent number (not in DND, ready and not in error) = 0, EWT = 2.
- total talk time = incalls talk time + outcalls talk time
- EWT = ((total talk time * 1.05)/(total calls *available agent number) * in queue position + 59)/60
- if EWT > 240, EWT = 240.

Callback Licenses

In order to implement the Callback feature, you must have sufficient Callback licenses.

- AltiGen offers both Callback Seat licenses and Callback Session licenses.
- If you have purchased both Callback seat licenses and Callback session licenses, when an agent logs in, the seat license will be used if one has been assigned to that user. If no seat license has been assigned to that user, then one session license will be used.
- In order to log into a workgroup that has been set as a Callback target workgroup, the agent must either have a seat license or must be using an available session license. If no session licenses are available, then the agent will not be able to log into that workgroup and will see an error message.
- One seat license can apply to multiple workgroups that are enabled for the Callback feature. In other words, if a user belongs to two workgroups that are Callback enabled, the user only needs a single Callback license. The user does not need one for each workgroup.

Step 1: Assign Licenses and Record Phrases

This feature is a workgroup *Advanced Queue Management* enhancement.

1. Acquire the appropriate number of seat and/or session licenses, and assign any seat licenses to the appropriate agents.
2. Record the Callback Announcement and the Callback Phrase. Update any other phrases as needed.

Step 2: Configure the Workgroups that will handle the Callback Calls

First, perform these steps on the workgroup that will be handling the return (callback) calls. Keep in mind that the workgroup offering the callback option and the workgroup that will handle the return calls must be on the same server.

1. Select **Call Center** > **Workgroup Configuration**.
2. Select which workgroup will handle callback calls.
3. On the **Call Handling** tab, select the option **Enable Callback Call Handling**. Configure the parameters for the return calls.

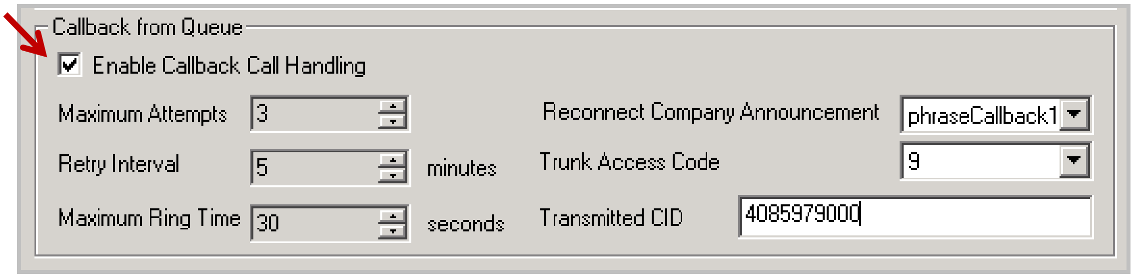


Figure 14: The Callback parameters for the responding Workgroup

Workgroup Parameter	Description
Maximum Attempts	The number of times the system will attempt another call if the initial return call fails, including the initial callback. Enter a number between 1 and 10; the default value is 3.
Retry Interval	The interval between two return call attempts. Enter a number between 1 and 10; the default interval is 5 minutes.
Maximum Ring Time	The number of seconds that the callback call should ring before dropping the call.
Callback Phrase	The phrase that will be played at the beginning of the return call, to identify the organization that is calling. A default, generic phrase is provided for you; if you like, you can record a custom phrase that includes your company name. Following is an example of this phrase: “Hello, this is a return call that was requested by <caller name>. If this is <caller name>, please press 1. To decline this call, press 3.”
Trunk Access Code	The trunk access code, including the outcall routing access code, which will be used when placing the return call.
Transmitted CID	The Caller ID that will be provided when placing the return call. This phone number is also logged in the Target Number field of the callback attempt CDR records.

4. We recommend that you set the Callback Workgroup to a higher priority if that workgroup’s agents also handle other workgroups at the same time. To do this, on the **Call Handling tab,** and increase the value of the *Inter Workgroup Call Distribution* parameter.

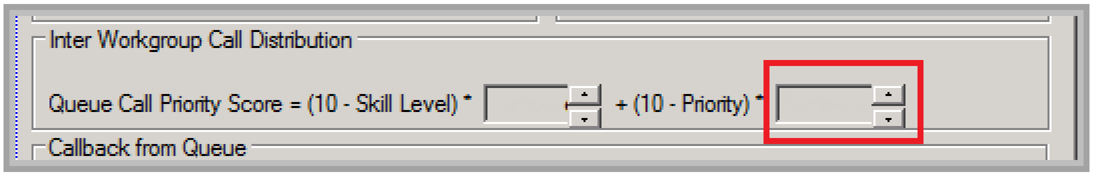


Figure 15: Inter-Workgroup Call Distribution options

Step 3: Configure the Workgroups that will Offer the Callback Option

Next, perform these steps for the workgroups that will be offering the Callback option.

1. Select **Call Center** > **Workgroup Configuration**.

2. Switch to the **Queue Management** tab.

3. Select the workgroup that will be offering the callback option.

4. In the *Queue Control* group, select **Advanced and** click **Setup.** Note: If your system has numerous extensions, there may be a slight delay while opening the Advanced Queue Management panel.

