ACM Administration Manual

MAX Communication Server
Release 9.0.1

January 2021

WARNING! Toll fraud is committed when individuals unlawfully gain access to customer telecommunication systems. This is a criminal offense. Currently, we do not know of any telecommunications system that is immune to this type of criminal activity. AltiGen® Communications, Inc. will not accept liability for any damages, including long distance charges, which result from unauthorized and/or unlawful use. Although Altigen Communications, Inc. has designed security features into its products, it is your sole responsibility to use the security features and to establish security practices within your company, including training, security awareness, and call auditing.

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

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

Altigen Communications, Inc.
670 N. McCarthy Boulevard, Suite 200
Milpitas, CA 95035 USA
Telephone: 888-Altigen (258-4436)
Fax: 408-597-9020
E-mail: info@altigen.com
Web site: www.altigen.com

Contents

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER 6

CHAPTER 7

CHAPTER 8

CHAPTER 9

CHAPTER 10

CHAPTER 11

CHAPTER 12

CHAPTER 13

CHAPTER 17

CHAPTER 18

CHAPTER 19

CHAPTER 20

CHAPTER 21

CHAPTER 22

CHAPTER 23

CHAPTER 24

CHAPTER 25

CHAPTER 26

CHAPTER 27

CHAPTER 28

CHAPTER 30

CHAPTER 31

CHAPTER 32

CHAPTER 33

About This Documentation

This manual is designed for Altigen Partners, administrators, and technicians who are responsible for configuration and administration of a MaxCS system.

Related Publications

Related MAXCS documentation can be found on the Altigen Communications web site:

http://www.altigen.com/support/:

- MAXCS Upgrade Guidelines
- MAXCS New Features Guide
- MaxCommunicator Manual
- MaxOutlook Manual
- MaxAgent Manual
- MaxSupervisor Manual
- MaxInsight Manual
- MaxMobile iPhone User Guide
- MaxMobile Android User Guide
- AltiConsole Manual
- CDR Manual
- Advanced Call Router Manual
- AltiGen IP Phone User Manuals
- ActiveX Manual
- AlitReport Manual
- VRManager Pro Manual
- Quality Management User Guide
- Polycom Configuration Guide and User Guides
- MeetMe Manual
- Service Hub Guides

CHAPTER

1

New Features

This section describes features that have been added or enhanced since MaxCS Release 8.6.0. It includes the following topics:

- *Enhancements Included in Release 9.0.1* on page 3
- *Enhancements Included in Patch 8.6.1.215* on page 4
- *Enhancements Included in Patch 8.6.1.213* on page 5
- *Enhancements Included in Release 8.6.1* on page 6
- *Enhancements Included in Release 8.6* on page 7

For a list of features going back to MaxCS Release 6.0, see the article *History of updates to Max Communication Server* in the Altigen Knowledgebase.

Enhancements Included in Release 9.0.1

The following enhancements were included in MaxCS Release 9.0.1

- **Service Hub** - A new component, Service Hub, is now included in order to support web-based client applications, including the new web-based MaxCommunicator. Refer to the separate documents; there are separate Service Hub guides for users, company administrators, and resellers.
- **TrustID Authentication** - TRUSTID is a call authentication service. When a call comes into a MaxCS system, the service analyzes, in real time, various aspects of the call to determine if the call is authentic. This feature allows your agents to spend more time helping your callers and less time verifying their identities.
- **MaxCommunicator Web Edition** - The MaxCommunicator client is now available as a web application. This client is available for deployments that are hosted in the cloud.

  This new client supports direct chat, group chat, and group/channel messaging features.

  Note that your organization can still use the Windows version of MaxCommunicator as needed.

  See the separate manual for instructions on using this web application.
- **MaxAgent IPTalk Hold Options** - Two new options are introduced in Release 9.0. These options apply to IPTalk users. Read more about these options in the *MaxAgent Manual*.
  - Workgroup queue hold - Agents can now converse with callers while callers are in a workgroup queue.
  - Double hold - Agents can put a caller on hold and the caller can put the agent on hold.
- **Call Answer Enhancements** - With MaxClient, when making outbound calls ring-back to extension is now automatically answered.

- **Click to Answer in MaxClient** - When a user of MaxClient has an incoming call, the user can click the Connect button to pick up the call. This applies to Polycom IP phones and Altigen IP phones.
- A **Configuration Option** was added to send Extension's Transmitted CID when calling Mobile Extension.
- **Adjunct SIP Trunk** - This feature can be used when MaxCS is connected to a 3rd party PBX and functions as an adjunct call center. Note that 3rd party PBX needs to be configured to accept these dialing numbers. You enable it by selecting Enable Tie Trunk option at the SIP trunk channel in the registry. Adjunct SIP Trunk allows you to do the following:
  - Send the extension number as caller ID when making a SIP trunk call
  - Allows you to do hop-off dialing through the third party PBX
  - Allows you to call an extension number from incoming SIP trunk calls
- **Disable Automatic Area Code Insertion for MaxClient** - This configuration option controls whether MaxClient inserts an area code when performing 7-digit or 8-digit dialing number auto formatting
- Calls to Voice Mail moved from Abandoned Calls to Redirected/Overflowed Calls. These changes are applied to Workgroup Statistics in MaxSupervisor and CDR Search.
- **Not Ready Reason Code With #91 Feature Code** - When Not Ready Reason Code Required is enabled, the agent can now enter #91 feature code to change to Not Ready state and enter a Not Ready reason code.
- **Busy is now added to Activity** - User can also record Busy greeting.
- The User Data field is now available in the Call Entry in MaxCommunicator and MaxOutlook.
- An UPN field is added to Extension General configuration. This field can be imported as Service Hub Login ID.
- **AltiReport Enhancements**
  - AltiReport now supports two operating modes, standalone or integrated with Service Hub. AltiReport integrated with Service Hub is available for the cloud only
  - The AltiReport configuration backup file is now encrypted.
- **SQL 2019** - Release 9.0.1 supports SQL Server 2019.
- **Windows** - Release 9.0.1 supports Windows Server 2019.

Enhancements Included in Patch 8.6.1.215

The following enhancements were included in MaxCS 8.6.1.215. Details for these new security improvements can be found in the chapter *Trunk Configuration* on page 123.

- **Enhancements for the Trusted SIP Device List**

  The following enhancements have been added to the Trusted/Malicious SIP Device List features.

  To reach this panel, double-click a SIPSP board in Boards view and then click Board Configuration. Then click the Advanced Configuration button to access the Trusted SIP Device list.

  - **Auto-Learning Options** - In the Trusted/Malicious SIP Device Lists panel, there are now three options for configuring auto-learning:
    - Disable auto-learning for all SIP devices.
    - Disable auto-learning only for third-party SIP devices. This is the default option for release 8.6.1.215.
    - Enable auto-learning for all SIP devices. This option is the least restrictive choice.
  - **New Devices with Incorrect Passwords Put in Malicious List** - When a new (non-configured) SIP device tries to register with an invalid password, that device's IP address will now be put immediately into the Malicious SIP Device List. No further SIP packets from this device will be processed.

  - **Adding IP Ranges into Trusted Device Lists** - You can now add IP ranges into the Trusted/Malicious SIP Device lists. To do this, in the IP address dialog box type in the beginning IP address and the ending IP address. You will see your entry as a range; for example, 10.0.2.120 ~ 10.0.2.125.
  - **Selecting Multiple IP Addresses in a List** - You can now select more than one IP Address in the Trusted/Malicious SIP Device lists, to move to the other list or to remove. Use Ctrl-Click to select individual IP addresses in the list. Use Shift-Click to select the beginning and ending IP addresses, to select a contiguous range.
- **Password Configuration Enhancements**
  - The following options have been moved from Extension Checker into MaxAdministrator's System Configuration > Call Restrictions tab:
    - Maximum wrong passwords allowed
    - Minimum password length
  - Extension Checker now checks the password length for both the extension password and the SIP registration password. In addition, Extension Checker now shows an additional column for the SIP registration password length.

Enhancements Included in Patch 8.6.1.213

- **MaxSupervisor Updates**
  - **Held Calls** - When an agent places a customer on hold, the agent will now show within MaxSupervisor as On Hold instead of Available. In Workgroup View (on the Agent State tab) and in Agent View, the icon changes to yellow. Note that with IPTalk, you may need to wait a few seconds to see this state change.
  - **Auto-Sort Limit** - The maximum number of unique agents allowed in MaxSupervisor before auto-sort is disabled has been in-creased from 100 to 200 unique agents.
  - **Duration for Not-Ready Reason Code** - Along with addressing the Total Not Ready Duration when an agent is not ready and takes a personal call, MaxSupervisor Agent View and Agent State View now have a “Time in Not Ready Reason” column. This column shows the current amount of time that an agent is in their current Not Ready Reason Code.
  - **Show Workgroup Name** - In MaxSupervisor Agent View, there is a new column called 'WG Name.' It will display the name of the workgroup.
- **MaxAgent Updates**
  - **Call Alerts** - When the agent has incoming call alerts turned on, those alerts will now show the phone number/extension and/or the workgroup name. This applies to IPTalk users.
  - **Clearing Call Alerts** - If there are too many stacking call queue alerts on the screen, agents can now right-click any alert to display a pop-up. The pop-up offers the agent an option to delete all queue alerts. This way, agents do not have to delete each alert individually.
  - **Auto-Answer Workgroup Calls Only** - In the client's Configuration > Extension > Call Handling page, there is now an additional “Workgroup calls only” option below the “Automatically answer after…” option. When this second option is checked, the auto-answer setting will only apply for incoming workgroup calls. Personal calls will not be automatically answered unless this option is unchecked.
  - **Change the Not Ready Reason Code** - When an agent selects a Not Ready reason code, the reason code status is now shown next to the Ready/Not Ready text. Agents can now change the specified Not Ready reason code without going back to Ready mode.
  - **Show Name/Number in Top/Bottom Mode** - When an agent has arranged the MaxAgent client view to show calls at the top or bottom, the caller name (if available), the calling number, and the workgroup name/number will now appear.

- **Apply Workgroup RNA Settings to Agents Who Reject Calls** - In earlier releases, MaxCS does not apply the workgroup's RNA rules to an agent who rejects a call, even if the workgroup has RNA Not Ready or RNA Log Out rules configured. In AltiReport, this behavior is considered as RNA. Altigen has added a registry setting for organizations that wish to apply the workgroup RNA setting to agents when they reject a call.
- **Logging in Without Being Changed to Ready Mode** - Altigen has included a registry entry that will prevent agent states from automatically changing to Ready mode when logging into workgroups.

Enhancements Included in Release 8.6.1

The following enhancements were included in MaxCS 8.6.1.

- **Callback from Queue**
  - **Reserved callbacks** - In addition to having a separate workgroup handle return calls (referred to as Redirected Callback), you can now configure workgroups that handle their own return calls (Reserved Callback).
  - **Streamlined setup** - The Callback from Queue configuration GUI has been streamlined. These changes make the feature easier to configure.
- **MaxSupervisor**
  - **Hide logged out or Unstaffed agents** - Supervisors can now hide logged-out agents and Unstaffed agents in the Agent State tab, via new options in the Configuration window.
  - **Manually set agents to Ready or Not Ready** - Supervisors can now manually set agents to Ready or Not Ready state. There is also a new Reason Code available for this action: 97 - Supervisor Override.
  - **Auto-sorting no longer disabled** - When the Agent State tab lists more than 200 agents, the Auto-sort feature will not longer be disabled. You may experience slight performance issues.
  - **New columns** - The application now includes two new columns: *Workgroup Name* and *Time in Not Ready Reason*
- **MaxAgent and MaxCommunicator**
  - In these client applications, there is a new call handling option. Under **Configuration** > **Extension** > **Call handling**, if users enable the *Automatically Answer after*… option, an additional checkbox Workgroup calls only lets users indicate whether personal calls will be automatically answered in addition to workgroup calls. If this checkbox is cleared, personal calls will automatically be answered following the same timing rule as workgroup calls.
  - Agents can now change their Not Ready Reason code as needed, by right-clicking the Not Ready icon and choosing a different reason code. If the agent changes the Not Ready Reason code, it resets the Time in Not Ready Reason duration that is displayed in MaxSupervisor.
- **VMWare** - MaxCS now supports VMWare release 6.7.
- **AltiReport -** AltiReport now bundles OpenJDK JRE instead of Oracle JRE 8 and supports Tomcat 8.5.43
- **Polycom**
  - **SoundStation** - The Polycom SoundStation 6000 conference phone now supports TLS 1.2 with firmware version 4.0.14.1580. You must update to this new firmware version, which is provided with MaxCS 8.6.1, on order to support TLS 1.2. Note that the model 7000 does not support TLS 1.2, and is still supported on firmware version 4.0.13.1445.
  - **VVX** - The Polycom VVX450 model IP phone is now supported. Polycom VVX Firmware version 5.9.3.2489 is now supported, and it is bundled with Release 8.6.1.
- **Exchange Server** - This release supports Exchange Server 2019.
- **Workgroups** - Remote access to Advanced Queue Management is now supported.

- **Headset support** - The following headsets are now supported with IPTalk.
  - Plantronics
    - USB SAVI models for wireless headsets
    - CS500 Series
    - USB Blackwire models 435, 3200/3210/3220 series, 700/710 series for corded headsets
    - Voyager 5200 UC
    - Encore Pro Plus Series with DA80
  - Logitech
    - H390 USB headset

Enhancements Included in Release 8.6

The following enhancements were included in MaxCS 8.6.

- **Polycom Firmware Upgrade Enhancements** - Unlike in earlier releases, you can now control firmware upgrades on individual VVX Polycom phones. The individual VVX extension's "Update firmware to…" setting is no longer automatically disabled. You can choose to enable or disable each VVX phone's update option. (**PBX** > **AltiGen IP Phone Configuration** on the Polycom tab).
- **Polycom VVX 201 support** - MaxCS now supports the VVX 201 model phone. This model does not support BLF or Line Park.
- **Polycom VVX Firmware** - This release supports Polycom VVX Firmware version 5.9.3.2489.
- **Backup Program Enhancements** - For better performance and to reduce the amount of disk space used by backup logs, the Backup process no longer includes Polycom log files.
- **MaxCS Client Upgrade Enhancements** - This release includes two enhancements to the MaxCS client upgrade process. Client applications only upgrade when there are compatibility issues with the previous release. And you can now upgrade client applications from an external source.
- **Trace Enhancements** - In this release, the log process has been streamlined to run more efficiently. In addition, several new traces have been added to the list of traces that you can run:
    - SIP KeepAlive SP Log
    - Polycom Phone Log
    - QESL Log
- **"Midnight" Task Scheduling Enhancements** - You can now set a custom schedule for nightly MaxCS tasks, through a registry entry. See the chapter *Tools and Applications*.
- **Exception Routing Rules** - In earlier releases, you could create holiday routing rules for full days and you could create business hours for specific days of the week and weekends. In this release, Exception routing rules can be entered for a specific period of a specific day.
- **OpenJDK Support** - MaxCS AltiReport now supports OpenJDK JRE to run Tomcat 8.5. In Release 8.6.1, AltiReport bundles OpenJDK JRE instead of Oracle JRE 8.
- **Not Ready Reason Codes** - You can now configure various codes that agents can use to specify why they are switching to Not Ready status. You can make reason codes mandatory or optional.
- **Call Disposition Codes** - Admins can now set up custom Call Disposition codes. These codes are typically descriptions of the final outcome of the call, and are a simple way for agents to label or categories calls. Codes can be configured as optional or mandatory.
- **Account Code Enhancements** - You can now require account codes for inbound calls in addition to outbound calls. You configure this on an extension basis.

- **Security update** - The system now prevents a configuration file from being read remotely; MaxAdmin is now initially set to accept only local access. Because of this change, you must update the IP Dialing Table in Enterprise Manager to add IP addresses that you want to have access.
- **VRM Pro update** - You can now disable Server Message Block signing (SMB) v1 on servers without obstructing the transfer of voice recordings to the VRM Pro server.
- **Remote access to Advanced Queue Management** - You can now access the Setup button for Advanced Queue Management for workgroups.
- **AltiSDK updates** - APIs have been added to AltiSDK for Not Ready Reason codes, Call Disposition codes, and for Account codes.

CHAPTER 2

2

System Requirements and Installation

MaxCS supports Softswitch, Private Cloud, and hardware deployments.

Minimum System Requirements

This section lists the operating systems supported by each MaxCS component, as well as system requirements.

For on-premise deployments, we recommend that your system have an overall passmark score of 10,000 or higher. Refer to the MaxCS Deployment Guide for details.

MaxCS Requirements	
MAXCS All-in-One Softswitch (Software only)	• Windows Server 2019 64-bit • Windows Server 2016 64-bit • Windows Server 2016 64-bit supported on VMware ESX and 6.0 • Windows Server 2012 R2 (64-bit) supported on Hyper-V 6.1 and VMware ESXi 6.0, 6.5, or 6.7. • Windows 10 Professional (64-bit) Softswitch • Windows 10 Professional (64-bit) on VMware ESXi 6.0, 6.5, or 6.7 • Windows 8.1 Professional (64-bit) Softswitch • Windows 8.1 Professional (64-bit) on Hyper-V 6.1 or VMware ESXi 6.0, 6.5, or 6.7.
Office 2G/3G	• Windows Server 2008 SP2 (32-bit) with 2GB RAM The 64-bit version of Windows will not work on Max2000/Office series chassis. (No version of Altigen MaxCS Server Software supports TLS 1.2 on Windows 2008 Server).
MaxAdministrator	**Operating Systems:** • Windows Server 2019, 2016, 2012 R2 • Windows 8.1 (64-bit) • Windows 10
	System Requirements: • Monitor with at least 1024x768 resolution

MaxCS Requirements	
Enterprise Manager	**Operating Systems:** **Note:** Windows XP is no longer supported**.** • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2
	System Requirements: • 1 GB RAM • 20 GB available hard drive disk space **Note:** The installation program will install JAVA JRE automatically
HMCP	**Operating Systems:** • Windows Server 2008 R2 SP1 (64-bit) • Windows Server 2012 R2
	Note: Only Intel-based processors are supported
Integration	**CDR Database Support:** • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 and Express • Microsoft SQL Server 2016 SP2 and Express • Microsoft SQL Server 2014 SP3 • Microsoft SQL Server 2012 SP4 **Note:** Running SQL Server in the same server as MaxCS is not supported.
	Email Server Integration: • Microsoft Office 365 Exchange Online • Microsoft Exchange Server 2010, 2013, 2016, and 2019

Note: To read online Help pages, the system must be running Internet Explorer 6.0 or later.

Performance Note

If your MaxCS server is running Windows Defender, for optimal performance we recommend that you add the following to Windows Defender's exclusion folder: “AltiDB”, “AltiServ” and “Postoffice.” If you are using VRM or voice recording feature, you may also want to add the recording folder to Windows Defender's exclusion folder.

Virtual Server Requirements

MAXCS supports the following virtual server environments:

- VMware ESX 6.0, 6.5 and 6.7: Allocate 4 Intel cores @ 2GHz each, 4GB memory, and 160GB hard drive
- Hyper-V version 6.1

MAXCS Client Applications

This section describes the operating systems supported by each individual client, and lists each client’s minimum system requirements.

For Polycom phone requirements, refer to the *MaxCS Polycom Configuration Guide*.

VRM Pro Server Requirements	
Operating Systems	• Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2
System/Processor	• IBM/PC AT compatible system • Intel 2 GHz Pentium 4 or equivalent
Disk Space	40 GB
RAM	4 GB RAM
Notes	• The installation program will install JAVA Open JRE automatically • Installation requires 1 GB available hard drive disk space. However, more space is required for CDR storage. • Must run on a stand-alone system
VRManager client	• Windows Server 2019 • Windows Server 2016 • Windows 10 • Windows 8.1 (64-bit)

Advanced Call Router Requirements	
Operating Systems	• Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows 10
System/Processor	• IBM/PC AT compatible system • Intel 2 GHz Pentium 4 or faster
Disk Space	40 GB
ODBC	Requires a 32-bit ODBC
RAM	1 GB RAM

AltiReport Requirements	
Operating Systems	• Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2
Applications	• Java JRE 8u212 or Open JDK version 212 • Database with JDBC Driver SQL Server • Client system: Internet Explorer 10.0 or 11.0
System/Processor	• IBM/PC AT compatible system • Intel 2 GHz Pentium 4 or equivalent
Disk Space	60 GB
RAM	1 GB RAM (2GB RAM required if it runs with SQL Server)
Notes	• Tomcat 8.5.43 will be installed automatically • Must run on a stand-alone system • AltiReport client system must have Internet Explorer 10 or 11, Chrome, or Edge

MaxAgent, MaxCommunicator, MaxSupervisor Requirements	
Operating Systems	• Windows 10 • Windows 8.1 (64-bit)
Third-Party Integration Software (MaxCommunicator and Altigen Clients)	Outlook 2010, 2013, and 2016 (32-bit only; **the 64-bit version of Outlook is not supported**)
System/Processor	• IBM/PC AT compatible system • 2 GHz CPU or faster
Disk Space	1 GB
RAM	1 GB RAM
Notes	• Microsoft .NET 4.5 framework or higher • SVGA monitor (1024x768) with 256-color display or better; Keyboard and mouse

MaxOutlook Requirements	
Operating Systems	• Windows 10 • Windows 8.1 (64-bit)
3rd Party Software	• Outlook 2007, 2010, 2013, or 2016 (32-bit only) **Note:** The 64-bit version of Outlook is not supported
System/Processor	• IBM/PC AT compatible system • 2 GHz CPU or faster
.NET Framework	Microsoft .NET 3.5 framework only
Disk Space	1 GB
RAM	1 GB RAM
Notes	• SVGA monitor (1024x768) with 256-color display or better • Keyboard and mouse

AltiConsole Requirements	
Operating Systems	• Windows 10 • Windows 8.1 (64-bit)
System/Processor	• IBM/PC AT compatible system • 1 GHz CPU or faster
Disk Space	1 GB
RAM	1 GB RAM
Notes	• SVGA monitor (1024x768) with 256-color display or better • Keyboard and mouse

Altigen SDK Requirements	
ActiveX Control for MaxCommunicator and AltiAgent	• Windows 10 • Windows 8.1 (64-bit)
AltiAPI (Alticomlib.dll)	• Windows 2019 • Windows 2016 • Windows 10 • Windows 8.1 (64-bit) • Windows Server 2012 R2 • Windows Server 2008 R2 SP1 (64-bit) • Windows Server 2008 SP2 (32-bit or 64-bit)

MaxInsight Requirements	
Operating Systems	• Windows 10 • Windows 8.1 (64-bit)
System/Processor	• IBM/PC AT compatible system • 1 GHz CPU or faster
Disk Space	1 GB
RAM	1 GB RAM
Notes	• SVGA monitor (1024x768) with 256-color display or better • Keyboard and mouse

MaxMobile Requirements	
iPhone	• iOS 12
Android	• 9.0

Quality Management Requirements
• The server must be running Windows Server 2012 R2 • The MaxCS 9.0.1 server must already be installed • The CDR database must be deployed on an external SQL Server • VRManager Pro must already be installed • You must have the appropriate *Quality Management* licenses • The Quality Management tool will work with only encrypted *MaxCS 8.5 Update 1 and later* recordings; it will not work with non-encrypted recordings from earlier releases of MaxCS

MaxCS Licenses

In MaxCS, most client licenses are available in both concurrent session mode and seat-based mode. Both types can be mixed in a MaxCS system.

The following licenses are available for MaxCS:

Licenses for MaxCS	
Per System	
Advanced Call Router	Per system
AltiReport	Per system
MaxCS ACM	Per system
Multilingual	Per system

Licenses for MaxCS	
VRManager Pro	Per system
Quality Management	Per System
TrustID License	Per System
Per Seat or Per Session	
AltiConsole	Per session
Callback from Queue Licenses	Per seat or per session
ChatBeacon Integration License	Per seat
Concurrent Recording Session License	Per session
Dedicated Recording Seat License (for VRManager)	Per seat assigned to record to a centralized folder, and per trunk port with recording enabled
Enterprise Manager	Per server license
IPTalk	Per seat or per session
MaxAgent	Per seat
MaxAgent Concurrent License	Per session
MaxCommunicator	Per seat or per session
MaxInSight	Per session
MaxMobile	Per seat
MaxSupervisor	Per seat
MaxSupervisor Concurrent License	Per session
Polycom Advanced Features License	Per seat
Quality Management Seat License	Per seat
SDK Connection Session	Per session
Third-Party SIP Device	Per seat registering as an IP extension (non-concurrent)
Trunk Control APC SDK	Per session
Other	
Exchange Integration	Per user
SIP Trunk	Per activated SIP trunk

The following licenses are available for **all-in-one (stand alone) systems** only:

Licenses for Stand Alone Systems	
Station License	Per activated extension
ACM Agent Seat	Per concurrent login (Single agent logged into multiple WGs will only take one license)

The following licenses are available for **Softswitch/HMCP Media Server/Gateway systems** only:

Licenses for Softswitch / HMCP Media Server / Gateway Systems	
HMCP Media Server License	Available resources in the system
HMCP G.711/G.723/G.729 Voice Processing Resources	Available resources in the system
HMCP MeetMe Conference	Available resources in the system
HMCP Supervision	Available resources in the system

Licenses for Softswitch / HMCP Media Server / Gateway Systems	
Softswitch Station License	Per extension configuration
Softswitch ACM Agent Session License	Per session
Softswitch ACM Agent Migration License	Per ACC agent session
Gateway	Per gateway

Preparation for Installation

Before you start installing MaxCS, you need the following:

- **Windows Update** – Make sure your server has the recommended Windows Service Pack or Update.
- **MaxCS installation media** – The MaxCS installation DVD or other media that contains the MaxCS programs.
- **MaxCS latest update** – Check to see if there is an update available to the MaxCS Release.
- **System Key** – The system key can be either a USB hardware security device that must be attached to the server MAXCS is running on, or it can be a soft system key.
    - You cannot use both a hardware device and the soft system key at the same time.
    - When using a soft system key, the MAXCS system must be a member of an Active Directory domain.
- **Software license key** – A 20-digit key located on the front of the End User License Agreement.

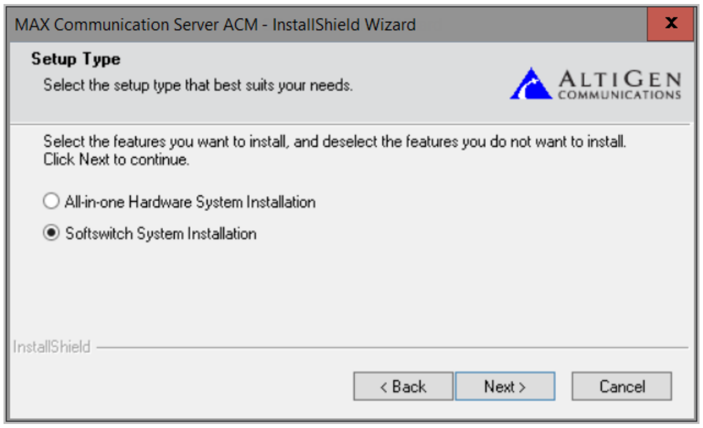
Installing MAX Communication Server

Softswitch installations – If you are installing the MaxCS Softswitch version, follow the instructions in the *MaxCS All-Software Solution Deployment Guide*.

Upgrades – If you are upgrading from a previous release of MAXCS, review the instructions in the *MaxCS Upgrade Guidelines* before you begin any installation steps. If you are upgrading from a release prior to MaxCS 7.0 Update 1, then the installation program will check whether Microsoft Outlook has been installed on the server. If it detects Outlook, you must uninstall Outlook before you can install *MaxCS*. In addition, if you have used a previous version of VRManager, you will be upgraded to VRManager Pro; see the separate guide, *VRManager Pro Manual*, for instructions.

To install MaxCS, load the installation media, click the setup program in the folder, and follow the instructions

on the installation screens. when prompted, select a setup type.



MAX Communication Server ACM - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Select the features you want to install, and deselect the features you do not want to install.
Click Next to continue.

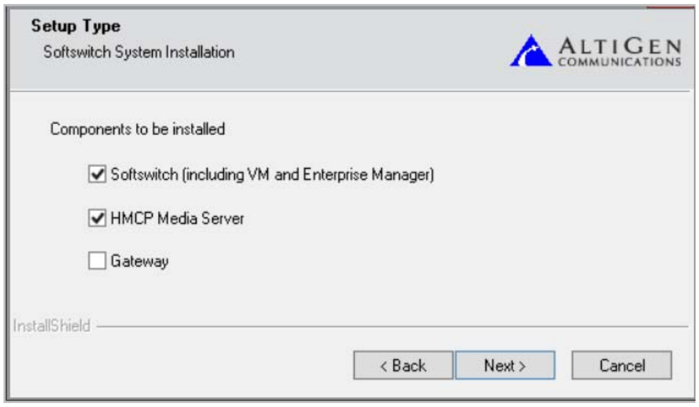
○ All-in-one Hardware System Installation

● Softswitch System Installation

- **All-in-one Hardware System Installation** – Select this option if you have a hardware system that includes Altigen boards, such as Max1000, Max2000, and 3G.
- **Softswitch System Installation** – Select this option if you have a softswitch system. On the next screen you can select which components to install.

Softswitch System Installation

If you chose to install the Softswitch System installation, you can install the following components.



Components to be installed

☑ Softswitch (including VM and Enterprise Manager)

☑ HMCP Media Server

☐ Gateway

- **Softswitch (including VM and Enterprise Manager)** – Select this option to install Softswitch to the server. Softswitch provides the following functions:
    - Devices Control
        - IP Phone
        - HMCP Media Server
        - IP Gateway
    - Call Control
        - Call Signal Processing (SIP tie trunk)
        - PBX Switching, Routing, and Call Handling
    - System Management
        - Configuration and Directory
        - Phrases and Prompts (System, Custom, Personal)
    - Feature Server
        - Voice Mail Server
        - Multi-Site Enterprise Manager
        - Call Center Feature Server
        - CTI Server
        - Exchange Integration Server
        - CDR Server
- **HMCP Media Server** – For softswitch deployment, select this option.

  The **HMCP Media Server** check box is not available if the operating system is not supported by HMCP (refer to *Minimum System Requirements* on page 9). Altigen supports HMCP Media Server only on servers provided by Altigen.

- **Gateway** – This option is not supported starting with Release 8.5.

For detailed instructions on installing and upgrading MaxCS, Altigen Partners should refer to the readme file.

Installing MaxAdministrator on a Network Client

MaxAdministrator can be installed on a client workstation, providing the ability to manage the MaxCS server remotely. The system running MaxAdmin and the MaxCS server must be on the same Windows domain.

When you install MaxAdministrator on a machine that is not a MaxCS server, it does not contain the switching, SMTP/POP3 server, messaging agent, AltiBackup, and Exchange integration services that are included in the full MaxCS installation.

The following features cannot be accessed via a Remote MaxAdministrator client:

- System Data Management
- Shutdown Switching Services
- VOIP Enterprise Network Manager
- MeetMe Conference configuration and management
- Recording configuration
- Diagnostic tools such as Trace Collector and Altigen Network log

Beginning in Release 8.6.1, you can remotely access the workgroup **Setup** button for Advanced Queue Management.

To install MaxAdministrator on a client workstation,

1. From the MaxCS installation media, run **SETUP.EXE** in the **MaxAdministrator** folder.
2. Follow the instructions on the screen.

Uninstalling MaxCS

To uninstall MaxCS be sure to stop all MaxCS-related services before uninstallation. To do this, run MaxAdministrator, log in, and select **Services** > **Shutdown Switching** from the menu.

In the event that the auxiliary services were not stopped, stop them one at a time in Windows, using the **Start** > **Programs** > **Administrative Tools** > **Services** tool.

Then open the Control Panel. In **Add/Remove Programs**, select **MAX Communication Server ACM** and then click **Remove**.

CHAPTER

3

Getting Around MaxAdministrator

This section gives a brief overview of MaxAdministrator, the program used to configure and administer MAXCS and its client applications.

MaxAdmin has a graphical user interface with tabbed windows that makes it easy to use.

Logging In and Out

To log into MaxAdministrator,

1. From the Windows Start menu, select **Max Communication Server ACM** > **MaxAdministrator.**

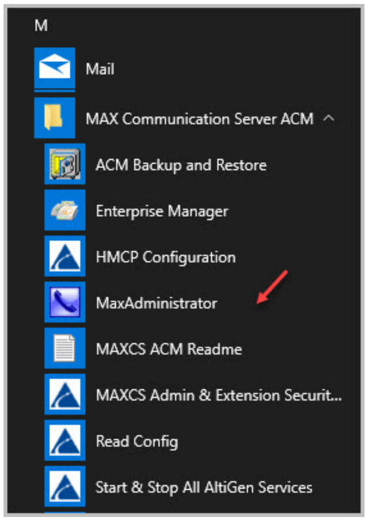


Figure 1. Opening MaxAdmin

2. Select the server.
3. Enter your username and password. Click **OK**.

   As of MaxCS Release 8.5.0.215, usernames are case sensitive; they must be entered exactly as they have been configured in your MaxCS user account. This includes the default account of “admin”.

   The first time you log in, use the system default password, 22222. To ensure system security, change the system password as soon as possible.

To log out, click the **Logout** button, or select **Services** > **Logout**.

Remote Login

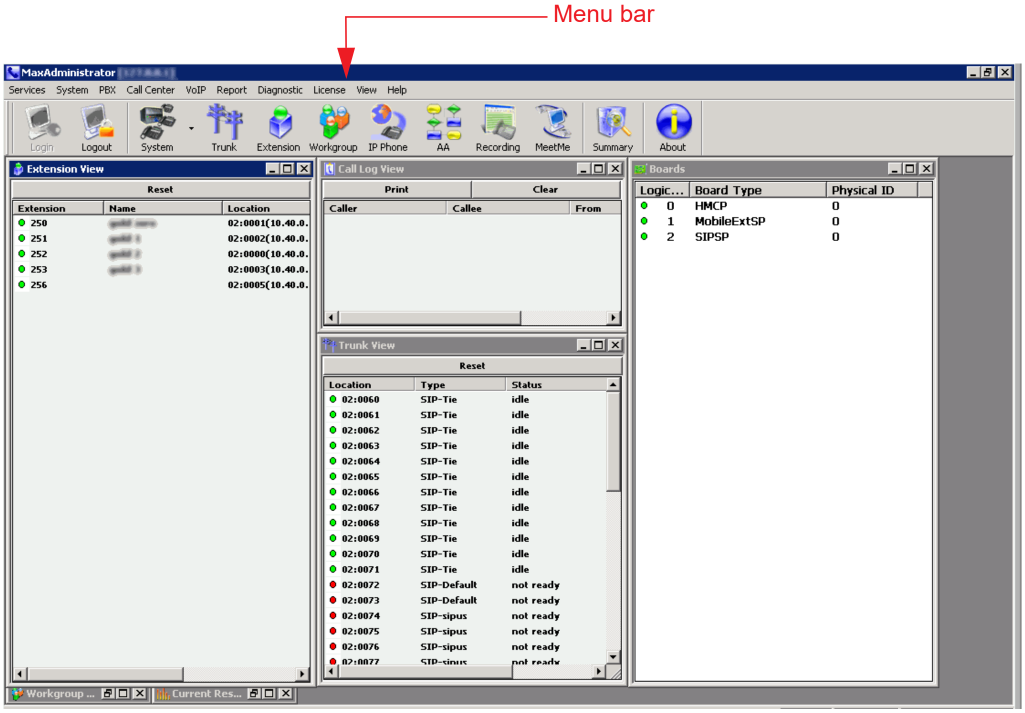
Beginning with MaxCS Release 8.5.0.215, TCP port 10078 is used for secured MaxAdministrator connection. Make sure that TCP port 10078 is opened on the server side firewall if you need a remote MaxAdministrator connection.

Changing the Password

Select **Services** > **Change Password** to change to a new password.

The Main Window

When you run MaxAdmin, you'll see a window similar to the following figure.



Extension	Name	Location
● 250	[redacted]	02:0001(10.40.0.
● 251	[redacted]	02:0002(10.40.0.
● 252	[redacted]	02:0000(10.40.0.
● 253	[redacted]	02:0003(10.40.0.
● 256		02:0005(10.40.0.

Caller	Callee	From

Logic...	Board Type	Physical ID
● 0	HMCP	0
● 1	MobileExtSP	0
● 2	SIPSP	0

Location	Type	Status
● 02:0060	SIP-Tie	idle
● 02:0061	SIP-Tie	idle
● 02:0062	SIP-Tie	idle
● 02:0063	SIP-Tie	idle
● 02:0064	SIP-Tie	idle
● 02:0065	SIP-Tie	idle
● 02:0066	SIP-Tie	idle
● 02:0067	SIP-Tie	idle
● 02:0068	SIP-Tie	idle
● 02:0069	SIP-Tie	idle
● 02:0070	SIP-Tie	idle
● 02:0071	SIP-Tie	idle
● 02:0072	SIP-Default	not ready
● 02:0073	SIP-Default	not ready
● 02:0074	SIP-sipus	not ready
● 02:0075	SIP-sipus	not ready
● 02:0076	SIP-sipus	not ready
● 02:0077	SIP-sipus	not ready

Figure 2. MaxAdmin main window

The main menu bar is at the top. Below that are buttons for quick access to more commonly used configuration screens. A status bar at the bottom contains information on the current runtime status.

The Main Menu

These are the menus and the functions found under each menu:

- **Services** – Log in and log out, change password, access utilities (backup and restore, convert work/hunt group, import and export an extension list), shut down all services, and exit.

  Note that the commands **Services** > **Utilities** > **Backup and Restore**, and **Services** > **Shut Down All Services** cannot be performed remotely.

- **System** – Opens windows where you can configure system settings, gateways and media servers, voice mail, auto attendants, multilingual support, call recording, application extensions, Unified Communications, and Admin User accounts. Also where you can request and import certificates and create directories for Polycom users (refer to the *MAXCS 8.5 Update 1 Polycom Configuration Guide*).
- **PBX** – Opens windows where you can configure trunks, in call routing, out call routing, extensions, Altigen IP phones, hunt groups, line park, and MeetMe conference. You can also *manage* MeetMe conferences from this menu.
- **Call Center** – Opens windows where you can configure workgroups, agent logout reasons, account codes, call disposition codes, and MaxCall.
- **VoIP** – Opens windows where you can configure the enterprise network, the multi-site domain, and the refresh enterprise settings.
- **Report** – Opens windows where you can view the system summary and IP traffic statistics and configure SNMP (simple network management protocol).
- **Diagnostic** – Opens windows where you can view the trace, view the system log, and view the Altigen network log.
- **License** – Shows system and seat license information.
- **View** – Lets you show, hide, and set default alignment of the view windows, the toolbar, and the status bar.
- **Help** – Opens the Help window and offers a link to the Altigen Technical Support site.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

Quick Access Toolbar

Toolbar buttons give you quick access to frequently used functions.

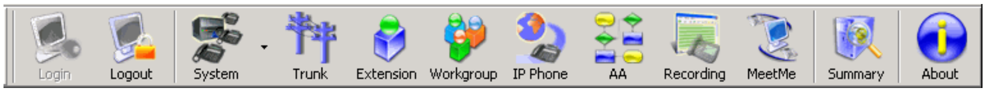


Figure 3. MaxAdministrator quick access toolbar

From left to right, the toolbar buttons serve the following purposes:

Login	**Login**. Opens the Password dialog box to log in to the system.
Logout	**Logout**. Logs out of the system.
System	**System**. Opens the System Configuration window, or the System menu. Shortcut for **System > System Configuration**.
Trunk	**Trunk**. Opens the Trunk Configuration window. Shortcut for **PBX > Trunk Configuration**.
Extension	**Extension**. Opens the Extension Configuration window. Shortcut for **PBX > Extension Configuration**.

Workgroup. Opens the Workgroup Configuration window.
Shortcut for **CallCenter > Workgroup Configuration**.

IP Phone. Opens the IP Phone Configuration window.
Shortcut for **PBX > Altigen IP Phone Configuration**.

AA. Opens the AA Configuration window.
Shortcut for **System > AA Configuration**.

Recording. Opens the Recording Configuration window.
Shortcut for **System > Recording Configuration**.

MeetMe. Opens the MeetMe Conference window.
Shortcut for **PBX > MeetMe Conference**.

Summary. Opens the System Summary window.
Shortcut for **Report > System Summary**.

About. Opens a window that displays version and file information. Gives information about the Altigen Technical Support Web Site. This is a shortcut for **Help > About MaxAdministrator**.

Status Bar

The **Status Bar** at the bottom of the main window displays disk usage, the status of SMDR, the status of the call detail reporting log, the status of the operator, and current date and time.

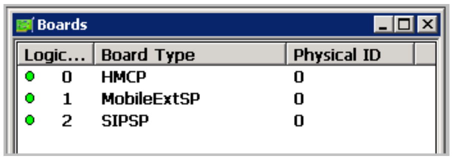
The View Windows

The MaxAdmin main window hosts a number of child windows that provide various views into the internal system real-time status.

Boards View Window

The **Boards** window displays the hardware board types and their logical and physical IDs. For each installed board, it displays:

- The board's logical ID (the sequential ID of the board assigned by the system).
- Board type.
- The physical ID (including the ID on the faceplate of the board and the gateway ID). If it is an all-in-one system, the gateway ID is the system itself, and the ID is 0.



Logic...	Board Type	Physical ID
● 0	HMCP	0
● 1	MobileExtSP	0
● 2	SIPSP	0

Double-click a board to open a configuration window for that board.

Figure 4. Boards window

Click on any column heading to sort by that column. Click again to reverse the sort order.

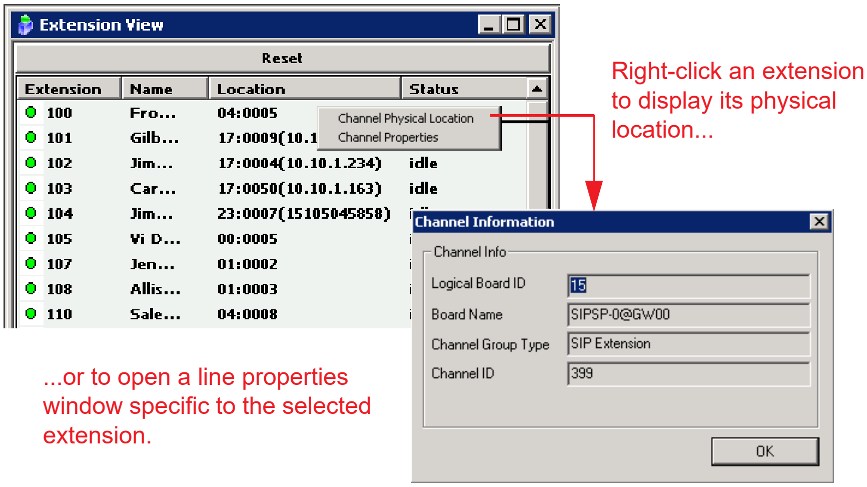
Extension View Window

The **Extension View** window displays the name, location, and status of all assigned extensions.

Click on any column heading to sort by that column. Click again to reverse the sort order.

Double-click any extension number to open the Extension Configuration window for the selected extension.

The radio button to the left of each extension number is green when the extension is idle, and red when the extension is *not ready* or *in use.* The **Location** number (for example, 01:0005) identifies the card logical ID and port (channel) number on the board. For example, in location 01:0005, the card logical ID is 1 and the port number is 5. If an IP Extension is logged on, the location will show the IP address.



Extension	Name	Location	Status
● 100	Fro...	04:0005	
● 101	Gilb...	17:0009(10.1	
● 102	Jim...	17:0004(10.10.1.234)	idle
● 103	Car...	17:0050(10.10.1.163)	idle
● 104	Jim...	23:0007(15105045858)	i
● 105	Vi D...	00:0005	i
● 107	Jen...	01:0002	i
● 108	Allis...	01:0003	i
● 110	Sale...	04:0008	i

Channel Info

Logical Board ID: 15

Board Name: SIPSP-0@GW00

Channel Group Type: SIP Extension

Channel ID: 399

Right-click an extension to display its physical location...

...or to open a line properties window specific to the selected extension.

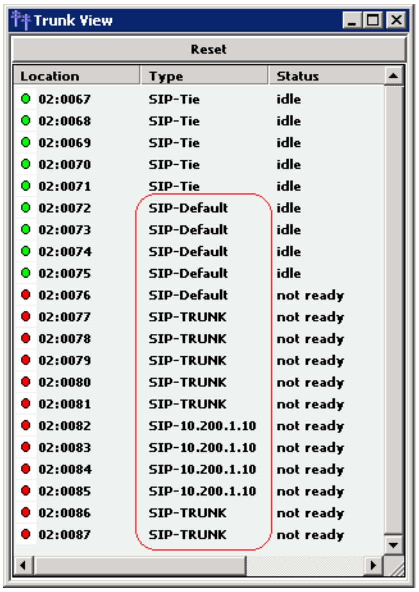
Figure 5. Extension View window

The **Reset** button resets the selected extension to the idle status. You'll be asked to confirm the reset.

You can click the **Reset** button without selecting an extension, and then type in the extension number for the extension to reset.

Trunk View Window

The **Trunk View** window displays the status of all trunks.



Location	Type	Status
🟢 02:0067	SIP-Tie	idle
🟢 02:0068	SIP-Tie	idle
🟢 02:0069	SIP-Tie	idle
🟢 02:0070	SIP-Tie	idle
🟢 02:0071	SIP-Tie	idle
🟢 02:0072	SIP-Default	idle
🟢 02:0073	SIP-Default	idle
🟢 02:0074	SIP-Default	idle
🟢 02:0075	SIP-Default	idle
🔴 02:0076	SIP-Default	not ready
🔴 02:0077	SIP-TRUNK	not ready
🔴 02:0078	SIP-TRUNK	not ready
🔴 02:0079	SIP-TRUNK	not ready
🔴 02:0080	SIP-TRUNK	not ready
🔴 02:0081	SIP-TRUNK	not ready
🔴 02:0082	SIP-10.200.1.10	not ready
🔴 02:0083	SIP-10.200.1.10	not ready
🔴 02:0084	SIP-10.200.1.10	not ready
🔴 02:0085	SIP-10.200.1.10	not ready
🔴 02:0086	SIP-TRUNK	not ready
🔴 02:0087	SIP-TRUNK	not ready

The trunk type or group name shows in the "Type" column.

Right-click a trunk to display its physical location or to open a properties window specific to the selected trunk.

Figure 6. Trunk View window

The radio button to the left of each trunk location is green when the trunk is idle, and red when the extension is *not ready* or *in use.* The location format is *logical board ID:channel* – for example, channel 3 on the board in logical board ID 9 is location 09:03. The **Type**, **Status,** and **Duration** of trunk use are also shown.

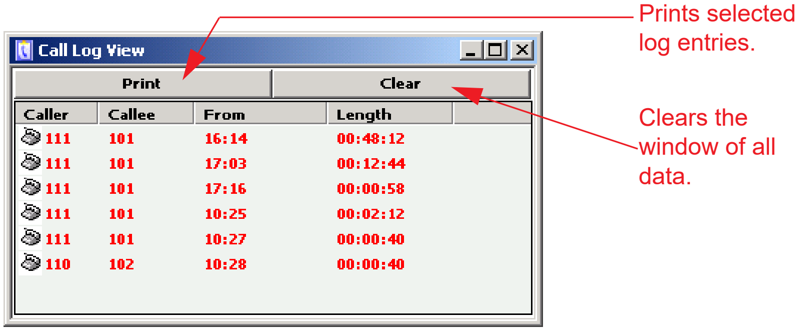
Note: The **Duration** field displays the duration of the trunk only if the call is connected after MaxAdmin is started. The field will be empty if the trunk is idle, not ready, out of service, or the call was connected prior to MaxAdministrator being launched.

You can double-click any trunk location to open the *Trunk Configuration window* for the selected trunk.

The **Reset** button resets the selected trunks to the idle status if the trunk is connected to a carrier. You'll be asked to confirm the reset, and a status message will tell you if the reset was successful.

Call Log View Window

The **Call Log View** window displays the line and trunk traffic history.



Caller	Callee	From	Length
☎ 111	101	16:14	00:48:12
☎ 111	101	17:03	00:12:44
☎ 111	101	17:16	00:00:58
☎ 111	101	10:25	00:02:12
☎ 111	101	10:27	00:00:40
☎ 110	102	10:28	00:00:40

Prints selected log entries.

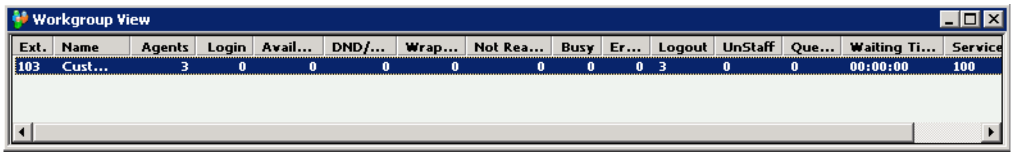
Clears the window of all data.

Figure 7. Call Log View window

The window displays, for the last 30 calls, the caller line or number, the callee, the starting time in 24-hour format and the length of the call. When the call is from another Altigen system, the call is displayed as "*Caller System IP Address-Extension Number*."

Workgroup View Window

The **Workgroup View** window displays data and statistics for workgroups:



Ext.	Name	Agents	Login	Avail...	DND/...	Wrap...	Not Rea...	Busy	Er...	Logout	UnStaff	Que...	Waiting Ti...	Service
103	Cust...	3	0	0	0	0	0	0	0	3	0	0	00:00:00	100

Figure 8. Workgroup View window

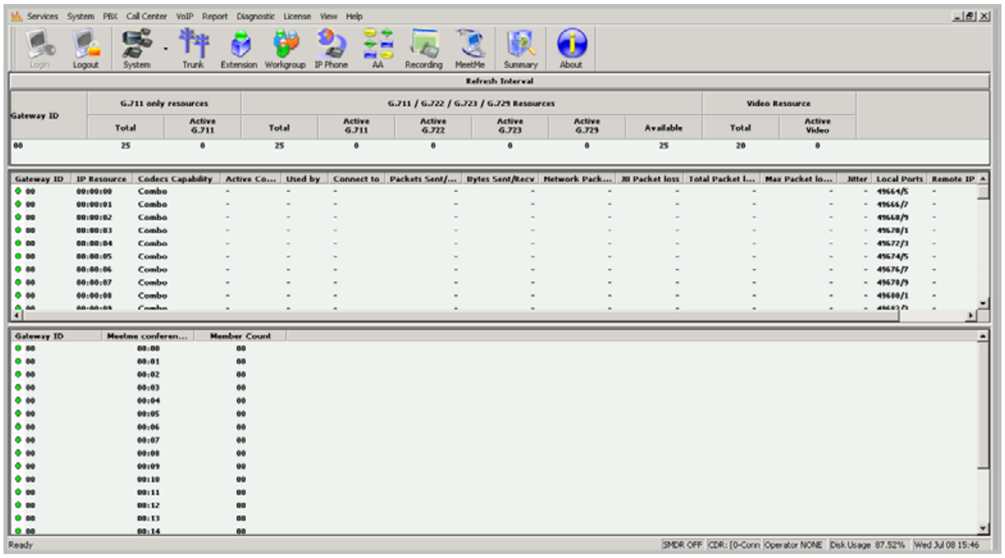
This window displays the following data:

- **Extension** – The workgroup pilot extension number
- **Name** – The workgroup name
- **Agents** – The number of agents assigned to the workgroup
- **Login** – The number of agents logged into the workgroup
- **Available** – The number of logged in agents who are available to receive workgroup calls
- **DND** – The number of logged in agents who are unavailable with the Do Not Disturb status
- **Wrapup** – The number of agents who are in wrapup mode
- **Not Ready** – The number of logged in agents who are in Not Ready state
- **Busy** – The number of logged in agents who are currently on the phone
- **Error** – The number of logged in agents with extensions that are left off-hook or other user error
- **Logout** – The number of agents who are logged out from the workgroup
- **Unstaff** – The number of agents who are logged out from the system and have become a virtual extension
- **Queue** – The number of calls waiting in queue
- **Waiting Time** – The longest wait time of callers in queue
- **Service Level** – The percentage of calls in queue with queue time less than or equal to the defined service level threshold

Current Resource Statistics Window

The **Current Resource Statistics** window displays the total VoIP channels, available channels, and in-use channels.

The window allows administrators to monitor VoIP channel usage and MeetMe conference resource use.



Gateway ID	G.711 only resources		G.711 / G.722 / G.723 / G.729 Resources						Video Resource	
	Total	Active G.711	Total	Active G.711	Active G.722	Active G.723	Active G.729	Available	Total	Active Video
00	25	0	25	0	0	0	0	25	20	0

Gateway ID	IP Resource	Codecs Capability	Active Co...	Used by	Connect to	Packets Sent/...	Bytes Sent/Recv	Network Pack...	JB Packet loss	Total Packet l...	Max Packet lo...	Jitter	Local Ports	Remote IP
● 00	00:00:00	Combo	-	-	-	-	-	-	-	-	-	-	49664/5	-
● 00	00:00:01	Combo	-	-	-	-	-	-	-	-	-	-	49666/7	-
● 00	00:00:02	Combo	-	-	-	-	-	-	-	-	-	-	49668/9	-
● 00	00:00:03	Combo	-	-	-	-	-	-	-	-	-	-	49670/1	-
● 00	00:00:04	Combo	-	-	-	-	-	-	-	-	-	-	49672/3	-
● 00	00:00:05	Combo	-	-	-	-	-	-	-	-	-	-	49674/5	-
● 00	00:00:06	Combo	-	-	-	-	-	-	-	-	-	-	49676/7	-
● 00	00:00:07	Combo	-	-	-	-	-	-	-	-	-	-	49678/9	-
● 00	00:00:08	Combo	-	-	-	-	-	-	-	-	-	-	49680/1	-
● 00	00:00:09	Combo	-	-	-	-	-	-	-	-	-	-	49682/3	-

Gateway ID	Meetme conferen...	Member Count
● 00	00:00	00
● 00	00:01	00
● 00	00:02	00
● 00	00:03	00
● 00	00:04	00
● 00	00:05	00
● 00	00:06	00
● 00	00:07	00
● 00	00:08	00
● 00	00:09	00
● 00	00:10	00
● 00	00:11	00
● 00	00:12	00
● 00	00:13	00
● 00	00:14	00

Ready | SMDR OFF | CDR: [0-Conn | Operator NONE | Disk Usage 87.52% | Wed Jul 08 15:46

Figure 9. Current Resource Statistics window

Top part of the window

Contains a summary of codec usage.

Middle part of the window

Displays the following data:

- **Gateway ID** – The ID of the VoIP channel's home gateway
- **IP Resource** – The Triton VoIP *logical board ID:internal DSP channel ID*
- **Codecs Capability** – The codecs the IP channel can use
- **Active Codec** – The codec currently being used
- **Used By** – The extension, trunk, or SIP channel that is using this channel
- **Connect To** – The extension, trunk, or channel the channel is connected to
- **Packets Sent/Received** – The number of voice packets sent and received
- **Bytes Sent/Received** – The total size (in bytes) of all voice packets sent and received
- **Network Packet Loss** – The number of voice packets that have been lost due to prolonged delays, network congestion, or routing failure
- **JB Packet Loss** – The number of voice packets that have been discarded due to jitter buffer overflow
- **Total Packet Loss Rate** – The ratio of total number of lost packets versus total received packets
- **Max Packet Loss Rate** – The maximum packet loss rate observed over a period of time during a whole session
- **Jitter** – Displays the average length of delay per voice packet in milliseconds. This number can be used to measure the quality of service on the network that connects the source and destination sites. Under 100 milliseconds is good, while a higher figure indicates a longer than average delay. (See *Setting VoIP Codec Profiles* on page 315 for more detailed information on jitter.)
- **Local Ports** – Displays the local RTP/RTCP port for the voice stream
- **Remote IP Address:Port** – Displays the remote RTP port for the voice stream

Bottom part of the window

Shows information about the MeetMe 30-party conference bridge:

- Gateway ID of the 30-party conference board (for example, 00)
- MeetMe Conference Bridge ID (from 00:00 to 00:09)
- Number of members currently participating in a conference using each bridge

Note: Each system can have only one 30-party MeetMe conference board.

Setting the Refresh Interval

The **Current Resource Statistics** window is updated according to the **Refresh Interval** configuration. By default, the **Refresh Interval** is set to refresh the data in the window every 5 seconds. To change the refresh interval, click the **Refresh Interval** button at the top of the window, and set the refresh interval to a number of seconds up to one minute. To set the time to 0 is to *turn off* the refresh interval.

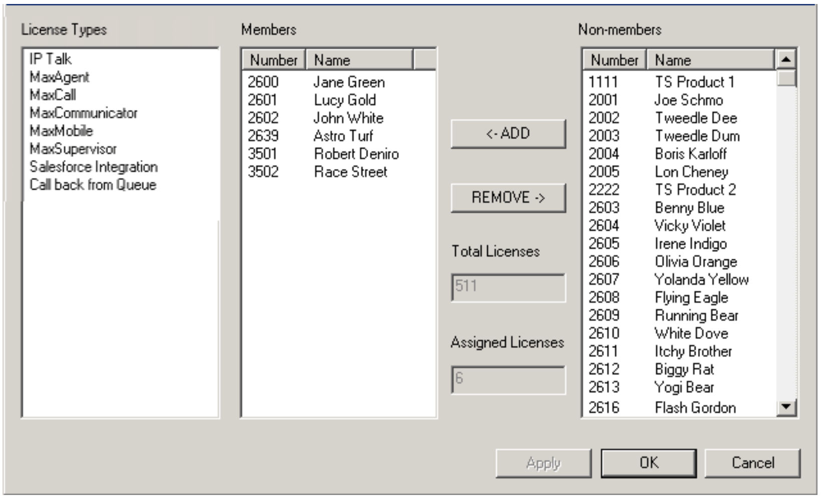
Assigning Seat-Based Client Licenses

Most MaxCS client products require either session- or seat-based licenses. You may have purchased both types. A session license allows a certain number of extensions to use a client product.

If you have purchased seat licenses so that particular extensions always have access to the client product, those extensions must be assigned to the client product in MaxAdministrator. If an extension is not assigned to a product, that extension may not be able to use the client product. You may have seat-based licenses for the following client products:

- MaxCommunicator
- MaxOutlook (uses MaxCommunicator license)
- MaxAgent
- MaxSupervisor
- Quality Management
- AltiConsole
- IP Talk
- Salesforce Integration
- MaxCall
- Callback from Queue

Assign extensions to seat-based licenses in the Client SEAT License Management configuration screen (**License** > **Client SEAT License Management**). Licenses are sorted in alphabetical order.



License Types

- IP Talk
- MaxAgent
- MaxCall
- MaxCommunicator
- MaxMobile
- MaxSupervisor
- Salesforce Integration
- Call back from Queue

Members

Number	Name
2600	Jane Green
2601	Lucy Gold
2602	John White
2639	Astro Turf
3501	Robert Deniro
3502	Race Street

Non-members

Number	Name
1111	TS Product 1
2001	Joe Schmo
2002	Tweedle Dee
2003	Tweedle Dum
2004	Boris Karloff
2005	Lon Cheney
2222	TS Product 2
2603	Benny Blue
2604	Vicky Violet
2605	Irene Indigo
2606	Olivia Orange
2607	Yolanda Yellow
2608	Flying Eagle
2609	Running Bear
2610	White Dove
2611	Itchy Brother
2612	Biggy Rat
2613	Yogi Bear
2616	Flash Gordon

Total Licenses: 511

Assigned Licenses: 6

Figure 10. The Client SEAT License window

Select a license type and then select extensions to add to the list of “members” who can always use the selected product. To make multiple selections, use Shift+click and Ctrl+click. The screen shows the total number of licenses you have for a client product and the number of licenses assigned.

Stopping the Altigen Switching Service

Normally, when you exit MaxAdministrator, the Altigen services that provide the various telephony and data services remain active. If you need to shut down the phone system, do one of the following:

- From MaxAdmin, select **Services** > **Shut Down All Services**.
- From the Windows Start menu, select **MAX Communication Server ACM** > **Start and Stop All Altigen Services**, and click the **Shutdown All Altigen Services** button.

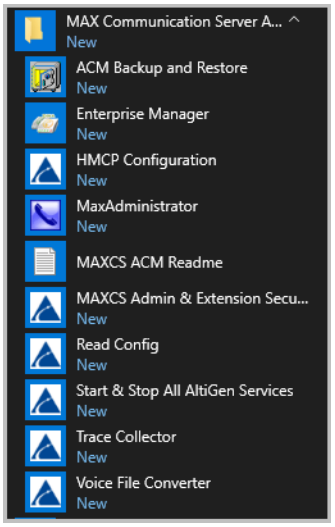
This stops the MaxCS system services, including the MaxAdmin application itself. When you re-open MaxAdmin, the switching services are reactivated.

These options are available when you are logged in at the MaxCS system computer; they are *not* available from a remote MaxCS client.

Note: Stopping the Altigen services from the Windows Services tool is not recommended, because it requires you to know what all the services are and is time-consuming.

Programs Available from the Windows Start Menu

Several MaxCS programs and utilities are available from the Windows **Start** menu.



MAX Communication Server A... ^
New
ACM Backup and Restore
New
Enterprise Manager
New
HMCP Configuration
New
MaxAdministrator
New
MAXCS ACM Readme
MAXCS Admin & Extension Secu...
New
Read Config
New
Start & Stop All AltiGen Services
New
Trace Collector
New
Voice File Converter
New

Figure 11. The programs on the Windows Start menu

Available under **MAX Communication Server ACM**:

- **ACM Backup and Restore –** Backs up your configurations and extension voice mail. See “Backup and Restore Utility” on page 386.
- **Enterprise Manager**
- **HMCP Configuration**
- **MaxAdministrator** – Lets you configure and administer your MaxCS system.
- **MaxCS ACM Readme** – Readme file for MaxCS ACM.

- **MaxCS Admin and Extension Security Checker** – Checks the security status of every extension in your MaxCS system. See “MaxCS Admin & Extension Security Checker” on page 388.
- **Read Config** – Creates a subdirectory of HTML files that shows details of your MaxCS configuration. See “Read Config” on page 398.
- **Start and Stop All Altigen Services** – Opens a dialog box that gives you the option to start or stop all Altigen services by clicking a button.
- **Trace Collector** – Collects the trace in selected MaxCS categories, within a time range specified, for debugging purposes. See “Trace Collector” on page 391.
- **Voice File Converter** – A voice phrase conversion tool that converts WAV files to ADPCM, WAV to PCM, or ADPCM/PCM to WAV format. See “Voice File Converter” on page 397.

CHAPTER

4

System Configuration

The **System Configuration** window is where you can configure the MAXCS system-wide settings.

To open this window, select **System** > **System Configuration**.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

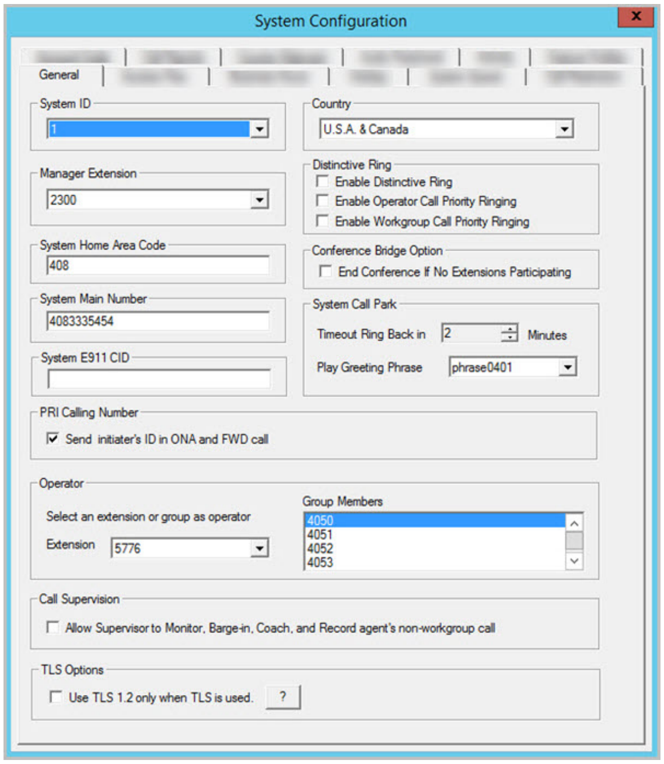
The System Configuration button

You can then work with the following settings, each of which is accessed by a tab in the System Configuration window.

- **General** – System ID, area code and number, operator and manager extensions, country, distinctive ring, conference call, and system call park options
- **Number Plan** – How the system responds to each first digit dialed
- **Business Hours** – Used by system functions
- **Holiday** – How calls are routed on designated holidays
- **Exception Routing** - Exception routing rules can be entered for a specific period of a specific day
- **System Speed** – Speed dial numbers that can be used by all extension users
- **Call Restriction** – Prefixes to block, toll call prefixes, and call control
- **Account Code** – Tables for creating and removing account codes
- **Call Reports** – CDR logging and data export
- **Country Relevant** – Settings for toll call prefixes and emergency numbers
- **Audio Peripheral** – Settings for music on hold and system default prompts
- **Activity** – Settings for pre-defined or customized activity codes
- **Feature Profiles** – Settings for extension feature profiles

Setting General Parameters

Use the **General** tab in the **System Configuration** window to set the system ID, area code, main number, and country; extensions for the manager and operator; options for distinctive ring, conference bridge, and system call park; options for TLS 1.2 and E911 Caller ID.



System Configuration

General

System ID: 1

Country: U.S.A. & Canada

Manager Extension: 2300

Distinctive Ring
□ Enable Distinctive Ring
□ Enable Operator Call Priority Ringing
□ Enable Workgroup Call Priority Ringing

System Home Area Code: 408

Conference Bridge Option
□ End Conference If No Extensions Participating

System Main Number: 4083335454

System Call Park
Timeout Ring Back in 2 Minutes
Play Greeting Phrase phrase0401

System E911 CID:

PRI Calling Number
☑ Send initiater's ID in ONA and FWD call

Operator
Select an extension or group as operator
Extension 5776
Group Members: 4050, 4051, 4052, 4053

Call Supervision
□ Allow Supervisor to Monitor, Barge-in, Coach, and Record agent's non-workgroup call

TLS Options
□ Use TLS 1.2 only when TLS is used.

Figure 12. System Configuration, General tab

You can set the following parameters and options:

System General Parameter	Description
System ID	Assign a number (1-100) to the system. This ID will be used to differentiate call records if multiple systems are writing call records to a same external database. In a multi-site VoIP domain, each System ID/Server ID must be unique and must be the same length. Once a server is part of a VoIP domain, you cannot change the **System ID**.
Country	Select a country for the system. This configuration ties to a tone table matched to the country's telecom interface specification.
Manager Extension	Select the system manager’s extension number. The system manager has access to the following system administrator functions: • Record custom phrases • Turn on trunk blocking (#38) • Manage voice mail’s System Distribution List from phone • Run CDR search as administrator login account

System General Parameter	Description
Distinctive Ring	Enables users to distinguish between internal, external, and operator calls by the way the phone rings: • **Enable Distinctive Ring** – establishes a short double ring cadence for internal calls and a normal, single ring for external calls. When disabled, both rings are normal. • **Enable Operator Call Priority Ringing** – produces a long single ring between short pauses on calls to the operator. • **Enable Workgroup Call Priority Ringing** – produces a short single ring between short pauses on calls to the workgroup. **Note:** This feature is not supported on Polycom phones.
System Home Area Code	Area code for the system location. **Note**: This field cannot be blank in the U.S. and Canada.
Conference Bridge Option	Selected, conference calls will end when all internal lines have disconnected from the conference bridge. Not selected, the conference connection can continue between outside parties, even after all internal parties have disconnected.
System Main Number	The main system telephone number, which is sent to the pager's display when a user's messaging options are configured to call a pager. This number will be used by a PRI trunk as the outbound caller ID in the event that no number is assigned in the trunk Phone Number, 10-digit DID, or extension **Transmitted CID** field. **Note**: This field cannot be blank.
System E911 CID	The default system E911 Caller ID. Make sure that you include your area code in your entry. • You can overwrite this default to assign different E911 Caller IDs for individual extensions • If an extension does not have an E911 CID configured, it will use this new *System E911 CID* More information on E911 options in MaxCS can be found in the chapter *Location-Based E911* on page 295.
PRI Calling Number	Check the check box to send a caller's caller ID when the call is going through one-number access (ONA) or when the call is being forwarded.
System Call Park • Timeout, Ring Back in ... Minutes • Play Greeting Phrase	System Call Park (**#41**) allows the extension user to park a call, then pick up the call from another extension. If the call is forgotten, the **Timeout** sets the number of minutes a call remains parked before the user's extension rings again. To the caller, the call park sounds like being put on hold. Valid entry: 1 – 60 minutes. Select a greeting that the caller will hear before being placed on hold.
Operator Extension and Group Members	Select the extension to be used by the system operator. If the extension number you select is a workgroup or a hunt group, member extensions will show up in the Group Members box. This extension is used in the following applications: • Trunk incall routing • DNIS incall routing • Auto Attendant

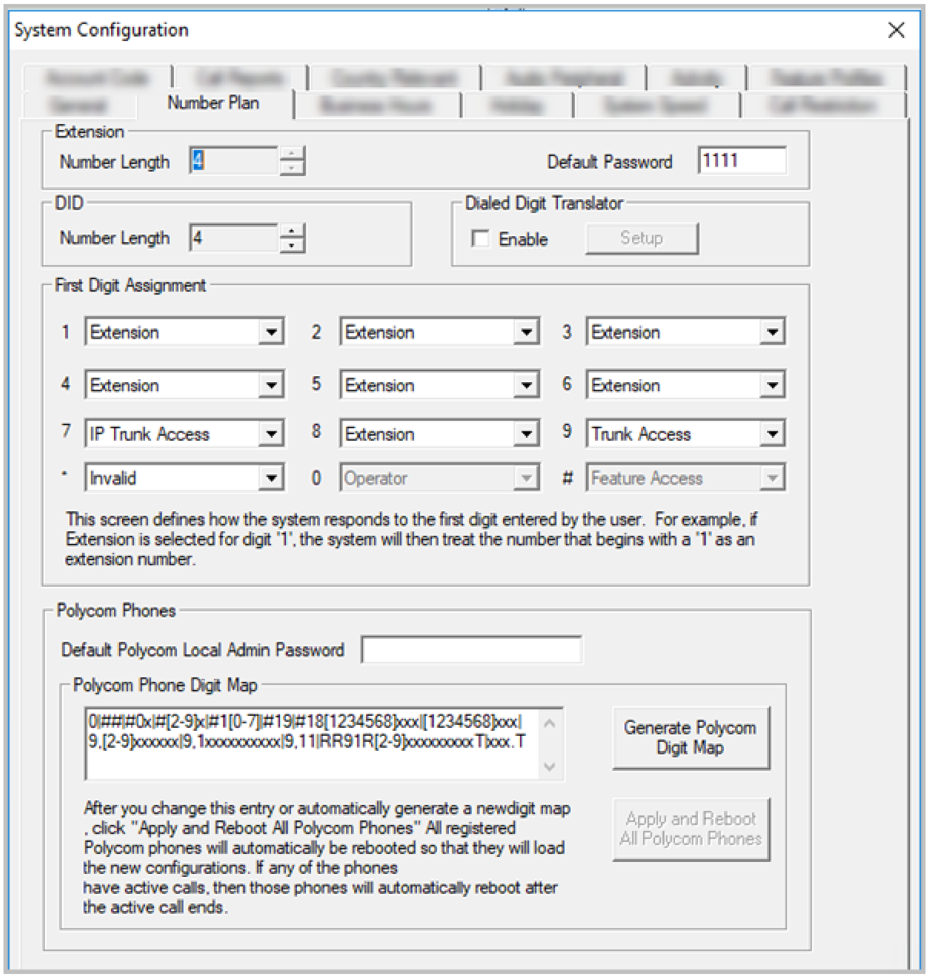
System General Parameter	Description
Call Supervision	Check the box to allow supervisors to monitor, barge in on, coach, and record an agent’s non-workgroup calls. **Notes**: • If this check box is checked, the supervisor can listen, barge-in on, coach, and record an agent's conversation regardless of the agent's login status. • Supervisor extension does not have to be a workgroup member to listen to, barge-in on, coach, or record an agent's conversation. • For the coaching feature, the agent’s extension can be either an IP extension or a Triton analog extension. **WARNING!** Listening in to or recording a conversation without the consent of one or both parties may be a violation of local, state and federal privacy laws. It is the responsibility of the users of this feature to assure they are in compliance with all applicable laws.
TLS Options	A new option allows you to enforce TLS version 1.2 whenever TLS is used. For details, refer to *TLS 1.2 Configuration* on page 413.

Setting a System Number Plan

The system number plan defines the extension digit length. You can use from 3 - 6 digits for extensions. You also use the system number plan to set a DID number length to use, and to define the system response to the first digit dialed — for example, pressing **9** to get a trunk line.

The numbering scheme requires some thoughtful planning.

To set the number plan, select **System** > **System Configuration**, then click the **Number Plan** tab.



Extension
Number Length 4
Default Password 1111

DID
Number Length 4

Dialed Digit Translator
☐ Enable

First Digit Assignment

1	Extension	2	Extension	3	Extension
4	Extension	5	Extension	6	Extension
7	IP Trunk Access	8	Extension	9	Trunk Access
*	Invalid	0	Operator	#	Feature Access

This screen defines how the system responds to the first digit entered by the user. For example, if Extension is selected for digit '1', the system will then treat the number that begins with a '1' as an extension number.

Polycom Phones

Default Polycom Local Admin Password

Polycom Phone Digit Map

```
0|##|#0x|#[2-9]x|#1[0-7]|#19|#18[1234568]xxx|[1234568]xxx|
9,[2-9]xxxxxx|9,1xxxxxxxxxx|9,11|RR91R[2-9]xxxxxxxxxT|xxx.T
```

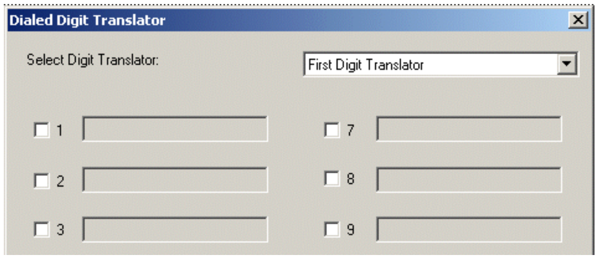
Generate Polycom Digit Map
Apply and Reboot All Polycom Phones

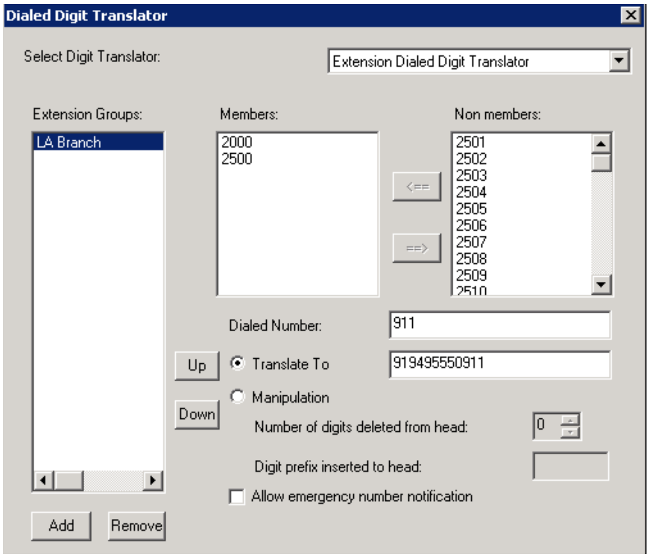
After you change this entry or automatically generate a newdigit map , click "Apply and Reboot All Polycom Phones" All registered Polycom phones will automatically be rebooted so that they will load the new configurations. If any of the phones have active calls, then those phones will automatically reboot after the active call ends.

Figure 13. System Configuration, Number Plan tab

Use the **Number Plan** tab to specify the following parameters:

System Number Plan Parameter	Description
Extension - Number Length	The number of digits for your extension numbering system. Valid entries are from 3 - 6. For example, extension 2001 and 4020 are 4-digit extension numbers. **Note:** Once the first extension is configured, the extension number length *cannot be changed* without totally reconfiguring the system or deleting all the extensions already configured. Further, if a *first digit dialed* is assigned to extensions and you have set up extensions beginning with that digit, you cannot change the digit assignment without first deleting all affected extensions. For example, if **7** is assigned to *Extension* and you're using extensions 7010, 7113, and so on, you cannot reassign **7** to IP trunk access, without first deleting all the 7*nnn* extensions.
Extension - Default Password	The default password for newly created extensions is randomly generated by the system. (When the password is changed, it must meet your password requirements.)

System Number Plan Parameter	Description
DID Number Length	The number of digits needed to match a DID (Direct Inward Dialing) number. The range is from 2 – 16. Each extension can be assigned a DID number. A DID number does not have a fixed length. For example, suppose the DID number length is 4 and the extension DID number is 2522999. Depending on the service contract with the Central Office (CO), the DID trunk can send all 7 digits (2522999) or just the last 4 digits (2999). If the DID Number Length option is set to 4, the system always tries to match the last 4 digits received to the last 4 digits of a DID number, regardless of what is received. **Note**: To accommodate future growth and minimize disturbance, it is recommended that the length of the DID numbers assigned to an extension be greater than or equal to this DID Number Length.
Dialed Digit Translator	This feature is capable of intercepting and manipulating a dialed digit string before it is sent out for outbound call processing. To set up a dialed digit translator entry, check the **Enable** checkbox and click the **Setup** key. This opens a dialog box where you can select **First Digit Translator** or **Extension Dialed Digit Translator**. This feature supersedes the first digit assignment of the system number plan. When configured, any extension user can dial a single DTMF digit that will be translated to any internal or external number. After digit manipulation, the translated digits go through the system number plan to find the internal or external target. For example, you can configure "*" to call an internal workgroup to report an urgent situation. Typical applications are: • One-digit emergency dialing • One-digit dialing to branch or headquarters over PSTN or VoIP • One-digit dialing to activate a feature code
	First Digit Translator Configuration  Select Digit Translator: First Digit Translator Dialed Digit Translator □ 1 □ 2 □ 3 □ 7 □ 8 □ 9 *Figure 14. Single Digit Routing* To set up a **First Digit Translator** entry, select the check box (to the left of 1-9, * or #), then enter the desired digits. When a box is checked, the digit preprocessor will replace the first digit 1-9, * or # that user dials with the digits indicated in the corresponding field. In the above example, if a user dials "*", the system replaces this with "911". **Note:** This feature is for internal extension users only. It does not support dialing out from voice mail. Improper configuration may cause conflict with the system numbering plan. Be sure to fully test any configuration change in this area before going "live."

System Number Plan Parameter	Description
	Extension Dialed Digit Translator **Note:** This feature is intended for, but not limited to, allowing a remote IP extension to make an emergency call (911) through MAXCS. If MAXCS is in a different location than the IP extension, the emergency call can be routed to the emergency center where the IP extension is located.  Dialed Digit Translator Select Digit Translator: Extension Dialed Digit Translator Extension Groups: LA Branch Members: 2000 2500 Non members: 2501 2502 2503 2504 2505 2506 2507 2508 2509 2510 Dialed Number: 911 ● Translate To 919495550911 ○ Manipulation Number of digits deleted from head: 0 Digit prefix inserted to head: □ Allow emergency number notification *Figure 15. Extension Call Routing* To set up an Extension Dialed Digit Translator entry: 1. Select **Extension Dialed Digit Translator** from the **Select Digit Translator** list. 2. In the **Extensions Group** field, use the **Add** button to create and select an extension group that the Extension Dialed Digit Translator will apply to. 3. (optional) From the **Non members** list, you may select an IP extension that the Extension Dialed Digit Translator will apply to. You can apply the same **Members** to multiple locations. You may also enable the **Bypass Account Code** option if Account Codes are required. 4. Enter digits in the **Dialed Number** field and **Translate To** field. In (see Figure 15), assuming the system is located in area code 510, when an IP extension user in LA dials “**911**,” MAXCS will translate the digits into “**919495550911**.” (9 = IP trunk access code, 19495550911 = the emergency center in LA that covers the remote IP phone user’s area.) 5. The **Manipulation** option allows you to remove or add digits to a number dialed by the IP extension. The most common situation requiring this option is to hop-off a VoIP call from a remote system to a remote CO line.

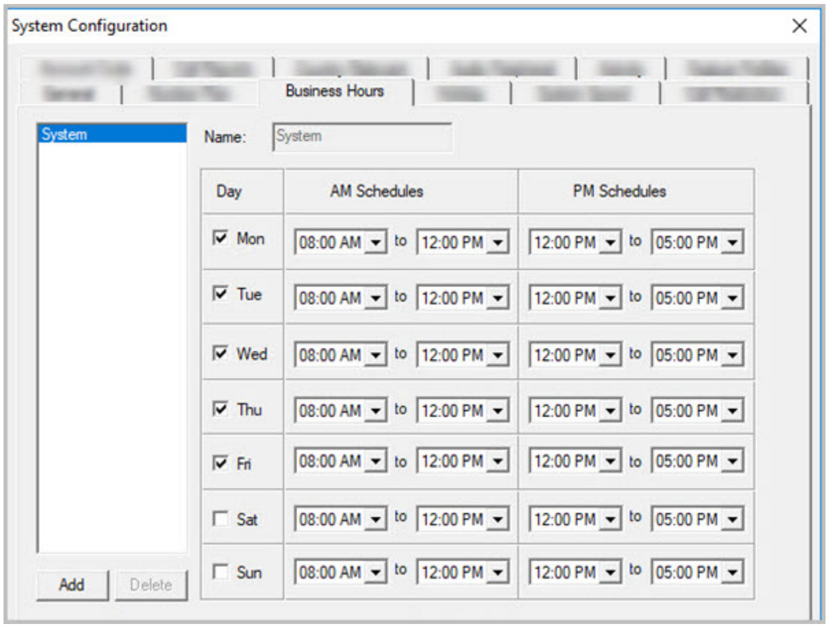
System Number Plan Parameter	Description
First Digit Assignment	These define how the system responds to the first digit dialed by the user. The list options for each digit are: • Extension • Trunk Access • Feature Access • Operator • Invalid (no action) • IP Trunk Access • Route Access **Trunk Access** – Defines how to get a PSTN trunk line to dial an outside number. “9” is the default trunk access code. If you have a more complicated dialing number and routing plan, **change “9” to the Route Access code and configure the Outcall Routing table**. **Feature Access** – By default, **#** is set to Feature Access, which is used as part of feature access codes. In addition, you may also set **1-9** to Feature Access. For example, if **7** is set to Feature Access, Station Login (**#27**) can also be accessed using **727**. **IP Trunk Access** – Only one IP trunk access option is allowed per system. To use Voice over IP, you must set up this access and, in addition, configure the IP Dialing Table as discussed in “Defining the IP Dialing Table” on page 326 and set the VoIP codecs as discussed in “Setting VoIP Codec Profiles” on page 315. **Note:** *After* setting the IP Trunk Access code here, you should set the Trunk Access Codes of any 30-port VoIP boards to “None” on the **General** tab of the Trunk Configuration window (see “Setting General Trunk Attributes” on page 125). This will prevent users from directly accessing the 30-port boards – which use the G.711 codec only – for calls to MAXCS servers or other gateways that may require the G.723 codec. If you still want users to have access to this trunk for outgoing calls, you can set it up through out call routing (see *Chapter 15, Out Call Routing Configuration*). **Route Access** – The Route Access option can be assigned to one or more digits, to route the call per the out call routing table. Out call routing, which is sometimes called ARS (Automatic Route Selection) or LCR (Least Cost Routing without carrier rate table), is described in *Chapter 15, Out Call Routing Configuration*. Out call routing is designed to help 10-digit dialing, Zoomerang dialing, digit manipulation, and tie trunk hop-off dialing.
Default Polycom Local Admin Password	You can change the default Polycom administrator password (which is currently 456). This is the password for the Polycom phone itself; users must enter this password on the phone in order to access menus on the phone to change its configuration. The system will initially generate a random 5-digit string; you can change this to a string between 4 and 32 characters. See the *MAXCS Polycom Configuration Guide* for details.
Polycom Phone Digit Map	See the *MAXCS Polycom Configuration Guide* for details.

Setting Business Hours

The Business Hours tab contains group boxes for setting the business hours and days of the week for which the business or organization is in operation. The business hours schedules are used to set other system settings such as trunk, and DNIS and caller ID in-call routing.

Note: Because the business hours are used throughout the system, you or the appropriate administrator must ***make sure the system time has been set correctly***. The system time can be changed using the **Date** and **Time** options in the Windows Control Panel.

To access the Business Hours settings, select **System** > **System Configuration**, then click the **Business Hours** tab.



Name: System

Day	AM Schedules			PM Schedules		
☑ Mon	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
☑ Tue	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
☑ Wed	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
☑ Thu	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
☑ Fri	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
□ Sat	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM
□ Sun	08:00 AM	to	12:00 PM	12:00 PM	to	05:00 PM

Figure 16. System Configuration, Business Hours tab

Multiple Business Hours profiles can be configured in a system. A default "System" Business Hours profile is already configured. Multiple Business Hours profiles can also be assigned to DNIS Routing and Trunk In Call Routing entries.

To add a new Business Hours profile, click **Add**. Enter a name for the profile, then click **OK**.

For each business hour profile, set the business schedule parameters.

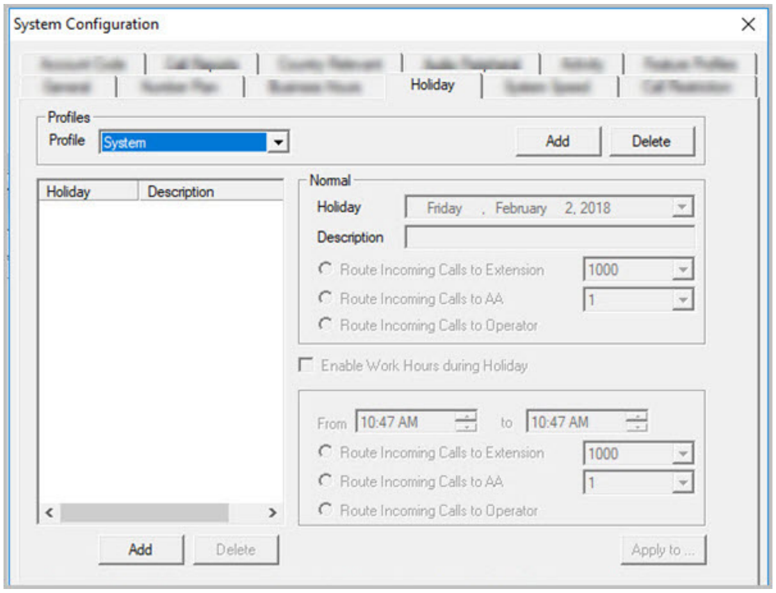
System Business Hours Parameter	Description
Day	Select the days of the week on which the company does business. For example, if the company does business Monday – Friday, check the check boxes for those days.
AM and PM Schedules	For each day of the week, select the time periods during which the company is available for business. The time between the AM and PM times can be used to indicate a lunch break or time between shifts. If you don't want to set a break between AM and PM schedules, set the PM starting time to be the same as the AM ending time. Or if you want to specify 24 hours as standard business hours, select the following hours: AM Schedules: From 08:00 AM to 12:00 PM PM Schedules: From 12:00 PM to 08:00 AM

Routing Calls on Holidays

You can create special routes for incoming DNIS and trunk calls that come in on designated holidays. For holidays that your organization treats as half-days, you can create separate profiles for business and non-business hours.

Note: Incoming DID and tie trunk calls will not follow holiday routes, but go to the dialed extensions directly.

To configure Holiday routing rules, select **System** > **System Configuration**, and then click the **Holiday** tab.


System Configuration

Profiles

Profile: System

Normal

Holiday: Friday , February 2, 2018

Description:

○ Route Incoming Calls to Extension: 1000

○ Route Incoming Calls to AA: 1

○ Route Incoming Calls to Operator

□ Enable Work Hours during Holiday

From 10:47 AM to 10:47 AM

○ Route Incoming Calls to Extension: 1000

○ Route Incoming Calls to AA: 1

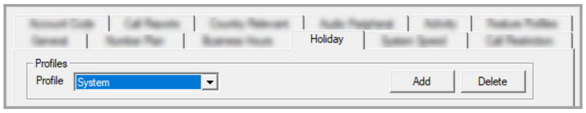
○ Route Incoming Calls to Operator

Figure 17. System Configuration, Holiday tab

Multiple Holiday Profiles can be configured in a system. Each Holiday Profile can include multiple holidays. A default “System” Holiday profile is already configured. Multiple Holiday Profiles can also be assigned to DNIS Routing and Trunk In Call Routing entries.

Creating a Holiday Profile

1. Click the **Add** button beside **Profile**. Enter a name for the profile, then click **OK**.
2. To each profile, add holidays that will be included in that profile: Click the **Add** button below the **Holiday** list to create a new holiday.
3. In the dialog box, select a date from the calendar and enter a description. Click **OK**.


Profiles

Profile: System

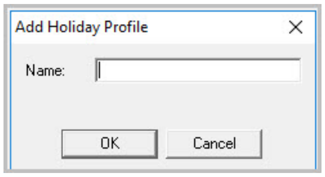


Figure 18. Adding a holiday to a profile

The holiday you added appears in the **Holiday** list. Additional holidays you create appear in the list and together make up the Holiday Profile.

Setting Call Routing Rules for a Holiday

1. Select a Holiday Profile from the **Profile** list, and then select a holiday in that profile from the **Holiday** list.
2. Set call routing for “normal” holiday hours using the field group in the **Normal** section of the Holiday tab. This will be the default route for calls coming in on that holiday.
3. If you have special work hours during holidays, check the **Enable Work Hours during Holiday** option and configure special hour routing.

   This route will override the route for normal holiday hours, for the hours you specify. Use this option, for example, to route calls for the working portion of a holiday that your organization treats as a half-day.
4. To apply these hours to more than one holiday, click the **Apply To** button and in the **Apply To** dialog box, select all the holidays to which you want the hours to apply. You can select multiple holidays by using **Ctrl-click** or **Shift-click**. Click **OK**.
5. When you are finished with the dialog box, click **OK**.

When a new year begins, the dates on which holidays fall usually change. You can edit the dates for annual holidays, making them accurate for the new year.

Updating the Dates of Annual Holidays

1. Select a Holiday Profile, and then the holiday from the **Holiday** list. Its date and description appear in the **Normal** section.
2. Click the drop-down arrow beside the date to open a calendar and assign a new date. Click **Apply**.