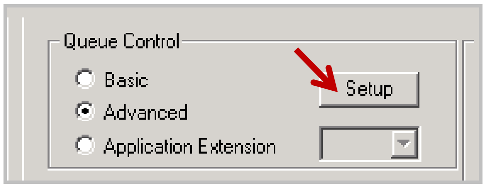


Figure 16: The Queue Control options

5. On the *Announcement* tab, select **Queue position**, **Expected Wait Time**, or both.

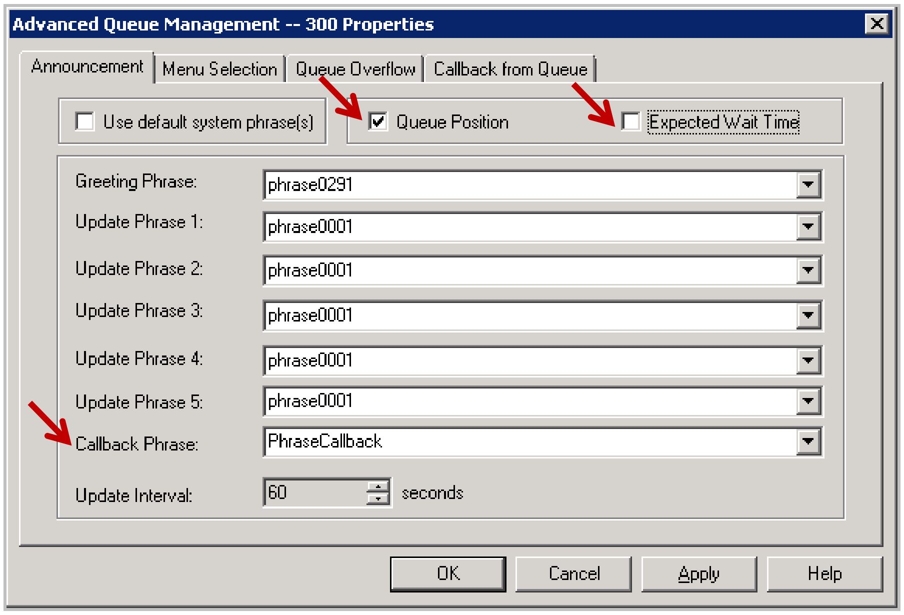


Figure 17: The Callback options in the Advanced Queue Management tab

6. Select the phrase for the *Callback Phrase* entry. This phrase will be played after each queue update phrase for those calls that meet the callback criteria.

7. On the *Menu Selection* tab, add the action “Callback from Queue” to whichever key you have told callers to press. Note: If you do not specify an Action here, the Callback feature will not be enabled.

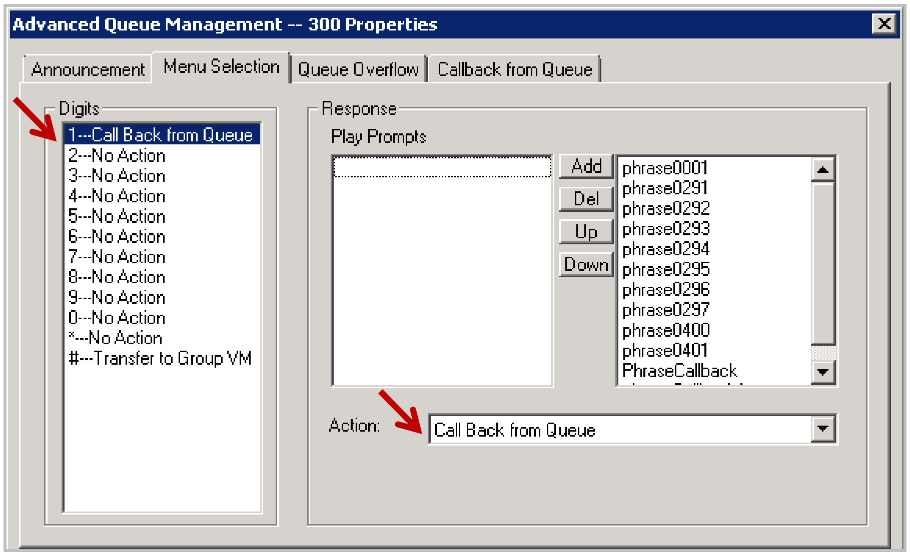


Figure 18: The Callback from Queue action on the Menu Selection tab

8. On the *Callback from Queue* tab, specify the following parameters:

Callback from Queue Parameter	Description
Enable Callback from Queue when	To enable callback, you must choose at least one of the two options. If you check both options, then both conditions must be met for the caller to be offered the callback choice: • **Queue position greater than xx** – Calls that have a queue position higher than the value you specify will be offered the callback option. Enter a value between 1 and 1,000. The default value is 10. • **Expected Wait Time longer than xx minutes** – Calls with an expected wait time that is greater than the value you specify will be offered the callback option. Enter a value between 1 and 1,000. The default value is 20 minutes.
Target Workgroup	Specify the workgroup that will be handling the return calls (you desig-nated a workgroup as a target workgroup on page 23). You can select *any* workgroup that has the Callback feature enabled; we recommend that you allocate a single workgroup to handle all callback calls, to simplify reporting of incoming and Callback calls.
Offer callback option only when the callback time is at least xx minutes before the end of the Target Workgroup’s business hours.	If this option is enabled, then the callback option will not be offered to callers if the return call would be within xxx minutes of the Target Workgroup’s end of business hours. For example, suppose that you set this value to 20 minutes. If the return call is calculated to be placed at 4:45pm, and the Target Workgroup’s business day ends at 5:00pm, then the caller will not be offered the

Callback from Queue Parameter	Description
	callback option. This is because you have specified a minimum 20-minute buffer, but the return call would be placed 15 minutes before the end of the workday.

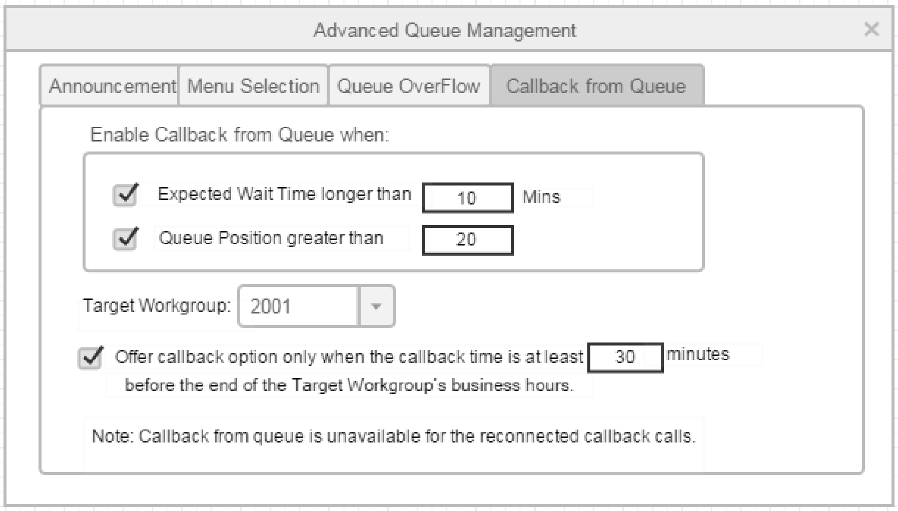


Figure 19: The parameters on the Callback from Queue tab

Blocking Area Codes from Callback

You can create a list of area codes that you want to block from return calls.

1. In the Call Restriction section of the Workgroup Configuration, General tab, select **Block Callback Numbers by Area Code**, and then click **Blocked List**. (This option may not be available unless you have enabled that workgroup for callback handling.)