Exception Routing

In earlier releases of MaxCS you could create holiday routing rules for full days, and you could create business hours for specific days of the week and weekends.

Starting with Release 8.6.1, your ability to route calls has been expanded. MaxAdmin has a new tab, *Exception Routing*. Exception routing rules can be entered for a specific period of a specific day. One example of this would be for a company meeting lasting 1 hour on a specific date. Or perhaps a company training session that lasts the morning of a specific date.

Considerations:

- You can add multiple exception routing rules, even for the same date and time.
- Exception routing rules can have one or more DNIS numbers.

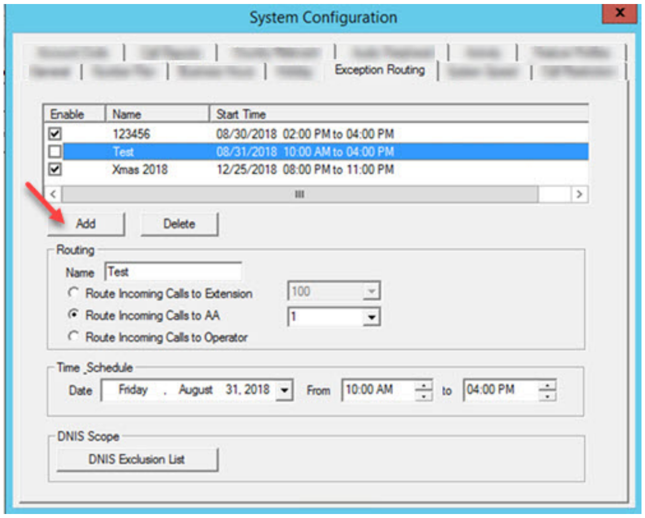
Routing Precedence

- Exception routing rules have precedence over Holiday Profile definitions.
- Holiday Profile definitions have precedence over Business Hours settings.

Creating Exception Routing Rules

To create a new routing rule,

1. In MaxAdmin, select **System** > **System Configuration** > **Exception Routing**. This tab shows you routing rules that have already been configured.
2. To add a new rule, click the **Add** button below the list of rules.
3. In the *Routing* section below the table, enter a name for this rule. We recommend that you use a unique and descriptive name that will make it easy to identify among other rules.



Enable	Name	Start Time
☑	123456	08/30/2018 02:00 PM to 04:00 PM
□	Test	08/31/2018 10:00 AM to 04:00 PM
☑	Xmas 2018	12/25/2018 08:00 PM to 11:00 PM

Routing

Name: Test

○ Route Incoming Calls to Extension: 100

● Route Incoming Calls to AA: 1

○ Route Incoming Calls to Operator

Time Schedule

Date: Friday , August 31, 2018 From: 10:00 AM to: 04:00 PM

DNIS Scope

Figure 19. The Exception Routing tab

4. Choose a routing option:

- **Route Incoming Calls to Extension** - Enter or select the extension for calls during this period.
- **Route Incoming Calls to AA** - Select the AA for calls during this period
- **Route Incoming Calls to Operator** - Routes calls to the Operator during this period.

5. Set the schedule for this routing rule by selecting the date and then specifying the beginning and ending of this period.
6. (Optional) If you want to exclude certain numbers from this routing rule, click **DNIS Exclusion List**. In the next panel, you can add and remove DNIS numbers to / from the Exclusion list. Numbers that you place on the Exclusion list will ignore the rules in this routing rule.
7. Save your changes.

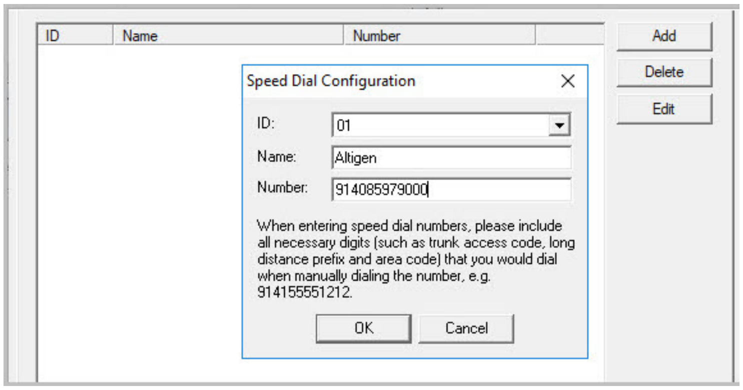
To enable or disable an individual exception routing rule, check or clear its Enable checkbox. To delete a routing rule, select the rule and click **Delete**.

Configuring System Speed Dialing

You can set up to 60 system speed dial numbers. The IDs available are from 00 – 59. Users press #88, and follow that with one of the system speed dial access codes you set here.

Speed dial settings for individual extensions are set in Extension Configuration. (See "Setting up Station Speed Dialing" on page 178.)

To configure Speed Dialing, select **System** > **System Configuration**, and then click the **System Speed** tab.



ID: 01

Name: Altigen

Number: 914085979000

When entering speed dial numbers, please include all necessary digits (such as trunk access code, long distance prefix and area code) that you would dial when manually dialing the number, e.g. 914155551212.

Figure 20. System Configuration, System Speed tab

Adding Speed Dial Entries

To add a speed dial entry,

1. Click **Add**.
2. The next available ID is filled in for you, or you can select the ID number using the drop-down arrow.
3. Type a name for the Speed Dial entry, then enter the full number as you would dial it, with a maximum of 20 digits per entry. For example, the phone number 914085551212 comprises **9** (trunk access code), **1** (long distance prefix), followed by **408** (area code), and then the seven-digit telephone number.

   Valid digits include **0** through **9**, **#**, *****, and **(,)** comma. **The comma represents a one-second pause**, when IP trunks are not used.

Editing Speed Dial Entries

To edit an entry, double-click the number you want to work with, or select the number and click **Edit**. In the dialog box that opens, edit the entry and click **OK.**

To delete a system speed dial entry, select it in the System Speed tab and click **Delete**.

Note: System speed dial is read-only from MAXCS and MaxAgent.

Defining System Call Restrictions

The **Call Restriction** tab contains settings for the following functions:

- Block calls to area codes from all extensions
- Define local/toll-free (unrestricted) area codes
- Lock an attacked extension
- Block all outgoing trunk calls

- Restrict other system users from hopping-off to make an outbound call via a tie trunk
- Set 10-digit dialing area codes for using trunk access code

To set up call restrictions, select **System > System Configuration**, then click the **Call Restriction** tab.

Figure 21. System Configuration, Call Restriction tab

Blocking Calls to Area Codes from All Extensions

To add or edit system-prohibited area codes:

1. Double-click an index entry in **System Prohibited Prefixes** list, or select the index entry and click **Edit**. This opens a dialog box that allows you to enter a prefix number.
2. Enter a **1** and the dialing prefix to block (for example, 900, 976). You can enter up to 20 digits maximum for each prefix. For example, to block calls from all extensions to 976 numbers, type 1976. Click **Apply**.

Note: A maximum of 20 prefixes can be defined.

Setting Unrestricted Area Codes

To add or remove “local” call definitions (including calls that begin with 1 but are free: 800, 888), use the **Add** or **Delete** button in the Unrestricted Area Code panel, and click **Apply**. The **Extension Configuration**’s **Restriction** tab references these area codes (as local and unrestricted) in its Outcall Restrictions panel.

Setting the Extension Lockout Period

If a user enters too many consecutive invalid passwords when logging on to voice mail or to activate an extension, MAXCS considers this an attack.

To protect your company from theft of services, you can lock an attacked extension for the period of time you specify (1-72 hours) in the **Lock Extension Access** section.

As of Release 9.0.1 1he default lockout period is 23 hours. You can enter a value from 1-72 hours (or select *Permanent*). If you had entered a lockout period in hours:minutes:seconds format in earlier releases of MaxCS, your entry will be rounded up to the nearest hour once you upgrade to Release 9.0.1.

If you set the lockout period to *Permanent*, then the only way to unlock a locked extension is to use Extension Checker. (MaxCS Admin & Extension Security Checker is a separate tool provided with MaxCS.)

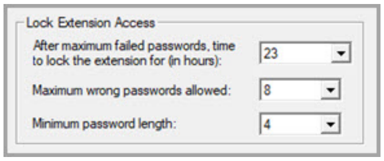
Setting the Maximum Allowed Password Attempts

To adjust how many incorrect password attempts are allowed before an extension is locked, use the *Maximum wrong passwords allowed* option on the *Call Restrictions* tab. This option was moved from Extension Checker in Release 9.0.

Setting Minimum Password Lengths

You can set a long minimum password length for stronger security. As of Release 9.0.1, the default minimum password length is 8 digits.

Note that it is possible to set a system minimum password length that is longer than some users' current passwords. In this case, when the user tries to log in, the system will indicate that the password has expired and will prompt the user to change it.



Lock Extension Access

After maximum failed passwords, time to lock the extension for (in hours): 23

Maximum wrong passwords allowed: 8

Minimum password length: 4

Figure 22. The Lock Extension Access options

To unlock a locked extension, use the Extension Checker tool that is installed with MAXCS. See “MaxCS Admin & Extension Security Checker” on page 388.

Extension Checker Updates

Extension Checker now checks the password length for both the extension password and the SIP Registration password. It will display a warning if a password is shorter than the minimum length required. In addition, Extension Checker now shows an additional column for the SIP registration password length.

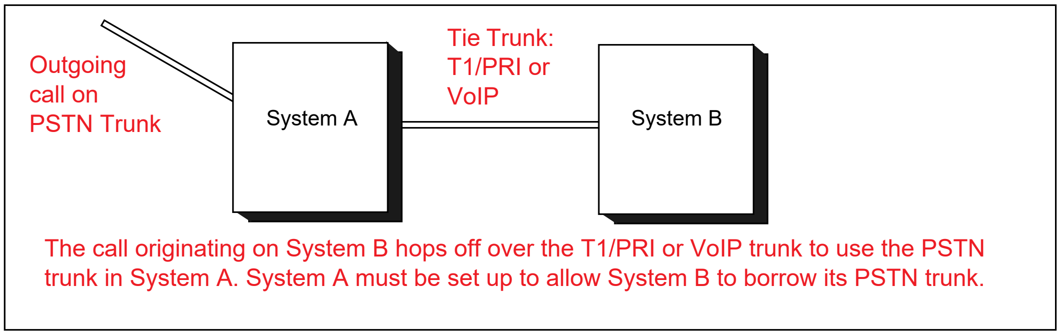
ExtChecker.exe will be bundled with the MaxAdministrator installation, so in default remote MaxAdministator installations, there will be an ExtChecker.exe located in C:\Program Files (x86)\AltiGen\AltiWare Administrator.

Blocking All Outgoing Calls

To block all outgoing calls – for example, during the night when no employee is in the office – check the **Block All Outgoing Calls** check box. If you block all outgoing calls, then calls between two systems will not go through. This is because #38 blocks all trunks, including remote SIP-tie trunks

Enabling Hop Off for Tie Trunks

When selected, this function allows users from another system to borrow a PSTN trunk in this system to make an outbound call over a VoIP tie trunk.



The call originating on System B hops off over the T1/PRI or VoIP trunk to use the PSTN trunk in System A. System A must be set up to allow System B to borrow its PSTN trunk.

Figure 23. Hop Off for Tie Trunks

Restricting Tie Trunk Calls

You can set call restrictions on hop-off calls by telling the system to use the same restrictions as the ones set up for an extension. Using the **Call restriction follows extension** list, you can select the extension with the restrictions to use for the hop-off calls.

Setting 10-Digit Dialing Area Codes

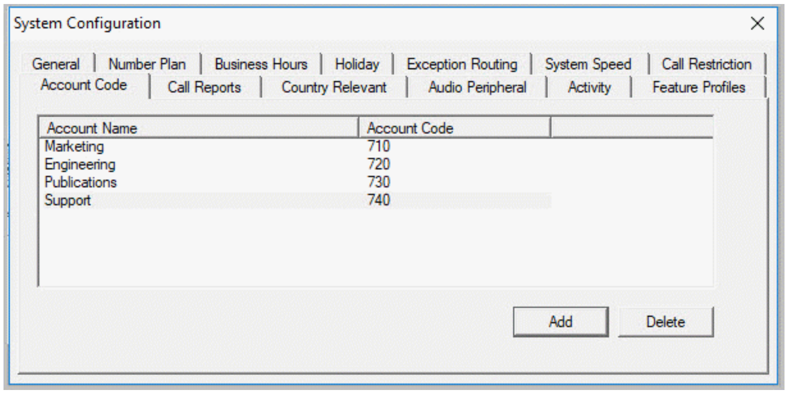
The **Trunk Access 10-Digit Dialing Area Code** field lets you define area codes that do not require dialing a “1” before the area code. To enter an area code, click the **Add** button.

Note: Applies only to calls that use a trunk access code. For calls using a route access code, 10-digit dialing area codes must be configured in the Out Call Routing Configuration window, Dialing Pattern tab. See “About Dialing Patterns” on page 160.

Creating Account Codes

Account Codes let you enable or force users to assign incoming and outgoing calls to particular account codes for billing, tracking, or forecasting purposes. Up to 10,000 account codes can be created.

To access the Account Code tab, select **System** > **System Configuration**, then click the **Account Code** tab.



Account Name	Account Code
Marketing	710
Engineering	720
Publications	730
Support	740

Figure 24. System Configuration, Account Code tab

Adding and Deleting Account Codes

To create an account/code association, click **Add**. Enter an Account Name and Account Code in the dialog box. The Account Code may contain 1-10 digits.

To delete an account and its code, select it and click **Delete**. You can select multiple items for deletion by using **Ctrl-click** or **Shift-click.** Click **Apply** to save your changes and **OK** to save and close the window.

You can now set options for each extension that determine whether account codes must be entered or can be bypassed. You can also block display of the Account Code table (in which case, you would want to supply users with the account codes they need). See “Setting Personal Information” on page 169.

Setting up Call Reports

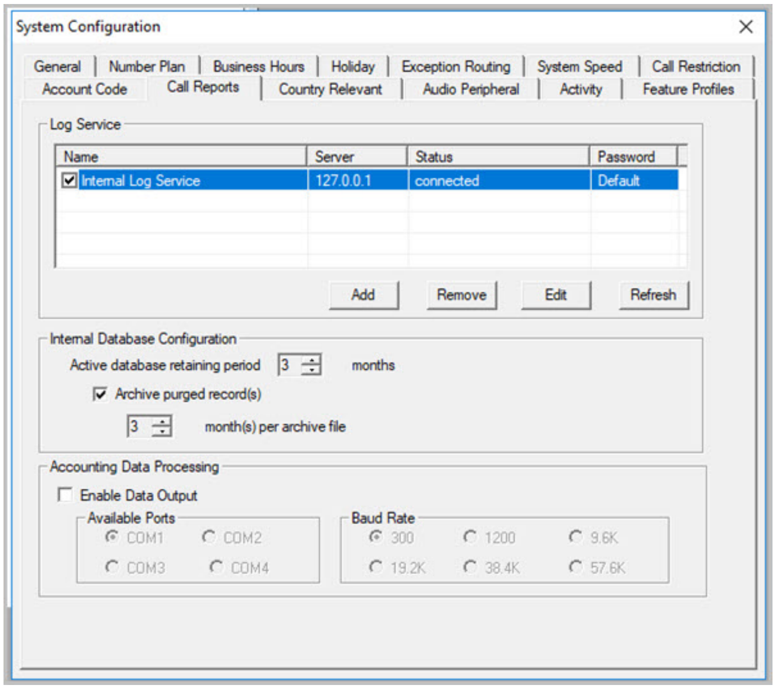
You can set up the call report logging option only if MAXCS and MaxAdministrator are installed on the same server.

On the **Call Reports** tab, specify the following:

- Where to log the call detail records (CDR). The location can be an internal database, an external database, or both.
- How you want the system to manage an internal CDR database.
- If CDR needs to be output through a COM port to another computer, which COM port and which baud rate to use.

To learn more about internal and external CDR databases and schema, refer to the *Call Detail Reporting Manual*.

To set up Call Reports, select **System** > **System Configuration**, then click the **Call Reports** tab.



Log Service

Name	Server	Status	Password
☑ Internal Log Service	127.0.0.1	connected	Default

Internal Database Configuration

Active database retaining period 3 months

☑ Archive purged record(s)

3 month(s) per archive file

Accounting Data Processing

□ Enable Data Output

Available Ports: ● COM1 ○ COM2 ○ COM3 ○ COM4

Baud Rate: ● 300 ○ 1200 ○ 9.6K ○ 19.2K ○ 38.4K ○ 57.6K

Figure 25. System Configuration, Call Reports tab

Internal Database Configuration (Internal Log Service)

The Internal Log Service (shown in the **Log Service** display table) is created by default. You can enable or disable the service, but you cannot remove this database or add another Internal Log Service.

To manage the internal CDR database:

1. Make sure the **Internal Log Service** check box is checked.
2. In the Internal Database Configuration field, use the up/down arrows to select the **Active database retaining period** in months. This determines how long the data will be kept in the database. Valid entry is 1-12 months.
3. (Optional) In the **Archive purged record(s)** field, use the up/down arrows to select the number of months per archive file. This determines the number of months that the system will archive an existing CDR database before creating a new database.
4. Press **OK** or **Apply**.

External (Remote) Logging of Call Data

MAXCS allows you to output CDR records to a Microsoft SQL Server database (“Minimum System Requirements” on page 9 lists the versions of SQL Server that are supported). Before you enable external logging, you need to set up and configure the SQL database and external logger application. Please refer to the *CDR Search Manual* to learn how to set up an external logger service.

Some considerations:

- The SQL database cannot be on the same server as the MAXCS system. A system integrator or database developer will need to write a custom query to extract data from the SQL database.
- You can send reports from a number of different systems to the same database.

- Altigen does not provide any SQL backup and restore utility. We strongly recommend that you use SQL Backup and Maintenance utility to perform daily backup and maintenance jobs, and use a restore utility to restore the database. If you need to reconstruct the SQL server, run the External Logger Setup to create an empty calldb database before restore.
- There is no Altigen license required for external logging.

To set up and enable external CDR login service to the local or network drive, click **Add**. Fill in the fields, and click **OK**.

Parameter	Description
Name	The name of the external log service machine (optional)
Address	The IP address of the external log service machine
Port	The TCP port of the machine
Password	The password to connect to the external service machine

Exporting Through a Local Port

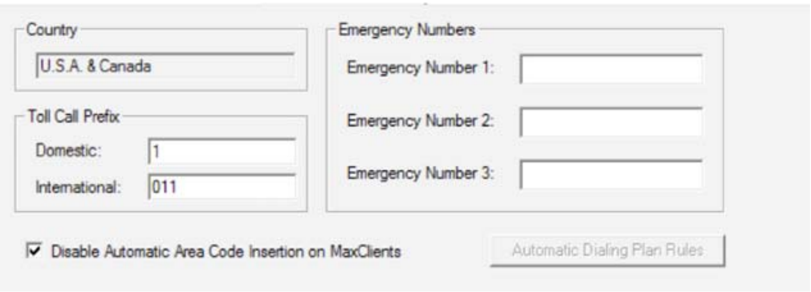
You can send the CDR to a COM Port to export to, for example, a call accounting data processing system.

To do this, select the **Enable Data Output** box in the **Accounting Data Processing** section. Then select an **Available Port** and the **Baud Rate**.

Country-Relevant Settings

The **Country Relevant** tab in the **System Configuration** window contains group boxes for setting toll call prefixes and emergency numbers.

The **Country** field displays the country selected on the System Configuration, General tab.



Country

U.S.A. & Canada

Toll Call Prefix

Domestic: 1

International: 011

Emergency Numbers

Emergency Number 1:

Emergency Number 2:

Emergency Number 3:

☑ Disable Automatic Area Code Insertion on MaxClients

Figure 26. System Configuration, Country Relevant tab

Note that if your system is not in North America, then the Automatic Dialing Plan Rules button will not be available.

Setting Toll Call Prefixes

MAXCS uses **Toll Call Prefixes** to determine the type of outside call and imposes restrictions when necessary. For example, if the international toll call prefix is **011** and a user attempts to make an international call from an extension without international call privileges, the call will be terminated as soon as the user dials **011** after the trunk or route access number. The caller hears an error tone.

The toll prefixes set here should match the dialing plan prefixes for the country set in the General tab (see “Setting General Parameters” on page 31). You can set the following toll call prefixes.

- **Domestic**. The dialing plan for your country’s domestic long distance prefix. For example, type in a **1** for 1-plus dialing within the U.S. dialing plan (also known as the North American Numbering Plan).
- **International**. The prefix used for international calls. For example, this is **011** for international calls made in the U.S.

Setting Emergency Numbers

The number in the **Emergency Number** field will have the system automatically find a trunk to process the call without the extension user dialing a trunk access code first. You may enter up to three emergency numbers in the appropriate fields.

This feature works with both trunk access code and route access code.

Important: Make sure that you review Altigen Knowledgebase article 1203 for instructions on E911 DID testing on Altigen SIP trunks.It describes how E911 can be confirmed to be configured correctly without incurring charges from testing.

Disabling Automatic Area Code Insertion in Max Client

If you check this option and Disable Auto Format is not checked in Max Client, auto adding area code and access code for all MaxClient users is disabled.

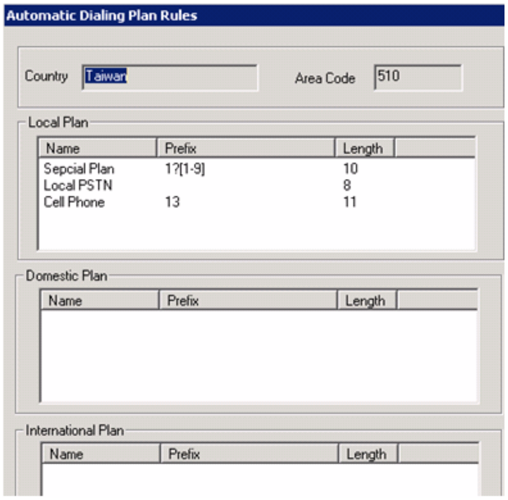
If Disable Auto Format is checked in Max Client, setting this option on the Admin has no effect.

Note: This option only affects US systems.

Dialing Plan Rules for Non-North American Country

If your MAXCS system is in a country other than the U.S.A. or Canada, you can configure a call return rule based on the country, which will greatly improve the call return feature from Caller ID, Zoomerang, and making a call from Microsoft Outlook.

Click the **Automatic Dialing Plan Rules** button.



Automatic Dialing Plan Rules

Country: Taiwan

Area Code: 510

Local Plan

Name	Prefix	Length
Sepcial Plan	1?[1-9]	10
Local PSTN		8
Cell Phone	13	11

Domestic Plan

Name	Prefix	Length

International Plan

Name	Prefix	Length

Figure 27. Automatic Dialing Plan Rules dialog box

Define the Local Plan, Domestic Plan, and International Plan. A character of the pattern can be a digit from 0 to 9. It can also be a range of digits, for example, [0-3]. If it is a question mark, '?', it is equivalent to [0-9].

When return calls are made, these rules are followed:

- When the number matches Local Plan, the system will send the number out to the trunk directly.
- When the number matches the Domestic Plan, the system will send the number out with the domestic toll call prefix.
- When the number matches the International Plan, the system will send the number out with the international toll call prefix.

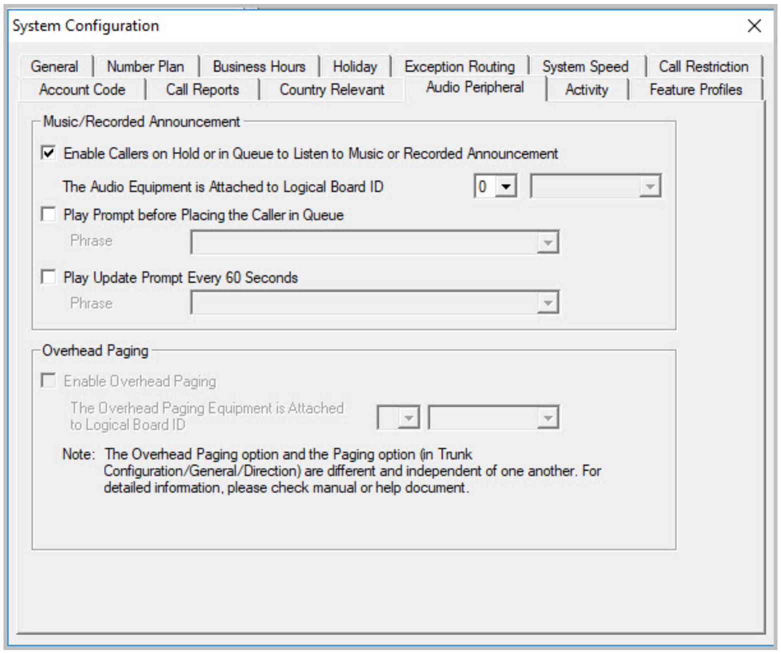
When a number matches multiple entries, the match with the most digits has priority.

Audio Peripheral Configuration

You can configure audio peripheral settings:

- Music on hold
- System default beginning and update prompts for callers in queue

To access the **Audio Peripheral** configuration window, select **System** > **System Configuration**, then click the **Audio Peripheral** tab.



Music/Recorded Announcement

☑ Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement

The Audio Equipment is Attached to Logical Board ID 0

□ Play Prompt before Placing the Caller in Queue

Phrase

□ Play Update Prompt Every 60 Seconds

Phrase

Overhead Paging

□ Enable Overhead Paging

The Overhead Paging Equipment is Attached to Logical Board ID

Note: The Overhead Paging option and the Paging option (in Trunk Configuration/General/Direction) are different and independent of one another. For detailed information, please check manual or help document.

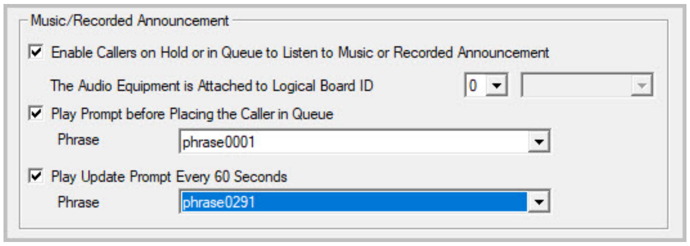
Figure 28. System Configuration, Audio Peripheral tab

Configuring Music On Hold and Recorded Announcements

Callers will hear the music or recorded announcement configured on this tab *only* if the user places the caller on hold.

To configure music on hold when using audio equipment,

1. Check **Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement**.
2. Select the Triton Analog Station board number to which the audio equipment is attached.



Music/Recorded Announcement

☑ Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement

The Audio Equipment is Attached to Logical Board ID 0

☑ Play Prompt before Placing the Caller in Queue

Phrase phrase0001

☑ Play Update Prompt Every 60 Seconds

Phrase phrase0291

Figure 29. Select phrase file for prompts

To configure music on hold to play a file,

1. Make sure a VoIP board is installed (required for playing a file).
2. Check **Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement**.
3. Use the list to select the logical board ID of the VoIP board.

   The system will play the default music-on-hold file when the user places the caller on hold.

The default music-on-hold file is a .wav file called “MusicOnWaiting.wav”. The file is located in the C:\PostOffice\phrases\Music folder. You can replace the file with a .wav file (or an Altigen PCM file). The .wav file must be in 8 kHz/ 8 bit/ Mono/ u-Law format. Any optional music-on-hold files included with MAXCS are in that format.

Note: You may need to reduce the music volume level 70-80% to avoid distortion.

To replace the default music-on-hold file,

1. Back up the default file.
2. On the **Audio Peripheral** tab, uncheck the **Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement** check box.
3. Rename the desired .wav file to “MusicOnWaiting.wav” and put it in the C:\PostOffice\phrases\Music folder.
4. On the **Audio Peripheral** tab, check the **Enable Callers on Hold or in Queue to Listen to Music or Recorded Announcement** check box.

Note: If you have two files named MusicOnWaiting in the MusicOnWaiting folder, one a .wav file and one a PCM file, the .wav file takes precedence.

RTP Resource Usage

In the event that MAXCS is controlling multiple gateway systems, the music source can come from the primary system or another gateway system. When a music source is in one gateway and listeners are in another gateway, one VoIP resource channel in each gateway is used to convey the music stream.

Setting Greeting and Update Prompts

To play a prompt before placing the caller into a hold queue,

1. Select the **Play Prompt Before Placing the Caller in Queue** check box.
2. Use the list to select the prompt number you want to use for the greeting message. (Creating prompts is discussed in “Phrase Management” on page 67.)

To play an update prompt every 60 seconds,

1. Check the **Play Update Prompt Every 60 Seconds** check box.
2. Use the list to select the prompt number you want to use for the greeting message.

Note: These settings will be used by all hunt groups and workgroups as the default system queue phrase. However, these settings will be overridden by the workgroup’s queue management phrase setting.

Configuring Overhead Paging

Note: This feature is not supported in the MAXCS Private Cloud service.

1. Connect overhead paging equipment to the audio out jack on a Triton telephony board.
2. On the **System Configuration > Audio Peripheral** tab, select **Enable Overhead Paging.**

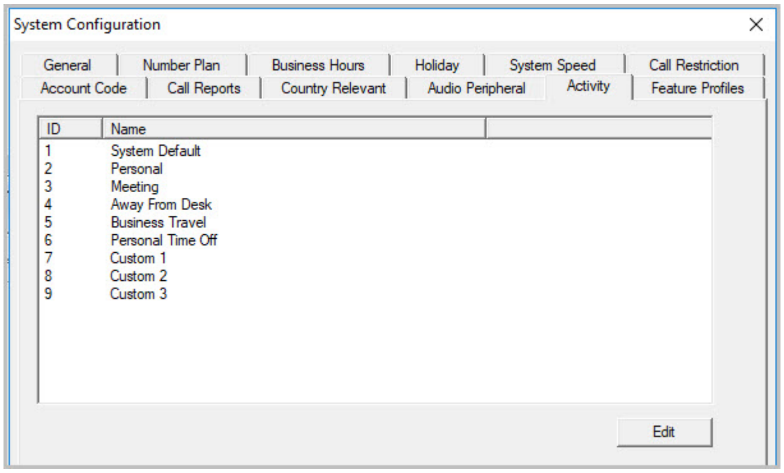
Use the list to select the board to which the overhead paging is attached.

Activity Tab

The **Activity** configuration tab is used to configure activity codes that can be displayed at AltiConsole when the extension user is absent. MaxCommunicator users, MaxAgent users and Altigen IP phone users can select from these activity codes to let others know where they are when they are away from their desks (meeting, business travel, and so on).

A greeting associated with the activity can be recorded and played to the caller. When the user changes the Activity, the extension’s greeting is also automatically changed to the greeting associated with this activity.

To access **Activity** configuration, select **System > System Configuration**, then click the **Activity** tab.



ID	Name
1	System Default
2	Personal
3	Meeting
4	Away From Desk
5	Business Travel
6	Personal Time Off
7	Custom 1
8	Custom 2
9	Custom 3

Figure 30. System Configuration, Activity tab

There are a total of nine activity codes; the first six are pre-configured as follows:

1 – System Default, 2 – Personal, 3 – Meeting, 4 – Away From Desk,
5 – Business Travel, 6 – Personal Time Off

The remaining three activity codes (7, 8, 9) are not assigned and can be customized by the administrator. To customize an activity code, click on the activity code and click **Edit**.

In the **Edit Activity** dialog box, enter name of the Activity and click **OK**.

Feature Profiles

Select **System** > **System Configuration**, then click the **Feature Profiles** tab to configure feature profiles.

The **Feature Profiles** configuration tab allows the system administrator to create an extension feature profile that includes enabling or disabling of the following extension features:

Altigen Voice Mail:

## <pwd> – Login to VM
#14 – Personal Options

Making Calls:

#34 – Dial by Name
#35 – Station Privilege Override
#93 – Intercom

Answering Calls:

#29 – Individual Call Pickup
#30 – System Call Pickup
#31 – Personal Call Park
#41 – System Call Park
#51 – Line Park Pickup
#81 – Hands Free Mode *
#82 – Dial Tone Disabled *

Call Management:

#17 – Polycom Phone Device Override (#17 requires a SIP-Tie trunk to communicate with the server)
#26 – Station Logout *
#27 – Station Login *
#32 – Enter Account Code

#33 – Do Not Disturb
#36 – Call Forwarding
#37 – Remote Call Forwarding

Other Features:

#12 – Language Setting *
#38 – Outside Call Blocking
#39 – Operator Offline
#44 – Overhead Paging *
#45 – Overhead Paging by Trunk *
#46 – Group Paging *
#53 – Outgoing Workgroup
#54 – Login Workgroup
#56 – Logout Workgroup
#59 – Workgroup Call Monitor
#66 – Trace Collection
#73 – Silent System Call Park
#90 – READY to Receive Workgroup Call
#91 – NOT READY to Receive Workgroup Call

* *Feature is not supported by Polycom IP phones*

Note: If the extension is an IP extension, **#26** / **#27** is still available when the phone is in the onhook position, even if it is disabled in the extension's feature profile.

Adding Feature Profiles

By default, a **System** feature profile is assigned as **0**. To add a new Feature Profile, click the **Add** button and type a name for the feature profile.

Note: When adding a feature profile, the system will automatically assign the lowest available number.

Select the check boxes for the MAXCS feature codes that you want to be associated with this feature profile, then click **Apply**.

After the System Administrator creates a **Feature Profile**, the **Feature Profile** can be assigned to a specific extension from the **General** page of **Extension Configuration**. (See "Setting Personal Information" on page 169 for more information on assigning a feature profile to an extension.)

Important: If you assign a feature profile (for example: *2 – Sales Group*) to an extension in Extension Configuration, and that feature profile is subsequently deleted and a new feature profile is created that uses the same number (for example: *2 – Marketing Group*), the extension will automatically be assigned to the new feature profile. So, it is important to note which extensions are assigned to certain feature profiles, especially when adding new profiles or deleting old ones.

Notes

You should include #26 (Station Logout) in a feature profile assigned to an Altigen IP phone. If #26 is *dis*abled in that phone's feature profile, phone registration issues arise.

TRUSTID Configuration

A new feature is available in relese 9.0 – TRUSTID. This new feature, which requires a new license, is documented in a separate guide, the *TrustID Guide*.

CHAPTER

5

Voice Mail Configuration

Use the **Voice Mail Configuration** window to control the following:

- How the system processes voice mail notification
- How the system processes voice mail deletion and expired messages
- How the system records voice mail, system phrases, custom phrases, personal greetings, directory name recording, and queue phrases
- Enable or disable SMTP/POP3 service to deliver voice mail to an e-mail address as an attachment
- Enable or disable Microsoft Exchange synchronization service, or select Exchange's bridged access or native VM integration with Exchange's Automated Attendant or Unified Messaging Server

As of Release 9.0.1, users must press the # key to indicate the end of the password entry process. In earlier releases, users could enter only the password to log in.

For example, if a user's password is 215783, the user must now end the sequence with the # key: 215783#.

The system will play a prompt to alert users to the new behavior.

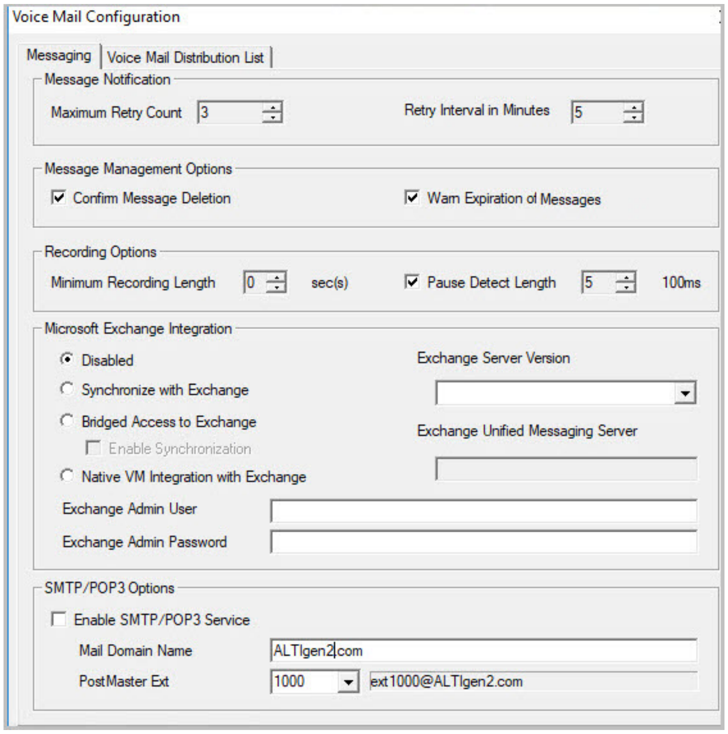
Note: A built-in throttle checks the amount of available disk space before allowing users to record a call. If the available space on the hard disk is less than 10% of the total space, the system will warn the caller that there is not enough room to record the call, and the call will not be recorded. This default threshold, 90%, can be adjusted (between 50% to 95%) by modifying a registry entry: HKLM\SOFTWARE\Wow6432Node\AltiGen Communications, Inc.\AltiWare\DiskSpace; the default value is DWORD 90.

To open the Voice Mail Configuration window, select **System** > **Voice Mail Configuration**.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

Managing Messages

The Messaging tab in the Voice Mail Configuration window provides for setting basic parameters and options for messaging, including message notification retry attempts, message management options, recording options, and e-mail activation and usage.



Voice Mail Configuration

Messaging | Voice Mail Distribution List

Message Notification

Maximum Retry Count: 3

Retry Interval in Minutes: 5

Message Management Options

☑ Confirm Message Deletion

☑ Warn Expiration of Messages

Recording Options

Minimum Recording Length: 0 sec(s)

☑ Pause Detect Length: 5 100ms

Microsoft Exchange Integration

● Disabled

○ Synchronize with Exchange

○ Bridged Access to Exchange

□ Enable Synchronization

○ Native VM Integration with Exchange

Exchange Server Version:

Exchange Unified Messaging Server:

Exchange Admin User:

Exchange Admin Password:

SMTP/POP3 Options

□ Enable SMTP/POP3 Service

Mail Domain Name: ALTIgen2.com

PostMaster Ext: 1000 ext1000@ALTIgen2.com

Figure 31. Voice Mail Configuration, Messaging tab

Setting Message Notification Retries

When a message is sent to a user’s voice mailbox and outcall notification is configured, the system will try to call a phone number, pager, or an extension to deliver notification. You can set the retry setting for the notification as follows:

Message Notification Parameter	Description
Maximum Retry Count	Can be between **0** and **16**. This is the number of times the system will try to deliver a voice message notification *after* the original attempt. For example, **5** retries means five tries after the original, or 6 total attempts.
Retry Interval in Minutes	The number of **minutes** between retry attempts. Five minutes is the minimum and 60 minutes is the maximum interval allowed. Choices are in 5-minute increments. The default is 5 minutes.

Setting Message Management Options

Set voice mail message confirmation and warning parameters:

Message Management Parameter	Description
Confirm Message Deletion	If checked, the system plays a voice message instructing the user to confirm request for deletion by pressing the # key. This prevents users from accidentally deleting messages with a single key entry.
Warn Expiration of Messages	If checked, the system warns the user that saved messages will be deleted due to their retention time expiring. The message is given the day before the messages are automatically deleted, and the user then has the option to either keep or delete the messages. By default, this feature is enabled. • Users will be alerted about expiring messages when they log into their voicemail account using # #. • Users will not be alerted, however, if they simply select a message in MaxAgent and click **Play Message**. **Note:** If this feature is disabled, expired messages are deleted automatically without warning when they expire.

Setting Message Recording Options

Set voice mail message recording parameters:

Message Recording Parameter	Description
Minimum Recording Length	Sets the minimum length in seconds for any recording (incoming voice mail message, personal greeting, system prompts, introductions to forwarded voice mails). This can be from 1 - 5 seconds, or 0, which means no minimum. All recordings that are shorter than the designated Minimum Recording length are deleted. This feature is recommended when users receive many short, empty voice mail messages on a regular basis and would like them automatically deleted.
Pause Detect Length	Selected, this feature causes the deletion of pauses in messages. The default pause detect length is **500 ms**. The pause detect can be disabled by deselecting the check box, or the length can be set to a value between **200–2000 ms (.2–2 seconds)**.

Setting Exchange Integration Options

Set Exchange integration options. Access to these options requires an Altigen Exchange Integration License. To assign this license to an extension, see “Assign Exchange Integration License” on page 180.

If you are opting to use Exchange’s Speech Enabled Voice Mail features or Unified Messaging, Exchange Server and MaxCS need to be installed on the same domain with a network throughput rate of no less than 100 Mbps.

Note: If a user moves an Exchange email message to a folder other than the Inbox, or to a sub-folder of the Inbox, then that message will be deleted from MaxCS during the next Exchange synchronization. The email message will remain in the user's personal folder or Inbox subfolder.

Full configuration details are given in “Microsoft Exchange Integration” on page 353.

You may choose an option when you install MaxCS, and you may change the option later. If you change the option later, you need to restart services.

Exchange Integration Parameter	Description
Disabled	Disables Exchange integration.
Synchronize with Exchange	Allows a two-way synchronization between a user's MaxCS voice mail and the user’s Outlook-readable mail messages with their attached .wav files in the user's Inbox. When e-mails or voice mails are deleted from one server, they are automatically deleted from the other server as well. (This is what Altigen’s previous releases have offered.) If you select the “Synchronize With Exchange” option, select the Exchange Server Version type from the drop down menu.
Bridged Access to Exchange	Through bridged access integration, via a SIP connection, Altigen’s Voice Mail System provides an option to the user to directly access Exchange Unified Messaging (by pressing **7** in extension voice mail after entering the password). Once connected, users can check and reply to e-mail, manage calendars, and send messages. **Note:** If Exchange server is offline or down, the user pressing **7** will hear an error message, “This voice mailbox is not accepting new messages at this time.” All other VM features still function, as they are provided by the MaxCS system and not Exchange server. If you select this option, enter the DNS name of the Exchange server in the **Exchange Unified Messaging Server** field (do *not* enter the IP address).
Enable Synchronization	If you want to synchronize voice mail between the Altigen mail box and the Exchange server, check the **Enable Synchronization** check box. If you don’t check this, voice mail is not synchronized between the two message stores.
Native VM Integration with Exchange	Uses Exchange as a native voice mail box to store voicemail files, providing a unified mailbox for all message types. Callers are forwarded to the Exchange mailbox when an extension is ring-no-answer, busy, or in DND. Accessing voice mail is done through the Exchange system. When this option is activated, all physical/virtual/WG mail boxes with associated Exchange mailboxes are switched to Exchange. Extensions that do not have an Exchange mail box are treated as mailbox disabled. Users with an Exchange account press **##** to log into the Exchange voicemail box. The system establishes a voice stream to the Exchange mailbox through a SIP connection. To turn on the message waiting light on the desktop phone and allow Altigen CTI client applications to manage voice mails, the voicemail files are replicated back to MAX Communication Server. When a voicemail file is heard, marked save, or deleted from an Altigen client application, the voicemail attribute is changed in the Exchange server accordingly. Limitations: • Personal options usually invoked by pressing **4** on the Altigen Voice Mail System menu must be invoked by pressing **#14**. • The following Altigen voice mail functions are *not* supported: activity greeting, voice mail distribution list, voice mail out call. • One Number Access is not available. If you select this option, enter the DNS name of the Exchange server in the **Exchange Unified Messaging Server** field (do *not* enter the IP address).
Exchange Server Version	Select the version of Exchange you are using.
Exchange Unified Messaging Server	Enter the DNS name of the Exchange Unified Messaging Server.

Setting E-mail Messaging Options

To use the MaxCS e-mail services, configure the following settings.

E-mail Messaging Parameter	Description
Enable SMTP/POP3 Service	Selected, this enables incoming and outgoing mail services on MaxCS — Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP3).
Mail Domain Name	Specify the email domain name.
Postmaster Ext	This field defines the extension that will be assigned as a Postmaster Extension. When the e-mail system receives an e-mail with an invalid e-mail account, the automatic reply to the sender (informing of the invalid e-mail account used) is sent from the defined extension. **Note:** The system always requires an extension to be specified as the Postmaster Extension. By default, the first extension in the system is used. If an extension is selected as the Postmaster Extension, it cannot be deleted until the Postmaster Extension is re-assigned to another extension.

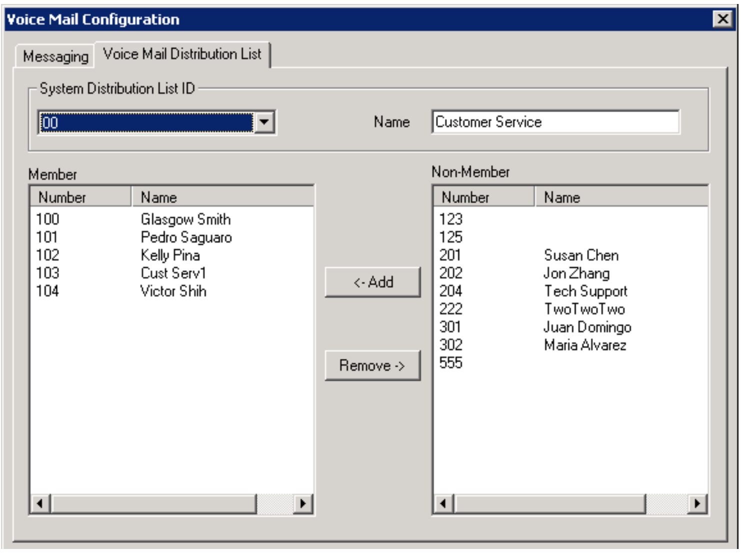
Creating Distribution Lists

The System Distribution Lists provide for forwarding voice mail messages to multiple recipients defined as list members. To forward a voice mail to all list members, a user needs to enter only the two-digit ID instead of entering numerous individual extensions.

You can create up to 100 distribution lists, each composed of up to 64 extensions. The extension list member can represent another distribution list.

Note: The *system* distribution lists discussed here are different from the *extension* distribution lists, which are configured through the phone sets or the MaxCommunicator or MaxAgent user applications.

To configure distribution lists, select **System** > **Voice Mail Configuration**, then click the **Voice Mail Distribution List** tab.



System Distribution List ID: 00

Name: Customer Service

Member

Number	Name
100	Glasgow Smith
101	Pedro Saguaro
102	Kelly Pina
103	Cust Serv1
104	Victor Shih

Non-Member

Number	Name
123	
125	
201	Susan Chen
202	Jon Zhang
204	Tech Support
222	TwoTwoTwo
301	Juan Domingo
302	Maria Alvarez
555	

Figure 32. Voice Mail Configuration, Voice Mail Distribution List tab

Defining a Distribution List

1. On the Voice Mail Distribution List tab, select an ID (00 – 99) in the **System Distribution List ID** list.

   The list name, if any, now appears in the **Name** box; the members of the list are now displayed in the **Member** box, and other available extensions are displayed in the **Non-Member** box.

2. To give the list a name or change the existing name, type a descriptive name into the **Name** box.
3. To *add* a member, select the name(s) in the **Non-Member** list and click the **Add** button to move it to the **Member** list.

   To *remove* a member, select the name(s) in the **Member** list and click the **Remove** button to move it to the **Non-Member** list.

   You can select multiple names by using **Shift**-click or **Ctrl**-click.

4. Click **Apply** to save your changes, or click **OK** to save and close the Voice Mail Configuration window.

CHAPTER

6

Auto Attendant Configuration

The auto attendant (AA) feature provides quick and courteous processing of all incoming calls. An AA can be configured to serve as a primary attendant or as a backup to a receptionist. In a call-heavy environment the AA can greatly reduce the number of calls that need to be handled by the operator.

You can set up to 255 different AAs. AA features include:

- Multiple levels of tree structure.
- Repeat current level or jump to a specific level.
- Transfer call to extension, workgroup, hunt group, or operator.
- Dial by Name – allows a caller who does not know the extension number to spell the name using the telephone key pad. The system will search the Directory and make a match on the name to connect the caller to the intended party's extension.
- Name Directory Service – allows callers to hear a list of employees and their extension numbers.
- Records a voice mail message to a specific mail box.
- Allows employees to call into the system and access voice from an external location.
- Collects caller input data, for example, account code, ID, and so on.
- Data-Directed Routing – Allows the routing of calls directed by the caller's input (digit or text).
- Sets call priority and skill level requirement for workgroup call processing.
- Other advanced features include System Call Back and routing calls to SDK-based add-on applications.

Note: As of Release 9.0.1, the default value for the # symbol in AA trees has been changed from the action *Mailbox Access* to *No Action*. This default will only affect new AA trees that you create.

Planning Is Essential

Follow the steps below before you set up an AA.

1. Before you configure tasks for one or more AAs, plan the entire setup. Decide how many options you will provide at each menu and how many menu levels you will use. Based on the choices in each menu, write down the appropriate prompts or phrases to play at each menu level.
2. Record phrases for each menu level or use the pre-recorded phrases that are available to you. See “Phrase Management” on page 67 for more details on how to record custom phrases, use pre-recorded phrases and use professionally recorded phrases.

Example: AA Planning

Auto Attendant ID: *100, Phrase 10*
Main Menu for XYZ Office

Digit	Meaning	Action
1	*Reserved for Extensions (no prompts)*	*Collect Extension*
2		*Collect Extension*
3		*Collect Extension*
4	*Express Support*	*Expand Tree (No. 110)*
5	*Sales*	*Expand Tree (No. 120)*
6	*Technical Support*	*Expand Tree (No. 130)*
7	*Phone FAQs*	*Expand Tree (No. 140)*
8		
9		
0	*Operator*	*To Operator*

Auto Attendant ID: *110, Phrase 20*
Express Support

Digit	Meaning	Action
1	*Installation*	*Call Extension (Workgroup 350)*
2	*Board Support*	*Call Extension (Workgroup 360)*
3	*Version 5 Support*	*Call Extension (Workgroup 370)*
4	*Version 6 Support*	*Call Extension (Workgroup 380)*
5		
6		
7		
8		
9		
0	*Operator*	*To Operator*
*	*Repeat Menu*	*Repeat Level*
#	*Main Menu*	*GoTo Top Level*

Auto Attendant ID: *120, Phrase 30*
Sales

Digit	Meaning	Action
1	*Hardware*	*Call Extension (Workgroup 310)*
2	*Applications*	*Call Extension (Workgroup 320)*
3	*Check Order Status*	*GoTo Item 127 (Collect Order #)*
4	*Other: Questions, etc.*	*Call Extension (Workgroup 311)*
5		
6		
7		
8		
9		
0		
*	*Repeat Menu*	*Repeat Level*
#	*Main Menu*	*GoTo Top Level*

Planning is essential in organizing an AA menu structure that makes sense. Planning also helps you to identify needs for custom prompts.

This simple example, using sample work forms for each menu, shows a beginning structure: a main menu and two of the four expansions.

When callers are routed to workgroup extensions, the workgroups have their own call handling settings for greetings, update phrases, rules for sending to voice mail, and so on.

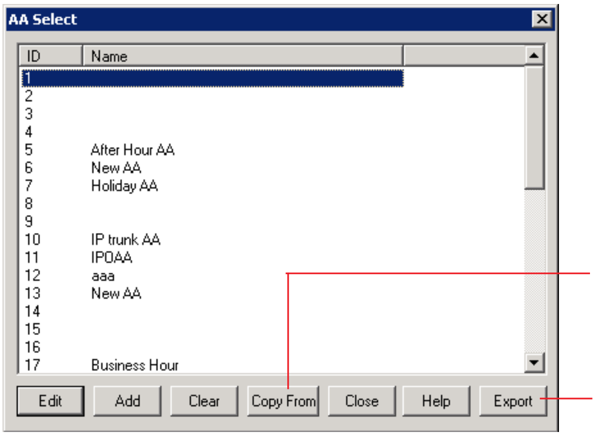
Timeout (not shown on forms): after 7 seconds on first level, call the operator; on any other level, go to top level by default.

Adding Auto Attendants

The first 16 AAs are provided with the menus blank. You can edit these as described in “Configuring Auto Attendants” on page 63. You don’t need to add a new AA if you’re going to use 16 or fewer.

To add an AA beyond the first 16, click the **AA Configuration** button, or select **System** > **AA Configuration**.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.



ID	Name
1	
2	
3	
4	
5	After Hour AA
6	New AA
7	Holiday AA
8	
9	
10	IP trunk AA
11	IPOAA
12	aaa
13	New AA
14	
15	
16	
17	Business Hour

Copies an AA to a selected ID.

Exports all your AA settings to an HTML file

Figure 33. The AA Select window

- **Edit** – Opens the AA window, where you can edit the selected AA.
- **Add** – Opens the Add AA dialog box, where you can add a new AA.

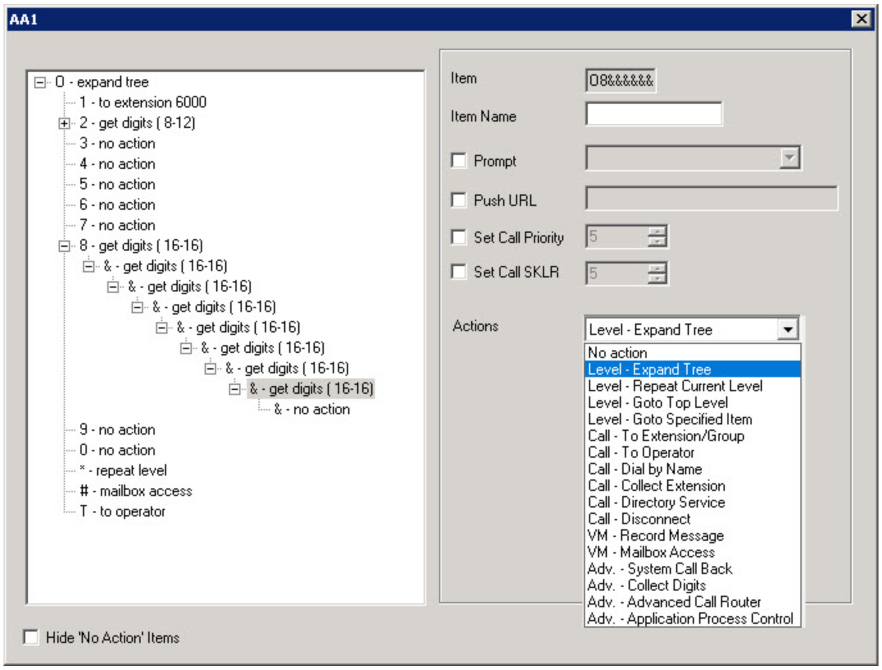
Select an **ID** in the list and type in a descriptive **Name** for the AA, then click **OK**.

- **Clear** – Clears all edits to the selected AA, restoring system defaults.
- **Copy From** – Lets you make a copy of an AA (and then modify it, as you like).
    1. Select your target ID from the AA Select window.
    2. Click the **Copy From** button.
    3. From the list, choose the AA you want to copy to your selected ID.
    4. In the pop-up box, click **Yes** to complete the copy.
- **Close** – Closes the AA Select dialog box.
- **Help** – Opens the help file for AA.
- **Export** – Exports all AA settings to an HTML file.

Configuring Auto Attendants

To configure an AA, click the **AA Configuration** button, or select **System** > **AA Configuration**. When the **AA Select** window opens, select an AA in the list and click the **Edit** button.

This opens the **AA** window, showing details for the AA that you selected.



AA1

- 0 - expand tree
  - 1 - to extension 6000
  - 2 - get digits (8-12)
  - 3 - no action
  - 4 - no action
  - 5 - no action
  - 6 - no action
  - 7 - no action
  - 8 - get digits (16-16)
    - & - get digits (16-16)
      - & - get digits (16-16)
        - & - get digits (16-16)
          - & - get digits (16-16)
            - & - get digits (16-16)
              - & - get digits (16-16)
                - & - get digits (16-16)
                  - & - no action
  - 9 - no action
  - 0 - no action
  - * - repeat level
  - # - mailbox access
  - T - to operator

Item: 08&&&&&&

Item Name:

□ Prompt

□ Push URL

□ Set Call Priority: 5

□ Set Call SKLR: 5

Actions: Level - Expand Tree

□ Hide 'No Action' Items

Figure 34. The AA window

Note: You can check the **Hide 'No Action' Items** check box to hide items that are set to "no action." This will give you a cleaner view of your various action items.

Configuring Menu Items

The AA is a tree-based structure with unlimited tree levels. The following rules guide the basic AA configuration:

- Each item is an action point with its ID number and name.
- The top of the tree is a "O" (for Origin).
- A timeout is indicated by a "T".
- Any action item can have a "Prompt". The list displays phrase files located at C:\Postoffice\Phrases\LangCustom directory. A phrase file can be any file name. (Note: Prior to the 5.1 Release, the "Phrase" directory was under C:\AltiServ, and custom phrases had to use a phrase number from 0001 to 0999.)
- If one action item has multiple choices, you need to select "Expand Tree" instead of using "Go to next menu" to create a new level.
- You can jump to any action item within the same AA.

Every item will execute steps according to the following rules:

- First step – Play prompt if the box is checked. If the prompt box is not checked, the AA will go to the second step without delay.
- Second step – Push URL/Web-Page forces a web page to a Web caller's screen when the call reaches the AA using AtliWeb's Webcall button over the Internet. If this box is not checked, go to the next step without delay.
- Third step – Set Call Priority for MaxCS ACM priority queuing. You can assign a priority number from 1-9 to the caller who selects this menu item. The highest priority is 1, the lowest priority is 9. If this box is not checked, go to the next step without delay.

- Fourth step – Set Call SKLR (Skill Level Requirement) for MaxCS ACM skill-based routing. You can assign an SKLR from 1-9 to the caller who selects this menu item. If this box is not checked, go to the next step without delay.
- Fifth step – Execute the action selected from the drop down list. The following table describes each action.

Auto Attendant Actions

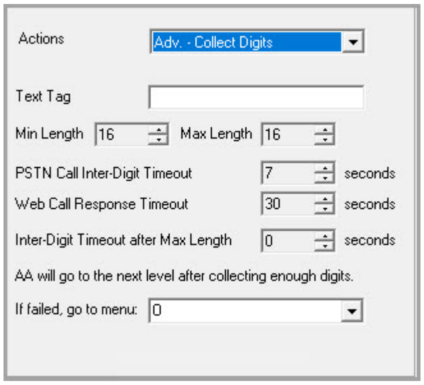
Action	Description
No Action	An “invalid” message plays and the menu is repeated.
Level – Expand Tree	Expand menu item to create additional level.
Level – Repeat Current Level	Repeats the level that contains the “Repeat Current Level” menu item.
Level – Go to Top Level	Go to the top level and repeat action items on the top level.
Level – Go to Specified Item	Goes to selected menu item at any level. A list opens from which you select the item.
Call – To Ext./Group	Transfers call to an extension or group number you select in the list.
Call – To Operator	Routes the call to the operator (the operator is defined in the System Configuration window).
Call – Dial By Name	Prompts the caller to enter the name (first, or last, or both in any order) of the person they want to speak with and dials the extension that matches the name. Callers may not have to enter the entire first or last name before a match is found.
Call – Collect Extension	The top level of each AA collects the extension number automatically. The system has a timing delay to differentiate if the first digit the caller entered is a menu option or the first digit of an extension number. Once past the top level, the system will not have the timing delay to differentiate digits. If you would like to provide the option for a caller to enter an extension number, you need to map this action item to one of the menu options.
Call – Directory Service	Lists the system users and their extensions to the caller. For this to work properly, users need to record their directory names.
Call – Disconnect	Disconnects the call.
VM – Record Message	Leaves a voice mail message in the specified voice mail box. If you want the caller to hear the extension’s greeting before hearing the start-recording beep, check **Play Extension Greeting**.
VM – Mailbox Access	Allows the caller to log in to the voice mail system to retrieve voice mail or change personal options from the outside.
Adv. – System Call Back	Allows outside caller to dial into the system, enter a call back number, hang up, and wait for the system to call back. The system will request the caller to enter an extension and password for authentication. The call back number needs to include the toll call prefix and area code for long distance and international calls. The trunk or route access code is not required when entering a call back number.
Adv. – Collect Digits	See the discussion on “Collecting Digits.
Adv. – Advanced Call Router	When selected, the system will hand over the call to the Advanced Call Router application through the SDK API interface. The ACR application needs to log in to a virtual extension with the correct password. If the ACR application fails to connect, the system will execute the sub-level "&" as a fail action.
Adv. – Application Process Control	When selected, the system will hand over the call to the APC (Application Process Control) SDK through an application extension as a control extension. An SDK APC based application needs to log in to the application extension to receive the call. If the APC application fails to connect, the system will execute the sub-level "&" as a fail action. **Note:** The APC SDK license is not supported in the MaxCS Private Cloud service.

Collecting Digits

When a caller selects the "Collect Digits" action item, a custom phrase is required to advise the caller how many digits are required. The system will look at "Min Length" and "Max Length" to determine if the collect digit action was successful or failed.

- If successful, the system executes the sub-level "&" action item.
- If failed, the system executes the menu item you define as a fail over action.

To use the Collect Digits action, select the **Adv. – Collect Digits** action, then set additional parameters.



Actions: Adv. - Collect Digits

Text Tag:

Min Length: 16 Max Length: 16

PSTN Call Inter-Digit Timeout: 7 seconds

Web Call Response Timeout: 30 seconds

Inter-Digit Timeout after Max Length: 0 seconds

AA will go to the next level after collecting enough digits.

If failed, go to menu: 0

Figure 35. Collect digits options

- **Text Tag** – A tag name, which is critical for the following operations:
  - For CDR logging, the **IVRData** field will log the collected digits as "Tag=xxxxx". For example, if tag is configured as “Account” and collected digits is “67663”, the CDR database will log `“Account=67663”` in the **IVRData** field.
  - For MaxAgent client display, the above example is displayed as "Account=67663" on the **View > IVRData** section.
  - For CDR Search, the above example is displayed as "Account=67663" on the **IVRData** column.
  - To display collected digits on the Altigen IP phone, you need to set the tag as “DISP” (stands for “Display” and is case-sensitive. The **Phone Display/Name Line** of the extension configuration needs to be configured as **IVR Data (Display)**. This feature supports inbound trunk calls only.
- **Min. Length** – The *minimum* length of digits to be collected.
- **Max. Length** – The *maximum* length of digits to be collected.
- **PSTN Call Inter-Digit Timeout** – The length of time the system will wait between collecting of digits before timing out.
- **Web Call Response Timeout** – The length of time the system will wait for digits after responding to a Web call before timeout.
- **Inter-Digit Timeout after Max Length** – The length of time the system will wait after the maximum length of digits is collected.
- **If failed, go to menu** – Specify which menu to switch to if the digit collection fails.

Making Auto Attendant Assignments

Once the AAs are set up, you can use them in various in-call routing situations – trunk, DNIS, caller ID, in-call routing, and an answering option for an extension or workgroup.

For example, for trunk /AA assignments, see “Incoming Call Routing” on page 148. For extension or group assignments, see “Setting Answering Options” on page 187.

Phrase Management

You might want to record unique phrases to customize an AA or a group. When the system is configured to have the AA answer incoming calls, callers hear a customized greeting. For example:

> “Thank you for calling ABC Company.
> Enter the extension number of the person you wish to speak with.
> Press 1 for sales.
> Press 2 for technical support.
> Press 3 for accounts payable.
> Press 0 to reach the operator.
> To repeat this menu, press star (*).”

An example of a group greeting phrase:

> “Please hold; someone will be with you shortly.”

You might also want to give callers the option of hearing prompts in another language. For information on configuring for a multilingual AA, see “Multilingual Configuration” on page 69.

This section covers information on how to use pre-recorded phrases, record custom phrases, and use professionally recorded phrases.

Using Pre-Recorded Prompts

MaxCS provides ready-to-use pre-recorded phrases. Phrase 0001 is the default AA greeting at the root menu level. Phrases 0291 through 0297 are phrases used for group queue prompts. Select the phrase you want to use in the **Prompt** field. To hear the pre-recorded phrases:

1. Use any phone to dial “###”, and log in with the system manager’s extension and password.
2. Press 6 for the Phrase Management option.
3. Press 1 to review a phrase.
4. Enter the 4-digit phrase number from the list below to hear the phrase.

Phrase #	Phrase
0001 (default)	Thank you for calling. If you know the extension of the person you wish to speak with, please enter it now. To reach the operator, press **0** or simply stay on the line.
0291 (default)	Please hold; someone will be with you shortly. For your convenience, you may leave a message if you wish by pressing the # key on your telephone and we will get right back to you.
0292	Please hold; someone will be with you shortly.
0293	We appreciate your call and will be with you as quickly as possible.
0294	Thank you for your patience. We should be with you soon.
0295	Thank you for your patience. We should be with you soon. For your convenience, you may leave a message if you wish by pressing the # key on your telephone and we will get right back to you.
0296	We apologize for the extended delay, but our current call load is abnormally high. Remember, you may leave a message by pressing the # key on your telephone and we will get right back to you.
0297	You may still wait if you prefer, but we suggest you leave a message by pressing the # key on your telephone and we will get right back to you.
0400	Please hold. Someone will be with you shortly.
0401	Thank you for holding. Someone will be with you as soon as possible.
callback	You can also press 1 to schedule a callback.
callback1	This is a callback for…

Recording Custom Phrases from an Altigen IP Phone

Note: If you have an Altigen SDK license, you can use the Altigen Custom Phrase Manager discussed in "Altigen Custom Phrase Manager" on page 403. This application has a graphical user interface that makes recording phrases easier.

When you create custom phrases from the Altigen phone, keep a record of phrase numbers and the corresponding phrases so that if a phrase needs to be changed, the correct phrase number is readily available.

To record a custom phrase,

1. Log in from any phone on the system by dialing "###", and entering the system manager's extension and password. This brings you to the Altigen Voice Mail System Main Menu.
2. Press **6** for the Phrase Management option.
3. Press **2** to record a phrase.
4. Enter a four-digit phrase number between 0001 and 0999.
5. Record the phrase after the tone. Press **#** at the end of the recording.
6. The system will replay the recorded phrase. Press # if the recording is acceptable.
7. At the Phrase Management menu, press **2** to record additional prompts or star (*) to exit Phrase Management.

Phrases are stored in the C:\PostOffice\Phrases\LangCustom directory. You can modify the phrase file to any meaningful name if you want.

Using Professionally Recorded Phrases

Recording studios such as Worldly Voices provide professionally recorded prompts as electronic files that can be installed and used on the MaxCS system.

Altigen provides the Voice File Converter utility to convert these files into the proper MaxCS format (use the Windows **Start** > **MAX Communication Server ACM** menu). Some recording studios provide the conversion service for an additional fee. The converted file can then be used for an AA or for a workgroup or huntgroup group setup.

To install professionally recorded phrases or prompts,

1. Assign a prompt number to each prompt you would like recorded. Or give the prompt a unique identifying name. Altigen-supplied phrases are numbered, but phrases don't have to be numbered.
2. Submit your prompt script and prompt name to the recording studio.
3. Instruct the recording studio to record prompts in either 8KHz or 11.025KHz mono in the WAV format.
4. Ask the studio to convert the WAV files into the proper MaxCS format.
   - If using Worldly Voices, this conversion is done for you.
   - When using any other studio, use the Voice File Conversion utility. This utility converts an audio file recorded at either 8KHz or 11.025KHz in the WAV format to an MaxCS playable audio file.
5. Once you receive the prompts in the MaxCS format, place them in the **C:\PostOffice\phrases\LangCustom** directory on the gateway that is running MaxCS.

Your prompts are now ready to be used.

CHAPTER

7

Multilingual Configuration

MaxCS supports multiple language prompts (8 languages maximum) for trunk calls and extension users, letting you configure your system to handle the following types of scenarios in a multilingual environment:

- An auto attendant (AA) may serve callers who speak different languages. MaxCS can be configured to let the caller select a preferred language in which to hear prompts. Once a language is selected, the whole call session will use the selected language.
- An internal user may use a feature code to execute a certain action, including logging into voice mail. Normally the user hears system prompts first. If the user is not fluent in the default system language, another language can be assigned to his extension. Whenever that extension user encounters prompts, the system will use the assigned language to play the prompts.
- DNIS may also be used to select a language for the caller. If your company has multiple phone numbers, you can configure MaxCS to direct a caller to a language based on the phone number the caller has dialed. For example, if you give out different 800 numbers to different countries, and a call comes in from the 800 number you give out to customers in Mexico, you can configure MaxCS to direct that 800 number to the “Mexico Spanish” language prompts or to an extension that uses the corresponding language in its prompts. This eliminates the caller having to select a language.

Note: The MaxCS multilingual feature requires the purchase of an Altigen Multilingual License.

Configuration Overview

Configuring multilingual features involves most or all of the following actions, which are discussed in subsequent sections:

- Have the appropriate system and custom phrases recorded in each language that your company wants to use (in addition to the default language).
- Store the custom phrases in new directories under the C:\PostOffice\Phrases directory, using the prescribed naming convention.
- Add the new languages to the Multilingual Configuration screen.
- Enable auto attendant support in the Multilingual Configuration screen, AA tab.
- In the Extension Configuration screen, choose an available language for the internal user, if desired.
- Enable the extension user to change the preferred language for the extension by using a feature code **#12**, if desired.
- Configure the **Language Setting** in DNIS, if desired.

Creating Language Phrase Packages

For each set of phrases you want in a different language, you need to have phrases recorded in that language. See *Using Professionally Recorded Phrases* on page 68 for details. Each language's phrase package must contain phrase files, and two text files: one text file that lists syntax rules for numbers, and one that lists syntax rules for sentence structure, since these vary from language to language.

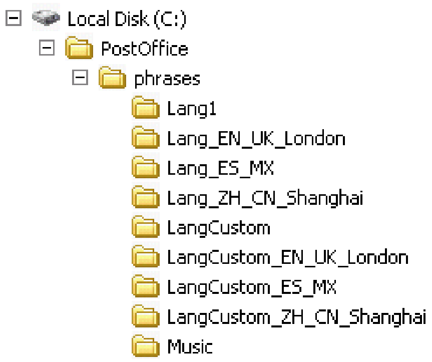
The phrase files will have the exact same name/number as in the default language directory and will be part of the same AA, but they will be stored in a different directory.

Note: Altigen authorized distributors in each country will perform localization procedures to create language packages, including syntax rules for numbers and sentence structure for their local market. For international customers, please contact the authorized Altigen distributor in your country to obtain localized language phrases.

Storing Language Phrase Packages

Additional language phrases (system and custom) and syntax styles need to be copied to the correct directory before system startup, so that the system can recognize them. If they are added *after* system startup, MaxCS needs to be shut down and restarted, before the directories are recognized.

The following figure illustrates the directory storage structure for language phrases.



```
⊟ Local Disk (C:)
    ⊟ PostOffice
        ⊟ phrases
              Lang1
              Lang_EN_UK_London
              Lang_ES_MX
              Lang_ZH_CN_Shanghai
              LangCustom
              LangCustom_EN_UK_London
              LangCustom_ES_MX
              LangCustom_ZH_CN_Shanghai
              Music
```

Figure 36. Storage structure for multilingual phrases

The directories `Lang1` and `LangCustom` contain the phrases of the system default language.

Phrases for language *X* should be saved in a pair of directories: Lang_X and LangCustom_X. Lang_*X* stores the phrases required by the system, and LangCustom_*X* stores your custom phrases.

For example, to add a language for Mexico, you need to create two directories:

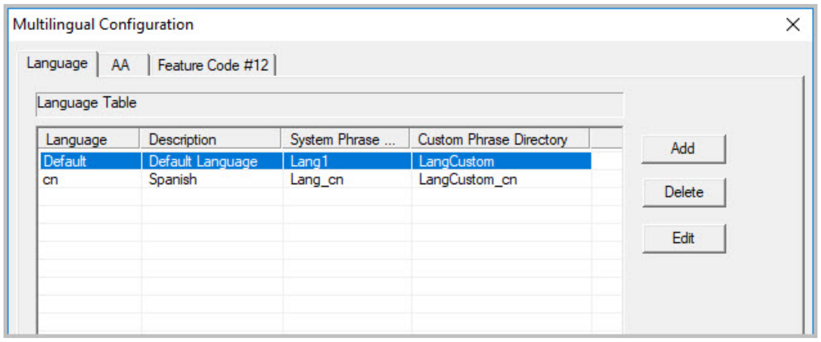
- Lang_Mexico
- LangCustom_Mexico

Configuring for a Multilingual System

To configure MaxCS as a multilingual system, select **System** > **Multilingual Configuration**.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

The configuration screen opens to the **Language** tab. Here, you will add references to the language directories you created. These are the directories that contain phrases in other languages.



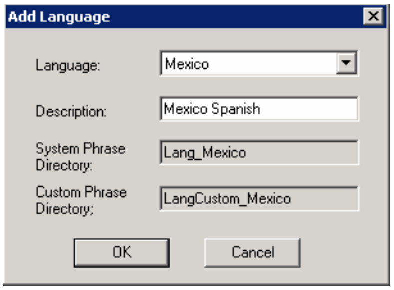
Language	Description	System Phrase ...	Custom Phrase Directory
Default	Default Language	Lang1	LangCustom
cn	Spanish	Lang_cn	LangCustom_cn

Figure 37. Multilingual Configuration, Language tab

When you first run MaxCS, only the default language is listed in the Multilingual Configuration screen, and the description of the default language is displayed as **Default Language**. Each language added to the table will have a formal name, a description, a system phrase directory (LangDir_*X*), and a custom phrase directory (LangCustomDir_*X*), as shown in the following figure.

To add a language,

1. Click the **Add** button.



Language: Mexico

Description: Mexico Spanish

System Phrase Directory: Lang_Mexico

Custom Phrase Directory: LangCustom_Mexico

Figure 38. Adding a language

2. Choose a language from the list. The list shows the language directories you have added to the C:\PostOffice\Phrases directory.
3. Enter a description for the language. This description will appear elsewhere in the graphical user interface, for example in the **Extension Configuration** window and the **AA** tab in this screen. Click **OK**.
4. Repeat these steps for each language you want to add.

The contents of the fields **System phrase directory** and **Custom phrase directory** are fetched from the location where the language phrases are stored. They are not editable.

Only the description of the language is editable here. To edit it, click the **Edit** button or double-click the row.

The default language cannot be deleted. After you add languages, any language used by DNIS, an extension, or an AA cannot be deleted.

Enabling Multilingual Support in the Auto Attendant

After you have recorded phrases and added a reference to their directories in the **Multilingual Configuration** > **Language** tab, as described earlier, you are ready to enable multilingual support in auto attendants.

A new option in Release 8.5 Update 1 lets you specify language options for AA branches. The *Single Language* option specifies the language for the AA. All prompts played to trunk callers will be in the specified language.

- If the AA routes the trunk caller to another a *Single Language* AA with a different language setting, then the new language setting will be used from that point on.

- If the AA routes the trunk caller to an AA set to *Multiple Languages*, then no language selection prompt will be played; the original language setting remains.

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

Multilingual AA Example: DNIS Routing

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

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

Multilingual AA Example: Virtual Extension Forwarding

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

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

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

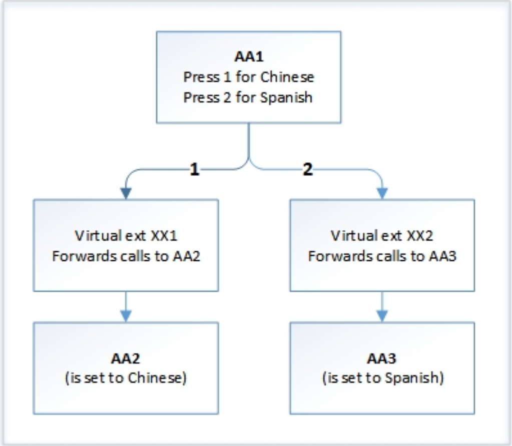
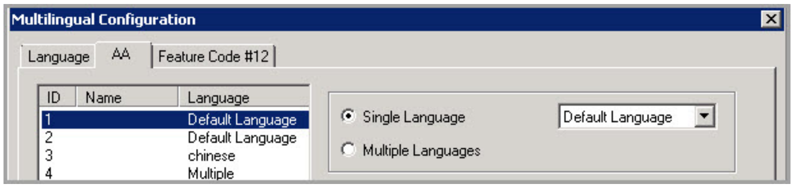


Figure 39. Example: Using the Multiple Languages option to route callers

Configuring Multilingual Options for AAs

1. Select **System** > **Multilingual Configuration** > **AA** tab.



ID	Name	Language
1		Default Language
2		Default Language
3		chinese
4		Multiple

● Single Language   Default Language

○ Multiple Languages

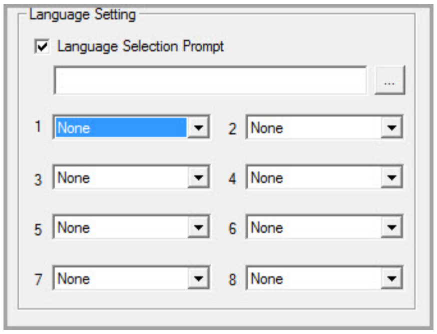
Figure 40. Selecting AA Language options

2. From the list at the left, select the AA that you want to configure with multilingual support.
3. On the right, select *Single Language* or *Multiple Language*:

- **Single Language**: Specifies the language for that AA. All the phrases played to this trunk caller will be in the language that you choose, including system phrases and custom phrases. You must choose the language that you want to use as the default language.
- **Multiple Language:** This option functions the same as the Multilingual option in previous releases. In the fields.

  In the *Language Setting* group of fields, check the **Language Selection Prompt** check box and choose the phrase that lets the caller select a language, Beside each appropriate field 1-8, select a language from the list that corresponds to the phone key the user would press to hear that language. (For example, “For English, press 1; for Spanish, press 2...”)

  You can use the In Call Routing table to manage inbound calls to a *Multiple Language* AA.



Language Setting

☑ Language Selection Prompt

1 None 2 None

3 None 4 None

5 None 6 None

7 None 8 None

Figure 41. For the Multiple Language option, specify prompt and language choices

4. Click **Apply** if you have more work to do here, or click **OK** to accept the changes and close the screen.

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

Note: This configuration is on top of the regular AA configuration. The system will execute the regular AA action items after a language preference is selected by the caller.

Operational Notes for Multi Language Configuration

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

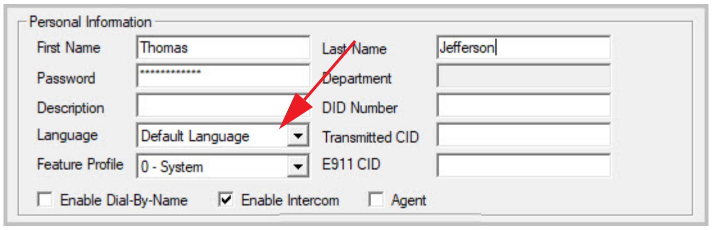
Because the call originated as a direct DID call, it did not go through an AA that offered the caller a language preference. Therefore, if the user transfers the call to a workgroup/huntgroup with foreign language agents, the caller will hear prompts in the system default language.

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

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

Configuring the Extension

Extension users have a default language configured, and that language is always used for them whenever they hear a prompt on their extension. The default language is assigned in **PBX** > **Extension Configuration** > **General** tab.



Personal Information

First Name: Thomas
Last Name: Jefferson
Password: ************
Department:
Description:
DID Number:
Language: Default Language
Transmitted CID:
Feature Profile: 0 - System
E911 CID:

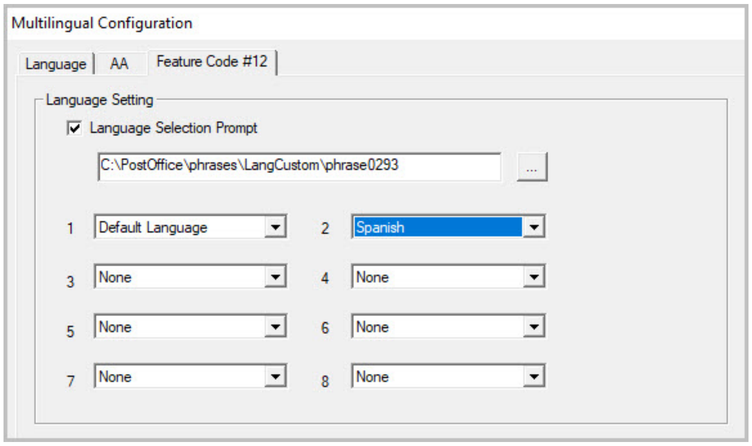
☐ Enable Dial-By-Name ☑ Enable Intercom ☐ Agent

Figure 42. Selecting a language for an extension user

In the **Language** list, select the desired language, and click **OK**.

Extension User Can Change Language Setting

Extension users can change the extension's language setting by using feature code #12, if feature code #12 is configured on the **System > Multilingual Configuration** > **Feature Code** tab.



Multilingual Configuration

Language | AA | Feature Code #12

Language Setting

☑ Language Selection Prompt

C:\PostOffice\phrases\LangCustom\phrase0293

1 Default Language
2 Spanish
3 None
4 None
5 None
6 None
7 None
8 None

Figure 43. Configuring feature code #12 to allow a user to change an extension's selection

Configuring Feature Code #12 for Language Selection

1. Check the **Language Selection Prompt** check box.
2. Select the prompt the extension user will hear after pressing **#12**. You must know the text of this prompt, so you can match the languages to the correct numbers in the next step.

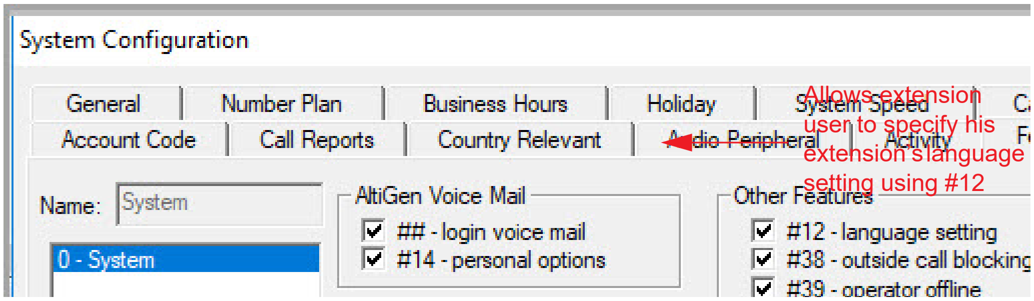
   For example, the prompt the extension user might hear after pressing #12 might be "To change the preferred language for this extension, press 1 for English, press 2 for Spanish, press 3 for Chinese."
3. Beside each number, select a language from the list that corresponds to the prompt. The languages listed are those that you have added to MaxCS on the **Language** tab of this window.

   For example, if you were working from the example prompt in step 2, you would select **English** beside the number 1, **Spanish** beside the number 2, and **Chinese** beside the number 3. The remaining fields would be left as **None**.

Feature code **#12** must also be enabled in **System Configuration** > **Feature Profiles** tab.

To enable feature code #12,

1. In **System** > **System Configuration** > **Feature Profiles** tab, check the **#12 -language setting** check box.
2. Click **OK**.



Name: System

0 - System

AltiGen Voice Mail

☑ ## - login voice mail

☑ #14 - personal options

Other Features

☑ #12 - language setting

☑ #38 - outside call blocking

☑ #39 - operator offline

Allows extension user to specify his extension slanguage setting using #12

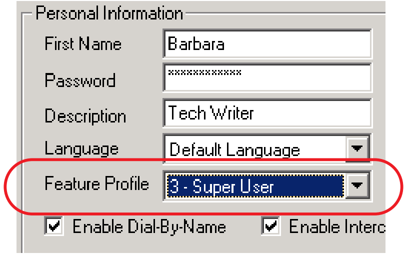
Figure 44. The Language option on the System Configuration Features Profile tab

All feature codes are enabled, by default. The default feature profile name is “0-System.”

Lastly, the extension user must have a feature profile assigned to him that includes #12. This is done on the **PBX** > **Extension Configuration** > **General** tab.

To assign feature code #12 to an extension,

1. On the **PBX** > **Extension Configuration** > **General** tab, select the extension.
2. In the “Personal Information” panel of the **General** tab, assign a **Feature Profile** that includes #12.



Personal Information

First Name: Barbara

Password: ************

Description: Tech Writer

Language: Default Language

Feature Profile: 3 - Super User

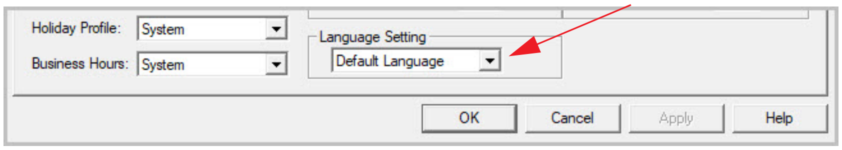
☑ Enable Dial-By-Name ☑ Enable Interc

Using DNIS to Set the Language

If your company has multiple phone numbers, you can configure MaxCS to direct a caller to prompts in a selected language based on the phone number the caller has dialed.

To direct specified DNIS calls to a selected-language AA or extension,

1. Select **PBX** > **In Call Routing Configuration** > **DNIS Routing** tab .
2. Click the **Add** button to add a number.
3. Select where you want to route callers who have dialed that number.
4. Select the appropriate language from the **Language Setting** list.
5. Click **OK**.



Holiday Profile: System

Business Hours: System

Language Setting: Default Language

Figure 45. Configuring the language setting in DNIS

See “DNIS Routing” on page 153 for rules and restrictions on routing using DNIS.

Which Language Will Be Used?

MaxCS follows these rules to determine which language to use:

1. The extension user hears the prompts in the language configured or selected via the **#12** feature code.
2. If the external caller selects a language in the auto attendant, MaxCS uses the selected language. If a language selection is invalid or times out (7 seconds) three times in a row, the default language is selected.
3. If an extension is set for ONA (one number access), the caller will hear the prompt in the language selected previously, but when the callee picks up the ONA notification call, the callee will hear the prompt in the language according to the extension's language setting.
4. When the user logs in to the voice mail of an extension, the extension's language is used.
5. If DNIS is configured for language setting, the external caller hears the prompts in the language specified by the number he dialed.
6. In any other case, the system default language is used.

CHAPTER

8

Call Recording Configuration

To use the centralized call recording function, make sure the following requirements are met:

- You need a recording seat license for each extension that will be recording: either Dedicated Recording Seat licenses assigned to particular extensions or a Concurrent Recording Session license that is shared by a fixed number of extensions.
- It is recommended that you have a separate storage server to store recorded files.
- Recorded files (64 Kbps PCM format) can be managed by the VRManager Pro (licensed) application.
- If your system has a multi-chassis configuration and the gateway needs to transmit recorded files to a storage server, you need to set up an FTP server to facilitate the file transfer. You do *not* need to set up an FTP server for a single chassis (all-in-one) installation.
- If an agent is using an IP phone and recording is turned on, the system will use a recording channel on a VoIP board to process the recording session. The IP phone will occupy a codec channel on the VoIP board to allow the recording channel to tap into the conversation. You need to make sure that the MaxCS server that agents belong to (and the gateway for a multi-chassis installation) have adequate VoIP codec channels to record conversations. The basic guideline is to have one codec channel per agent.
- Because recording files require a large amount of disk storage space, a NAS (Network Attached Storage) system is recommended, unless VRManager Pro is used.

Automatic Shutdown of Recordings when Space is Insufficient

Beginning with Release 8.5.1, MaxCS now regularly checks the available disk space of four drives, **before allowing users to record a call**.

This process affects not just users who are recording individual calls; it also affects VRManager Centralized Recording. If the available disk space for a drive falls below a threshold, then the monitoring program **will automatically shut down recording for that drive, including VRManager Centralized Recording.**

The four drives that are being monitored are:

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

If you are using VRM Pro and you do not see any new recordings, then check that there is sufficient space for recordings, especially the D: drive space.

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

Within MaxAdministrator, the status bar will show you the remaining disk space of the drive that has the lowest capacity of these four drives.

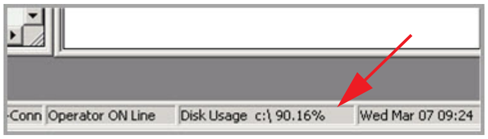


Figure 46. Example of the status bar showing disk capacity for call recording

If MaxCS detects that one of those drives has exceeded the capacity of the registry value that you configured, you will see an alert when you open MaxAdministrator, to warn you. The alert will list the capacity of each drive.

The registry entry where you assign this threshold is:

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

This threshold setting can be set between 50% and 95%. We recommend that you set this percentage no lower than 80%.

Note that this registry setting is designed only to pre*vent any further calls from being recorded*, until you clear out enough space on that drive to continue recordings. There are other built-in capacity checks that do nothing but send out alerts when a drive has exceeded certain disk space thresholds.

Automatic Email Notifications Sent When Drive Capacity is Nearing

These thresholds are set by the system and cannot be customized. These alerts do not shut down recording; they merely send an alert when a threshold has been exceeded.

Alerts sent for C: drive capacity:

- Warning Severity: Trigger at 81%, clear at 80%
- Average Severity: Trigger at 90.5%, clear at 90%
- High severity: Trigger at 95.5%, clear at 95%
- Disaster severity: Trigger at 99%, clear at 95%

Alerts sent for D: drive capacity:

- Warning: Trigger at 90%, clear at 80%
- Average Severity: Trigger at 95%, clear at 94.5% (this was recently changed from 95.1% / 95%)
- High severity: Trigger at 98%, clear at 94.5%
- Disaster severity: Trigger at 99%, clear at 94.5%

Notes:

- These alerts are sent when the threshold has been passed, then sent again every 24 hours thereafter if the level has not gone back down below the *clear* threshold.
- These alerts are sent to the “Notifications” email address that you specified when you ordered your service.

Recording with Polycom VVX Phones

Polycom VVX models can also record calls; you can enable a **Record** softkey for those models. This option is found on the **PBX** > **Altigen IP Phone Configuration** *Polycom* tab.

Once this feature has been enabled, the extension user can tap a *Record* softkey on their Polycom phone to record the call in progress. This feature requires a *Polycom Advanced Features* license; see the *MAXCS Polycom Configuration Guide* for details.

Description of the Recorded File Name

The recorded file name contains the following information:

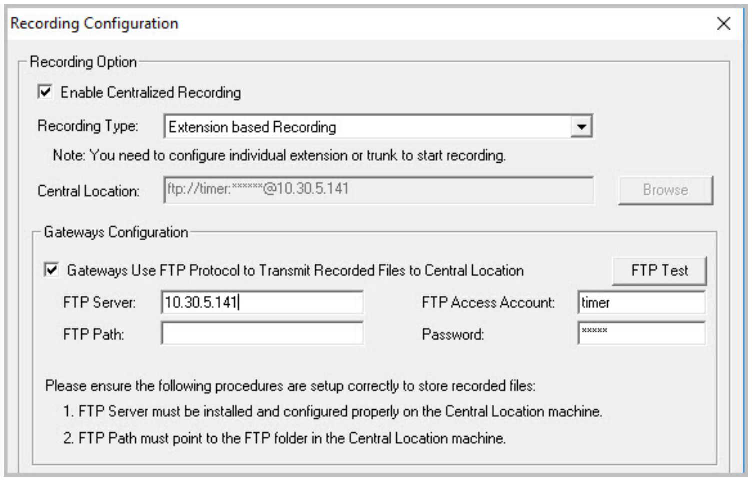
- R!**mmddyyyy_hhmmss!callerID!calleeID!workgroupID!DNIS!sessionID**!R
- **mmddyyyy_hhmmss** is the time stamp when the recording starts
- **callerID** is the caller ID or extension number. It could also be:
  - **bgn** for barge-in call
  - **sm** for a silent monitor call
  - **trk(bbcc)** for an inbound trunk call without caller ID. *bb* is the board logical ID and *cc* is the channel ID
- **calleeID** is the target number or **trk**(bbcc)
- **workgroupID** is the workgroup number for a workgroup call, or **ext** for extension call
- **DNIS** is the DNIS number or NA for no DNIS number
- **sessionID** is the CDR session ID

Configuring Call Recording

Note: During recording, any communication from a barge-in or coach supervisor's extension becomes part of that call recording.

To configure system-wide call recording, including centralized recording for multiple gateways, either click the **Recording** button on the toolbar or select **System** > **Recording Configuration**.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.



Recording Configuration

Recording Option

☑ Enable Centralized Recording

Recording Type: Extension based Recording

Note: You need to configure individual extension or trunk to start recording.

Central Location: ftp://timer:******@10.30.5.141

Gateways Configuration

☑ Gateways Use FTP Protocol to Transmit Recorded Files to Central Location

FTP Server: 10.30.5.141

FTP Path:

FTP Access Account: timer

Password: *****

Please ensure the following procedures are setup correctly to store recorded files:

1. FTP Server must be installed and configured properly on the Central Location machine.
2. FTP Path must point to the FTP folder in the Central Location machine.

Figure 47. Recording Configuration window

Call recording options for specific extensions/workgroups can be set up on the **General** tab of **Extension Configuration** and **Workgroup Configuration**, respectively.

To enable centralized recording,

1. Check the **Enable Centralized Recording** check box.
2. Select a **Recording Type** from the drop-down list.
3. In the **Central Location** field, browse for the directory you want to set as the destination folder and path for saving the call recordings.

Important: If you are using FTP protocol, the FTP server must be installed and configured properly on the same machine as the Central Location directory. An FTP folder must be created for the Central Location, so that it can be fully accessible through FTP. The FTP Path must be pointed to the Central Location.

Note: Windows Server users using a remote shared directory should refer to the steps described in “Using a Remote Shared Directory” on page 80.

4. If you are using multiple gateways, and you are *not* using network attached storage, check **Gateways Use FTP Protocol to Transmit Recorded Files to Central Location**.
   – **FTP Server** – Enter the IP address of the FTP server.
   – **FTP Access Account** – An FTP server account name that gateways can log in to.
   – **FTP Path** – Enter the directory that the files will be transmitted to on the FTP server.
   – **Password** – FTP account password.
5. Click the **FTP Test** button to verify that login to the FTP server is successful.
6. When you are finished configuring, click **OK**.

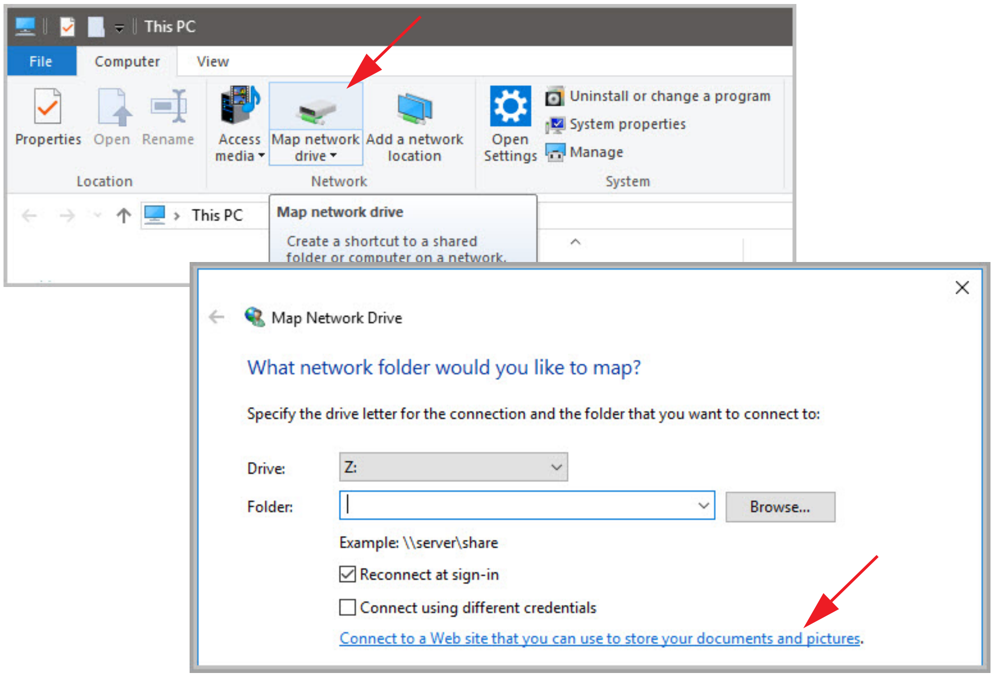
Note: To allow supervisors to record an agent’s non-workgroup call, check the appropriate check box on the System Configuration **General** tab. For details, see “Setting General Parameters” on page 31.

Using a Remote Shared Directory

It is strongly recommended that you use VRManager Pro (new in Release 8.5 update 1) to manage centralized recording and that you save recordings to a local drive or network attached storage on the gateway that is running MaxCS 8.5. If you save recordings to a network drive, and the network becomes unstable, you could lose any files of conversations being recorded at that time.

However, if you need to use a remote shared directory, and you are using Windows Server, follow the steps below. Note that the exact steps will vary, depending upon your Windows operating system.

1. From your Windows desktop, open **This PC**.
2. On the toolbar, click **Map network drive**.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder:

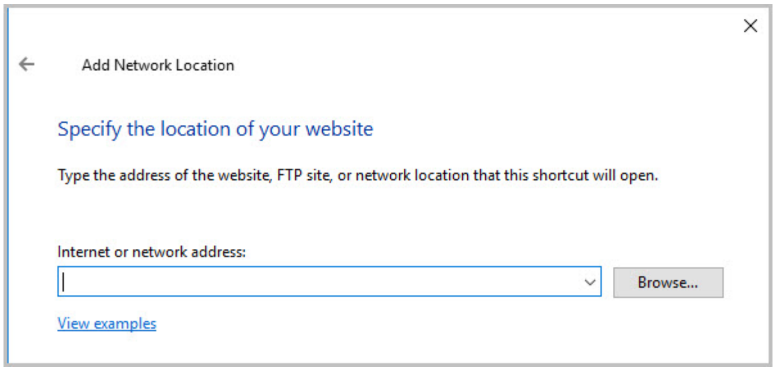
Example: \\server\share

☑ Reconnect at sign-in

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

Figure 48. Map Network Drive


Add Network Location

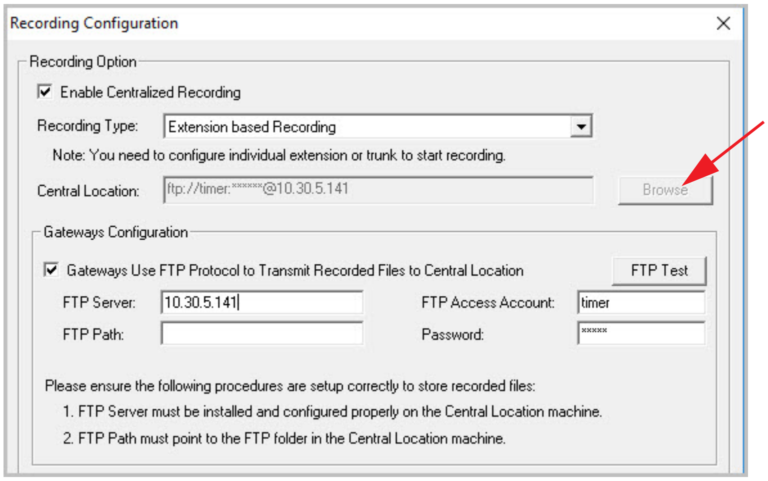
Specify the location of your website

Type the address of the website, FTP site, or network location that this shortcut will open.

Internet or network address:

Figure 49. Add Network Place Wizard

3. In the *Add Network Location* wizard, when prompted, specify the location of your website. Type the address of the web site, FTP site, or network location in the field, for example,"\\ServerName\sharefolder"; or use the **Browse** button to locate the destination path. Click **View examples** for correct formatting. Then click **Next**.
4. Continue through any other panels of the Wizard. At the end, click **Finish**. The network place that you created should appear as a mapped location in **This PC**.
5. In MaxAdministrator in the **Recording Configuration** window, use the **Browse** button to select the network place as the **Central Location**.



Recording Option

☑ Enable Centralized Recording

Recording Type: Extension based Recording

Note: You need to configure individual extension or trunk to start recording.

Central Location: ftp://timer:******@10.30.5.141

Gateways Configuration

☑ Gateways Use FTP Protocol to Transmit Recorded Files to Central Location

FTP Server: 10.30.5.141

FTP Access Account: timer

FTP Path:

Password: *****

Please ensure the following procedures are setup correctly to store recorded files:

1. FTP Server must be installed and configured properly on the Central Location machine.
2. FTP Path must point to the FTP folder in the Central Location machine.

Figure 50. Recording Configuration Window

CHAPTER

9

Application Extension Configuration

The application extension is an extension pilot number that allows an SDK-based add-on application to log into the system and establish a communication channel to control trunk channels and interact with the system core PBX switching and voice processing service.

Typical applications that use an application extension are:

- IVR
- Outbound dialer
- Inbound call routing logic for a special business application

To connect an SDK-based add-on application, you need:

- An APC license (concurrent session)
- A separate application extension to log in to for each application

For more information about SDK, please send e-mail to sdksupport@altigen.com.

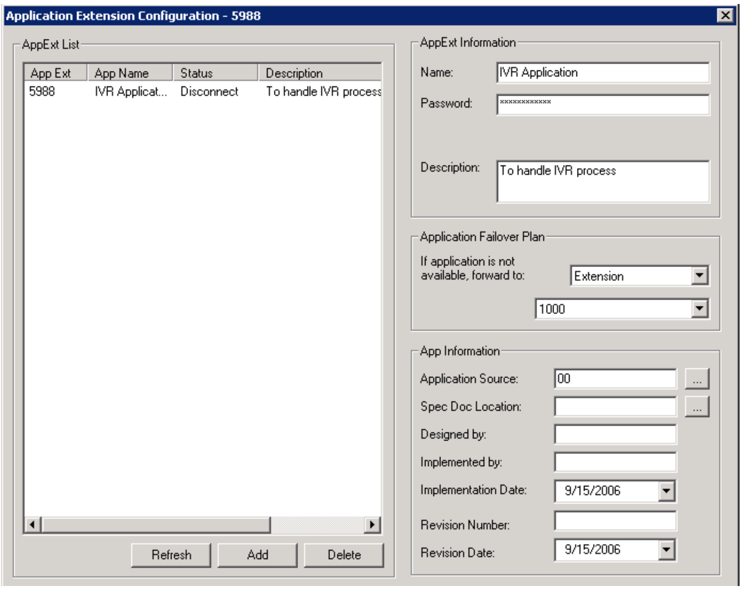
Note: The APC SDK license is not supported in the MaxCS Private Cloud service.

Application Extension Setup

Note: Before you begin, make sure a **Trunk Control APC SDK Session** license is registered and activated for your system. You can find this information in **License** > **License Information**.

To access the **Application Extension Configuration** window, select **System** > **Application Ext Configuration**.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.



Application Extension Configuration - 5988

AppExt List

App Ext	App Name	Status	Description
5988	IVR Applicat...	Disconnect	To handle IVR process

AppExt Information

Name: IVR Application

Password: ************

Description: To handle IVR process

Application Failover Plan

If application is not available, forward to: Extension

1000

App Information

Application Source: 00

Spec Doc Location:

Designed by:

Implemented by:

Implementation Date: 9/15/2006

Revision Number:

Revision Date: 9/15/2006

Figure 51. Application Extension Configuration window

To set up an application extension,

1. In the Application Extension Configuration window, click the **Add** button and enter an extension number in the dialog box. Click **OK**.
2. The application extension appears in the **AppExt List**.
3. Type a password in the **Password** field.
4. Type a description of the application in the **Description** field, if desired.
5. Click **OK**.

Application Failover Plan

The **Application Failover Plan** ensures that a call made to the extension will be automatically transferred if the application is not available. Use the **If application is not available, forward to** list to select the forwarding destination. The options are:

- **AA** – Select the auto attendant number to use in the list under the option. AA settings are configured in **System > AA Configuration**.
- **Extension** – Select an extension from the list.
- **Operator** – Select an operator from the list.
- **Disconnect** – Disconnect the call

Important: If the failover setting for the application extension is set to an extension, and the extension is RNA or busy, the call will follow the extension's RNA or busy call handling.

Application Information

Additional information can be described in the **App Information** fields. If desired, enter the appropriate information in the fields for **Application Source**, **Spec Doc Location**, **Designed by**, **Implemented by**, **Implementation Date**, **Revision Number** and **Revision Date**.

Readying the Application

If a third-party application is connecting to this extension, make sure the application is properly set to log into the application extension. If the third-party application is logged in, the status shown in the figure in *Application Extension Setup* changes to “connected.”

CHAPTER

10

Board Configuration

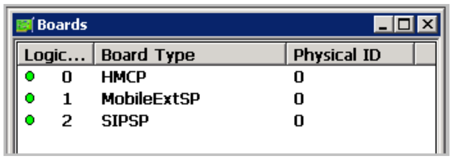
This chapter shows how to configure Altigen telephony boards:

- Triton Resource Board: see Using the Triton Resource Board
- Triton 30-Party Conference Board: see “Using the Triton MeetMe Conference Board” on page 89
- Triton Analog Station Board: see “Configuring the Triton Analog Station Board” on page 89
- Triton Analog Trunk LS/GS and LS Boards: see “Configuring the Triton Analog Trunk LS/GS and LS Boards” on page 90
- Triton VoIP Board: see “Configuring the Triton VoIP Board” on page 90
- Triton T1/E1 Boards: see “Configuring the Triton T1/E1 Board” on page 91
- Virtual Board SIP: see “Configuring Virtual Board SIPSP” on page 104
- Virtual Board HMCP: see “Configuring Virtual Board HMCP” on page 109
- MAX1000/2000 Board: see “Configuring the MAX1000/2000 Board” on page 115
- Virtual MobileExtSP Board: see “Configuring the Virtual MobileExtSP Board” on page 116

For information on how to install Altigen boards, refer to the ***Quick Installation Guide*** provided with every board package.

Configuring Boards

Board attributes and functions are accessible from the Boards window. Double-click the board that you want to configure. The Board Configuration window opens.

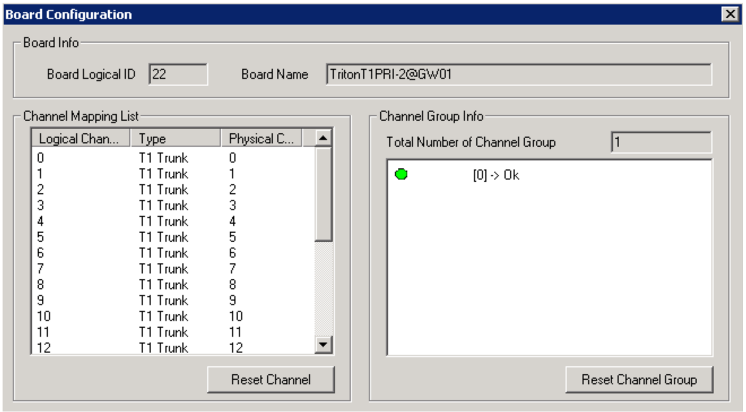


Boards

Logic...	Board Type	Physical ID
● 0	HMCP	0
● 1	MobileExtSP	0
● 2	SIPSP	0

Figure 52. Boards window

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.



Board Configuration

Board Info

Board Logical ID: 22

Board Name: TritonT1PRI-2@GW01

Channel Mapping List

Logical Chan...	Type	Physical C...
0	T1 Trunk	0
1	T1 Trunk	1
2	T1 Trunk	2
3	T1 Trunk	3
4	T1 Trunk	4
5	T1 Trunk	5
6	T1 Trunk	6
7	T1 Trunk	7
8	T1 Trunk	8
9	T1 Trunk	9
10	T1 Trunk	10
11	T1 Trunk	11
12	T1 Trunk	12

Channel Group Info

Total Number of Channel Group: 1

● [0] -> Ok

Figure 53. Board Configuration window

Board Configuration Parameters

These are the attributes and buttons in the Board Configuration window (see each board type in the sections that follow for additional notes on each type):

Parameter	Description
Board Info	**Board Logical ID**: assigned by MaxCS. **Board Name**: the type of board installed in the system and its physical ID.
Channel Mapping List	**Logical Channel**, **Type**, and **Physical Channel** for the entire board. Double-click a channel to open a line configuration dialog box or a trunk configuration dialog box, as appropriate. To reset the channel, select the channel to reset and click the **Reset Channel** button, then click **OK**.
Channel Group Info	Applicable to T1/E1 and the MAX family of boards only. Double-click a channel group to open a configuration dialog box. To reset a channel group, select it and click the **Reset Channel Group** button.
Board Configuration button	Opens a configuration dialog box.
Reset Board button	Resets the board, after you confirm. **Important!** Resetting a board will disconnect all calls in progress on that board. Be sure to inform all users before resetting a board. Additionally, if the board is a resource board (VoIP 12 port, VoIP 30 port, Triton resource board, 30-party conference board), resetting it will disconnect all calls that use the resource.

Important: To implement some board configuration changes, you must shut down and restart by choosing **Services > Shut Down All Services** (which also closes MaxCS) and then restarting MaxCS. If this is necessary, a message will pop up telling you so.

Using the Triton Resource Board

The Triton resource board requires no configuration. Board resources are available when the board is installed.

The resource board has a maximum of 12 bridges for:

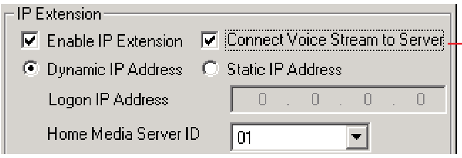
- 6-party conferencing. When an extension is trying to make a conference call, the system will try to use the conference bridge on the resource board first. If conference bridges on the resource board are all busy, the system will use the conference bridges on the extension board, analog or VoIP board.
- Workgroup supervisor silent monitoring, barge-in, and coaching.

For example, if two supervisors are coaching agents, only 10 bridges are left for 6-party conferencing.

Notes:

If a supervisor tries to perform silent monitoring, barge-in, or coaching ***and there is no resource board in the system,* the supervisor will hear an error tone**.

If the supervisor is using an IP phone, then **Connect Voice Stream to Server** should be checked in the Extension Configuration window so that the system can pull the caller and agent's voice stream to the resource board to allow the supervisor to tap into the conversation.


IP Extension

☑ Enable IP Extension ☑ Connect Voice Stream to Server

● Dynamic IP Address ○ Static IP Address

Logon IP Address: 0 . 0 . 0 . 0

Home Media Server ID: 01

This option is in the Extension Configuration window

Using the Triton MeetMe Conference Board

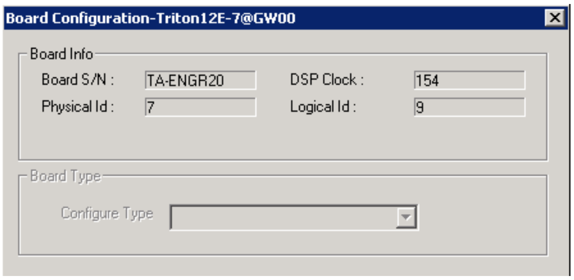
The Triton MeetMe conference board requires no configuration. Board resources are available when it is installed. You do have to assign a MeetMe Conference extension (select **PBX > MeetMe Conference Configuration**).

One MeetMe conference board is supported in a system.

Configuring the Triton Analog Station Board

Double-click the Triton Analog Station board in the **Boards** window to open the **Board Configuration** window, similar to Figure 53. Note the following additional information:

- Double-clicking a channel in the **Channel Mapping List** opens a Triton Analog Line configuration dialog box. See “Triton Analog Station Line Properties” on page 173.
- Clicking the **Board Configuration** button opens a configuration dialog box that displays the board’s serial number, DSP clock, physical and logical IDs.


Board Configuration-Triton12E-7@GW00

Board Info

Board S/N : TA-ENGR20

DSP Clock : 154

Physical Id : 7

Logical Id : 9

Board Type

Configure Type:

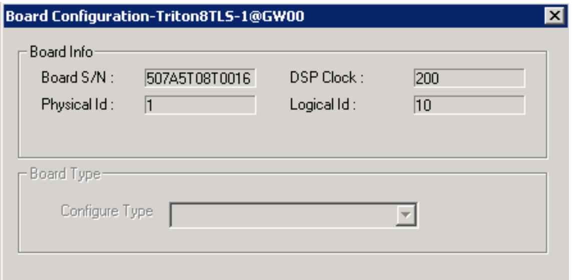
Figure 54. Board Configuration dialog box

Configuring the Triton Analog Trunk LS/GS and LS Boards

The Triton Analog Trunk board is a long form factor PCI telephony card that supports 8 or 12 trunks. The 8 port card supports only loop start (LS). The 12 port card is available in two models; loop start/ground start (LS/GS) and LS. Both models have the same features regarding LS. The LS/GS board is required when ground start trunks may be required.

Double-click the board in the **Boards** window to open the **Board Configuration** window, Note the following additional information:

- Double-clicking a channel in the **Channel Mapping List** opens a channel configuration dialog box. See “Triton Analog Station Line Properties” on page 173.
- Clicking the **Board Configuration** button opens the following dialog box that displays the board’s serial number, DSP clock, physical and logical IDs.


Board Configuration-Triton8TLS-1@GW00

Board Info

Board S/N : 507A5T08T0016

DSP Clock : 200

Physical Id : 1

Logical Id : 10

Board Type

Configure Type

Figure 55. Board Configuration dialog box

Configuring the Triton VoIP Board

It is strongly recommended that system administrators review the “Network Configuration Guidelines for VoIP” on page 303 before setting up VoIP features.

VoIP for MaxCS runs on SIP protocols that allow voice calls to be made through an IP network. It includes an integrated VoIP gateway to convert voice calls into IP packets and transmit them through the IP network.

MaxCS VoIP uses DSP engines residing on the Triton VoIP board to perform the voice coding/decoding functions needed for SIP devices.

The Triton VoIP board can be configured as a 12-port G.711/G.723.1/G.729AB or 30-port G.711 board.

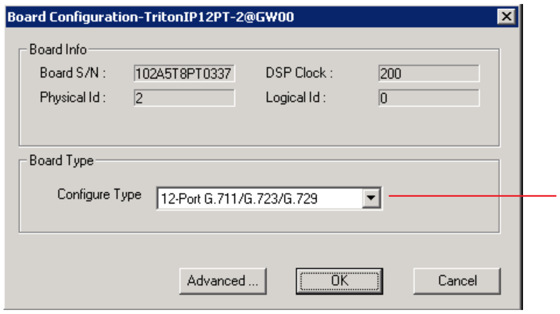
For limitations on configuring Triton VoIP boards and ports see Altigen’s *Telephony Hardware Manual*.

To configure the board,

Double-click the TritonIP board in the **Boards** window to open the **Board Configuration** window, similar to (see Figure 53 on page 88). See the attribute descriptions in *Board Configuration Parameters*.

Note the following additional information:

- Clicking the **Board Configuration** button opens a window that displays the board serial number, DSP clock, and physical and logical IDs. The list in the **Configure Type** field lets you select between a 12-port G.711/G.723/G.729 configuration and a 30-port G.711 configuration.



Board Configuration-TritonIP12PT-2@GW00

Board Info

Board S/N : 102A5T8PT0337 DSP Clock : 200

Physical Id : 2 Logical Id : 0

Board Type

Configure Type 12-Port G.711/G.723/G.729

If you change this configuration, you must restart the switching services for the change to take effect.

Figure 56. Board Configuration window

Configuring the Triton T1/E1 Board

Through MaxAdministrator, the Triton T1/E1 board can be configured for either digital T1 CAS (channel associated signaling), T1 PRI (Primary Rate Interface), E1 CAS, or E1 PRI.

Both T1 CAS and T1 PRI carry 24 channels using time-division multiplexing (TDM) at an overall rate of 1.544 Mbps. Voice T1 provides 24 64K channels with robbed bit signaling. T1 PRI provides 23 64K channels, using one 64K channel for D channel messaging.

E1 CAS and E1 PRI carry 32 channels using TDM at an overall rate of 2.048 Mbps. Both of them provide 30 64K channels for voice.

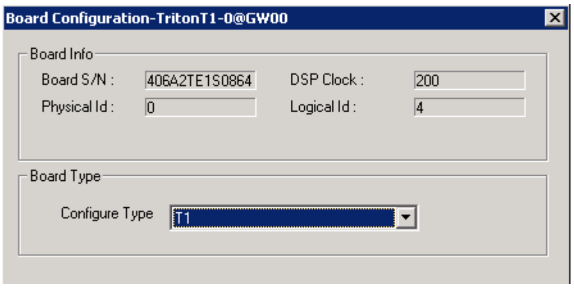
To subscribe to T1 CAS, T1 PRI, E1 CAS, or E1 PRI service, you must supply certain parameters. These parameters are listed in Appendix B on page 421.

Configuring the Board

Double-click the Triton T1/E1 board in the **Boards** window to open the **Board Configuration** window, similar to (see Figure 53 on page 88). See attribute descriptions below (see Figure 53). Note the following additional information:

- The Board ID must be in the range 0 - 7.
- Double-click a channel in the **Channel Mapping List** to open a trunk configuration dialog box.
- Double-click a channel group to open a configuration window, discussed in the following section.
- Clicking the **Board Configuration** button opens a configuration dialog box that displays the board’s serial number, DSP clock, physical and logical IDs.

  You can configure the board type: either **T1** or **E1** to run T1 CAS, T1 PRI, or E1 CAS, E1 PRI. Additional steps are needed to further configure the CAS or PRI protocol in the Protocol Configuration window, shown in the figures in section *Setting up Channels on the Triton T1/E1 Board*.



Board Configuration-TritonT1-0@GW00

Board Info

Board S/N : 406A2TE1S0864 DSP Clock : 200

Physical Id : 0 Logical Id : 4

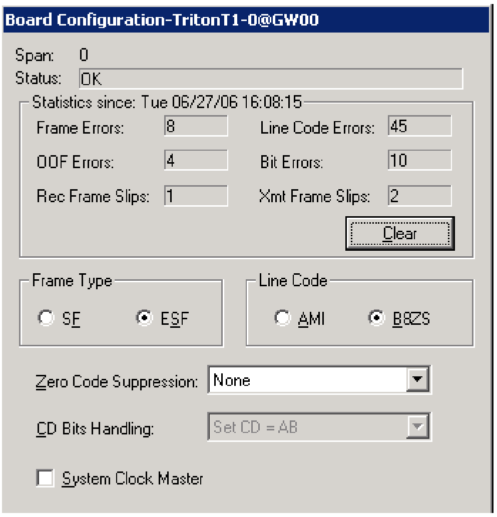
Board Type

Configure Type T1

Figure 57. Triton T1/E1 Configuration dialog box

T1 and E1 Configuration

Double-clicking a channel group for a Triton T1 board in the **Channel Group Info** pane opens a **T1** or **E1 Configuration** dialog box, as in the next two figures.



Board Configuration-TritonT1-0@GW00

Span: 0

Status: OK

Statistics since: Tue 06/27/06 16:08:15

Frame Errors: 8

Line Code Errors: 45

OOF Errors: 4

Bit Errors: 10

Rec Frame Slips: 1

Xmt Frame Slips: 2

Frame Type: ○ SF ● ESF

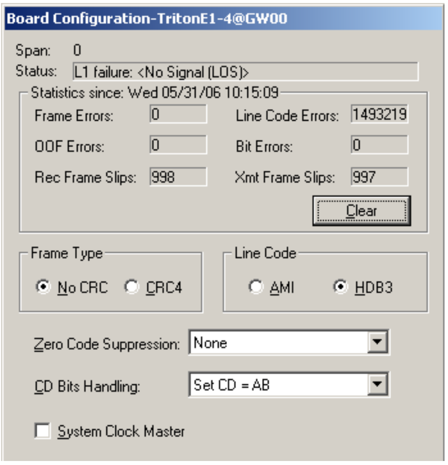
Line Code: ○ AMI ● B8ZS

Zero Code Suppression: None

CD Bits Handling: Set CD = AB

☐ System Clock Master

Figure 58. Triton T1 configuration dialog box



Board Configuration-TritonE1-4@GW00

Span: 0

Status: L1 failure: <No Signal (LOS)>

Statistics since: Wed 05/31/06 10:15:09

Frame Errors: 0

Line Code Errors: 1493219

OOF Errors: 0

Bit Errors: 0

Rec Frame Slips: 998

Xmt Frame Slips: 997

Frame Type: ● No CRC ○ CRC4

Line Code: ○ AMI ● HDB3

Zero Code Suppression: None

CD Bits Handling: Set CD = AB

☐ System Clock Master

Figure 59. Triton E1 configuration dialog box

Reading the Status Messages

If the channel group is working, the **Status** line displays **OK**. This status line is updated every 3 seconds. If there is an error, a message is displayed. The following table lists the types of error messages and the appropriate actions.

Error Message	Meaning	Action
HW failure: <No Answer>	Major hardware problem. Board is not responding to commands. Reasons could be: 1) DSP loading failure; 2) If PRI, board failed.	1. Reset board. 2. If error continues, replace board.
HW failure: <No Clocks>	No clock signal is detected on T1 interface drop.	1. Check MVIP clock. 2. Reset board. If this does not work, replace board.
L1 failure: <No Signal (LOS)>	Layer 1 failure, physical layer; LOS = Loss of Analog Signal	Check T1/PRI cable and change if necessary. If cable is okay, CO is not sending any signal. Contact CO.
L1 failure: <Alarm Indication Signal (AIS)>	Layer 1 failure, CO sends all 1's to our T1/E1; AIS = Alarm Indicator Signal; all ones detected	To locate the AIS alarm, have the carrier check the T1 network element connected to the T1 interface and trace the problem.
L1 failure: <Remote Alarm Indication (RAI)>	Layer 1 failure, CO notifies that the configuration is wrong; RAI = Remote Alarm Indicator	Correct the settings.
L1 failure: <No Sync Frames	Layer 1 failure, physical layer; no valid framing is detected.	Possible span mis-configuration (ESF is selected but the actual framing is SF, or vice versa). Check span configuration.
L1 failure: <Red Alarm>	Layer 1 failure, physical layer; Bi-Polar Violations (BPV), Line Code Violations (LCV), or Out Of Frame detected	Location condition, equipment problem. - For excessive BPV/LCV, check AMI/B8ZS setting. - For OOF, check the MVIP bus master setting. OR Have CO perform a line test to check for a faulty cable or line.
[PRI only] L2 Failure: <No Sync Flag>	Layer 2 failure, data link layer; no sync flag has been detected in data link layer	Check if D-channel is active or not
[PRI only] L2 Failure: <Not established>	Layer 2 failure, data link layer; the peer-to-peer link has not established in data link layer	CO must activate HDLC link

Reading the Statistics

The **Statistics** panel displays the number of errors that have occurred since the last system reboot or statistics clearing. There may be non-zero values when configuring the T1 span for the first time. You can clear these fields with the **Clear** button.

Error	Meaning
Frame Errors	Number of framing bit errors. In T1 mode, a framing bit error is defined as an incorrect FS-bit value. The counter is suppressed when framer loses frame alignment
OOF Errors	The Out Of Frame counter registers every time the T1 chip is forced to re-frame when receiving a frame with severe errors.
Rec Frame Slips	The Receiver Frame Slips counter shows the number of frame slips for the receiver.
Line Code Errors	Line Code Error is defined as an occurrence of a bi-polar variation or excessive zeroes.
Bit Errors	Bit Errors are defined as a CRC-6 error in ESF, FT-bit error in SLC-96 and F-bit or sync bit error in SF.
Xmt Frame Slips	Transmit Frame Slips counter shows the number of frame slips for the transmitter
Clear button	Use the **Clear** button to reset the statistics counters.

Note: For ideally synchronized systems, **Transmit** and **Receive Frame Slips** counters should be ‘0.’ Continuous update of the frame slips counters means that transmit and receive frequencies are not equal. In this case, you should check the system and CT-Bus clock setup.

Setting the Configurable Options

These are the options you can set:

Option	Notes
Frame Type	• For T1, you can set the **Frame Type** to either **SF** or **ESF**. **SF** (Superframe Format) consists of 12 consecutive frames. **ESF** (Extended Superframe Format) consists of 24 consecutive frames. • For **E1**, you can set the **Frame Type** to either **No CRC** or **CRC4**. **CRC4** is embedded into 16 consecutive frames.
Line Code	• For T1, you can set the **Line Code** to either **AMI** or **B8ZS**. **AMI** (Alternate Mark Inversion) is the line coding format in T1 transmission systems whereby successive ones (marks) are alternately inverted and sent with opposite polarity of the preceding mark. **B8ZS** (Binary 8 Zero Substitution) sends two violations of the bipolar line encoding technique, rather than inserting a one for every seven consecutive zeros. • For **E1**, you can set the **Line Code** to either **AMI** or **HDB3**. **HDB3** (High Density Bipolar Order) is based on AMI, but extends this by inserting violation codes whenever there is a run of four or more zeros.
Zero Code Suppression	You can set the **Zero Code Suppression** to **None** (default setting), **Jam Bit 8**, **GTE** or **Bell**. **Zero Code Suppression** inserts a “one” bit to prevent the transmission of eight or more consecutive “zero” bits; **Jam Bit 8** forces every bit 8 to a one; **GTE** Zero Code Suppression replaces bit 8 of an all zero channel byte to a one, except in signaling frames where bit 7 is forced to a one. **Bell** Zero Code Suppression replaces bit 7 of an all zero channel byte with a one.

Option	Notes
CD Bits Handling	CD Bits Handling is not editable.
System Clock Master	You can set the **System Clock Master** *if* you have a back-to-back configuration and you want this span to be the master clock to the system. (Only one clock master should be selected in a back-to-back system.) See the following section on T1/E1 clocking.

T1/E1 Clocking

Depending on the configuration of the T1/E1 boards and span for your MaxCS systems, the **System Clock Master** setup should be set according to the follow conditions:

- If all of the T1/E1 boards are connected to a carrier's switch, the **System Clock Master** check box must ***not*** be checked for *any* of the T1/E1 boards.
- If two MaxCS systems are connected back-to-back with a T1/E1 span, the **System Clock Master** check box *must be checked* for only *one* of the T1/E1 boards.
- If two T1/E1 boards in the same MaxCS system are connected back-to-back with a T1/E1 span, the **System Clock Master** check box *must be checked* for the T1/E1 board that has ***not*** been designated by the CT-Bus setting as the system's master clock to drive the CT-Bus.

Important: For all back-to-back cases, the CT-Bus Clock Configuration should be set to "Manual," and the board that is connected to the board configured as the back-to-back clock master **must** be designated at the CT-Bus master.

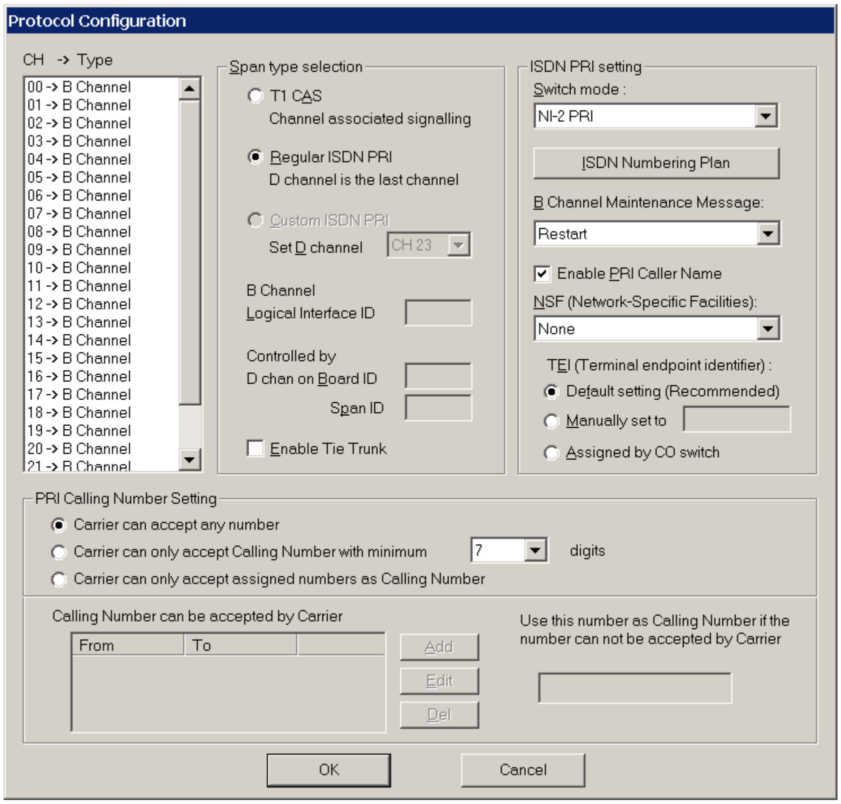
Setting up Channels on the Triton T1/E1 Board

This section discusses setting up T1 CAS, T1 PRI, E1 CAS, or E1 PRI channels on the Triton T1/E1 board.

Click the **Protocol** button in the T1 or E1 configuration dialog box (see the figure in *Configuring the Triton T1/E1 Board*) to open the **Protocol Configuration** window, shown below. The Triton T1/E1 Board can be configured to either CAS or PRI through the configuration options in the window.

The **CH -> Type** list on the left side of the window displays the channel types.

Note: In a tie-trunk configuration, set the trunks to "Out of Service" before changing the trunk type from T1 to PRI or vice versa. Otherwise, the system will generate garbage call records to your internal or external logger service. See "Setting General Trunk Attributes" on page 125 for details.



Protocol Configuration

CH -> Type

00 -> B Channel
01 -> B Channel
02 -> B Channel
03 -> B Channel
04 -> B Channel
05 -> B Channel
06 -> B Channel
07 -> B Channel
08 -> B Channel
09 -> B Channel
10 -> B Channel
11 -> B Channel
12 -> B Channel
13 -> B Channel
14 -> B Channel
15 -> B Channel
16 -> B Channel
17 -> B Channel
18 -> B Channel
19 -> B Channel
20 -> B Channel
21 -> B Channel

Span type selection

○ T1 CAS
Channel associated signalling

● Regular ISDN PRI
D channel is the last channel

○ Custom ISDN PRI
Set D channel: CH 23

B Channel
Logical Interface ID:

Controlled by
D chan on Board ID:
Span ID:

□ Enable Tie Trunk

ISDN PRI setting

Switch mode : NI-2 PRI

ISDN Numbering Plan

B Channel Maintenance Message: Restart

☑ Enable PRI Caller Name

NSF (Network-Specific Facilities): None

TEI (Terminal endpoint identifier) :
● Default setting (Recommended)
○ Manually set to
○ Assigned by CO switch

PRI Calling Number Setting

● Carrier can accept any number
○ Carrier can only accept Calling Number with minimum 7 digits
○ Carrier can only accept assigned numbers as Calling Number

Calling Number can be accepted by Carrier

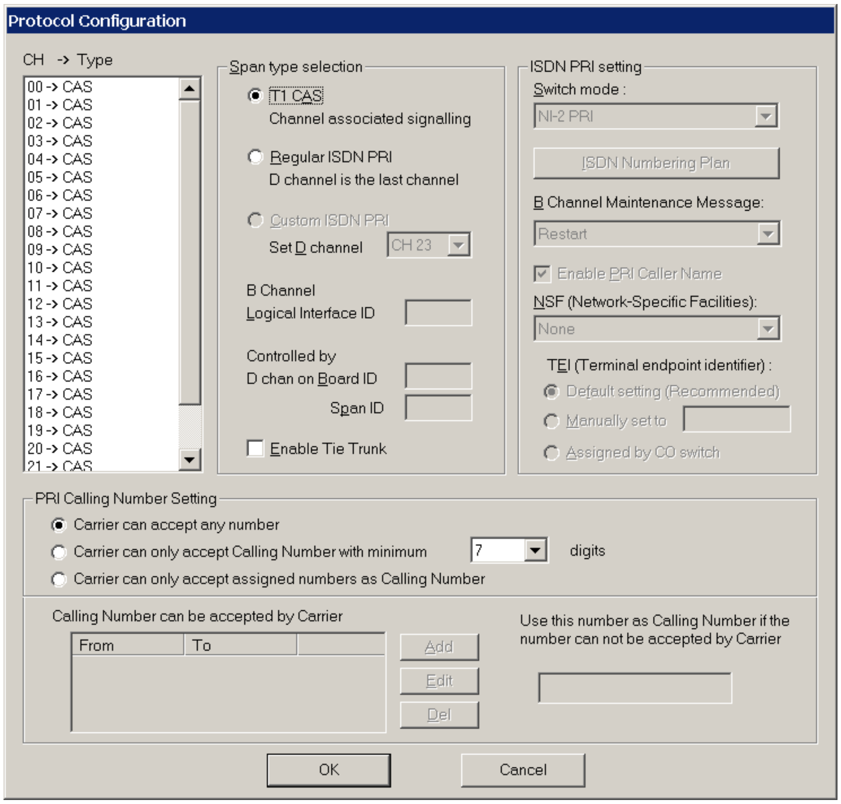
From	To

Add Edit Del

Use this number as Calling Number if the number can not be accepted by Carrier

OK Cancel

Figure 60. T1 PRI Protocol Configuration dialog box (top half)



Protocol Configuration

CH -> Type

00 -> CAS
01 -> CAS
02 -> CAS
03 -> CAS
04 -> CAS
05 -> CAS
06 -> CAS
07 -> CAS
08 -> CAS
09 -> CAS
10 -> CAS
11 -> CAS
12 -> CAS
13 -> CAS
14 -> CAS
15 -> CAS
16 -> CAS
17 -> CAS
18 -> CAS
19 -> CAS
20 -> CAS
21 -> CAS

Span type selection

● T1 CAS
Channel associated signalling

○ Regular ISDN PRI
D channel is the last channel

○ Custom ISDN PRI
Set D channel: CH 23

B Channel
Logical Interface ID:

Controlled by
D chan on Board ID:
Span ID:

☐ Enable Tie Trunk

ISDN PRI setting

Switch mode: NI-2 PRI

ISDN Numbering Plan

B Channel Maintenance Message: Restart

☑ Enable PRI Caller Name

NSF (Network-Specific Facilities): None

TEI (Terminal endpoint identifier):
● Default setting (Recommended)
○ Manually set to
○ Assigned by CO switch

PRI Calling Number Setting

● Carrier can accept any number
○ Carrier can only accept Calling Number with minimum 7 digits
○ Carrier can only accept assigned numbers as Calling Number

Calling Number can be accepted by Carrier

From	To

Add
Edit
Del

Use this number as Calling Number if the number can not be accepted by Carrier

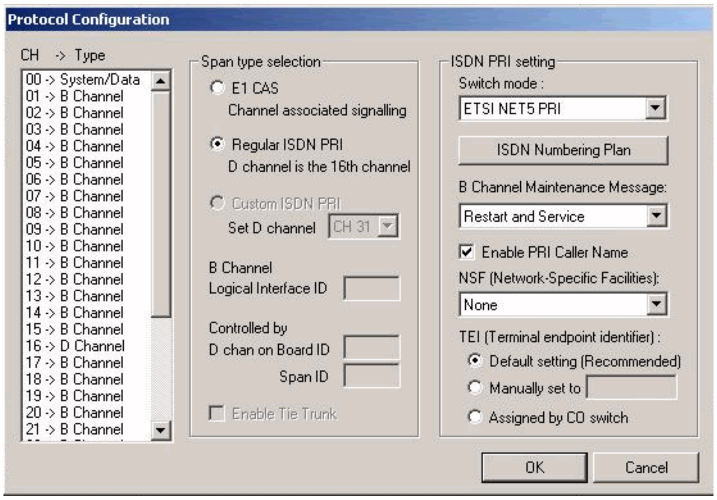
OK Cancel

Figure 61. T1 CAS Protocol Configuration dialog box (top half)

Selecting Span Types

- **T1 CAS –** Select this option to associate all channels on the span to T1 CAS.
- **Regular ISDN PRI** – Select this option to indicate 23B+D ISDN PRI span and to designate the last channel as the D channel.
- **Enable Tie Trunk** – Check this box to enable a tie trunk. Tie trunks must terminate to a system also configured as a tie trunk.

  Note: This option not available when **E1 CAS** is selected.



Protocol Configuration

CH -> Type

00 -> System/Data
01 -> B Channel
02 -> B Channel
03 -> B Channel
04 -> B Channel
05 -> B Channel
06 -> B Channel
07 -> B Channel
08 -> B Channel
09 -> B Channel
10 -> B Channel
11 -> B Channel
12 -> B Channel
13 -> B Channel
14 -> B Channel
15 -> B Channel
16 -> D Channel
17 -> B Channel
18 -> B Channel
19 -> B Channel
20 -> B Channel
21 -> B Channel

Span type selection

○ E1 CAS
Channel associated signalling

● Regular ISDN PRI
D channel is the 16th channel

○ Custom ISDN PRI
Set D channel: CH 31

B Channel Logical Interface ID:

Controlled by D chan on Board ID:

Span ID:

□ Enable Tie Trunk

ISDN PRI setting

Switch mode: ETSI NET5 PRI

ISDN Numbering Plan

B Channel Maintenance Message: Restart and Service

☑ Enable PRI Caller Name

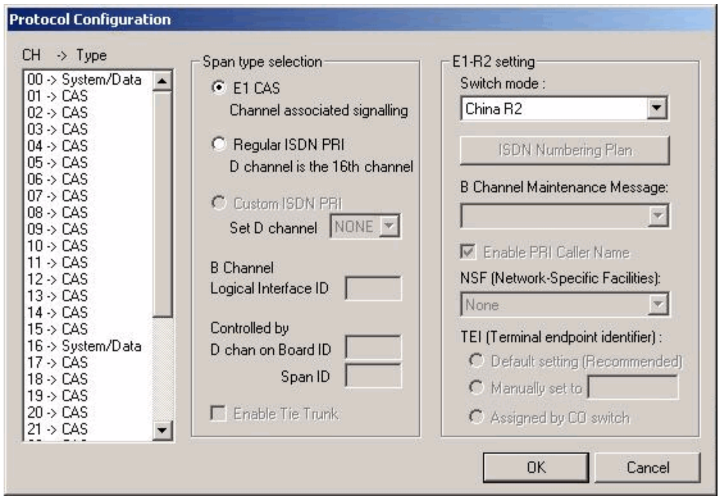
NSF (Network-Specific Facilities): None

TEI (Terminal endpoint identifier):

● Default setting (Recommended)
○ Manually set to
○ Assigned by CO switch

OK | Cancel

Figure 62. E1 PRI Protocol Configuration dialog box (top half)



Protocol Configuration

CH -> Type

00 -> System/Data
01 -> CAS
02 -> CAS
03 -> CAS
04 -> CAS
05 -> CAS
06 -> CAS
07 -> CAS
08 -> CAS
09 -> CAS
10 -> CAS
11 -> CAS
12 -> CAS
13 -> CAS
14 -> CAS
15 -> CAS
16 -> System/Data
17 -> CAS
18 -> CAS
19 -> CAS
20 -> CAS
21 -> CAS

Span type selection

● E1 CAS
Channel associated signalling

○ Regular ISDN PRI
D channel is the 16th channel

○ Custom ISDN PRI
Set D channel: NONE

B Channel Logical Interface ID:

Controlled by D chan on Board ID:

Span ID:

□ Enable Tie Trunk

E1-R2 setting

Switch mode: China R2

ISDN Numbering Plan

B Channel Maintenance Message:

☑ Enable PRI Caller Name

NSF (Network-Specific Facilities): None

TEI (Terminal endpoint identifier):

○ Default setting (Recommended)
○ Manually set to
○ Assigned by CO switch

OK | Cancel

Figure 63. E1 CAS Protocol Configuration dialog box (top half)

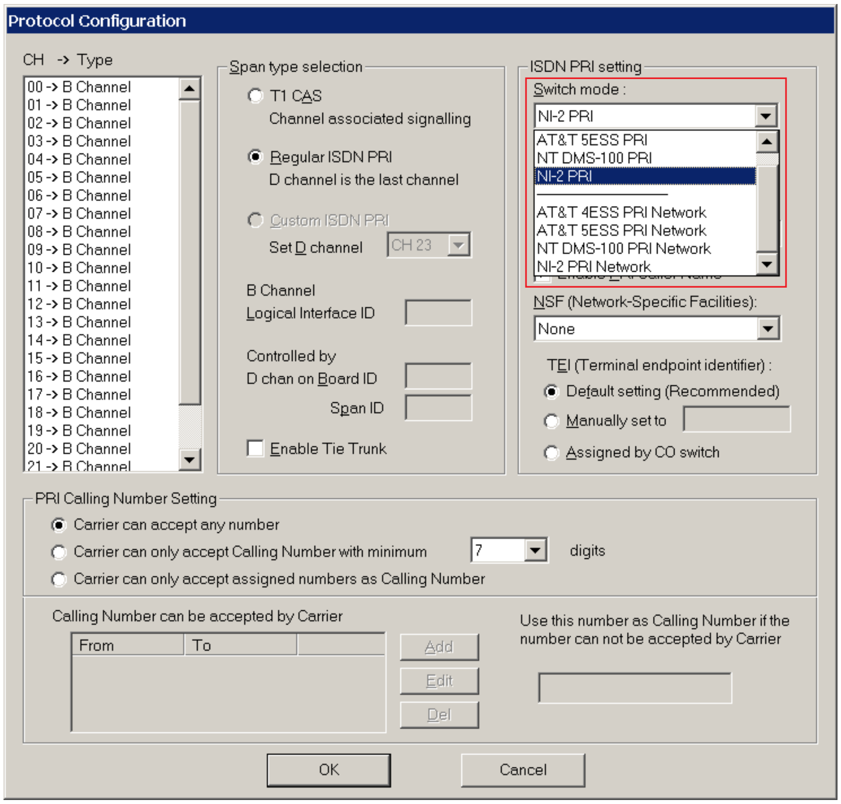
Selecting Span Types

- **E1 CAS –** Select this option to associate all channels on the span to E1 channel associated signaling.
- **Regular ISDN PRI –** Select this option to indicate 30B+D ISDN PRI span and to designate the 16th channel as the D channel.
- **Enable Tie Trunk** – Check this box to enable a tie trunk. Tie trunks must terminate to a system also configured as a tie trunk.

  Note: This option not available when **T1 CAS** is selected.

Setting the ISDN PRI Switch Mode

If you select a Span Type of Regular ISDN PRI in the T1 PRI Configuration Window, use the following guidelines to set the ISDN PRI Switch mode.



Protocol Configuration

CH -> Type

00 -> B Channel
01 -> B Channel
02 -> B Channel
03 -> B Channel
04 -> B Channel
05 -> B Channel
06 -> B Channel
07 -> B Channel
08 -> B Channel
09 -> B Channel
10 -> B Channel
11 -> B Channel
12 -> B Channel
13 -> B Channel
14 -> B Channel
15 -> B Channel
16 -> B Channel
17 -> B Channel
18 -> B Channel
19 -> B Channel
20 -> B Channel
21 -> B Channel

Span type selection

○ T1 CAS
Channel associated signalling

● Regular ISDN PRI
D channel is the last channel

○ Custom ISDN PRI
Set D channel: CH 23

B Channel
Logical Interface ID:

Controlled by
D chan on Board ID:
Span ID:

□ Enable Tie Trunk

ISDN PRI setting

Switch mode: NI-2 PRI

AT&T 5ESS PRI
NT DMS-100 PRI
NI-2 PRI

AT&T 4ESS PRI Network
AT&T 5ESS PRI Network
NT DMS-100 PRI Network
NI-2 PRI Network

NSF (Network-Specific Facilities): None

TEI (Terminal endpoint identifier):
● Default setting (Recommended)
○ Manually set to
○ Assigned by CO switch

PRI Calling Number Setting
● Carrier can accept any number
○ Carrier can only accept Calling Number with minimum 7 digits
○ Carrier can only accept assigned numbers as Calling Number

Calling Number can be accepted by Carrier

From	To

Use this number as Calling Number if the number can not be accepted by Carrier

Figure 64. T1 PRI Switch Mode

The top four settings are used for a connection to a CO switch:

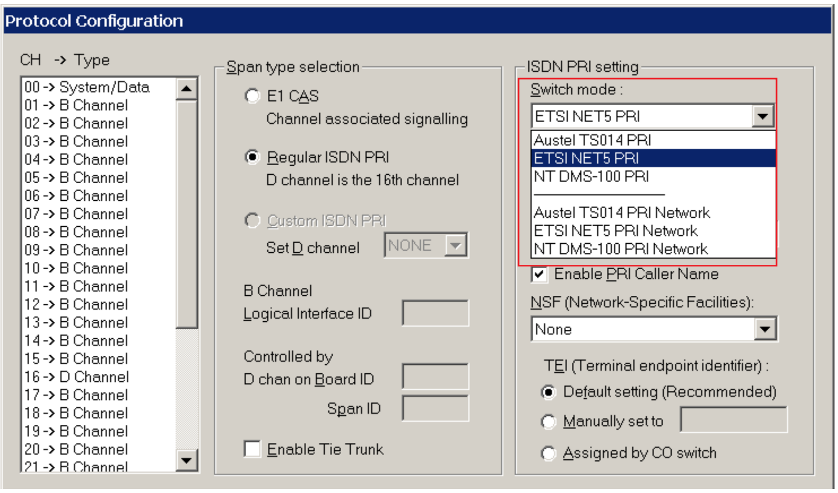
- AT&T 4ESS PRI
- AT&T 5ESS PRI
- NT DMS-100 PRI
- NI-2 PRI (default)

The bottom four settings are used for a PRI tie trunk configuration where two MaxCS systems are connected back to back. In such a configuration, one MaxCS system must be configured as Network and the other as User. For example, set one to NI-2 PRI Network and the other to NI-2 PRI.

- AT&T 4ESS PRI Network
- AT&T 5ESS PRI Network
- NT DMS-100 PRI Network
- NI-2 PRI Network

If you select a Span Type of Regular ISDN PRI in the E1 PRI Configuration window, use the following guidelines to set the ISDN PRI Switch mode.

E1 PRI



Protocol Configuration

CH -> Type

00 -> System/Data
01 -> B Channel
02 -> B Channel
03 -> B Channel
04 -> B Channel
05 -> B Channel
06 -> B Channel
07 -> B Channel
08 -> B Channel
09 -> B Channel
10 -> B Channel
11 -> B Channel
12 -> B Channel
13 -> B Channel
14 -> B Channel
15 -> B Channel
16 -> D Channel
17 -> B Channel
18 -> B Channel
19 -> B Channel
20 -> B Channel
21 -> B Channel

Span type selection

○ E1 CAS
Channel associated signalling

● Regular ISDN PRI
D channel is the 16th channel

○ Custom ISDN PRI
Set D channel: NONE

B Channel
Logical Interface ID

Controlled by
D chan on Board ID
Span ID

□ Enable Tie Trunk

ISDN PRI setting

Switch mode : ETSI NET5 PRI

Austel TS014 PRI
ETSI NET5 PRI
NT DMS-100 PRI
Austel TS014 PRI Network
ETSI NET5 PRI Network
NT DMS-100 PRI Network

☑ Enable PRI Caller Name

NSF (Network-Specific Facilities): None

TEI (Terminal endpoint identifier) :
● Default setting (Recommended)
○ Manually set to
○ Assigned by CO switch

Figure 65.   E1 PRI Switch Mode

The top three settings are used for a connection to a CO switch:

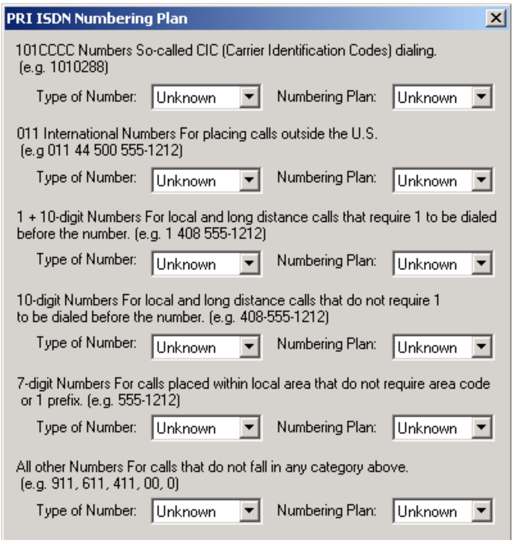
- Austel TS014 PRI
- ETSI NET5PRI
- NT DMS-100 PRI

The bottom three settings are used for a PRI tie trunk configuration where two MaxCS systems are connected back to back. In such a configuration, one MaxCS system must be configured as Network and the other as User. For example, set one to NT DMS-100 PRI Network and the other to NT DMS-100 PRI.

- Austel TS014 PRI Network
- ETSI NET5PRI Network
- NT DMS-100 PRI Network

Configuring an ISDN Numbering Plan

The **ISDN Numbering Plan** button in the Protocol Configuration window opens the **PRI ISDN Numbering Plan** dialog box. This function allows you to select how the system will identify and code the Called Number for six different types of calls. This coding instructs the CO on how to interpret the number being sent to it.



PRI ISDN Numbering Plan

101CCCC Numbers So-called CIC (Carrier Identification Codes) dialing.
(e.g. 1010288)

Type of Number: Unknown Numbering Plan: Unknown

011 International Numbers For placing calls outside the U.S.
(e.g 011 44 500 555-1212)

Type of Number: Unknown Numbering Plan: Unknown

1 + 10-digit Numbers For local and long distance calls that require 1 to be dialed before the number. (e.g. 1 408 555-1212)

Type of Number: Unknown Numbering Plan: Unknown

10-digit Numbers For local and long distance calls that do not require 1 to be dialed before the number. (e.g. 408-555-1212)

Type of Number: Unknown Numbering Plan: Unknown

7-digit Numbers For calls placed within local area that do not require area code or 1 prefix. (e.g. 555-1212)

Type of Number: Unknown Numbering Plan: Unknown

All other Numbers For calls that do not fall in any category above.
(e.g. 911, 611, 411, 00, 0)

Type of Number: Unknown Numbering Plan: Unknown

Figure 66. PRI ISDN Numbering Plan dialog box

The **PRI ISDN Numbering Plan** dialog box displays the six *classes* of numbers (call type) that can be sent to a CO:

- 101CCCC Numbers – CIC (Carrier Identification Codes) dialing.
- 011 International Numbers – For placing calls outside the U.S.
- 1+10-digit Numbers – For local and long distance calls that require dialing 1 before the number.
- 10-digit Numbers – For local and long distance calls that do not require 1 before dialing.
- 7-digit Numbers – For calls placed within the local area that do not require an area code or a 1 prefix.
- All Other Numbers – For calls that do not fall into any category above, for example, 911, 311.

For each class, select the type of *number/numbering plan* from the list:

- Type of Number:
  - Unknown
  - International
  - National
  - Network Specific
  - Subscriber Number
- Numbering Plan:
  - Unknown
  - ISDN
  - National
  - Private

The setting **Unknown** is used when the user or network has no knowledge of the numbering plan. In this case, the number digits field is organized according to the network dialing plan.

B Channel Maintenance Message:

This setting controls B channel initialization and maintenance message exchange between MaxCS and the CO, when the system starts up. Select the maintenance message that will be delivered on the B Channel:

- **None** – No maintenance message sent; puts channel in ready state automatically.
- **Restart** – Only sends RESTART message; puts channel in ready state when RESTART ACK (acknowledgement) response is received from CO.
- **Service** – Only sends SERVICE message; puts channel in ready state when SERVICE ACK (acknowledgement) response is received from CO.
- **Restart and Service** – (The default setting) sends both RESTART and SERVICE message; puts channel in ready state when RESTART ACK and SERVICE ACK is received from CO.

Enable PRI Caller Name – Check this to enable PRI caller name

Setting the NSF

The **NSF (Network-Specific Facilities)** is used with PRI to instruct the CO to route a call to a specific carrier or long distance service. Use the list to identify the type of carrier service you want to use for your ISDN PRI lines.

The choices in the list depend on the specific switch and your long distance service provider. An example of such service includes AT&T Megacom.

Note: If your CO requires specific NSF features to be present in the call setup packet, please contact Altigen’s Technical Support department with such information from the CO and they will help you configure it.

Setting a TEI

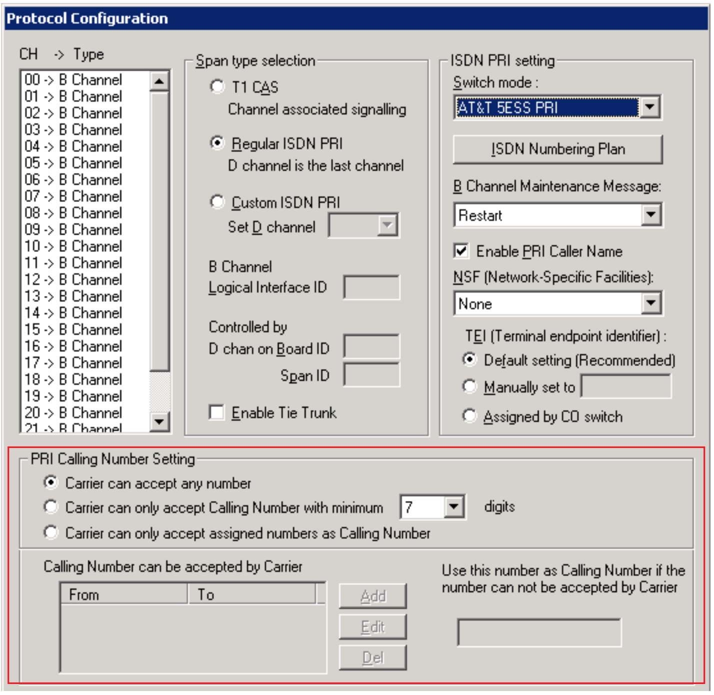
The **TEI (Terminal Endpoint Identifier)** defines which terminal device is communicating with the CO switch for a given message. PRI messages involve point-to-point configuration in which each side already knows the source of any message received. ISDN messages involve point to multi-point locations in which the source can only be identified by the TEI.

Select one of the following TEI settings:

- **Default setting** – This is the recommended setting.
- **Manually set to** – This should always be set to 0. Typically, a zero (0) is used for TEI on a PRI connection. In some cases where a shared D channel is used, other TEI values might be required to identify which span will be used for a call.
- **Assigned by CO switch** – Do not use this setting unless advised by your CO.

Setting PRI Calling Numbers

A PRI Calling Number Setting in the bottom half of the Protocol Configuration dialog box lets you set the numbers you want your Carrier to accept.



Protocol Configuration

CH -> Type

00 -> B Channel
01 -> B Channel
02 -> B Channel
03 -> B Channel
04 -> B Channel
05 -> B Channel
06 -> B Channel
07 -> B Channel
08 -> B Channel
09 -> B Channel
10 -> B Channel
11 -> B Channel
12 -> B Channel
13 -> B Channel
14 -> B Channel
15 -> B Channel
16 -> B Channel
17 -> B Channel
18 -> B Channel
19 -> B Channel
20 -> B Channel
21 -> B Channel

Span type selection
○ T1 CAS
Channel associated signalling
● Regular ISDN PRI
D channel is the last channel
○ Custom ISDN PRI
Set D channel
B Channel Logical Interface ID
Controlled by D chan on Board ID
Span ID
□ Enable Tie Trunk

ISDN PRI setting
Switch mode : AT&T 5ESS PRI
ISDN Numbering Plan
B Channel Maintenance Message: Restart
☑ Enable PRI Caller Name
NSF (Network-Specific Facilities): None
TEI (Terminal endpoint identifier) :
● Default setting (Recommended)
○ Manually set to
○ Assigned by CO switch

PRI Calling Number Setting
● Carrier can accept any number
○ Carrier can only accept Calling Number with minimum 7 digits
○ Carrier can only accept assigned numbers as Calling Number

Calling Number can be accepted by Carrier

From	To

Use this number as Calling Number if the number can not be accepted by Carrier

Figure 67. PRI Calling Number Setting

Most PRI trunks allow a MaxCS system to send calling numbers. For example, 10 different extensions in the same PBX system have 10 different DID numbers. With the calling number feature provided by Carriers, the callee will receive a more accurate caller ID.

PRI Calling Number can also be used in a mobile extension or IP hop-off to PRI trunk, so the callee can receive a more accurate caller ID.

When a PRI span is subscribed, a block of DID numbers will be provided by the Carrier. The Carrier should be able to accept Calling Numbers in the DID number block. However, if the numbers are not in the blocks or the digit lengths are mismatched, the Carrier might "reject" the call.

The **PRI Calling Number Setting** addresses this issue. Choose from three options:

- Carrier can accept anything as Calling Number (default)
- Carrier can only accept Calling Number with a minimum of *n* digits
- Carrier can accept only assigned numbers as the Calling Number.

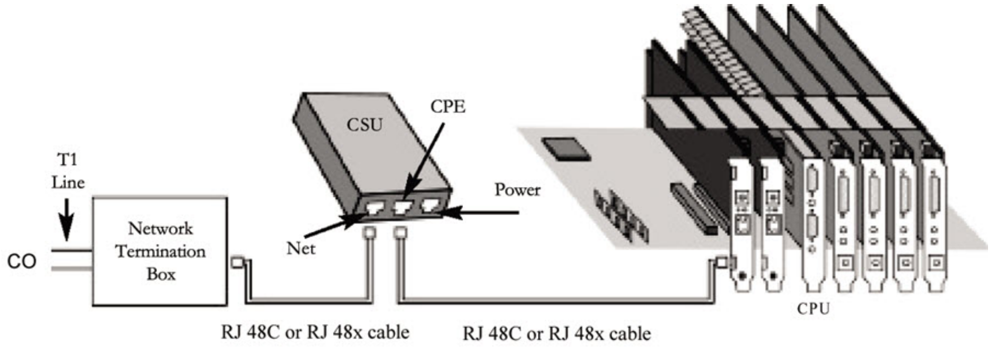
If you select the third option, specify “assigned numbers” by clicking the **Add** button and entering the numbers. To edit or delete a number you added, select it and click the **Edit** or **Delete** button.

If MaxCS detects the Calling Number is not accepted by the Carrier, it will always send the number you enter in the text box at the lower right side of the dialog box as the Calling Number. Enter an appropriate Calling Number in this box.

Installing a Channel Service Unit (CSU)

This section discusses installing a CSU to the Triton T1 or T1/E1 Board. The channel service unit is a device used to connect a digital trunk line coming in from the phone company to the PBX. A CSU can terminate signals, repeat signals, and respond to loopback commands sent from the central office. A CSU is mandatory for connecting to Altigen’s T1/E1 board.

1. Connect the CSU (Adtran model T1 CSU ACE used as an example) to the T1/PRI or T1/E1 PRI board using an RJ-48C or RJ-48X cable.
2. Connect the CSU to the network termination box using an RJ-48C or RJ-48X cable.



Altigen T1 Socket (RJ-48)
Pin 1=Receive Ring (INPUT)
Pin 2=Receive Tip (INPUT)
Pin 4=Transmit Ring (OUTPUT)
Pin 5=Transmit Tip (OUTPUT)

Refer to your CSU manufacturer's manual for the proper pinout.

Note: CSUs also are used for line lengths over 75 feet, which helps to resolve attenuation issues.

Troubleshooting T1/E1 Common Symptoms

The most common problems when installing T1 CAS or T1 PRI services:

1. The service provider misconfigures your T1 CAS/T1 PRI service or terminates your service improperly.
2. T1 is installed but not turned on because there is no termination device for a period of time.
3. T1 is turned on but channel is not in service.

MaxCS provides basic troubleshooting information in the T1 Span Configuration window, described in “T1 and E1 Configuration” on page 92.

Configuring Virtual Board SIPSP

A VoIP connection typically consists of two parts.

- **Signal Channel** – Responsible for setting up and tearing down a call using protocol. For example, SIP protocol is used in MaxCS to build a signal channel between the server and the IP phone.
- **Media Path** – Responsible for encoding, transmitting, and decoding voice for both parties. For example, when an IP phone user makes a call to an outside number, the voice will be encoded at the IP phone, transmitted to the system via the IP network, decoded by the VoIP codec, and passed to a trunk port so that the external party will hear the voice.

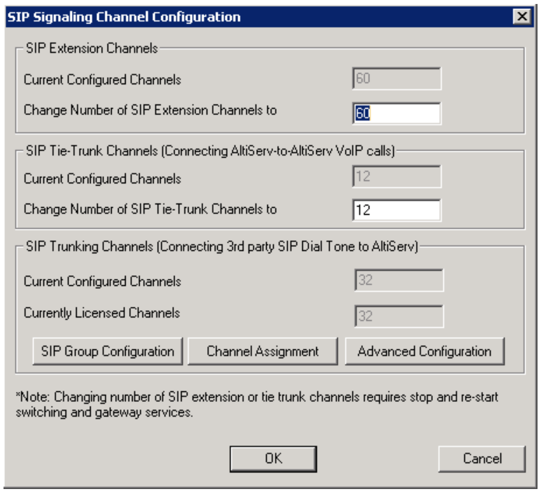
The purpose of the virtual boards SIPSP is to build signal channels for different connection types, IP extensions, SIP Tie Trunks, and SIP Trunking from ITSP. Each channel will have its channel ID similar to channels on a Triton extension or trunk board. When an IP phone registers to the system, a channel ID will be assigned to the IP extension. However, these channels are only responsible for processing protocol and call control signals. They require a media path from a VoIP board or from the IP phone to establish a voice steam so that both sides can hear.

Notes:

- Make sure you have enough VoIP resource boards.
- The more signal channels, the more system memory and CPU power required. Proper planning is essential.
- Changing the number of signal channels requires that you stop and restart the switching and gateway services.
- SIP Trunking Channel requires a license to activate.

Configuring the SIPSP Board

Double-clicking a SIPSP board in **Boards** view and then clicking the **Board Configuration** button opens the SIP Signaling Channel Configuration panel.



SIP Signaling Channel Configuration

SIP Extension Channels

Current Configured Channels: 60

Change Number of SIP Extension Channels to: 60

SIP Tie-Trunk Channels (Connecting AltiServ-to-AltiServ VoIP calls)

Current Configured Channels: 12

Change Number of SIP Tie-Trunk Channels to: 12

SIP Trunking Channels (Connecting 3rd party SIP Dial Tone to AltiServ)

Current Configured Channels: 32

Currently Licensed Channels: 32

*Note: Changing number of SIP extension or tie trunk channels requires stop and re-start switching and gateway services.

Figure 68. The SIP Signalling Channel Configuration panel

MaxCS is set by default to support 60 SIP extension channels. You can change the number of SIP extension channels and tie-trunk channels. The maximum number possible depends of the system CPU performance, call volume, and usage. If a high performance machine is used as the Softswitch server, the number of channels can be more than 1000. If you change the numbers in this dialog box, you must shut down and restart the switching and gateway services for this change to take effect. When the services restart, the new configuration appears in the **Currently Configured Channels** fields.

Note: If you change the number of SIP extension or tie trunk channels, you must stop and restart the switching and gateway services.

The **SIP Trunking Configuration** button opens the SIP Trunking Configuration dialog box. (See “SIP Trunk Properties” on page 129.)

Click **Advanced Configuration** to manage the *Trusted SIP Device* list.

About The Trusted SIP Device List

The Trusted SIP Device list, and its counterpart, the Malicious SIP Device list, show you which SIP devices have been registered (the Trusted list) and which SIP devices have been blocked from MaxCS (the Malicious list).

In earlier releases of MaxCS, administrators had a single option: whether to automatically blockSIP Invite requests if the IP address associated with that device was not already configured in the IP Dialing Table or the Trusted SIP Device list. In addition, IP extensions for the following devices were added to the Trusted SIP Device list automatically, once they successfully register to the system (unless they are found in the Malicious SIP Device list): Altigen IP phones, Third-Party SIP devices, and IPTalkdevices.

Beginning with Release 9.0.1, you have more options, which are described in the following sections.

Automatically Add Unknown Devices to Malicious Device Lists

This release includes updates to give you more flexible control over new devices registering with your MaxCS server.

In general,

- If a packet comes in and the device's IP address is listed in the Malicious SIP Device list, then no traffic is allowed from that device.
- If the device's IP address is listed in the Trusted SIP Device list, then traffic is allowed but the device still needs the correct password to register to the MaxCS server.

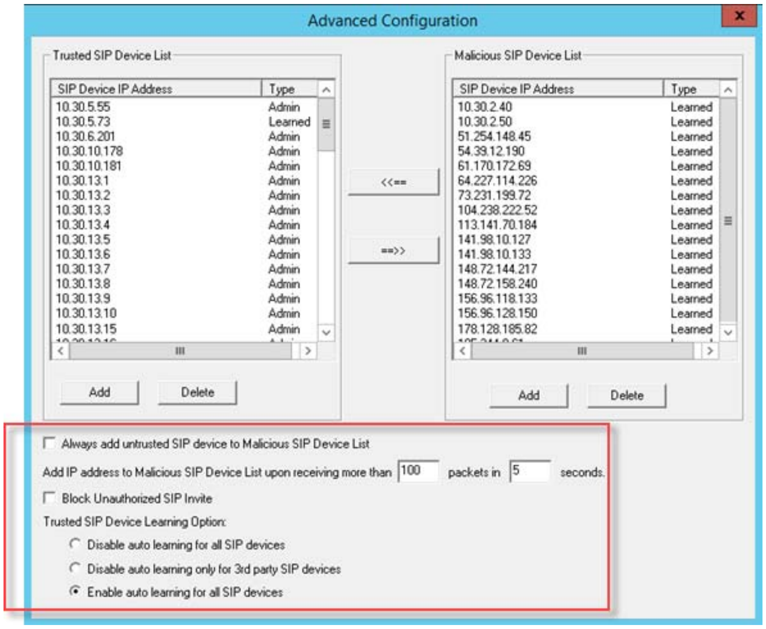
A new option in the Advanced Configuration panel lets you have tighter control on device access.

- Always add untrusted SIP devices to Malicious SIP Device List

  When this option is enabled, if a device tries to connect with this MaxCS server and the device's SIP Address is not listed in the Trusted SIP Device list, then the device's IP address will be added to the Malicious SIP Device List automatically.

Note that if a user works from home and tries to register a phone, its IP address may show up in the Malicious SIP Device List. The admin can then manually move this device IP address from the Malicious List to the Trusted List.

If you enable this option, all other options in this panel will be disabled.



Advanced Configuration

Trusted SIP Device List

SIP Device IP Address	Type
10.30.5.55	Admin
10.30.5.73	Learned
10.30.6.201	Admin
10.30.10.178	Admin
10.30.10.181	Admin
10.30.13.1	Admin
10.30.13.2	Admin
10.30.13.3	Admin
10.30.13.4	Admin
10.30.13.5	Admin
10.30.13.6	Admin
10.30.13.7	Admin
10.30.13.8	Admin
10.30.13.9	Admin
10.30.13.10	Admin
10.30.13.15	Admin

Malicious SIP Device List

SIP Device IP Address	Type
10.30.2.40	Learned
10.30.2.50	Learned
51.254.148.45	Learned
54.39.12.190	Learned
61.170.172.69	Learned
64.227.114.226	Learned
73.231.199.72	Learned
104.238.222.52	Learned
113.141.70.184	Learned
141.98.10.127	Learned
141.98.10.133	Learned
148.72.144.217	Learned
148.72.158.240	Learned
156.96.118.133	Learned
156.96.128.150	Learned
178.128.185.82	Learned

☐ Always add untrusted SIP device to Malicious SIP Device List

Add IP address to Malicious SIP Device List upon receiving more than 100 packets in 5 seconds.

☐ Block Unauthorized SIP Invite

Trusted SIP Device Learning Option:

○ Disable auto learning for all SIP devices

○ Disable auto learning only for 3rd party SIP devices

● Enable auto learning for all SIP devices

Figure 69. The Trusted SIP Device Learning options

SIP Device Auto-Learning Options

Starting with Release 9.0.1, once a SIP device successfully registers to the MaxCS server you have three options for controlling whether or not that device's SIP address will be added to the Trusted SIP Device list. After a SIP device is added to Trusted SIP Device List, its SIP Address will not be added to Malicious SIP Device List regardless of how heavy the traffic pattern is.

- **Disable auto-learning for all SIP devices**. This is the strictest option; no SIP device that has successfully registered will be automatically added to the Trusted SIP Device list. This option requires administra-tors to manually add any new devices that should be considered trusted.
- **Disable auto-learning only for third-party SIP devices**. This is the default option; only Altigen IP Phones and Polycom phones that have successfully registered will be automatically added to the Trusted SIP Device list.
- **Enable auto-learning for all SIP devices**. This option is the least restrictive choice; all SIP devices that have successfully registered will be automatically added to the Trusted SIP Device list.

  Note that your existing devices will become trusted as learned devices after you upgrade to Release 9.0.

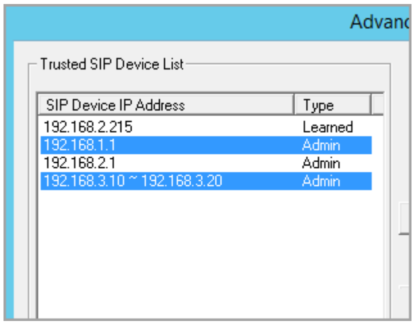
In the SIP Device List, the Type column will show one of two categories:

- **Learned** - The device was auto-learned
- **Admin** - The device was manually added to the trusted list by an admin

Note: Your existing devices will automatically become trusted (as Learned devices) after you upgrade to Release 9.0.1.

In the SIP Device List, the *Type* column will show one of two categories for each IP Address:

- **Learned** - The device was auto-learned
- **Admin** - The device was manually added to the trusted list by an admin



SIP Device IP Address	Type
192.168.2.215	Learned
192.168.1.1	Admin
192.168.2.1	Admin
192.168.3.10 ~ 192.168.3.20	Admin

Figure 70. The Trusted SIP Device list showing entries as Learned or Admin

To move an IP address from one list to the other, select the IP address and click either the right or left arrow.

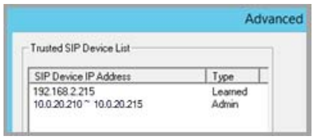
New Devices With Incorrect Passwords Put in Malicious List Immediately

Beginning with Release 9.0.1, when a new (non-configured) SIP device tries to register with an invalid password, that device's IP address will now be put *immediately* into the Malicious SIP Device List. No further SIP packets from this device will be processed.

Adding IP Ranges into Trusted Device Lists

Beginning with Release 9.0.1, you can now add IP ranges into the SIP Device lists.

To do this, type in both the beginning IP address and the ending IP address in the dialog box.



SIP Device IP Address	Type
192.168.2.215	Learned
10.0.20.210 ~ 10.0.20.215	Admin

Figure 71. The Trusted SIP Device list showing a range of SIP addresses

You will see the entry in the SIP Device list as a range; for example, 10.0.2.120 ~ 10.0.2.125.

When adding ranges to a SIP Device List, please observer the following limitations:

- A maximum of 20 IP ranges are allowed in a list
- Each IP range can contain up to 1,024 IP addresses

Selecting Multiple IP Addresses in a List

Beginning with Release 9.0, you can select more than one IP Address in the SIP Device lists.

You can use these techniques to move multiple IP addresses from one list to another or to delete multiple IP addresses from a list:

- Use Ctrl-Click to select individual IP addresses in the list.
- User Shift-Click to select the beginning and ending IP addresses, to select a contiguous range.

Fax Routing

To simplify administrative tasks, you can allow voice and fax calls to run on the same SIP trunk channel. This feature applies only to systems using Altigen SIP trunks. The trunks must be configured to support both voice and fax.

The SIP trunk uses the same SIP server IP address, but different authentication credentials for voice trunk versus a fax trunk.

You configure fax routing through options for the SIP Group. See the discussion in the section *SIP Group Configuration* on page 131.

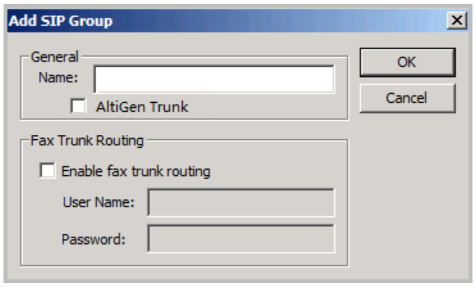


Figure 72. The Enable Fax Trunk Routing checkbox

Configure Out Call routing just as voice and fax are supported in the same SIP trunk assigned with this SIP Trunk Profile. Outbound calls made through SIP channels configured for fax channels are for fax only. Hence they should not be assigned trunk access codes or be included in the out call routing for voice calls.

For Altigen SIP trunks, you must configure one SIP trunk channel to perform SIP registration for GW1 and GW2 of voice trunk and GW1 and GW2 of the fax trunk individually.

Configuring Virtual Board HMCP

This section is for a gateway Softswitch with an HMCP media server installation only. A single all-in-one system does not require configuration of this board.

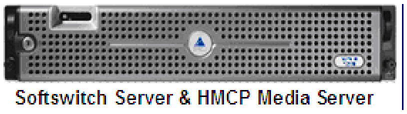
Host Media Control Processing (HMCP) is a virtual board that uses an Intel CPU to provide the following functions:

1. Process VoIP Media Stream
   - Encode, decode, and transcode voice stream
   - Detect and generate tone for IP devices
   - Play music when device is on hold
2. Play and Record Voice Files

- Announce system and queue phrases
   - Process auto attendant
   - Process voice mail
   - Call recording for IP extensions

3. Provide Conferencing Resources
   - Station conference
   - Meet-Me conference
   - Barge-in/silent monitor/coaching

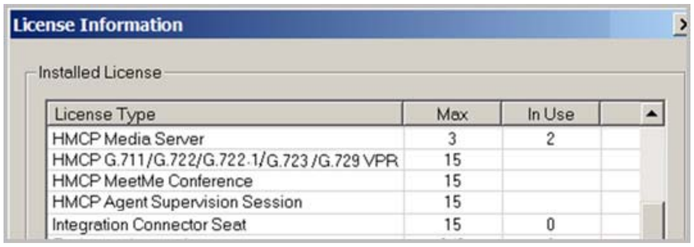
From a deployment point of view, an HMCP media server can be installed in the same Softswitch system sharing the same CPU or can be in a stand-alone server with a dedicated CPU.



In MaxCS, the HMCP system has been redesigned 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 better more consistent performance.

Notes

- Do not install HMCP service in a system with Altigen's Triton telephony board. It will cause resource conflict.
- Remove the Triton Resource board and MeetMe conference board from OFFICE systems running as a gateway.
- An HMCP Media Server license is required to activate an HMCP virtual board.



License Information

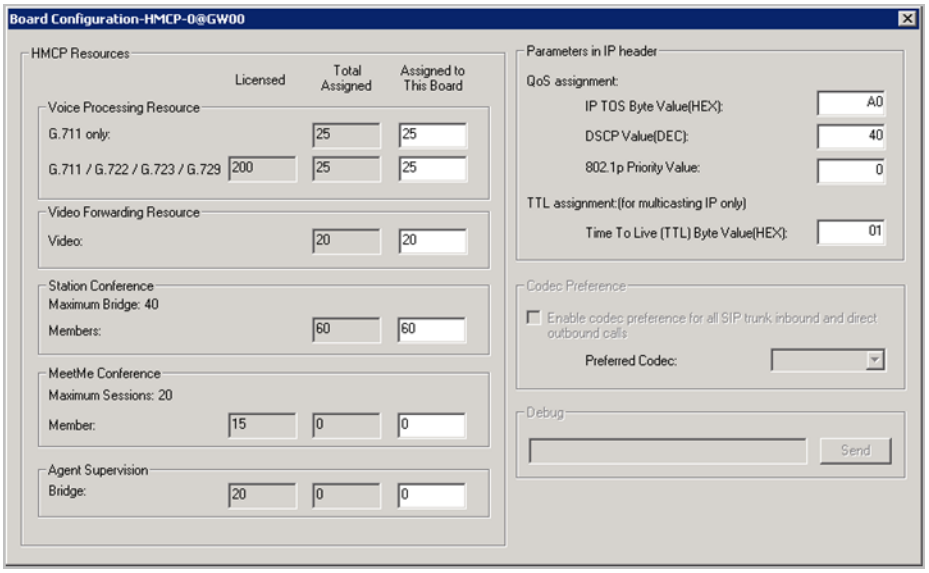
Installed License

License Type	Max	In Use
HMCP Media Server	3	2
HMCP G.711/G.722/G.722.1/G.723/G.729 VPR	15	
HMCP MeetMe Conference	15	
HMCP Agent Supervision Session	15	
Integration Connector Seat	15	0

Figure 73. Example of HMCP licenses in the License Information list

By default the system grants 60 conference members in a maximum of 40 bridges.

You can change the number to as many as 120 members in a maximum of 40 bridges, and you can activate other HMCP resources, by double-clicking an HMCP board in Boards view and then clicking **Board Configuration**.



Board Configuration-HMCP-0@GW00

HMCP Resources

	Licensed	Total Assigned	Assigned to This Board
Voice Processing Resource			
G.711 only:		25	25
G.711 / G.722 / G.723 / G.729	200	25	25
Video Forwarding Resource			
Video:		20	20
Station Conference Maximum Bridge: 40			
Members:		60	60
MeetMe Conference Maximum Sessions: 20			
Member:	15	0	0
Agent Supervision			
Bridge:	20	0	0

Parameters in IP header

QoS assignment:

IP TOS Byte Value(HEX): A0

DSCP Value(DEC): 40

802.1p Priority Value: 0

TTL assignment:(for multicasting IP only)

Time To Live (TTL) Byte Value(HEX): 01

Codec Preference

☐ Enable codec preference for all SIP trunk inbound and direct outbound calls

Preferred Codec:

Debug

If you decrease the number of HMCP resources, the system must be rebooted for the configuration to take effect.

If you increase the number of resources, the system does not have to be rebooted.

Figure 74. The HMCP Board Configuration window

You may change the assigned number by entering a different number (up to the number your system is licensed for and not to exceed the maximum limit for each HMCP board) in the **Assigned to this board** fields and clicking **Apply**.

HMCP Resources – Shows the total number licensed (if applicable), total currently assigned, and the number assigned to this HMCP board for the following resource types:

- Voice Processing Resources (VPR)
- Video Forwarding Resources (for Polycom VVX phones) – You must assign sufficient video forwarding resources. Be aware that the additional resources you assign may result in a small performance decrease. Refer to the *MaxCS 8.0 Polycom Configuration Guide* for details.
- Station Conference Members
- MeetMe Conference Members
- Agent Supervision Bridges

The maximum number of resources that can be supported on an HMCP virtual board is as follows:

- G.711 VPR — 1,000
- G.711 / G.722 / G.723 / G.729 VPR
- Station Conference Members — 120
- MeetMe Conference Members — 120
- Agent Supervision Bridges — 20

Notes

- Codec G.722 is part of a combo codec and is controlled by license.
- When adding additional combo licenses, the system will also increase the RTP ports it uses and will use these new ports. If these additional ports are not added to the firewall ,calls will not have audio.
- 1,000 G.711 voice processing resources will be licensed to the system when one HMCP Media Server license is registered.
- The more VPR assigned, the slower the system will be when it starts up. To calculate the optimized number of VPR you need, use the following formula:

  Total G.711 VPR = Total number of extensions X 2

  Total G.711/G.722/G.723/729 VPR = Total number of remote IP phone users + Total Tie Trunk Channels that will use compressed codec
- Adding HMCP licenses or changing assigned numbers does not require restarting the Altigen switching service.
- In the event that you need to decrease the assigned numbers of HMCP resources (reassigned to the second HMCP server, for example), the system must be rebooted for the configuration to take effect.

Parameters in IP Header - QoS and TTL assignments.

QoS assignment – IP TOS/DiffServ Byte Value. The default TOS/DiffServ byte hex value **"**A0**"** (10100000) signals the network switch and router that RTP packets are "Critical". To set the value for Diffserv Code Expedited Forwarding (DSCP EF), you can enter hex value "B8" (10111000).

TTL assignment – For IP paging multicasting only. The purpose of the TTL (Time To Live) is to regulate how many hosts the IP paging packets can pass through. The TTL value is reduced by one on every hop. You may need to adjust this value if there are remote Altigen IP phones at different locations that register to MaxCS through WAN and require the IP paging feature. The value will be the number of routers from MaxCS to remote IP phone plus one.

Media Pass-Through Support for HMCP

One feature in MaxCS for system performance and voice quality is the Media Pass-through feature. This feature applies only to HMCP Softswitch systems; it is enabled by default.

While the Media Pass-through feature is enabled, the HMCP driver doesn't need to do encoding and decoding on both channels. This approach has the following benefits:

- Improved system performance, because no MIPS is required for codec processing
- Improved voice quality, because no distortion is introduced by additional compressed codecs
- Reduced voice latency, because it eliminates the delay introduced by codec and jitter buffer processing

In addition to benefits to direct calls, pass-through applies during call recording, silent monitoring, and coaching.

G.722 pass-through is enabled by default.

Conditions Not Supported

Media pass-through cannot support all conditions in the HMCP system, even if both connected channels are using same codec. The following MaxCS features do not supported media pass-through:

- Call playing – The trunk call playing must use encoder and decoder on RTP channel
- Conference calls – All RTP channels in a conference bridge must be encoded and decoded voice

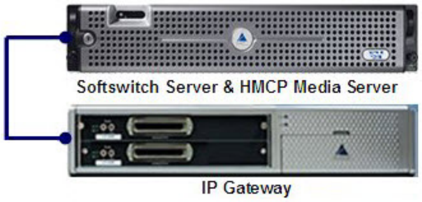
Assign HMCP Resources to IP Extensions

After you configure the HMCP board, you need to configure extensions to use the HMCP voice processing, conferencing, and recording resources.