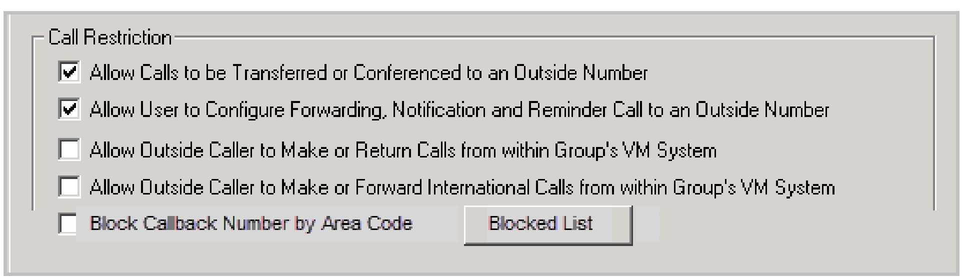


Figure 20: The block option for callbacks

   Most North American dial plan long distance area codes are prepopulated. Be sure to check the validity and completeness of this list, as new area codes are added periodically.

2. Click **Add** and enter the area code that you wish to block. Click **OK**. To remove an area code from the blocked list, select it and click **Remove**. Note that there is a default list of blocked area codes. The list includes the area codes for international calls.

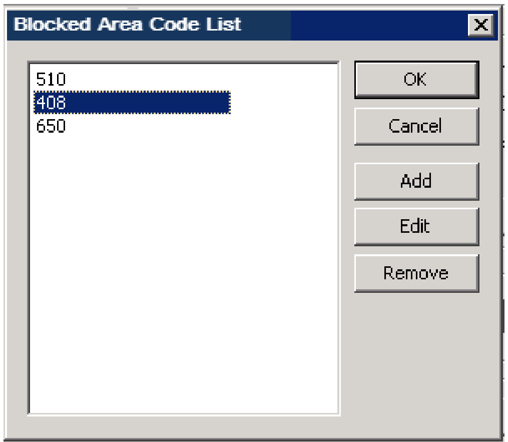


Figure 21: The Blocked Area Code list

Operational Notes

- Return calls to US Domestic and toll-free numbers are allowed
- Return calls to International and 900 numbers are not supported
- Return calls must be directed to a *different* workgroup that has been enabled to handle Callback calls. You cannot direct calls to the same workgroup.
- In some cases, the announcements may begin playing before the party answers the return call. The announcements will repeat, so that the person hears them.
- In a scenario such as an internal IT help desk, employees will be calling in, and requesting return calls, from their extensions. If these employees are calling in from other systems, then Enterprise Manager must be set up and employee extensions must be global extensions on the system offering the return call.
- If the MaxCS server reboots after a return call is scheduled, the return call will not be placed.
- The workgroup offering the callback option and the workgroup that will handle the return calls must be on the same server.
- If a return call is requested by an extension on the same MaxCS system and that extension is a virtual extension, then the callback request will be deleted and no call attempts will be made.
- When a return call is placed and the party accepts the call, the party cannot request a second callback option.
- If an extension with *Multiple Call Waiting* enabled is connected to call while waiting on callback, the extension will not receive the return call until the extension is in *Idle* state.
- It is the responsibility of the workgroup supervisor/administrator to make sure that the callback workgroup has enough agents available to serve the call at the callback time. If no agents are available, then the return call could potentially go directly to the workgroup's voicemail (depending upon the workgroup's call handling settings).
- If your system has many extensions, there may be a slight delay while opening the Advanced Queue Management panel.
- When you enable callback, the Busy Call Handling, No Answer Call Handling, Forward all calls and Group RNA Handling options will be disabled. Busy call handling option is set to *Queue*. The other options are set

to the Workgroup VM. The Queue management *Overflow Forwarding* and *Quit Queue* options can only set the target to workgroup VM. The Queue management page's queue control can only be set to *Basic*.

- If a callback call is directed to a virtual extension in the same MAXCS system, and the user logs out and back in again, then the callback request will be deleted – no further callback attempts will be made.
- The Callback feature is not supported over SIP-Tie trunks. For SIP-Tie trunks, the extension must be a global extension or extension forwarding must be setup correctly. For PSTN numbers over SIP-Tie trunks, outcall routing must be set up correctly. The PSTN callback call will follow outcall routing rules, and it may not use a SIP-Tie Trunk for callback calls.

Callback Data in CDRs

Callback data has been added to CDRs.

1. Call in WG1 then callback from WG2
    - WG1
        - Counted as 1 in the field "Callback requests" under Overflow Calls
        - Counted as an "Inbound call" and "Queued calls"
    - WG2
        - Callback calls that are re-connected with the correct caller are counted as an "Inbound call"
        - Connected callback calls that re-entered the queue then were abandoned, redirected or over-flowed are counted as 1 WG "Abandoned/Redirect/Overflow calls" respectively
        - Callback calls that failed when all attempts failed due to RNA, busy, reject, or error are counted as 1 "Callback Failed"
2. Number of workgroup outbound calls – does not count callback calls
3. Real time calls in queue – does not include in-progress callback calls
4. Call queue time definition; callback into a different WG
    A. Original WG inbound call – Queue time before hanging up
    B. Callback WG - Queue time after the call re-enters a queue
5. Call wait time definition – Queue time + Ring time (callback time is excluded)
6. Workgroup queue time definition – Use Call Queue time for workgroup queue time calculation
7. Workgroup service level – Includes inbound call wait time in the calculation
8. Each callback attempt should log a CDR record
9. Each callback re-connected queue call should have one WG CDR record
10. In each callback call's CDR record, Caller is the customer and Target is the workgroup TX caller id. If no TX caller id, it shows the main number.
11. CDR database changes
    - Main Table changes:
        - No workgroup number if the callback attempt failed
        - Callback SessionID – The same as the Callback SessionID in the callback table

- Callback Type – Request/Attempt

- New Callback Table:
  - Callback Attempt CDR SessionID – This is the link to the main CDR
  - Type – Request/Attempt
  - Start Date
  - Start Time
  - Original Caller Id – Attempt only
  - Original Caller Name – Attempt only
  - Callback Number – Request only
  - Position In Queue when leaving the queue – Request only
  - Callback Time – Request only
  - Callback Request WG
  - Callback Target WG
  - Callback Session ID (same as the Request call CDR Session ID)
  - Callback Attempt ID – attempt only
  - Callback Exit Status – Success/ Denial/No Answer/Busy/Error – attempt only

Callback Data in MaxAgent

The Callback from Queue feature adds additional data to the various displays in MaxAgent.

When the callback call comes into the new workgroup, if it enters the workgroup queue the *Type* will display as *Callback*.