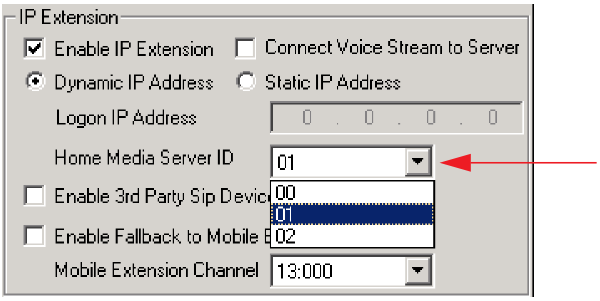
In **Extension Configuration** > **General** > **IP Extension** panel, change the **Home Media Server ID** to the HMCP Media Server ID if necessary. Please refer to the following scenarios.

Scenario: Single Standalone HMCP Media Server

For 200 to 1,000 users without an extensive amount of recording resources, fewer than 200 concurrent recording sessions, deploy a stand-alone HMCP Media server as shown below.



The Home Media Server ID should be changed to "01" for all IP extensions, assuming HMCP Media server is using ID 01.


IP Extension

☑ Enable IP Extension ☐ Connect Voice Stream to Server

● Dynamic IP Address ○ Static IP Address

Logon IP Address 0 . 0 . 0 . 0

Home Media Server ID 01

☐ Enable 3rd Party Sip Devic

☐ Enable Fallback to Mobile E

Mobile Extension Channel 13:000

HMCP Codec Preference

MaxCS includes a feature that is designed to help you reduce the CPU consumption that occurs are a result of codec encoding and decoding. It allows you to indicate a codec preference (G.729 or G.711) for calls handled via a SIP trunk. This approach eliminates the steps of encoding and decoding - packets are directly forwarded to the endpoint.

Note: Hardware chassis and hardware gateway configurations do not support the Codec Preference option.

The preference that you set must be supported by the SIP Trunk provider, and must be included in the codec profile list for SIP Trunks.

While this feature is enabled, then the SIP device's codec configuration in Enterprise Manager will be ignored.

Codec preference applies to HMCP only.

All SIP devices must support G.711 uLaw; if there are no common codecs on the device side, and then G.711 uLaw will be used.

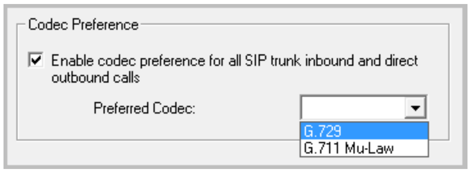
This codec preference applies to all SIP Trunk inbound calls and direct extension to SIP trunk outbound calls that are initiated from a phone or dialed via a MaxCS client.

Fax-over IP overrides this setting; it will always use G.711.

Outbound calls initiated by the system (such as calls from the voicemail system or ONA) may not use the preferred codec.

To configure this feature,

1. Log into MaxAdministrator with the superpassword. If you do not log in via the superpassword, the feature will not be enabled.
2. Open the HMCP board configuration panel (double-click **HMCP** in the Boards window).
3. To enable the feature, select the checkbox and specify which codec to use (G.729 or G.711 Mu-Law). Click **Ok**.



Codec Preference

☑ Enable codec preference for all SIP trunk inbound and direct outbound calls

Preferred Codec:

Figure 75. The Codec Preference setting

Codec Preference - Incoming Calls

When the Codec Preference feature is enabled, the system uses the following logic for handling incoming calls, based upon the content of the first SIP INVITE request.

Preferred Codec G.729	
First SIP Invite Request Content	**Codec Used for the Call**
SIP Trunk supports G.729	The IP Codec table of Enterprise Manager is ignored. The system uses codec G.729 to negotiate with the endpoint.
SIP Trunk does not support G.729	No codec is enforced.

Preferred Codec G.711 Mu-Law	
First SIP Invite Request Content	**Codec Used for the Call**
SIP Trunk supports G.711 Mu-Law	The IP Codec table of Enterprise Manager is ignored. The system uses codec G.711 Mu-Law to negotiate with the endpoint.
SIP Trunk does not support G.711 Mu-Law	No codec is enforced.

If the target extension or DNIS number is enabled for Fax-Over-IP (FoIP), then no codec is enforced.

Codec Preference - Outgoing Calls, Third-Party IP Phones

When the Codec Preference feature is enabled, the system uses the following logic for handling outgoing SIP trunk calls from third-party IP phones. (Calls are considered SIP trunk calls if the target has a SIP trunk access code or an outcall routing access code prefix.)

Preferred Codec G.729	
First SIP Invite Request Content	**Codec Used for the Call**
Supports G.729	The IP Codec table of Enterprise Manager is ignored. The system uses codec G.729 to negotiate with the endpoint.
Does not support G.729	No codec is enforced.

Preferred Codec G.711 Mu-Law	
First SIP Invite Request Content	**Codec Used for the Call**
Supports G.711	The IP Codec table of Enterprise Manager is ignored. The system uses codec G.711 to negotiate with the endpoint.
Does not support G.711	No codec is enforced.

If the source extension is enabled for Fax-Over-IP (FoIP), then no codec is enforced.

Codec Preference - Outgoing Calls, IP Phones

Because IP Phone SIP call requests are always from MaxCS, the behavior is different from calls from third-party phone extensions.

When a user makes an outgoing call from an IP phone, the system follows the IP Codec table in Enterprise Manager. All IP phones support G.729 and G.711 Mu-Law.

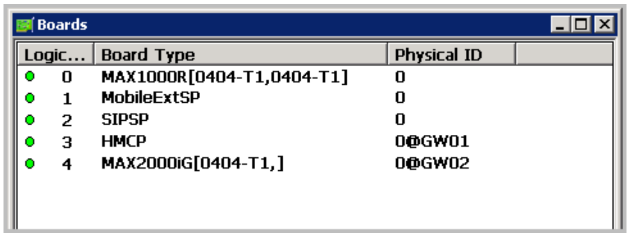
When the Codec Preference feature is enabled, the system uses this logic to handle outgoing SIP trunk calls.

Preferred Codec	Codec Used for the Call
G.729	The system modifies the IP phone's codec in the RE-INVTE SDP body with G.729 codec. After the modification, MaxCS must pick G.729 and G.711 codecs as the preferred codecs to negotiate with the endpoint.
G.711 Mu-Law	The system modifies the IP phone's codec in the RE-INVTE SDP body with G.711 codec. After the modification, MaxCS must pick G.711 and G.729 codecs as the preferred codecs to negotiate with the endpoint.

If the source extension is enabled for Fax-Over-IP (FoIP), then no codec is enforced.

Configuring the MAX1000/2000 Board

The MAX1000/2000 Server is a telecom appliance that consists of an embedded DSP board and two access board slots. MaxCS treats the entire MAX system as one board with two access board options. The Boards window displays the name of the MAX board, followed by [xxyy(-T1),xxyy]:



	Logic...	Board Type	Physical ID
●	0	MAX1000R[0404-T1,0404-T1]	0
●	1	MobileExtSP	0
●	2	SIPSP	0
●	3	HMCP	0@GW01
●	4	MAX2000iG[0404-T1,]	0@GW02

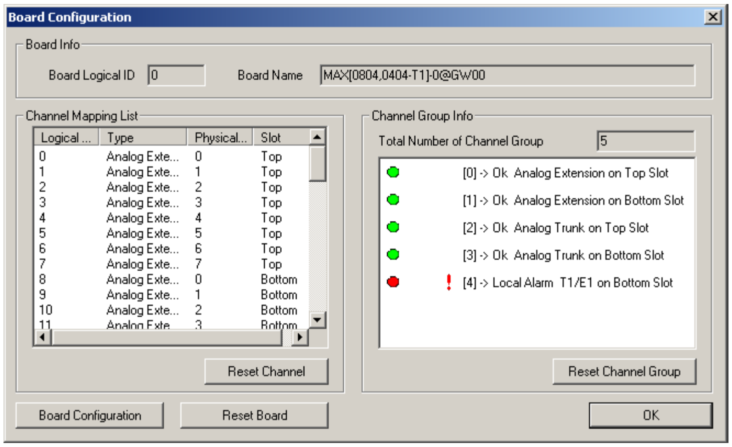
Figure 76. Boards View showing MAX board

xx refers to the number of analog trunks, and yy refers to the number of analog extensions. If an access board has a T1/E1 port, -T1 is added to the end.

In the Boards window, double-click the MAX 1000/2000 board to open the main Board Configuration window.

The **Channel Group Info** panel shows the channel groups (groups of channels that belong to the same type). For example, if one 4x4xT1 access board and one 4x8 access board are installed in the MAX 1000/2000 main board, there will be three channel groups for the 4x4xT1 card, and two channel groups for the 4x8. When one of the channel groups is selected, the **Channel Mapping List** reflects the selection.

- Double-clicking a T1/E1 channel group opens the channel group configuration dialog box. For information on configuring in this dialog box, see “T1 and E1 Configuration” on page 92. This is available on T1 or E1 channel groups only.
- In the channel group configuration dialog box, click the **Protocol** button to open the **Protocol Configuration** dialog box. For information on configuring protocol, see “Setting up Channels on the Triton T1/E1 Board” on page 95.



Board Logical ID: 0

Board Name: MAX[0804,0404-T1]-0@GW00

Logical ...	Type	Physical...	Slot
0	Analog Exte...	0	Top
1	Analog Exte...	1	Top
2	Analog Exte...	2	Top
3	Analog Exte...	3	Top
4	Analog Exte...	4	Top
5	Analog Exte...	5	Top
6	Analog Exte...	6	Top
7	Analog Exte...	7	Top
8	Analog Exte...	0	Bottom
9	Analog Exte...	1	Bottom
10	Analog Exte...	2	Bottom
11	Analog Exte	3	Bottom

Total Number of Channel Group: 5

● [0] -> Ok Analog Extension on Top Slot

● [1] -> Ok Analog Extension on Bottom Slot

● [2] -> Ok Analog Trunk on Top Slot

● [3] -> Ok Analog Trunk on Bottom Slot

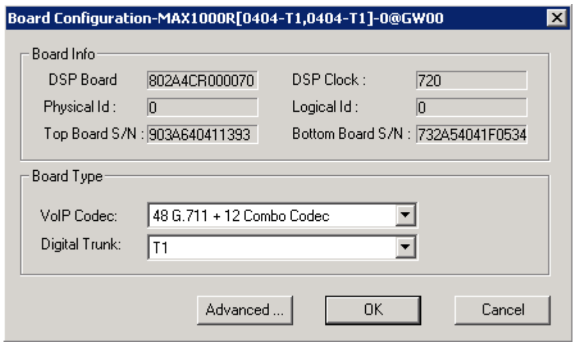
● ! [4] -> Local Alarm T1/E1 on Bottom Slot

Figure 77. Board Configuration window

Double-clicking a channel in the **Channel Mapping List** opens the appropriate dialog box for that channel.

- For details on configuring the T1/E1 trunk, see “Triton T1/E1 Trunk Properties” on page 139.
- For details on the Triton Analog Trunk, see “Triton Analog Trunk GS/LS Properties” on page 142.
- For details on configuring a Triton Analog Line, see “Triton Analog Station Line Properties” on page 173.

In the Board Configuration dialog box for the MAX 1000/2000 board, clicking the **Board Configuration** button opens a panel.



Board Configuration-MAX1000R[0404-T1,0404-T1]-0@GW00

Board Info

DSP Board 802A4CR000070 DSP Clock : 720

Physical Id : 0 Logical Id : 0

Top Board S/N : 903A640411393 Bottom Board S/N : 732A54041F0534

Board Type

VoIP Codec: 48 G.711 + 12 Combo Codec

Digital Trunk: T1

Figure 78. MAX 1000/2000 Board Configuration window

This panel displays the board serial number, top access card serial number, bottom access card serial number, DSP clock, board ID, physical ID, and logical ID. You can choose to configure the board as either T1 or E1, then click **OK**. Additional steps are needed to further configure the CAS or PRI protocol in the Protocol Configuration window, shown in Figure 60 and Figure 61.

Note: Hardware chassis such as Max1000 do not support G.722 codec, the media pass-though feature, or the T.38 feature.

Configuring the Virtual MobileExtSP Board

A simulated physical board – MobileExtSP board – is created in the Softswitch server when you install the MaxCS system. This single MobileExtSP board handles all mobile extensions.

Configuring the virtual MobileExtSP board is discussed on page 218 in the chapter “Mobile Extension Configuration.”

CHAPTER

11

Admin User Configuration

There are several admin user types for MaxAdministrator:

- **Super Admin** — This is the same as the Super Admin user in previous releases; it is primarily used for trouble-shooting with Technical Support. This admin type has full access to menus and fields in MaxAdministrator.

  There is only one Super Admin user in the system.
- **Full Admin** — This is same scope as the Admin user in previous releases; these users can manage all three levels of user. This admin type has full access to menus and fields in MaxAdministrator.
  - You cannot delete the default “Admin” account; this account is used for initial login.
  - You can create multiple Full Admin users, to track individual configuration changes.
  - Full Admin users can assign workgroups and AAs for Supervisor users.
- **Basic Admin** - These users can manage workgroup and extension configurations, in addition to call routing configuration.
  - Basic Admin users cannot configure system or trunk details.
  - You can create multiple Basic Admin users.
  - Basic Admin users can assign workgroups and AAs for Supervisor users.
- **Supervisor** — These users can manage workgroup configurations and MaxAdministrator utilities such as log-in/out, change password.
  - You can create multiple Supervisor users.
  - Beginning in Release 8.6.1, Supervisors cannot delete workgroups.

Because Basic Admin and Supervisor users do not have full privileges to every field within MaxAdministrator, some fields and menus will not be enabled for them; others will not be visible. In other words, these users will have access to only the fields, menus, and workgroups that are appropriate for their user type.

Configuring Admin Accounts

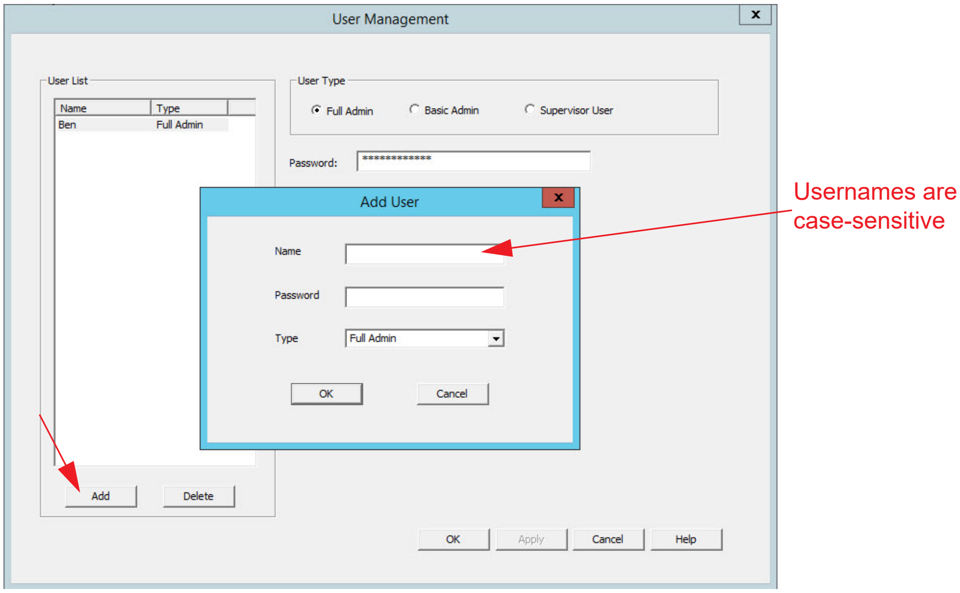
The *User Management* option on the System menu is available to Full Admin and Basic Admin user types. Supervisor user types will not see this menu choice and cannot configure admin user accounts.

To add a new Admin user,

1. On the *System* menu, select **User Management**.
2. Click the **Add** button below the user list on the left.

3. In the *Add User* panel, enter a username and password.

Note: As of MaxCS Release 8.5.0.215, all usernames are case sensitive.



User List

Name	Type
Ben	Full Admin

User Type: ● Full Admin ○ Basic Admin ○ Supervisor User

Password: ************

Add User

Name:

Password:

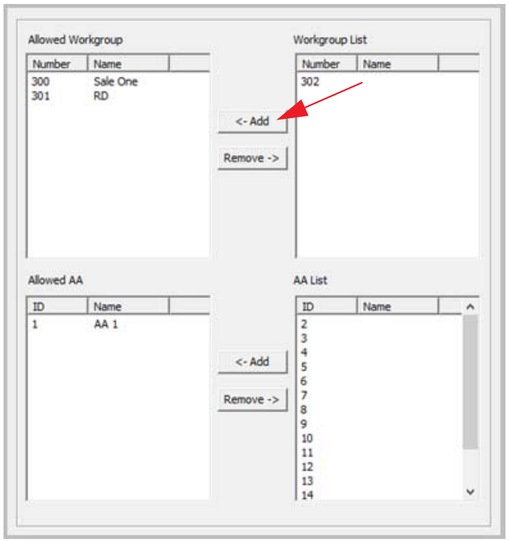
Type: Full Admin

Usernames are case-sensitive

Figure 79. Enter the details for the new Admin user

4. From the pulldown menu, select an admin type for this user.

5. If you selected the *Supervisor* admin type, indicate which workgroups this user can supervise. To do this, select a workgroup in the right panel and click **Add** to add it to the Allowed Workgroup panel on the left. To remove a WG, select it on the left and click **Remove**.



Allowed Workgroup

Number	Name
300	Sale One
301	RD

Workgroup List

Number	Name
302	

Allowed AA

ID	Name
1	AA 1

AA List

ID	Name
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	

Figure 80. Add the workgroups that this admin user can supervise

You can also indicate which AA entries this Supervisor user can manage. To do this, select an AA entry in the right panel and click **Add** to add it to the *Allowed AA* panel on the left. To remove an AA entry, select it on the left and click **Remove**.

6. Click OK.

To remove an Admin user account, select the user in the list and click **Delete**.

Configuration Change Log

Configuration changes are logged with the name of the user who made the change. The configLog.txt file will list the date and time, the name of the admin user who made the change, and a short description of the specific setting the user changed.

The number of configLog backup files has been increased to 20. For security, password changes will be hashed in the log file.

See the section *Change Log* for details.

CHAPTER

12

Unified Communications Configuration

MaxCS is fully integrated with Skype for Business, and synchronizes user presence and activity between MaxCS user extensions and Skype for Business clients.

In order to use Altigen's hosted Skype for Business, you must order your Skype for Business service through the MaxCS Private Cloud portal.

Within MaxAdministrator, there are a few UC settings which you can configure during UC deployment.

On the *System* menu, select **Unified Communications Configuration**.

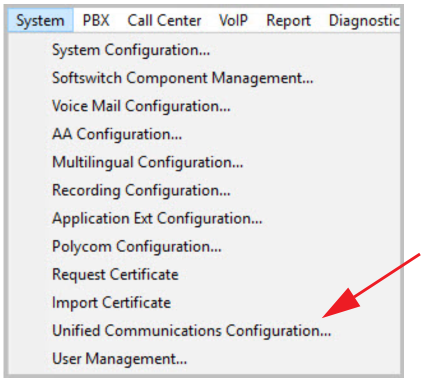
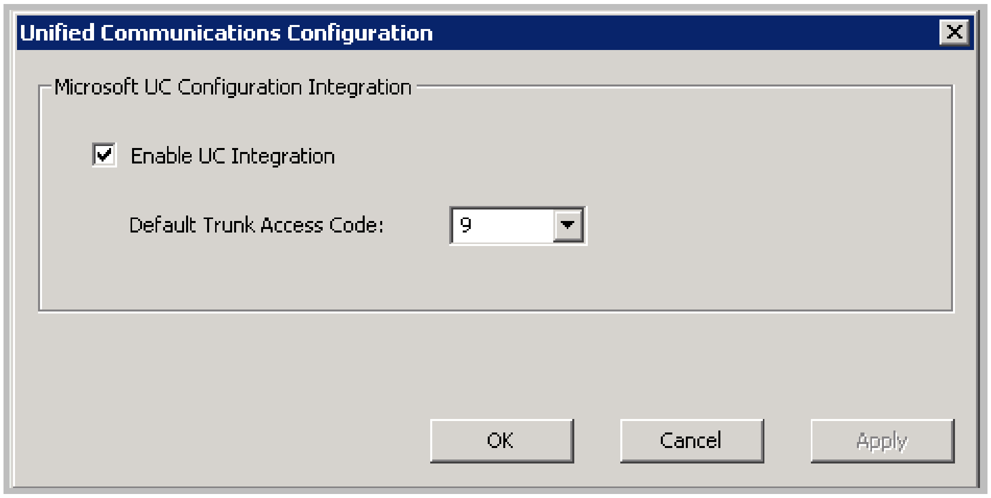

System
PBX
Call Center
VoIP
Report
Diagnostic
System Configuration...
Softswitch Component Management...
Voice Mail Configuration...
AA Configuration...
Multilingual Configuration...
Recording Configuration...
Application Ext Configuration...
Polycom Configuration...
Request Certificate
Import Certificate
Unified Communications Configuration...
User Management...

Figure 81. The Unified Communications Configuration option on the System menu

In this panel, you can enable or disable Unified Communications for your organization, and set the default trunk access code.



Unified Communications Configuration

Microsoft UC Configuration Integration

☑ Enable UC Integration

Default Trunk Access Code: 9

Figure 82. The Unified Communications Configuration panel

For full details on implementing UC for your organization and users, refer to the steps in the *MAXCS 8.6.1 UC Configuration Guide*.

CHAPTER

13

Trunk Configuration

Trunk attributes and parameters are set using the **Trunk Configuration** window. The attributes and options available depend on the type of board and trunk. This chapter discusses general configuration options applicable to all trunks, followed by specific configuration options for the following trunk types:

- SIP tie trunk, page 128
- SIP trunk for ITSP, page 129
- Triton T1/PRI trunk, page 139
- Triton analog trunk, page 142

This chapter also discusses incoming call routing (page 148) and outgoing call blocking (page 150), both configurable on tabs in the **Trunk Configuration** window.

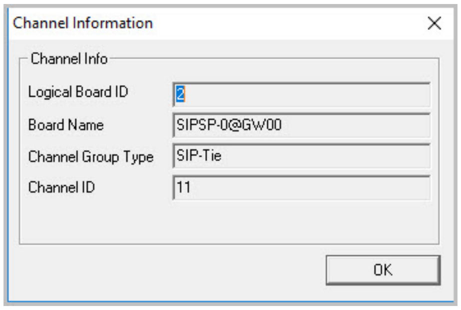
Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

Trunks Out of Service

If none of the trunks are available when an outside call is placed, the caller will hear the system prompt: "All outside lines are busy. Please try again later."

Channel Identification

To find out channel information, right-click a trunk in the Trunk View window (see Figure 83) and select **Channel Physical Location**. The Channel Information panel shows logical board ID, board name, channel group type, and channel ID:



Channel Information

Channel Info

Logical Board ID: 2

Board Name: SIPSP-0@GW00

Channel Group Type: SIP-Tie

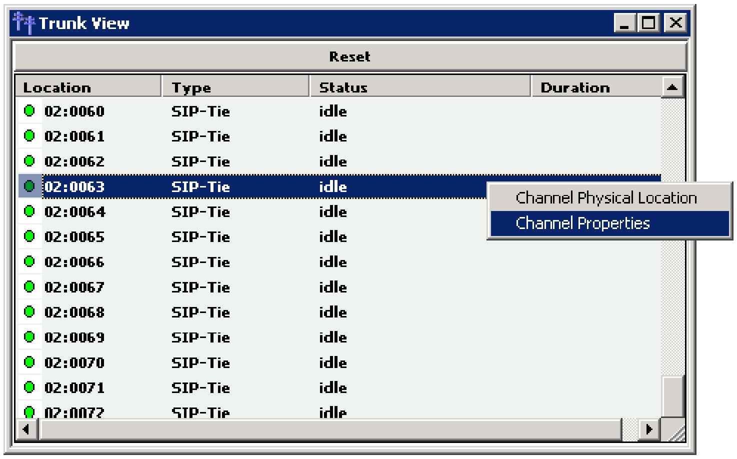
Channel ID: 11

Figure 83. Channel Information box

Opening the Trunk Configuration Window

To open the general **Trunk Configuration** window, do one of the following:

- Click the **Trunk Configuration** button in the toolbar.
- Select **PBX** > **Trunk Configuration**.
- Double-click a trunk in the **Trunk View** window.

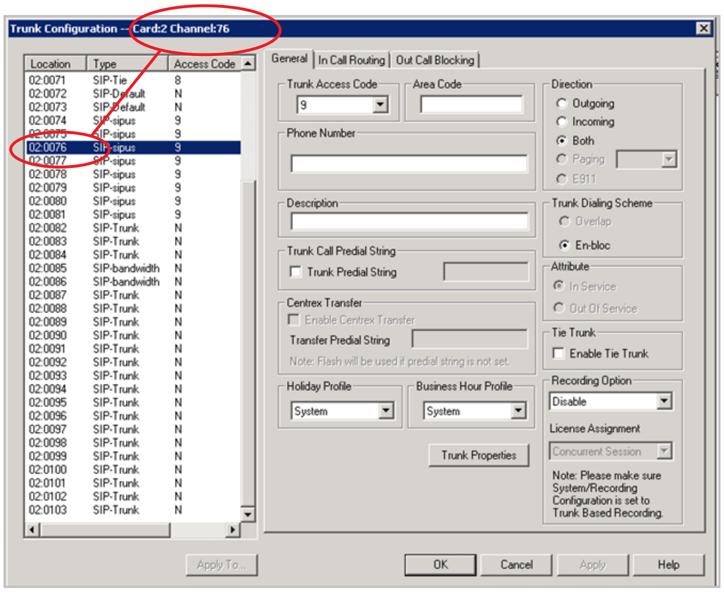


Location	Type	Status	Duration
● 02:0060	SIP-Tie	idle	
● 02:0061	SIP-Tie	idle	
● 02:0062	SIP-Tie	idle	
● 02:0063	SIP-Tie	idle	
● 02:0064	SIP-Tie	idle	
● 02:0065	SIP-Tie	idle	
● 02:0066	SIP-Tie	idle	
● 02:0067	SIP-Tie	idle	
● 02:0068	SIP-Tie	idle	
● 02:0069	SIP-Tie	idle	
● 02:0070	SIP-Tie	idle	
● 02:0071	SIP-Tie	idle	
● 02:0072	SIP-Tie	idle	

Selecting **Channel Properties** from the right-click menu in Trunk View bypasses the general Trunk Configuration window to open a trunk properties window specific to the selected trunk.

Figure 84. Trunk View window

The Trunk Configuration window opens.



Location	Type	Access Code
02:0071	SIP-Tie	8
02:0072	SIP-Default	N
02:0073	SIP-Default	N
02:0074	SIP-sipus	9
02:0075	SIP-sipus	9
02:0076	SIP-sipus	9
02:0077	SIP-sipus	9
02:0078	SIP-sipus	9
02:0079	SIP-sipus	9
02:0080	SIP-sipus	9
02:0081	SIP-sipus	9
02:0082	SIP-Trunk	N
02:0083	SIP-Trunk	N
02:0084	SIP-Trunk	N
02:0085	SIP-bandwidth	N
02:0086	SIP-bandwidth	N
02:0087	SIP-Trunk	N
02:0088	SIP-Trunk	N
02:0089	SIP-Trunk	N
02:0090	SIP-Trunk	N
02:0091	SIP-Trunk	N
02:0092	SIP-Trunk	N
02:0093	SIP-Trunk	N
02:0094	SIP-Trunk	N
02:0095	SIP-Trunk	N
02:0096	SIP-Trunk	N
02:0097	SIP-Trunk	N
02:0098	SIP-Trunk	N
02:0099	SIP-Trunk	N
02:0100	SIP-Trunk	N
02:0101	SIP-Trunk	N
02:0102	SIP-Trunk	N
02:0103	SIP-Trunk	N

Trunk Access Code: 9
Area Code:
Phone Number:
Description:
Trunk Call Predial String: ☐ Trunk Predial String
Centrex Transfer: ☐ Enable Centrex Transfer
Transfer Predial String:
Note: Flash will be used if predial string is not set.
Holiday Profile: System
Business Hour Profile: System

Direction: ○ Outgoing ○ Incoming ● Both ○ Paging ○ E911
Trunk Dialing Scheme: ○ Overlap ● En-bloc
Attribute: ● In Service ○ Out Of Service
Tie Trunk: ☐ Enable Tie Trunk
Recording Option: Disable
License Assignment: Concurrent Session
Note: Please make sure System/Recording Configuration is set to Trunk Based Recording.

Figure 85. Trunk Configuration, General tab

Selecting Trunks to Set Attributes

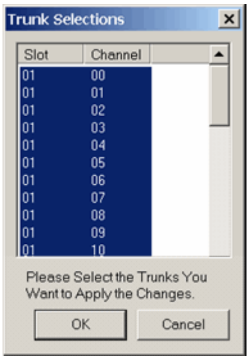
The title bar of the Trunk Configuration window displays the card and the channel of the selected trunk.

The list on the left shows all the configured trunks. The **Location** format is the same as in the Trunk View window, that is, *Logical Board ID : Channel Number*. The logical board ID is assigned by the system. This ID may change when a telephony board is added into or removed from the system.

When you select a trunk in this list, the options and parameters for the trunk appear in the settings in the right side of the window.

Configuring One or Multiple Trunks

To customize trunk characteristics, you work on one trunk at a time. To apply the same configuration to multiple trunks, use the **Apply To** button. This opens a list of all trunks, with all of the trunks selected by default. Select the trunks you want to apply changes to, then click **OK**. (Use **Ctrl**+click and **Shift**+click to select several trunks.) This applies changes to multiple trunks for *only the attribute or option that you changed***.**



Slot	Channel
01	00
01	01
01	02
01	03
01	04
01	05
01	06
01	07
01	08
01	09
01	10

Please Select the Trunks You Want to Apply the Changes.

Figure 86. The Trunk Selection window

Setting General Trunk Attributes

Select a channel to view its current attributes. You can then set or change the following attributes. If an option is grayed out, it is not available for that type of trunk:

- **Access Code** – Assign a trunk access code to the selected trunk. If you need to use a trunk access code other than 9, you must first set this up on the **Number Plan** tab of **System Configuration** (see “Setting a System Number Plan” on page 34).

  Note: There are two types of access code: Trunk Access Code (TAC) and Route Access Code (RAC). TAC is a quick and easy way to select which trunk(s) you would like to dial out from, especially when you want to reserve trunks for a special dialing purpose. For example, you can set up TAC "7" and assign that to trunk(s). These trunks will be reserved exclusively for users who know the TAC "7".

  Although TAC is easy to use, it does have limitations especially when you are located in an area with a complicated dialing pattern or you need to set up VoIP hop-off dialing.

  RAC uses the Out Call Routing table, which has the flexibility to group trunks into a route, assign routes to a specific dialing pattern, and add/delete digits from the dialing pattern. It can solve most of the complicated dialing problems. If your system is using RAC, you can set this TAC field to "None".

- **Area Code** – The local area code for each trunk. Enter a three-digit area code. If left blank, the trunk assumes the home area code defined in the **General** tab of the System Configuration window. *This configuration is for each trunk in the system and will negatively affect features such as Zoomerang if the area code is not configured prop*erly.

- **Direction** – The trunk direction can be **Outgoing** only, **Incoming** only, **Both** Outgoing and Incoming, **Paging**, or **E911**. The **Both** option is the system default.

Note: If a trunk is in the hunt group of your company main number and you configure this trunk as an "Outgoing" trunk, the incoming call will be rejected by the system. To avoid this mistake, make sure you check with your carrier to verify the hunting number before you configure a trunk to **Outgoing**.

Paging – This configuration is for an overhead paging device and requires a Loop Start trunk port. The paging equipment will provide loop current to the trunk port.

When this option is selected, you can assign an ID in the list. The range of paging IDs are from **00** to **99**, which allows MaxCS to be connected to up to 100 paging systems through trunks for multi-zone paging applications.

To activate a trunk paging port, dial **#45** and the ID number. For example, a user dials **#4508** to connect to a paging system through the trunk with paging ID of **08**.

The **Trunk Paging** option and the Overhead Paging option (in “Audio Peripheral Configuration” on page 51) are different and independent of one another. The Overhead Paging option is to set up the Audio Out port on the telephony board and uses **#44** to activate.

The **E911** option is exclusively for an analog Centralized Automatic Message Accounting (CAMA) trunk connecting to a Triton analog trunk board. CAMA trunk is a special type of trunk from your carrier for E911 service. When an analog trunk port is assigned as an E911 CAMA trunk, the system will send the station identification number, defined in the extension configuration E911 CID field, to the PSAP via multi-frequency signaling. The E911 CID is needed to:

- Allow PSAP to identify the caller's information and exact location by matching the Automatic Location Identifier database in PSAP.
- Have the callback number in case the call is disconnected.

Note: Do not select the **E911** option for a T1-CAS or PRI trunk. T1-CAS cannot transmit the ID. PRI trunk will transmit calling party's ID automatically. When the **E911** option is checked, this trunk will no longer receive inbound calls, and only 911 calls will go out through this trunk. Each state may have different E911 regulations and requirements. Please check with the local authority to understand what is required by law.

- **Phone Number** – If this trunk is an analog or T1-CAS trunk, this field is used for labeling purposes only. Enter the number without area code in this field. If this trunk is a PRI trunk, the system will output this number to the carrier as the calling party CallerID.

  PRI trunk transmitting caller ID rules:

  1. If extension has **Transmitted CID** configured, this number will be transmitted first. If not configured, go to next.
  2. If extension has **DID Number** configured, the 10-digit DID number will be transmitted. If not configured, go to next.
  3. If PRI trunk channel has area code and caller ID configured, this number will be transmitted. If not configured, go to next.
  4. PRI will transmit the system home area code and main number defined in System Configuration, **General** tab.

- **Description** – Descriptive information such as the company name for the assigned Phone Number, or appropriate agency if this trunk provides 911 access.
- **Trunk Dialing Scheme** – Overlap or En-bloc dialing.
  - **Overlap** – Transmitting dialed DTMF digits to the CO without buffering digits in the system first. Use Overlap dialing for analog and T1-CAS trunks for best results. Calls will be completed faster.

- **En-bloc** – The system will buffer all dialed digits and send it to the CO at once. Typically is used in ISDN-PRI trunk and SIP trunk.

  Note: For IP Tie trunks, use the IP Dialing Table in Enterprise Manager to set the dialing scheme (Enterprise Manager is available by selecting **VoIP** > **Enterprise Network Management**, or from the Windows **Start** menu).

- **Trunk Call Predial String** – To have the system automatically insert the configured digits whenever the selected trunk is used for outgoing calls. This feature is used to prevent having to dial “9” twice for trunk access when the system is used behind another PBX system or this trunk is a Centrex line, which requires dialing “9” to make a call. If you select this option, type the predial digit(s) into the text box.
- **Enable Centrex Transfer** – When checked, the system is able to transfer an incoming call to another outside number through the same trunk and release the incoming trunk. Before you configure this option for the trunk, please make sure your trunk is a Centrex line or supports the Release Line Transfer (RLT) feature. Depending on the type of trunk, your configuration may be different:
  - If this is an analog Centrex line, you only need to check the **Enable Centrex Transfer** check box. A FLASH signal will be transmitted to the CO if the incoming trunk call needs to be transferred to an outside number.
  - If this is a T1-CAS trunk, you may need to add “transfer predial string.” From the CO point of view, it is their feature code to initiate RLT. Please check with your carrier to get the specification.
  - If this is a PRI trunk, you need to ask your carrier if they support RLT through DTMF. Some carriers accept *8 to signal RLT. Altigen PRI trunks currently do not support 2-B channel transfer feature.

  How to signal MaxCS that it is a Centrex transfer:

  - If a call is connected to an extension, the extension user needs to dial FLASH * plus trunk access code and the outside number.
  - If a virtual extension forwarding or speed dialing number is configured to an outside number and the extension user transfers a call to the virtual extension or speed dialing number, the system will add the Centrex FLASH automatically. You don’t need to add the “*” in the forwarding or speed dialing digit stream.
- **Attribute – In Service** makes the trunk available for use. **Out of Service** prevents the trunk from being used (for example, while performing maintenance).
- **Enable Tie Trunk** – This configuration field is meaningful only if you use T1 or PRI to connect two MaxCS systems back-to-back. Do not check this box if you connect a MaxCS to a third-party PBX via T1 or PRI trunk.

  When this configuration is checked, the system software will interpret the incoming [ANI] [DNIS] digit sequence as [Caller’s Extension Number] and [Target Extension Number]. An incoming tie trunk call will be routed to the target extension and all the Incall Routing rules will be bypassed. If you do not check this box for system-to-system tie trunk, the system will check the extension DID/DNIS Routing/Caller ID Routing table first. If there is no match, then the trunk incall routing rule will apply.

  Note: The **Enable Tie Trunk** field under **Board Configuration** > **Protocol** needs to be enabled for T1/PRI tie trunks as well. It will tell the system to transmit [Caller’s Extension Number] and [Target’s Extension Number] as [ANI] [DNIS] to the other system. In case this is a T1-CAS, which typically cannot transmit any data to the CO, the system will use DTMF as a way to transmit [Caller’s Extension Number] and [Target’s Extension Number] to the other side of the tie trunk. Because the format is Altigen proprietary, you may have a problem if you enable this configuration when connecting to a non-Altigen PBX.

- **Holiday Profile** – A holiday profile can be assigned to a trunk. The list selection is based on settings configured in the **Holiday** tab of System Configuration (see “Routing Calls on Holidays” on page 40).
- **Business Hour Profile** – A business hour profile can be assigned to a trunk. The list selection is based on settings configured in the **Business Hours** tab of System Configuration.

- **Recording Option** – Recording for incoming and outgoing calls is supported for Triton Analog, T1/E1, and IP trunks; use the list to select **Disable** or **Enable**. If you select **Enable**, choose the license you want to assign (**Concurrent Session** or **Dedicated Seat**), and make sure that in **System > Recording Configuration** one of the trunk-based recording options is selected.

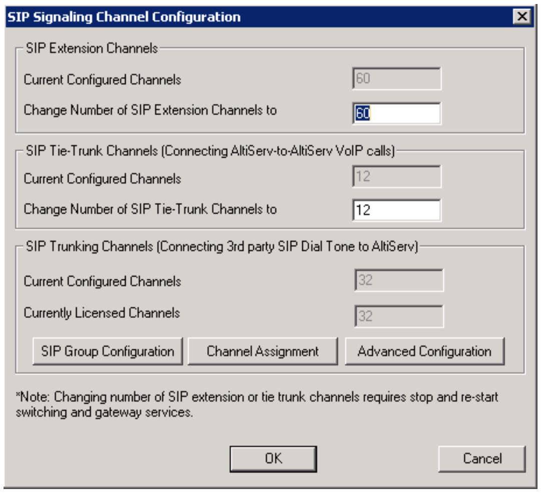
  Note: When you use trunk-based recording, inbound or outbound calls are recorded as long as the trunk is in use. For example, an inbound call that is answered by an AA, routed to an operator, and transferred to an extension will begin recording when the AA answers the call and end recording when the trunk is released.

  With extension recording, recording starts only when the extension user answers the call.
- **Trunk Properties** – Opens a dialog box that allows you to configure low-level, hardware-specific properties for each trunk. The options vary depending on the type of board and trunk; this is discussed in subsequent sections.

SIP Tie Trunk Properties

To open a configuration dialog box for a SIP tie-trunk channel, do one of the following:

- If you're in the **Trunk Configuration** window, select a Triton VoIP channel from the trunk channels list, then click the **Trunk Properties** button, or just double-click the channel in the list.
- If you're in the **Trunk View** window, right-click the channel and select **Channel Properties**.


SIP Signaling Channel Configuration

SIP Extension Channels

Current Configured Channels: 60

Change Number of SIP Extension Channels to: 60

SIP Tie-Trunk Channels (Connecting AltiServ-to-AltiServ VoIP calls)

Current Configured Channels: 12

Change Number of SIP Tie-Trunk Channels to: 12

SIP Trunking Channels (Connecting 3rd party SIP Dial Tone to AltiServ)

Current Configured Channels: 32

Currently Licensed Channels: 32

*Note: Changing number of SIP extension or tie trunk channels requires stop and re-start switching and gateway services.

Figure 87. Configuration dialog box for a Triton VoIP channel

See "Configuring the SIPSP Board" on page 105 for board configuration information.

Note: This is signal only trunks. Make sure you have enough IP resource boards to cover your needs.

Cisco Gateways

Be aware of the following when configuring MaxCS to work with Cisco gateways.

For MaxCS to communicate with a Cisco Gateway with TLS, you should set the SIP Tie Trunk's *SIP Destination Port* to **0**. (This is a field in the SIP Group configuration panel., on the Register tab.) This means that MaxCS will reuse the existing TLS connection established from the Cisco Gateway.

You will need to turn on the SIP Option or TCP keep alive option on the Cisco gateway to maintain the TLS connection.

SIP Trunk Properties

Traditionally, telecom trunks are from your local carrier's PSTN switch and the dial tone is provided via either analog trunks or T1/PRI digital trunks. A new type of service called "IP Dial Tone," which allows you to dial a long distance call at a lower rate, is available. IP Dial Tone is delivered through your IP data network, and the service provider can be anywhere in the world, as long as the VoIP data packets can be routed properly.

If you have SIP-based IP dial tone service from an Internet Telephony Service Provider (ITSP), you need to configure SIP trunk channels to connect to the service. Before you start, note the following:

- An Altigen SIP Trunking channel is licensed. You need to buy and register a license to be able to configure this option. Note that Altigen SIP Trunks do not require a SIP Trunk license.
- Beginning in release 8.0, the number of SIP trunk channels allocated is now based on the configuration. In earlier releases, this was based upon the number of SIP trunk licenses.
- Altigen does not guarantee the voice quality of the SIP dial tone coming from your service provider. You need to work with your data service and SIP trunking service provider to make sure adequate QoS is provisioned for your WAN service.
- Altigen does not guarantee SIP trunk implementation will work with all SIP dial tone service providers. Altigen dealers are notified of Altigen-tested and certified SIP-Trunk service providers. Configuration guidelines for each Altigen-certified SIP-Trunk service provider can be found in the Altigen authorized Partner Knowledge Base, available from the Altigen Partner Web Site. SIP dial tone service providers need to support the following:
    - G.711, G.723.1, G.729 codec
    - RFC 2833 for DTMF tone delivery
    - SIP MD5 authentication with SIP registration
    - If MaxCS is behind NAT, verify that your SIP SP can support this configuration.

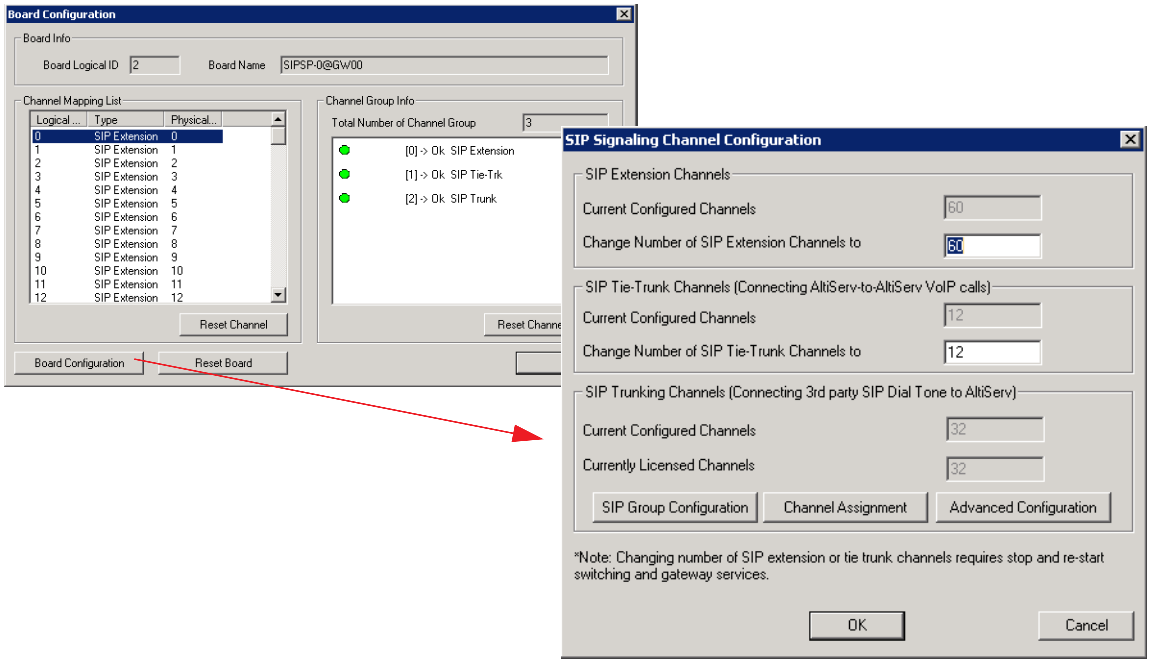
When subscribing to a SIP dial tone service, typically your service provider will provide you with the information required in the configuration dialog box shown in (see Figure 88 on page 130). Enter these service parameters to each SIP trunk channel configuration individually.

Note: This is signal only trunks. Make sure you have enough IP resource boards to cover your needs.

Important: You must add the SIP Trunk service provider's IP address to the IP Device Range in Enterprise Manager and select the proper codec profile for this service. See "Assigning Codec Profiles to IP Addresses" on page 321. Failure to do this step may cause no voice path, even if the SIP Trunk channel shows the call is connected.

SIP Groups

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



Board Info

Board Logical ID: 2

Board Name: SIPSP-0@GW00

Channel Mapping List

Logical ...	Type	Physical...
0	SIP Extension	0
1	SIP Extension	1
2	SIP Extension	2
3	SIP Extension	3
4	SIP Extension	4
5	SIP Extension	5
6	SIP Extension	6
7	SIP Extension	7
8	SIP Extension	8
9	SIP Extension	9
10	SIP Extension	10
11	SIP Extension	11
12	SIP Extension	12

Channel Group Info

Total Number of Channel Group: 3

- [0] -> Ok SIP Extension
- [1] -> Ok SIP Tie-Trk
- [2] -> Ok SIP Trunk

SIP Extension Channels

Current Configured Channels: 60

Change Number of SIP Extension Channels to: 60

SIP Tie-Trunk Channels (Connecting AltiServ-to-AltiServ VoIP calls)

Current Configured Channels: 12

Change Number of SIP Tie-Trunk Channels to: 12

SIP Trunking Channels (Connecting 3rd party SIP Dial Tone to AltiServ)

Current Configured Channels: 32

Currently Licensed Channels: 32

*Note: Changing number of SIP extension or tie trunk channels requires stop and re-start switching and gateway services.

Figure 88. SIP Trunk Configuration dialog box and Edit box

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.

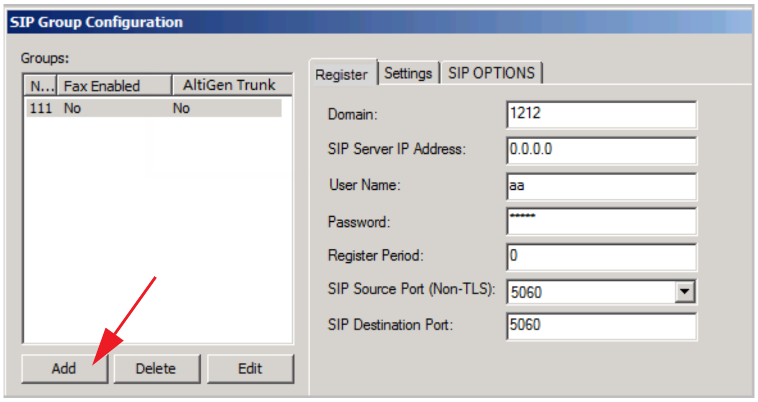
In the SIP Signaling Channel Configuration panel, you can do the following:

- 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

SIP Group Configuration

To create a new SIP Group,

1. Double-click a **SIPSP** board in *Boards* view and then click **Board Configuration** > **SIP Group Configuration**.



N...	Fax Enabled	AltiGen Trunk
111	No	No

Domain: 1212

SIP Server IP Address: 0.0.0.0

User Name: aa

Password: *****

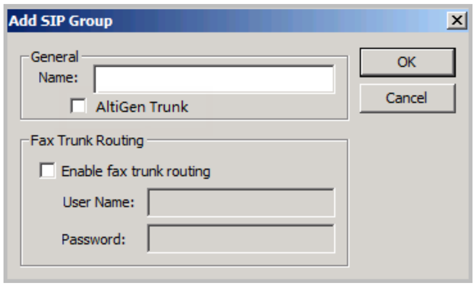
Register Period: 0

SIP Source Port (Non-TLS): 5060

SIP Destination Port: 5060

Figure 89. The SIP Group Configuration window

2. Below the *Groups* list, click **Add**.



Name:

□ AltiGen Trunk

□ Enable fax trunk routing

User Name:

Password:

Figure 90. SIP Group parameters

3. Enter a name for the group and indicate whether this is an Altigen SIP Trunk.

   Note: MaxCS includes license checking for Altigen SIP trunks. The SIP Server address and registration UID will be validated. Be aware that trunks will show as *not registered* if you start MaxAdministrator 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 are ready.

4. (Optional) If this group will handle fax calls, select the option **Enable fax trunk routing** and enter the appropriate user name and password. This feature is supported on Altigen SIP trunks only.

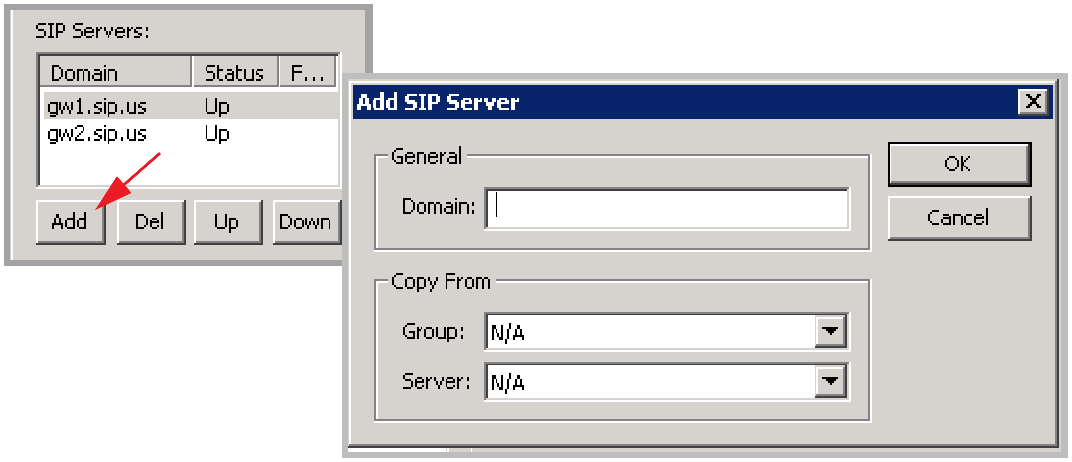
   If the extension is a fax extension and **Enable fax Trunk routing** is checked, that means the SIPSP should use the Fax Username and Fax password of the SIP Trunk instead of regular username and password of SIP Trunk to negotiate with the SIP Trunk.

   If the extension is a fax extension but **Enable fax trunk routing** is unchecked, that means the SIPSP should use the regular username and password of the SIP Trunk to negotiate with the SIP Trunk side.

Adding 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**.



SIP Servers:

Domain	Status	F...
gw1.sip.us	Up	
gw2.sip.us	Up	

Add SIP Server

General

Domain:

Copy From

Group: N/A

Server: N/A

Figure 91. Add a SIP Server to a 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.

Note: In the SIP Group Configuration panel, click **Refresh** when you want to update the view

Removing Servers from a SIP Group

To remove a server from a SIP group,

1. Double-click an 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).

Changing the Order of Servers in a SIP Group

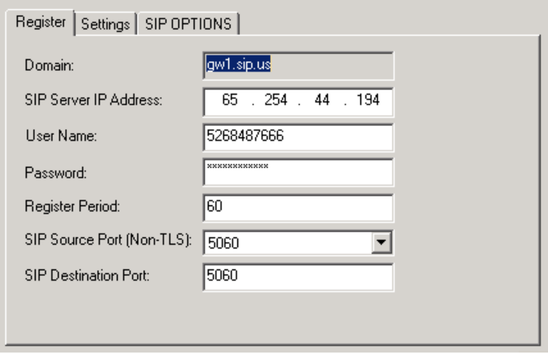
The order of the servers in the *Servers* list determines how to severs are accessed. The first server is always used; when that server is not available, the second server in the list is use, and so on.

To change the order of SIP servers within 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. In the Servers list, select the server that you want to move.
4. Click **Up** or **Down** as appropriate.

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.



Domain: gw1.sip.us
SIP Server IP Address: 65 . 254 . 44 . 194
User Name: 5268487666
Password: ************
Register Period: 60
SIP Source Port (Non-TLS): 5060
SIP Destination Port: 5060

Figure 92. The SIP Server Register tab

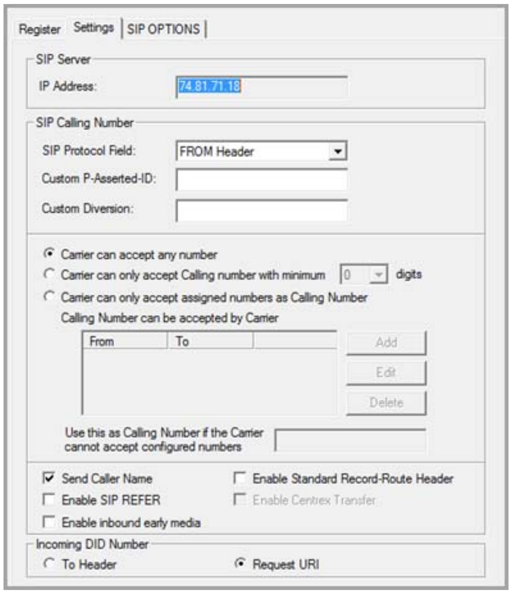
The lone exception is the earlier *Enable Channel* option, which beginning with Release 8.0 is found in the *Channel Assignment* panel.

SIP Register Parameter	Description
Domain	The Domain Name of the SIP Trunk service provider, if required. If there is no domain, you may make the domain the same as the SIP Server IP address.
SIP Server IP Address	The SIP Trunk service provider’s server IP address.
User Name	This is assigned by the SIP Trunk service provider.
Password	This is assigned by the SIP Trunk service provider.
Register Period	How frequently the Altigen system needs to send SIP registration packets to the service provider. This can detect if the service provider is up or not. Some service providers do not accept SIP Register messages. In these cases, you can disable sending SIP Register messages from MaxCS by setting the SIP Register Period to **0**.
SIP Source Port (Non-TLS)	For SIP UDP, select the source port from 5060 or 10060. For TCP or TLS, you cannot change ports. Using a port other than 5060 will prevent SIP-ALG firewall/router from changing the SIP packets.
SIP Destination Port	A SIP Trunk can have different source port and destination port.

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.

SIP Server General Parameters

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



SIP Server

IP Address: 74.81.71.18

SIP Calling Number

SIP Protocol Field: FROM Header

Custom P-Asserted-ID:

Custom Diversion:

● Carrier can accept any number

○ Carrier can only accept Calling number with minimum 0 digits

○ Carrier can only accept assigned numbers as Calling Number

Calling Number can be accepted by Carrier

From	To	

Use this as Calling Number if the Carrier cannot accept configured numbers

☑ Send Caller Name

☐ Enable Standard Record-Route Header

☐ Enable SIP REFER

☐ Enable Centrex Transfer

☐ Enable inbound early media

Incoming DID Number

○ To Header

● Request URI

Figure 93. The SIP Server Settings tab

SIP Server General Parameter	Description
IP Address	
SIP Protocol Field	**Not Sent** (default) – Do not send transmitted caller ID **FROM Header** – Send the caller ID using the SIP FROM header **P-Preferred Identity** – Send the caller ID using the SIP P-Preferred Identity header **P-Asserted Identity** – Send the caller ID using the SIP P-Asserted Identity header
Custom P-Asserted-ID	This field 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. This field 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.
Custom Diversion	This field 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. 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*
Carrier can accept any number	This is the default.

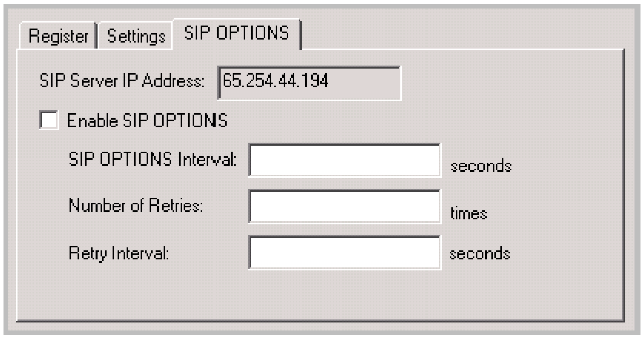
SIP Server General Parameter	Description
Carrier can only accept Calling Number with minimum x digits	Enter the number of digits, then enter a calling number in the field below the table in case the carrier cannot accept configured numbers.
Carrier can only accept assigned numbers as Calling Number	If you select the this option, specify “assigned numbers” by clicking the **Add** button and entering the numbers. To edit or delete a number you added, select it and click the **Edit** or **Del** button. Enter a calling number in the field below the table in case the carrier cannot accept configured numbers.
Send Caller Name	Check to also send the caller name to callees.
Enable Standard Record-Route Header	Check this box if the SIP service provider uses SIP Record-Route and the SIP trunk cannot make or receive calls. If it already works, DO NOT CHECK or UNCHECK this box. [Service provider Bandwidth.com with Edgewater Route require this checked]
Enable SIP REFER	This option, in conjunction with the **Enable Centrex Transfer** option, 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 extension-specific setting for the Release SIP Tie-Link Trunk feature is discussed in the section *Setting Personal Information*. This option is provided to support various gateway devices. For instructions on configuration AudioCodes gateways and other-third party devices, refer to the configuration guides stored in the Altigen Knowledgebase.
Enable inbound early media	Some carriers require SDP to be included with the Ringing message. To accommodate those carriers, check the *Enable inbound early media* option to avoid audio issues with incoming calls. This option will send a single Ringing message with SDP.
Enable Centrex Transfer	This option, in conjunction with the **Enable SIP Refer** option, 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 extension-specific setting for the Release SIP Tie-Link Trunk feature is discussed in the section *Setting Personal Information*. This option is provided to support various gateway devices. For instructions on configuration AudioCodes gateways and other-third party devices, refer to the configuration guides stored in the Altigen Knowledgebase.
Incoming DID Number Field	When a call comes in, the SIP trunk uses **To Header** or **Request URI** as the DID/DNIS number
Enable Local From Header	Enabling this option will change the IP address in the FROM header to the local IP address (NAT address if applicable) of the MaxCS server.

SIP Server SIP Options Parameters

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

You can configure trunk groups so that SIP devices can exchange their status. By sending a “keepalive” message and checking for a valid response, SIP devices will know whether remote peers are ready to receive a new request.

Once the MaxCS server has been set up, SIP trunks will try to register to the SIP servers first. If the registration is successful and if the SIP Options feature is enabled, the system will send the “keepalive” message to SIP providers according the interval setting. Only one “keepalive” message will be sent for each group of trunks.



Register | Settings | SIP OPTIONS

SIP Server IP Address: 65.254.44.194

☐ Enable SIP OPTIONS

SIP OPTIONS Interval: seconds

Number of Retries: times

Retry Interval: seconds

Figure 94. The SIP OPTIONS tab

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. You can see the status of severs on the *SIP Group Configuration* panel.

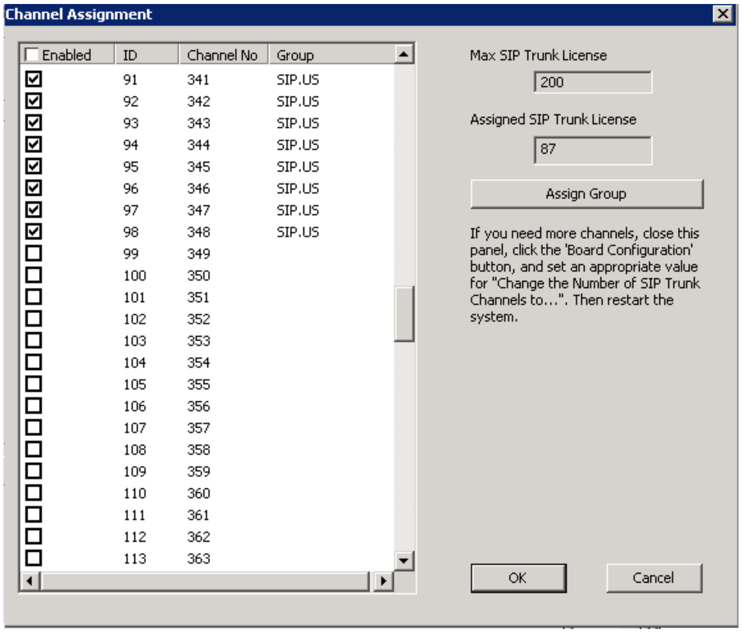
SIP Options can be enabled or disabled for each SIP Server. By default, the SIP Options parameter is disabled.

SIP OPTIONS Parameter	Description
Enable SIP OPTIONS	Enable or disable this feature for the selected SIP Server.
SIP OPTIONS Interval	How often, in seconds, the server sends a "keepalive" message to this enabled SIP trunk group. The default interval is 30 seconds.
Number of Retries	If MaxCS receives no 200 (OK) response, the number of times a "keepalive' message should be sent. After these retries, if there still has been no valid response, then the system marks all SIP trunks in the group as Not Ready. The default number of attempts is 5.
Retry Interval	While a SIP trunk group is in a Retry state and is not receiving a valid response, how often MaxCS should send another "keepalive" message to the SIP server. The default interval is 2 seconds. If the system does not receive a SIP 200 (OK) message after the set number of retries, it then sets all SIP trunks in that group to Not Ready.

View List of 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**. The panel shows a list of the channels, indicating their status and SIP Group.



Channel Assignment

□ Enabled	ID	Channel No	Group
☑	91	341	SIP.US
☑	92	342	SIP.US
☑	93	343	SIP.US
☑	94	344	SIP.US
☑	95	345	SIP.US
☑	96	346	SIP.US
☑	97	347	SIP.US
☑	98	348	SIP.US
□	99	349	
□	100	350	
□	101	351	
□	102	352	
□	103	353	
□	104	354	
□	105	355	
□	106	356	
□	107	357	
□	108	358	
□	109	359	
□	110	360	
□	111	361	
□	112	362	
□	113	363	

Max SIP Trunk License: 200

Assigned SIP Trunk License: 87

If you need more channels, close this panel, click the 'Board Configuration' button, and set an appropriate value for "Change the Number of SIP Trunk Channels to...". Then restart the system.

Figure 95. The Channel Assignment panel

A checkbox indicates whether a channel is enabled.

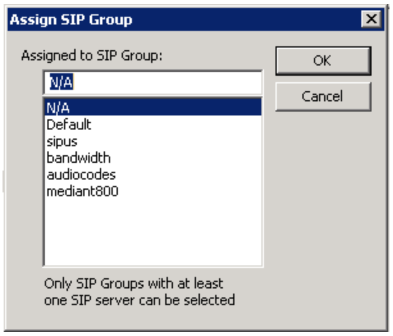
To disable or enable a channel, check or clear its checkbox. To enable or disable all channels, check or clear the checkbox in the column heading at the top of the list.

If you discover that you need to add more channels, close this panel, click **Board Configuration**, and set an appropriate value for the *Change Number of SIP Trunk Channels to…* option (see Figure 88, “SIP Trunk Configuration dialog box and Edit box"). 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**.



Assign SIP Group

Assigned to SIP Group: N/A

- N/A
- Default
- sipus
- bandwidth
- audiocodes
- mediant800

Only SIP Groups with at least one SIP server can be selected

Figure 96. Assign channels to a SIP Group

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.'

SIP Trunk TLS Support

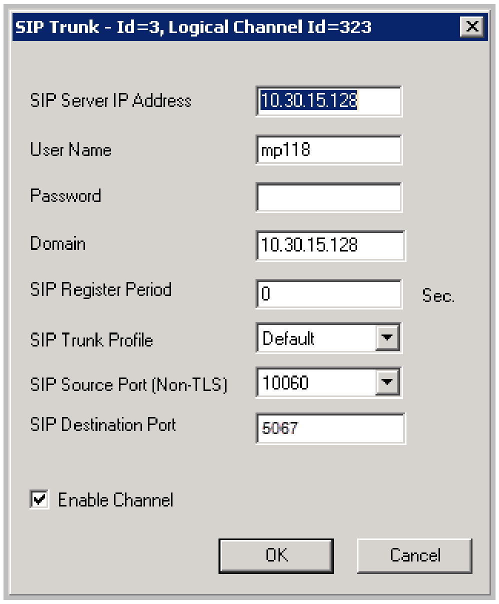
MaxCS supports TLS/SRTP on SIP Trunks.

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.

The following devices are supported for TLS:

- AudioCodes MP-11x
- AudioCodes Mediant 1000-B PRI / T1

When configuring SIP Trunks, you no longer see the option *Automatic NAT Traversal* as you did in previous releases. As of Release 8.0, SIP Trunks no longer have this parameter. The pre-8.0 option *SIP Source Port* has been changed to SIP *Source Port (Non-TLS)*.



SIP Trunk - Id=3, Logical Channel Id=323

SIP Server IP Address	10.30.15.128
User Name	mp118
Password	
Domain	10.30.15.128
SIP Register Period	0 Sec.
SIP Trunk Profile	Default
SIP Source Port (Non-TLS)	10060
SIP Destination Port	5067

☑ Enable Channel

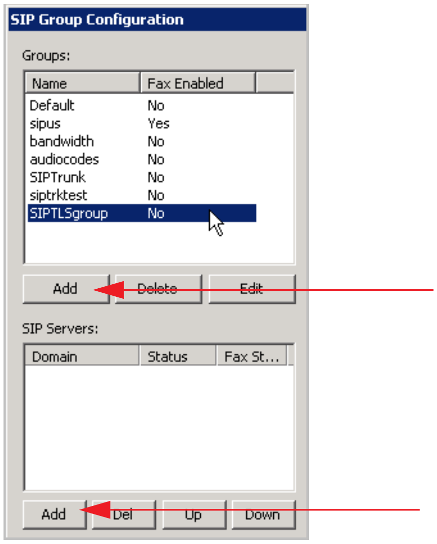
Figure 97. The SIP Destination Port field set to 5067 for Altigen SIP Trunks

Note: Effective in the 8.0 Release, Enterprise Manager has a new option, TLS/SRTP codec setting.

Following is an example of a generic setup for SIP TLS; configuration may differ from one SIP trunk to another. Refer to the configuration guide for your SIP Trunk for specific details; these guides can be found in the Altigen Knowledgebase.

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.



Name	Fax Enabled
Default	No
sipus	Yes
bandwidth	No
audiocodes	No
SIPTrunk	No
siptrktest	No
SIPTLSgroup	No

Click here to add a new SIP Group for TLS.

Then click here to add a server to that new SIP group.

Figure 98. Add a new SIP Group for TLS; add a server to that new 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.

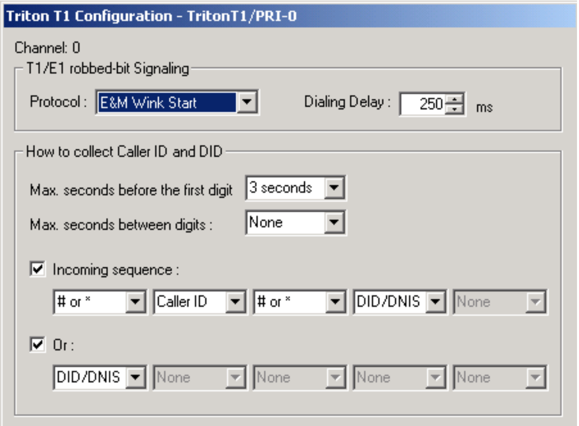
6. Save the changes.

Note: SIP OPTION over TLS is not supported.

Triton T1/E1 Trunk Properties

To open a configuration dialog box for a Triton T1/E1 channel, do one of the following:

- If you’re in the **Trunk Configuration** window, select a Triton T1/E1 channel from the trunk channels list, then click the **Trunk Properties** button, or just double-click the channel in the list.
- If you’re in the **Trunk View** window, right-click the channel and select **Channel Properties**.



Triton T1 Configuration - TritonT1/PRI-0

Channel: 0

T1/E1 robbed-bit Signaling

Protocol : E&M Wink Start

Dialing Delay : 250 ms

How to collect Caller ID and DID

Max. seconds before the first digit: 3 seconds

Max. seconds between digits : None

☑ Incoming sequence :

or * | Caller ID | # or * | DID/DNIS | None

☑ Or :

DID/DNIS | None | None | None | None

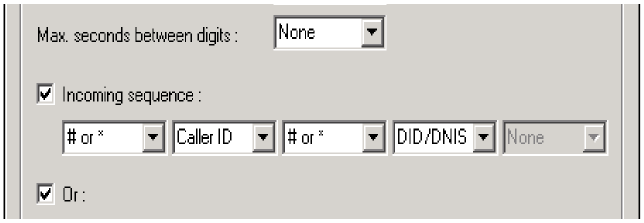
Figure 99. Triton T1 Configuration dialog box

Following are the parameters for the Triton T1 Configuration dialog box.

Parameter	Description
T1 robbed-bit signaling	
Protocol	You can set Protocol to one of the following: • E&M Wink Start (default) • E&M Immediate Start • Ground Start • Loop Start For signaling from one board to another, only **E&M Wink Start** is supported. Loop Start, Ground Start, and E&M Immediate Start protocols cannot be used for interfacing between two boards.
Dialing Delay	Specifies the delay, in milliseconds, after trunk seizure and before digit dialing. This configuration will slow down the system transmitting digits to the CO by a defined delay to avoid missing digits. Do *not* change this value unless advised.
Caller ID and DID Collection	
You can select the maximum time-out delays, in seconds, and the appropriate sequence of symbols to be collected for Caller ID and DID.	
Max. seconds before the first digit	Maximum wait time before time-out for the system to identify this digit after either the first *ring* in ground start or loop start or the *wink* in wink start. The range is from 1-6 seconds, or **None**, with a default value of 3 seconds. Do *not* change this value unless advised. **None** means *no* Caller ID or DID information will be collected. All other options will be grayed out. Use this option to disable Caller ID and DID collection.
Max. seconds between digits	Maximum wait time before time-out between two digits. Default value is **None**. Do *not* change this value unless advised. Selecting **None** means the system will only wait for the sequence of digits that are collected within the length of time specified in the Max. seconds before the first digit field.

Parameter	Description
Incoming sequence	Select up to five incoming symbols to collect from the Caller ID or DID digits: • None • # • * • # or * • Caller ID • DID/DNIS Selecting **None** in any field of the sequence will terminate the sequence and automatically disable subsequent entries in the sequence. The default sequence is: “# or *” (and then) “Caller ID” (and then) “# or *” (and then) “DID/DNIS”
Or	Sets up an additional, alternative sequence. You can select another set of up to five incoming symbols to collect. Not checking any box is equivalent to checking **None** in the first field. The default sequence is: “DID/DNIS”
Apply to	If appropriate, you can use this button, as described in “Configuring One or Multiple Trunks” on page 125, to apply the Caller ID Collection to multiple T1 trunks.

Note: In order for back-to-back T1 and tie trunk T1 configurations to perform properly, it is recommended that you use the system’s default incoming call sequences:



Max. seconds between digits : None

☑ Incoming sequence :

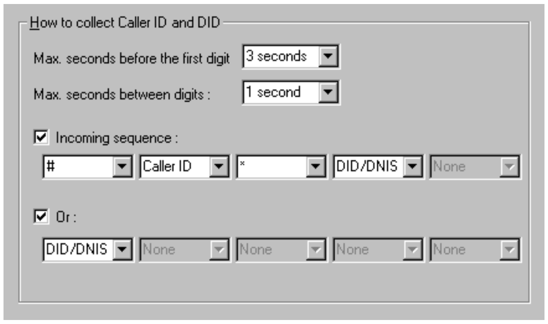
or * | Caller ID | # or * | DID/DNIS | None

☑ Or :

Figure 100. Incoming call sequence parameters

Caller ID and DID Incoming Sequence Example

The following is an example of a Caller ID and DID/DNIS incoming sequence window.



How to collect Caller ID and DID

Max. seconds before the first digit 3 seconds

Max. seconds between digits : 1 second

☑ Incoming sequence :

| Caller ID | * | DID/DNIS | None

☑ Or :

DID/DNIS | None | None | None | None

Figure 101. Sample Incoming Sequence window

When a call comes in, the system tries to match the incoming sequence to either the first or second Incoming Sequence Digit String sequence. If no match is found, no Caller ID or DID digits will be collected.

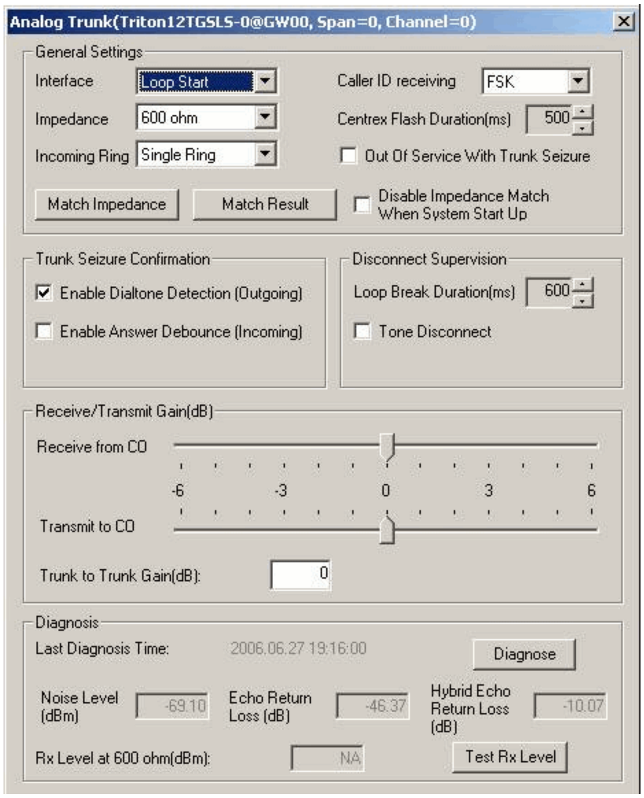
- The system waits 3 seconds for the first digit to arrive. If the symbol is a #, it continues with the first sequence. Otherwise, it looks for a match to the first (and only) symbol in the second sequence, the DID/ DNIS number.
- For the example, let’s say the system receives the #. It then waits 1 second between each digit for the next digit until all digits are received. The * symbol is a delimiter between Caller ID and DID digits.

In this example, the MaxCS ACC/ACM system is expecting either the sequence #CID*DID or only DID digits for incoming calls. If no match is found for either sequence, no Caller ID or DID digits are collected.

Triton Analog Trunk GS/LS Properties

To open a configuration dialog box for a Triton Analog Trunk GS/LS channel, do one of the following:

- If you’re in the **Trunk Configuration** window, select a Triton Analog Trunk GS/LS channel from the trunk channels list, then click the **Trunk Properties** button, or just double-click the channel in the list.
- If you’re in the **Trunk View** window, right-click the channel and select **Channel Properties**.



Analog Trunk(Triton12TGSLS-0@GW00, Span=0, Channel=0)

General Settings

Interface: Loop Start

Impedance: 600 ohm

Incoming Ring: Single Ring

Caller ID receiving: FSK

Centrex Flash Duration(ms): 500

□ Out Of Service With Trunk Seizure

□ Disable Impedance Match When System Start Up

Trunk Seizure Confirmation

☑ Enable Dialtone Detection (Outgoing)

□ Enable Answer Debounce (Incoming)

Disconnect Supervision

Loop Break Duration(ms): 600

□ Tone Disconnect

Receive/Transmit Gain(dB)

Trunk to Trunk Gain(dB): 0

Diagnosis

Last Diagnosis Time: 2006.06.27 19:16:00

Noise Level (dBm): -69.10

Echo Return Loss (dB): -46.37

Hybrid Echo Return Loss (dB): -10.07

Rx Level at 600 ohm(dBm): NA

Figure 102. Triton Analog Trunk GS/LS Properties window

Note that you can use **Apply to** in this dialog box to apply changes to other trunks of the same type.

Triton Parameter	Description
Interface Type	Select the type of trunk that will interface with this trunk channel: • Loop Start Trunk • Ground Start Trunk
Incoming Ring	Single – Default setting for North America Double – For countries using Ring-Ring-Silent type of ring pattern
Impedance	The resistance of electrical current to alternating current, measured in Ohms. Impedance occurs when power or signal is transferred from one circuit to another. When a trunk interface impedance is greatly mismatched with the CO analog line, it may result in static noise and echo heard by IP phone users. The system automatically selects the impedance profile that best matches the Triton trunk interface with the CO. In the rare case where you are not getting the best match, you can disable this feature by checking **Disable Impedance Match During System Startup**, and you can set the **Impedance** manually.
Match Impedance button	Changes the **Impedance** setting to the best match for the selected trunk channel, and then measures noise and returned echo with this impedance setting. Results are displayed in the Diagnosis section of the dialog box. The system automatically runs a matching test upon system startup, unless you disable the feature. If later you connect a new analog line to an empty port or replace an existing line, you need to click this button to best match the impedance.
Match Result button	Shows the result obtained the last time the **Match Impedance** button was clicked for that trunk.
Disable Impedance Match During System Startup	Check to disable automatic impedance matching during system startup.
Caller ID Receiving	Select as **None**, **FSK** or **DTMF** for receiving caller ID digits. For North America, the caller ID is FSK signal on analog trunk.
Centrex Flash Duration (ms)	Specifies the Flash Duration time in milliseconds, with a range from 150 ms to 1000 ms.
Out of Service With Trunk Seizure	When checked, if the trunk is set to *Out of Service*, the system will busy out the trunk. The CO will treat this trunk as a busy line and WILL NOT place a call to this trunk. (By default, this option is unchecked.)
Enable Dial Tone Detection (Outgoing)	When enabled, the trunk channel must detect outgoing dial tone prior to making the call.
Enable Answer Debounce (Incoming)	Enables a timeout period of 2 seconds (for ignoring false CO disconnect signal), after answering an incoming call.
Loop Break Duration (ms)	Disconnects signal if CO breaks loop current. You can set the duration from 200 to 1000 ms. 600 ms is common in North America.
Tone Disconnect	Busy tone (reorder tone, fast busy tone, error tone, and so on) or dial tone (continuous tone, and so on). This should be used in conjunction with drop in loop current. For COs who cannot guarantee loop break, this may be the only option.
Receiver/Transmission Gain	Slide setting adjusts the gain from -6 dB to 6 dB for every Triton Analog Trunk channel. The gain is not adjustable, by default. The user needs to run the diagnosis first to change the gain. The diagnosis process determines the max gain based on the diagnosis results. The default setting is **0 dB**, and it is highly recommended that you not change this setting. **Caution!** Setting the volume too high will cause distortion in voice quality and/or missed DTMF digits.

Triton Parameter	Description
Trunk to Trunk Gain	This configuration is to set Gain for calls that involve two analog trunks (one in and one out). Because an analog trunk typically has energy loss of 3-12 dB, a two-trunk operation, like VM out call and MobileExt, may have low volume issues because energy loss is doubled. This configuration can compensate for the energy loss. The valid range is 0 to 6 dB. Recommended value is 3 dB. **Caution**: Setting the Gain too high may cause distortion in voice quality and DTMF tone. Your CO may not be able to recognize the dialing number if DTMF tones are distorted.
Last Diagnosis Time	The last time the **Diagnosis** button was clicked.
Diagnose button	Use this button to view the Noise Level, Echo Return Loss, and Hybrid Echo Return Loss, measured using the current **Impedance** setting.
Noise Level	The noise level (displayed after you click the **Diagnose** button or the **Match Impedance** button). Acceptable range for Noise Level is less than -67 dBm in value. For example, Noise Level of -72 dBm is good and -63 dBm is poor. You may experience high background noise and low voice volume if Noise Level is poor.
Echo Return Loss	The measurement for echo return loss (displayed after you click the **Diagnose** button or the **Match Impedance** button). Acceptable range for Echo Return Loss is less than -12 dB. For example, Echo Return Loss of -19 dB is good and -8dB is poor. The IP phone users may hear their voice coming back (echo) if Echo Return Loss is poor.
Hybrid Echo Return Loss	The measurement for hybrid echo return loss (displayed after you click the **Diagnose** button or the **Match Impedance** button). Acceptable range for Hybrid Echo Return Loss is less than -6 dB.
Rx Level at 600 Ohms	The Rx Level measurement at 600 Ohms, obtained by clicking the **Test Rx Level** button. See **Test Rx Level** button, below.
Test Rx Level button	Tests the receiving level of the trunk channel on a call to your local CO's Milli-Watt Test Number after you set the **Impedance** parameter to 600 Ohms and the **Rx Gain** to 0dB. Results are displayed in the **Rx Level at 600 Ohms** field.

Performing Impedance Match on Your Own

For each individual analog trunk that is connected to the CO when the system starts up, MaxCS automatically selects an impedance profile to best match the Triton trunk interface with the CO. In the unlikely event that this automatic selection does not yield the optimal voice quality, you may want to disable the feature and select the best impedance by trial and error method.

To disable automatic impedance matching, check the **Disable Impedance Match During System Startup** check box.

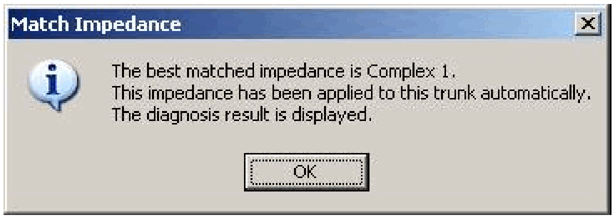
Using the Match Impedance Button

Whenever a new analog trunk is connected to an empty port or is replacing an existing trunk, you will need to use the **Match Impedance** button to select the best impedance profile.

To do this, follow these steps:

1. Click the **Impedance Match** button. While the impedance match is in process, you'll see a “progress” box.

   When the process is complete, the Match Impedance dialog box opens, with information relevant to this trunk:



The best matched impedance is Complex 1.
This impedance has been applied to this trunk automatically.
The diagnosis result is displayed.

Figure 103. Match Impedance dialog box

The **Impedance** parameter setting in the main dialog box is changed to the best match selection, and the measurement for noise and returned echo is performed with this impedance setting. The results of this measurement are displayed in the **Diagnosis** section of the main dialog box. The **Hybrid Echo Return Loss** field shows the measurement before adaptation of the selected Impedance profile, and the **Echo Return Loss** field shows the measurement after adaptation of the selected Impedance profile.

> **Note:** If the Hybrid Echo Return Loss reading of a trunk is worse than -6 dB, for example, -5 db, the trunk may be subject to VoIP voice quality problems. Use this trunk to connect to analog phones only, or configure it to be the least used trunk. (Acceptable range for Hybrid Echo Return Loss is -6 dB to -26 dB.)

Noise Level should be less than -67 dBm (acceptable range is -67 dBm to -90 dBm).

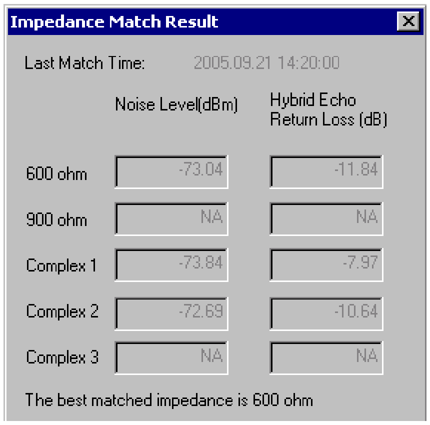
2. Make calls from the trunks to test voice quality.
3. Repeat steps 1 and 2 for all other trunk channels.

If the Hybrid Echo Return Loss and Noise Level are not within the acceptable range, take the following steps to troubleshoot:

1. Change the trunk to a different port on the Triton board, then diagnose again (this is to rule out a hardware problem).
2. Check to see if any wire taps to the trunk wire (bridge tap). If so, remove them, then test again.
3. Request the CO to check the trunk conditions, including Line Loss, and longitudinal balance.

The Match Result Button

Clicking the **Match Result** button shows you the result you got the last time you clicked the **Match Impedance** button for that trunk.



Last Match Time: 2005.09.21 14:20:00

	Noise Level(dBm)	Hybrid Echo Return Loss (dB)
600 ohm	-73.04	-11.84
900 ohm	NA	NA
Complex 1	-73.84	-7.97
Complex 2	-72.69	-10.64
Complex 3	NA	NA

The best matched impedance is 600 ohm

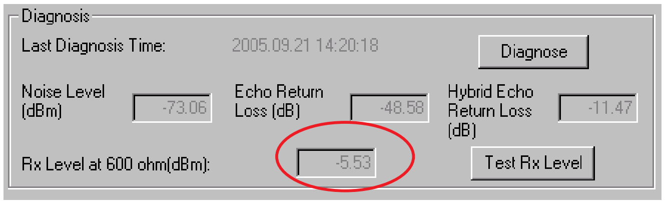
Figure 104. Impedance Match Result dialog box

Measuring the Rx Level of a Trunk Channel

In order to perform this test, you need to obtain the local CO’s Milli-Watt Test Number from your CO. When dialing this number, a 0dB tone is sent. For example, if your number is 510-252-9712, the Milli-Watt Test Number from the local CO is 510-252-0020 (the prefix 510-252 is the same).

1. Write down the **Rx Gain**, then set it to 0dB and click OK.
2. Write down the **Impedance** setting, then change it to 600ohm, and click OK.
3. Call the number you got from your CO, as noted above.
4. Click the **Test Rx Level** button. When the test is complete, the Test Rx Level dialog box opens.
5. Click **OK**. The Rx Level measurement is displayed in the Diagnosis section of the main dialog box.

   If you call your local CO’s Milli-Watt Test Number, the acceptable range for Rx Level should be between -6dB and -3 dB, with -5dB being ideal.



Last Diagnosis Time: 2005.09.21 14:20:18

Noise Level (dBm) -73.06

Echo Return Loss (dB) -48.58

Hybrid Echo Return Loss (dB) -11.47

Rx Level at 600 ohm(dBm): -5.53

6. Restore the **Impedance** and **Rx Gain** settings, and click **OK**.

If You Need to Improve the Rx Level

If the Rx Level measurement is between -6 to -9 dB, and IP phones are used, take the following steps to increase the gain for the Triton analog trunk to IP phone connection:

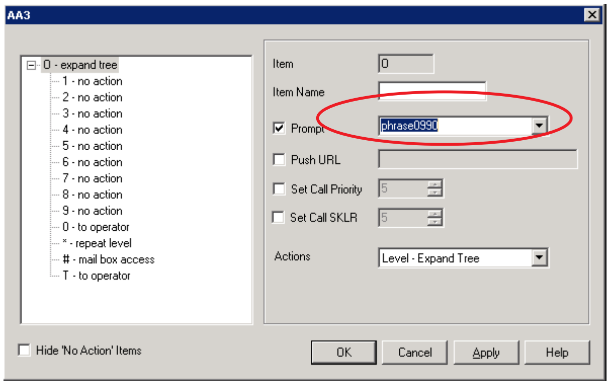
1. Go to VoIP Board configuration and click the **Advance** button.
2. Increase the Transmitting gain to IP Extension to 9 for the Triton Analog Trunk. (Do NOT change the gain in the trunk property of the Triton Analog Trunk Board, since it may impact the echo canceller performance.)

If the Rx Level measurement is worse than -9dB (for example, -10 dB) you should contact the CO to adjust the line loss to the acceptable range.

If You Don’t Have the Milli-Watt Test Number

If you don’t have the local CO’s Milli-Watt Test Number, you can follow the steps below to measure the line loss when calling two local trunks:

1. Copy C:\Post Office\Phrases\Lang1\phrase9900 to C:\Post Office\Phrases\LangCustom folder. Rename it an unused phrase name, for example, phrase0990 (the number must be less than 1000).
   This phrase is a 1 kHz test tone.
2. Select an unused AA and set the AA to play the prompt phrase you named in step 1 (0990 in this example).



AA3

- 0 - expand tree
  - 1 - no action
  - 2 - no action
  - 3 - no action
  - 4 - no action
  - 5 - no action
  - 6 - no action
  - 7 - no action
  - 8 - no action
  - 9 - no action
  - 0 - to operator
  - * - repeat level
  - # - mail box access
  - T - to operator

Item: 0

Item Name:

☑ Prompt: phrase0990

□ Push URL

□ Set Call Priority: 5

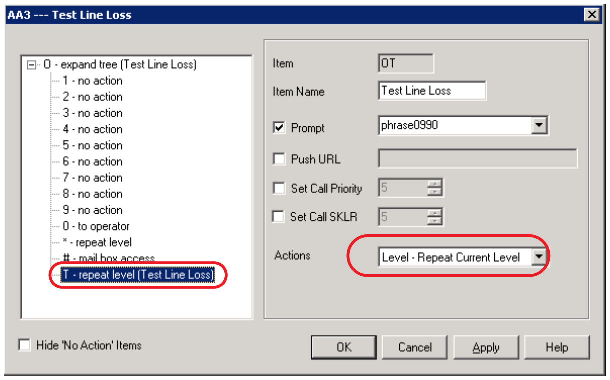
□ Set Call SKLR: 5

Actions: Level - Expand Tree

□ Hide 'No Action' Items

Figure 105. Setting the AA to play a prompt phrase

3. Set the Timeout to **Repeat Current Level**.



AA3 --- Test Line Loss

- 0 - expand tree (Test Line Loss)
  - 1 - no action
  - 2 - no action
  - 3 - no action
  - 4 - no action
  - 5 - no action
  - 6 - no action
  - 7 - no action
  - 8 - no action
  - 9 - no action
  - 0 - to operator
  - * - repeat level
  - # - mail box access
  - T - repeat level (Test Line Loss)

Item: 0T

Item Name: Test Line Loss

☑ Prompt: phrase0990

□ Push URL

□ Set Call Priority: 5

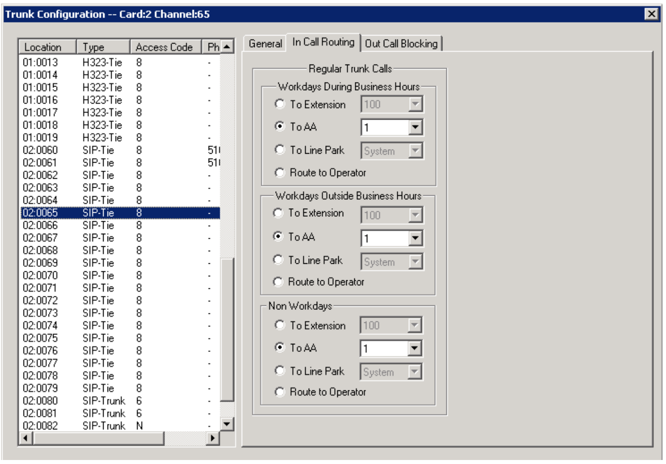
□ Set Call SKLR: 5

Actions: Level - Repeat Current Level

□ Hide 'No Action' Items

Figure 106. Setting Timeout to Repeat Current Level

4. Select a trunk as a testing reference – an analog trunk with a specific phone number is best – and set the trunk In Call Routing to the Test Line Loss AA.



Trunk Configuration -- Card:2 Channel:65

Location	Type	Access Code	Ph
01:0013	H323-Tie	8	-
01:0014	H323-Tie	8	-
01:0015	H323-Tie	8	-
01:0016	H323-Tie	8	-
01:0017	H323-Tie	8	-
01:0018	H323-Tie	8	-
01:0019	H323-Tie	8	-
02:0060	SIP-Tie	8	51
02:0061	SIP-Tie	8	51
02:0062	SIP-Tie	8	-
02:0063	SIP-Tie	8	-
02:0064	SIP-Tie	8	-
02:0065	SIP-Tie	8	-
02:0066	SIP-Tie	8	-
02:0067	SIP-Tie	8	-
02:0068	SIP-Tie	8	-
02:0069	SIP-Tie	8	-
02:0070	SIP-Tie	8	-
02:0071	SIP-Tie	8	-
02:0072	SIP-Tie	8	-
02:0073	SIP-Tie	8	-
02:0074	SIP-Tie	8	-
02:0075	SIP-Tie	8	-
02:0076	SIP-Tie	8	-
02:0077	SIP-Tie	8	-
02:0078	SIP-Tie	8	-
02:0079	SIP-Tie	8	-
02:0080	SIP-Trunk	6	-
02:0081	SIP-Trunk	6	-
02:0082	SIP-Trunk	N	-

Regular Trunk Calls

Workdays During Business Hours
- ○ To Extension: 100
- ● To AA: 1
- ○ To Line Park: System
- ○ Route to Operator

Workdays Outside Business Hours
- ○ To Extension: 100
- ● To AA: 1
- ○ To Line Park: System
- ○ Route to Operator

Non Workdays
- ○ To Extension: 100
- ● To AA: 1
- ○ To Line Park: System
- ○ Route to Operator

Figure 107. Setting trunk In Call Routing to an AA

5. Call from one trunk to the testing reference trunk. You should hear a 1 kHz tone playing at the originating side.

6. While the tone is playing, measure the Rx Level at the trunk that is making the outgoing call.

If the reading is less than -6 dB, for example -3 dB, take the following steps to attenuate the gain for the Triton Analog Trunk to IP phone connection:

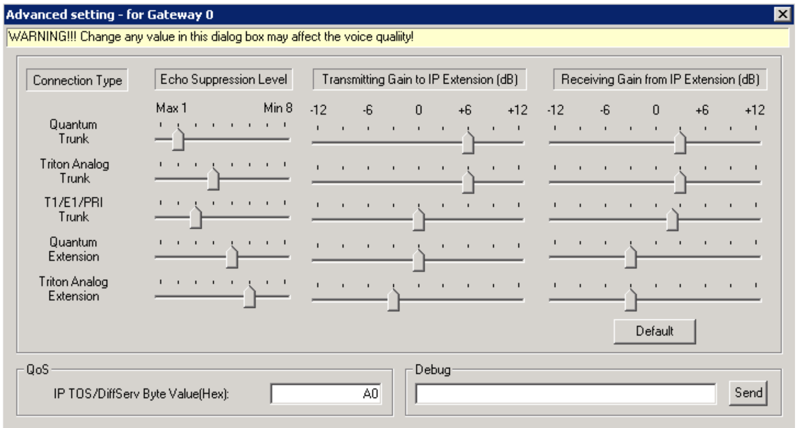
a. Go to VoIP Board configuration and click the **Advance** button.

b. Set the Transmitting gain to IP Extension to 3 for the Triton Analog Trunk. (Do NOT change the gain in the trunk property of the Triton Analog Trunk Board, since it may impact the echo canceller performance. If the reading is -6 dB to -14 dB, for example, -12 dB, no change is needed.

If the reading is -15 dB to -18 dB, take the following steps to increase the gain for the Triton Analog Trunk to IP phone connection:

a. Go to VoIP Board configuration and click the **Advance** button.

b. Set the Transmitting gain to IP Extension to 9 for the Triton Analog Trunk. (Do NOT change the gain in the trunk property of the Triton Analog Trunk Board, since it may impact the echo canceller performance.)


Advanced setting - for Gateway 0

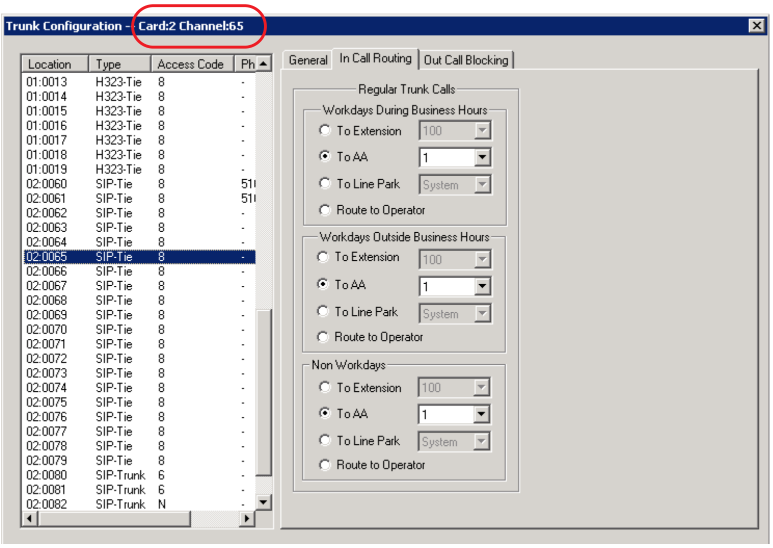
WARNING!!! Change any value in this dialog box may affect the voice quality!

IP TOS/DiffServ Byte Value(Hex): A0

If the reading is worse than -18 dB, you should contact your CO to adjust the line loss to the acceptable range.

Incoming Call Routing

To set incoming call routing for a trunk, select the trunk on the **General** tab, then click the **In Call Routing** tab in the **Trunk Configuration** window. The trunk location shows in the title bar.



Trunk Configuration -- Card:2 Channel:65

Location	Type	Access Code	Ph
01:0013	H323-Tie	8	-
01:0014	H323-Tie	8	-
01:0015	H323-Tie	8	-
01:0016	H323-Tie	8	-
01:0017	H323-Tie	8	-
01:0018	H323-Tie	8	-
01:0019	H323-Tie	8	-
02:0060	SIP-Tie	8	51
02:0061	SIP-Tie	8	51
02:0062	SIP-Tie	8	-
02:0063	SIP-Tie	8	-
02:0064	SIP-Tie	8	-
02:0065	SIP-Tie	8	-
02:0066	SIP-Tie	8	-
02:0067	SIP-Tie	8	-
02:0068	SIP-Tie	8	-
02:0069	SIP-Tie	8	-
02:0070	SIP-Tie	8	-
02:0071	SIP-Tie	8	-
02:0072	SIP-Tie	8	-
02:0073	SIP-Tie	8	-
02:0074	SIP-Tie	8	-
02:0075	SIP-Tie	8	-
02:0076	SIP-Tie	8	-
02:0077	SIP-Tie	8	-
02:0078	SIP-Tie	8	-
02:0079	SIP-Tie	8	-
02:0080	SIP-Trunk	6	-
02:0081	SIP-Trunk	6	-
02:0082	SIP-Trunk	N	-

Regular Trunk Calls

Workdays During Business Hours
- ○ To Extension 100
- ● To AA 1
- ○ To Line Park System
- ○ Route to Operator

Workdays Outside Business Hours
- ○ To Extension 100
- ● To AA 1
- ○ To Line Park System
- ○ Route to Operator

Non Workdays
- ○ To Extension 100
- ● To AA 1
- ○ To Line Park System
- ○ Route to Operator

Figure 108. Trunk Configuration, In Call Routing tab

Regular Trunk Calls

For each trunk - or using "**Apply to"** to apply the settings to multiple trunks - you can set routing for the three time periods defined in the **System Configuration** window, **Business Hours** tab ("Setting Business Hours" on page 38):

- During Business Hours
- Outside Business Hours
- Non Workdays

Within each of these three time slots, you have the following routing options for incoming calls:

- Route to an extension selected in the list
- Route to an auto attendant number selected in the list
- Route to a Line Park line selected in the list (see "Line Park Configuration" on page 245 for more detail)
- Route to the operator

Web IP Calls

For web IP calls, you can set routing for the three time periods defined in the **System Configuration** window, **Business Hours** tab ("Setting Business Hours" on page 38):

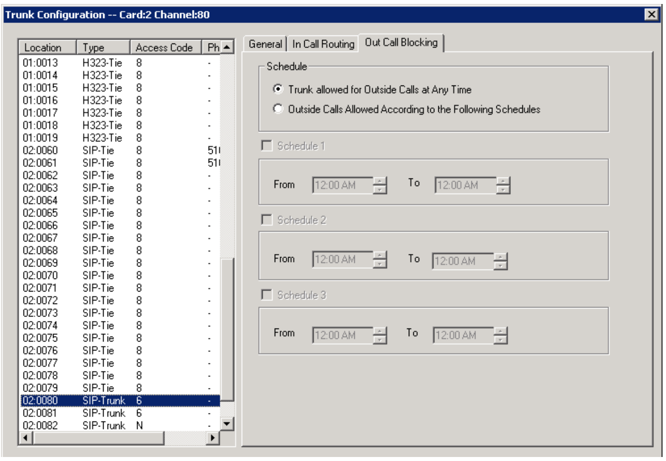
- During Business Hours
- Outside Business Hours
- Non Workdays

Within each of these three time slots, you have the following routing options for incoming calls:

- Route to an extension selected in the list
- Route to an auto attendant number selected in the list
- Route to the operator

Outgoing Call Blocking

To set outgoing call blocking for a trunk, select the trunk in the **General** tab, then click the **Out Call Blocking** tab in the **Trunk Configuration** window.



Trunk Configuration -- Card:2 Channel:80

Location	Type	Access Code	Ph
01:0013	H323-Tie	8	-
01:0014	H323-Tie	8	-
01:0015	H323-Tie	8	-
01:0016	H323-Tie	8	-
01:0017	H323-Tie	8	-
01:0018	H323-Tie	8	-
01:0019	H323-Tie	8	-
02:0060	SIP-Tie	8	51
02:0061	SIP-Tie	8	51
02:0062	SIP-Tie	8	-
02:0063	SIP-Tie	8	-
02:0064	SIP-Tie	8	-
02:0065	SIP-Tie	8	-
02:0066	SIP-Tie	8	-
02:0067	SIP-Tie	8	-
02:0068	SIP-Tie	8	-
02:0069	SIP-Tie	8	-
02:0070	SIP-Tie	8	-
02:0071	SIP-Tie	8	-
02:0072	SIP-Tie	8	-
02:0073	SIP-Tie	8	-
02:0074	SIP-Tie	8	-
02:0075	SIP-Tie	8	-
02:0076	SIP-Tie	8	-
02:0077	SIP-Tie	8	-
02:0078	SIP-Tie	8	-
02:0079	SIP-Tie	8	-
02:0080	SIP-Trunk	6	-
02:0081	SIP-Trunk	6	-
02:0082	SIP-Trunk	N	-

Schedule

● Trunk allowed for Outside Calls at Any Time

○ Outside Calls Allowed According to the Following Schedules

□ Schedule 1

From 12:00 AM To 12:00 AM

□ Schedule 2

From 12:00 AM To 12:00 AM

□ Schedule 3

From 12:00 AM To 12:00 AM

Figure 109. Trunk Configuration, Out Call Blocking tab

If you select **Trunk allowed for Outside Calls at Any Time**, call restrictions set in System Configuration, Outcall Routing, and Extension Configuration still apply to calls made on the trunk.

If you select **Outside Calls Allowed According to The Following Schedules**, you can then use the Schedule 1, 2, and 3 options to set up to three different time periods during which calls are allowed. You can use **Apply to** to apply the settings to multiple trunks.

CHAPTER

14

In Call Routing Configuration

In Call Routing rules determine how the system routes incoming trunk calls to various targets. The system's routing steps are as follows:

Step	Routing Process
1	Match DID number configured in extension, workgroup, or hunt group. If there is no match, go to the next step.
2	Match caller ID defined in the Caller ID Routing table. If there is a match and • today is a holiday, route the call according to the Holiday Profile's routing rules. • today is *not* a holiday, route the call according to business hour routing rules defined in the Caller ID Routing configuration. If there is no caller ID match, go to the next step.
3	Match DNIS number defined in the DNIS Routing table. If there is a match and • today is a holiday, route the call according to the Holiday Profile's routing rules. • today is *not* a holiday, route the call according to business hour routing rules defined in the DNIS Routing configuration. If there is no DNIS number match, go to the next step.
4	If today is a holiday, route the call according to the Holiday Profile configured for the trunk port that the call is coming in on. If today is *not* a holiday, route the call according to the business hours routing rules defined in the **In Call Routing** tab of the Trunk Configuration window.

The In Call Routing Configuration window lets you enter Caller ID and DNIS numbers into a routing table and set routing rules for a matched number.

To configure In Call Routing, select **PBX** > **In Call Routing Configuration**.

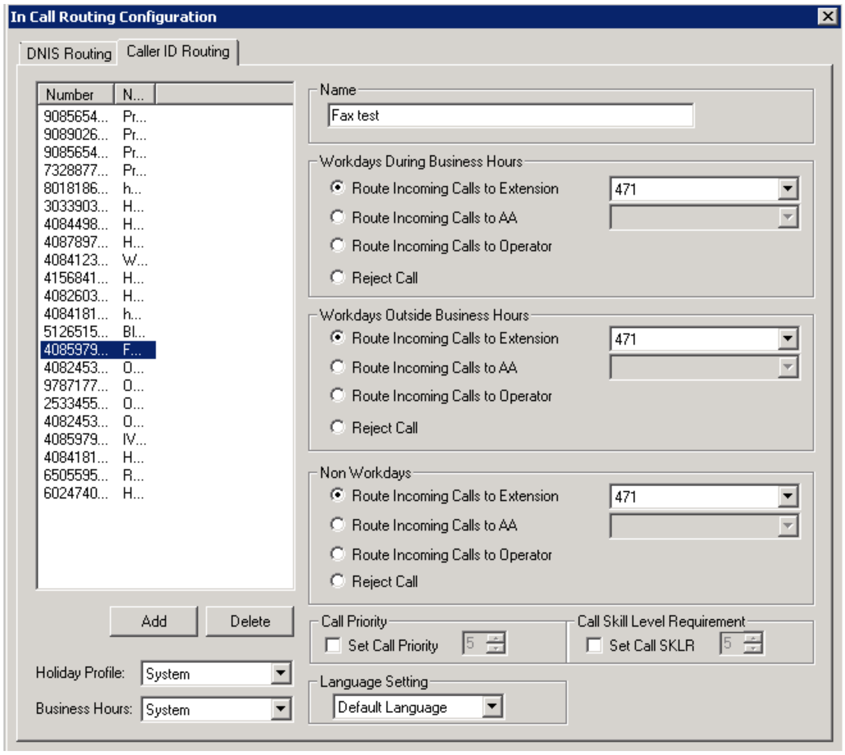
Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

Caller ID Routing

When an incoming call comes through a trunk with Caller ID, the system can route the call to the proper extension, to the auto attendant, or to the operator, based on the Caller ID number collected.

In order to locate an entry in the Caller ID table for an incoming call, a full match is required.

To access Caller ID routing, click the **Caller ID Routing** tab in the In Call Routing Configuration window.



In Call Routing Configuration

Number	N...
9085654...	Pr...
9089026...	Pr...
9085654...	Pr...
7328877...	Pr...
8018186...	h...
3033903...	H...
4084498...	H...
4087897...	H...
4084123...	W...
4156841...	H...
4082603...	H...
4084181...	h...
5126515...	Bl...
4085979...	F...
4082453...	O...
9787177...	O...
2533455...	O...
4082453...	O...
4085979...	IV...
4084181...	H...
6505595...	R...
6024740...	H...

Name: Fax test

Workdays During Business Hours
● Route Incoming Calls to Extension: 471
○ Route Incoming Calls to AA
○ Route Incoming Calls to Operator
○ Reject Call

Workdays Outside Business Hours
● Route Incoming Calls to Extension: 471
○ Route Incoming Calls to AA
○ Route Incoming Calls to Operator
○ Reject Call

Non Workdays
● Route Incoming Calls to Extension: 471
○ Route Incoming Calls to AA
○ Route Incoming Calls to Operator
○ Reject Call

Call Priority: □ Set Call Priority 5

Call Skill Level Requirement: □ Set Call SKLR 5

Holiday Profile: System

Business Hours: System

Language Setting: Default Language

Figure 110. In Call Routing window, Caller ID Routing tab

Adding and Deleting Caller ID Route Entries

To add entries to the Caller ID routing table, click the **Add** button. In the dialog box, type a **Caller ID Number** and a descriptive **Caller ID Name**, then click **OK**.

The number and name entries have the following requirements:

- The **Caller ID Number** field allows only 0-9, "-" (hyphen), and "*" (asterisk). For example, both 5102529712 and 510-252-9712 are acceptable.
- The **Caller ID Name** is descriptive and optional; it can be used to remind you about the nature of the number and routing. For example, you might give the 2529712 number the name "Tech Support."

To delete an entry, select it in the Caller ID number list, then click **Delete**.

Defining Caller ID Routing

After adding an entry, you define it by first selecting it in the list. When you select an entry, its name and other defined attributes, if any, appear in the fields of the tab. You can edit any of these attributes.

For each number, you can set routing for three distinct time periods defined in the **Business Hours** tab (see "Setting Business Hours" on page 38):

- During Business Hours
- Outside Business Hours
- Non Workdays

Within each of these three time slots, you have the following routing options for incoming calls:

- Route to a particular extension selected in the list

- Route to a particular auto attendant selected in the list
- Route to the operator
- Reject call

Also, you can set additional routing attributes based on:

- **Holiday Profile** – Routes incoming calls based on Holiday Profiles configured in System Configuration (see “Routing Calls on Holidays” on page 40)
- **Business Hours Profile** – Routes incoming calls based on Business Hours Profiles configured in System Configuration (see “Setting Business Hours” on page 38). **During Business Hours**, **Outside Business Hours** and **Non Working Day** are defined and selected by Business Hours profile.
- **Set Call Priority** – Lets you assign a call priority from 1-9 to the selected caller ID number. The highest priority is 1, the lowest priority is 9.
- **Set Call SKLR** – For workgroup-directed calls. Lets you assign a skill level requirement from 1-9 to the selected caller ID number. This setting tells the system to match the call to an agent’s skill level setting. (Setting an agent’s skill level is explained in “Skill Based Routing” on page 256.)
- **Language Setting** – Lets you specify that callers who dialed from the selected caller ID will hear prompts in the language you set here. This field will have choices only if you added sets of prompts according to the instructions in “Multilingual Configuration” on page 69.

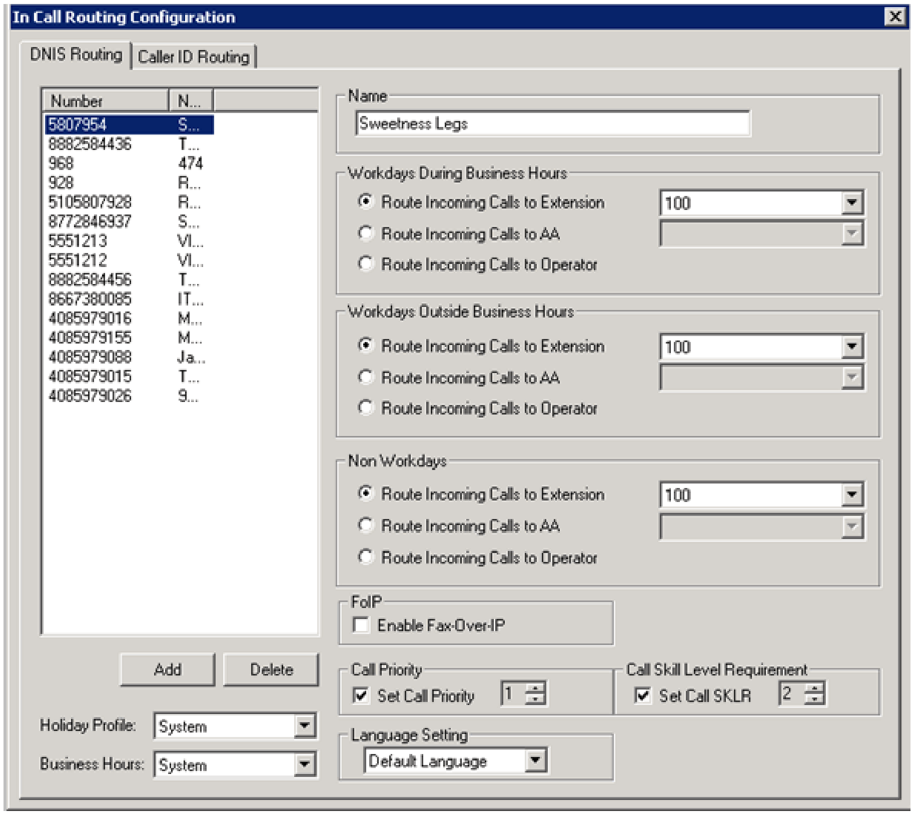
DNIS Routing

When an incoming call comes through a trunk with DNIS or DID numbers, the system can route the call to the proper extension, auto attendant or operator based on the DNIS or DID number collected.

In order to locate an entry in the DNIS table for an incoming call, a full match is required.

Note: For Altigen SIP trunks, use 11-digit numbers when configuring DNIS routing.

To access DNIS routing settings, click the **DNIS Routing** tab in the In Call Routing Configuration window.


In Call Routing Configuration

Number	N...
5807954	S...
8882584436	T...
968	474
928	R...
5105807928	R...
8772846937	S...
5551213	VI...
5551212	VI...
8882584456	T...
8667380085	IT...
4085979016	M...
4085979155	M...
4085979088	Ja...
4085979015	T...
4085979026	9...

Holiday Profile: System

Business Hours: System

Name: Sweetness Legs

Workdays During Business Hours
- ● Route Incoming Calls to Extension: 100
- ○ Route Incoming Calls to AA
- ○ Route Incoming Calls to Operator

Workdays Outside Business Hours
- ● Route Incoming Calls to Extension: 100
- ○ Route Incoming Calls to AA
- ○ Route Incoming Calls to Operator

Non Workdays
- ● Route Incoming Calls to Extension: 100
- ○ Route Incoming Calls to AA
- ○ Route Incoming Calls to Operator

FoIP
- □ Enable Fax-Over-IP

Call Priority
- ☑ Set Call Priority: 1

Call Skill Level Requirement
- ☑ Set Call SKLR: 2

Language Setting: Default Language

Figure 111. In Call Routing window, DNIS Routing tab

Adding and Deleting DNIS Route Entries

To add entries to the DNIS routing table, click the **Add** button. In the dialog box, type in a **DNIS Number** and a descriptive **DNIS Name**, then click **OK**.

The number and name entries have the following requirements:

- The **DNIS Number** must be the numbers 0 - 9 (the hyphen is not accepted in this dialog box). For example, 2529876 is an acceptable entry, but 252-9876 is not.
- The **DNIS Name** is descriptive and optional; it can be used to remind you about the nature of the number and routing. For example, you might give the 2529876 number the name “Tech Support.”

To delete an entry, select it in the DNIS number list, then click **Delete**.

Defining DNIS Routing

After adding an entry, you define it by first selecting it in the list. When you select an entry, its name and other defined attributes, if any, appear in the fields of the tab. You can edit any of these attributes.

For each number, you can set routing for three distinct time periods defined in the **Business Hours** tab (see “Setting Business Hours” on page 38):

- During Business Hours
- Outside Business Hours
- Non Workdays

Within each of these three time slots, you have the following routing options for incoming calls:

- Route to a particular extension selected in the list
- Route to a particular auto attendant selected in the list
- Route to the operator

Also, you can set additional routing attributes based on:

- **Holiday Profile** – Routes incoming calls based on Holiday Profiles configured in the System Configuration window (see “Routing Calls on Holidays” on page 40)
- **Business Hours Profile** – Routes incoming calls based on Business Hours Profiles configured in the System Configuration window (see “Setting Business Hours” on page 38). **During Business Hours**, **Outside Business Hours** and **Non Working Day** are defined and selected by the Business Hours profile.
- **Enable Fax-over-IP** – Lets you enable the FoIP feature. (Note that FoIP support is best effort and can be dependent on the fax device make/model – MaxCS fax device configuration guides can be found in the Altigen Knowledge Base)
- **Set Call Priority** – Lets you assign a call priority from 1-9 to the selected DNIS number. The highest priority is 1, the lowest priority is 9.
- **Set Call SKLR** – For workgroup-directed calls. Lets you assign a skill level requirement from 1-9 to the selected DNIS number. This setting tells the system to match the call to an agent’s skill level setting. (Setting an agent’s skill level is explained in “Skill Based Routing” on page 256.)
- **Language Setting** – Lets you specify that callers who dialed the selected number will hear prompts in the language you set here. This field will have choices only if you added sets of prompts according to the instructions in “Multilingual Configuration” on page 69.

FoIP In-Call Routing

For instructions on FoIP In Call Routing, see *Fax-over-IP Configuration*.

CHAPTER

15

Out Call Routing Configuration

There are two ways to initiate outbound dialing in an Altigen PBX:

- **Using the trunk access code**. The trunk access code is easy to configure and use. However, it does not have the capability to resolve complicated dialing situations.
- **Using the route access code.** Using the route access code with the Out Call Routing table can resolve the following complicated dialing situations:
  - Multiple 10-digit dialing area codes.
  - Both 10-digit and 11-digit dialing in the same area code.
  - Multiple carriers providing trunks for different purposes. For example, you may have a local carrier provide trunks for local calls only and a long distance carrier provide trunks that can accept only long distance dialing.
  - Block certain dialing patterns by creating an exceptions list.
  - Assist VoIP hop-off dialing to another system.
  - Assist T1/PRI tie trunk hop-off to other system.
  - Assist system Zoomerang and client application dialing, for example, MaxCommunicator and MaxAgent. For example, dialing from MaxCommunicator will carry 11 digits and require the system to remove a digit before making a call to the carrier if it is a 10-digit dialing area.
  - Divide trunks with the same characteristics into multiple routes and prioritize them when assigning routes on the **Default Routes** tab or on the **Dialing Pattern** tab of the Out Call Routing Configuration window.

When a user dials an outside number using the route access code, the system performs the following tasks:

- Compares the dialed number with entries in the **Dialing Pattern** table. If there is a match, the system uses the route assigned to the dialing pattern to make the outbound call. The route assigned to the special dialing pattern may have a digit manipulation rule to add or remove digits from the dialed number.
- If there is no match in the **Dialing Pattern** table, the system examines the digits to determine if the call is a local, long distance, international, or emergency call. The routes defined in the **Default Routes** tab are used to process the call.

Configuring Out Call Routing

To configure out call routing, select **PBX** > **Out Call Routing Configuration**.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

The following configuration steps may help you configure out call routing correctly.

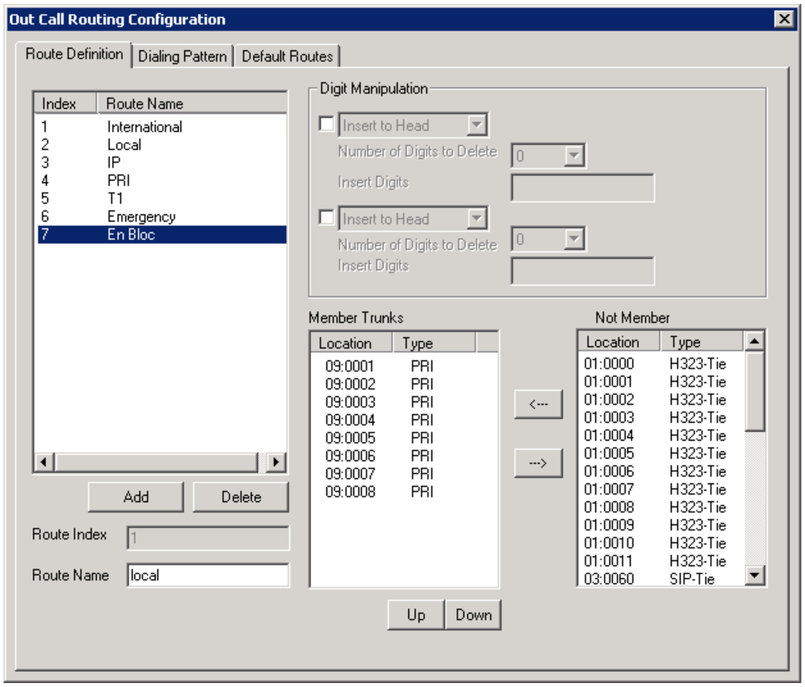
1. Before you configure Out Call Routing, make sure a route access code is configured in the System Configuration window, **Number Plan** tab. If you have a problem changing a first-digit assignment in the **Number Plan** tab to a route access code, you may need to set the **Access Code** in the Trunk Configuration window for all trunks to **None**.
2. Create a route and assign trunks to the route. Typically, different types of trunks will be grouped to different routes. For example, you may need to create a local route for local trunks, a long distance route for long distance trunks, and a VoIP route for IP trunks.
3. Assign routes as Default Routes so that regular 7-digit, 11-digit, international, and emergency calls will go through.
4. Solve a complicated dialing situation by adding an entry into the **Dialing Pattern** table and assigning a route to the specific dialing pattern.
5. If the dialing pattern requires adding or removing digits, you may need to edit the **Digit Manipulation** on the **Route Definition** tab to solve the problem. Repeat steps 4 and 5 until all complicated dialing patterns are entered and configured properly.
6. If a dialing pattern will use another system's trunk to hop-off, you may need to create a VoIP or T1/PRI tie trunk route and configure digit manipulation to indicate which system to hop-off to and how to tell another system that this is a hop-off dialing by adding a trunk access code or route access code in the dialing stream.
7. If you would like to block a specific dialing pattern, add the dialing pattern and check **Disallow this dialing pattern** check box.
8. Fax trunk channels used for fax routing should not be added to Out Call Routing.

Warning! Make sure the default 911 route is configured to a route that can accept 911 calls (see Figure 113). Failure to do so may cause failure of direct 911 dialing. If you do not want a user to call 911 directly because of too many 911 dialing errors, you can leave the 911 route not configured. In this case, you need to let all extension users know that they need to dial 9+911 to call emergency service. A proper warning sticker on the phone to notify employees about 9+911 dialing would be a good practice.

Some configuration examples are provided at the end of the chapter. Please use them as a reference to help you configure your dialing pattern correctly.

About Route Definitions

A route definition consists of a route name and group of trunks, listed in the order that the system will use for outgoing calls.



Index	Route Name
1	International
2	Local
3	IP
4	PRI
5	T1
6	Emergency
7	En Bloc

☐ Insert to Head
Number of Digits to Delete: 0
Insert Digits:

☐ Insert to Head
Number of Digits to Delete: 0
Insert Digits:

Route Index: 1
Route Name: local

Member Trunks

Location	Type
09:0001	PRI
09:0002	PRI
09:0003	PRI
09:0004	PRI
09:0005	PRI
09:0006	PRI
09:0007	PRI
09:0008	PRI

Not Member

Location	Type
01:0000	H323-Tie
01:0001	H323-Tie
01:0002	H323-Tie
01:0003	H323-Tie
01:0004	H323-Tie
01:0005	H323-Tie
01:0006	H323-Tie
01:0007	H323-Tie
01:0008	H323-Tie
01:0009	H323-Tie
01:0010	H323-Tie
01:0011	H323-Tie
03:0060	SIP-Tie

Figure 112. Out Call Routing Configuration, ***Route Definition*** *tab*

Route Parameter	Description
Route Index	For identification purposes only.
Route Name	Description of the route (maximum 30 characters).
Digit Manipulation	You can insert or delete digits from the dialed number. See configuration samples to learn how to use digit manipulation in different situations. **Insert to Head**: Insert a string of digits in front of the dialed number. **Delete from Head**: Remove a string of digits from the beginning of the dialed number.
Member Trunks	Displays the trunks assigned to the selected route. The order in which member trunks are added determines the order in which the trunks are used by the system when making an outbound call (the first trunk listed is used first, and so forth).
Not Member	Displays all trunks that are not assigned to the selected route.

Creating /Deleting Routes

1. Click **Add** under the route definition list.
2. Type in a name and index number, and click **OK**.
3. To add trunks to the route, select trunks from the **Not Member** list and use the <--- button to move selected trunks to the **Member Trunks** list.
4. Use the **Up** and **Down** buttons to change the position of a trunk in the **Member Trunks** list. This is the order in which trunks are accessed.
5. Click **Apply**.

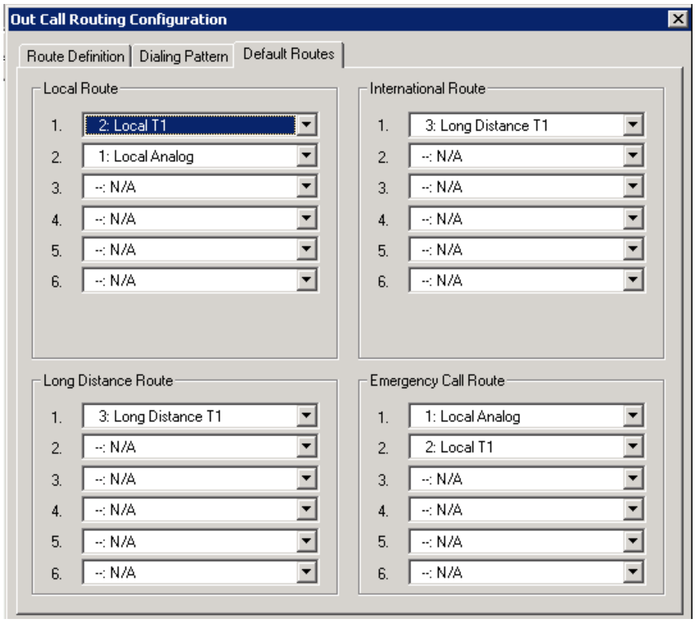
To delete a route, select the route and click the **Delete** button.

Setting Default Routes

You can set default routes for four types of outgoing calls: **local, long distance, international,** and **emergency**.

Warning! It is important that you set up default routes **right after routes are defined**. Failing to do so will cause outbound dialing failure.

Click the **Default Routes** tab in the **Out Call Routing Configuration** window to configure default routes.



Local Route

1. 2: Local T1
2. 1: Local Analog
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

International Route

1. 3: Long Distance T1
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

Long Distance Route

1. 3: Long Distance T1
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

Emergency Call Route

1. 1: Local Analog
2. 2: Local T1
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

For each type of call, the system will use trunks specified in the “1” field, if available, otherwise use trunks in the “2” field, and so on.

Figure 113. Out Call Routing Configuration, ***Default Routes*** *tab*

The above configuration means:

- The system has a group of analog trunks and a T1 digital trunk from a local carrier that can accept local and emergency calls.
- The system has a T1 digital trunk from a long distance carrier that can only accept long distance calls.
- The administrator segmented local trunks into two routes, "Local Analog" and "Local T1". A "Long Distance T1" route is created for the T1 from the long distance carrier.
- When a user makes a local call, the administrator wants the system to use local T1 trunks first. If local T1 trunks are busy, then the system uses local analog trunks.
- When a user makes an emergency call, the administrator wants the system to dial out from local analog trunks first. If local analog trunks are busy, the system uses the local T1 trunk.

About Dialing Patterns

If your system is using a route access code, most likely you have one of the following situations:

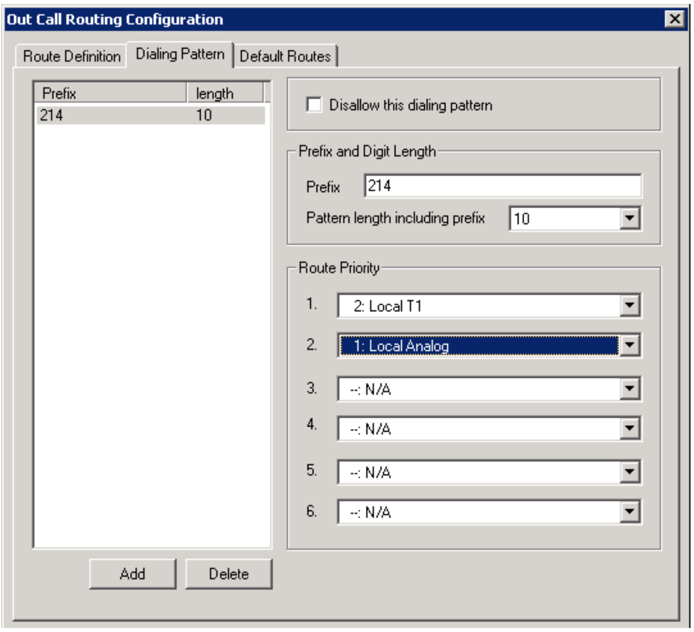
- Your area may have multiple 10-digit dialing area codes.
- Your area may have both 10-digit and 1+10 digit dialing in a same area code.
- Your system needs to borrow another system's trunk to make an outbound call over an IP or tie trunk.
- You would like to block a dialing pattern in addition to system restriction setting.

Dialing patterns are exceptions. If you can, minimize the number of dialing pattern entries. Most companies don't need to create dialing patterns.

Creating/Deleting Dialing Patterns

to create a dialing pattern,

1. Click the **Dialing Pattern** tab on the Out Call Routing Configuration window.



Out Call Routing Configuration

Prefix	length
214	10

☐ Disallow this dialing pattern

Prefix and Digit Length

Prefix: 214

Pattern length including prefix: 10

Route Priority

1. 2: Local T1
2. 1: Local Analog
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

*Figure 114. Out Call Routing Configuration, **Dialing Pattern** tab*

2. Click the **Add** button.
3. Type in the prefix and pattern length, and click **OK**.
4. Assign routes to this prefix by selecting routes from the lists in the Route Priority section of the **Dialing Pattern** tab.
5. If this is a restricted number or pattern, skip step 4 and check the **Disallow this dialing pattern** check box.

If you need to delete a dialing pattern, select the pattern you want to remove and click the **Delete** button.

Dialing Pattern Configuration Tips

- If a dialing pattern has multiple routes assigned to it, the system will try to use the first route configured to process the call that has this dialing pattern. If the first route is busy or not in service, the system will use the second route, and so on.
- If a dialing pattern requires the system to add or remove digits, a route with digit manipulation configuration needs to be set up correctly. This means that you may need to have the same group of trunks belong to different routes. Each route may have a different digit manipulation rule.
- If you are using dialing pattern to restrict outgoing calls, you need to be aware of the following system implementations:
  - The system first checks to see if the number is blocked for this extension (a setting in the Extension Configuration window, **Restriction** tab).

- The system then checks the System Configuration **Call Restriction** tab settings to see if this number is blocked by the system.
- The system then checks the **Dialing Pattern** configuration, and if a specific number or pattern is not blocked, the system will dial the number through a proper route.

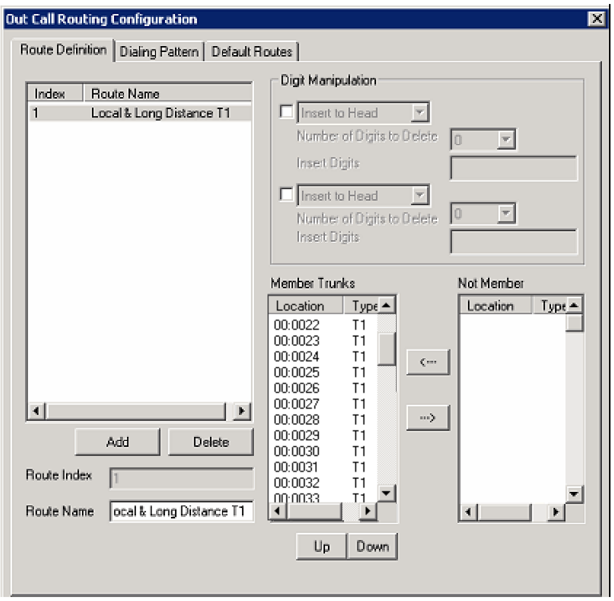
In other words, if extension and system call restrictions are not blocking a number or pattern, you can use Out Call Routing to build restriction rules to block numbers or patterns.

Configuration Example – Solving 10-digit Dialing

Situation: Company ABC located in Dallas, area code 214, has one PRI circuit from the local carrier. Both 214 and 972 area codes are local 10-digit dialing area codes. The carrier will reject the call if the system dials 1214 or 1972 when dialing a local call.

Configuration Steps:

1. Create a route to include all the T1 channels.



Index	Route Name
1	Local & Long Distance T1

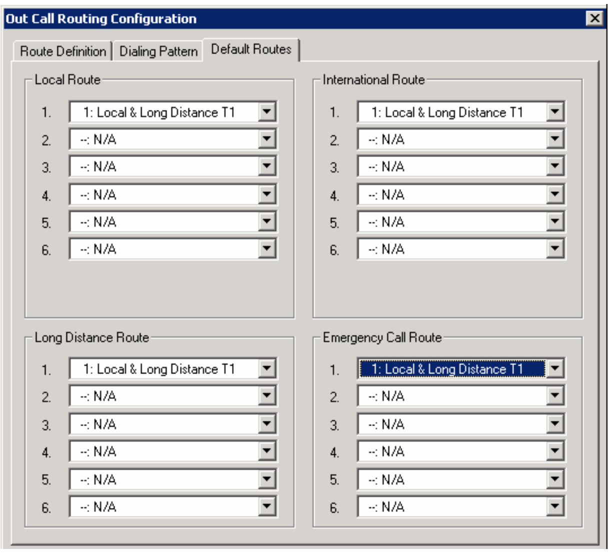
Route Index 1

Route Name ocal & Long Distance T1

Member Trunks:

Location	Type
00:0022	T1
00:0023	T1
00:0024	T1
00:0025	T1
00:0026	T1
00:0027	T1
00:0028	T1
00:0029	T1
00:0030	T1
00:0031	T1
00:0032	T1
00:0033	T1

2. Apply the route to **Default Routes**.



Out Call Routing Configuration

Route Definition | Dialing Pattern | Default Routes

Local Route

1. 1: Local & Long Distance T1
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

International Route

1. 1: Local & Long Distance T1
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

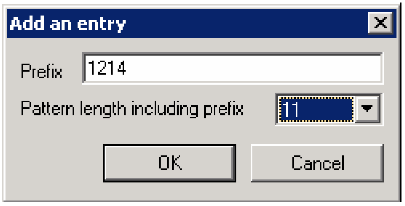
Long Distance Route

1. 1: Local & Long Distance T1
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

Emergency Call Route

1. 1: Local & Long Distance T1
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

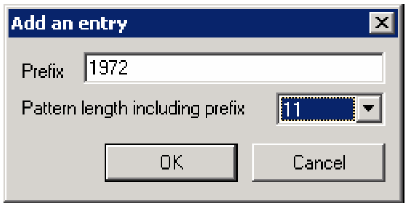
3. On the Dialing Pattern tab, add two dialing patterns: “1214” and “1972”, each with a pattern length of 11.



Add an entry

Prefix: 1214

Pattern length including prefix: 11

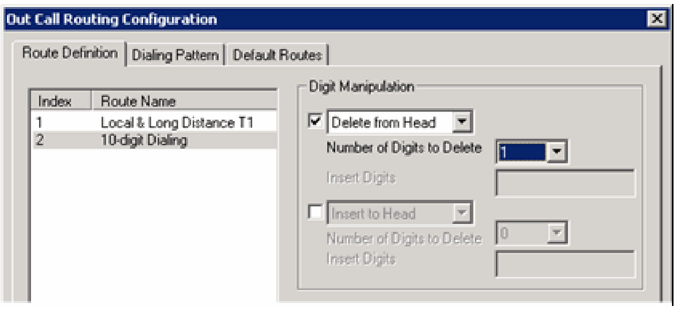


Add an entry

Prefix: 1972

Pattern length including prefix: 11

4. Define a route called “10-digit Dialing” and add all T1 channels to the route. In the “Digit Manipulation” section, check the first box, select **Delete from Head**, and delete 1 digit:



Out Call Routing Configuration

Route Definition | Dialing Pattern | Default Routes

Index	Route Name
1	Local & Long Distance T1
2	10-digit Dialing

Digit Manipulation

☑ Delete from Head

Number of Digits to Delete: 1

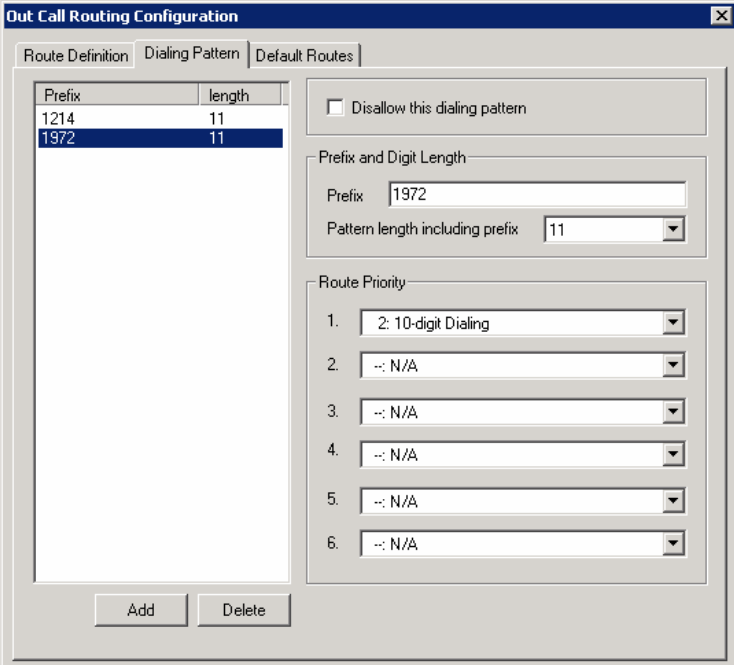
Insert Digits:

☐ Insert to Head

Number of Digits to Delete: 0

Insert Digits:

5. Apply the “10-digit Dialing” route to dialing pattern 1214 and 1972:



Prefix	length
1214	11
1972	11

□ Disallow this dialing pattern

Prefix and Digit Length

Prefix: 1972

Pattern length including prefix: 11

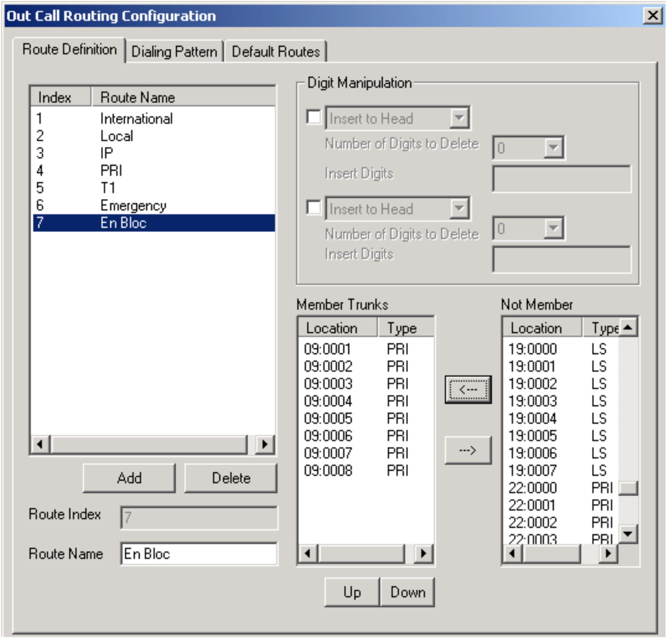
Route Priority

1. 2: 10-digit Dialing
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

Resolving Dialing Delay: Non-USA/Canada Countries

When installing the Altigen system outside of North America, you may experience dialing delay when dialing through E1/PRI trunks that are using en-bloc (buffering digits and sending all digits at once). The system dialing logic may cause a 7-second inter-digit dialing delay for en-bloc trunks. To reduce the dialing delay, the following configuration is recommended:

1. On the **Number Plan** tab in the **System Configuration** window, select a digit for route access.
2. On the **Route Definition** tab of the **Out Call Routing Configuration** window, add a route definition entry for en-bloc and assign the member en-bloc trunk(s).



Index	Route Name
1	International
2	Local
3	IP
4	PRI
5	T1
6	Emergency
7	En Bloc

Route Index: 7

Route Name: En Bloc

Member Trunks

Location	Type
09:0001	PRI
09:0002	PRI
09:0003	PRI
09:0004	PRI
09:0005	PRI
09:0006	PRI
09:0007	PRI
09:0008	PRI

Not Member

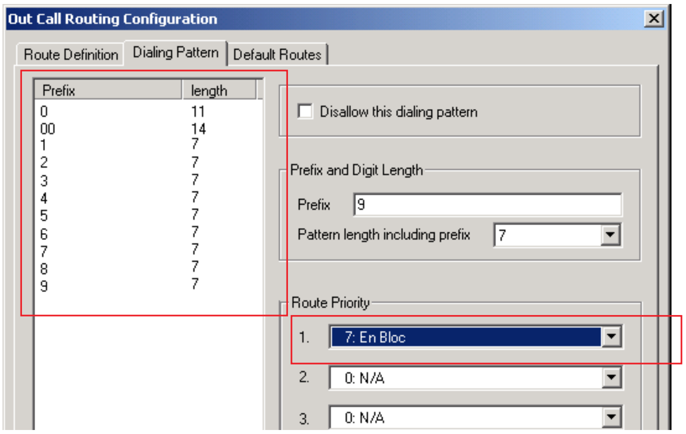
Location	Type
19:0000	LS
19:0001	LS
19:0002	LS
19:0003	LS
19:0004	LS
19:0005	LS
19:0006	LS
19:0007	LS
22:0000	PRI
22:0001	PRI
22:0002	PRI
22:0003	PRI

3. On the **Dialing Pattern** tab of the **Out Call Routing Configuration** window, add dialing pattern definition entries for the following prefixes:

- prefix = 0, length = 11
- prefix = 00, length = 14
- prefixes = 1-9, each length = 7

In the **Route Priority** field, use the list to select the **En-Bloc** route definition (assigned in step 2).

The Dialing Pattern tab should look as follows:



Prefix	length
0	11
00	14
1	7
2	7
3	7
4	7
5	7
6	7
7	7
8	7
9	7

□ Disallow this dialing pattern

Prefix: 9

Pattern length including prefix: 7

1. 7: En Bloc
2. 0: N/A
3. 0: N/A

With this configuration, the system will see that all digits have been collected and will send digits to the CO, instead of waiting 7 seconds for the dialing to finish.

CHAPTER

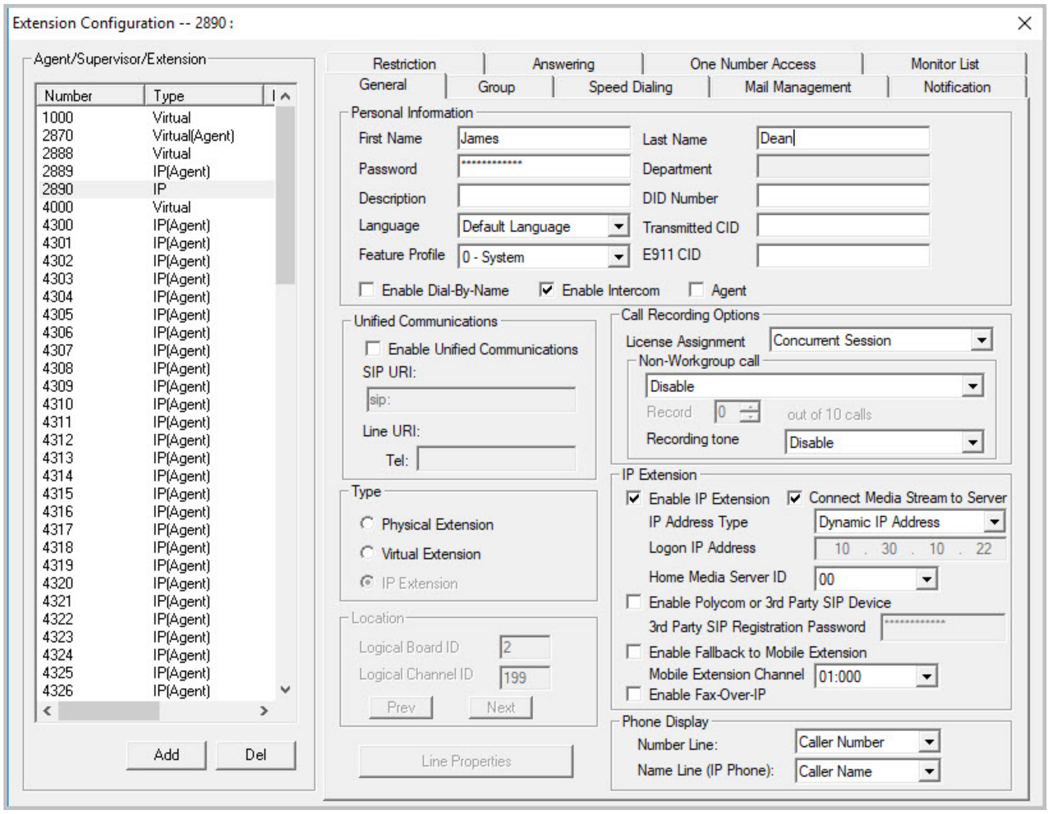
16

Extension Configuration

The Extension Configuration window provides for creating extensions and setting their attributes. To open the Extension Configuration window, select **PBX** > **Extension Configuration**.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

To set up an application extension, see *Application Extension Configuration*. To set up an IP extension, see *Setting Up IP Extensions*. To set up a mobile extension, see *Mobile Extension Configuration*.



Extension Configuration -- 2890 :

Agent/Supervisor/Extension

Number	Type
1000	Virtual
2870	Virtual(Agent)
2888	Virtual
2889	IP(Agent)
2890	IP
4000	Virtual
4300	IP(Agent)
4301	IP(Agent)
4302	IP(Agent)
4303	IP(Agent)
4304	IP(Agent)
4305	IP(Agent)
4306	IP(Agent)
4307	IP(Agent)
4308	IP(Agent)
4309	IP(Agent)
4310	IP(Agent)
4311	IP(Agent)
4312	IP(Agent)
4313	IP(Agent)
4314	IP(Agent)
4315	IP(Agent)
4316	IP(Agent)
4317	IP(Agent)
4318	IP(Agent)
4319	IP(Agent)
4320	IP(Agent)
4321	IP(Agent)
4322	IP(Agent)
4323	IP(Agent)
4324	IP(Agent)
4325	IP(Agent)
4326	IP(Agent)

Personal Information

First Name	James	Last Name	Dean
Password	************	Department	
Description		DID Number	
Language	Default Language	Transmitted CID	
Feature Profile	0 - System	E911 CID	

□ Enable Dial-By-Name ☑ Enable Intercom □ Agent

Unified Communications

□ Enable Unified Communications

SIP URI: sip:

Line URI:

Tel:

Type

○ Physical Extension

○ Virtual Extension

● IP Extension

Location

Logical Board ID 2

Logical Channel ID 199

Call Recording Options

License Assignment: Concurrent Session

Non-Workgroup call: Disable

Record 0 out of 10 calls

Recording tone: Disable

IP Extension

☑ Enable IP Extension ☑ Connect Media Stream to Server

IP Address Type: Dynamic IP Address

Logon IP Address: 10 . 30 . 10 . 22

Home Media Server ID: 00

□ Enable Polycom or 3rd Party SIP Device

3rd Party SIP Registration Password: ************

□ Enable Fallback to Mobile Extension

Mobile Extension Channel: 01:000

□ Enable Fax-Over-IP

Phone Display

Number Line: Caller Number

Name Line (IP Phone): Caller Name

Figure 115. Extension Configuration window

There are three types of extensions:

- **Physical Extensions** are associated with a physical port and device, usually a telephone set. This is what most users think of as an *extension*.
- **Virtual Extensions** are not associated with a physical port. Virtual extensions can be used as message mailboxes and in telephone sharing environments. Users of a virtual extension can log in on any available station to access physical extension features using Feature Codes.
- **IP Extensions** are generally associated with an IP phone. The option is unavailable when the **Enable IP Extension** option is not checked. When **Enable IP Extension** is checked, it will allow the IP phone to log on as an IP extension.

About the Apply To Button

A change you make to an extension can often be applied to one or more other extensions by using the **Apply To** button.

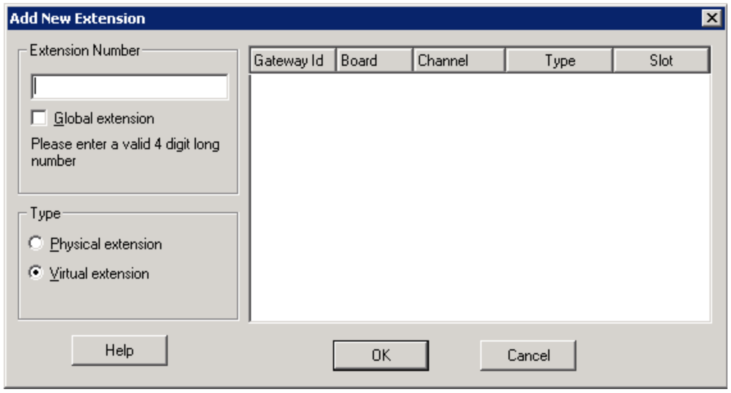
Clicking the **Apply To** button opens a list of all extensions to which the change can apply. Select the extensions to which you want to apply the change (all are selected, by default). Use the **Shift** or **Ctrl** keys to select several extensions.

The **Apply To** button is disabled unless a change you made can be applied to other extensions. When you use the button to apply changes to multiple extensions, it works on only those changed attributes that can be applied.

Setting up Extensions

Set up new extensions in the Extension Configuration window.

1. Click the **Add** button below the **Agent/Supervisor/Extension** list.



Add New Extension

Extension Number

□ Global extension

Please enter a valid 4 digit long number

Type

○ Physical extension

● Virtual extension

Gateway Id	Board	Channel	Type	Slot

Figure 116. The Extension parameters

2. Type in an **Extension Number**.

   The number must begin with a number assigned to be used for extensions, and it must be the length assigned to extensions, both of which are set on the **Number Plan** tab in the System Configuration window, as described in “Setting a System Number Plan” on page 34.

3. If you have a multi-site setup, with multiple MaxCS systems connected over IP, a VoIP domain is created in the Enterprise configuration. If you want to publish the extension to all MaxCS systems within the VoIP domain, check the **Global Extension** check box. “(Global)” will be displayed beside the extension’s type in the **Agent/Supervisor/Extension** list. No configuration is needed on other MaxCS systems on behalf of this extension.

   These are the benefits of making an extension a Global extension in a multi-site installation:

- A user from any system only has to dial the Global Extension number, and MaxCS will resolve the routing through the VoIP domain setting.
- Any user within the VoIP domain can forward voice mail to this Global extension.
- The client applications MaxCommunicator and MaxAgent can see this Global extension number even it is not an extension in the local system.

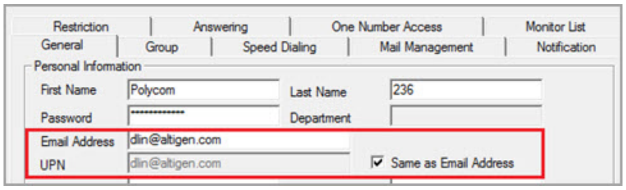
4. Select the **Type** of extension from the two options, **Physical** or **Virtual**. Unless this is an analog extension and you know the Gateway ID, Board ID, or Channel number, creating a new extension as a virtual extension is recommended. You can activate the extension from an analog or Altigen IP phone by using #27+password to log in. The system will determine the Gateway ID, Board ID, channel number, or IP address automatically.
5. Depending on the type of extension you're creating, take one of the following actions:
   - If you're setting a *virtual number*, you're done. Click **OK**.
   - If you're setting up a physical extension, select an available physical location—***gateway, board*** and ***channel*** for the line—then click **OK**.

     The board ID and the channels (the ports) are displayed and available if they have not yet been assigned to an extension. Use the **Next** and **Prev** buttons in the Location section to select a location.

After you create an extension, you can set basic attributes on the Extension Configuration **General** tab. These attributes are discussed below.

Setting Personal Information

The top section of the **General** tab is for Personal Information:



First Name: Polycom
Last Name: 236
Password: ************
Department:
Email Address: dlin@altigen.com
UPN: dlin@altigen.com
☑ Same as Email Address

- **First Name** and **Last Name** of the extension user, each with a maximum of 32 characters.

  Note: Only alphanumerical characters (A-Z, a-z,1-9) are supported for extension/group first name and last name. Symbols (such as “#”, “*”, “/”, “-”) are blocked, so as not to conflict with Dial by Name (#34) and other feature codes.

- **Password** for the extension user. The default is the system default password set on the **Number Plan** tab in the System Configuration window.

  A valid password must meet your password requirements and cannot be the same as its extension number. Basic password patterns, such as repeated digits (1111), consecutive digits strings (1234), or digits that match the extension (Ext. **101** using **101**2, 9**101**, **101**01, and so on) are not allowed. The letters map to numbers as follows:

Numbers	Letters	Numbers	Letters
2	A, B, C, a, b, c	6	M, N, O, m, n, o
3	D, E, F, d, e, f	7	P, Q, R, S, p, q, r, s
4	G, H, I, g, h, i	8	T, U, V, t, u, v
5	J, K, L, j, k, l	9	W, X, Y, Z, w, x, y, z

- **Department** – In an Enterprise VoIP domain, departments can be defined and extensions can be assigned to a department by using Enterprise Manager. When this is done, the department is displayed here.
- **Email Address** – The email address of this user. If you export extension configuration settings and import them to the Service Hub, this Email Address field is used for Presence and Meeting Synchronization and Contact Integration with Exchange in MaxCommunicator Web.
- **UPN** – This field is the User Principal Name(UPN) of the AD user. If the user does not have an UPN name, Email Address is recommended for this field.. If you export extension configuration settings and import them to the Service Hub, this UPN field is used as the Service Hub login.
- **DID Number** – Each extension can be assigned a DID number. This number does not have a fixed length, but the length must be long enough (range 2 - 16) for the system to match the DID incoming call.

  If you configure a 10-digit DID number and inbound digital trunks only receive 4 digits, the last 4 digits of the DID number configured will be matched.
- **Transmitted CID** – Each extension number can be assigned a caller ID number. When an outgoing call is made by this extension through PRI or IP trunks, the caller ID number entered in this field will be transmitted to the receiving caller.

  When an extension user makes an outbound call through a PRI trunk, the system will transmit the Caller ID based on the following rules:
  - If the Transmitted CID is configured, the number will be sent.
  - If the Transmitted CID is not configured, the DID number will be sent if it is a valid 10-digit number.
  - If the DID number is not configured or not valid, the **Area Code** and **Phone Number** entered in the Trunk Configuration window will be sent.
  - If the **Area Code** and **Phone Number** are not configured in the Trunk Configuration window, the **System Main Number** in the System Configuration window will be sent.

  Note: These rules may be overridden by your PRI CID configuration or the SIP Trunk Profile you're using.
- **E911 CID** – A number entered in this field will be transmitted as the caller ID for 911 calls made by this extension. See "Location-Based E911" on page 295 for instructions on setting up E911 Location IDs for IP phones.
- **Language** – Sets the language the extension user will hear for voice mail and system prompts. If voice mail and system phrases have been translated into other languages and properly added to the C:\PostOffice\Phrases directory, the languages will be selectable from the **Language** list. (See "Multilingual Configuration" on page 69 for information on adding translated prompts to the MaxCS system).
- **Feature Profile** – Sets an extension feature profile that includes enabling or disabling of extension features. The feature profile must first be configured by the administrator on the **Feature Profiles** tab of System Configuration.
  - A feature profile assigned to an Altigen IP phone should have #26 enabled.
- **Enable Dial-By-Name –** Select this box to allow incoming callers to search the extension list by employee name for this extension.
- **Enable Intercom** – Select this box to enable the intercom call feature for this extension. Pressing **#93** allows the user to make an intercom call to another intercom-enabled extension.

  Note: Intercom is available for extensions on Triton Analog Extension Boards and Altigen IP Phone Extensions.
- **Agent** – Allows the extension to be added as a member of one or multiple hunt groups or workgroups. "(Agent)" will be displayed in the extension's **Type** field, next to the extension type.

- **Release SIP Tie-Link Trunk** – This option has been added to support various AudioCodes devices. For full AudioCodes configuration instructions, refer to the appropriate article for your AudioCodes model. Third-party configuration guides are stored in the Altigen Knowledge base (https://know.altigen.com).

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

  For a discussion of the options *Enable SIP REFER* and *Enable Centrex Transfer,* which are part of the Release SIP Tie-Link Trunk feature, see the section *SIP Server General Parameters*.

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

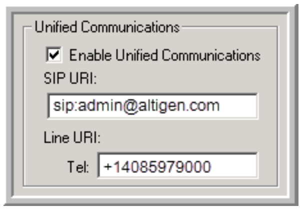
Unified Communications

You can specify whether this extension is enabled for Unified Communications (UC). Release 8.5 includes full Presence synchronization with Altigen-hosted Skype for Business. Your organization must subscribe to the Altigen-hosted Skype for Business service in the Altigen Cloud Portal to enable these features.

Refer to the separate document, *MaxCS UC Deployment Guide*, for implementation details.

To enable UC for this user,

1. Check the **Enable Unified Communications** option.
2. Enter the user's SIP URI and Line URI.



Unified Communications

☑ Enable Unified Communications

SIP URI: sip:admin@altigen.com

Line URI:

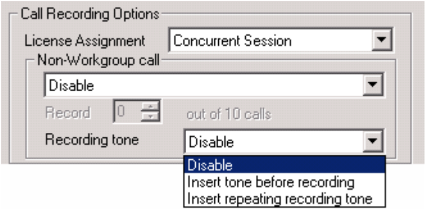
Tel: +14085979000

Figure 117. Enable Unified Communications

To forward incoming extension calls to the user's Skype for Business client, see "Enable Call Forwarding" on page 188.

Call Recording Options

The system administrator can specify the following *non-workgroup* call recording options for an agent extension.



Call Recording Options

License Assignment: Concurrent Session

Non-Workgroup call: Disable

Record 0 out of 10 calls

Recording tone: Disable

Figure 118. Call Recording options

Warning! Listening in to or recording a conversation without the consent of one or both parties may be a violation of local, state, and federal privacy laws. It is the responsibility of the users of this feature to assure they are in compliance with all applicable laws.

License Assignment

- **Concurrent Session** – When this extension is in recording state, a recording license is consumed; otherwise, a recording license is not being consumed by this extension.

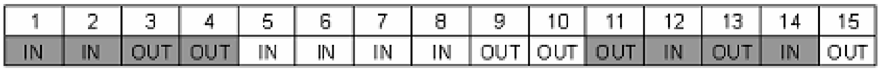
- **Dedicated Seat** – Assigns this extension a recording license for its exclusive use. The license is consumed whether or not the extension is recording.

Recording Options for Non-Workgroup Calls

- **Disable** – No recording of non-workgroup calls.
- **Auto record to central location** – Records all non-workgroup calls, which are saved to a centralized location (defined in **System > Recording Configuration** – see *Configuring Call Recording* on page 79); this option requires either a shared Concurrent Recording Session license or a Dedicated Recording Seat license to be available.
- **Record on demand to central location** – Records non-workgroup calls on demand, which are saved to a centralized location (defined in **System > Recording Configuration** – see *Configuring Call Recording* on page 79); this option requires either a shared Concurrent Recording Session license or a Dedicated Recording Seat license to be available.
- **Record on demand to extension VM** – Records non-workgroup calls on demand, which are saved to the extension's voicemail box. No license is required for this option. If the recording file size is larger than the mailbox size set for the extension, the recording file is discarded. The administrator should assign a large enough mailbox size to this extension. (The mailbox size setting is on the **Mail Management** tab.)

  Note: The recorded file will not be forwarded to e-mail as an attachment even if mail forwarding is enabled to forward voice mail to e-mail.
- **Record X out of 10 calls** – If recording to a central location, automatically records all incoming *non-workgroup* calls at a specified interval for every 10 calls. Group calls are not recorded.

  For example, if you set to record 4 out of 10 calls, the 1st-4th and 11th-14th, and so on, will be recorded. The shaded calls will be recorded in the following example:



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
IN	IN	OUT	OUT	IN	IN	IN	IN	OUT	OUT	OUT	IN	OUT	IN	OUT

Recording Tone

- **Disable** – No tone is played during a recording.
- **Insert tone before recording** – Plays one recording beep to alert the parties that the conversation is being recorded.
- **Insert repeating recording tone** – Plays a low-volume background beep every 15 seconds to alert the parties that the conversation is being recorded. The tone is recorded together with the conversation. The beep does not disrupt the conversation.

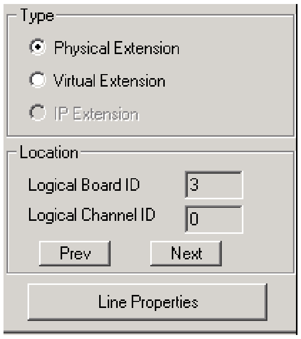
  In MaxCS systems, the repeating tone is only available if one channels in use is SIP. With two TDM channels, repeating tones will not be available.

Note:

- The recording session starts when the call enters the connected state and ends when hang up or flash is pressed, or when the call is transferred.
- Except for license assignment, the recording setting in Extension Configuration only applies to *non-workgroup* calls. The recording setting in Workgroup Configuration only applies to *workgroup* calls. To allow an agent to record all calls (*non-workgroup* and *workgroup*), both recording settings must be enabled.

Physical Location and Type

You can change the extension's type and location.



Type

● Physical Extension

○ Virtual Extension

○ IP Extension

Location

Logical Board ID: 3

Logical Channel ID: 0

Figure 119. Extension Location and Type options

- **Type**

  The type of extension—physical or virtual—is set when you create the extension. After you create the extension, the type is displayed in brackets in the **Agent/Supervisor/Extension** list on the left side of the Extension Configuration window.

  You can change a **Virtual** extension to a **Physical** one, and *vice versa*.

  If you change the type to physical, you can also set the location and configure the line as discussed in the "Setting the Line Properties" on page 173.

  For information about IP extension configuration, see "Setting Up IP Extensions" on page 197.

- **Location**
  - Assigning a location to a physical extension – When changing a virtual extension to a physical extension, the Location parameters are available. If you know which board and channel this extension is wired to, you can use the **Prev** and **Next** buttons to select the correct board and channel number for this physical extension.
  - Changing the location – To change the location of a physical extension, select the extension number in the list of extensions, then click the **Prev** or **Next** buttons to change the board and channel settings until the location you want is displayed. Like other changes, this change isn't finalized until you click **Apply**.

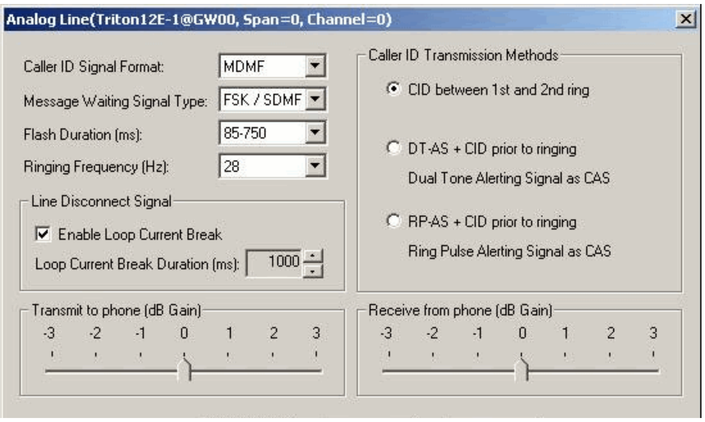
Setting the Line Properties

For a physical extension, you can configure hardware options on the port used for the extensions. To do so, select the extension number in the list of extensions, then click the **Line Properties** button to open a dialog box that is specific to the board used for the extension.

Triton Analog Station Line Properties

If you select a Triton Analog Station Board extension and click the **Line Properties** button, you'll see the Triton Analog Station Line Properties dialog box.

You can also access this window by double-clicking a span in **Channel Mapping List** of the Triton Analog Station Board configuration window.



Analog Line(Triton12E-1@GW00, Span=0, Channel=0)

Caller ID Signal Format: MDMF

Message Waiting Signal Type: FSK / SDMF

Flash Duration (ms): 85-750

Ringing Frequency (Hz): 28

Line Disconnect Signal

☑ Enable Loop Current Break

Loop Current Break Duration (ms): 1000

Caller ID Transmission Methods

● CID between 1st and 2nd ring

○ DT-AS + CID prior to ringing

Dual Tone Alerting Signal as CAS

○ RP-AS + CID prior to ringing

Ring Pulse Alerting Signal as CAS

Figure 120. Triton Analog Station Line Properties dialog box

Configure the following hardware extension-specific features:

Triton Analog Station Line Parameter	Description
Caller ID Signal Format	Message format with which to send Caller ID information: • **None** • **SDMF** – Single Data Message Format for supporting and sending a single data type, such as phone numbers. • **MDMF** – Multiple Data Message Format for supporting and sending multiple data types, such as name and number information. (Default for US/Canada installation.) • **DTMF** – Dual Tone Multi-Frequency, composed of high and low frequencies, for touch tone dialing.
Message Waiting Signal Type	Type of Message Waiting indicator for the phone set: • **None** • **FSK/SDMF** – Frequency Shift Keying/Single Data Message Format indicator. • **FSK/MDMF** – Frequency Shift Keying/Multiple Data Message Format indicator. (Default for US/Canada installation.)
Flash Duration	Specifies the Flash Duration time in milliseconds: • 85-750 (default) • 50-600 • 100-700 • 150-800 • 200-900 • 300-1000
Ringing Frequency (Hz)	Select the frequency in Hz that is necessary for the equipment attached to this line: **28** (default) or **20**.
Line Disconnect Signal	The loop current break desired for answering supervision. Range **600-1000 ms** (1000 ms is default).

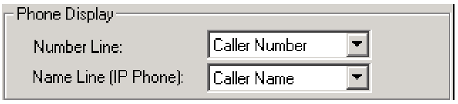
Triton Analog Station Line Parameter	Description
Caller ID Transmission Methods	Specifies how Caller ID will be detected: • CID between 1st and 2nd ring – Caller ID is received between first and second ring. (Most common in US/Canada) • DT-AS+CID prior to ringing – Dual Tone Alerting Signal Caller ID is received prior to ringing. • RP-AS+CID prior to ringing – Ring Pulse Alerting Signal Caller ID is received prior to ringing.
Receive from phone (dB Gain)	Range -3 ~ +3 db You can decrease or increase the extension phone's talk volume with this setting. Default is 0 dB.
Transmit to phone (dB Gain)	Range -3 ~ +3db You can decrease or increase the extension phone's receiving volume with this setting. The volume will be lower or higher for the extension user. Default is 0 dB.

IP Extension Configuration

See *Setting Up IP Extensions* for information on configuring this section of the Extension Configuration **General** tab.

Phone Display Options

For analog and Altigen IP phones, the administrator can select what information is to be displayed.



Number Line: Caller Number

Name Line (IP Phone): Caller Name

Figure 121. Phone Display options

Depending on the number of display lines on the LCD, the phone can be set up to show two lines of specific caller information on the display.

In the **Phone Display** field, use the **Number Line** and **Name Line** lists to select the caller information to display:

- **Caller Number**
- **Caller Name**
- **DNIS Number**
- **DNIS Name**
- **AA Data (Display)**
- **User Data (Display)**

Note: For most phones, the number line can only display a number. If the **Number Line** is set to **Caller Name**, **DNIS Name**, **User Data** or **AA Data**, the phone may display “Unknown” on the number line.

IP 600, IP 705, and IP 805 Phone Display Notes

For the IP 600, IP 705, and IP 805 models, the **Name Line** displays caller information under the following conditions:

- If **Name Line** is set to **Caller Name**, it will display caller name. If there is no name information, the number will be displayed.

- If **Name Line** is set to **Caller Number**, it will display the caller number. If there is no number information, “Unknown” will be displayed.
- If **Name Line** is set to **DNIS Name**, it will display DNIS name. If there is no name information, the DNIS number will be displayed.
- If **Name Line** is set to **DNIS Number**, it will display the DNIS number. If there is no number information, “Unknown” will be displayed.

Configuring Group Options for an Extension

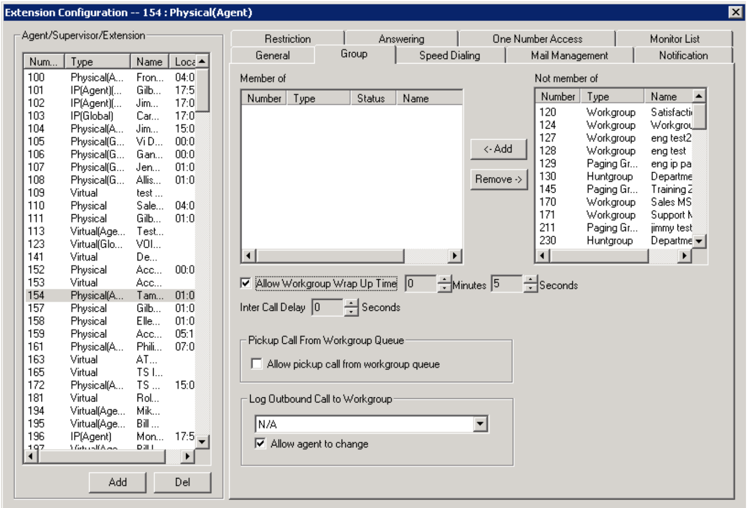
In the Extension Configuration window, **Group** tab, you can see the groups to which an extension is assigned, and you can change those assignments. Hunt groups are created in the Huntgroup Configuration window (see “Establishing Hunt Group Membership” on page 228). Workgroups are created in the Workgroup Configuration window (see “Establishing Workgroup Membership” on page 254). Group members are assigned in those configuration windows, as well.

Once a group is established, use the Extension Configuration window, **Group** tab, to configure hunt group and workgroup options for an individual agent extension, such as how much wrap-up time to allow that individual agent after a workgroup call.

You can assign an extension to and remove an extension from a group in the Extension Configuration window too. To assign an extension to a workgroup, the extension must be designated as an Agent extension. This is done on the **General** tab of Extension Configuration (check the **Agent** check box). A hunt group member does not have to be designated as an Agent.

To configure group options for an individual extension,

1. Select the extension number from the **Agent/Supervisor/Extension** list in the Extension Configuration window. The extension number and type appear in the title bar of the window.
2. Click the **Group** tab. You see a list of groups the extension is a member of and a list of groups the extension is not a member of. If the extension is an agent, both workgroups and hunt groups are shown. If the extension is not an agent, only hunt groups are shown.



Num...	Type	Name	Loca
100	Physical(A...	Fron...	04:0
101	IP(Agent)(...	Gilb...	17:5
102	IP(Agent)(...	Jim...	17:0
103	IP(Global)	Car...	17:0
104	Physical(A...	Jim...	15:0
105	Physical(G...	Vi D...	00:0
106	Physical(G...	Gan...	00:0
107	Physical(G...	Jen...	01:0
108	Physical(G...	Allis...	01:0
109	Virtual	test ...	
110	Physical	Sale...	04:0
111	Physical	Gilb...	01:0
113	Virtual(Age...	Test...	
123	Virtual(Glo...	VOI...	
141	Virtual	De...	
152	Physical	Acc...	00:0
153	Virtual	Acc...	
154	Physical(A...	Tam...	01:0
157	Physical	Gilb...	01:0
158	Physical	Elle...	01:0
159	Physical	Acc...	05:1
161	Physical(A...	Phili...	07:0
163	Virtual	AT...	
165	Virtual	TS I...	
172	Physical(A...	TS ...	15:0
181	Virtual	Rol...	
194	Virtual(Age...	Mik...	
195	Virtual(Age...	Bill ...	
196	IP(Agent)	Mon...	17:5

Member of

Number	Type	Status	Name

Not member of

Number	Type	Name
120	Workgroup	Satisfacti
124	Workgroup	Workgrou
127	Workgroup	eng test2
128	Workgroup	eng test
129	Paging Gr...	eng ip pa
130	Huntgroup	Departme
145	Paging Gr...	Training Z
170	Workgroup	Sales MS
171	Workgroup	Support N
211	Paging Gr...	jimmy test
230	Huntgroup	Departme

☑ Allow Workgroup Wrap Up Time 0 Minutes 5 Seconds

Inter Call Delay 0 Seconds

Pickup Call From Workgroup Queue

☐ Allow pickup call from workgroup queue

Log Outbound Call to Workgroup

N/A

☑ Allow agent to change

Figure 122. Extension Configuration window, Group tab

Adding or Removing Group Assignments

You can assign an extension to a hunt group in the Huntgroup Configuration window and to a workgroup in the Workgroup Configuration window. Conversely, you can assign a hunt group or a workgroup to an extension in the Extension Configuration window.

To assign a group to the selected physical or virtual extension,

1. On the **Group** tab, click the group number in the **Not Member** list.
2. Click the **Add** button to move it to the **Member** list.

   Note: If a hunt group or workgroup is configured to Ring All Available Members, the maximum number of members is 20. See “Setting Call Handling Options” on page 234 for details.

To remove a group assigned to a physical or virtual extension,

1. Click the group number in the **Member** list.
2. Click the **Remove** button. The group moves to the **Not Member** list.

Note: You can use **Shift**+click and **Ctrl**+click to select more than one group.

Setting Wrap-up Time

You can set the Wrap-up Time for the selected physical agent extension. This option doesn’t appear for a virtual extension or a non-agent extension. Wrap-up time is a system delay between the time an agent finishes a workgroup call and the time the next workgroup call is routed to the extension. It gives the agent time to finish up with notes, prepare for the next call, log out of the group, or click the “Not Ready” button in MaxAgent. You can set a wrap-up time of up to 29 minutes, 59 seconds. Note that agents will still get *direct* calls during wrap-up time.

To set the extension wrap-up time,

1. Check the **Allow Workgroup Wrap Up Time** check box.
2. Using the lists, select the minutes and seconds for the delay. Be sure to set at least enough time (for example, 5 seconds) to allow an agent to click the “Not Ready” button in MaxAgent after putting the caller on hold and going onhook.

Setting Inter Call Delay

This configuration applies only to calls waiting in queue. The Inter Call Delay can create a time delay before the next workgroup call *in queue* rings the extension after the extension finishes one of the following activities:

- Makes an internal or outbound call
- Receives a direct inbound call
- Accesses voice mail
- Parks a call
- Transfers a call

It is possible that an agent may execute one of the above activities during the wrap-up period after finishing a workgroup call. The following rules govern which delay timer will take effect:

- If Wrap-up time is still active, the Inter call delay will be ignored.
- If Wrap-up time is expired when one of the above activities is completed, the Inter Call Delay will be applied. The system will not pass a workgroup call to an agent until Inter Call Delay is expired.

To set the extension Inter Call Delay time,

1. Check the **Inter Call Delay** check box.
2. Using the lists, select the seconds for the delay.

Picking Up a Call from the Workgroup Queue

Check **Allow pickup call from workgroup queue** to allow a MaxAgent user to pick up a call from the workgroup the agent belongs to. The agent needs to be in the log-in state to be able to pick up a call from the queue.

Logging Outbound Workgroup Calls

You can assign an agent to an outgoing workgroup, which is useful for call detail reporting and workgroup statistics. All calls made by the agent while logged into the workgroup will be tracked as calls from the workgroup. The agent's outgoing workgroup can be assigned to any workgroup of which he is a member.

To set an agent's outgoing workgroup,

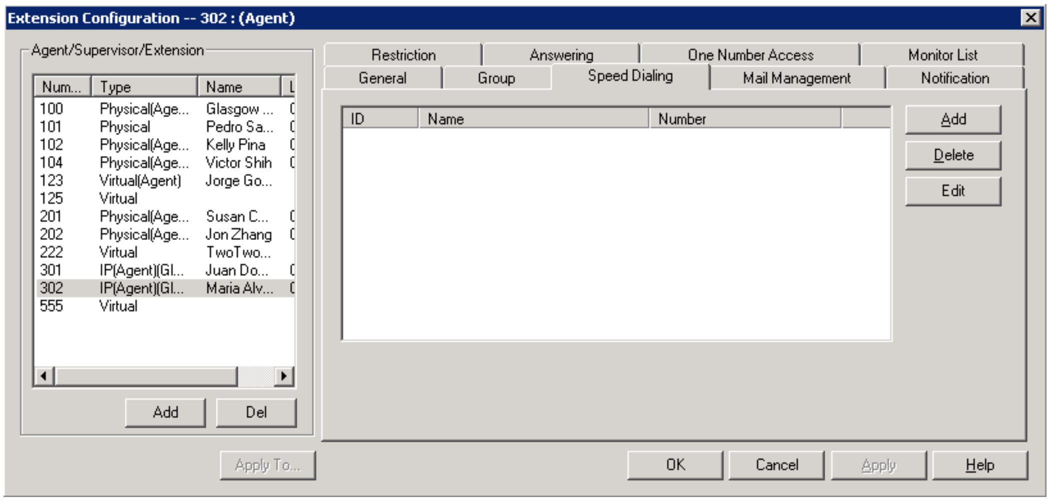
In the **Log Outbound Call to Workgroup** field, use the list to choose a workgroup from among the workgroups the agent belongs to. If the **Allow agent to change** check box is selected, the agent can change the outgoing workgroup from the phone set by using feature code #53 or from MaxAgent.

When a user is first assigned to a workgroup, it is set as their default outgoing workgroup and remains so no matter how many workgroups the user is subsequently assigned to. If an agent is unassigned from their outgoing workgroup, the outgoing workgroup is automatically set to N/A.

Setting up Station Speed Dialing

For each extension, you can set up to 20 station speed dial numbers. The numbers available are from 00–19, and are entered by the user following the extension speed dial access code, #77.

To work with Speed Dialing settings, click the **Speed Dialing** tab, then select the extension you want to set speed dialing for.



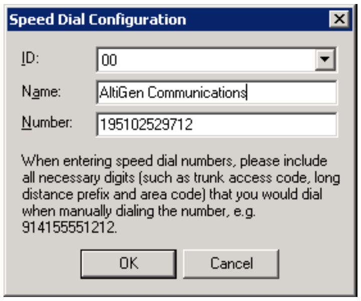
Num...	Type	Name	L
100	Physical(Age...	Glasgow ...	(
101	Physical	Pedro Sa...	(
102	Physical(Age...	Kelly Pina	(
104	Physical(Age...	Victor Shih	(
123	Virtual(Agent)	Jorge Go...	
125	Virtual		
201	Physical(Age...	Susan C...	(
202	Physical(Age...	Jon Zhang	(
222	Virtual	TwoTwo...	
301	IP(Agent)(Gl...	Juan Do...	(
302	IP(Agent)(Gl...	Maria Alv...	(
555	Virtual		

Figure 123. Extension Configuration, Speed Dialing tab

Editing Speed Dial Entries

To add or edit an entry,

1. Double-click the **Station Speed ID** number you want to work with, or select the number and click **Edit**. Or click **Add** to add an entry.



Speed Dial Configuration

ID: 00

Name: AltiGen Communications

Number: 195102529712

When entering speed dial numbers, please include all necessary digits (such as trunk access code, long distance prefix and area code) that you would dial when manually dialing the number, e.g. 914155551212.

Figure 124. Speed Dial details

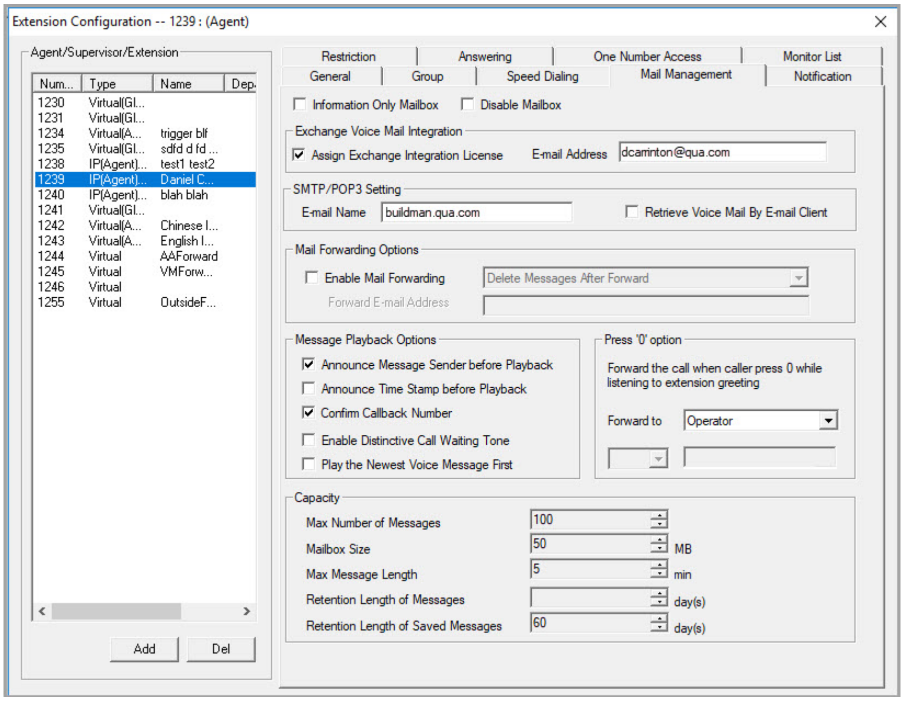
2. Select the ID number using the arrow, type in a name for the Speed Dial entry, then the full number as you would dial it, with a maximum of 20 digits per entry. For example, the phone number 914085551212 comprises **9** (trunk access code), **1** (long distance prefix), followed by **408** (area code), and finally the seven digit telephone number.