MaxAgent - WG Queue

Three new columns have been added to the WG Queue list:

- Original Caller ID – The original call's caller ID.
- Original Caller Name – The original caller's name
- Original Group – The original workgroup where customer chose the callback option.

By default, these columns are hidden. Agents can display them display them by right clicking the column heading.

For callback calls, the data for each column is either from the original call or from the current call:

- Queue Time – Current call
- Pri Queue Time –Current call
- Caller ID – Current call
- Caller Name – Current call
- DNIS – Original call
- Priority – Carry forward from the Original call and then escalate / de-escalate based upon the target workgroup's rules
- SKLR -- Carry forward from the original call and then escalate/de-escalate based upon the target workgroup's rules

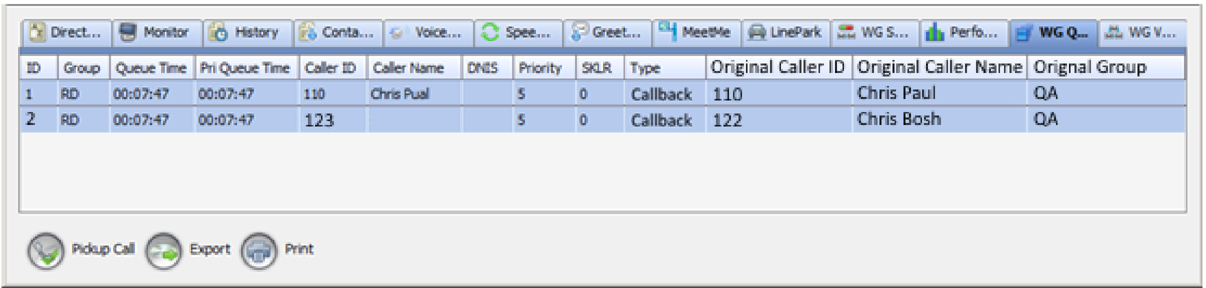


Figure 22: MaxAgent, Workgroup Queue view

MaxAgent - Call View

Four columns are added in Call List view, including:

- Type – "Normal" for a normal call or "Callback" for a callback call
- Original Number – The original caller ID
- Original Name – The original caller name
- Original Group – The original workgroup where the caller opted for a return call.

These columns are hidden by default; agents can display hidden columns by right clicking on any column header.

For a call back call, the value for each column should be:

- Record – Current call
- State – Current call
- Name – Current call
- Number – Current call
- Group – Current call
- DNIS – Original call
- Duration – Current call
- Conference – Current call
- User Data – Original call
- IVR Data – Original call

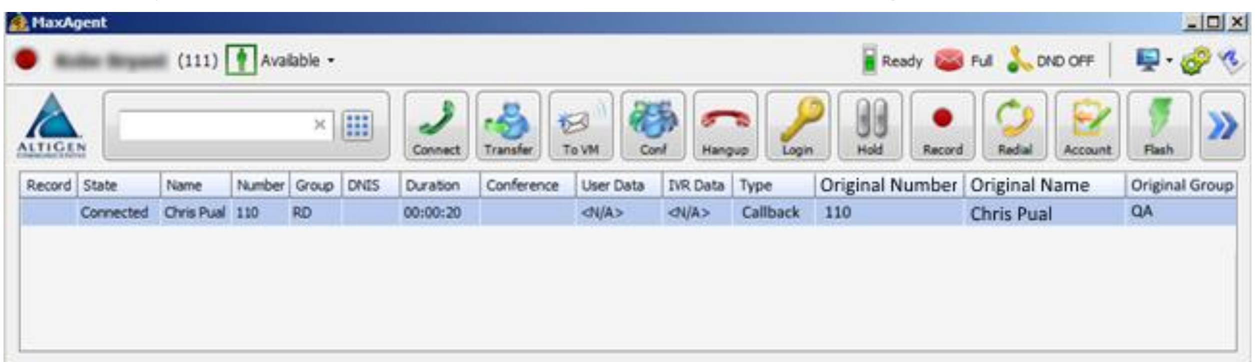


Figure 23: MaxAgent, Call List view

Callback Data in MaxSupervisor

When the callback call comes into the new WG, if it enters the WG Queue, it will display as "Callback."

MaxSupervisor - Workgroup Queue

Three new columns have been added to the Workgroup Queue view:

- Original Caller ID – Original caller ID
- Original Caller Name – Original caller name
- Original WG – Original workgroup where customer issue callback request

These columns are hidden by default; agents can display hidden columns by right clicking on any column header.

For a callback call, the value for each column should be:

- WG – Current call
- Queue Time – Current call
- PQT – Current call
- Caller ID – Current call
- Caller Name – Current call
- DNIS – Original call
- Priority – Original call
- SKLR – Original call

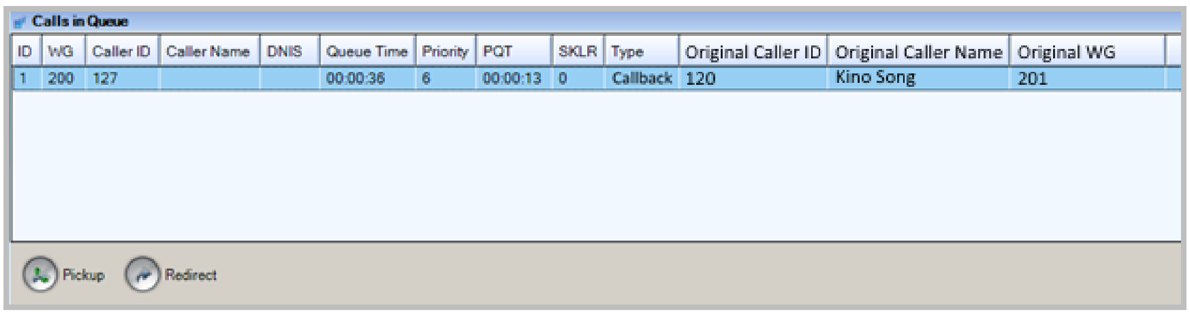


Figure 24: MaxSupervisor, Call List view

Four columns have been added to the Call List view:

- Type – "Normal" for a normal call or "Callback" for a callback call
- Original Number – The original caller ID
- Original Name – The original caller name
- Original Group – The original workgroup where the caller opted for a return call.

These columns are hidden by default; agents can display hidden columns by right clicking on any column header.