   Valid digits include **0** through **9**, **#**, *, and **(,)** comma. **The comma represents a one-second pause**.

Setting Mailbox Options

The **Mail Management** settings define how voice messages are handled for an extension: whether the mailbox is information only or is full-featured, how messages are announced and processed, and how much capacity is allotted to message storage.

To work with mailbox settings, select the extension number you want to work with from the **Agent/Supervisor/ Extension** list, then click the **Mail Management** tab.



Extension Configuration -- 1239 : (Agent)

Agent/Supervisor/Extension

Num...	Type	Name	Dep.
1230	Virtual(Gl...		
1231	Virtual(Gl...		
1234	Virtual(A...	trigger blf	
1235	Virtual(Gl...	sdfd d fd ...	
1238	IP(Agent)...	test1 test2	
1239	IP(Agent)...	Daniel C...	
1240	IP(Agent)...	blah blah	
1241	Virtual(Gl...		
1242	Virtual(A...	Chinese I...	
1243	Virtual(A...	English I...	
1244	Virtual	AAForward	
1245	Virtual	VMForw...	
1246	Virtual		
1255	Virtual	OutsideF...	

□ Information Only Mailbox □ Disable Mailbox

Exchange Voice Mail Integration

☑ Assign Exchange Integration License E-mail Address dcarrinton@qua.com

SMTP/POP3 Setting

E-mail Name buildman.qua.com □ Retrieve Voice Mail By E-mail Client

Mail Forwarding Options

□ Enable Mail Forwarding Delete Messages After Forward

Forward E-mail Address

Message Playback Options

☑ Announce Message Sender before Playback

□ Announce Time Stamp before Playback

☑ Confirm Callback Number

□ Enable Distinctive Call Waiting Tone

□ Play the Newest Voice Message First

Press '0' option

Forward the call when caller press 0 while listening to extension greeting

Forward to Operator

Capacity

Max Number of Messages 100

Mailbox Size 50 MB

Max Message Length 5 min

Retention Length of Messages day(s)

Retention Length of Saved Messages 60 day(s)

Figure 125. Extension Configuration, Mail Management tab

Setting an Information-Only Mailbox

You can check the **Information Only Mailbox** check box to set virtual or physical extension mailboxes to Information Only, then click **Apply to** to set one or more extension mailboxes.

An Information Only mailbox allows callers to listen to customized recorded announcements. To repeat the announcement, callers are instructed to press the # key. This mailbox does not take messages from the caller.

Disabling a Mailbox

When you disable a mailbox, a special greeting is played to announce that this mailbox is not accepting new messages.

Assign Exchange Integration License

Check this check box if the selected extension is to be integrated with Microsoft Exchange, and enter the email address.

SMTP/POP3 Setting

- **Email Name** – the user's e-mail name without the @domain. The default e-mail name is ext*[extension number],* that is, the letters "ext" followed by the extension number. For example, the default e-mail name for extension 2497 would be **ext2497**.
- **Retrieve Voice Mail by Email Client** – selected, this sends voice mail to the user's e-mail as an attachment.

Mail Forwarding Options

- **Enable Mail Forwarding** – selected, the user's e-mail will be forwarded to the e-mail address you specify in the **Forward Email Address** box. The address should be a full address, including the domain (for example, *jsmith@thecompany.com*).

  If you enable mail forwarding, you also specify what you want done with the original messages after they have been forwarded. In the drop down list you can choose to:

  - **Delete Messages after Forward** (if you enable this option and a voicemail forward fails, you will get an SNMP trap and the failed voicemail will be forwarded to the extension)
  - **Keep the Messages as New**
  - **Keep Messages as Saved**

Setting Message Playback Options

You can use the following check boxes to turn on or off options for listening to playback of recorded messages. These options apply to both new messages and saved messages, and they can be applied to multiple extensions using **Apply to**.

Message Playback Parameter	Description
Announce Message Sender Before Playback	Selected, the user hears the *type* of the message sender (internal or outside) before listening to recorded messages.
Announce Time Stamp Before Playback	Selected, the user hears the timestamp (time and date) of each message before playback.
Confirm Callback Number	Selected, the system reads back the caller's number and asks the caller to confirm.

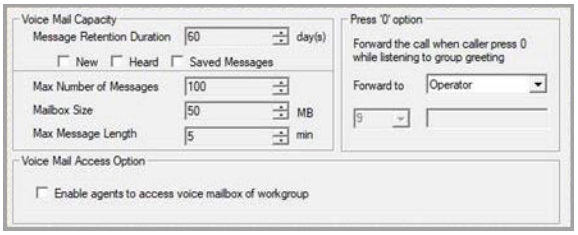
Message Playback Parameter	Description
Enable Distinctive Call Waiting Tone	Selected, the extension user will hear a "beep" tone when there is a call waiting in the extension's queue.
Play the Newest Voice Message First	Selected, new voicemail will be retrieved first. When not selected, the system will play voicemail based on first-in-first- out (FIFO).

Press Zero Option

This option allows a caller to press “0” while listening to this extension’s greeting. Use the list to select one of the following forwarding destinations for the call: **Voice Mail**, **AA**, **Extension**, **Group**, **Operator** (default), **Outside Number**, **Application Extension**, or **Line Park**. When the caller presses “0”, the call will forward to the specified destination.

Setting Mailbox Capacities

You can set various mailbox capacities with the following options.



Voice Mail Capacity

Message Retention Duration: 60 day(s)

□ New □ Heard □ Saved Messages

Max Number of Messages: 100

Mailbox Size: 50 MB

Max Message Length: 5 min

Press '0' option

Forward the call when caller press 0 while listening to group greeting

Forward to: Operator

9

Voice Mail Access Option

□ Enable agents to access voice mailbox of workgroup

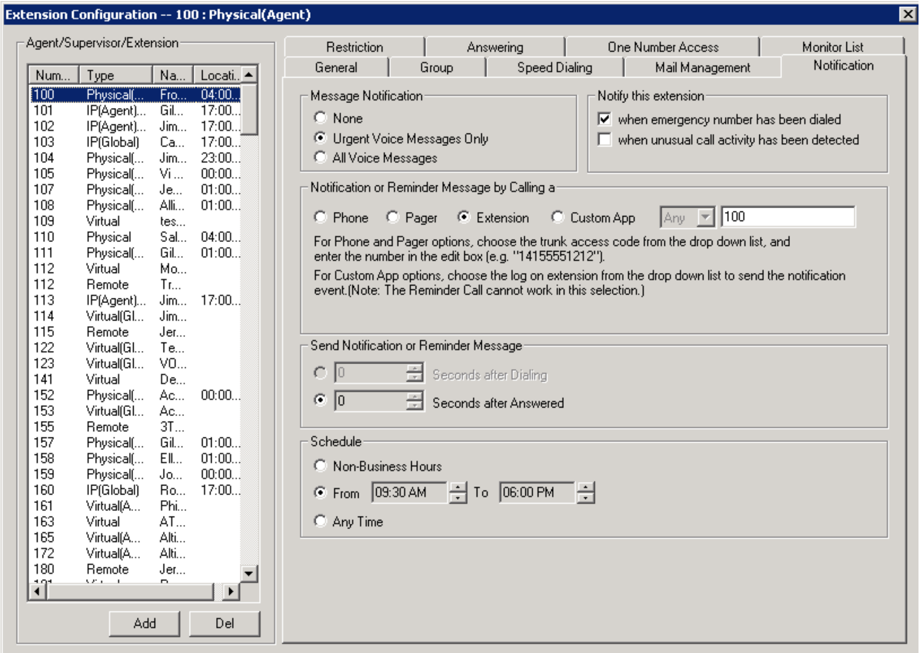
Voicemail Capacity Parameter	Description
Message Retention Duration	Set how long (in days) new, heard and/or saved voicemail messages are retained. The default duration is 60 days. By default, only the *Saved Messages* option is selected. Any message type that is **not** selected will have no duration limit. Notes: • Agents will hear notifications that old voicemail messages will be deleted when they log into their voicemail account using # # on their phones. • Agents will **not** hear these notifications when they select a message in MaxAgent and click **Play Message**.
Max Number of Messages	Maximum number of voicemail messages stored in the user’s mailbox. The range is **1**–**999**, with a default of 100. This setting works In conjunction with the *Mailbox Size* setting. When your voicemail mailbox capacity is reached, the voicemail system will announce “Your mailbox is full” and no further messages will be accepted until you delete enough messages to fall back below your set capacity.
Mailbox Size	Maximum size of voicemail mailbox, in MBs. The range is **1**–**500** MB, with a default of 50. This setting works In conjunction with the *Max Number of Messages* setting. When your voicemail mailbox capacity is reached, the voicemail system will announce “Your mailbox is full” and no further messages will be accepted until you delete enough messages to fall back below your set capacity.
Max Message Length	Maximum length of voice messages, in minutes. The range is **1**–**30** minutes, with a default of 5 minutes.

These options can be applied to multiple extensions using **Apply to**.

Setting Message Notification Options

The **Notification** tab of Extension Configuration provides for setting notification options on new incoming e-mail as well as voice messages.

To work with notification settings, select the extension number from the **Agent/Supervisor/Extension** list, then click the **Notification** tab.



Extension Configuration -- 100 : Physical(Agent)

Agent/Supervisor/Extension

Num...	Type	Na...	Locati...
100	Physical(...	Fro...	04:00...
101	IP(Agent)...	Gil...	17:00...
102	IP(Agent)...	Jim...	17:00...
103	IP(Global)	Ca...	17:00...
104	Physical(...	Jim...	23:00...
105	Physical(...	Vi ...	00:00...
107	Physical(...	Je...	01:00...
108	Physical(...	Alli...	01:00...
109	Virtual	tes...	
110	Physical	Sal...	04:00...
111	Physical(...	Gil...	01:00...
112	Virtual	Mo...	
112	Remote	Tr...	
113	IP(Agent)...	Jim...	17:00...
114	Virtual(Gl...	Jim...	
115	Remote	Jer...	
122	Virtual(Gl...	Te...	
123	Virtual(Gl...	VO...	
141	Virtual	De...	
152	Physical(...	Ac...	00:00...
153	Virtual(Gl...	Ac...	
155	Remote	3T...	
157	Physical(...	Gil...	01:00...
158	Physical(...	Ell...	01:00...
159	Physical(...	Jo...	00:00...
160	IP(Global)	Ro...	17:00...
161	Virtual(A...	Phi...	
163	Virtual	AT...	
165	Virtual(A...	Alti...	
172	Virtual(A...	Alti...	
180	Remote	Jer...	

Message Notification
○ None
● Urgent Voice Messages Only
○ All Voice Messages

Notify this extension
☑ when emergency number has been dialed
□ when unusual call activity has been detected

Notification or Reminder Message by Calling a
○ Phone ○ Pager ● Extension ○ Custom App Any 100

For Phone and Pager options, choose the trunk access code from the drop down list, and enter the number in the edit box (e.g. "14155551212").
For Custom App options, choose the log on extension from the drop down list to send the notification event.(Note: The Reminder Call cannot work in this selection.)

Send Notification or Reminder Message
○ 0 Seconds after Dialing
● 0 Seconds after Answered

Schedule
○ Non-Business Hours
● From 09:30 AM To 06:00 PM
○ Any Time

Figure 126.   Extension Configuration, Notification tab

Individual users can also configure **Message Notification** within the Altigen client applications MaxCommunicator and MaxAgent.

Note: You can use **Apply to** to apply notification settings to one, some, or all extensions. See “About the Apply To Button” on page 168 for more information on using **Apply to**.

Setting the Message Types for Notification

Select the types of messages for which the extension user is notified:

- **None** – No notification. Selecting this option does not prevent the user from getting message waiting indicators or stutter dial tone when new messages are received.
- **Urgent Voice Messages Only**
- **All Voice Messages**

The system will perform notification under the following conditions:

- Extension's message notification is set to **Urgent Voice Messages Only**.
- Extension's notification Schedule is set to **Non-Business Hours**.
- Voice mail received during business hours is marked urgent.
- Extension user does not check the urgent message.

The system will start notification as soon as it enters non-business hours.

Note: Message notification can also be set in MaxCommunicator and MaxAgent, and the settings are reflected in MaxAdministrator.

Emergency Notification

When any extension dials an emergency number, the system can make calls to specified extensions, groups, or outside numbers. To configure this option, select the extension/group/outside number, and check the **When Emergency Number Has Been Dialed** check box.

Emergency-number calls are logged to *SecurityAlert.txt* (see “Where Security Alerts Are Logged” on page 184.)

Unusual VM Activity Notification

When certain unusual activity is detected from an extension’s voice mail, the system can notify a designated extension. This option is intended to help detect if a hacker has obtained control of and is making calls from an extension’s voice mail. To alert an extension (usually the administrator) when either of the following abnormal activities are happening, select the extension and check the option **When unusual call activity has been detected**:

- When calls made from voice mail are unusually long (by default, more than 120 minutes)
- When the number of calls made from voice mail is unusually high (by default, more than 20 calls in one voice mail session)

When the designated extension is notified, the system will play “Unusual call activity has been detected from Extension xxx. More than yy calls have been made from the extension's voice mail. Please verify with the extension user.” Or “Unusual call activity has been detected from Extension xxx. The extension made more than a yyy-minute call from the extension's voice mail. Please verify with the extension user.” The security notification will be made only once within a call.

Setting Parameters for Unusual VM Activity

To change the parameters for the number of calls or length of a call, you must add the following strings and values to the Windows registry:

- *SecurityConnectionDuration* (value range is from 1-1440 minutes [24 hours]). When the setting is out of range, the default of 120 minutes will be used.
- *SecurityNumberOfCalls* (value range is from 1-100 calls). When the setting is out of range, the default of 20 calls will be used.

Adding security values to the registry

To add one or both of the above security values to the Windows registry:

1. Choose **Run** from the Windows **Start** menu, type **regedit**, and click **OK**.
2. Go to **HKEY_LOCAL_MACHINE\SOFTWARE\Altigen Communications, Inc.\AltiWare\InitInfo**.
3. On the right side of the Registry window, right-click and choose **New > DWORD Value**.
4. Type one of the security strings listed above, then double-click the entry.
5. Choose **Decimal** as the **Base** option.
6. Type the value you want (see the allowed range listed above) in the **Value data** text box, and click **OK**.
7. The value you enter appears in parentheses in the **Data** column.
8. For the values you entered in the registry to take effect, from the MaxAdministrator menu, choose **Diagnostic > Trace**. The Trace Filter dialog box opens. Click the **Minute Task** button in the dialog box. Alternatively, you could restart the system for the values to take effect.

Where Security Alerts Are Logged

Security alerts are logged to **..\AltiServ\Log\SecurityAlert.txt**. The log includes date, time, extension number, pad number, and the alert reason. Emergency calls are also logged to this file. Following are some examples:

2007-02-04 08:30:25 Extension 212 made more than 20 calls from voicemail(1:2)

2007-02-04 16:00:50 Extension 395 made more than a 120-minute call from voicemail(0:6).

2007-02-18 09:05:32 Extension 395(2:3) made an emergency call-###.

Note: A *SecurityAlert.txt* file does not appear in the **..AltiServ\Log** folder until a security alert event has created it.

Setting the Type of Notification

There are four options for sending the notification or reminder message: **Phone**, **Pager**, **Extension** or **Custom Application**.

- **Extension** – To use the Extension option, select the **Extension** radio button, then type the extension number into the text box.
- **Phone/Pager** – For the **Phone** and **Pager** options, first specify the trunk or route access code using the list next to the **Phone** radio button. The **Any** option means to locate any available trunk. Then type in the number with all relevant dialing prefixes other than the trunk code, using a maximum of 63 digits.
- **Custom App** – When used in conjunction with a third-party notification application, the **Custom App** feature enables an extension to connect to an application that can receive the notification event; use the list to choose the log-on extension to which the third-party application is connected. Contact your local Altigen Partner for more information on using this feature.

  Note: The Reminder Call will not work with this selection.

Note also the following considerations:

- For the **Pager** option, the system calls the specified pager number and then dials the system main number (as set in System Configuration, **General** tab), which is then displayed on the user's pager.

  For the operator-assisted paging function, the operator phone number **and** the pager number must be entered in the **<phone number>*<pager number>** format. For example, if the phone number to call the pager operator is **7654321** and the pager number to page the user is **12345678**, the notification outcall number that needs to be entered is **7654321*12345678**. When the pager operator answers the Message Notification call, MaxCS announces the **pager number and** the **System Main Number** (as configured on the **General** tab of **System Configuration**), which will be displayed on the user's pager. The operator is also given the option to repeat these numbers by pressing '**#**'.

Outcall to Cellular or PCS Phone Numbers

When an outcall is made by the system (for One Number Access, Message Notification, Zoomerang, Call Forwarding, and so on) to a cellular or PCS phone, it may ring the phone once but not necessarily present the call and make a connection. This will happen if the ringback tone played by the cellular service provider does not conform to standard ringback tones. To work around this problem, append a few commas (**,**) to the outcall (cellular) number when entering it. Each comma provides a one second pause.

Setting Notification Timing

When notification is configured to an *outside phone number*, the system will announce, "This is the outcall notification message for…" after call connection. However, there are situations when the system may not be able to receive an answer supervision signal from the carrier. If the system plays the announcement phrase before the notification call is answered, the phrase will be cut off. The following two options can be configured based on answer supervision capability:

- **Seconds after Dialing –** If the carrier of the outside phone number cannot provide an answer supervision signal, check this option and set a delay time. (Default 5 seconds, maximum 30 seconds.)

  Note: If the delay is set too long, the notified party will hear silence before the announcement is played.
- **Seconds after Answered –** This field is set to 0 seconds and it is not configurable for notification to a phone number. It means the system will play the announcement immediately after answer supervision is received.

When notification is configured to a *pager*, the system will transmit DTMF digits as the return phone number (the **System Main Number** as set in the System Configuration **General** tab) after call connection. However, there are situations when the system may not be able to receive an answer supervision signal from the pager system. If the system sends digits before the call is connected, some digits will be cut off. The following two options can be configured based on answer supervision capability:

- **Seconds after Dialing –** If the pager carrier cannot provide an answer supervision signal, check this option and set a delay time. (Default 5 seconds, maximum 30 seconds.)
- **Seconds after Answered –** If the answer supervision signal is provided by the carrier, check this option and set the delay timer to 2 to 5 seconds. In some cases, the pager carrier cannot detect DTMF right after the call connection. (Default is 10 seconds, maximum is 30.)

  Note: You may need to try a different delay setting to make sure the user return number is transmitted properly after configuration.

Setting Notification Business Hours

You can choose one of three options for when the extension user is to be notified of new messages:

- **Non-Business Hours** – Notify only during non-business hours. Business hours are set in System Configuration, **Business Hours** tab (see “Setting Business Hours” on page 38).
- **From/To** – Notify during a specified time of day. Select the hours in the **From** and **To** time scroll boxes.
- **Any Time** – Notify at all times (every day).

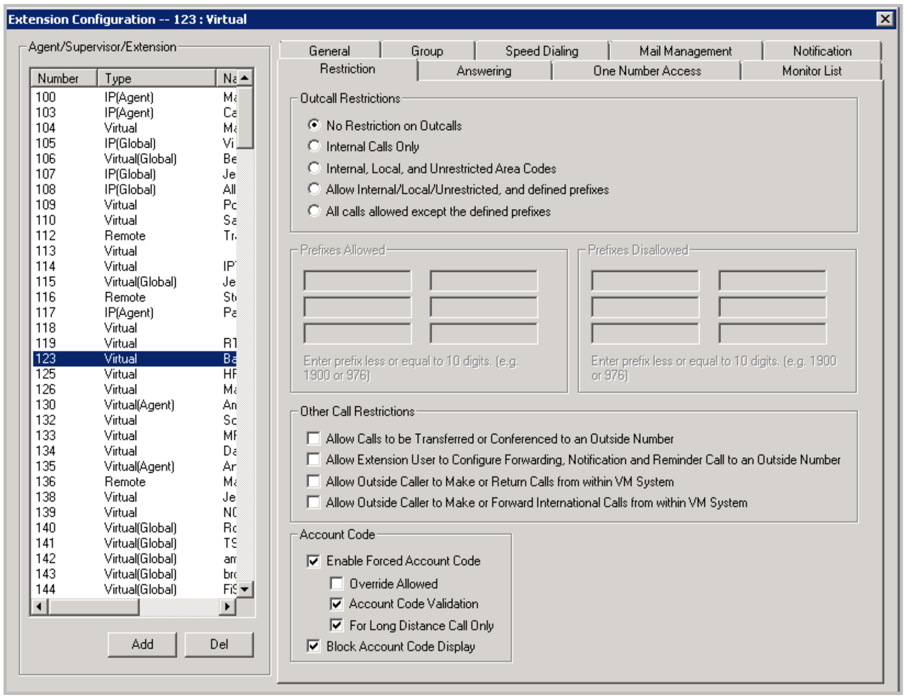
Enabling Message Notification

After configuring your message notification settings, to enable message notification, check the **Allow Extension User to Configure Forwarding, Notification and Reminder Call to an Outside Number** check box on the **Restriction** tab of Extension Configuration.

Configuring Calling Restrictions

To work with extension call restrictions, select the extension number you want to work with from the **Agent/ Supervisor/Extension** list, then click the **Restriction** tab.

Note: You can use **Apply to** to apply call restriction settings to one, some, or all extensions. See “About the Apply To Button” on page 168 for more information on using **Apply to**.



Extension Configuration -- 123 : Virtual

Agent/Supervisor/Extension

Number	Type	Na
100	IP(Agent)	Ma
103	IP(Agent)	Ca
104	Virtual	Ma
105	IP(Global)	Vi
106	Virtual(Global)	Be
107	IP(Global)	Je
108	IP(Global)	All
109	Virtual	Pc
110	Virtual	Sa
112	Remote	Tr
113	Virtual	
114	Virtual	IP
115	Virtual(Global)	Je
116	Remote	St
117	IP(Agent)	Pa
118	Virtual	
119	Virtual	R1
123	Virtual	Ba
125	Virtual	HF
126	Virtual	Ma
130	Virtual(Agent)	An
132	Virtual	Sc
133	Virtual	MF
134	Virtual	Da
135	Virtual(Agent)	Ar
136	Remote	Ma
138	Virtual	Je
139	Virtual	NC
140	Virtual(Global)	Rc
141	Virtual(Global)	TS
142	Virtual(Global)	an
143	Virtual(Global)	brc
144	Virtual(Global)	FiS

Outcall Restrictions

● No Restriction on Outcalls
○ Internal Calls Only
○ Internal, Local, and Unrestricted Area Codes
○ Allow Internal/Local/Unrestricted, and defined prefixes
○ All calls allowed except the defined prefixes

Prefixes Allowed

Enter prefix less or equal to 10 digits. (e.g. 1900 or 976)

Prefixes Disallowed

Enter prefix less or equal to 10 digits. (e.g. 1900 or 976)

Other Call Restrictions

□ Allow Calls to be Transferred or Conferenced to an Outside Number
□ Allow Extension User to Configure Forwarding, Notification and Reminder Call to an Outside Number
□ Allow Outside Caller to Make or Return Calls from within VM System
□ Allow Outside Caller to Make or Forward International Calls from within VM System

Account Code

☑ Enable Forced Account Code
□ Override Allowed
☑ Account Code Validation
☑ For Long Distance Call Only
☑ Block Account Code Display

Figure 127. Extension Configuration, Restriction tab

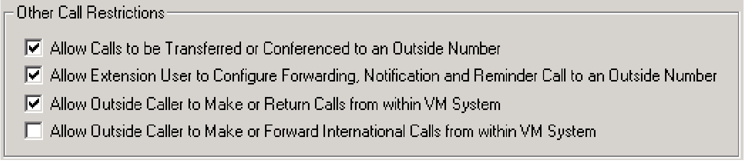
Setting Call Restriction Options

You can use one of the following options in setting restrictions on an extension or on multiple extensions using **Apply to**.

- **No Restrictions on Outcalls**
- **Internal Calls Only** – extension-to-extension.
- **Internal, Local, and Unrestricted Area Codes** – Allow extension to call internal, local, and area codes defined in the **Unrestricted Area Codes** in the **Call Restriction** tab of the System Configuration window.
- **Allow Internal/Local/Unrestricted, and Defined Prefixes** – In addition to the above privilege, allow the extension to call prefixes you specify in the **Prefixes Allowed** boxes. Include all relevant prefix numbers (for example, if appropriate, you would include 1+area code before the number). This configuration will not override **System Prohibited Prefixes** set in System Configuration.
- **All Calls Allowed Except the Defined Prefixes** – In addition to System Prohibited Prefixes, you can block this extension from dialing the numbers defined in the **Prefixes Disallowed** boxes.

Setting Other Call Restrictions

Other call restriction rules can deny or allow the following:



Other Call Restrictions

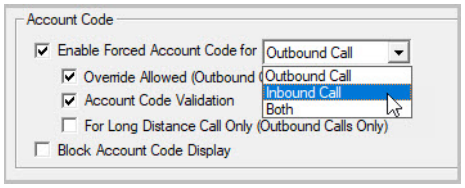
☑ Allow Calls to be Transferred or Conferenced to an Outside Number
☑ Allow Extension User to Configure Forwarding, Notification and Reminder Call to an Outside Number
☑ Allow Outside Caller to Make or Return Calls from within VM System
□ Allow Outside Caller to Make or Forward International Calls from within VM System

- **Allow Calls to be Transferred or Conferenced to an Outside Number** – when checked, the internal extension user can log into voice mail, make a call to a second party, then transfer or conference to a third party.
- **Allow Extension User to Configure Forwarding, Notification, and Reminder Call to an Outside Number** – This setting regulates extension call forwarding, voice mail notification, and reminder call configuration. If this setting is not checked, you will see a warning message pop up when trying to set up forwarding to an outside number. International calls are not allowed if the fourth option is not checked.
- **Allow Outside Caller to Make or Return Calls from within VM System** – when checked, an outside caller can dial into the system, log in to the extension's voice mail, and make or return calls from the voice mail (Zoomerang feature). International calls are not allowed if the fourth option is not checked.
- **Allow Outside Caller to Make or Forward International Calls from within VM system** – This setting regulates making international calls from voice mail and forwarding to an international number. You need to check the second and third options to be able to check this configuration.

Caution! Allowing any of these options may increase the potential for toll fraud. Make sure the password is properly configured to prevent an intruder from using this voice mail box to make an outbound call. Altigen recommends that you leave the fourth option unchecked for all extensions at all times.

Account Codes

These settings determine how callers use any account codes you have established when making outgoing trunk calls.



Account Code

☑ Enable Forced Account Code for: Outbound Call

☑ Override Allowed (Outbound (

☑ Account Code Validation

☐ For Long Distance Call Only (Outbound Calls Only)

☐ Block Account Code Display

Figure 128. Account Code options

For information on creating account/code associations, see "Creating Account Codes" on page 46.

- **Enable Forced Account Code** – Forces the user to enter an account code. You can specify whether account codes are required for inbound calls, outbound calls, or both.
  - **Override Allowed** – Prompts the user to enter an account code, or the user can press # to bypass the account code.
  - **Account Code Validation** – Forces the user to enter a valid account code.
  - **For Long Distance Call Only** – The system determines if an outgoing call starts with a long distance or international prefix. If it does, the call will require an account code.
- **Block Account Code Display** – The account code table will not be displayed when the user tries to tag the account from MaxCommunicator and MaxAgent. This prevents the user from seeing account codes they do not need to see.

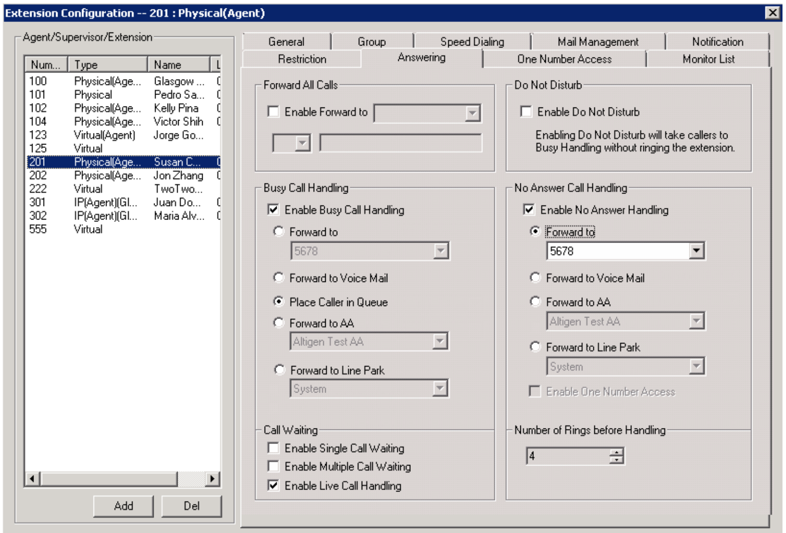
Setting Answering Options

Answering options include forwarding, handling busy calls, handling no-answers and other options. Which options are available depends on the type of extension. Virtual and physical extensions each use somewhat different answering options.

You can use **Apply to** to apply answering settings to one, some, or all extensions. See "About the Apply To Button" on page 168 for more information on using **Apply to**. However, since the available options vary with the type of extension, you can only apply the choices to the same type of extension.

For example, If you are working with the settings for a virtual extension, you can use **Apply to** to apply changes to one, some, or all virtual extensions, but not to physical extensions.

To work with extension answering options, select the extension number from the **Agent/Supervisor/ Extension** list, then click the **Answering** tab.



Extension Configuration -- 201 : Physical(Agent)

Agent/Supervisor/Extension

Num...	Type	Name	L
100	Physical(Age...	Glasgow ...	(
101	Physical	Pedro Sa...	(
102	Physical(Age...	Kelly Pina	(
104	Physical(Age...	Victor Shih	(
123	Virtual(Agent)	Jorge Go...	
125	Virtual		
201	Physical(Age...	Susan C...	(
202	Physical(Age...	Jon Zhang	(
222	Virtual	TwoTwo...	
301	IP(Agent)(Gl...	Juan Do...	(
302	IP(Agent)(Gl...	Maria Alv...	(
555	Virtual		

Forward All Calls
- ☐ Enable Forward to

Do Not Disturb
- ☐ Enable Do Not Disturb

Enabling Do Not Disturb will take callers to Busy Handling without ringing the extension.

Busy Call Handling
- ☑ Enable Busy Call Handling
- ○ Forward to: 5678
- ○ Forward to Voice Mail
- ● Place Caller in Queue
- ○ Forward to AA: Altigen Test AA
- ○ Forward to Line Park: System

No Answer Call Handling
- ☑ Enable No Answer Handling
- ● Forward to: 5678
- ○ Forward to Voice Mail
- ○ Forward to AA: Altigen Test AA
- ○ Forward to Line Park: System
- ☐ Enable One Number Access

Call Waiting
- ☐ Enable Single Call Waiting
- ☐ Enable Multiple Call Waiting
- ☑ Enable Live Call Handling

Number of Rings before Handling: 4

Figure 129. Extension Configuration, Answering tab

Forwarding All Calls

Call Forwarding is available to all types of extensions.

This is the Call Forwarding feature that is also accessible by the extension user by dialing **#36**.

One Hop Limit to Call Forwarding for a Transferred Call

There is a one hop limit to call forwarding when the call that is being passed is a transferred call. For example, extension 100 receives a transferred call and forwards this call to extension 101; extension 101 is set to forward all calls to extension 102; extension 102 receives the call but CANNOT forward this call to another extension.

10-Hop Limit to Call Forwarding for Direct Calls

For direct calls, there is a “10-hop” limit to call forwarding. For example, extension 100 forwards to extension 101, 101 forwards to 102, 102 forwards to 103, and so on, through extension 120. A call to extension 100 will be forwarded to 101, which will forward to 102, which will forward to 103, and so on, until the call has been forwarded 10 times. At this point, the call will not be forwarded again; if the last extension in the forwarding chain does not answer, the call is sent to extension 100’s voice mail.

If there is a loop condition in the forwarding chain (for example, 100 forwards to 101, 101 to 102, and 102 back to 100), the call is sent to the first destination’s voice mail.

Enable Call Forwarding

To enable call forwarding, check the **Enable Call Forward to** check box, then, using the list, indicate the forwarding destination. You can use **Apply to** to act on multiple extensions, with the restrictions discussed in the previous section. The forwarding options are as follows:

- To **Voice Mail**
- To **AA** – Select the auto attendant number to use in the list under the option.

- To an **Extension** – Select an extension from the list.
- To a **Group** – Select a group from the list.
- To the **Operator**
- To an **Outside Number** – This option is available if it is allowed in the **Other Call Restrictions** option in the **Restriction** tab, as discussed in “Setting Other Call Restrictions” on page 186. Also, see “Outcall to Cellular or PCS Phone Numbers” on page 184.

  If you choose **Outside Number**, select a trunk or route access code to use in the small list on the left, and type in the full prefix and phone number.
- To an **App Ext** – When used in conjunction with an SDK-based application.
- To **Line Park** – If configured, select a **Line Park** group (configured in “Line Park Configuration” on page 245) from the list.
- To **Free Format** – This option is available only to virtual extensions. See the section “Free Format Forwarding” on page 189.
- To **Paging Trunk** – This option is available only to virtual extensions. To use this option, you have to select a paging trunk in Trunk Configuration.
- To **UC Client** – Forwards incoming calls to the user’s Skype for Business client. It is important to understand the ramifications of this option. There are two call integration options. Before you set forwarding to the UC client, review the details and instructions in the *MaxCS UC Deployment Guide*.

Note: Forwarding calls to a pager is possible but **not recommended** since callers will only hear what is heard when calling a pager and will not know to enter a return phone number unless instructed.

Free Format Forwarding

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

MaxCS supports forwarding for SIP Trunk and SIP extensions.

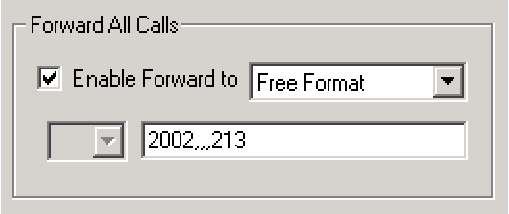
There are various uses for this virtual-forwarding feature. For example, you can configure an extension to forward fax calls to the first available fax hunt group. Another example would be to forward calls to a FaxFinder extension. You can embed several commas to add a delay before MaxCS releases the 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. Using an IP extension, APC extension, or Paging Group as a forward target is not supported. Forwarding over IP and E1 trunks is not supported.

You can embed commas to insert a delay; each comma inserts a one-second delay. For a trunk call, the wait time starts right after the digits are dialed (even while the target phone is ringing). For an extension call, the wait time starts after connecting to the extension (it does not start when ringing begins).

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 following figure.



Forward All Calls

☑ Enable Forward to: Free Format

2002,,,213

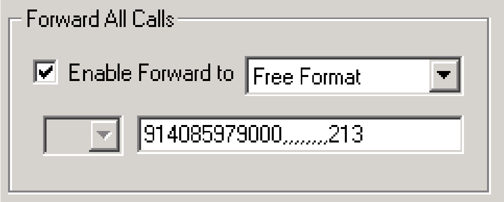
Figure 130. Example of call forwarding with a 3-second delay and DTMF digits to send

The string in the figure above indicates that the call should be forwarded to extension 2002 (for FaxFinder). The next three commas each insert 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.



Forward All Calls

☑ Enable Forward to: Free Format

914085979000,,,,,,,,213

Figure 131. Example of call forwarding to a specific extension at an external phone number

The string in the figure above indicates to forward the call to that outside phone number (our example is Altigen's corporate 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.

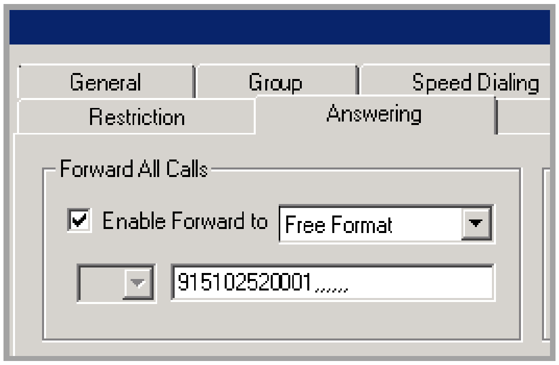
Format Guidelines

- 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 call setup time 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.



Forward All Calls

☑ Enable Forward to: Free Format

915102520001,,,,,,

Figure 132. Example of call forwarding to an outside phone number with a long delay

Do Not Disturb

Enable Do Not Disturb – Check this option to send all calls for the selected extension(s) to the extension's voice mail. This feature is also accessible by the user at the user's station by dialing **#33**. Note that this overrides any One Number Access settings for the extension. Polycom phone users can press the DND button if their extension has an Advanced Features license.

Handling Busy Calls

You have several options for handling calls while the extension is busy, and again, the options vary depending on the extension type. If you do not enable busy call handling, the caller simply hears a busy signal.

To enable the options, check the **Enable Busy Call Handling** check box, then select from the following options:

- **Forward to Extension** – Select an extension number in the drop-down list. See "10-Hop Limit to Call Forwarding for Direct Calls" on page 188.
- **Forward to Voice Mail**
- **Place Caller in Queue** – Places caller in the extension's personal queue. This option is available only if **Multiple Call Waiting** or **Live Call Handling** is turned on.
- **Forward to AA** – Select the auto attendant number to use in the list under the option.
- **Forward to Line Park** – Use the list to select a Line Park group to route the call. (See "Line Park Configuration" on page 245.)

Setting Call Waiting Options

Call waiting options are available only if the **Enable Busy Call Handling** check box has been checked.

- **Enable Single Call Waiting** – Sets up single call waiting. This feature gives an alert tone (audio beep) to indicate that a call is waiting. This feature must be enabled in order to conference incoming calls.
- **Enable Multiple Call Waiting** – Enables a "personal queue" of multiple calls waiting. This allows the user to transfer or park the current call before picking up the next call in queue.
- **Enable Live Call Handling** – This feature is mainly for the system operator. It allows callers to stay in the personal queue while the extension user is checking voice mail or operating other features. The caller will hear a ring back tone while in queue. The call will be shown as "ringing" on AltiConsole.

  Note: On a Polycom phone, the incoming call will follow the extension's RNA handling rules instead of showing as "ringing."

Handling Unanswered Calls

The **No Answer Call Handling** function provides options for handling calls when no one answers the extension within a specified number of rings.

Except for Enabling One Number Access, these options are *not available to virtual extensions*.

To enable these options, check the **Enable No Answer Handling** check box.

Use the **Number of Rings Before Handling** scroll box to select a number between 2 and 20 for the times the telephone rings before the call is handled by the system.

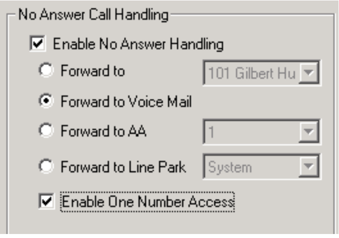
Select one of the following options for no answer call handling:

- **Forward to Extension** – Select an extension number in the drop-down list. See “10-Hop Limit to Call Forwarding for Direct Calls” on page 188.
- **Forward to Voice Mail**
- **Forward to AA** – Select the auto attendant number to use in the list under the option.
- **Forward to Line Park** – Use the list to select a Line Park group to route the call to. (See “Line Park Configuration” on page 245.)

Configuring One Number Access

One Number Access (ONA) gives the caller an option to find the extension user when the extension is ring no answer. Caller still has the option to leave a voice mail if the system is unable to find the extension user.

Note: Options on the tab are disabled unless One Number Access has been enabled as a **No Answer** option on the Answering tab of the Extension Configuration window.



No Answer Call Handling

☑ Enable No Answer Handling

○ Forward to 101 Gilbert Hu

● Forward to Voice Mail

○ Forward to AA 1

○ Forward to Line Park System

☑ Enable One Number Access

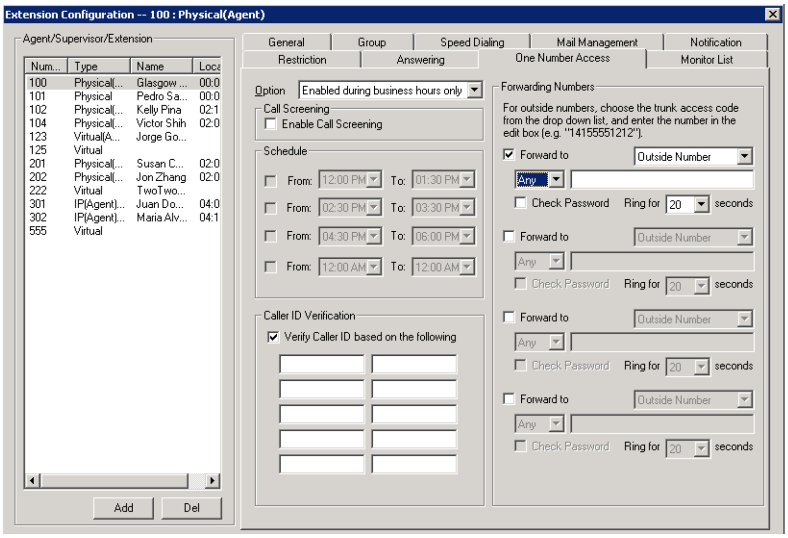
Figure 133. Enable One Number Access option on the Answering tab

This check box option is available to all extension types, but with qualifications:

- It is available to physical extensions only when the **Forward to Voice Mail** option is selected.
- It is *not* available when **Forward to AA**, **Forward to Extension**, or **Forward to Line Park** is selected.

Also, if the **Enable Do Not Disturb** option is selected in the Answering tab, the call is forwarded to voice mail regardless of ONA settings.

To configure ONA, select the extension number from the **Agent/Supervisor/Extension** list, then click the **One Number Access** tab.



Agent/Supervisor/Extension

Num...	Type	Name	Loca
100	Physical(...	Glasgow ...	00:0
101	Physical	Pedro Sa...	00:0
102	Physical(...	Kelly Pina	02:1
104	Physical(...	Victor Shih	02:0
123	Virtual(A...	Jorge Go...	
125	Virtual		
201	Physical(...	Susan C...	02:0
202	Physical(...	Jon Zhang	02:0
222	Virtual	TwoTwo...	
301	IP(Agent)...	Juan Do...	04:0
302	IP(Agent)...	Maria Alv...	04:1
555	Virtual		

Option: Enabled during business hours only

Call Screening
□ Enable Call Screening

Schedule
□ From: 12:00 PM To: 01:30 PM
□ From: 02:30 PM To: 03:30 PM
□ From: 04:30 PM To: 06:00 PM
□ From: 12:00 AM To: 12:00 AM

Caller ID Verification
☑ Verify Caller ID based on the following

Forwarding Numbers
For outside numbers, choose the trunk access code from the drop down list, and enter the number in the edit box (e.g. "14155551212").

☑ Forward to: Outside Number
Any
□ Check Password Ring for 20 seconds

□ Forward to: Outside Number
Any
□ Check Password Ring for 20 seconds

□ Forward to: Outside Number
Any
□ Check Password Ring for 20 seconds

□ Forward to: Outside Number
Any
□ Check Password Ring for 20 seconds

Figure 134. Extension Configuration, One Number Access tab

One Number Access Options

In the **One Number Access** tab, use the list to select an option for One Number Access:

- **Disabled**
- **Enabled at any time**
- **Enabled during business hours only**
- **Enabled during non-business hours**
- **Enabled based on schedule**

If you select this last option, **Enabled based on schedule**, you can then select and set up to four different time periods using the **From** and **To** time lists.

After choosing any of the enabling options, you set the **Verify Caller ID** and **Forwarding** choices, and these are discussed below.

Note: You can also enable and set up One Number Access remotely through MaxCommunicator.

Disabling One Number Access

You can disable ONA for the extension by selecting the **Disable** option. Selecting **Disable** on this tab does not destroy the data you might have entered. For example, if you entered a group of Caller IDs to use to identify the caller, these will be available if you enable one number access at a future time.

Enable Call Screening

When the **Enable Call Screening** option is checked, callers accessing One Number Access will be prompted to record a name in order to continue the ONA process. The recorded name is played after the callee (ONA target) answers the call and optionally enters a correct password. The callee will then hear the caller's name and can decide whether or not to accept the call.

Setting Caller ID Verification

You can check the **Verify Caller ID based on the following** check box and then type in up to 10 phone numbers in the text boxes. Whenever the system detects a call from one of the numbers entered here during the selected schedule, the system searches for you by dialing the numbers configured in the Forwarding Number fields.

Caution! If ONA is enabled and no numbers are entered for Caller ID Verification, ONA is available to all callers.

Caller ID verification entries should be complete phone numbers.

Using a Password Verification

You can also enter a random “password” number such as “5555” so that any caller who knows this password can use ONA to find you, regardless of where they are calling from. Once you’ve set this up, you need to instruct the caller to dial 1 during your personal greeting, then enter the “password” to use ONA.

Specifying Forwarding Numbers

The **Forwarding Numbers** are used by the system to find the user when ONA is active. You can set up to four different numbers. When ONA is active, the system dials the forwarding number(s) in the order they are displayed on the **One Number Access** tab. The Forwarding Number order does *not* correspond to the Schedule order.

You can forward to another extension, or to an outside number. You can use an outside number *only if* the extension is set to allow for **Transferred/Conferenced/Forwarded** calls on the an Extension Configuration **Restriction** tab under **Other Call Restrictions**.

When you use the outside number option, select a trunk or route access code in the list and type in the phone number as it would be dialed after keying the access code.

Check the **Check Password** option to force users to enter their extension password when a call is forwarded to them via ONA. This ensures that only the owner of the extension can answer the call.

You can set the **ONA ring duration** from 5 to 45 seconds using the **Ring for** ... **seconds** list. Default value is 20 seconds. The system will ring the ONA target within the specified time limit. If the ONA call is not answered within the ring duration, the system will terminate the ONA call. This option will prevent a cell phone voice mail from answering the ONA call and recording the ONA announcement phrase into the cell phone voice mail box.

Setting Up Monitor Lists

The **Monitor List** tab provides for setting up lists of extensions for which call processing events can be monitored by the extension user. Once a monitor list is established, the application logging into the extension can receive call events for the monitored extensions. The monitor list is available in the MaxCommunicator and MaxAgent Monitor windows, AltiConsole, and in Line Monitoring events in Altigen SDK.

Warning! Listening in to or recording a conversation without the consent of one or both parties may be a violation of local, state, and federal privacy laws. It is the responsibility of the users of this feature to assure they are in compliance with all applicable laws.

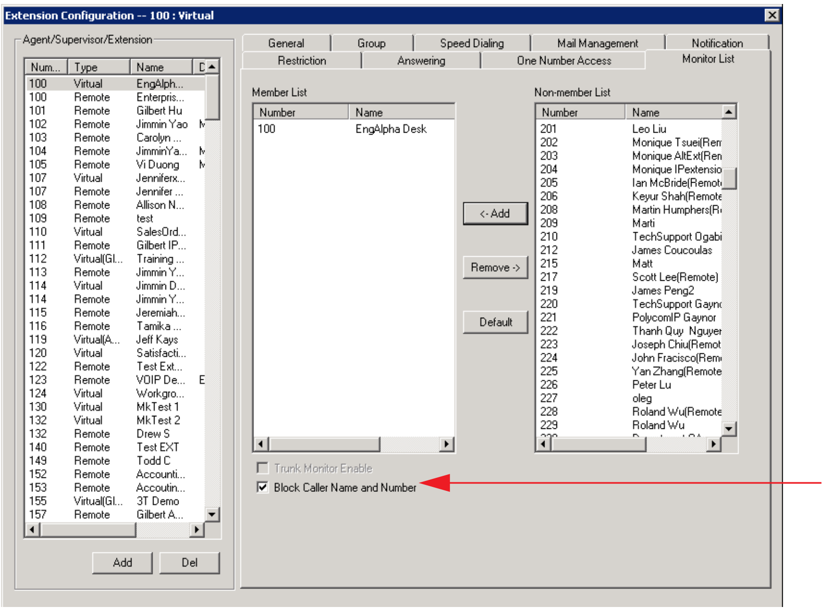
Restrictions and Defaults

- Monitoring is effective for *physical* and *virtual* extensions; physical and virtual extensions have monitoring rights, and can be monitored. If you place a physical or virtual extension in a Monitor List, that extension will show in the client application’s Monitor window.

- If you add an extension (1001, for example) that belongs to Workgroup A to the Monitor List for a member of Workgroup B, the Workgroup B member will only be able to pick up *personal* calls to 1001, not workgroup calls.
- In MaxSupervisor, the user can monitor only the workgroup(s) he or she logs in to, regardless of the monitoring rights assigned to his or her extension in MaxAdministrator.

Configuring a Monitor List

To set up a monitor list, select the extension number to receive the monitoring rights from the **Agent/ Supervisor/Extension** list, then click the **Monitor List** tab.


Extension Configuration -- 100 : Virtual

Agent/Supervisor/Extension

Num...	Type	Name	D
100	Virtual	EngAlph...	
100	Remote	Enterpris...	
101	Remote	Gilbert Hu	
102	Remote	Jimmin Yao	M
103	Remote	Carolyn ...	
104	Remote	JimminYa...	M
105	Remote	Vi Duong	M
107	Virtual	Jenniferx...	
107	Remote	Jennifer ...	
108	Remote	Allison N...	
109	Remote	test	
110	Virtual	SalesOrd...	
111	Remote	Gilbert IP...	
112	Virtual(Gl...	Training ...	
113	Remote	Jimmin Y...	
114	Virtual	Jimmin D...	
114	Remote	Jimmin Y...	
115	Remote	Jeremiah...	
116	Remote	Tamika ...	
119	Virtual(A...	Jeff Kays	
120	Virtual	Satisfacti...	
122	Remote	Test Ext...	
123	Remote	VOIP De...	E
124	Virtual	Workgro...	
130	Virtual	MkTest 1	
132	Virtual	MkTest 2	
132	Remote	Drew S	
140	Remote	Test EXT	
149	Remote	Todd C	
152	Remote	Accounti...	
153	Remote	Accoutin...	
155	Virtual(Gl...	3T Demo	
157	Remote	Gilbert A...	

Member List

Number	Name
100	EngAlpha Desk

Non-member List

Number	Name
201	Leo Liu
202	Monique Tsuei(Rem
203	Monique AltExt(Ren
204	Monique IPextensio
205	Ian McBride(Remot
206	Keyur Shah(Remote
208	Martin Humphers(R
209	Marti
210	TechSupport Ogabi
212	James Coucoulas
215	Matt
217	Scott Lee(Remote)
219	James Peng2
220	TechSupport Gaync
221	PolycomIP Gaynor
222	Thanh Quy Nguyer
223	Joseph Chiu(Remot
224	John Fracisco(Rem
225	Yan Zhang(Remote
226	Peter Lu
227	oleg
228	Roland Wu(Remote
229	Roland Wu

□ Trunk Monitor Enable

☑ Block Caller Name and Number

To block the extension from seeing caller names and numbers, check this box

Figure 135. Extension Configuration, Monitor List tab

To block the extension from seeing any Caller Name and Number details on the Monitor tab of MaxAgent and MaxCommunicator, check the **Block Caller Name and Number** box.

To add members to the list,

1. From the **Monitor Available** list, select the extensions to add to the extension user's MaxCommunicator Change Monitor window.
2. Click **Add** to move the extensions to the **Monitor List**.

To remove members,

1. Select the extensions in the **Monitor List** and click **Remove.**

Check the **Trunk Monitor Enable** check box to allow monitoring of the AltiLink Plus trunk events at the selected extension.

Click the **Default** button to return the settings to the default – the extension can monitor its own calls.

About Viewing Remote Extension Activity

In order for agents in MaxAgent and MaxCommunicator to see the activity for remote extensions on the Directory tab, those agents must add the remote extensions to their Monitoring lists.

If they do not add the remote extensions to their Monitoring list, they will still see the remote extensions, but they will not see any activity for them.

CHAPTER

17

Setting Up IP Extensions

IP phones communicate with the system using SIP protocol to establish the signaling channel and media channel (the voice steam, using RTP protocol). With SIP implementation, the system establishes a signaling channel to an IP phone when the IP phone is in use.

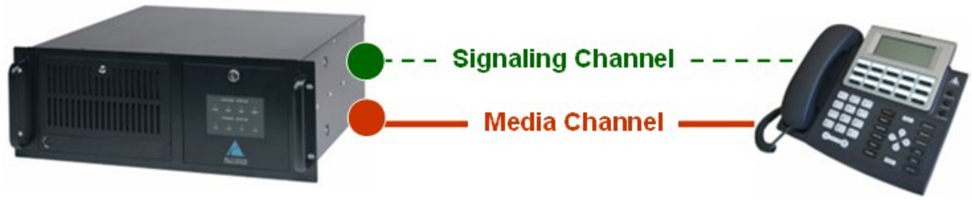


Figure 136. Concept of signaling and media channels

The media channel (voice stream) is connected between two IP phones under normal operation. There are some special situations that require you to configure the IP phone to connect its voice stream to the server. Please see “Setting an IP Extension” on page 201 for information.

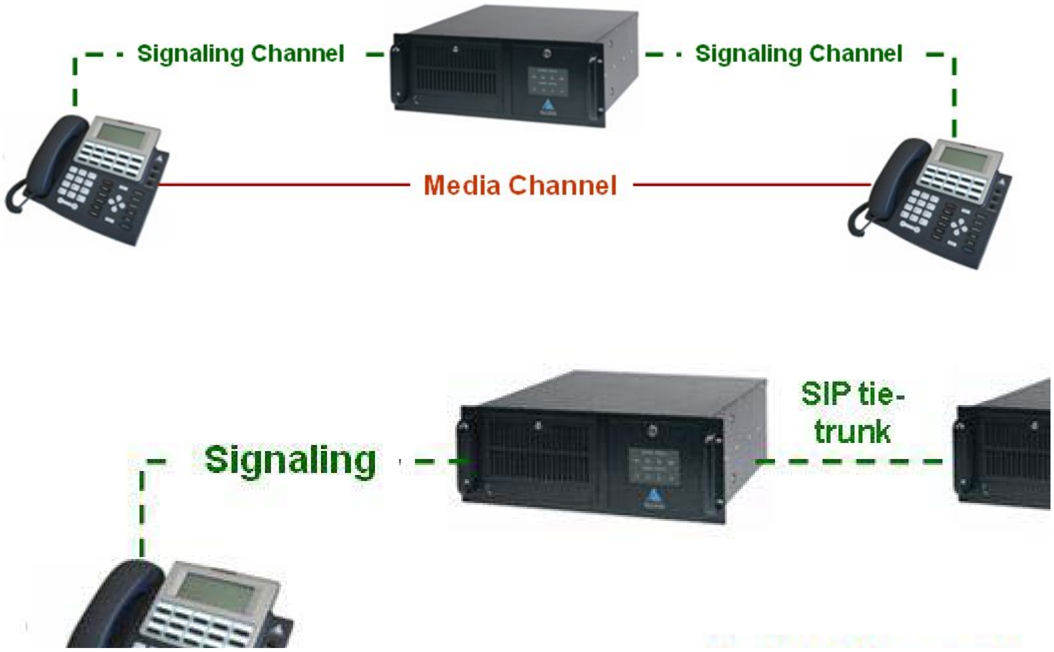


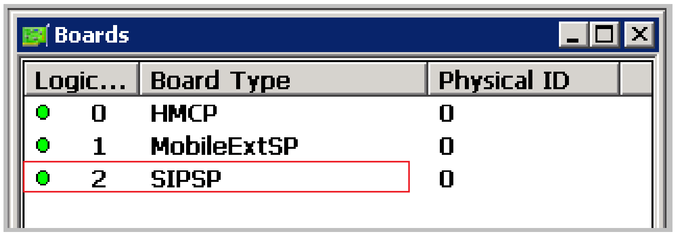
Figure 137. Signaling and media channel between two IP phones

Signaling Channels

A SIP signaling channel communicates between the system and the IP phone to perform call control, including call setup, tear down, registration, and phone feature access.

The signaling channel implementation consists of the following elements:

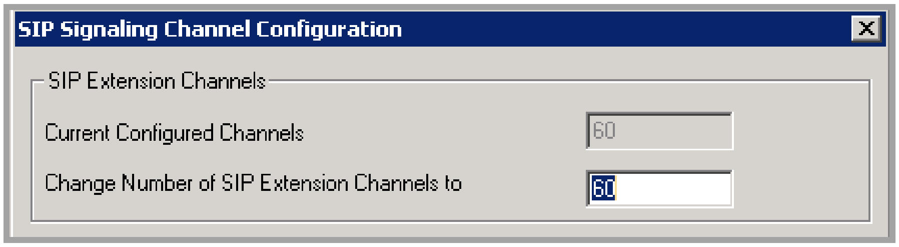
- **SIP Virtual Board** – Establishes a logical board ID relationship with other types of physical boards in the system (displayed on Board View window as SIPSP board).



Boards

Logic...	Board Type	Physical ID
● 0	HMCP	0
● 1	MobileExtSP	0
● 2	SIPSP	0

- **SIP Signaling Channel** – Creates SIP signaling channels for IP Extensions (access through SIPSP board, Channel Group configuration).



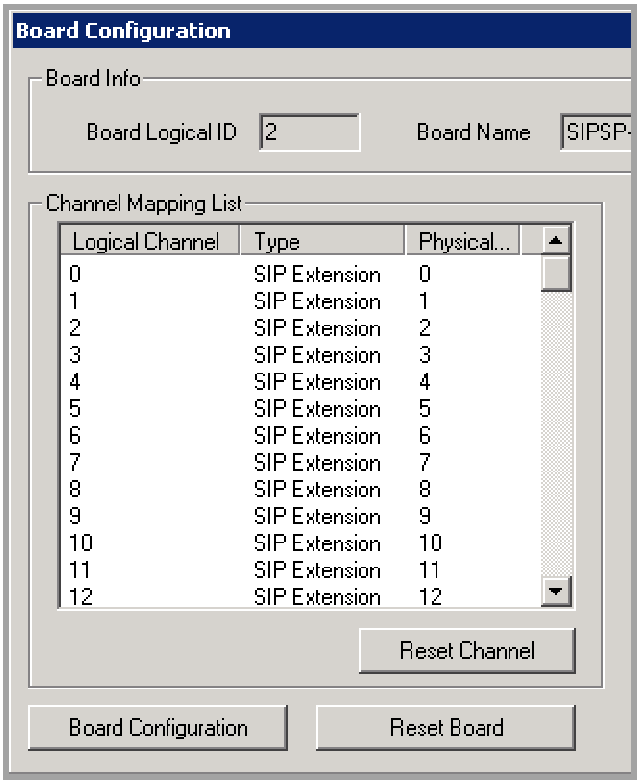
SIP Signaling Channel Configuration

SIP Extension Channels

Current Configured Channels: 60

Change Number of SIP Extension Channels to: 60

- **SIP Extension Channel** – Establishes a logical channel relationship with other analog and MobileExt ports (displayed on the SIPSP board configuration, Channel Mapping List).



Board Configuration

Board Info

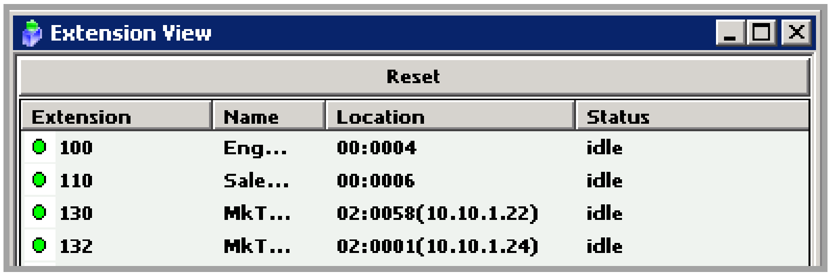
Board Logical ID: 2

Board Name: SIPSP-

Channel Mapping List

Logical Channel	Type	Physical...
0	SIP Extension	0
1	SIP Extension	1
2	SIP Extension	2
3	SIP Extension	3
4	SIP Extension	4
5	SIP Extension	5
6	SIP Extension	6
7	SIP Extension	7
8	SIP Extension	8
9	SIP Extension	9
10	SIP Extension	10
11	SIP Extension	11
12	SIP Extension	12

- **SIP Extension Channel Activation** – Associates an extension with a SIP Extension channel when IP phones register to the system (displayed in the Extension View window).



Extension View

Extension	Name	Location	Status
● 100	Eng...	00:0004	idle
● 110	Sale...	00:0006	idle
● 130	MkT...	02:0058(10.10.1.22)	idle
● 132	MkT...	02:0001(10.10.1.24)	idle

Media Channels

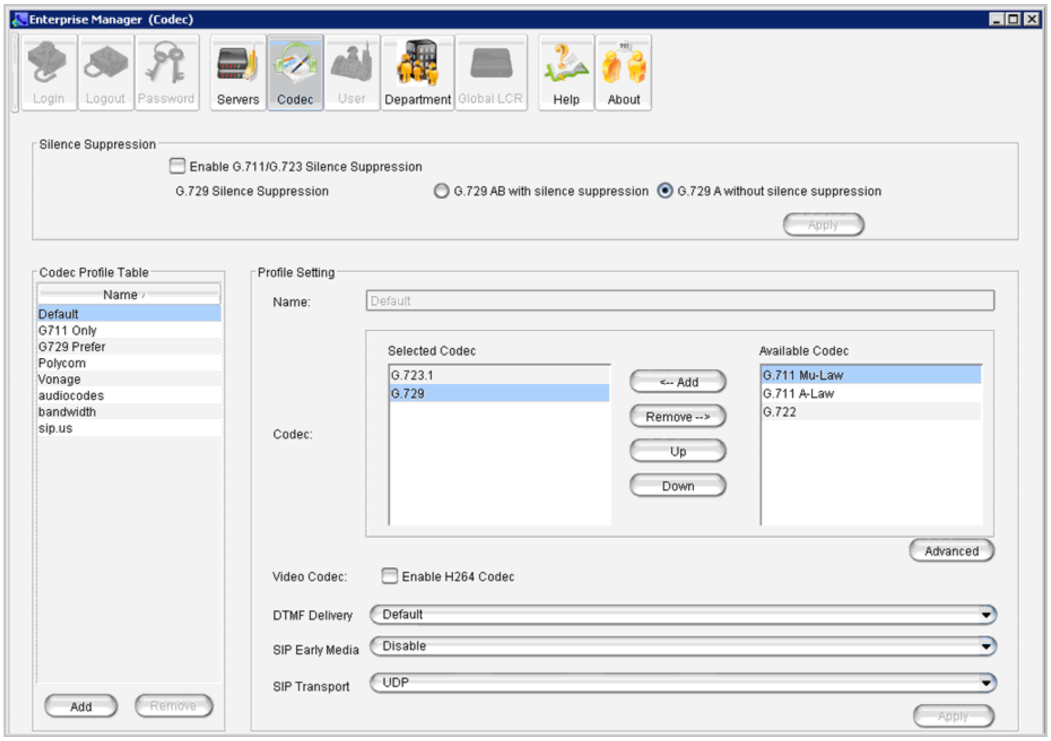
A media channel is an RTP channel that connects system-to-phone, or phone-to-phone, system-to-system to carry the digitized voice stream. The codec resource on the VoIP board will be allocated dynamically based on connection types. If both end devices are IP phones, the media channel can be connected from IP phone to IP phone using the IP phone’s codec, except when the following is true:

- SIP trunk is used
- Codecs at two end devices are mismatched
- Extension has **Agent** setting checked
- Voice recording is enabled at the IP extension

- A NAT router exists between MaxCS and remote IP phone
- SIP supports a direct connection of the voice stream between IP phones.

The media channel implementation consists of the following elements:

- **Configure Codec Profile** – Creating a profile for each codec type, jitter buffer, packet length, DTMF tone delivery, and ring back tone treatment (SIP Early Media).



Silence Suppression

☐ Enable G.711/G.723 Silence Suppression

G.729 Silence Suppression ○ G.729 AB with silence suppression ● G.729 A without silence suppression

Codec Profile Table

Name
Default
G711 Only
G729 Prefer
Polycom
Vonage
audiocodes
bandwidth
sip.us

Profile Setting

Name: Default

Codec:

Selected Codec	Available Codec
G.723.1	G.711 Mu-Law
G.729	G.711 A-Law
	G.722

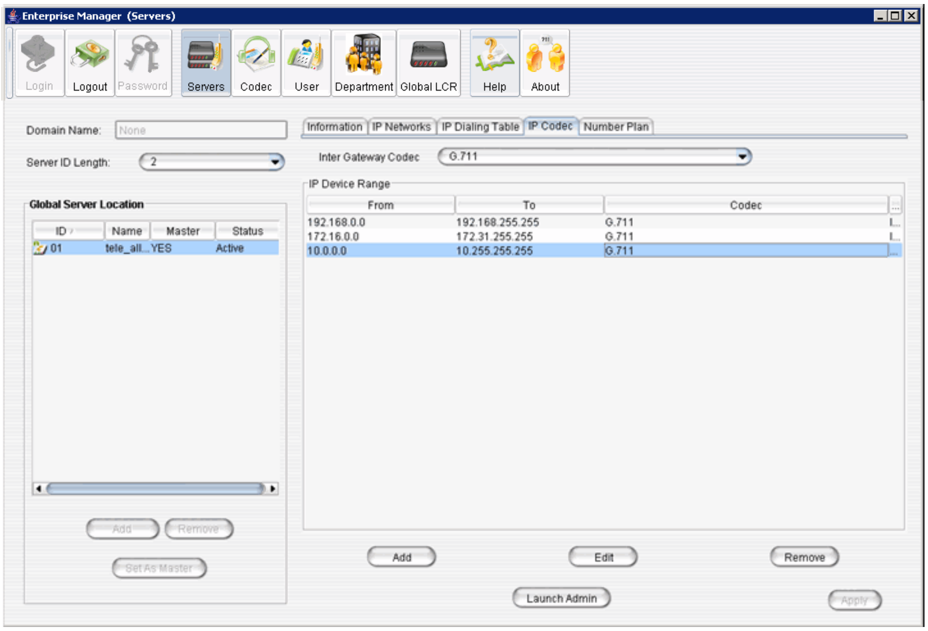
Video Codec: ☐ Enable H264 Codec

DTMF Delivery: Default

SIP Early Media: Disable

SIP Transport: UDP

- **Assign Codec to Device** – Configuring codec profile to a single IP address or a range of IP addresses.



Domain Name: None

Server ID Length: 2

Inter Gateway Codec: G.711

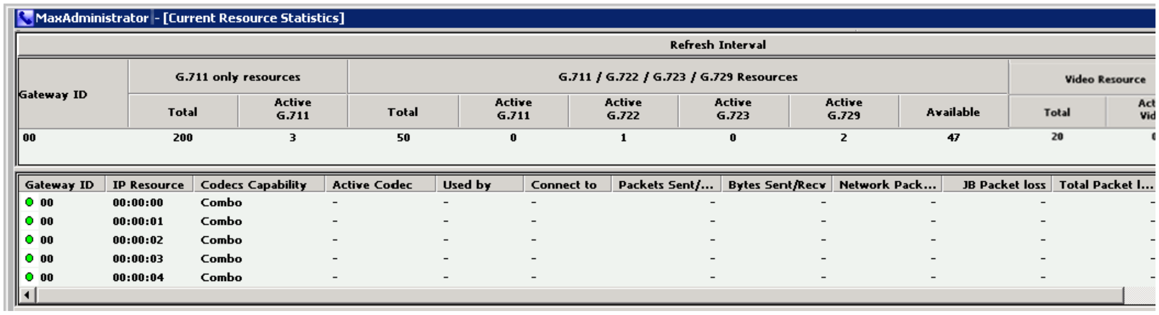
Global Server Location

ID	Name	Master	Status
01	tele_all...	YES	Active

IP Device Range

From	To	Codec
192.168.0.0	192.168.255.255	G.711
172.16.0.0	172.31.255.255	G.711
10.0.0.0	10.255.255.255	G.711

- **Monitor Codec Usage** – Viewing codec usage status.



Gateway ID	G.711 only resources		G.711 / G.722 / G.723 / G.729 Resources						Video Resource	
	Total	Active G.711	Total	Active G.711	Active G.722	Active G.723	Active G.729	Available	Total	Act Vid
00	200	3	50	0	1	0	2	47	20	0

Gateway ID	IP Resource	Codecs Capability	Active Codec	Used by	Connect to	Packets Sent/...	Bytes Sent/Recv	Network Pack...	JB Packet loss	Total Packet l...
● 00	00:00:00	Combo	-	-	-	-	-	-	-	-
● 00	00:00:01	Combo	-	-	-	-	-	-	-	-
● 00	00:00:02	Combo	-	-	-	-	-	-	-	-
● 00	00:00:03	Combo	-	-	-	-	-	-	-	-
● 00	00:00:04	Combo	-	-	-	-	-	-	-	-

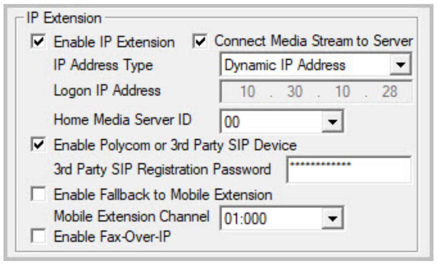
Setting an IP Extension

To make an extension an IP extension:

1. In the Extension Configuration **General** tab, select the extension from the list at the left and check the **Enable IP Extension** check box.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

2. Select the address type.



IP Extension

☑ Enable IP Extension ☑ Connect Media Stream to Server

IP Address Type: Dynamic IP Address

Logon IP Address: 10 . 30 . 10 . 28

Home Media Server ID: 00

☑ Enable Polycom or 3rd Party SIP Device

3rd Party SIP Registration Password: ************

☐ Enable Fallback to Mobile Extension

Mobile Extension Channel: 01:000

☐ Enable Fax-Over-IP

Figure 138. IP Extension options

- **Dynamic IP Address** – The system will associate the IP address to the extension when the IP phone registers automatically, or when the user logs on using **#27**+**Enter** from the Altigen IP phone. This is the recommended setting.
- **IP Address Type** – Static or Dynamic. Enter the IP address for each IP extension. This setting is recommended only when connecting to third-party SIP devices such as a Multi-Tech MVP VoIP gateway with FXS ports support. (Refer to the *MultiTech Gateway Application Note* on the Altigen web site.)

3. Configure the rest of the IP Extension panel:
   - **Connect Media Stream to Server** – The IP phone will always connect the media channel to the server when this box is checked. This box is checked by the system in the following situations:
     - The non-workgroup call recording option is checked for this extension.
     - This IP extension is a workgroup agent and the workgroup recording is checked.
     - You allow a workgroup supervisor to barge-in, listen to, coach, or record this agent's conversation.
   - **Home Media Server ID** – This configuration is meaningful for a gateway Softswitch system. When multiple chassis are configured to be a single system, you need to assign IP extensions to the configuration’s Home Media Server to be able to use its resources for activities such as the following:
     - Access voice mail
     - Initiate a conference call
     - Record a conversation
     - Barge in, listen, and coach by workgroup supervisor

     Guidelines:

     - If the Softswitch and HMCP Media Server are in the same server, the default ID “00” will be the **Home Media Server ID**. No change is required.
     - If the HMCP Media Server and Softswitch server are separated, you need to assign IP extensions to the **HMCP Media Server ID**.
     - If you have two or more HMCP Media Servers, you need to assign each IP extension to one of them, based on resource usage.
   - **Enable Polycom or 3rd Party SIP Device** – If the extension is a Polycom phone or another SIP device, check this box. You must have a license for each 3rd party SIP device.
   - **3rd Party SIP Registration Password** – Polycom phones and other standard SIP 3rd-party IP phones require a SIP Registration password to register the phone to the MaxCS server. The password should be the same as the password that is configured in the Polycom IP phone configuration file. This password is used only for phone registration purposes.

     Note: For Polycom phones, several password fields in earlier releases of MaxCS have been consolidated; refer to the *MaxCS Polycom Configuration Guide* for details.

- **Enable Fallback to Mobile Extension** – When this option is checked, and the IP phone loses its network connection, it will automatically fall back to a Mobile Extension. The mobile extension channel must be specified from the list. This feature is only available for an IP Extension with a dynamic IP address.

  Note: Polycom phones support the fallback feature.

  Losing network connection can happen in the following cases:

  – The user presses **#26** to log out from the Altigen IP phone

  – The server loses connectivity to the IP phone

  – The IP Extension's channel is taken over by another extension

  – The user exits from an IP Talk session

  Users may need to re-register when a phone falls back to a Mobile extension.

  Once associated with a fallback mobile extension, when the network connectivity is restored, the fallback mobile extension stays active, and the user must re-register the phone (#27) to reconnect to the server. For Polycom phones, #17 can be used to re-register the phone.

- **Enable Fax-Over-IP** – Enables the FoIP capability for this extension. Refer to *Fax-over-IP Configuration*.

Setting VoIP Codec for IP Extension

The system has a pre-configured IP range and codec settings to assist IP phone deployment.

In Enterprise Manager, click the **Codec** button. In the **Codec** list, three codec profiles are pre-configured:

- G.711 Mu-Law
- G.729
- G.723.1

In Enterprise Manager, click **Servers** > **IP Codecs** tab. Three local IP address ranges are pre-configured to use the G.711 codec profile:

- 192.168.0.0 ~ 192.168.255.255
- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255

When an IP phone registers to an IP extension, the system will check the IP address to determine which codec to use for the IP phone.

Also see *HMCP Codec Preference* on page 113 for a discussion of the Codec Preference feature.

For Local IP Phone Deployment

If your local IP address is not in the pre-configured range, you need to add the local IP address range into the IP Codec setting. Otherwise the system will use the **Default** (Prefer G.723.1 support G.729) setting for your IP extensions.

For Remote IP Phone Deployment

If you do not enter the remote IP phone's IP address into the IP Codec table, the system will use the **Default** (Prefer G.723.1 support G.729) setting. You can change the Default to **Prefer G.729 support G.723.1**, if desired.

To set up the VoIP codec and define IP address ranges, see *Setting VoIP Codec Profiles* on page 315 and *Assigning Codec Profiles to IP Addresses* on page 321.

Setting Fax-Over-IP for an IP Extension

MaxCSsupports T.38 Pass-through on systems using Altigen SIP trunks.

T.38 is a standard protocol for real-time fax transmission over IP networks. T.38 Pass-through relays two T.38 sessions between the SIP trunk and MaxCS and MaxCS gateway.

- T.38 pass-through is supported only on Softswitch and MaxCS Cloud
- T.38 pass-through is supported **only** on systems using Altigen SIP trunks

For FoIP configuration instructions, see *Fax-over-IP Configuration*.

CHAPTER

18

IP Phone Configuration

This chapter discusses both Altigen IP phones and Polycom IP phones. For instructions on configuring Polycom IP phones, refer to the *MaxCS Polycom Configuration Guide*.

The system administrator can control and program the following areas for each type of Altigen IP phone (some settings apply to Polycom phones as well; refer to each specific section for details):

- Specify the server IP address that the IP phone needs to register
- Protect the IP phone configuration with a password
- Prevent the user from changing the configuration from the IP phone
- Configure the Trunk Access (Route Access) code
- Configure the time zone and time format
- Specify the TFTP server for firmware updates
- Force the IP phone to reset and download new firmware
- Set SIP transport settings for SIP security
- Enable SIP telephony service for a selected third-party SIP device
- Configure programmable keys
- Allow the IP phone to receive workgroup real time status
- Allow the phone to auto-discover the server's IP address

Environments with both Polycom and Altigen IP Phones

If your environment includes both Polycom IP phones and Altigen IP phones, be aware that while Polycom phones support the G.722 codec, Altigen IP phone models IP-705, IP-710, and IP-720 models do not support that codec. (Altigen's IP-805 model does support G.722.)

Remote sites running Polycom and Altigen IP phones can coexist even with only one public IP address, as long as you configure one codec profile with the following settings:

- DTMF must be set to RFC 2833.
- You must configure a list of codecs that include at least one of the following: G.711, G.723 or G.729. You cannot configure G.722 as the only codec. You can include G.722 in the list, as long as you have at least one of those other codecs in the list as well.

Configuring the Altigen IP Phone

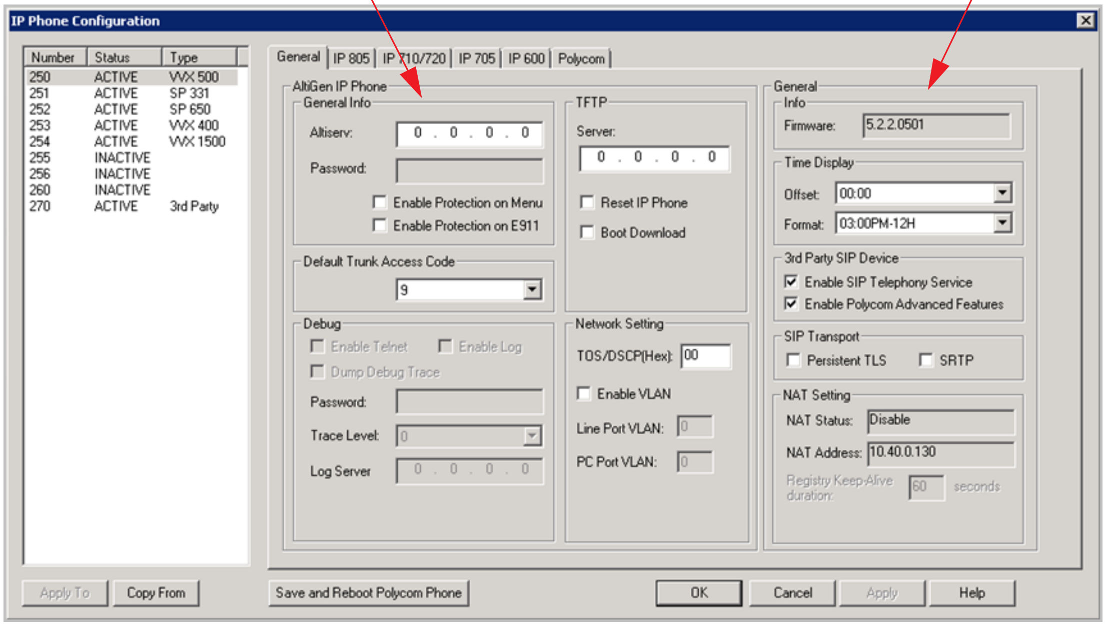
Note: You will need to upgrade the firmware on the Altigen IP phones to the latest release, so that the phones will work with MaxCS.

To configure the Altigen IP phone, select **PBX** > **Altigen IP Phone Configuration**.

This opens the IP Phone Configuration window, where, after setting up an IP extension, you can set parameters for the extension.

This panel applies only to Altigen IP phones

This panel applies to both Altigen and Polycom IP phones



Number	Status	Type
250	ACTIVE	VVX 500
251	ACTIVE	SP 331
252	ACTIVE	SP 650
253	ACTIVE	VVX 400
254	ACTIVE	VVX 1500
255	INACTIVE	
256	INACTIVE	
260	INACTIVE	
270	ACTIVE	3rd Party

Altiserv: 0 . 0 . 0 . 0
Password:
□ Enable Protection on Menu
□ Enable Protection on E911
Server: 0 . 0 . 0 . 0
□ Reset IP Phone
□ Boot Download
Firmware: 5.2.2.0501
Offset: 00:00
Format: 03:00PM-12H
☑ Enable SIP Telephony Service
☑ Enable Polycom Advanced Features
Default Trunk Access Code: 9
□ Enable Telnet □ Enable Log
□ Dump Debug Trace
Password:
Trace Level: 0
Log Server: 0 . 0 . 0 . 0
TOS/DSCP(Hex): 00
□ Enable VLAN
Line Port VLAN: 0
PC Port VLAN: 0
□ Persistent TLS □ SRTP
NAT Status: Disable
NAT Address: 10.40.0.130
Registry Keep-Alive duration: 60 seconds

Figure 139.   IP Phone Configuration General tab

The left side of the IP Phone Configuration window displays all the IP phone extensions that have been set up in the system. The status "Inactive" means the **Enable IP Extension** box is checked for this extension in the Extension Configuration window, but there is no IP phone logged in to the extension. The extension may be a physical extension using an analog phone, a MobileExt, or a virtual extension.

After creating the IP extensions, you can set the parameters on the **General** tab.

Note: The **Apply To** button works with the following parameters: **General Info**, **TFTP** (excluding Reset IP Phone), **Debug, Network Settings**, **Time display**, **3rd party SIP Device**, **SIP Transport**, **NAT setting** (Registry keep alive duration).

Altigen IP Phone Parameters

The fields in the left part of the window apply only to Altigen IP phones.

Altigen IP Phone Parameter	Description
General Info	Lets you specify the IP address of the MaxCS system the IP phone is connected to. Also see *Configuring Auto-Discovery of Server IP Address* on page 211. The version of firmware associated with the IP phone is automatically displayed in the **Version** field. To protect the configuration on the IP phone, check the **Enable Protection on Menu** check box and assign a numerical password. When the user presses the **Menu** button on the IP phone to access the phone configuration menu, the user will need to enter the assigned password. You can use this check box for two purposes: • If you publish the configuration password to the user, only the phone user would be able to change the phone configuration. • If you do not publish the configuration password, you can block the phone user from changing the phone configuration. To protect only the E911 Location ID assigned to this phone, check the **Enable Protection on E911** checkbox and enter the password that the user must type on the device in order the change the E911 configuration. See the chapter *Location-Based E911* on page 295 for instructions on configuration E911 for IP phones.
Default Trunk Access Code	Lets you set the digit required to enable a user to return an outside call from the Call Log. The default trunk access code can be the route access code, if it is set in MaxAdministrator.
Debug	This is for debugging the IP phone using Telnet. You must enter a Diagnostic password when logging in to MaxAdministrator (before you enter your Admin password) to enable this configuration.
TFTP	Lets you assign the TFTP server to which the IP phone can connect for updating firmware when necessary. Enter the IP address of the TFTP server in the **Server** field. To reset the phone and download the latest firmware image, check the **Reset IP Phone** and **Boot Download** check boxes. If you only check the **Boot Download** box, the firmware will be downloaded when the IP phone reboots (power cycles) next time. **Note:** Make sure the TFTP server is running and the new firmware image is loaded to the correct directory before you reset and download firmware.
Network Setting	• **TOS/DSCP (Hex)** – Type of Service. 8 bits in the IP header are reserved for the service type. They can be divided into 5 subfields: The 3 precedence bits have a value from 0 to 7 and are used to indicate the importance of a datagram. Default is 0 (higher is better). Bits 3 4 5 represent the following: D: requests low delay T: requests high throughput R: requests high reliability • **Enable VLAN** – If your network administrator has configured VLAN, check this check box to enable VLAN for the selected phone. Then enter the VLAN ID for the line port (voice service) and the VLAN ID for the PC port (data service). (Get these IDs from your network administrator.) See “Virtual LANs” on page 303 for information on VLANs.

General IP Phone Parameters

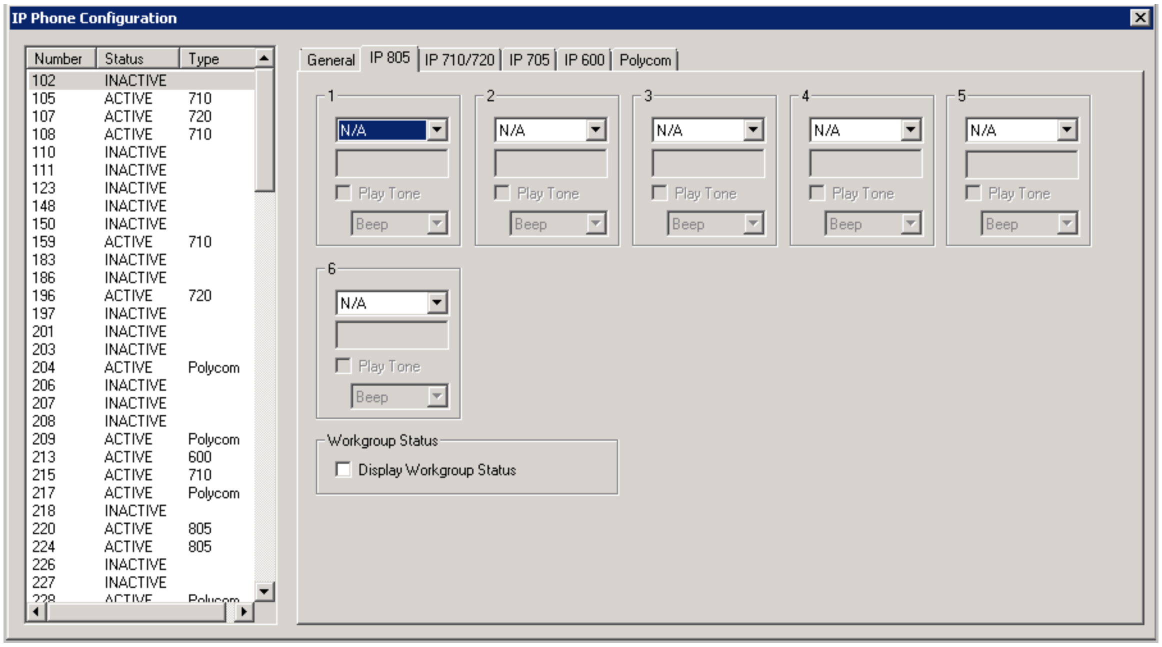
The fields in the right part of the window apply to both Altigen IP phones and to Polycom IP phones.

General IP Phone Parameter	Description
Firmware	• Shows the current version of firmware that is loaded on the phone. This field is read-only.
Time Display	• **Offset** — A per phone-based configuration that allows a remote Altigen or Polycom IP phone to display a different time, based on location. The offset is the time difference, in hours, between the Altigen system and the IP phone. • **Format** — A per-phone-based configuration that allows the Altigen or Polycom IP phone to display the time in one of the following formats: 24 hour (example: *13:15*), 12 hour AM/PM (example: *1:15 PM*), or (on Altigen IP phones) AM/PM 12 hour (example: *PM 1:15*)
3rd Party SIP Device	• **Enable SIP Telephony Service** – Enables SIP hold, SIP transfer, and SIP server-side conference features for the selected 3rd party IP phone extension. If the IP phone is SIP-enabled, the Flash key (which includes the **Hold** button in MaxAgent/MaxCommunicator) is *not supported* when you check this setting. • **Enable Polycom Advanced Features** – Enables additional features for various models of Polycom phones. Refer to the *MaxCS Polycom Configuration Guide* for full details. This parameter must be enabled for Polycom phones.

General IP Phone Parameter	Description
SIP Transport	These settings secure the SIP signaling messages and the RTP. SIP signaling is secured using transport layer security (TLS). RTP or SIP-associated media is secured using the secure RTP (SRTP) protocol. • **Persistent TLS** – Check this setting to have the selected extension communicate using TLS. The TLS protocol allows applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications privacy for VoIP systems using cryptography. If either side initiates SIP messaging with an alternate transport like UDP or TCP, these are supported, as well. • **SRTP** – Check this setting to have the selected extension use SRTP. SRTP is a version of RTP that provides confidentiality and message authentication. Since the SRTP session key is sent in the SIP signaling via SDP, the key can be exposed to eavesdropping. So SRTP needs to co-exist with TLS for the communication to be fully secure. Changing the TLS/SRTP parameter settings for a Polycom phone will require rebooting the phone; otherwise the phone may not register with MaxCS. **IP Phone Configuration vs Enterprise Manager configuration:** SIP calls from one Altigen server to another go through a SIP Tie Trunk. Configuring TLS for this scenario is done in Enterprise Manager. See the section *Setting VoIP Codec Profiles*. Extension level policy has priority over the codec profile policy. If the IP extension supports TLS and the codec profile set in Enterprise Manager does not, then the IP extension policy holds. That way you can configure a range of IP addresses in the IP Dialing table or IP Codec screen, and have only a few IP addresses/extensions support TLS. If the IP extension does not have TLS configured as its transport, but the codec profile supports TLS for that extension, then the codec profile policy holds.
NAT Setting	This setting is for a remote IP phone with a private address and behind NAT. When connecting to the Altigen system, the system will use this information to execute the NAT traversal for the IP phone. The NAT status and address are read-only fields. • **NAT Status** — Indicates if the IP phone is behind a NAT router. Read only. • **NAT Address** – This is the NAT router's public IP address, as set in the Extension Configuration window. Read only. **Registry Keep-Alive Duration** — Indicates how often a SIP registration message is sent to the server when the IP phone is behind a NAT router. You need to enter a Diagnostic password when logging in to MaxAdministrator (before you enter your Admin password) to enable this configuration. Default setting is 60 seconds.

Configuring Programmable Keys and Workgroup Status

After setting parameters on the **General** tab, go to the tab that corresponds to the phone type, and configure the programmable keys (plus the **Display Workgroup Status** field on the Alti-IP 600, IP 705, and IP 805 phones). Programmable key settings are described in the next table.



Number	Status	Type
102	INACTIVE	
105	ACTIVE	710
107	ACTIVE	720
108	ACTIVE	710
110	INACTIVE	
111	INACTIVE	
123	INACTIVE	
148	INACTIVE	
150	INACTIVE	
159	ACTIVE	710
183	INACTIVE	
186	INACTIVE	
196	ACTIVE	720
197	INACTIVE	
201	INACTIVE	
203	INACTIVE	
204	ACTIVE	Polycom
206	INACTIVE	
207	INACTIVE	
208	INACTIVE	
209	ACTIVE	Polycom
213	ACTIVE	600
215	ACTIVE	710
217	ACTIVE	Polycom
218	INACTIVE	
220	ACTIVE	805
224	ACTIVE	805
226	INACTIVE	
227	INACTIVE	
228	ACTIVE	Polycom

1
N/A
□ Play Tone
Beep

2
N/A
□ Play Tone
Beep

3
N/A
□ Play Tone
Beep

4
N/A
□ Play Tone
Beep

5
N/A
□ Play Tone
Beep

6
N/A
□ Play Tone
Beep

Workgroup Status
□ Display Workgroup Status

Figure 140. IP Phone Configuration window, IP 805 tab

Note: The **Copy From** button allows you to copy Programmable Key settings from one IP phone extension to another. No other settings are carried over.

Parameter	Description
Programmable Keys	Use the list to assign one of the following functions to the desired keys: • **N/A** — When selected, the corresponding programmable key cannot be used. • **BLF** (Busy Lamp Field) — When selected, enter an extension number in the field below; this will be associated with the corresponding programmable key to this extension number; the light in this programmable key indicates that the extension number is busy or ringing. You can select the **Play Beep Tone** check box to also have the IP phone play an audible beep or one of several different ring tones when the extension number is ringing. **Note**: The **BLF** feature can be assigned only to *internal* extension numbers, not outside numbers. See the *MaxCS Polycom Configuration Guide* for details on configuring BLF keys for Polycom phones.

Parameter	Description
Programmable Keys	• **Feature Code** — When selected, enter a MaxCS feature code in the field below; this will be associated with the corresponding programmable key to dial this feature code. • **Admin Defined #** – When selected, this programmable key can be configured by the administrator only. Enter a valid number 0~9, *, #, or F (Flash) in the field below. One use for this can be to tag a call with an account code by pressing one button. For example, entering F#321 in programmable key 1 will cause a connected call to be tagged with account code 1 (F is for Flash, #32 is the extension feature code, and in this example, 1 is the account code). Account codes are set up in System Configuration, Account Code tab. • **EXT Speed Dial** • **Line Park** – When selected, enter the Line Park line ID in the field below. The user can press this programmable key to park a call or to retrieve a parked call. See the *MaxCS Polycom Configuration Guide* for details on configuring Line Park softkeys for Polycom phones. • **Call Record** – When selected, the user can press this programmable key to start conversation call recording. This only works for extensions with **Record on Demand** selected in the Extension Configuration window. • **WG Status** – (IP710 only) When selected, the user can press this programmable key to see the real-time workgroup status (callers in queue, longest queue time, number of callers who have waited longer than the service threshold, and service level). • **User Defined #** – (Default) Allows the user to define the programmable key from the IP phone. • **Headset** – (Alti-IP 600, IP 705) When configured from the list for programmable key 10 (Alti-IP 600) or programmable key 5 (IP 705), the IP phone user will be able to activate a third-party headset (certified by Altigen). • **Flash** – (Alti-IP 600) Upon initial installation, the lower left programmable key is set up as FLASH by default. This key can be re-assigned in MaxAdministrator, using the Altigen IP Phone Configuration window. No other programmable keys can be configured to FLASH.
Display Workgroup Status	(Alti-IP 600, IP 705, IP 805) When enabled, allows the IP phone to display workgroup queue status, such as number of queued calls, the current longest queue time, agent login/logout state by pressing the Down arrow key. This feature is not supported on Polycom phones.

Important: The configuration in MaxAdministrator will override the IP phone's local configuration after the IP phone is registered. If the IP phone's local configuration is changed while in Basic mode, these changes will be overwritten by MaxAdministrator settings.

Administrators should perform any updates to the IP phone's firmware **after** normal business hours or when the IP phone is not in use. If the IP phone is in use during an update, not only will the call will be disconnected, but *if the IP phone is powered off by the user during the firmware upgrade, the IP phone may become unusable*.

Configuring Auto-Discovery of Server IP Address

You can configure option 120, in your DHCP server with your MaxCS IP address, so that the Altigen IP phone automatically discovers the MaxCS server IP address and only needs to have the extension and password entered.

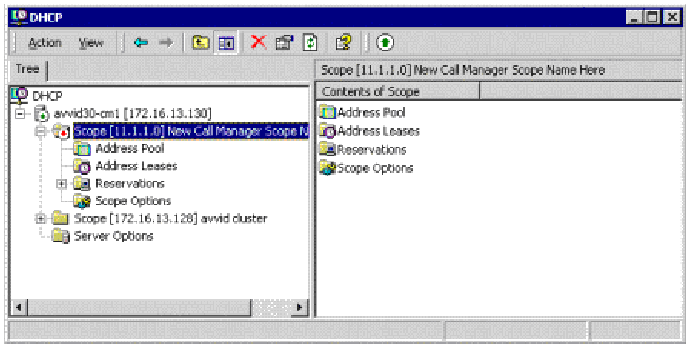
In addition to making initial IP phone setup easier, this feature is also helpful when there is a need to migrate MaxCS to a new IP address. The administrator just needs to update the new MaxCS IP address in the DHCP server and then reboot all Altigen IP phones. The phones will automatically pick up the new MaxCS IP address.

Warning! In the event that there are two MaxCS servers in a same network and all IP phones get their IP address from a single DHCP server, some IP phones will get the wrong server IP address. You need to disable the auto-discovery feature for those IP phones that log on to the MaxCS server that is not configured in the DHCP option 120.

Setting Up DHCP Option 120

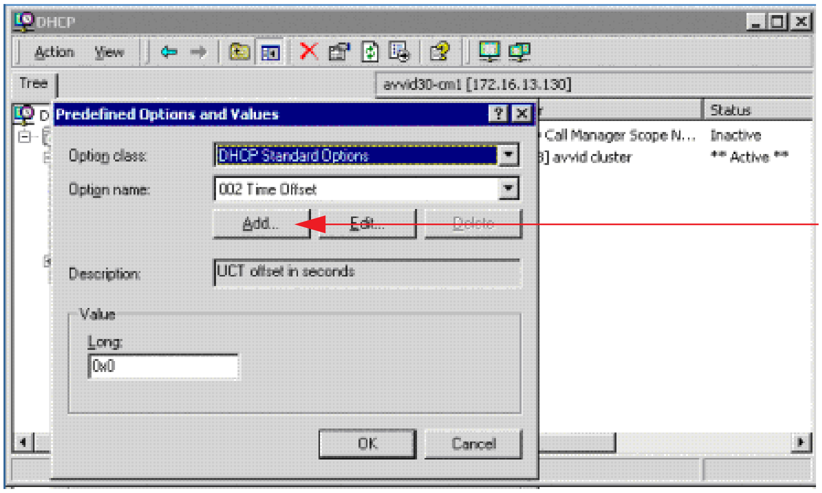
Different DHCP servers have different ways to set up options. The following example uses Microsoft Windows DHCP Server to define option 120. Since option 120 is not available by default, you must create it.

1. Open the DHCP configuration window.



Right-click the server and select Set Predefined Options

2. Right-click the server and select **Set Predefined Options**.



Option class: DHCP Standard Options

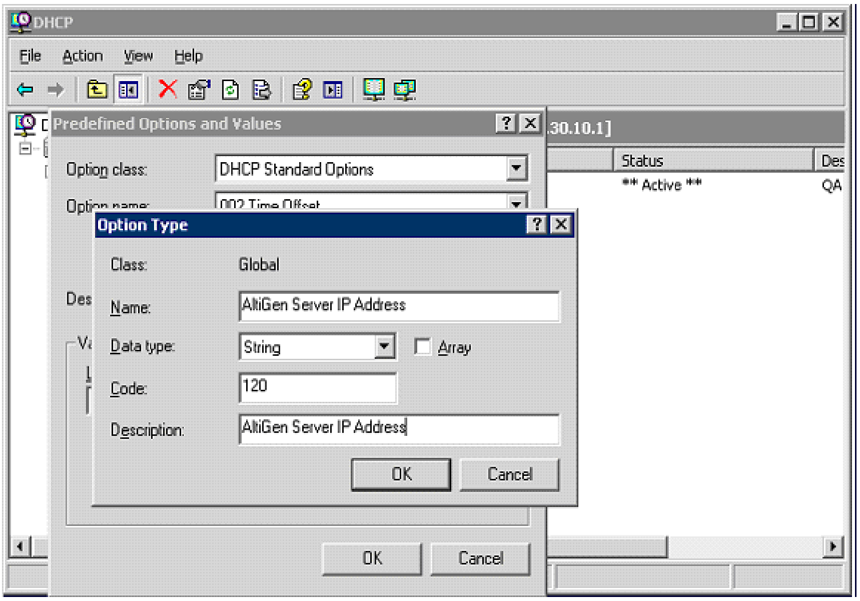
Option name: 002 Time Offset

Description: UCT offset in seconds

Long: 0x0

Click **Add**

3. Click the **Add** button.



Option class: DHCP Standard Options

Option name: 002 Time Offset

Class: Global

Name: AltiGen Server IP Address

Data type: String ☐ Array

Code: 120

Description: AltiGen Server IP Address

4. Enter the following:

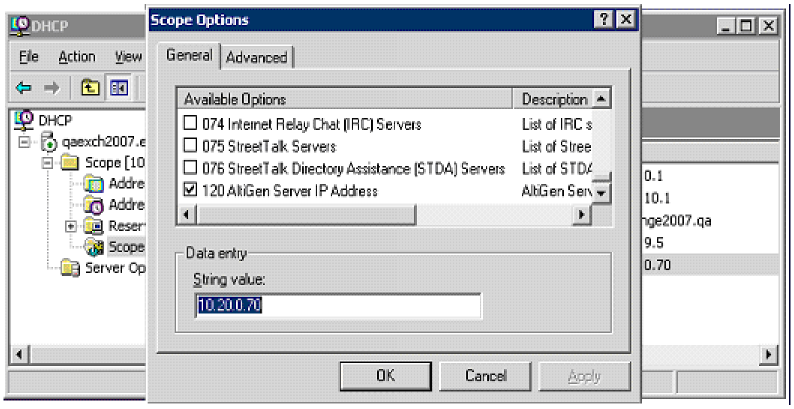
   Name: Altigen Server IP Address

   Data Type: String

   Code: 120

   Description: Altigen Server IP Address

5. Click **OK** twice.
6. Under the DHCP scope you created is a field labeled **Scope Options**. Right-click **Scope Options** and select **Configure Options**.



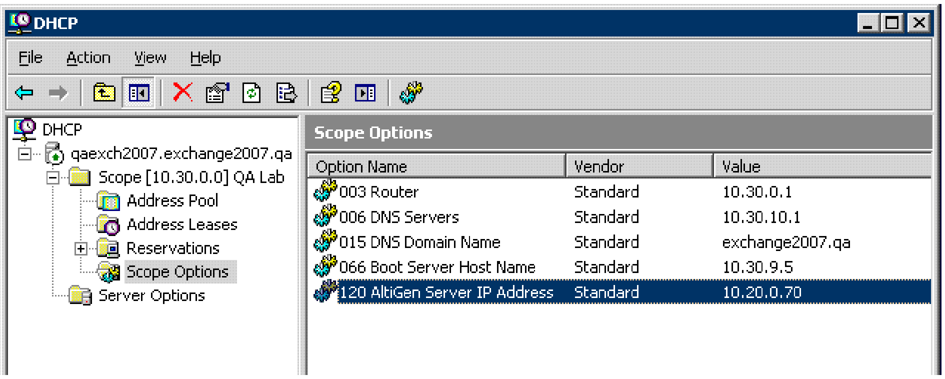
Available Options	Description
☐ 074 Internet Relay Chat (IRC) Servers	List of IRC s
☐ 075 StreetTalk Servers	List of Stree
☐ 076 StreetTalk Directory Assistance (STDA) Servers	List of STDA
☑ 120 AltiGen Server IP Address	AltiGen Serv

Data entry

String value: 10.20.0.70

Check option 120 and enter the IP address of your MaxCS server in the **String value** field

7. Check option 120.
8. Enter the IP address of your MaxCS server in the **String value** field.
9. Click **Apply** and **OK**. The scope now shows option 120.



Option Name	Vendor	Value
003 Router	Standard	10.30.0.1
006 DNS Servers	Standard	10.30.10.1
015 DNS Domain Name	Standard	exchange2007.qa
066 Boot Server Host Name	Standard	10.30.9.5
120 AltiGen Server IP Address	Standard	10.20.0.70

10. Right-click the scope option 120 and select **Activate** to activate the scope.

On the Altigen IP Phone

The IP phone's **System** menu includes an item called **Auto Discovery**. The user can select YES or NO for this menu item. The factory default is YES.

- When you upgrade from firmware that does not support Auto Discovery, Auto Discovery will be disabled by default.
- When you upgrade from firmware that does support Auto Discovery, the Auto Discovery setting will carry over.
- When the user erases the IP phone configuration by using **2 [enter] in the IP phone menu, Auto Discovery will be enabled by default.

Possible Auto-Discovery Scenarios

- During the Altigen IP phone’s start-up stage, if **Enable DHCP** is ON and **Auto Discovery** is set to YES, the IP phone configures its IP address from DHCP, and at the same time, it gets the MaxCS Server address from DHCP option 120. The user is then prompted to set the extension number and password.
- If **Enable DHCP** is OFF, then the phone’s IP address and the MaxCS Server address must be set manually.
- If **Enable DHCP** is ON and **Auto Discovery** is NO, the DHCP option 120 value is not sent to the Altigen IP phone. The MaxCS Server address must be set manually.
- If **Enable DHCP** is ON and **Auto Discovery** is YES and DHCP option 120 is set, the Altigen IP phone always gets a new IP address, and DHCP option 120 refreshes the value of MaxCS Server, even if MaxCS Server already has a value. The screen pauses for 2 seconds while the IP phone gets the MaxCS IP address from DHCP 120.

Disabling Auto-Discovery

To disable auto-discovery on individual Altigen IP phones, each phone must have its **Menu > System > Auto Discovery** menu item set to NO.

To disable auto-discovery on all phones, do not set DHCP option 120, or delete it if you have already set it.

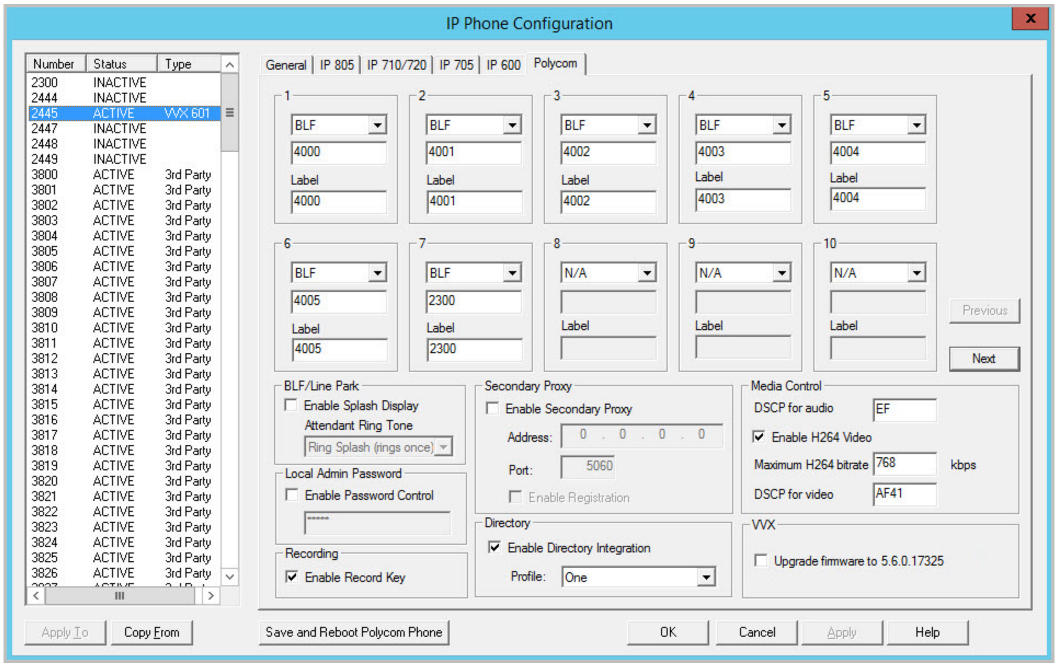
When auto-discovery is disabled, the MaxCS Server address must be set manually.

When You Have Two Altigen Servers in the Same Network

If there are two Altigen servers in the same network, some Altigen IP phones will get the wrong server IP address and cause log on failure. See the warning in *Configuring Auto-Discovery of Server IP Address*.

Polycom Configuration

For instructions on using the *Polycom* tab to configure extensions with Polycom phones, refer to the *MaxCS Polycom Configuration Guide*.



IP Phone Configuration

Number	Status	Type
2300	INACTIVE	
2444	INACTIVE	
2445	ACTIVE	VVX 601
2447	INACTIVE	
2448	INACTIVE	
2449	INACTIVE	
3800	ACTIVE	3rd Party
3801	ACTIVE	3rd Party
3802	ACTIVE	3rd Party
3803	ACTIVE	3rd Party
3804	ACTIVE	3rd Party
3805	ACTIVE	3rd Party
3806	ACTIVE	3rd Party
3807	ACTIVE	3rd Party
3808	ACTIVE	3rd Party
3809	ACTIVE	3rd Party
3810	ACTIVE	3rd Party
3811	ACTIVE	3rd Party
3812	ACTIVE	3rd Party
3813	ACTIVE	3rd Party
3814	ACTIVE	3rd Party
3815	ACTIVE	3rd Party
3816	ACTIVE	3rd Party
3817	ACTIVE	3rd Party
3818	ACTIVE	3rd Party
3819	ACTIVE	3rd Party
3820	ACTIVE	3rd Party
3821	ACTIVE	3rd Party
3822	ACTIVE	3rd Party
3823	ACTIVE	3rd Party
3824	ACTIVE	3rd Party
3825	ACTIVE	3rd Party
3826	ACTIVE	3rd Party

	Type	Value	Label
1	BLF	4000	4000
2	BLF	4001	4001
3	BLF	4002	4002
4	BLF	4003	4003
5	BLF	4004	4004
6	BLF	4005	4005
7	BLF	2300	2300
8	N/A		
9	N/A		
10	N/A		

BLF/Line Park
□ Enable Splash Display
Attendant Ring Tone: Ring Splash (rings once)

Local Admin Password
□ Enable Password Control
*****

Recording
☑ Enable Record Key

Secondary Proxy
□ Enable Secondary Proxy
Address: 0 . 0 . 0 . 0
Port: 5060
□ Enable Registration

Directory
☑ Enable Directory Integration
Profile: One

Media Control
DSCP for audio: EF
☑ Enable H264 Video
Maximum H264 bitrate: 768 kbps
DSCP for video: AF41

VVX
□ Upgrade firmware to 5.6.0.17325

Figure 141. The Polycom tab of the IP Phone Configuration page

CHAPTER

19

Mobile Extension Configuration

If your company has employees working at home or servicing customers in the field, you can connect their home phones or cell phones to the Altigen PBX, providing them with the same productivity features as if they were working in the office.

Altigen's ExtensionAnywhere capability allows an extension/agent to be:

- On-premise using voice or data wiring
- Mobile or remote using IP phone, cell phone, or PSTN phone
- An extension of another PBX via adjunct tie trunk or over a PSTN trunk simulated as a mobile extension port.

When configured, the property of the trunk interface is changed to simulate an extension. A mobile extension user will gain most of the system routing, call control, voice mail, CTI, and call center features through the PSTN telephone network.

A mobile extension includes the following capabilities:

- Call control – Transfer, hold, park, call pickup, conference
- Call handling – Single/multiple call waiting and queuing, RNA routing, account codes
- MaxCommunicator, MaxMobile Communicator, and MaxAgent CTI clients
- Conversation recording
- Workgroup agent with login/logout and ready/not-ready
- Pressing ****** terminates a call (soft on-hook) and gets a dial tone for the next call. The second * must be pressed within 1.5 seconds, or the system interprets it as one *.
- **#82** – Dial tone mute
- Supervisor silent monitoring, coaching, and barge-in

The extension can be dynamically logged in using **#27** from an internal, mobile, or IP device.

MobileExtSP Board Overview

A simulated physical board (MobileExtSP board) is created when you install the MaxCS Softswitch. You can configure this board with up to 1000 mobile extension ports. It handles all system-wide mobile extensions.

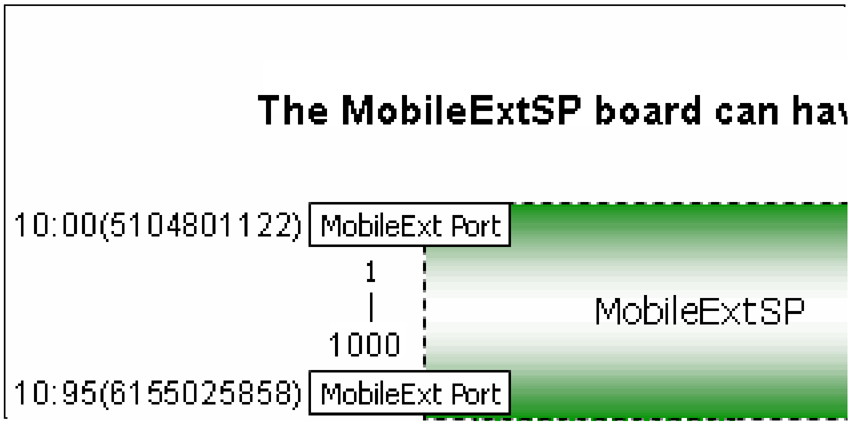


Figure 142.   MobileExtSP board diagram

T1, PRI, analog, and SIP trunks can be shared for regular incoming and outgoing calls and mobile trunk connections.

A mobile trunk can be assigned a Group ID and mobile extensions can be assigned to the appropriate group.

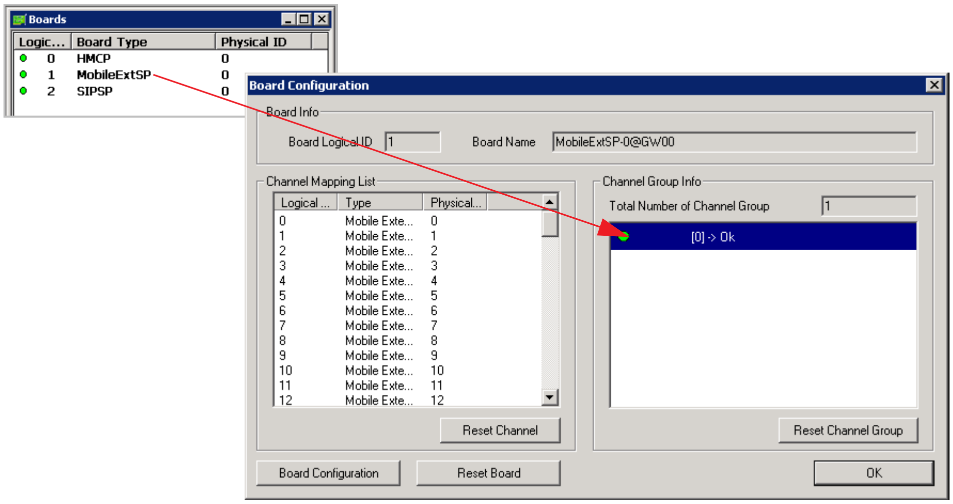
An analog trunk can be dedicated to one mobile extension user. A PRI trunk and SIP trunk can only be shared by all mobile extension users.

Configuring the MobileExtSP Board

To configure the MobileExtSP board,

1. In the **Boards** window, double-click the MobileExtSP board. In the Board Configuration window, double-click a channel group.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.



Logic...	Board Type	Physical ID
0	HMCP	0
1	MobileExtSP	0
2	SIPSP	0

Board Logical ID: 1

Board Name: MobileExtSP-0@GW00

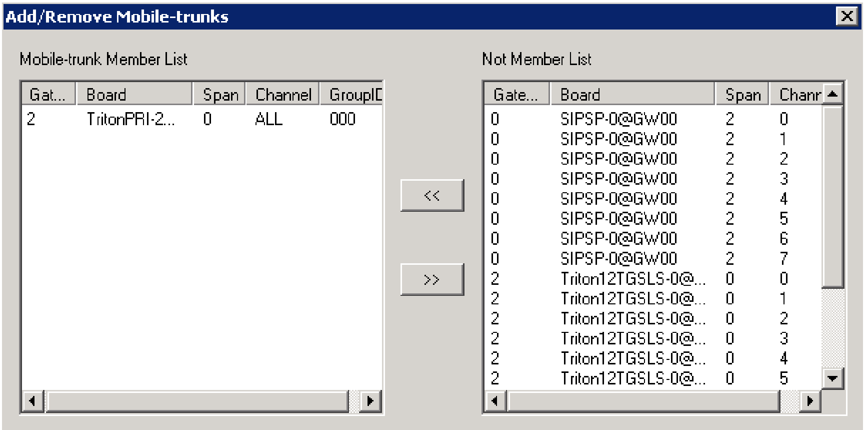
Logical ...	Type	Physical...
0	Mobile Exte...	0
1	Mobile Exte...	1
2	Mobile Exte...	2
3	Mobile Exte...	3
4	Mobile Exte...	4
5	Mobile Exte...	5
6	Mobile Exte...	6
7	Mobile Exte...	7
8	Mobile Exte...	8
9	Mobile Exte...	9
10	Mobile Exte...	10
11	Mobile Exte...	11
12	Mobile Exte...	12

Total Number of Channel Group: 1

[0] -> Ok

Figure 143.   Opening the Mobile Extension Board Configuration dialog box

2. Click the **Add/Remove** button to add mobile trunks.



Add/Remove Mobile-trunks

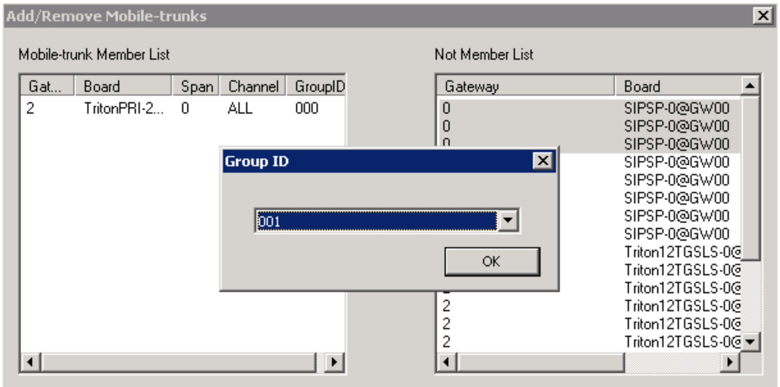
Mobile-trunk Member List

Gat...	Board	Span	Channel	GroupID
2	TritonPRI-2...	0	ALL	000

Not Member List

Gate...	Board	Span	Chanr
0	SIPSP-0@GW00	2	0
0	SIPSP-0@GW00	2	1
0	SIPSP-0@GW00	2	2
0	SIPSP-0@GW00	2	3
0	SIPSP-0@GW00	2	4
0	SIPSP-0@GW00	2	5
0	SIPSP-0@GW00	2	6
0	SIPSP-0@GW00	2	7
2	Triton12TGSLS-0@...	0	0
2	Triton12TGSLS-0@...	0	1
2	Triton12TGSLS-0@...	0	2
2	Triton12TGSLS-0@...	0	3
2	Triton12TGSLS-0@...	0	4
2	Triton12TGSLS-0@...	0	5

3. Add trunks to the **Mobile-trunk Member List** from the **Not Member List** by selecting the channels and clicking the Left Arrow button. You can use the Shift key or Ctrl key to select multiple channels.



Add/Remove Mobile-trunks

Mobile-trunk Member List

Gat...	Board	Span	Channel	GroupID
2	TritonPRI-2...	0	ALL	000

Not Member List

Gateway	Board
0	SIPSP-0@GW00
0	SIPSP-0@GW00
0	SIPSP-0@GW00
	SIPSP-0@GW00
	SIPSP-0@GW00
	SIPSP-0@GW00
	SIPSP-0@GW00
	SIPSP-0@GW00
	Triton12TGSLS-0@
	Triton12TGSLS-0@
	Triton12TGSLS-0@
2	Triton12TGSLS-0@
2	Triton12TGSLS-0@
2	Triton12TGSLS-0@

Group ID

001

You need to assign a Group ID to the channels. This Mobile Trunk Group ID allows you to differentiate MobileExt users connecting through different trunk types, like PSTN, SIP, or cell phone gateway. You can assign a mobile extension to use a specific trunk group. For example, if you assign SIP trunk channels from 1-3 to Group 001, and mobile extension 237 is assigned to Group 001, then when you make a call to extension 237, only the SIP Trunk channels from 1-3 can be seized. If all three channels are busy, the call will fail while other mobile extensions using another mobile trunk group ID may not be impacted.

Mobile extensions are assigned to a group in the Extension Anywhere Configuration dialog box (see Figure 145 on page 222).

Note: If a PRI span is used, only the whole span can be added or removed, not individual PRI channels. T1 and analog trunks are added or removed individually.

Although a whole PRI span is added, if **Mobile Trunk Allocation** is selected as **Shared** (see Figure 145 on page 222), individual trunks, when idle, still can be used dynamically by normal PRI trunk traffic or mobile extensions.

4. On the left side of the Mobile Extension Board Configuration dialog box, configure the fields:

- **Max Number of Extensions** – If more mobile channel support is required, change this to a larger number (1000 extensions maximum), and then reboot the system.
- **Key Simulation** – Check the first check box to allow the mobile phone user to use the * key to simulate “FLASH”. Check the second check box to allow the user to use ** to disconnect the current call and then get a dial tone without hanging up the cell phone. The user must press the second * within 1.5 seconds.

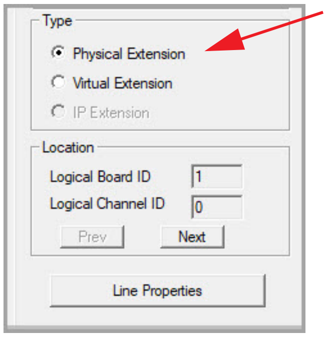
    - **Transmit Caller ID to MobileExt through PRI panel** Choose settings for Incoming Trunk Call Send and Incoming Extension Call Send:**Incoming Trunk Call Send** – If "Inbound caller ID" is checked, trunk calls to mobile extension will send the inbound caller ID.If "Specified number below" is checked, trunk calls to the mobile extension send the number from the configured box specified in Incoming Extension Call Send.**Incoming Extension Call Send** –
        - If "Extension number" is checked, extension calls to mobile extension send the caller's extension number.
        - If "Extension's TCID or System Main Number" is checked, extension calls to the mobile extension send the caller's transmitted caller ID (configured from Extension Configuration). If no TCID is configured,the system main number is sent.
    -
    - If incoming extension call "System Main Number" is checked, extension calls to mobile extension will send the system main number.
    - If "SIP Guest ID" is checked, extension calls to the mobile extension send the SipGuestID parameter in Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\AltiGen Communications, Inc.\AltiWare\Service Providers\SIPSP. The default value is "guest".
    - If "Specified number below" is checked, extension calls to the mobile extension send the number from the configured box.
- **DNIS Access Numbers** – If a PRI trunk is used for a mobile extension, a DNIS access number must be set, so that MaxCS can tell if the incoming call is a regular trunk call or a mobile extension off-hook request. Click the **Add** button in this panel to add a DNIS access number. To remove a number, select it and click the **Remove** button.
- **Mobile Extension Ports** table – Displays fields for the channel, target phone number, caller ID, trunk allocation (shared or dedicated), phrase 1 (Play Phrase After Answered), and phrase 2 (Play Phrase Before Dial Tone) of each extension port.
- **Mobile Trunks** table – Displays fields for the board, span, channel, trunk allocation, mobile extension and status of each mobile trunk.

5. Note the logical ID of the MobileExtSP board. You will need it when you assign an extension to a mobile port.
6. When you are finished adding channels as mobile trunks, restart MaxCS.

Configuring an Extension as a Mobile Extension

To configure an extension as a mobile extension,

1. Select **PBX** > **Extension Configuration**.
2. To assign an extension to a mobile extension port, select a virtual extension and change it to a physical extension.



Type

● Physical Extension

○ Virtual Extension

○ IP Extension

Location

Logical Board ID: 1

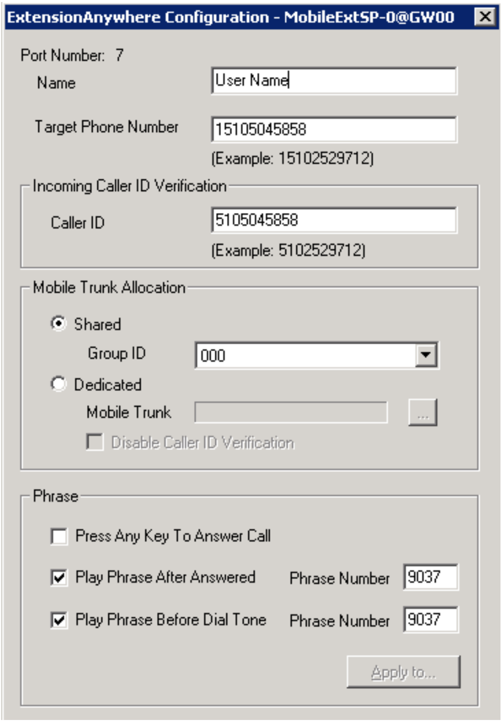
Logical Channel ID: 0

Figure 144. Changing a virtual extension to a physical extension and setting the location

3. By clicking the **Next** or **Prev** button in the **Location** panel, select the **Logical Board ID** of the MobileExtSP board and **Logical Channel ID** for this extension, then click **Apply**.

   The new location is displayed in the Agent/Supervisor/Extension list.

4. Click the **Line Properties** button to configure the mobile PSTN number and other options for the mobile extension. The **ExtensionAnywhere Configuration – MobileExtSP** dialog box opens. (Alternatively, from the Mobile Extension Board Configuration dialog box you can double-click the mobile extension port to open the ExtensionAnywhere Configuration.)



ExtensionAnywhere Configuration - MobileExtSP-0@GW00

Port Number: 7

Name: User Name

Target Phone Number: 15105045858

(Example: 15102529712)

Incoming Caller ID Verification

Caller ID: 5105045858

(Example: 5102529712)

Mobile Trunk Allocation

● Shared

Group ID: 000

○ Dedicated

Mobile Trunk:

□ Disable Caller ID Verification

Phrase

□ Press Any Key To Answer Call

☑ Play Phrase After Answered — Phrase Number: 9037

☑ Play Phrase Before Dial Tone — Phrase Number: 9037

For a mobile phone using MaxMobile Communicator, *clear* all the Phrase check boxes.

Figure 145. ExtensionAnywhere Configuration – MobileExtSP dialog box

- **Name** – Enter the name of the person using the mobile phone.
- **Target Phone Number** – Enter the number of the mobile phone. This is used when MaxCS makes a call through PSTN to the mobile phone. Do *not* include the trunk access code.

- **Caller ID –** Enter the phone number of the mobile phone. This is for incoming caller ID verification. MaxCS uses it to determine whether a call is from a mobile extension. If the caller ID is matched, the mobile extension user will hear a dial tone from the system, the same as an internal extension user hears when the phone is off-hooked.

It's also used to find a mobile channel in the MaxMobile Communicator application, and it is used in the MaxMobile Communicator login.

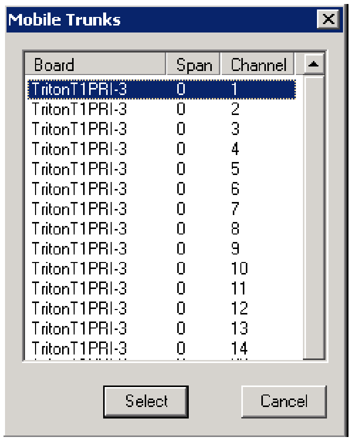
Note: When a MaxMobile user logs in to the MaxCS system, the assigned extension number, extension password and cell phone number are used as identification. First, MaxCS checks the extension number and extension, then it uses the cell phone number to search the mobile channel table. If MaxCS finds one channel's Caller ID is the same as the cell phone number, it will assign this channel to the extension number. The extension is allowed to log in as a mobile extension. If no channel is found, the login fails.

- **Mobile Trunk Allocation** – Select either **Shared** or **Dedicated**.

  Shared – When selected, this mobile extension will share mobile trunk ports with other mobile extension users. You need to assign a mobile trunk Group ID to this extension. The system will dynamically allocate a mobile trunk port within this Group ID when the system calls out to this mobile extension number.

  When the mobile extension user calls into the system, any mobile trunk port can answer the call, verify caller ID, and play a dial tone to the mobile extension user.

  Dedicated – Only analog trunks can be dedicated mobile trunks. When selected, you need to assign a mobile trunk port to this mobile extension. You have the option to disable caller ID verification if a mobile trunk port is dedicated to this mobile extension. The mobile extension user will hear a dial tone when calling into this specific trunk port. Use the **Browse** button (**…**) to select the desired mobile trunk.



Board	Span	Channel
TritonT1PRI-3	0	1
TritonT1PRI-3	0	2
TritonT1PRI-3	0	3
TritonT1PRI-3	0	4
TritonT1PRI-3	0	5
TritonT1PRI-3	0	6
TritonT1PRI-3	0	7
TritonT1PRI-3	0	8
TritonT1PRI-3	0	9
TritonT1PRI-3	0	10
TritonT1PRI-3	0	11
TritonT1PRI-3	0	12
TritonT1PRI-3	0	13
TritonT1PRI-3	0	14

Figure 146.   Mobile Trunks dialog box

- In the **Phrase** panel, you have three options: You can select either **Press Any Key To Answer Call** *or* **Play Phrase After Answered.** And you can select **Play Phrase Before Dial Tone.** You can use the **Apply** button to apply selections in this panel to other mobile extensions.

Note: **Note**: For mobile extensions running MaxMobile Communicator, you should clear all three check boxes in the Phrase panel.

  – **Press Any Key To Answer Call** – When a call is answered by this mobile extension user, the system will play the following phrase for the mobile extension user: “To accept this call, please press any digit.” The user must press any key within 3 seconds to connect the call; otherwise, it will time out and the call will be treated as an agent/extension RNA and will be routed according to its workgroup/extension setting.

- If there is a network error or a mobile extension trunk is not available, RNA handling is applied to the caller. Therefore, it is suggested that you don't check the **Set RNA Agent Logout** option for the group that contains the mobile extension as an agent (Workgroup Configuration, **Call Handling** tab).
- **Play Phrase After Answered** – The system will play the given phrase when the mobile extension user answers the call from the system. The default phrase (9037) is a special tone to signal the mobile extension user that this call can be put on hold, parked, transferred, conferenced.
- **Play Phrase Before Dial Tone** – The system will play the default phrase 9037 (a special tone) and then the dial tone when the mobile extension user calls into the system through a configured DNIS Access Number.

Additional Configuration for MaxMobile Communicator

For mobile phones running MaxMobile, do the following:

- If MaxCS is behind NAT, configure the NAT router to forward TCP port 10080 and 10081 to MaxCS's private IP address, so the data access from a 3G network can reach this server.
- Open firewall ports TCP 10080 and 10081 for both virtual public IP address and private IP address.
- Assign an Altigen MaxMobile license to the extension. To do this, from the MaxAdministrator main menu, select **License > Client SEAT License Management**. In the Client SEAT License Management dialog box, select **MaxMobile** in the License Types column, and add the appropriate extension to the Members list.
- When using a SIP trunk as MaxMobile trunk, the **Early Media** option must be enabled for the SIP trunk.

Voice Mail for Mobile Extensions

When the mobile extension phone is turned off or busy, messages can go to the extension's voice mail in Max-CS or to the mobile phone's voice mail:

- To send a call to the mobile extension's voice mail in MaxCS, check the **Press any key to answer call** check box. If the mobile phone is running MaxMobile Communicator, this check box should never be checked.
- To send a call to the mobile phone's voice mail, the **Press any key to answer call** check box must be *un*checked.

Mobile Extension Limitations

- Only PRI mobile trunks can deliver Caller ID information to the mobile extension.
- A mobile extension cannot support Centrex transfer.
- After adjusting the number of mobile extension ports in a mobile extension board, MaxCS must be restarted for the changes to take effect.
- Cannot deliver caller name to the mobile extension.
- Does not support Message Waiting Indicator on the mobile extension device. (Use Message Notification as a work-around).
- Since the DTMF key ***** is used for simulating the FLASH signal, there is no way to send ***** to the system.
- The RNA for mobile extension may not be accurate, because the system ring count may not be in sync with the mobile extension device ring count.

- When placing calls to mobile extensions that are cell phones, if the cell phone is out of signal range, the caller may hear long periods of silence. You can check the **Press any key to answer call** option to prevent this problem.
- Only analog trunks can be allocated as dedicated mobile trunks.

CHAPTER

20

Hunt Group Configuration

The hunt group is a simple call distribution application for operator, call coverage group, integration with a fax server, or a user with multiple extensions connecting to different devices. When adding a member to a hunt group, the following rules apply:

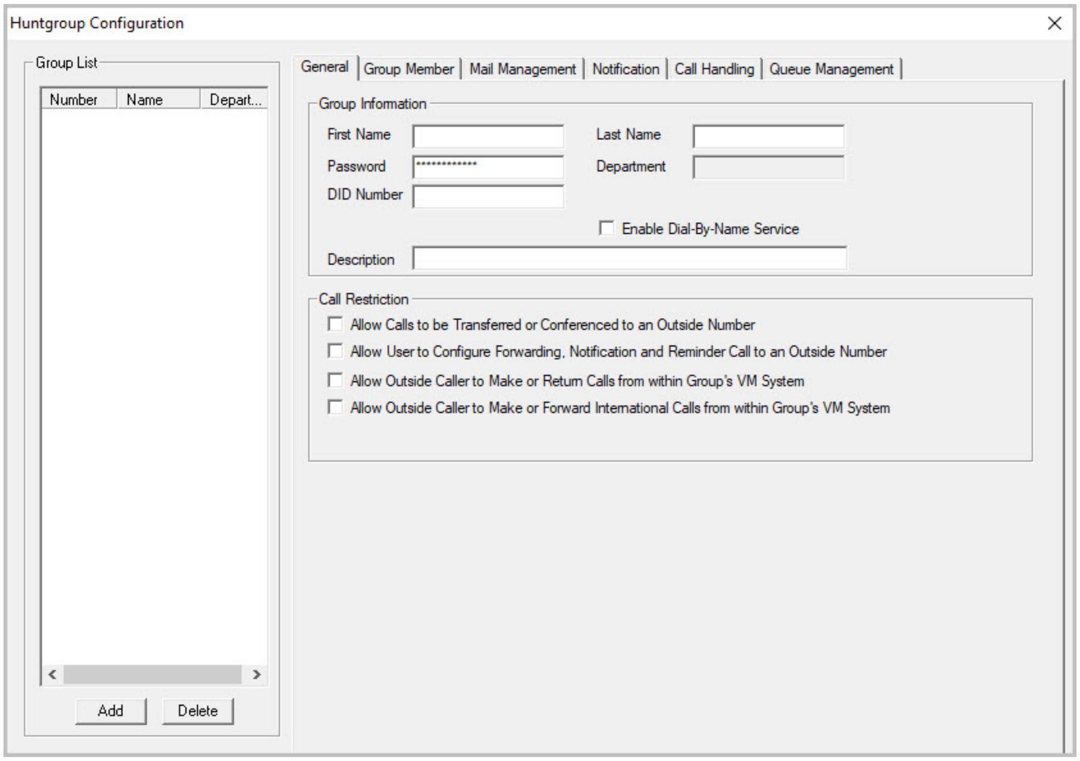
- No agent seat license required
- Any extension can be added to a hunt group
- Each hunt group can have up to 128 members
- An extension can belong to multiple hunt groups

Although a hunt group has call queuing capability, it lacks the following functions:

- Does not generate real-time queue and agent status for the hunt group
- Does not have a real-time counter to track hunt group activities for reporting purposes
- Does not have logout reason code tracking capability
- Does not have recording capability
- Does not have service level threshold setting
- Does not have queue overflow and quick queue option
- Limited call distribution capability
- No supervisor application to manage agents and calls in queue
- No client application for agents to perform login/logout

The Huntgroup Configuration window provides for creating hunt groups, setting their attributes, and assigning group members.

To open the Huntgroup Configuration window, select **PBX** > **Huntgroup Configuration**.



First Name
Last Name
Password ************
Department
DID Number
□ Enable Dial-By-Name Service
Description

□ Allow Calls to be Transferred or Conferenced to an Outside Number
□ Allow User to Configure Forwarding, Notification and Reminder Call to an Outside Number
□ Allow Outside Caller to Make or Return Calls from within Group's VM System
□ Allow Outside Caller to Make or Forward International Calls from within Group's VM System

Figure 147. Huntgroup Configuration window

Overview of Huntgroup Configuration Window

These are the tabs in the Huntgroup Configuration window:

- **General** – Add or delete a hunt group, assign a group name, password, and DID number
- **Group Member** – Add or remove members from huntgroups
- **Mail Management** – Capacity and feature options for hunt group mailboxes
- **Notification** – Preferences and options for voice mail notification
- **Call Handling** –Call forwarding, call waiting, and call handling preferences and options
- **Queue Management** – Options for setting default or custom phrases used as queue announcements

Apply to Button

The Huntgroup Configuration window often allows you to apply changes to a particular hunt group or to select many huntgroups to which to apply the changes.

The **Apply to** button is disabled unless there is a change that can be applied to multiple hunt groups, and when you use it to apply changes to multiple hunt groups, it works on only those changed attributes that can be applied.

Setting Up Huntgroups

Set up new huntgroups in the Huntgroup Configuration window.

To add a hunt group,

1. Click the **Add** button under the **Group List**.
2. Type in a group number for the hunt group.
3. Check the **Global group** check box if you want the group to be visible to other systems within the VoIP domain. See the section Enterprise VoIP Network Management for more information.
4. Click **OK**.

Establishing Basic Hunt Group Attributes

After you create a hunt group, you can set basic attributes in the Huntgroup Configuration, **General** tab:

To set Hunt Group information, enter the following information:

- **First Name** and **Last Name** – Each with a maximum of 32 characters.
- **Password** – The default is the system default password set on the **Number Plan** tab of the System Configuration window.

  A valid password cannot be the same as its hunt group number and must be 4 - 8 digits (numbers or letters A - Z) in length. Basic password patterns, such as repeated digits (1111), consecutive digit strings (1234), or digits that match the extension (Ext. **101** using **101**2, 9**101**, **101**01, etc.) are not recommended. The letters map to numbers (on a phone, for example) as follows:

Numbers	Letters	Numbers	Letters
2	A, B, C, a, b, c	6	M, N, O, m, n, o
3	D, E, F, d, e, f	7	P, Q, R, S, p, q, r, s
4	G, H, I, g, h, i	8	T, U, V, t, u, v
5	J, K, L, j, k, l	9	W, X, Y, Z, w, x, y, z

- **Department** – Enter the department for this hunt group, if appropriate.
- **DID Number** – Each hunt group can be assigned a DID number. This number does not have a fixed length, but the length must be long enough (range 2 - 16) for the system to match the DID incoming call.
- **Enable Dial-By-Name Service** – Check this box to allow callers to search the list by employee name for this hunt group extension.
- **Description** – Describe the purpose of this hunt group.

Setting Call Restrictions

The call restriction rules on the **General** tab apply to users making outbound calls from within voice mail and several hunt group settings. These settings do not impact the call restriction settings configured for the hunt group member's extension in Extension Configuration.

- **Allow Calls to be Transferred or Conferenced to an Outside Number** – When checked, the internal extension user can log into this hunt group voice mail, make a call to a second party, then transfer or conference to a third party.

- **Allow User to Configure Forwarding, Notification, and Reminder Call to an Outside Number** – This setting regulates hunt group call forwarding, voice mail notification, and reminder call configuration. If this setting is not checked, you will see a warning message pop up when trying to set up forwarding to an outside number. International calls are not allowed if the fourth option is not checked.
- **Allow Outside Caller to Make or Return Calls from within Group's VM System** – When checked, an outside caller can dial into the system, log in to hunt group voice mail, and make or return calls from the group's voice mail (Zoomerang feature). International calls are not allowed if the fourth option is not checked.
- **Allow Outside Caller to Make or Forward International Calls from within the Group's VM system** – This setting regulates making international calls from voice mail and forwarding to an international number.

Important: Allowing any of these options may increase the potential for toll fraud. Make sure the password is properly configured to prevent an intruder from using this voice mail box to make an outbound call. Altigen recommends that you leave the fourth option unchecked for all hunt groups at all times.

Establishing Hunt Group Membership

There are two ways to assign extensions to huntgroups.

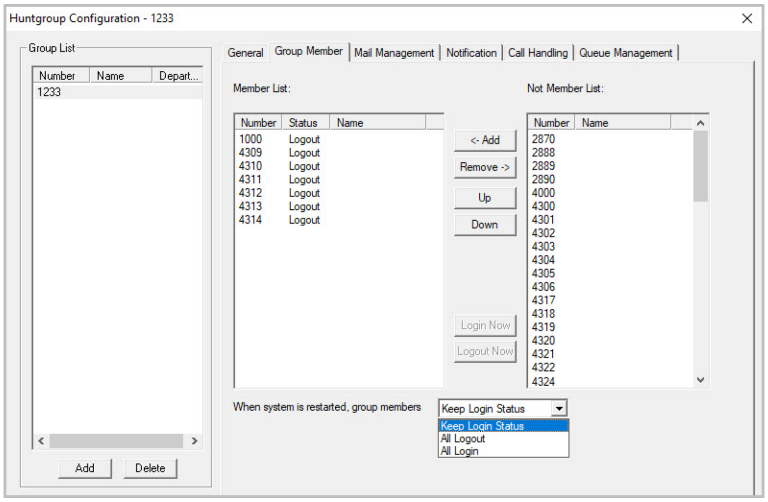
- In the Huntgroup Configuration window select a *group*, then click the **Group Member** tab. Here you can add extensions (group members) to the selected hunt group.
- In the Extension Configuration window select an *extension*, then click the **Group** tab. Here you can assign a hunt group to the selected extension (and you can see what other hunt groups the extension is a member of). For this second method, see “Adding or Removing Group Assignments” on page 177.

The order in which you add extensions to a hunt group may affect the call distribution sequence. See “Setting Call Handling Options” on page 234 for more information. To adjust the order, select the extension you would like to adjust and use the **Up** or **Down** button to change the order.

When you add an extension to a hunt group, the extension is in the "Logout" state. The hunt group member must manually log in using feature code **#54**.

Adding Extensions to a Hunt Group

1. In the Huntgroup Configuration window, select the hunt group number in the **Group List**. The hunt group number appears in the window title bar.
2. Click the **Group Member** tab.



Number	Name	Depart...
1233		

Member List:

Number	Status	Name
1000	Logout	
4309	Logout	
4310	Logout	
4311	Logout	
4312	Logout	
4313	Logout	
4314	Logout	

Not Member List:

Number	Name
2870	
2888	
2889	
2890	
4000	
4300	
4301	
4302	
4303	
4304	
4305	
4306	
4317	
4318	
4319	
4320	
4321	
4322	
4324	

When system is restarted, group members: Keep Login Status

- Keep Login Status
- All Logout
- All Login

Figure 148. Huntgroup Configuration, Group Member tab

3. Select the extension number(s) in the **Not Member** list. Use **Ctrl**+click or **Shift**+click to select several extensions.
4. Click **Add** to move them to the **Member** list.

   Note: If the hunt group pilot extension is configured to Ring All Available Members, the maximum number of members is 20. See “Setting Call Handling Options for details.

Removing Extensions from a Hunt Group

1. Click the extension number(s) in the **Member** list.
2. Click **Remove** to move them to the **Not Member** list.

Setting Login Status for System Restart

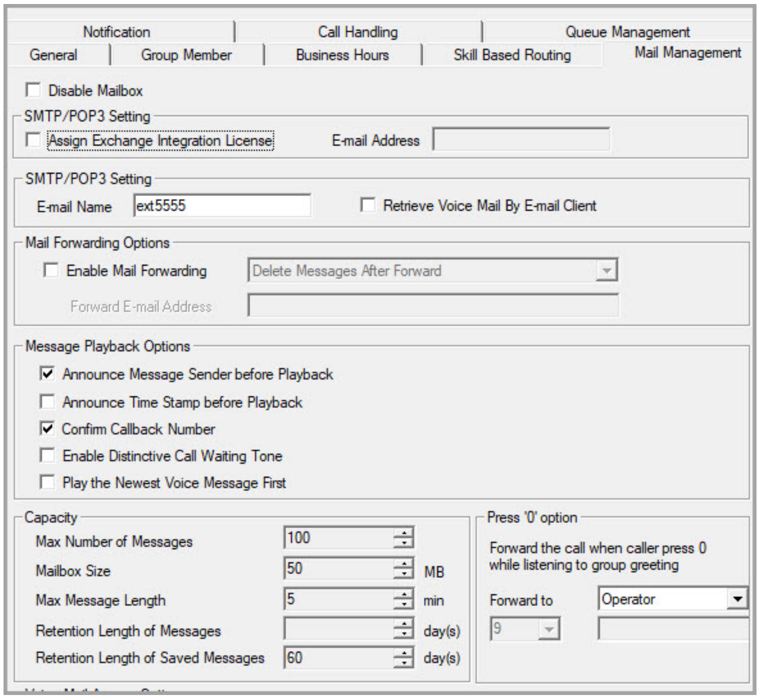
Whenever the system is restarted, the administrator can use the list at the bottom of the **Group Member** tab to:

- **Keep Login Status** – All group members retain their original login status for that group prior to restart (default setting).
- **All Login** – All group members are automatically logged into the assigned group after the system is restarted.
- **All Logout** – All group members are logged out of the group when the system is restarted.

Setting Hunt Group Mail Management

The Mail Management settings define how voice messages are handled for a hunt group, including how messages are announced and processed, and how much capacity is allotted to message storage.

To work with mail management settings, click the **Mail Management** tab, and select the hunt group number you want to work with from the **Group List**.



□ Disable Mailbox

SMTP/POP3 Setting

□ Assign Exchange Integration License E-mail Address

SMTP/POP3 Setting

E-mail Name ext5555 □ Retrieve Voice Mail By E-mail Client

Mail Forwarding Options

□ Enable Mail Forwarding Delete Messages After Forward

Forward E-mail Address

Message Playback Options

☑ Announce Message Sender before Playback
□ Announce Time Stamp before Playback
☑ Confirm Callback Number
□ Enable Distinctive Call Waiting Tone
□ Play the Newest Voice Message First

Capacity

Max Number of Messages 100
Mailbox Size 50 MB
Max Message Length 5 min
Retention Length of Messages day(s)
Retention Length of Saved Messages 60 day(s)

Press '0' option

Forward the call when caller press 0 while listening to group greeting

Forward to Operator

9

Figure 149. Huntgroup Configuration, Mail Management tab

Note: You can use the **Apply to** option to apply mailbox settings to one, some, or all huntgroups.

Disabling a Mailbox

When you disable a mailbox, the normal greeting is played but callers cannot leave messages.

Setting E-mail Options

On the **Mail Management** tab, you can set the e-mail options for the hunt group:

- **Assign Exchange Integration License** – Assign an Exchange Integration license to this group.You must also provide an email address.
- **E-mail Name** – The hunt group's e-mail name without the @domain. The default e-mail name is ext*<hunt group number>*, that is, the letters "ext" followed by the hunt group number. For example, the default e-mail name for hunt group 500 would be **ext500**.
- **Retrieve Voice Mail by E-mail Client** – When selected, this sends voice mail to the user's e-mail as an attachment. Deselected, voice mail is retrieved as voice mail.
- **Enable Mail Forwarding** – When selected, the hunt group's e-mail will be forwarded to the e-mail address you specify in the **Forward E-mail Address** box. The address should be a full address, including the domain (for example, *jsmith@thecompany.com*).

  If you enable mail forwarding, you also specify what you want done with the original messages after they have been forwarded. In the list you can choose to:

  - Delete Messages after Forward
  - Keep the Messages as New
  - Keep Messages as Saved

Setting Mailbox Playback Options

You can use the following check boxes to turn on or off options for listening to playback of recorded messages. These options apply to both new messages and saved messages, and they can be applied to multiple huntgroups using **Apply to**:

Message Playback Parameter	Description
Announce Message Sender Before Playback	Selected, the user hears the name of the message sender (internal sender only) before listening to recorded Altigen Voice Mail System messages.
Announce Time Stamp Before Playback	Selected, the user hears the timestamp (time and date) of each message before playback.
Confirm Callback Number	Selected, system confirms the accuracy of the caller's number.
Enable Distinctive Call Waiting Tone	Selected, the user hears three different call waiting tone cadences to distinguish between internal, external, and operator calls (see "Distinctive Ring" on page 33).
Play the Newest Voice Message First	Selected, new voice mail will be retrieved first. When not selected, the system will play voice mail based on FIFO (first in, first out).

Setting Mailbox Capacities

You can set various mailbox capacities with the following options, and you can apply the settings to multiple hunt groups using **Apply to**:

Mailbox Capacity Parameter	Description
Message Retention Duration	Set how long (in days) new, heard and/or saved voicemail messages are retained. The default duration is 60 days. By default, only the *Saved Messages* option is selected. Any message type that is **not** selected will have no duration limit.
Max Number of Messages	Maximum number of messages stored in the hunt group's mailbox. The range is **1** – **999**, defaulting to 100. When your voicemail mailbox capacity is reached, the voicemail system will announce "Your mailbox is full" and no further messages will be accepted until you delete enough messages to fall back below your set capacity.
Mailbox Size	Mailbox size in MBs of stored messages. The range is **1**–**500** MB, with a default of 50. When your voicemail mailbox capacity is reached, the voicemail system will announce "Your mailbox is full" and no further messages will be accepted until you delete enough messages to fall back below your set capacity.
Max Message Length	Maximum length of voice messages in minutes. The range is **1**–**30** minutes, with a default of 5 minutes.

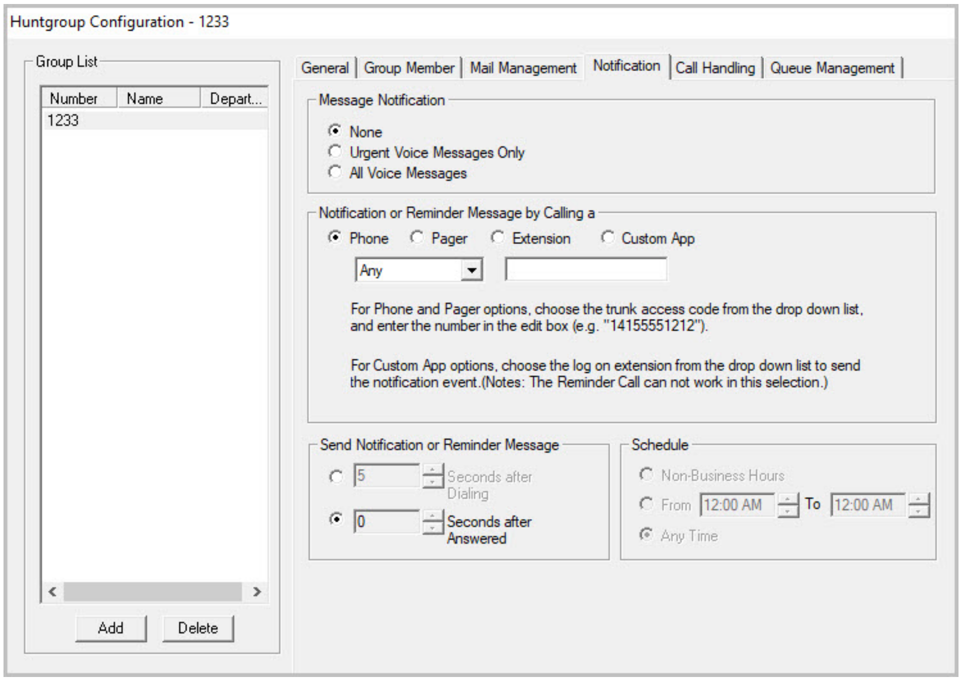
Setting Message "Press 0" Options

This option allows a caller to press "0" while listening to this hunt group's greeting. When the caller presses "0," the call will forward to the specified destination. Use the list to specify a forwarding destination for the call: **Voice Mail**, **AA**, **Extension**, **Group**, **Operator** (default), **Outside Number**, or **Line Park**.

If you choose to forward to an **Outside Number**, select a trunk or route access code to use in the small list on the left, and type in the full prefix and phone number.

Setting Message Notification Options

To set notification options on new incoming e-mail and voice messages, click the **Notification** tab in the Huntgroup Configuration window, and select the hunt group number from the **Group List**.



Huntgroup Configuration - 1233

Group List

Number	Name	Depart...
1233		

Message Notification

● None
○ Urgent Voice Messages Only
○ All Voice Messages

Notification or Reminder Message by Calling a

● Phone ○ Pager ○ Extension ○ Custom App

Any

For Phone and Pager options, choose the trunk access code from the drop down list, and enter the number in the edit box (e.g. "14155551212").

For Custom App options, choose the log on extension from the drop down list to send the notification event.(Notes: The Reminder Call can not work in this selection.)

Send Notification or Reminder Message

○ 5 Seconds after Dialing
● 0 Seconds after Answered

Schedule

○ Non-Business Hours
○ From 12:00 AM To 12:00 AM
● Any Time

Figure 150. Huntgroup Configuration, Notification tab

Individual users can also configure **Message Notification** within the Altigen Voice Mail System.

Note: You can use the **Apply to** option to apply mailbox settings to one, some, or all hunt groups. See "Apply to Button" on page 226 for more information on using **Apply to**.

Setting the Message Types for Notification

Select the types of messages for which the hunt group user will be notified:

- **None** – When selected, the user is *not* notified with a call regarding newly received messages. Selecting this option does not prevent the user from getting message waiting indicators or stutter dial tone when new messages are received.
- **Urgent Voice Messages Only**
- **All Voice Messages**

Please note that the system will start notification as soon as it enters non-business hours under the following conditions:

- Extension is set to notify **Urgent Voice Message Only**
- Notification is set to **Non-Business Hours**
- Voice mail is received during business hours and is marked urgent
- Extension user does not check the urgent message

Setting the Type of Notification

There are four options for sending the notification or reminder message: **Phone**, P**ager**, **Extension** or **Custom Application**.

- **Extension** – To use the Extension option, select the **Extension** radio button, then type the extension number into the text box.
- **Phone/Pager** – For the **Phone** and **Pager** options, first specify the trunk or route access code using the list next to the **Extension** radio button. The **Any** option means to locate any available trunk. Then type in the number with all relevant dialing prefixes other than the trunk code, using a maximum of 63 digits.
- **Custom App** – When used in conjunction with a third-party notification application, the **Custom App** feature enables an extension to connect to an application that can receive the notification event; use the list to choose the log-on extension to which the third-party application is connected. Contact your local Altigen Partner for more information on using this feature.

  Note: The Reminder Call will not work with this selection.

Note also the following considerations:

- For the **Pager** option, the system calls the specified pager number and then dials the system main number (as set in System Configuration, **General** tab), which is then displayed on the user's pager.

  For the operator-assisted paging function, the operator phone number **and** the pager number must be entered in the **<phone number>*<pager number>** format. For example, if the phone number to call the pager operator is **7654321** and the pager number to page the user is **12345678**, the notification outcall number that needs to be entered is **7654321*12345678**. When the pager operator answers the Message Notification call, MaxCS announces the **pager number and** the **System Main Number** (as configured on the **General** tab of **System Configuration**), which will be displayed on the user's pager. The operator is also given the option to repeat these numbers by pressing '**#**'.

Outcall to Cellular or PCS Phone Numbers

When an outcall is made by the system (for One Number Access, Message Notification, Zoomerang, Call Forwarding, and so on) to a cellular or PCS phone, it may ring the phone once but not necessarily present the call and make a connection. This will happen if the ringback tone played by the cellular service provider does not conform to standard ringback tones. To work around this problem, append a few commas (**,**) to the outcall (cellular) number when entering it. Each comma provides a one second pause.

Setting Notification Timing

When notification is configured to an *outside phone number*, the system will announce, "This is the outcall notification message for…" after call connection. However, there are situations when the system may not be able to receive an answer supervision signal from the carrier. If the system plays the announcement phrase before the notification call is answered, the phrase will be cut off. The following two options can be configured based on answer supervision capability:

- **Seconds after Dialing –** If the carrier of the outside phone number cannot provide an answer supervision signal, check this option and set a delay time. (Default 5 seconds, maximum 30 seconds.)

  Note: If the delay is set too long, the notified party will hear silence before the announcement is played.

- **Seconds after Answered –** This field is set to 0 seconds and it is not configurable for notification to a phone number. It means the system will play the announcement immediately after answer supervision is received.

When notification is configured to a *pager*, the system will transmit DTMF digits as the return phone number (the **System Main Number** as set in the System Configuration **General** tab) after call connection. However, there are situations when the system may not be able to receive an answer supervision signal from the pager system. If the system sends digits before the call is connected, some digits will be cut off. The following two options can be configured based on answer supervision capability:

- **Seconds after Dialing –** If the pager carrier cannot provide an answer supervision signal, check this option and set a delay time. (Default 5 seconds, maximum 30 seconds.)
- **Seconds after Answered –** If the answer supervision signal is provided by the carrier, check this option and set the delay timer to 2 to 5 seconds. In some cases, the pager carrier cannot detect DTMF right after the call connection. (Default is 10 seconds, maximum is 30.)

  Note: You may need to try a different delay setting to make sure the user return number is transmitted properly after configuration.

Setting Notification Business Hours

You can choose one of three options for when the extension user is to be notified of new messages:

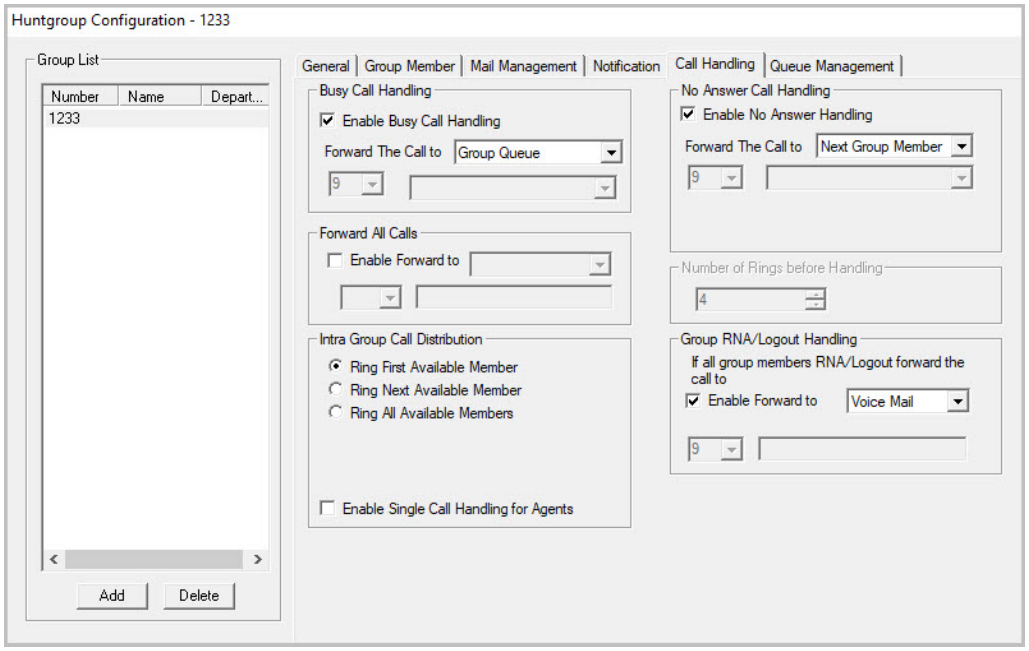
- **Non-Business Hours** – Notify only during non-business hours. Business hours are set in System Configuration, **Business Hours** tab (see “Setting Business Hours” on page 38).
- **From/To** – Notify during a specified time of day. Select the hours in the **From** and **To** time scroll boxes.
- **Any Time** – Notify at all times (every day).

Setting Call Handling Options

Call Handling options include handling busy calls, forwarding, handling no-answers, call distribution, and other options.

You can use the **Apply to** button to apply call handling settings to one, some, or all hunt groups. See “Apply to Button” on page 226 for more information on using **Apply to**.

To work with hunt group call handling options, click the **Call Handling** tab in the Huntgroup Configuration window, and select the hunt group number from the **Group List**.



Number	Name	Depart...
1233		

Busy Call Handling

☑ Enable Busy Call Handling

Forward The Call to: Group Queue

9

Forward All Calls

□ Enable Forward to

Intra Group Call Distribution

● Ring First Available Member

○ Ring Next Available Member

○ Ring All Available Members

□ Enable Single Call Handling for Agents

No Answer Call Handling

☑ Enable No Answer Handling

Forward The Call to: Next Group Member

9

Number of Rings before Handling: 4

Group RNA/Logout Handling

If all group members RNA/Logout forward the call to

☑ Enable Forward to: Voice Mail

9

Figure 151. Huntgroup Configuration, Call Handling tab

Handling Busy Calls

You have several options for handling calls while the agents in a hunt group are busy. If you do not enable busy call handling, the caller simply hears a busy signal.

To enable the options, check the **Enable Busy Call Handling** check box, then select from the following forwarding options:

- **Group Queue** – The caller will stay in the hunt group queue waiting for any agent to become available. If there is no agent logged in at this moment, the system will use **Group Logout Handling** to handle this call.
- **Group Voice Mail** – The caller will be forwarded to the hunt group voice mail box when all agents are busy
- **AA** – Forward caller to an auto attendant.
- **Extension** – Forward caller to an extension.
- **Group** – Forward caller to another group.
- **Line Park** – Forward caller to a Line Park group.

Forwarding All Calls

When you do not want the hunt group to handle any calls, check the **Enable Forward To** option in the Forward All Calls section of the **Call Handling** tab, and select an option.

The forwarding options are as follows:

- To **Voice Mail**
- To **AA** – Select the AA to use in the list under the option.
- To an **Extension** – Select an extension number in the drop-down list.
- To a **Group** – Select a group from the list.
- To the **Operator**

- To an **Outside Number** – This option is available if it is allowed in the **Other Call Restrictions** option in the **Restriction** tab, as discussed in “Setting Other Call Restrictions” on page 186. Also, see “Outcall to Cellular or PCS Phone Numbers” on page 233.

  If you choose **Outside Number**, select a trunk or route access code to use in the small list on the left, and type in the full prefix and phone number.
- To an **App Ext** – When used in conjunction with a third-party notification application, the **App Ext** feature enables an extension to connect to an application that can receive the notification event; use the list to choose the log-on extension to which the third-party application is connected. Contact your local Altigen Partner for more information on using this feature.
- To **Line Park** – If configured, select a **Line Park** group from the list.

Handling Unanswered Calls

The **Enable No Answer Handling** configuration provides options for handling calls when the system rings the first available agent and the call is not answered. If *all* agents in the hunt group are rung and no one answers the call, the system will use the Group RNA/Logout Handling rule. **Enable No Answer Handling** is not available if Intra Group Call Distribution is set to **Ring All Available Members**.

To configure this option, check the **Enable No Answer Handling** box.

Select one of the following forwarding options for no answer call handling:

- **Next Group Member** – Ring the next available agent until all available agents are rung. If all agents are busy, caller will stay in the hunt group queue.
- **Extension** – Take the call out of the hunt group and forward it to an extension.
- **Group** – Take the call out of hunt group and forward it to another group.
- **Group Voice Mail** – Transfer the caller to the hunt group voice mail when the first available agent does not answer the call.
- **Member Voice Mail** – Transfer the caller to the first available agent's voice mail if this agent does not answer the call.
- **AA** – Take the call out of the hunt group and forward it to an auto attendant.
- **Line Park** – Take the call out of the hunt group and forward it to a Line Park group.

If you select **Ring All Available Members** in the Intra Group Call Distribution section, then specify the **Number of Rings before Handling**, using the scroll box beside that option. The number of rings is the total number of times agents are rung before the call is handled by the Group RNA/Logout Handling configuration

Setting a Hunt Group’s Call Distribution Rule

The **Call Handling** tab in the Huntgroup Configuration window lets you set the distribution of normal inbound calls to group members, using one of the following three options:

- **Ring First Available Member** – First *available* extension in a hunt group. For example, if there are three member extensions in a hunt group, the call is always sent to the *first* member configured in the hunt group. If this member is busy, the call goes to the *second* member configured and so forth.
- **Ring Next Available Member** – A round-robin method that attempts to evenly distribute calls among the group members. This method sends the call to the *next* member configured in a hunt group (regardless of whether the previous member is busy or not). In other words, if the previous call was sent to #3 in the group, the present call is sent to #4, if #4 is not busy.
- **Ring All Available Members** – All extensions in a hunt group.

  Note: When this option is enabled, a single hunt group can have no more than 20 members.

  In addition, calls to the hunt group with this option enabled have higher priority than other hunt group calls. Therefore, if an agent belongs to multiple huntgroups, one of which has this option enabled, a call to that hunt group will be distributed before others, regardless of its Wait Time in the queue.

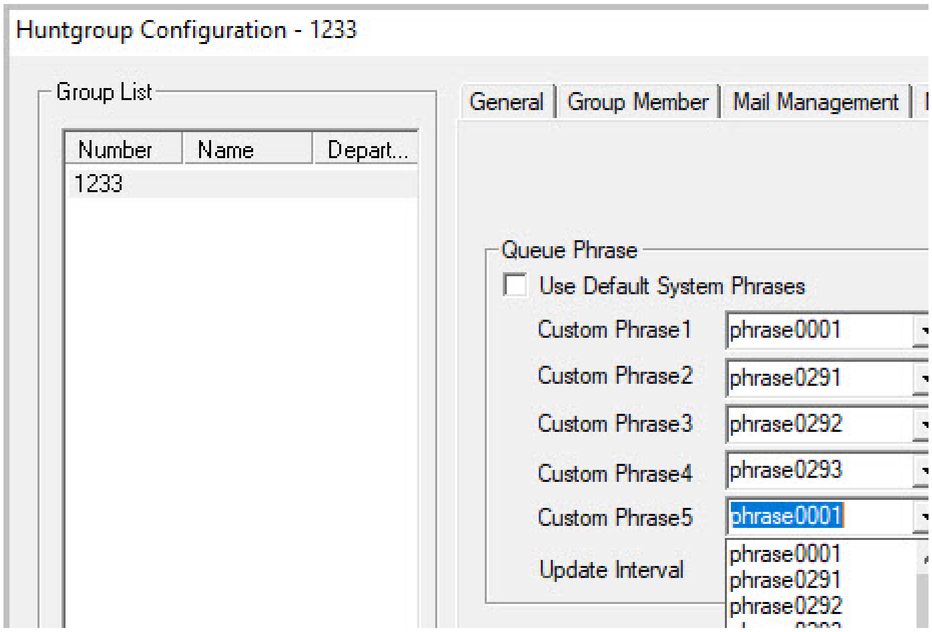
In addition, if you check the **Enable Single Call Handling for Agent** check box, the system will not send calls to an agent who puts a call on hold. If this option is not checked, the system will distribute calls to the agent even if the agent has a call on hold. In other words, this configuration determines if an agent can get multiple hunt group calls or not.

Handling Calls when Group Members Are RNA/Logged Out

You can set calls to forward to a specified destination when all group members either do not answer the call (RNA) or are logged out. To do so, in the **Group RNA/Logout Handling** section of the **Call Handling** tab, check the **Enable Forward to** check box, and select a destination from the list. The forwarding options are the same as for “Forwarding All Calls” on page 235.

Setting Queue Management Options

In the **Queue Management** tab of Huntgroup Configuration, you can specify which greetings and updates to use and you can set the update interval. For each hunt group you can either use the system default audio peripheral configuration or you can set up a custom configuration.



Huntgroup Configuration - 1233

Group List

Number	Name	Depart...
1233		

Queue Phrase

□ Use Default System Phrases

Custom Phrase1: phrase0001

Custom Phrase2: phrase0291

Custom Phrase3: phrase0292

Custom Phrase4: phrase0293

Custom Phrase5: phrase0001

Update Interval

phrase0001
phrase0291
phrase0292

Figure 152. Huntgroup Configuration, Queue Management tab

The default audio peripheral setup is discussed in “Audio Peripheral Configuration” on page 50. Setting a custom configuration in the Queue Management tab involves selecting other available phrases from the lists. Depending on how long the caller is in the queue, the caller will hear phrases 1-5, in order, after which phrase 5 will be repeated. For information about creating custom phrases, see the section Auto Attendant Configuration.

About Fax-over-IP Hunt Groups

MaxCS supports FoIP Hunt groups; there is no specific configuration type for such hunt groups.

In a FoIP hunt group, all group members must be FoIP extensions. Group queuing is not supported.

Limited FoIP group parameters are supported:

- First/Last Name, Password, Description, Department
- DID Number
- Ring First Available Member and Ring Next Available Member
- Busy Call Handling and No Answer Handling should be disabled
- Forwarding All Calls – forwarding target must be a FoIP extension or FoIP Hunt group

Configure FoIP Hunt groups as you would any other type of Hunt group; include only FoIP extensions.

CHAPTER

21

Paging Group Configuration

The IP paging group is a group of IP phones that can receive station paging. This feature also can be used as IP zone paging by creating multiple paging groups.

Note: Polycom paging groups are supported by the MaxCS Private Cloud service; Altigen paging groups are not supported by the Private Cloud service.

Paging is limited to the local LAN.

Altigen IP phone Implementation details:

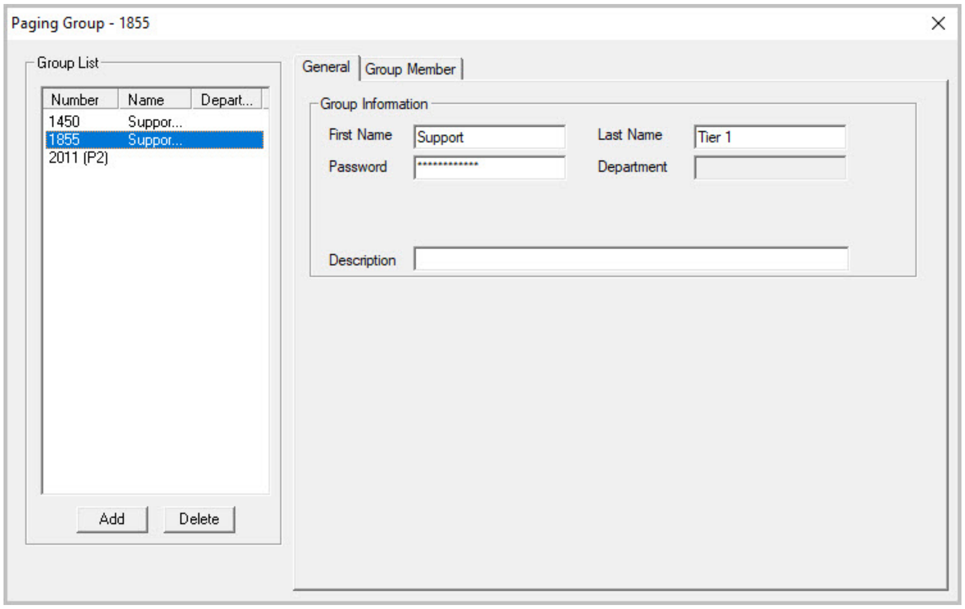
- Polycom paging groups are now supported. Polycom phones can page to Altigen paging group but cannot receive pages from Altigen paging groups. They can only receive pages from assigned Polycom paging groups. See *Polycom Paging Groups* on page 241.
- Altigen IP phone group paging uses SIP Tie-Trunk channels. Make sure that you have a sufficient number of SIP tie-trunk channels configured for group paging.
- Each paging session requires one G.711 codec channel. The voice stream is multicast to multiple IP phones on the LAN.
- Any extension (analog or IP) can initiate a paging call by dialing **#46** + the Paging Group number.
- When paged, an IP phone in idle state will automatically turn on the speaker, play a beep, and then play the page.
- When receiving an incoming call during a paging session, the IP phone will automatically stop the paging session and start ringing.
- The IP phone user can terminate a paging session by pressing the **Release** key on the phone.
- IP phones in DND mode will not be paged.

Some considerations:

- If an Altigen IP phone in a different network segment needs to be in a paging group, you need to configure intermediate routers to pass through the IP multicast packets.
- IP paging to remote IP phones over WAN is not supported.

Note: You can now set up Polycom paging groups; refer to the instructions in the *MAXCS Polycom Configuration Guide.*

To configure paging, select **PBX** > **Paging Group Configuration**.



Paging Group - 1855

Group List

Number	Name	Depart...
1450	Suppor...	
1855	Suppor...	
2011 (P2)		

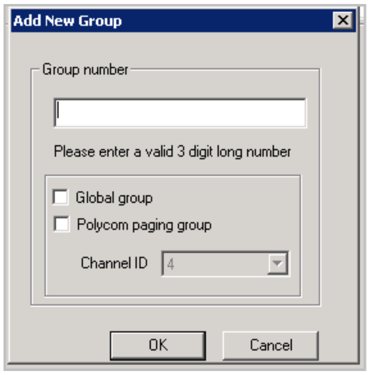
Group Information

First Name: Support
Last Name: Tier 1
Password: ************
Department:
Description:

Figure 153. Paging Group Configuration window

Setting Up a Paging Group

1. In the **Paging Group** configuration window, below the **Group List**, click the **Add** button.
2. Enter a number for the paging group.
3. Check the **Global Group** check box if you want this group to be visible to other gateways, or check **Polycom paging group** if this group is for Polycom phones. (Polycom paging groups cannot be Global groups.) Click **OK**.



Add New Group

Group number

Please enter a valid 3 digit long number

□ Global group
□ Polycom paging group

Channel ID: 4

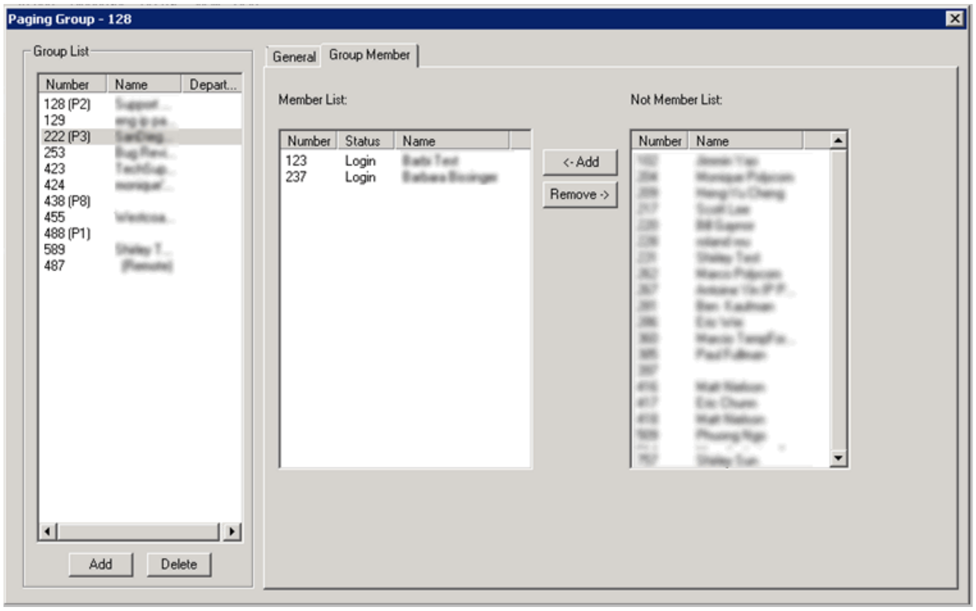
Figure 154. Paging group parameters

4. In the **Group Information** field, type in the following:

- **First Name** and **Last Name** of the paging group, each with a maximum of 32 characters.
- **Password** for the paging group. The default is the system password set on the **Number Plan** tab of the System Configuration window.
- **Description** for the paging group.

Adding Members to a Paging Group

1. On the **Group Member** tab of the Paging Group Configuration window, select the desired extension(s) in the **Not Member** list. Use **Shift**+click or **Ctrl**+click to select several extensions from the list.
2. Click the **Add** button to move them to the **Member** list.



Group List

Number	Name	Depart...
128 (P2)	[redacted]	
129	[redacted]	
222 (P3)	[redacted]	
253	[redacted]	
423	[redacted]	
424	[redacted]	
438 (P8)		
455	[redacted]	
488 (P1)		
589	[redacted]	
487	[redacted]	

Member List:

Number	Status	Name
123	Login	[redacted]
237	Login	[redacted]

Not Member List:

Number	Name
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Figure 155. Paging Group Configuration, Group Member tab

When a member is added, its default state is **Login**. Paging group members can use **#54** to perform group login or **#56** to log off. If a member is logged off, then it will not receive group paging.

Removing Members from a Paging Group

1. On the **Group Member** tab of the Paging Group Configuration window, click the extensions that you want to remove in the **Member** list.
2. Click the **Remove** button to move them to the **Not Member** List.

Polycom Paging Groups

Polycom extensions can make one-way audio announcements to other Polycom users who are in the same Polycom paging group.

There are now two different sets of Paging Groups in MaxCS:

- Polycom paging groups (paging group members must have a Polycom Advanced Features license)
- Altigen IP Phone paging groups

Polycom Paging Groups can include only users of Polycom phones who have a Polycom Advanced Features license assigned to their extension. Be aware of the following considerations while configuring Polycom Group paging for an extension:

- Polycom Paging Groups can only page subscribed Polycom phones; if you include a non-Polycom extension in a Polycom Paging Group, the phone on that extension will not play the page.

- In order to add an extension to a Polycom Paging Group, the extension must have a registered Polycom phone and it must have a Polycom Advanced Features license assigned to it.
- A total of 25 Polycom paging groups are available.
- Each Polycom Paging group must be assigned to a channel ID, 1-25. Channel IDs are shared across multiple MaxCS systems on the same network. In other words, phones subscribed to a Paging group assigned to channel 6 will receive pages for channel 6, no matter which MaxCS system sent the page.
- Polycom phones allow three paging groups to be specified, Default, Priority, and Emergency. MaxAdministrator assigns these three paging groups to channel ID 1, 24, and 25, respectively.
    - The Default group (when enabled) is always shown first in the Paging Group display.
    - A Priority group page will interrupt Normal pages or active calls.
    - An Emergency page will interrupt Normal pages, Priority pages, and active calls and plays out at near maximum volume even if Do Not Disturb (DND) is turned on.
- Polycom phones must be on the same network in order to send and receive Polycom group pages. If you add an extension to a line park group that is on a different network, then the user will not be able to receive or send pages for that paging group. In addition, if a user relocates and you move the extension to a different network, then that user will no longer be able to receive or send pages to that paging group.

Configure Polycom Paging

Once you have enabled Polycom Paging for an extension, the user can subscribe to paging groups, change the default paging group, configure whether pages play during active calls, and send pages.

To configure Polycom Paging groups,

1. In MaxAdministrator, select **PBX** > **Paging Group Configuration**.
2. Click **Add** to add a new group.
3. Enter a 4-digit number for the Paging group.
4. Check *Polycom paging group*.
5. Assign a unique paging channel ID number for the group (1-25).

Note: In the future, this channel ID number can only be removed by deleting this Paging group.

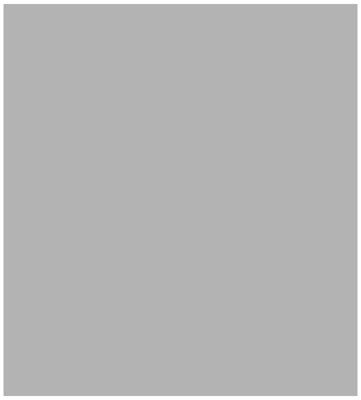
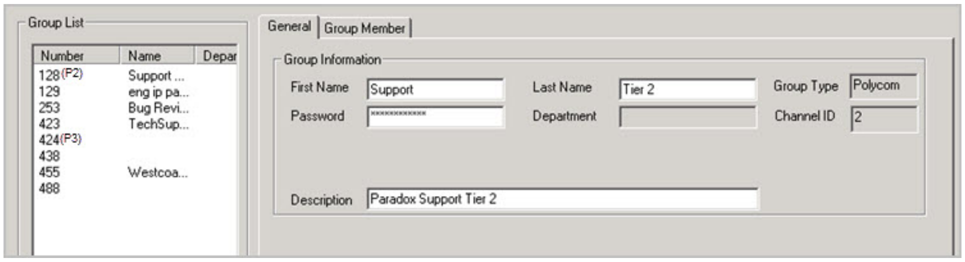


Figure 156. Add a new paging group

6. Click **OK**. You will see the new group in the Paging Group page, in the left panel. Polycom groups will show (P*x*) to the right of the number.

   Modify the group information as needed. For the First Name and Last Name fields, enter details up to a maximum of 32 characters. You can also enter a description for this group.



Group List

Number	Name	Depar
128(P2)	Support ...	
129	eng ip pa...	
253	Bug Revi...	
423	TechSup...	
424(P3)		
438		
455	Westcoa...	
488		

General | Group Member

Group Information

First Name: Support
Last Name: Tier 2
Group Type: Polycom
Password: ************
Department:
Channel ID: 2
Description: Paradox Support Tier 2

Figure 157. Enter information for the new Polycom paging group

7. To add extensions to Polycom Paging groups, select the group in the list and open the *Group Member* tab. Move extensions from the Not Member list to the Member list. Click Apply.
8. Click **Reboot affected Polycom phones**. This sends the updated configuration to any Polycom extensions that are impacted by the changes; phones with active calls will be rebooted after the call ends. After the phone reboots, the members of the paging group will see a new softkey on their Polycom phones for that paging group.

CHAPTER

22

Line Park Configuration

The Line Park feature is a kind of call park method. The main differences between Line Park and system call park are the following:

- A Line Park ID can be assigned to a specific IP phone's softkey or programmable key; the system call park cannot.
- Line Park IDs can be grouped as a Line Park Group for call routing purposes; the system call park ID is assigned by the system automatically.

The Line Park feature can be used for the following applications:

- Inbound call line appearance during business hours
- Operator parks a call for a group of IP phone users
- Executive/assistance call coverage
- Night hours call coverage
- Overflow new workgroup calls to a Line Park Group when the queue length or queue time is too long.