For a call back call, the value for each column should be:

- WG – Current call
- Rec – Current call
- Caller Name – Current call
- Caller ID – Current call
- Talk Time – Current call
- DNIS – Original call
- IVR Data – Original call
- User Data – Original call

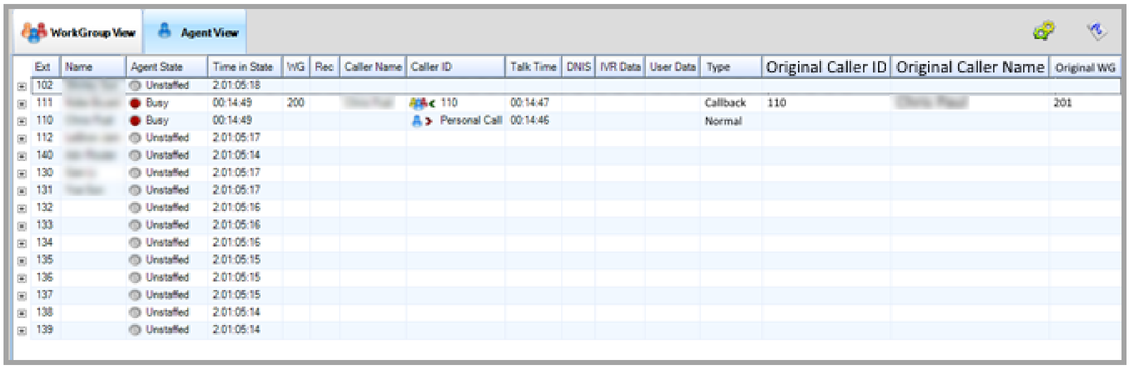


Figure 25: MaxSupervisor, Workgroup view

MaxSupervisor - Group Statistics

Several fields have been added to the Group Statistics table. These fields will appear when the workgroup is enabled for Callback call handling.

- Within Inbound Call Statistics Since Midnight, within Total Inbound Calls, Calls Overflowed/Redirected, are two statistics: Callback Requests and Others.
- A new section, Total Callback Calls Since Midnight, offers two statistics: Callback Connected and Callback Failed.

Group Statistics

InBound Call Statistic Since Midnight		%
Calls without Queueing	7	70.0 %
Calls in Queue	3	30.0 %
Total Inbound Calls	10	
Calls Answered	5	50.0 %
Calls Overflowed/Redirected	0	0.0 %
- Callback Requests	0	0.0 %
- Others	0	0.0 %
Calls Abandoned	5	50.0 %
- Abandoned in Queue	2	20.0 %
- Abandoned during Ring	3	30.0 %
- Abandoned to Voice Mail	0	0.0 %
* Leave Voice Mail	0	0.0 %
* Without Voice Mail	0	0.0 %
- Abandoned to App or others	0	0.0 %
Service Level		
SLT-Service Level Threshold (seconds)	120	
Calls Answered within SLT	5	
Service Level %	80 %	
All Calls with wait time less than SLT	3	
Wait Time and Talk Time		
Average Wait Time for Answered Calls	00:00:02	
Average Wait Time for Abandoned Calls	00:08:10	
Average Talk Time	00:25:54	
Maximum Calls in Queue	1	
Longest Queue Time	00:27:01	
OutBound Call Statistic Since Midnight		
Total Connected Outbound Calls	0	
Average Talk Time	00:00:00	
Total Callback Calls Since Midnight		
Callback Connected	0	
Callback Failed	0	

Figure 26: MaxSupervisor, Group Statistics view

Callback Data in CDR Search

Callback data has been added within CDR Search.

- Under CDR and Group CDR Search, a Callback Type column has been added.
  - Normal calls will show as blank
  - Request callback calls will show *Request*
  - Callback attempts will show as *Attempt*
- Under Statistics, details similar to those within MaxSupervisor Group Statistics have been added:
  - Total Callback Calls will show callbacks that connected versus callbacks that failed.
  - Total Calls Overflowed/Redirected will show callback requests versus other requests.

Callback Data in AltiReport

Callback data has been added to AltiReport:

- In reports 2206 and 2207, Workgroup Inbound Call Wait Time Summary and Handling Time Summary, under Overflow/Redirected Calls, the data is divided into “Callback Requests” and “Others” fields.
- There is a new Callback Detail Report. This report shows details for callback requests, callback failed attempts, and re-connected callback calls. You can group by date or show a summary.

Call Back detail report																
Report date:		Sort By: WG														
Sort By: WG		Futher sort By: Call Back Success,					Group by Date									
WG																
CallBack SessionID	Type	SessionID	CallBack Attempt ID	Start Date	Start Time	Caller Name	Caller Number	CallBack Number	CallBack Request WG	CallBack Target WG	Priority	Skill	Position In Queue	Queue Wait Time	CallBack Time	CallBack Exit State

Figure 27: Example, Callback Detail Report

Free Format Forwarding Support for SIP Trunk and SIP Extensions

This feature was added in MaxCS 7.5 Patch 1.

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

The string in Figure 28 indicates that the call should be forwarded to extension 2002 (for FaxFinder). Each comma inserts a one-second delay, for a total delay of three seconds. 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.

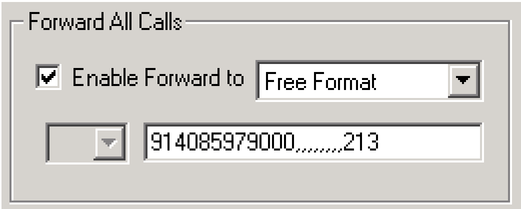


Figure 29: Example of call forwarding to a specific extension at an external phone number

In Figure 29, 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 eight 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 call setup time may require additional commas. However, too many commas will affect 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.

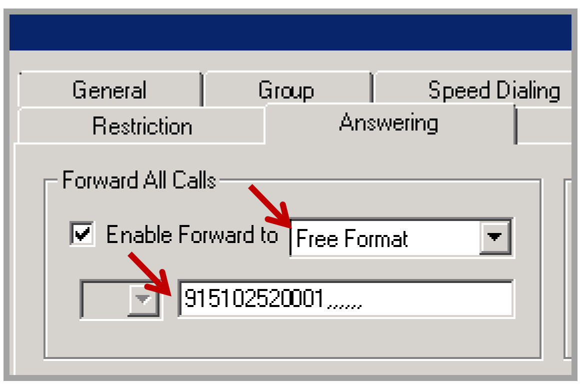


Figure 30: Example of call forwarding to an outside phone number with a long delay (for Centrex)

Expanded Caller ID Support

This feature was added in MaxCS 7.5 Patch 1.

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.

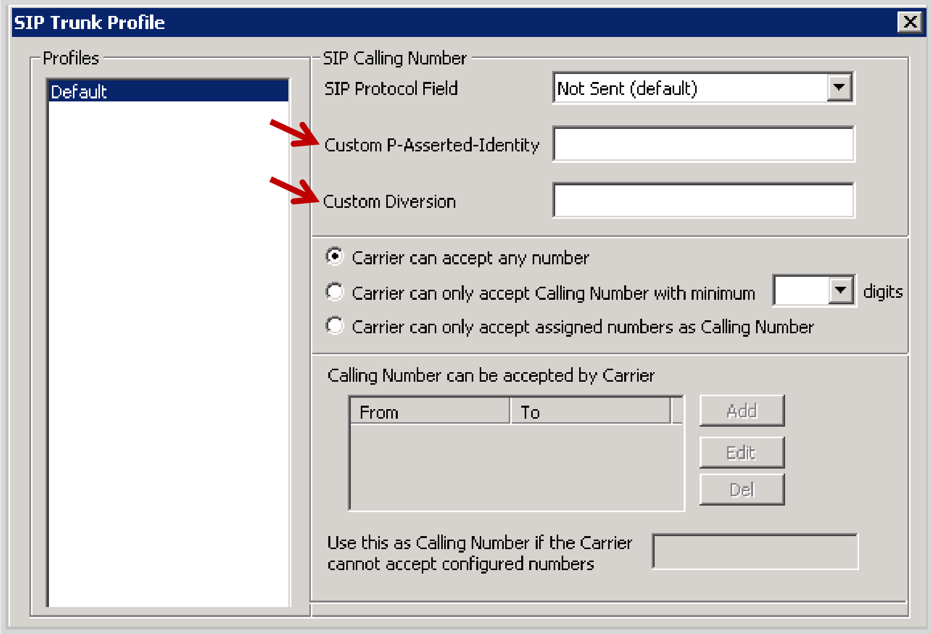


Figure 31: Two new SIP Trunk Profile parameters

- *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 was added in MaxCS 7.5 Patch 1.

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.

To reach the parameters for this feature, *Enable SIP REFER* and *Enable Centrex Transfer*, double-click **SIPSP** in Boards view, click **Board Configuration**, and click **SIP Group Configuration.** Select the appropriate SIP Group and SIP server**,** and switch to the **Settings** tab.

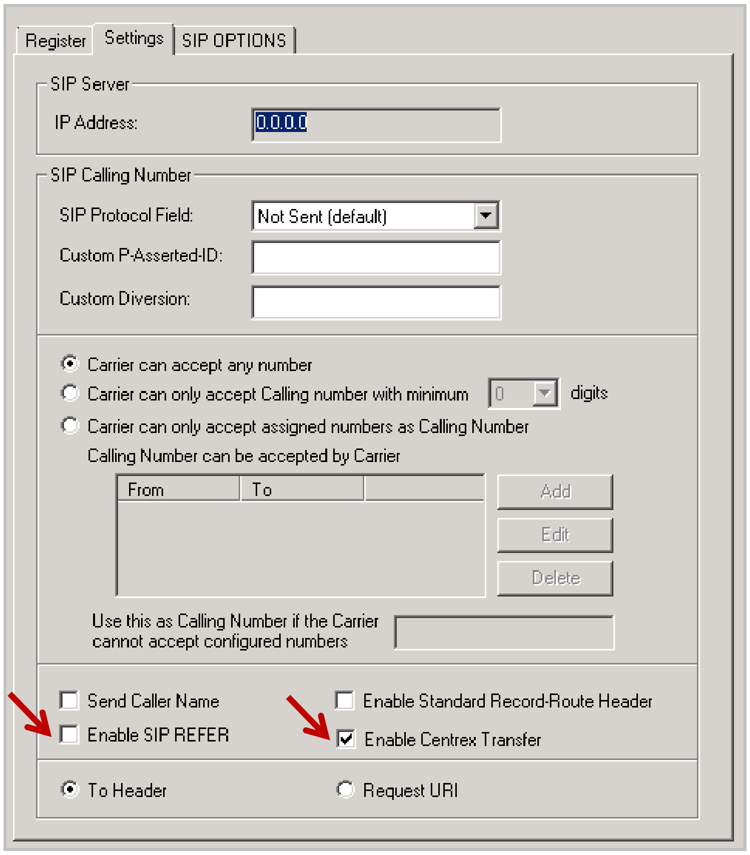


Figure 32: The "Enable SIP REFER" parameter for the SIP Trunk

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 configure the SIP Trunk, refer to the section *SIP Group Configuration* starting on page 12.

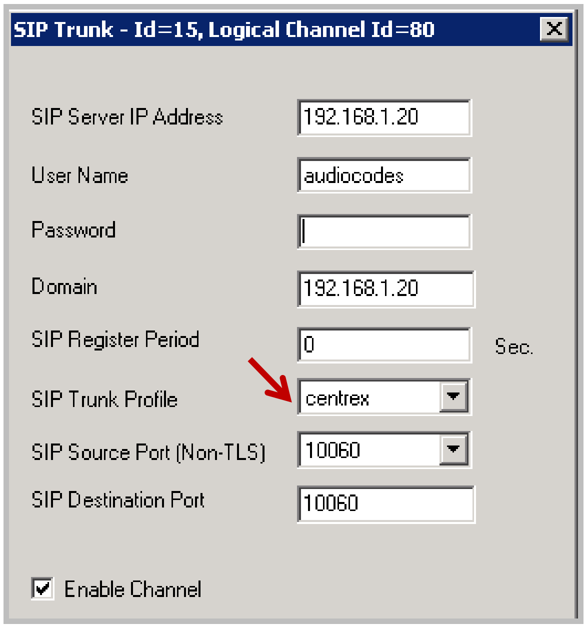


Figure 33: SIP Trunk configuration details

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.

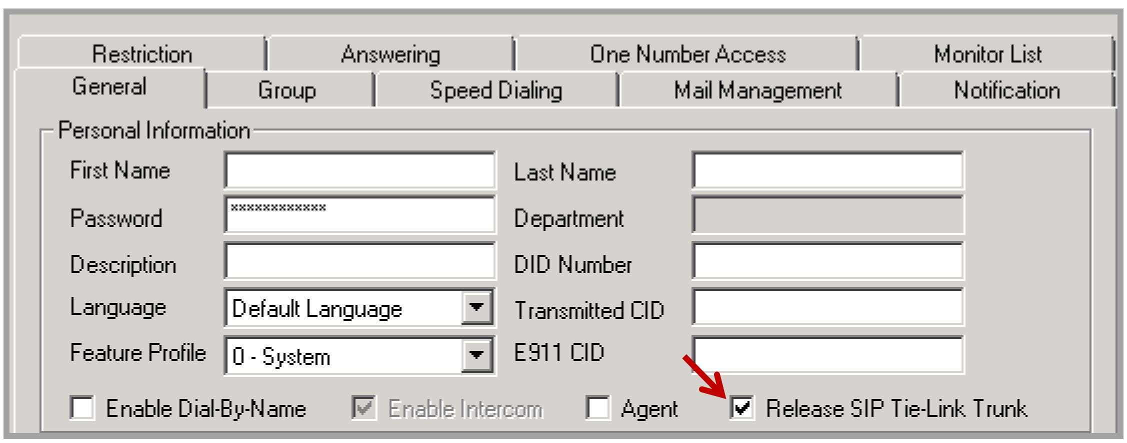


Figure 34: Check the "Release SIP Tie-Link Trunk" option

SIP Trunk TLS Support

This feature was added in MaxCS 7.5 Patch 1.

MaxCS now 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.

The following devices are supported for TLS:

- AudioCodes MP-11x

- AudioCodes Mediant 1000-B PRI / T1
- AltiGen 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 AltiGen SIP Trunks, this field should be set to port 5067.

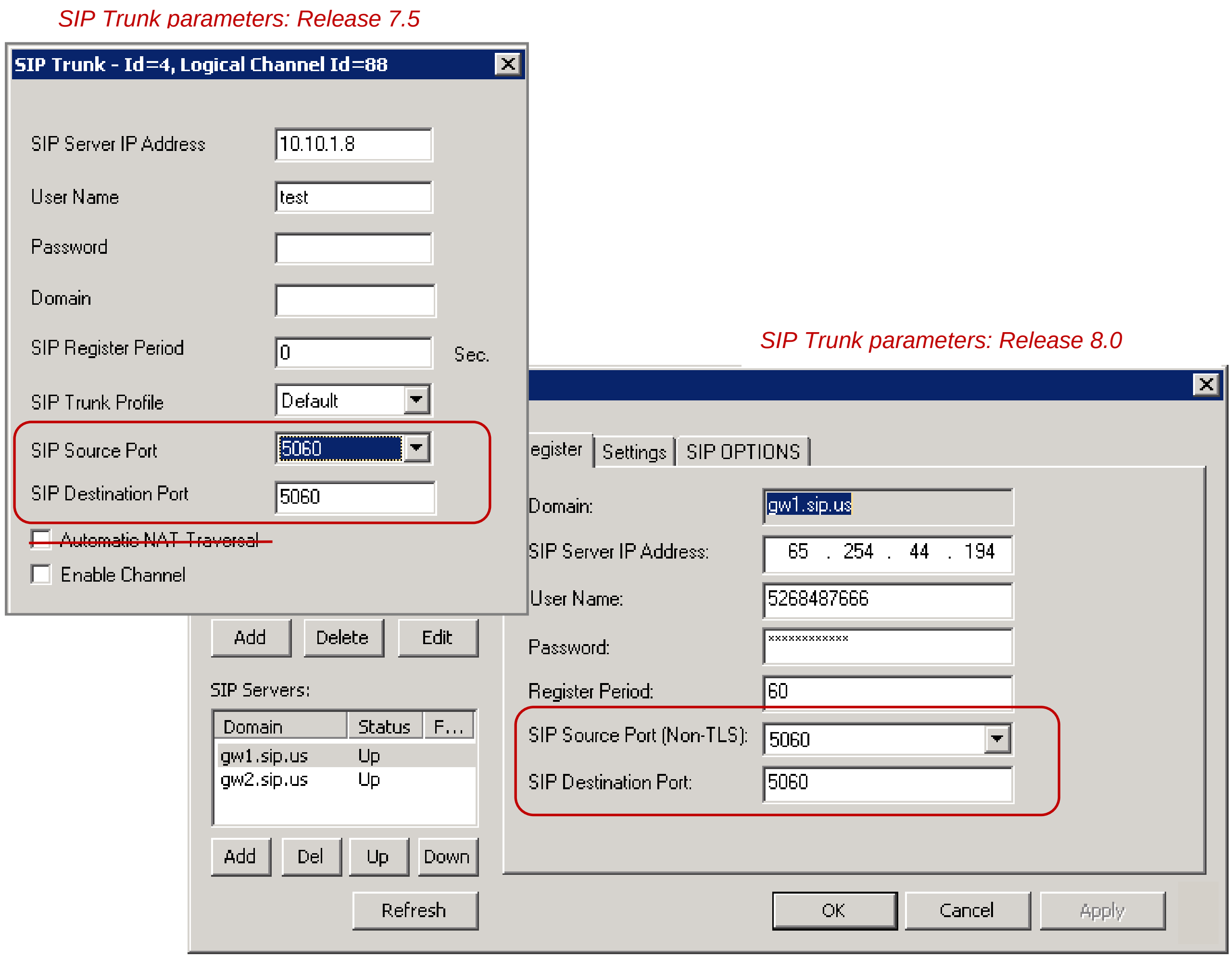
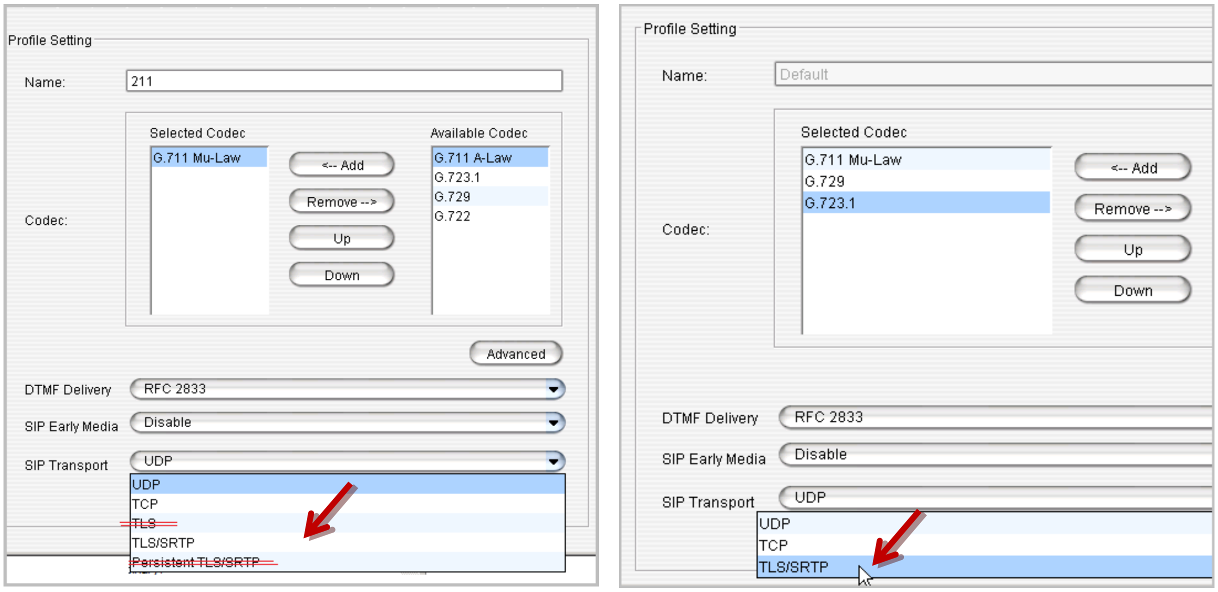


Figure 35: Changes to SIP Trunk parameters

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 8.0

Figure 36: Changes to the Codec Profile SIP Transport option

Following is a generic setup for SIP TLS; configuration may differ from one SIP trunk to another.

1. Make sure your SIP gateway or SIP trunk has TLS/SRTP enabled.
2. In MaxAdministrator, open Trunk view. Double-click a trunk and click **Trunk Properties** > **SIP Group Configuration.**
3. Add a group, for example, SIPTLSGrp, in the *Groups* panel.

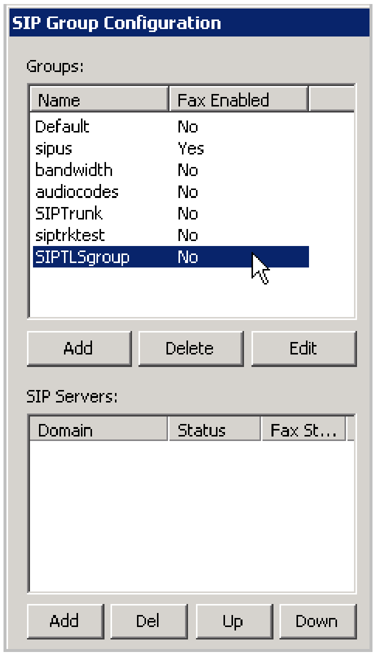


Figure 37: Add a SIP Group

4. Select the new group in the Groups panel. Below the SIP Servers list, click **Add** and add a server.
5. Select the new server in the SIP Servers list and enter the following parameters on the *Register* tab:
   - 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, enter the register period. Otherwise, enter “0”.
   - For the *SIP Destination Port*, use port **5067** for AltiGen SIP trunks. *SIP Source Port* is not used here. The SIP source port will always be 5061 if TLS/SRTP is used.
6. Save the changes.

SIP Option over TLS is not supported.

IPTalk Redirect

This feature was added in MaxCS 7.5 Patch 1.

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 to Enable the Redirect Feature

To enable the Redirect feature,

1. First, enable the Redirect feature for MaxCS. In MaxCS Administrator, select **VoIP** > **Enterprise Network Management** to open Enterprise Manager.
2. Click the *Servers* button on the Toolbar. Select the **Information** subtab.
3. Check the option *Enable Redirection to Alternate Server*.
4. For *Alternate Server*, select the server that you want to use as the alternate server. Click **Apply**.

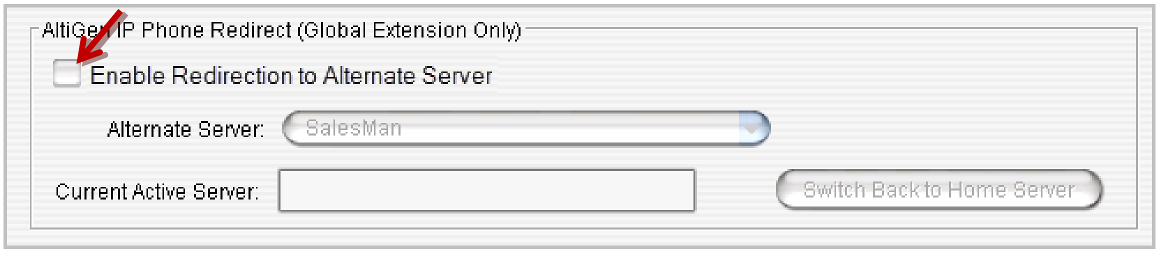


Figure 38: Enable the Redirect feature in Enterprise Manager

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

Figure 39: Enable Redirect individual users

9. 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**.

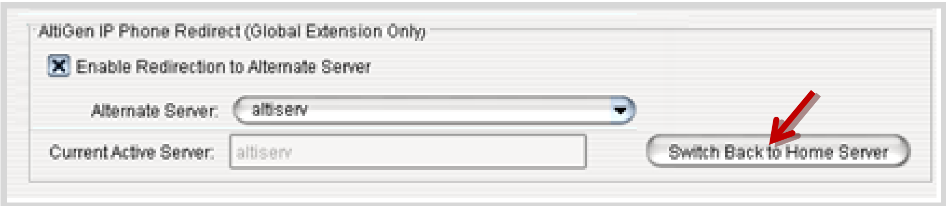


Figure 40: How to switch client applications back to the main server

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 41: 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:

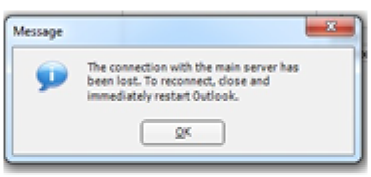


Figure 42: MaxOutlook user prompt

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

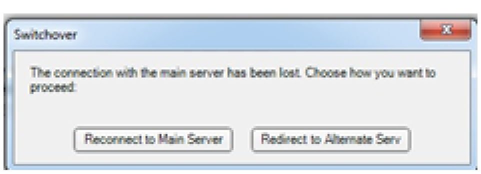


Figure 43: MaxOutlook prompt to reconnect

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.

Windows 10 Client Support

In addition to MaxCS Administrator, the following MAXCS client applications now support Windows 10:

- MaxCommunicator
- MaxAgent
- MaxOutlook
- MaxSupervisor
- MaxInsight
- AltiConsole
- CDR Search
- VR Manager client
- AltiSDK
- ActiveX Control SDK

Android OS Support

MaxCS Release 8.0 supports Android 4.4, 5.0, and 5.1.1.

Operational Limitations

If the MAXCS system has Windows Defender running on Windows 8.1, that application may affect the performance of MAXCS. If you see a performance issue on Windows 8.1, turn off the Windows Defender Real Time Protection.

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