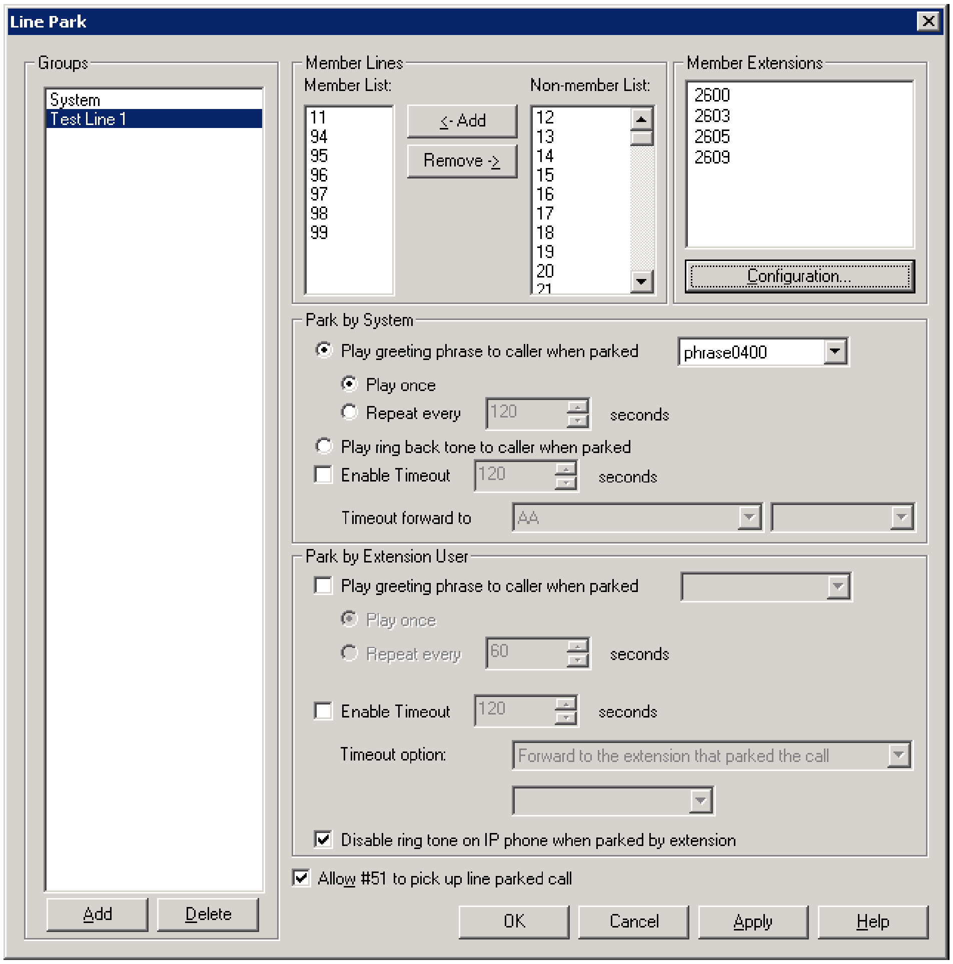
Implementation Notes

- A total of 99 (01 to 99) line IDs can be grouped into different Line Park Groups. The default "System" group cannot be removed.
- One Line Park ID can belong to only one group.
- A Line Park Group can be assigned to:
  - Trunk In-Call Routing
  - Extension/Workgroup Busy or RNA Handling
  - Extension/Workgroup Forwarding
  - Workgroup Quit Queue Option
- Extensions can be assigned as members of Line Park Groups, allowing the extension users to see and pick up a parked call from those groups in the **LinePark** tab of their MaxCommunicator or MaxAgent.
- The system will put the caller in queue when calls exceed the total lines assigned to the Line Park Group.
- The park line is released when the call disconnects, is answered, or is forwarded due to time out.

Note: You can configure Line Park slots for Polycom phones; refer to the instructions in the *MAXCS Polycom Configuration Guide*.

Configuring Line Park

To configure line park, select **PBX** > **Line Park Configuration**.



Groups: System, Test Line 1

Member List: 11, 94, 95, 96, 97, 98, 99

Non-member List: 12, 13, 14, 15, 16, 17, 18, 19, 20, 21

Member Extensions: 2600, 2603, 2605, 2609

Park by System

● Play greeting phrase to caller when parked phrase0400

● Play once

○ Repeat every 120 seconds

○ Play ring back tone to caller when parked

☐ Enable Timeout 120 seconds

Timeout forward to AA

Park by Extension User

☐ Play greeting phrase to caller when parked

● Play once

○ Repeat every 60 seconds

☐ Enable Timeout 120 seconds

Timeout option: Forward to the extension that parked the call

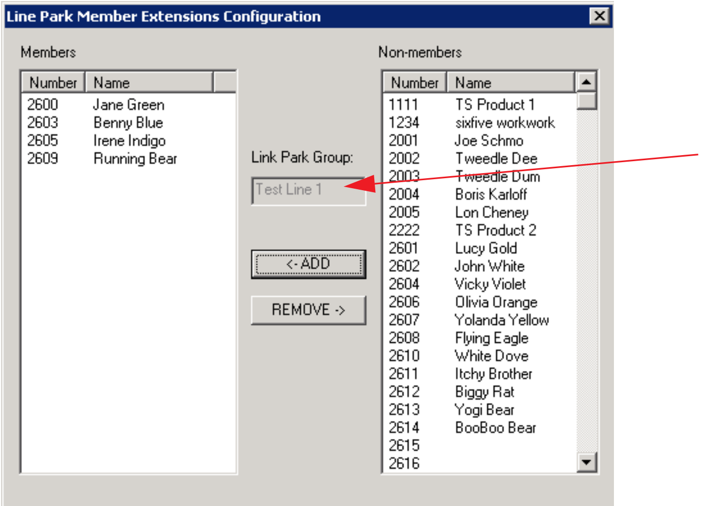
☑ Disable ring tone on IP phone when parked by extension

☑ Allow #51 to pick up line parked call

Figure 158. Line Park Configuration window

Setting Up a Line Park Group

1. In the **Line Park Configuration** window, click the **Add** button below the **Groups** list.
2. Enter a name in the dialog box, and click **OK**.
3. Select line ID numbers from the **Non-Member List** and click the **Add** button to add them to the **Member List**.
4. To assign extensions to a group, select the group, and then click the **Configuration** button below the Member Extensions panel.



Members

Number	Name
2600	Jane Green
2603	Benny Blue
2605	Irene Indigo
2609	Running Bear

Link Park Group: Test Line 1

Non-members

Number	Name
1111	TS Product 1
1234	sixfive workwork
2001	Joe Schmo
2002	Tweedle Dee
2003	Tweedle Dum
2004	Boris Karloff
2005	Lon Cheney
2222	TS Product 2
2601	Lucy Gold
2602	John White
2604	Vicky Violet
2606	Olivia Orange
2607	Yolanda Yellow
2608	Flying Eagle
2610	White Dove
2611	Itchy Brother
2612	Biggy Rat
2613	Yogi Bear
2614	BooBoo Bear
2615	
2616	

The name of the selected group appears here

Figure 159. Configuring a Line Park group's member extensions

5. Select members for this Line Park group from the Non-Members list, and click the **Add** button to move them to the Members list.

   Members of a Line Park group can use their MaxCommunicator or MaxAgent applications to see and pick up calls parked for this group.

   Any extension can park a call to any group. Any extension can pick up a call from any group using #51 followed by the line park location, if allowed by MaxAdministrator configuration.

6. Configure the following options:

   Park by System:

   - **Play greeting phrase to caller when parked** – Select this option to have the system play the greeting phrase you select from the box, before playing music on hold. Specify whether to play the greeting once only, or every x seconds.
   - **Play ring back tone to caller when parked** – Select this option when you want the caller to hear a ring back tone if the call has not been answered by any extension or voice mail. If the call is answered and parked, the caller will hear a greeting phrase and on-hold music.
   - **Enable Timeout** – When you check this box, a line park call will time out after the number of seconds set in the value box. Use the **Timeout forward to** boxes to route the call to an AA, voice mail, or an extension/group.

   Park by Extension User:

   - **Play greeting phrase to caller when parked** – Select this option to have the system play the greeting phrase you select from the box, before playing music on hold. Specify whether to play the greeting once only, or every x seconds.
   - **Enable Timeout** – Check this box to specify, in seconds, when a line park call will time out. Use the **Timeout option** boxes to forward the call to the extension that parked the call, alert the extension that parked the call, or forward the call to an AA, voice mail, or an extension/group.
   - **Disable ring tone on IP phone when parked by extension** – Check this box to prevent a line-parked call from ringing again while it is parked. (This feature is not supported on Polycom phones.)

Note: The IP phone's programmable key or softkey will be blinking when a call is parked at a line ID that is configured to the phone.

If the associated programmable key has Play Tone function turned on and a ring tone is configured, at the Altigen IP phone (in idle state) the user will hear a ring tone when a call is parked.

- **Allow #51 to pick up** – when this check box is checked, it allows a user to pick up parked calls from a phone set using **#51**, followed by the Park Line ID.

Deleting a Line Park Group

1. In the **Line Park Configuration** window, select a Line Park Group from the **Groups** list.
2. Click the **Delete** button below the **Groups** list.

CHAPTER

23

Workgroup Configuration

The workgroup is an automatic call distribution (ACD) feature designed to enhance customer service operations with queuing, distribution, agent management, real-time status, and call logging capability.

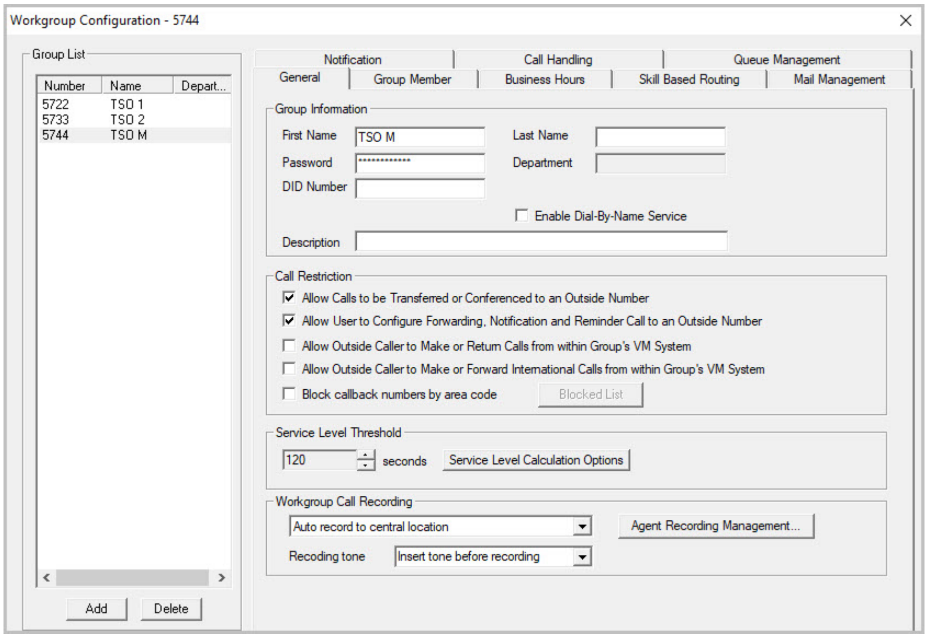
You can configure up to 128 groups, including workgroups, hunt groups, and paging groups.

When adding members to a workgroup, the following rules apply:

- Concurrent login agent seat license is required.
- One agent login to multiple workgroups requires only one license.

Creating and Configuring Workgroups

To open the Workgroup Configuration window, select **Call Center** > **Workgroup Configuration**.



Number	Name	Depart...
5722	TSO 1	
5733	TSO 2	
5744	TSO M	

Group Information

First Name: TSO M
Last Name:
Password: ************
Department:
DID Number:
☐ Enable Dial-By-Name Service
Description:

Call Restriction

☑ Allow Calls to be Transferred or Conferenced to an Outside Number
☑ Allow User to Configure Forwarding, Notification and Reminder Call to an Outside Number
☐ Allow Outside Caller to Make or Return Calls from within Group's VM System
☐ Allow Outside Caller to Make or Forward International Calls from within Group's VM System
☐ Block callback numbers by area code

Service Level Threshold

120 seconds

Workgroup Call Recording

Auto record to central location

Recoding tone: Insert tone before recording

Figure 160. Workgroup Configuration window, General tab

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

Overview of Workgroup Configuration Window

These are the tabs in the Workgroup Configuration window:

- **General** – Create workgroup pilot numbers, group descriptions, service level threshold and call recording options.
- **Group Member** – Add or remove members from workgroups
- **Business Hours** – Set business hours for workgroups
- **Skill Based Routing** – Define skill levels and skill-based routing rules.
- **Mail Management** – Set capacity and features options for extension mailboxes.
- **Notification** – Set preferences and options for voice mail notifications.
- **Call Handling** – Set call forwarding, call waiting, and call handling preferences and options.
- **Queue Management** – Set queue phrases, overflow routing, queue announcements, and callback from queue options.
- **Call Disposition** - Select which call disposition codes apply to each workgroup. You can also specify, for each workgroup, whether disposition codes are required or optional. See *Call Disposition Codes* on page 290 for full details.

Apply to Button

The Workgroup Configuration window often allows you to apply changes to a particular workgroup or to select many workgroups to which to apply the changes.

Clicking the **Apply to** button opens a list of all workgroups to which the change can apply. All workgroups are selected by default. You then de-select the ones you don’t want, or de-select all and then select the ones you want. Note that you cannot use the mouse to drag over and select multiple items; you must use the **Shift** and **Ctrl** keys.

The **Apply to** button is disabled unless there is a change that can be applied to multiple workgroups, and when you use it to apply changes to multiple workgroups, it works on only those changed attributes that can be applied.

Setting Up Workgroups

Set up new workgroups in the Workgroup Configuration window.

To create a workgroup,

1. Click the **Add** button under the **Group List**.
2. Type in a group number for the workgroup.
3. Check the **Global group** check box if you want the group to be visible to other gateways. Click **OK**.

Establishing Basic Workgroup Attributes

After you create a workgroup, you can set basic attributes on the Workgroup Configuration **General** tab.

- **First Name** and **Last Name** – Each with a maximum of 32 characters.
- **Password** – The default is the system default password set on the **Number Plan** tab of the System Configuration window.

  A valid password cannot be the same as its workgroup number and must be 4 - 8 digits (numbers or letters A - Z) in length. Basic password patterns, such as repeated digits (1111), consecutive digit strings (1234), or digits that match the extension (Ext. **101** using **101**2, 9**101**, **101**01, etc.) are not recommended. The letters map to numbers (on a phone, for example) as follows:

Numbers	Letters	Numbers	Letters
2	A, B, C, a, b, c	6	M, N, O, m, n, o
3	D, E, F, d, e, f	7	P, Q, R, S, p, q, r, s
4	G, H, I, g, h, i	8	T, U, V, t, u, v
5	J, K, L, j, k, l	9	W, X, Y, Z, w, x, y, z

- **Department** – The department associated with this workgroup.
- **DID Number** – Each workgroup can be assigned a DID number. This number does not have a fixed length, but the length must be long enough (range 2 - 16) for the system to match the DID incoming call.
- **Enable Dial-By-Name Service** – Check this box to allow callers to search the list by employee name for this workgroup extension.
- **Description** – Describe the purpose of this workgroup.

Setting Call Restrictions

The call restriction rules on the **General** tab apply to users making outbound calls from within voice mail and several workgroup settings. These settings do not impact the call restriction settings configured for the workgroup member's extension in Extension Configuration.

- **Allow Calls to be Transferred or Conferenced to an Outside Number** – When checked, the internal extension user can log into this workgroup voice mail, make a call to a second party, then transfer or conference to a third party.
- **Allow User to Configure Forwarding, Notification, and Reminder Call to an Outside Number** – This setting regulates workgroup call forwarding, voice mail notification, and reminder call configuration. If this setting is not checked, you will see a warning message pop up when trying to set up forwarding to an outside number. International calls are not allowed if the fourth option is not checked.
- **Allow Outside Caller to Make or Return Calls from within Group's VM System** – When checked, an outside caller can dial into the system, log in to workgroup voice mail, and make or return calls from the group's voice mail (Zoomerang feature). International calls are not allowed if the fourth option is not checked.
- **Allow Outside Caller to Make or Forward International Calls from within the Group's VM system** – This setting regulates making international calls from voice mail and forwarding to an international number.
- **Block callback number by area code** – see the discussion on page 284.

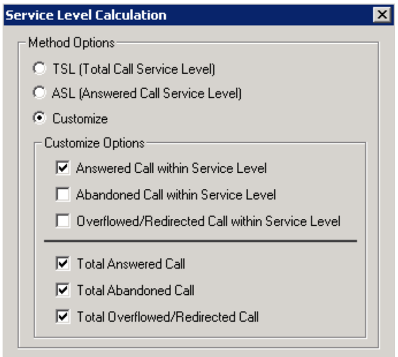
Caution! Allowing any of these options may increase the potential for toll fraud. Make sure the password is properly configured to prevent an intruder from using this voice mail box to make an outbound call. Altigen recommends that you leave the fourth option unchecked for all workgroups at all times.

Service Level Threshold

The **Service Level Threshold** scroll box allows you to select the length of time in seconds that a call can be in queue before the call is logged in workgroup performance statistics as having exceeded the allowable service level limits. You can set the value to any number between 1 - 1200 seconds.

Service level is a service quality index which calculates the percentage of calls serviced within a defined threshold for the defined period of time. The term "serviced" may not necessarily mean answered. You can define the calculation method based on your operation requirements. The service level percentage is calculated from midnight 00:00 am. and is reset daily. The calculated number will be output to the MaxAgent and MaxSupervisor applications.

The **Service Level Calculations Options** button opens the following dialog box.



Service Level Calculation

Method Options

○ TSL (Total Call Service Level)

○ ASL (Answered Call Service Level)

● Customize

Customize Options

☑ Answered Call within Service Level

☐ Abandoned Call within Service Level

☐ Overflowed/Redirected Call within Service Level

☑ Total Answered Call

☑ Total Abandoned Call

☑ Total Overflowed/Redirected Call

Figure 161. Service Level Calculation dialog box

In the **Method Options** section, select one of the following:

- **TSL** (Total Call Service Level) – The service level calculation is: TSL% = Total WG inbound calls within SLT / Total WG inbound calls. This is the default option.
- **ASL** (Answered Service Level) – The service level calculation is: ASL% = Total WG inbound calls answered within SLT / Total WG inbound calls.
- **Customize** – Use the check boxes to enable at least *one* of the following three options:
  - **Answered Calls within Service Level**
  - **Abandoned Calls within Service Level**
  - **Overflowed/Redirected Calls within Service level**

  divided by at least one of the following three options:
  - **Total Answered Calls**
  - **Total Abandoned Calls**
  - **Total Overflowed/Redirected Calls**

Workgroup Recording Options

The system administrator can specify the following *workgroup* call recording options for a workgroup:

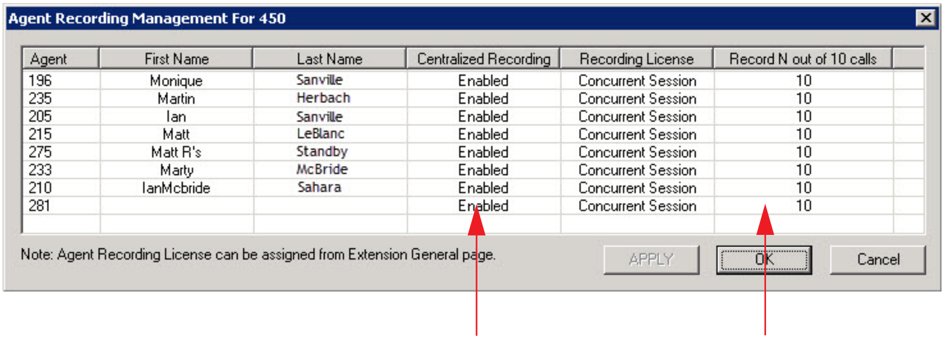
Warning! Listening in to or recording a conversation without the consent of one or both parties may be a violation of local, state and federal privacy laws. It is the responsibility of the users of this feature to assure they are in compliance with all applicable laws.

- **Disable** – No call recording.
- **Auto record to central location** – Records all workgroup inbound and outbound calls, which are saved to a central location (defined in Recording Configuration on the **System** menu – see *Call Recording Configuration*); this option requires that either a shared Concurrent Recording Session license is available or that a Dedicated Recording Seat license is assigned to each workgroup member (configured in Extension Configuration).

- **Record on demand to central location** – Records calls on demand, which are saved to a central location (defined in Recording Configuration on the **System** menu – see *Call Recording Configuration*); this option requires that either a shared Concurrent Recording Session license is available or that a dedicated Recording Seat license is assigned to each workgroup member (configured in Extension Configuration).
- **Record on demand to extension VM** – Records calls on demand, which are saved to the agent's voicemail box.

  Note: When retrieving voice mail as an e-mail, if the voice mail file has a recorded file attached, the recorded file is not forwarded in the e-mail.
- **Insert Recording Tone** – Plays a recording beep to alert the parties that the conversation is being recorded, then plays a periodic recording alert tone. The tone is recorded together with the conversation.
- **Record X out of 10 calls** – If recording to a central location, automatically records incoming and outgoing *workgroup* calls, as specified. (The default is to record all workgroup calls.)

  To see this option, click the **Agent Recording Management** button.

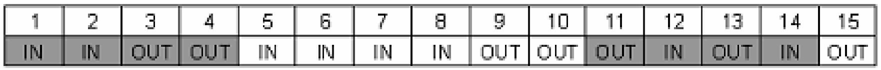


Agent	First Name	Last Name	Centralized Recording	Recording License	Record N out of 10 calls
196	Monique	Sanville	Enabled	Concurrent Session	10
235	Martin	Herbach	Enabled	Concurrent Session	10
205	Ian	Sanville	Enabled	Concurrent Session	10
215	Matt	LeBlanc	Enabled	Concurrent Session	10
275	Matt R's	Standby	Enabled	Concurrent Session	10
233	Marty	McBride	Enabled	Concurrent Session	10
210	IanMcbride	Sahara	Enabled	Concurrent Session	10
281			Enabled	Concurrent Session	10

Note: Agent Recording License can be assigned from Extension General page.

You can change these values

For each agent you can change the option **Record N out of 10 calls**. For example, if you set to record 4 out of 10 calls, the 1st-4th and 11th-14th, and so on, will be recorded. Using this example, in the following table the shaded calls will be recorded:



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
IN	IN	OUT	OUT	IN	IN	IN	IN	OUT	OUT	OUT	IN	OUT	IN	OUT

To change **Record N out of 10 calls** for an agent, click the cell you want to change, and make a selection from the list. Click **Apply**. When finished, click **OK**.

- **Centralized Recording** – You can also enable or disable centralized recording from the Agent Management Recording window shown above. Click the cell you want to change, and make a selection from the list. Click **Apply**. When finished, click **OK**.

  Notes:

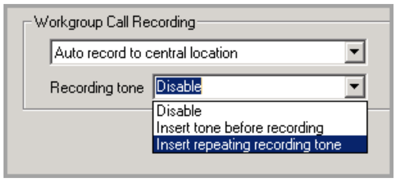
  - The recording session starts when the call enters the connected state and ends when hang up or flash is pressed, or when the call is transferred.
  - The recording setting at **Extension Configuration** applies only to *non-workgroup* calls. The recording setting at **Workgroup Configuration** applies only to *workgroup* calls. To allow an agent to record all calls (*non-workgroup* and *workgroup*), both recording settings must be enabled.
  - When an agent logs in to a workgroup, which is also an outbound workgroup, all outbound calls will be considered as workgroup calls and recorded according to workgroup configuration.
  - When an agent logs in to a workgroup and is in Not Ready, DND, Wrap-up, or Inter-call Delay state, outbound calls will be recorded if workgroup recording is configured.
  - When an agent does not log in to the workgroup that is configured as an outbound workgroup, all outbound calls are non-workgroup calls.

Recording Tone Options

When you select to record conversations, you can have the system insert a repeating recording tone.

On the General tab of the *Workgroup Configuration* window, set *Recording Tone* to **Insert repeating recording tone**.

With MaxCS systems, the repeating tone is only available if one channels in use is SIP. With two TDM channels, there can be no repeating tones.



Workgroup Call Recording

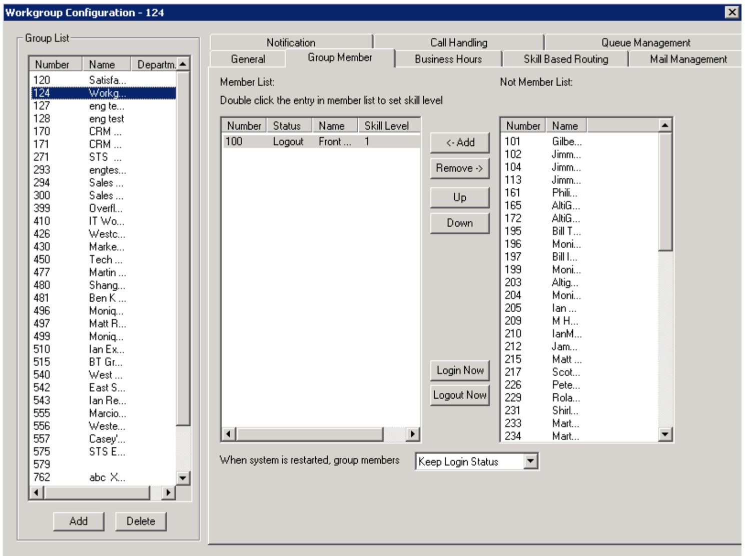
Auto record to central location

Recording tone: Disable

Figure 162. The Repeating recording tone option

Establishing Workgroup Membership

Add agent extensions to a workgroup on the **Group Member** tab in the Workgroup Configuration window.



Workgroup Configuration - 124

Group List

Number	Name	Departm.
120	Satisfa...	
124	Workg...	
127	eng te...	
128	eng test	
170	CRM ...	
171	CRM ...	
271	STS ...	
293	engtes...	
294	Sales ...	
300	Sales ...	
399	Overfl...	
410	IT Wo...	
426	Westc...	
430	Marke...	
450	Tech ...	
477	Martin ...	
480	Shang...	
481	Ben K ...	
496	Moniq...	
497	Matt R...	
499	Moniq...	
510	Ian Ex...	
515	BT Gr...	
540	West ...	
542	East S...	
543	Ian Re...	
555	Marcio...	
556	Weste...	
557	Casey'...	
575	STS E...	
579		
762	abc X...	

Member List:

Double click the entry in member list to set skill level

Number	Status	Name	Skill Level
100	Logout	Front ...	1

Not Member List:

Number	Name
101	Gilbe...
102	Jimm...
104	Jimm...
113	Jimm...
161	Phili...
165	AltiG...
172	AltiG...
195	Bill T...
196	Moni...
197	Bill I...
199	Moni...
203	Altig...
204	Moni...
205	Ian ...
209	M H...
210	IanM...
212	Jam...
215	Matt ...
217	Scot...
226	Pete...
229	Rola...
231	Shirl...
233	Mart...
234	Mart...

When system is restarted, group members: Keep Login Status

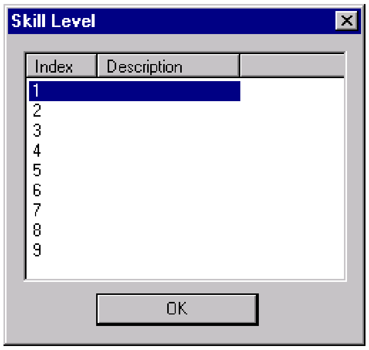
Figure 163. Workgroup Configuration, Group Member tab

To add extension(s) to a workgroup,

1. Select the workgroup in the **Group List**.
2. On the **Group Member** tab, click the extension number(s) in the **Not Member** list. Use **Shift**+click and **Ctrl**+click to select several extensions.
3. Click the **Add** button between the columns to move them to the **Member** list.

   Note: If the workgroup pilot extension is configured to Ring All Available Members, the maximum number of members is 20. See "Setting Call Handling Options" on page 265 for details.

   By default, a newly added member has the **Skill Level** set to 1.
4. To change the **Skill Level** designation for a member, double-click the member in the **Member List**. The Skill Level dialog box opens. (Skill Levels are defined in "Skill Based Routing" on page 256.)



Skill Level

Index	Description
1	
2	
3	
4	
5	
6	
7	
8	
9	

Figure 164. Skill Level dialog box

5. Click the desired Skill Level **Index**, then click **OK**.

Agents who are members of more than one workgroup can have a different skill level assigned in each group.

To remove extension(s) from a workgroup,

1. Click the extension number(s) in the **Member** list.
2. Click **Remove** to move them to the **Not Member** list.

Log In/Out a Group Member

An administrator can log in or log out a group member, by selecting the member in the Member List and clicking the **Login Now** or **Logout Now** button.

Setting Login Status for System Restart

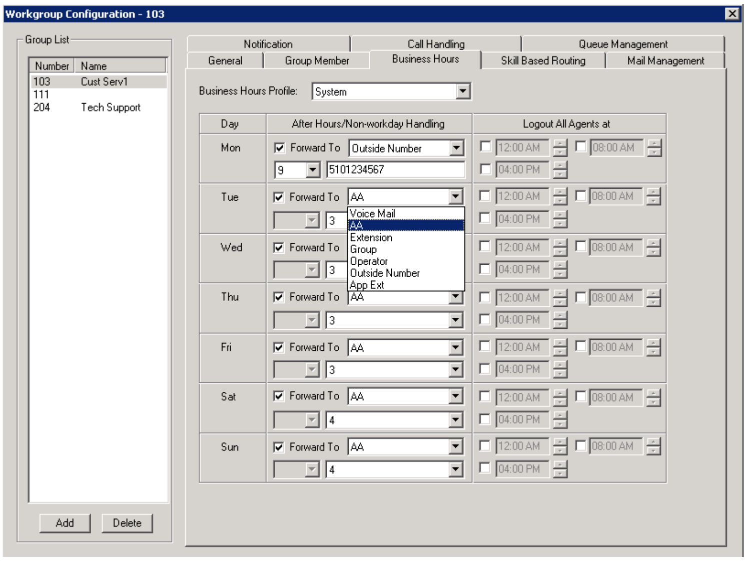
Whenever the system is restarted, the administrator can use the list at the bottom of the **Group Member** tab to:

- **Keep Login Status** – All group members retain their original login status for that group prior to restart (default setting)
- **All Logout** – All group members are logged out of the workgroup when the system is restarted.

Setting Business Hours

Settings on the **Business Hours** tab in the Workgroup Configuration window define how after-hours calls are handled for workgroups. An administrator can assign a Business Hours profile to a group, and also configure after-hours handling for each day of the week.

To set after-hours call handling, select the workgroup you want to work with from the **Group List** in the Workgroup Configuration window, then click the **Business Hours** tab.



Group List

Number	Name
103	Cust Serv1
111	
204	Tech Support

Business Hours Profile: System

Day	After Hours/Non-workday Handling	Logout All Agents at
Mon	☑ Forward To Outside Number 9 5101234567	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Tue	☑ Forward To AA 3	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Wed	☑ Forward To 3	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Thu	☑ Forward To AA 3	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Fri	☑ Forward To AA 3	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Sat	☑ Forward To AA 4	□ 12:00 AM □ 08:00 AM □ 04:00 PM
Sun	☑ Forward To AA 4	□ 12:00 AM □ 08:00 AM □ 04:00 PM

Figure 165. Workgroup Configuration, Business Hours tab

Set the business schedule parameters as follows:

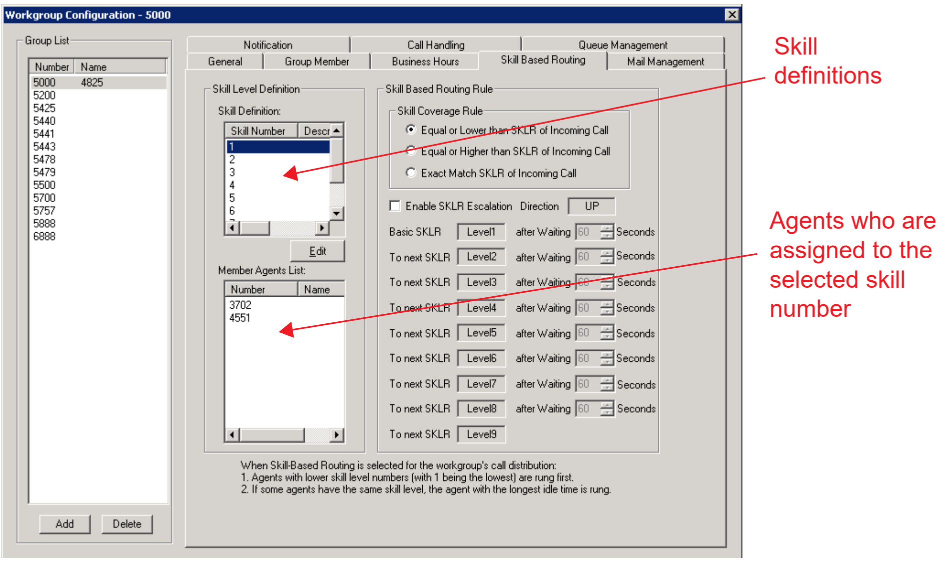
Workgroup Business hours Parameter	Description
Business Hour	Use the list to select a Business Hours profile to apply to the workgroup (profiles are configured in the System Configuration window - see “Setting Business Hours” on page 38).
After Hours/Non-Workday Handling	• For each day of the week, select a **Forward To** option for call handling after hours or for non-workdays: • To **Voice Mail** • To **AA** – Select the auto attendant to use in the list under the option. AAs are configured in the AA Configuration window, available from the **System** menu. • To an **Extension** – Select an extension from the list. • To a **Group** – Select a group from the list. • To the **Operator** • To an **Outside Number** – If you choose **Outside Number**, select a trunk or route access code to use in the small list on the left, and type in the full prefix and phone number. • To an **App Ext** – When used in conjunction with a third party notification application, the **App Ext** feature enables an extension to connect to an application that can receive the notification event; use the list to choose the log- on extension to which the third party application is connected. Contact your local Altigen Partner for more information on using this feature.
Logout All Agents At	For each day of the week, you can select up to three time periods for the system to automatically log out agents.

Skill Based Routing

If you want to set up skill-based routing, you can more closely match a customer’s call to an agent who has the skills needed to handle that customer’s issue.

Skill-based routing can increase customer issue resolution on the first call, lower the abandoned call rate, and in turn increase customer satisfaction.

The **Skill Based Routing** tab in the Workgroup Configuration window lets you define up to nine different levels of skill needed to handle the variety of a workgroup's calls.



Group List

Number	Name
5000	4825
5200	
5425	
5440	
5441	
5443	
5478	
5479	
5500	
5700	
5757	
5888	
6888	

Skill Level Definition

Skill Definition:

Skill Number	Descr
1	
2	
3	
4	
5	
6	

Member Agents List:

Number	Name
3702	
4551	

Skill Based Routing Rule

Skill Coverage Rule

● Equal or Lower than SKLR of Incoming Call
○ Equal or Higher than SKLR of Incoming Call
○ Exact Match SKLR of Incoming Call

□ Enable SKLR Escalation Direction UP

Basic SKLR	Level1	after Waiting	60	Seconds
To next SKLR	Level2	after Waiting	60	Seconds
To next SKLR	Level3	after Waiting	60	Seconds
To next SKLR	Level4	after Waiting	60	Seconds
To next SKLR	Level5	after Waiting	60	Seconds
To next SKLR	Level6	after Waiting	60	Seconds
To next SKLR	Level7	after Waiting	60	Seconds
To next SKLR	Level8	after Waiting	60	Seconds
To next SKLR	Level9			

When Skill-Based Routing is selected for the workgroup's call distribution:
1. Agents with lower skill level numbers (with 1 being the lowest) are rung first.
2. If some agents have the same skill level, the agent with the longest idle time is rung.

Skill definitions

Agents who are assigned to the selected skill number

Figure 166. *Workgroup Configuration, Skill Based Routing tab*

Skill number 1 could define the most basic skill and level 9 the most advanced, or vice versa. Or the skill numbers can be used in any other way that works for the way your company does business.

After skill numbers have been defined on this tab, each agent in the workgroup should be assigned a skill number, according to that agent's knowledge and ability, on the **Group Member** tab.

Incoming calls can be set to ring agents according to skill number, thus more closely directing the caller to an available agent qualified enough to help the caller, but ideally not *over*-qualified. You can determine the skill required by the caller and set the SKLR number in several places:

- The auto attendant, depending on the caller's responses (see "Configuring Menu Items" on page 64)
- The DNIS number the caller dialed, depending on how you have set up your DNIS numbers (see "Defining DNIS Routing" on page 154)
- The caller ID (see "Defining Caller ID Routing" on page 152)
- The Advanced Call Router – You can define SKLR in each rule entry in the Call Router, and if the Call Router routes a call, SKLR will be set.
- In the SDK – A call's SKLR can be set in some modules, and now, we just support APC interface, that is if a call is connected to an App Ext, this App Ext can set or change the call's SKLR

You can set rules on the **Skill Based Routing** tab to allow all calls coming into a workgroup to be handled by agents with a lower skill number or a higher skill number than is set for a call. And you can set time-based rules that alter the call's SKLR to allow either less able agents or over-qualified agents to handle a call so that the caller does not have to wait for an excessive period of time.

Note: For the settings configured on the **Skill Based Routing** tab to take effect, you must select the **Skill-Based Routing** option on the **Call Handling** tab of the Workgroup Configuration window (*see "Setting IntraGroup Call Distribution" on page 268*).

Operational Limitation

When configuration Skill based routing, be aware of a known operational limitation with queue announcements. If the announcement is shorter than the escalation time, then the system escalates the call at the end of the announcement instead of waiting for the escalation time to expire.

Defining Skills for a Workgroup

1. Select a workgroup in the **Group List**.
2. Double-click a skill number in the **Skill Definition** list, or select a skill number and click the **Edit** button.
3. In the **Skill Level Name** dialog box, enter the skill name in the **Description** field, then click **OK**.

The description appears in the **Skill Definition** list for that skill number.

Setting Rules for Skill Based Routing

The **Skill Coverage Rule** on the **Skill Based Routing** tab establishes the pool of agents who can handle a particular workgroup call, based on the SKLR setting for that call. The group may comprise:

- Only agents assigned that skill number
- Agents with a given skill number and lower
- Agents with a given skill number and higher

This setting must be configured.

To further help ensure that a workgroup is handling calls in a timely manner, you can specify how many seconds a caller can be in queue before opening the call to agents with the next skill number up or the next skill number down, in successive steps.

To set skill-based routing rules,

1. In the Workgroup Configuration window, **Skill Based Routing** tab, select the workgroup for which you want to set the rules.
2. Select a Skill Coverage Rule
   - **Exact Match SKLR of Incoming Call**

     Only agents whose skill number matches the SKLR of the incoming call can answer the call. For example, if you have three callers with SKLR equal to 2 in the workgroup queue, and all agents with skill level 2 are busy, and there are agents with skill level 1 and 3 who are idle, the system will keep the callers in queue waiting for an agent with skill level 2 to be available.
   - **Equal or Lower than SKLR of Incoming Call**

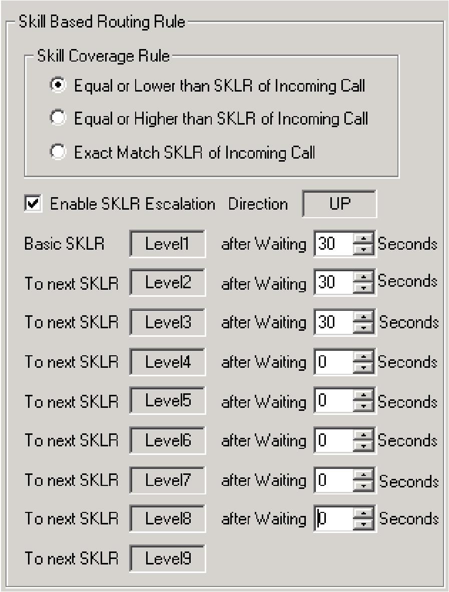
     Any agent whose skill number is equal to or lower than the SKLR of the incoming call may handle this call. Agents with the lowest skill number are rung first. With this option, that would be agents whose skill number is 1. Set the SKLR (see Skill Based Routing) as if you were setting a ceiling on the resources you are willing to use for this type of call. For example, you can set a regular call's SKLR to 1 and a preferred customer's SKLR to 3. Calls from preferred customers can be answered by agents with skill level 3, 2, and 1 while regular calls can only be answered by agents with skill level 1.
   - **Equal or Higher than SKLR of Incoming Call**

     Any agent whose skill number is equal to or higher than the SKLR of the incoming call may handle this call. Agents with the lowest skill number are rung first. With this option, that would be agents whose skill number matches the SKLR. Set the SKLR (see “Skill Based Routing” on page 256) as if you were setting a minimum skill level requirement for the call. For example, say a technical support group has agents with skill level 1 (beginner), 2 (intermediate), and 3 (expert). If you select the “Equal or Higher” option, calls with SKLR 2 will be queued for an agent with skill level 2 or 3.
3. To increase coverage of calls, check the **Enable SKLR Escalation** check box. (This check box is available if you selected the **Equal or Lower** option or the **Equal or Higher** option.)

4. For each level, specify the number of seconds a call can be in queue before the system will include the next level of agents in the pool of agents who may handle the call. Either use the Up/Down arrows or type in a number from 1-999.

Skill Based Routing Examples

Example 1: Coverage rule is **Equal or Lower** and **Enable SKLR Escalation** is checked.



Skill Based Routing Rule

Skill Coverage Rule

● Equal or Lower than SKLR of Incoming Call

○ Equal or Higher than SKLR of Incoming Call

○ Exact Match SKLR of Incoming Call

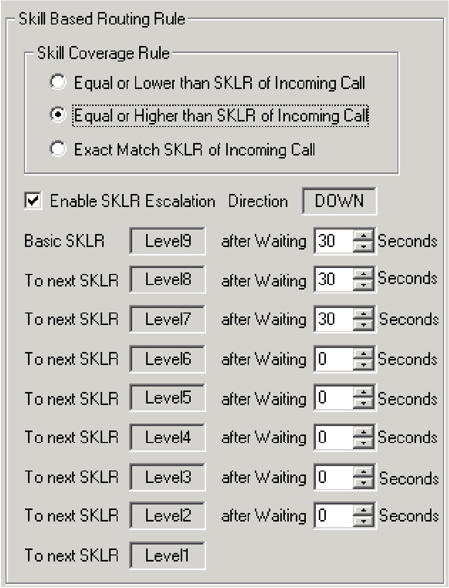
☑ Enable SKLR Escalation Direction UP

Basic SKLR	Level1	after Waiting	30	Seconds
To next SKLR	Level2	after Waiting	30	Seconds
To next SKLR	Level3	after Waiting	30	Seconds
To next SKLR	Level4	after Waiting	0	Seconds
To next SKLR	Level5	after Waiting	0	Seconds
To next SKLR	Level6	after Waiting	0	Seconds
To next SKLR	Level7	after Waiting	0	Seconds
To next SKLR	Level8	after Waiting	0	Seconds
To next SKLR	Level9			

The above configuration means:

1. When a caller with SKLR 1 is waiting in queue for 30 seconds, the caller's SKLR will be escalated to 2. Agents with skill levels 1 and 2 are able to handle the call.
2. If the caller stays in queue for more than 60 seconds, the caller's SKLR will be escalated to 3. Agents with skill levels 1, 2, and 3 are able to handle the call.
3. If the caller stays in queue for more than 90 seconds, the caller's SKLR will be escalated to 9 because all other escalation wait times are set to 0 seconds. The call will be distributed any idle agent in the workgroup.

Example 2: Coverage rule is **Equal or Higher** and **Enable SKLR Escalation** is checked.



Skill Based Routing Rule

Skill Coverage Rule

○ Equal or Lower than SKLR of Incoming Call

● Equal or Higher than SKLR of Incoming Call

○ Exact Match SKLR of Incoming Call

☑ Enable SKLR Escalation Direction DOWN

Basic SKLR	Level9	after Waiting	30	Seconds
To next SKLR	Level8	after Waiting	30	Seconds
To next SKLR	Level7	after Waiting	30	Seconds
To next SKLR	Level6	after Waiting	0	Seconds
To next SKLR	Level5	after Waiting	0	Seconds
To next SKLR	Level4	after Waiting	0	Seconds
To next SKLR	Level3	after Waiting	0	Seconds
To next SKLR	Level2	after Waiting	0	Seconds
To next SKLR	Level1			

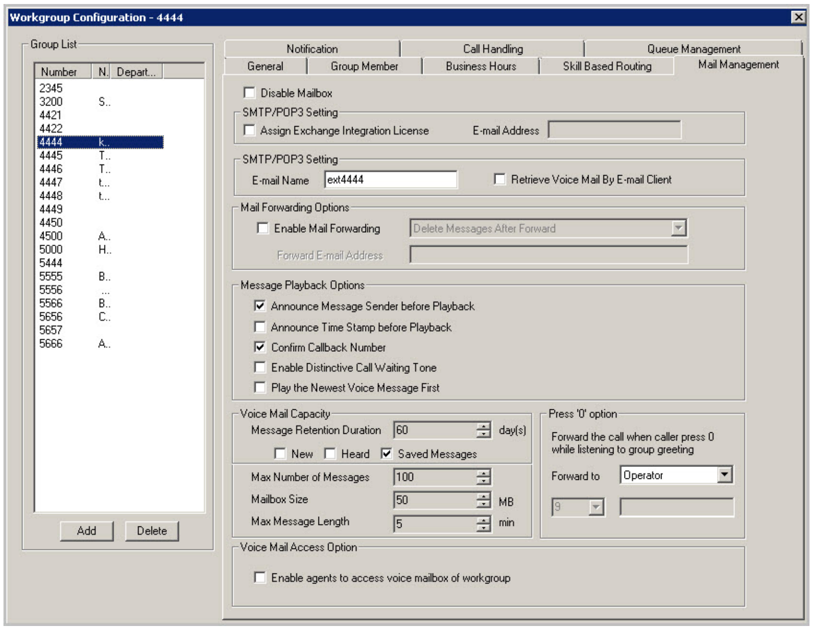
The above configuration means:

1. When a caller with SKLR 9 waiting is in queue for 30 seconds, the caller's SKLR will be changed to 8. Agents with skill level 8 and 9 are able to handle the call.
2. If the caller stays in queue for more than 60 seconds, the caller's SKLR will be changed to 7. Agents with skill level 7, 8, and 9 are able to handle the call.
3. If the caller stays in queue for more than 90 seconds, the caller's SKLR will be escalated to 1 because all other escalation wait times are set to 0 seconds. The call will be distributed to any idle agent in the workgroup.

Setting Workgroup Mail Management

The Mail Management settings define how voice messages are handled for a workgroup, including how messages are announced and processed, and how much capacity is allotted to message storage.

To work with mail management settings, click the **Mail Management** tab, and select the workgroup number you want to work with from the **Group List**.



Group List

Number	N.	Depart...
2345		
3200	S..	
4421		
4422		
4444	k..	
4445	T..	
4446	T..	
4447	t...	
4448	t...	
4449		
4450		
4500	A..	
5000	H..	
5444		
5555	B..	
5556	...	
5566	B..	
5656	C..	
5657		
5666	A..	

□ Disable Mailbox

SMTP/POP3 Setting
□ Assign Exchange Integration License E-mail Address

SMTP/POP3 Setting
E-mail Name ext4444 □ Retrieve Voice Mail By E-mail Client

Mail Forwarding Options
□ Enable Mail Forwarding Delete Messages After Forward
Forward E-mail Address

Message Playback Options
☑ Announce Message Sender before Playback
□ Announce Time Stamp before Playback
☑ Confirm Callback Number
□ Enable Distinctive Call Waiting Tone
□ Play the Newest Voice Message First

Voice Mail Capacity
Message Retention Duration 60 day(s)
□ New □ Heard ☑ Saved Messages
Max Number of Messages 100
Mailbox Size 50 MB
Max Message Length 5 min

Press '0' option
Forward the call when caller press 0 while listening to group greeting
Forward to Operator
9

Voice Mail Access Option
□ Enable agents to access voice mailbox of workgroup

Figure 167. Workgroup Configuration, Mail Management tab

Note: You can use the **Apply to** option to apply mailbox settings to one, some, or all workgroup.

Disabling a Mailbox

When you disable a mailbox, the normal greeting is played but callers cannot leave messages.

Setting E-mail Options

On the **Mail Management** tab, you can set the e-mail options for the workgroup:

- **Assign Exchange Integration License** – Assign an Exchange Integration license to this group.You must also provide an email address.
- **E-mail Name** – The workgroup's e-mail name without the @domain. The default e-mail name is `ext`*<workgroup number>,* that is, the letters "ext" followed by the workgroup number. For example, the default e-mail name for workgroup 500 would be **ext500**.
- **Retrieve Voice Mail by E-mail Client** – When selected, this sends voice mail to the user extension as an e-mail attachment. Deselected, voice mail is retrieved as voice mail.
- **Enable Mail Forwarding** – When selected, the workgroup's e-mail will be forwarded to the e-mail address you specify in the **Forward E-mail Address** box. The address should be a full address, including the domain (for example, *jsmith@thecompany.com*).

  If you enable mail forwarding, you also specify what you want done with the original messages after they have been forwarded. In the list you can choose to:

  - Delete Messages after Forward
  - Keep the Messages as New
  - Keep Messages as Saved

Setting Mailbox Playback Options

You can use the following check boxes to turn on or off options for listening to playback of recorded messages. These options apply to both new messages and saved messages, and they can be applied to multiple workgroups using **Apply to**:

Message Playback Parameter	Description
Announce Message Sender Before Playback	Selected, the user hears the name of the message sender (internal sender only) before listening to recorded Altigen Voice Mail System messages.
Announce Time Stamp Before Playback	Selected, the user hears the timestamp (time and date) of each message before playback.
Confirm Callback Number	Selected, system confirms the accuracy of the caller's number.
Enable Distinctive Call Waiting Tone	Selected, the user hears three different call waiting tone cadences to distinguish between internal, external, and operator calls (see "Distinctive Ring" on page 33).
Play the Newest Voice Message First	Selected, new voice mail will be retrieved first. When not selected, the system will play voice mail based on FIFO (first in, first out).

Setting Mailbox Capacities

You can set various mailbox capacities with the following options, and you can apply the settings to multiple workgroups using **Apply to**:

Voicemail Capacity Parameter	Description
Message Retention Duration	Set how long (in days) new, heard and/or saved voicemail messages are retained. The default duration is 60 days. By default, only the *Saved Messages* option is selected. Any message type that is **not** selected will have no duration limit.
Max Number of Messages	Maximum number of messages stored in the workgroup's mailbox. The range is **1 - 999**, with a default of 100. When your voicemail mailbox capacity is reached, the voicemail system will announce "Your mailbox is full" and no further messages will be accepted until you delete enough messages to fall back below your set capacity.
Mailbox Size	Mailbox size in MBs of stored messages. The range is **1–500** MB, with a default of 50. When your voicemail mailbox capacity is reached, the voicemail system will announce "Your mailbox is full" and no further messages will be accepted until you delete enough messages to fall back below your set capacity.
Max Message Length	Maximum length of voice messages in minutes. The range is **1–30** minutes, with a default of 5 minutes.

Press Zero Option

This option allows a caller to press "0" while listening to this workgroup's greeting. When the caller presses "0," the call will forward to the specified destination. Use the list to specify a forwarding destination for the call: **Voice Mail**, **AA**, **Extension**, **Group**, **Operator** (default), **Outside Number**, or **Line Park**.

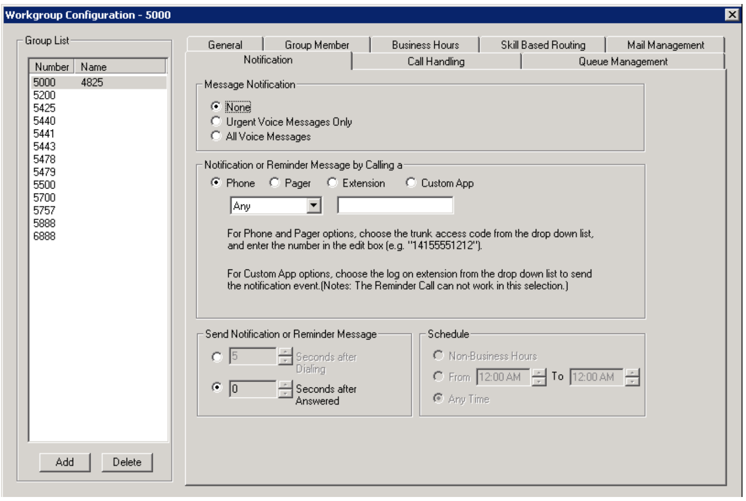
If you choose to forward to an **Outside Number**, select a trunk or route access code to use in the small list on the left, and type in the full prefix and phone number.

Voice Mail Access Option

To allow agents of a workgroup to access the group's voice mail in MaxAgent (MaxAgent's **WG VM** tab), select the group and check **Enable agents to access voice mailbox of workgroup**.

Setting Message Notification Options

To set notification options on new incoming e-mail and voice messages, click the **Notification** tab in the Workgroup Configuration window, and select the workgroup number from the **Group List**.



Group List

Number	Name
5000	4825
5200	
5425	
5440	
5441	
5443	
5478	
5479	
5500	
5700	
5757	
5888	
6888	

Message Notification

● None
○ Urgent Voice Messages Only
○ All Voice Messages

Notification or Reminder Message by Calling a

● Phone ○ Pager ○ Extension ○ Custom App

Any

For Phone and Pager options, choose the trunk access code from the drop down list, and enter the number in the edit box (e.g. "14155551212").

For Custom App options, choose the log on extension from the drop down list to send the notification event.(Notes: The Reminder Call can not work in this selection.)

Send Notification or Reminder Message

○ 5 Seconds after Dialing
● 0 Seconds after Answered

Schedule

○ Non-Business Hours
○ From 12:00 AM To 12:00 AM
● Any Time

Figure 168. Workgroup Configuration, Notification tab

Individual users can also configure **Message Notification** within the Altigen Voice Mail System.

Note: You can use the **Apply to** option to apply mailbox settings to one, some, or all workgroups.

Setting the Message Types for Notification

Select the types of messages for which the workgroup user will be notified:

- **None** – When selected, the user is *not* notified with a call regarding newly received messages. Selecting this option does not prevent the user from getting message waiting indicators or stutter dial tone when new messages are received.
- **Urgent Voice Messages Only**
- **All Voice Messages**

Please note that the system will start notification as soon as it enters non-business hours under the following conditions:

- Extension is set to notify **Urgent Voice Message Only**
- Notification is set to **Non-Business Hours**
- Voice mail is received during business hours and is marked urgent
- Extension user does not check the urgent message

Setting the Type of Notification

There are several options for sending the notification or reminder message: **Phone**, **Pager**, **Extension** or **Custom Application**.

- **Extension** – To use the Extension option, select the **Extension** radio button, then type the extension number into the text box.
- **Phone/Pager** – For the **Phone** and **Pager** options, first specify the trunk or route access code using the list next to the **Phone** radio button. The **Any** option means to locate any available trunk. Then type in the number with all relevant dialing prefixes other than the trunk code, using a maximum of 63 digits.
- **Custom App** – When used in conjunction with a third-party notification application, the **Custom App** feature enables an extension to connect to an application that can receive the notification event; use the list to choose the log-on extension to which the third-party application is connected. Contact your local Altigen Partner for more information on using this feature.

  Note: The Reminder Call will not work with this selection.

Note also the following considerations:

- For the **Pager** option, the system calls the specified pager number and then dials the system main number (as set in System Configuration, **General** tab), which is then displayed on the user's pager.

  For the operator-assisted paging function, the operator phone number **and** the pager number must be entered in the **<phone number>*<pager number>** format. For example, if the phone number to call the pager operator is **7654321** and the pager number to page the user is **12345678**, the notification outcall number that needs to be entered is **7654321*12345678**. When the pager operator answers the Message Notification call, MaxCS announces the **pager number and** the **System Main Number** (as configured on the **General** tab of **System Configuration**), which will be displayed on the user's pager. The operator is also given the option to repeat these numbers by pressing '**#**'.

Outcall to Cellular or PCS Phone Numbers

When an outcall is made by the system (for One Number Access, Message Notification, Zoomerang, Call Forwarding, and so on) to a cellular or PCS phone, it may ring the phone once but not necessarily present the call and make a connection. This will happen if the ringback tone played by the cellular service provider does not conform to standard ringback tones. To work around this problem, append a few commas (**,**) to the outcall (cellular) number when entering it. Each comma provides a one second pause.

Setting Notification Timing

When notification is configured to an *outside phone number*, the system will announce, "This is the outcall notification message for…" after call connection. However, there are situations when the system may not be able to receive an answer supervision signal from the carrier. If the system plays the announcement phrase before the notification call is answered, the phrase will be cut off. The following two options can be configured based on answer supervision capability:

- **Seconds after Dialing** – If the carrier of the outside phone number cannot provide an answer supervision signal, check this option and set a delay time. (Default 5 seconds, maximum 30 seconds.)

  Note: If the delay is set too long, the notified party will hear silence before the announcement is played.
- **Seconds after Answered** – This field is set to 0 seconds and it is not configurable for notification to a phone number. It means the system will play the announcement immediately after answer supervision is received.

When notification is configured to a *pager*, the system will transmit DTMF digits as the return phone number (the **System Main Number** as set in the System Configuration **General** tab) after call connection. However, there are situations when the system may not be able to receive an answer supervision signal from the pager system. If the system sends digits before the call is connected, some digits will be cut off. The following two options can be configured based on answer supervision capability:

- **Seconds after Dialing** – If the pager carrier cannot provide an answer supervision signal, check this option and set a delay time. (Default 5 seconds, maximum 30 seconds.)

- **Seconds after Answered** – If the answer supervision signal is provided by the carrier, check this option and set the delay timer to 2 to 5 seconds. In some cases, the pager carrier cannot detect DTMF right after the call connection. (Default is 10 seconds, maximum is 30.)

  Note: You may need to try a different delay setting to make sure the user return number is transmitted properly after configuration.

Setting Notification Business Hours

You can choose one of three options for when the extension user is to be notified of new messages:

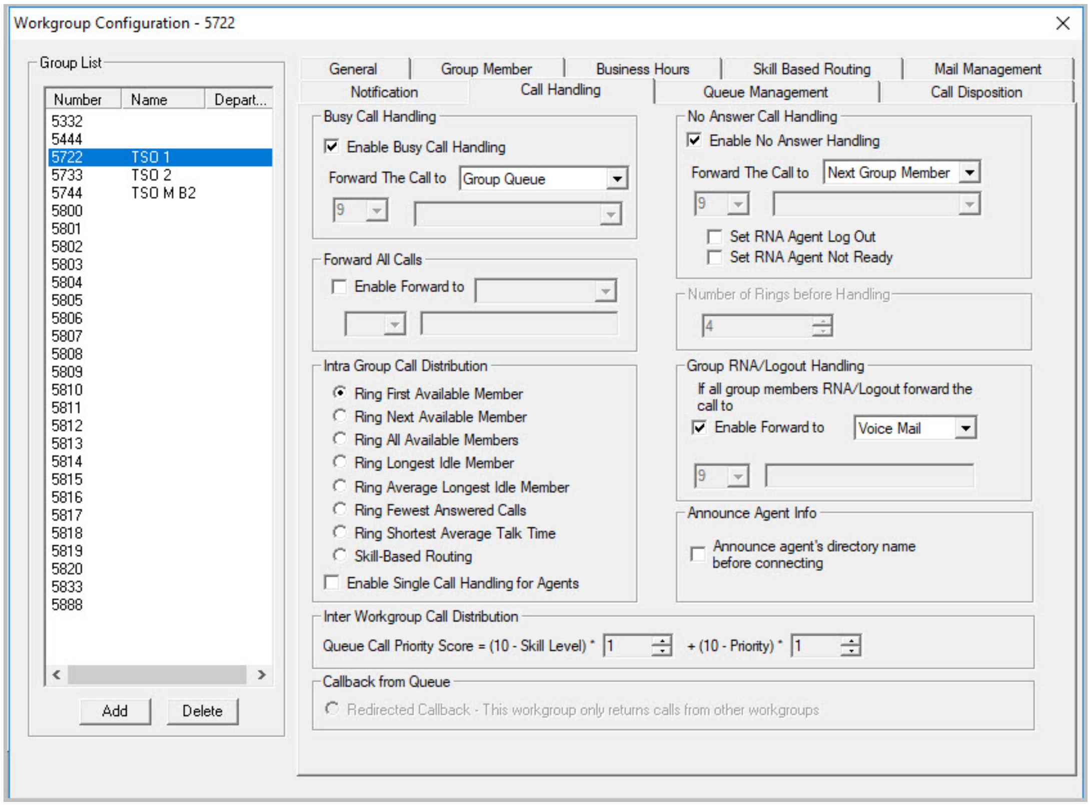
- **Non-Business Hours** – Notify only during non-business hours. Business hours are set in System Configuration, **Business Hours** tab (see “Setting Business Hours” on page 38).
- **From/To** – Notify during a specified time of day*.* Select the hours in the **From** and **To** time scroll boxes.
- **Any Time** – Notify at all times (every day).

Setting Call Handling Options

Call Handling options include forwarding, handling busy calls, handling no-answers and other options.

You can use the **Apply to** option to apply call restriction settings to one, some, or all workgroups.

To work with workgroup call handling options, click the **Call Handling** tab in the Workgroup Configuration window, and select the workgroup number from the **Group List**.



Group List

Number	Name	Depart...
5332		
5444		
5722	TSO 1	
5733	TSO 2	
5744	TSO M B2	
5800		
5801		
5802		
5803		
5804		
5805		
5806		
5807		
5808		
5809		
5810		
5811		
5812		
5813		
5814		
5815		
5816		
5817		
5818		
5819		
5820		
5833		
5888		

Busy Call Handling
☑ Enable Busy Call Handling
Forward The Call to: Group Queue
9

Forward All Calls
□ Enable Forward to

Intra Group Call Distribution
● Ring First Available Member
○ Ring Next Available Member
○ Ring All Available Members
○ Ring Longest Idle Member
○ Ring Average Longest Idle Member
○ Ring Fewest Answered Calls
○ Ring Shortest Average Talk Time
○ Skill-Based Routing
□ Enable Single Call Handling for Agents

No Answer Call Handling
☑ Enable No Answer Handling
Forward The Call to: Next Group Member
9
□ Set RNA Agent Log Out
□ Set RNA Agent Not Ready

Number of Rings before Handling: 4

Group RNA/Logout Handling
If all group members RNA/Logout forward the call to
☑ Enable Forward to: Voice Mail
9

Announce Agent Info
□ Announce agent's directory name before connecting

Inter Workgroup Call Distribution
Queue Call Priority Score = (10 - Skill Level) * 1 + (10 - Priority) * 1

Callback from Queue
○ Redirected Callback - This workgroup only returns calls from other workgroups

Figure 169. Workgroup Configuration, Call Handling tab

Handling Busy Calls

You have several options for handling calls when the workgroup extension is busy. If you do not enable busy call handling, the caller simply hears a busy signal.

To enable the options, select the **Enable Busy Call Handling** check box, then select from the following forwarding options:

- **Group Queue** – The caller will stay in the workgroup queue waiting for any agent to become available. If there is no agent logged in at this moment, the system will use **Group Logout Handling** to handle this call.
- **Group Voice Mail**
- **Extension** – Forward caller to an extension.
- **AA** – Forward caller to an auto attendant.
- **Group** – Forward caller to another group.
- **Line Park** – Forward caller to a Line Park group.

Forwarding All Calls

When you do not want the workgroup to handle any calls, check the **Enable Forward To** option in the Forward All Calls section of the **Call Handling** tab, and select an option.

The forwarding options are as follows:

- To **Voice Mail**
- To an **Extension** – Select an extension number in the drop-down list.
- To **AA** – Select the AA to use in the list below the option.
- To a **Group** – Select a group from the list.
- To the **Operator**
- To an **Outside Number** – This option is available if it is allowed in the **Other Call Restrictions** option in the **Restriction** tab, as discussed in “Setting Other Call Restrictions” on page 186. Also, see “Outcall to Cellular or PCS Phone Numbers” on page 264.

  If you choose **Outside Number**, select a trunk or route access code to use in the small list on the left, and type in the full prefix and phone number.
- To an **App Ext** – When used in conjunction with a third-party notification application, the **App Ext** feature enables an extension to connect to an application that can receive the notification event; use the list to choose the log-on extension to which the third-party application is connected. Contact your local Altigen Partner for more information on using this feature.
- To **Line Park** – If configured, select a **Line Park** group from the list.

Handling Unanswered Calls

The **Enable No Answer Handling** configuration provides options for handling calls when the system rings the first available agent and the call is not answered. If *all* agents in the workgroup are rung and no one answers the call, the system will use the Group RNA/Logout Handling rule. **Enable No Answer Handling** is not available if Intra Group Call Distribution is set to **Ring All Available Members**.

To configure this option, check the **Enable No Answer Handling** box.

Select one of the following forwarding options for no answer call handling:

- **Next Group Member** – Ring the next available agent until all available agents are rung. If all agents are busy, caller will stay in the workgroup queue.
- **Extension** – Take the call out of the workgroup and forward it to an extension.

- **Group** – Take the call out of workgroup and forward it to another group.
- **Group Voice Mail** – Transfer the caller to the workgroup voice mail when the first available agent does not answer the call.
- **Member Voice Mail** – Transfer the caller to the first available agent's voice mail if this agent does not answer the call.
- **AA** – Take the call out of the workgroup and forward it to an auto attendant.
- **Line Park** – Take the call out of the workgroup and forward it to a Line Park group.

Set RNA Agent Auto Logout Check Box

Select this option to have the system automatically log out an agent extension from a workgroup if RNA is encountered.

Set RNA Agent Not Ready Check Box

Select this option to have the system automatically set an agent’s extension in a workgroup to not ready if RNA is encountered.

Ring No Answer Details

If an agent does not answer an incoming workgroup call (Ring No Answer), the agent may be presented with that call again.

Two separate, independent timers are involved with the timing of presenting calls to agents who RNA:

- One timer tracks each agent’s availability; this is an *extension* timer
- Another timer checks, at specific intervals, whether any agents are available to take calls

Here is one scenario describing how an agent could be presented with the same call 1-2 minutes after it was first presented.

1. Agent A did not accept an incoming call.

   The system keeps a list of the agents that have been presented with that call. Agent A is now on that list.
2. When Agent A’s extension returns to *Idle* state, the extension timer starts counting. This timer counts how long the agent has been *Idle*, for routing purposes.
3. The call remains in the queue (because all agents are busy).
4. Meanwhile, Agent A’s extension counter continues counting. After 60 seconds of being in *Idle* state, Agent A’s extension drops from the system’s “Called” list for that call. This means the extension is now available to receive that call again.

Agent A may not receive the call right away. This is because the system has that separate timer. It checks every 60 seconds to see whether any agent is available for calls. So the call could be presented to Agent A again within 60 - 120 seconds of the agent returning to *Idle* state.

Number of Rings Before Handling

If you select **Ring All Available Members** in the Intra Group Call Distribution section, then specify the **Number of Rings before Handling**, using the scroll box beside that option. The number of rings is the total number of times agents are rung before the call is handled by the Group RNA/Logout Handling configuration

Handling Rejected Calls

In earlier releases, MaxCS did not apply the workgroup's RNA rules to an agent who rejects a call, even if the workgroup has RNA Not Ready or RNA Log Out rules configured. In AltiReport, this behavior was considered as RNA.

Beginning with Release 9.0.1, Altigen has added a registry setting for organizations that wish to apply the workgroup RNA setting to agents when they reject a call.

Make sure to back up your registry before making any changes.

1. In RegEdit, navigate to:

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

2. Find the following key:

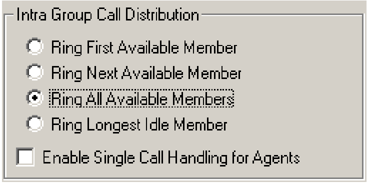
   EnableIPTalkRejectLogOutRNA

3. Change this key's value from 0 to 1. Save your changes.
4. In MaxAdmin, select **Diagnostic** > **Trace**. Locate and run *Minute Task* (NOT Midnight Task).

After applying this setting, agents who reject calls will be logged off or will be set to *Not Ready*, according to that workgroup's RNA configuration. That result will be reflected in the AltiReports Activity Report (1101).

Setting IntraGroup Call Distribution

The IntraGroup Call Distribution options let you set the handling of normal inbound calls: how to route the incoming call to a workgroup agent, using one of the following options:



Intra Group Call Distribution

○ Ring First Available Member

○ Ring Next Available Member

● Ring All Available Members

○ Ring Longest Idle Member

□ Enable Single Call Handling for Agents

Figure 170. The IntraGroup Call Distribution options

- **Ring First Available Member** – First *available* extension in a workgroup. For example, if there are three member extensions in a workgroup, the call is always sent to the *first* member configured in the workgroup. If this member is busy, the call goes to the *second* member configured and so forth.
- **Ring Next Available Member** – Around-robin method that attempts to evenly distribute calls among the group members. This method sends the call to the *next* member configured in a workgroup (regardless of whether the previous member is busy or not). In other words, if the previous call was sent to #3 in the group, the present call is sent to #4, if #4 is not busy.
- **Ring All Available Members** – All extensions in a workgroup.

  Note: When this option is enabled, a single workgroup can have no more than 20 members.

  In addition, calls to the workgroup with this option enabled have higher priority than other workgroup calls. Therefore, if an agent belongs to multiple workgroups, one of which has this option enabled, a call to that workgroup will be processed first, regardless of Wait Time of calls in other workgroups which are not set to Ring All.

  If members are using IP extensions, the system will not use the IP codec channel during ringing all IP phones. Only one codec will be used when a member of a workgroup answers the call.
- **Ring Longest Idle Member** – The agent who has the longest idle time, defined as follows:
  - The agent needs to be in login state
  - Idle time is calculated from the end of the last wrap-up event.
  - If the agent does not have wrap-up time configured, the idle time is calculated from the end of last busy state.
- **Ring Average Longest Idle Member** – The agent who averages being off the phone the longest:
  - Average Idle Time = (Total Login Time – Total Talk Time) / Total Calls Handled

  - Total Login Time = Cumulative WG login time since midnight
  - Total Talk Time = Cumulative WG Inbound + Outbound call duration since midnight
  - Total Calls Handled = Total number of WG calls (Inbound + Outbound) handled by the agent since midnight

  If a new agent logs into a WG that has been operating for several hours, this agent will have the highest priority to take the call.

  If multiple agents log into a WG that has been operating for several hours, the one with the longest idle time since login will have the highest priority to take the call.

- **Ring Fewest Answered Calls** – The agent who has answered the fewest number of calls.
- **Ring Shortest Average Talk Time** – The agent who averages the shortest talk time.

  Note: Average talk time is calculated as follows:

  ```
  Average Talk Time (ATT) = Total Inbound Talk Time / Total Inbound Calls
  Answered
  ```

  The agent calculated with the lowest value for ATT is rung first.

- **Skill-Based Routing** – The call will be routed according to the SKLR setting and skill-based routing rules set up on the Skill Based Routing tab in the Workgroup Configuration window (see “Skill Based Routing” on page 256). When **Skill-Based Routing** is selected, the agent with longest idle time will be selected to take the call when multiple agents with the same skill level are idle.

Enable Single Call Handling for Agents

Check this check box to enable single call handling for workgroup agents.

- If single call handling is *enabled* and the agent has one or more calls on hold, MaxCS will not distribute the call to this agent. If single call handling is *disabled*, MaxCS will distribute calls to this agent even when one or more calls are put on hold by this agent.
- If a workgroup agent uses a Polycom phone, Single Call Handling will be automatically enabled, regardless of the workgroup’s *Enable Single Call Handling for Agents* setting.

Handling Calls when Group Members Are RNA/Logged Out

You can set calls to forward to a specified destination when all group members either do not answer the call (RNA) or are logged out. To do so, in the **Group RNA/Logout Handling** section of the **Call Handling** tab, check the **Enable Forward to** check box, and select a destination from the list.

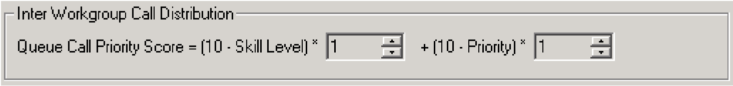
The forwarding options are described in “Forwarding All Calls” on page 266. An additional option, *Group Queue*, forwards incoming workgroup calls to the workgroup call queue. With this setting, when agents log back in, they can begin accepting the queued calls

Announce Agent Info

Check this check box to have the system announce the agent’s directory name before an incoming workgroup call is transferred to an agent from the queue.

Inter Workgroup Call Distribution

In the case where an agent belongs to multiple workgroups and there are queued calls in two or more of these workgroups, as soon as the agent becomes available, the queued call that will be distributed to this agent is determined by the **Inter Workgroup Call Distribution** setting.



Inter Workgroup Call Distribution

Queue Call Priority Score = (10 - Skill Level) * 1 + (10 - Priority) * 1

This field is used to calculate the score of each call in a workgroup's queue. Depending on the call's assigned priority and the skill of the agent that is available, the score will determine which workgroup's call gets answered first. The call with the highest score is answered first. Use the up/down arrows to increase or decrease the weight values for **Priority** and **Skill** values.

The first box is the weight for agent skill in a workgroup. The second box is the weight for priority of a queued call. The score is calculated as (10 – skill level) x weight for agent skill + (10 – queued call priority) x weight for call priority. When determining which call should be dispatched to an idle agent who is assigned to multiple workgroups, the system will consider the following factors:

- Caller's priority
- Agent's skill level
- Caller's SKLR
- Caller's wait time in queue

Configuration Guidelines:

- Assuming an agent is assigned with different skill levels for different workgroups, and call priority is the same for all calls, you can increase the skill weight to 9 and reduce the priority weight to 1 to better match an agent's skill.
- Assuming each call is assigned with a priority based on certain customer attributes, and an agent's skill is the same for all workgroups, you can increase the priority weight to 9 and lower the skill weight to 1 to have a call with higher priority answered first.
- Assuming all calls' priority is the same and agent's skill level is the same for all workgroups, you can use this scoring system to prioritize workgroups. For example, assign priority weight 9 to the most important group, 5 to the second most important group, and 1 to the least important group. Calls in the group with higher priority weight will be dispatched first.
- When there are callers with the same score in different workgroups, the queue time will be used as a tie breaker.
- If you have variable priority settings for callers, and agents belong to multiple workgroups with different skill levels, it is recommend that you set all calls' SKLR to 1 and set call coverage rule to "Equal or Lower than SKLR of Incoming Call". This will eliminate the complexity of matching caller's SKLR to agent's skill level.

Setting Workgroup Not Ready Behavior

A new registry setting lets you adjust how the system handles Ready/Not Ready behavior when an agent is a member of multiple workgroups.

By default, If an agent is logged into one or more workgroups and is set to *Not Ready*, if the agent logs into another workgroup, the system automatically changes the agent's state to *Ready*.

To prevent the system from automatically switching an agent's state to *Ready* in this scenario, you can make the following registry change. Make sure that you back up the registry before making any modifications.

1. In RegEdit, navigate to the following key:

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

2. Find the following key:

   EnableAgentLoginAutoReady

3. Change its value from 1 to 0. Save your change.

4. In MaxAdmin, select **Diagnostic** >**Trace**. Locate and run **Minute Task** (do not choose *Midnight Task* by mistake).

With this registry entry enabled, agents that set their status to *Not Ready* and then log into a workgroup (via MaxAgent or #54) will remain in the state *Not Ready*.

To change the system back to the default behavior, change the registry value from 0 to 1 and run **Minute Task** again.

Queue Management – Basic

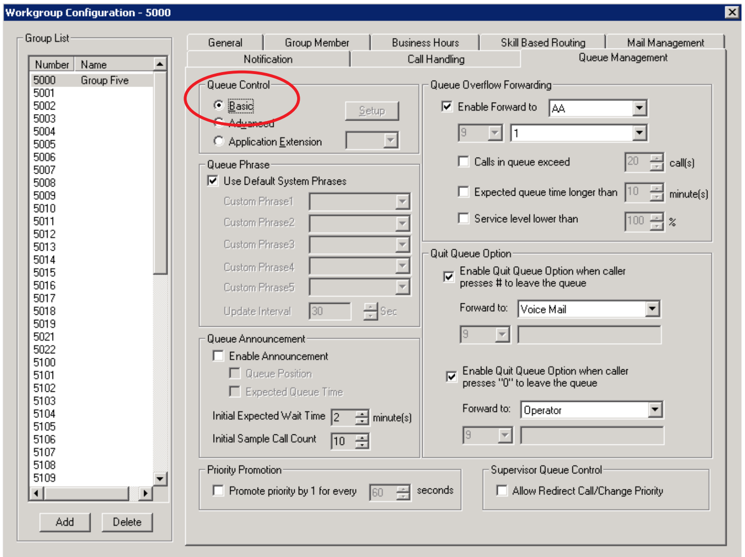
The **Queue Management** tab in Workgroup Configuration is where you set options for queue phrases and announcements, queue overflow routing and quit queue options. Options become enabled depending on the Queuing Control selected – **Basic**, **Advanced,** or **Application Extension**.

There are two modes for queue management.

Basic mode provides basic queue functions. Starting witih Release 9.0.1, the Setup option is disabled.

Advanced mode (refer to *Queue Management – Advanced* on page 273) offers additional functions, including:

- Additional announcements that you can play to callers waiting in the queue
- Menu selection, where a caller can press a digit to hear different prompts or options while waiting in the queue
- Additional queue overflow options
- Callback from Queue configuration


Workgroup Configuration - 5000

Group List

Number	Name
5000	Group Five
5001	
5002	
5003	
5004	
5005	
5006	
5007	
5008	
5009	
5010	
5011	
5012	
5013	
5014	
5015	
5016	
5017	
5018	
5019	
5021	
5022	
5100	
5101	
5102	
5103	
5104	
5105	
5106	
5107	
5108	
5109	

Queue Control
● Basic
○ Advanced
○ Application Extension

Queue Phrase
☑ Use Default System Phrases
Update Interval 30 Sec

Queue Announcement
☐ Enable Announcement
☐ Queue Position
☐ Expected Queue Time
Initial Expected Wait Time 2 minute(s)
Initial Sample Call Count 10

Queue Overflow Forwarding
☑ Enable Forward to AA
9 1
☐ Calls in queue exceed 20 call(s)
☐ Expected queue time longer than 10 minute(s)
☐ Service level lower than 100 %

Quit Queue Option
☑ Enable Quit Queue Option when caller presses # to leave the queue
Forward to: Voice Mail
9
☑ Enable Quit Queue Option when caller presses "0" to leave the queue
Forward to: Operator
9

Priority Promotion
☐ Promote priority by 1 for every 60 seconds

Supervisor Queue Control
☐ Allow Redirect Call/Change Priority

Figure 171. Workgroup Configuration, Queue Management tab, Basic Queue Control

Setting Queue Phrase Options

For each workgroup, you can either use the system default phrases or you can set up a custom configuration.

The default audio phrases are discussed in “Audio Peripheral Configuration” on page 50.

Queue Announcements

You can set up the system to announce a caller's queue status – queue position and expected queue time – when an incoming call enters a workgroup queue. To enable this option, check **Enable Announcement**, then check **Queue Position** and/or **Expected Queue Time**.

Queue Position – When checked, the system will tell the caller which position the caller is at in queue. Do not check this option if you assign different priorities to different calls based on DNIS, CID, or AA selection. Do not check this option if you configure matching a caller's SKLR to an agent's skill level. Queue position is not meaningful when a higher priority caller can push a lower priority caller or if no agent is available to answer a particular SKLR.

Expected Queue Time – When checked, the system will tell the caller how long the wait is expected to be. When calculating this number, the system will consider the average agent call handling time and the position of the caller in queue. Because queue position is a factor when calculating this number, do not check this option when call priority and caller SKLR matching are configured. Please note that the Expected Queue Time is an estimated number. Agents logging in or out of the workgroup during operation hours will affect the actual handling time and cause deviation to the expected queue time.

When Avg time in queue is less than 1 minute, the expected wait time in queue will not be played to the caller.

`Expected Queue Time` (round up to minutes) = `[(Average Call Handling Time x Queue Position) + 59 sec] / 60 sec`

Expected Wait Time Sampling

To calculate Expected Queue Time, the system needs to take samples when a workgroup starts operation. You can set the following parameters to set a sampling period and a fixed Expected Queue Time announcement during sampling period. The expected queue time counter is reset for all workgroups daily at midnight.

- **Initial Sample Call Count** [1 to 100] – How many calls you would like to use as initial samples.
- **Initial Expected Wait** (Queue) **Time** [1 to 10 minutes] – This field defines the expected queue time to be announced during the sampling period. One minute is the minimum you can set for expected wait time in queue.

Queue Overflow Forwarding

The Queue Overflow Forwarding options are for handling long queues or long wait times for callers. When a queue exceeds a set number of calls, or callers are waiting beyond a set length of time, calls can be automatically forwarded to a voicemail box, AA, extension, group, operator, outside number, or application extension.

To set options for handling queue overflow,

1. In the **Queue Overflow Forwarding** section, set options for:
   - **Calls in queue exceed** – When the number of calls in queue are greater than the defined number, new incoming calls will be overflowed to the defined target.
   - **Expected queue time longer than** – When the longest queue time is greater than the specified number of minutes, new incoming calls will be overflowed to the defined target.
   - **Service level lower than** – This number is not a historical service level defined in the workgroup threshold. This number is a real-time queue service level (RTSL) calculated as follows:

     `RTSL% = 1 – (# of queued calls exceed SL threshold / Total calls in queue)`
2. Check the **Enable Forward to** check box and from the list, select the forwarding destination list to use if the queue length, wait time or service level settings are exceeded. If this option is not checked, calls will go to the workgroup's voicemail.

Quit Queue Option

The quit queue feature gives a caller the option of leaving a workgroup queue at any time by pressing **#** and/or **0**. To enable this feature, check either or both of the **Enable Quit Queue Options**, then use the appropriate **Forward to** list to select the option the caller will have:

- **Voice Mail** – Sends to voicemail
- **AA** – Select the auto attendant to use. AAs are configured in **AA Configuration** on the **System** menu.
- **Extension** – Select an extension from the list.

  Note: If the forwarding extension is busy when a caller quits a queue, the call will go to this extension's voice mail.
- **Group** – Select a workgroup from the list.
- **Operator** – Sends to the operator
- **Outside Number** – This option is available if it is allowed in the **Other Call Restrictions** option in the **Restriction** tab, as discussed in "Setting Other Call Restrictions" on page 186.

  If you choose **Outside Number**, select a trunk or route access code to use in the small list on the left, and type in the full prefix and phone number.

  Note: Forwarding calls to a pager is possible but *not recommended* since callers will only hear what is heard when calling a pager and will not know to enter a return phone number unless instructed.
- **App Ext** – When used in conjunction with a third-party notification application, this feature enables an extension to connect to an application that can receive the notification event; use the list to choose the log-on extension to which the third-party application is connected. Contact your local Altigen Partner for more information on using this feature.
- **Callback Interview** – The System will record the caller's callback number and will prompt the caller to record a message into the voice mail box of the workgroup.

  Note: This option is only available to external callers.

Priority Promotion

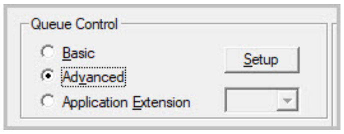
To prevent calls with lower priority staying in queue forever, causing high abandon rate, or lowering service level, you can set priority promotion to enhance a caller's position in queue. Check the box and enter the proper time interval in seconds.

Supervisor Queue Control

When the **Allow Redirect Call/Change Priority** check box is checked, this allows a workgroup supervisor to redirect queue calls or change the call priority of queued calls, using the MaxSupervisor application.

Queue Management – Advanced

When you select **Advanced** in the *Queue Control* section of the **Queue Management** tab, you have additional options that are not available in Basic mode.



Queue Control

○ Basic

● Advanced

○ Application Extension

Figure 172. The Advanced Queue Control option

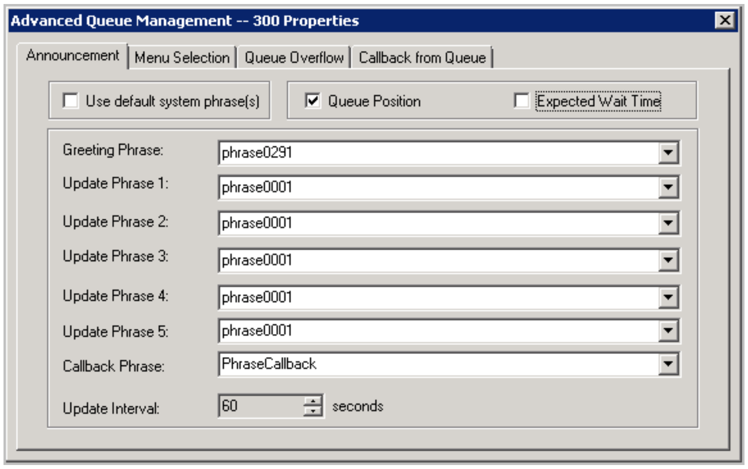
To configure advanced queuing options, select **Advanced** and click the **Setup** button. This opens the Advanced Queue Management (AQM) application configuration window with tabs for configuring **Announcement**, **Menu Selection**, **Queue Overflow,** and **Callback from Queue**.

Considerations

- If your system has a lot of extensions, there may be a slight delay opening the *Advanced Queue* panel.
- Once you configure advanced queue control settings for a workgroup, by default, callers to that workgroup can no longer press the # key to leave a voicemail message. If your queue announcement tells callers that they can press # to leave a message, consider updating the appropriate phrase.
- If you have previously configured any Advanced mode queue options, and then later you attempt to switch back to Basic mode, you will be warned that you are disabling all advanced queue management features.

Announcement Tab

The **Announcement** tab is where you configure queue announcements.



☐ Use default system phrase(s) ☑ Queue Position ☐ Expected Wait Time

Greeting Phrase: phrase0291

Update Phrase 1: phrase0001

Update Phrase 2: phrase0001

Update Phrase 3: phrase0001

Update Phrase 4: phrase0001

Update Phrase 5: phrase0001

Callback Phrase: PhraseCallback

Update Interval: 60 seconds

Figure 173. Workgroup Configuration, Advanced Queue Management, Announcement tab

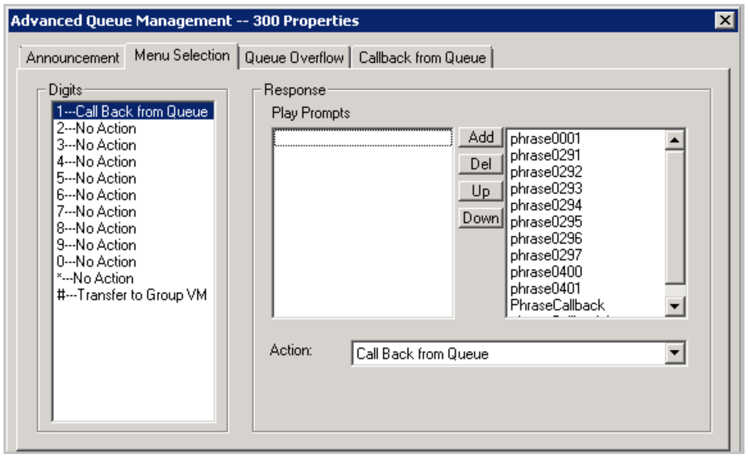
To configure queue announcements:

1. Select any of the following check boxes:
   - **Use Default System Phrases**
   - **Queue Position**
   - **Expected Wait Time**
2. If you are not using default system phrases, use the lists to select the **Greeting Phrase** and **Update Phrase**s that will be played to callers in queue.
3. Select the **Update Interval** (0 - 180 seconds) to be inserted between queue phrases.

   Note: If the interval is set to 0, the system will play phrases one after the other without music in between.
4. Click **OK** or **Apply**.

Menu Selection Tab

The **Menu Selection** tab allows for configuration of a voice menu selection that can be made available to callers in queue. When a workgroup queue is controlled by the Advanced Queue Management application, calls in queue will hear a menu prompt. The menu will allow callers to take certain actions based on digit input, and callers can also hear one or more phrases associated with the actions.


Advanced Queue Management -- 300 Properties

Digits
1---Call Back from Queue
2---No Action
3---No Action
4---No Action
5---No Action
6---No Action
7---No Action
8---No Action
9---No Action
0---No Action
*---No Action
#---Transfer to Group VM

Response
Play Prompts
phrase0001
phrase0291
phrase0292
phrase0293
phrase0294
phrase0295
phrase0296
phrase0297
phrase0400
phrase0401
PhraseCallback

Action: Call Back from Queue

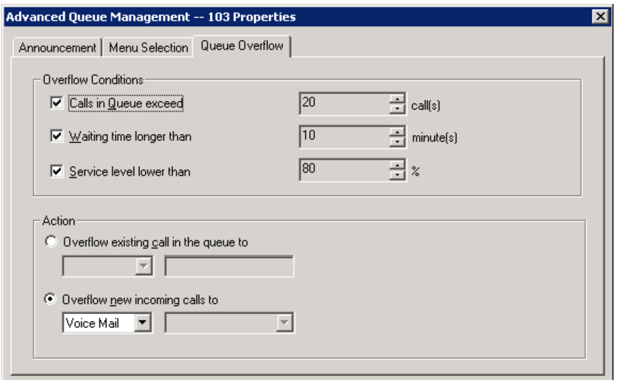
Figure 174. Workgroup Configuration, Advanced Queue Management, Menu Selection tab

To set up the Menu Selection:

1. In the **Digits** field, select **0 – 9**, **#** or *.
2. For the highlighted digit, select a **Prompt** from the phrase list and click **Add**. You can add one or more prompts, then use the **Up** or **Down** buttons to determine the order in which the prompts are played.
3. Use the list to select one of the following actions, then click **OK** or **Apply**.
   - **Callback from Queue**
   - **Transfer to Extension/Other Group**
   - **Transfer to AA**
   - **Transfer to Operator**
   - **Transfer to Outside Number**
   - **Transfer to Group VM**
   - **Play prompts**
   - **No Action**
   - **Disconnect**

Queue Overflow Tab

The **Queue Overflow** tab allows for configuration of overflow conditions and actions.


Advanced Queue Management -- 103 Properties

Overflow Conditions
☑ Calls in Queue exceed 20 call(s)
☑ Waiting time longer than 10 minute(s)
☑ Service level lower than 80 %

Action
○ Overflow existing call in the queue to
● Overflow new incoming calls to Voice Mail

Figure 175. Workgroup Configuration, Advanced Queue Management, Queue Overflow tab

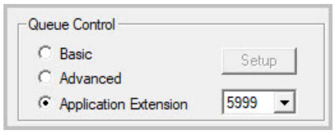
- **Overflow Conditions** – Select from any of the following check boxes (if all are checked, the conditions will be followed in order):
  - **Calls in Queue exceed** – Can be between 0 and 150. This is the number of calls in queue that will cause overflow. For example, 5 calls mean that once a queue has 5 calls in queue, the system will forward the overflow calls according to a specified action.
  - **Wait time longer than** – Can be between 0 and 200 minutes. This is the time that a call must have been waiting in queue for the call to be overflowed.
  - **Service level lower than** – Can be between 0 and 100%. This is the percentage of calls in queue longer than service level threshold.
- **Action** – Select from one of the following options:
  - **Overflow existing call in the queue to** (first in, first out)
  - **Overflow new incoming calls to** (last in, first out)

  When either is selected, use the list to select the overflow action:

  - **Voice Mail**
  - **Extension** – Select an extension from the list.
  - **Workgroup** – Select a workgroup from the list.
  - **AA** – Select the auto attendant to use in the list under the option. AAs are configured in **AA Configuration** on the **System** menu.
  - **Operator**
  - **Outside** – Type in the full prefix and phone number, preceded by the trunk or route access code, for example, 915102529712.

Application Extension Queue Control

When you select **Application Extension** in the **Queue Control** panel on the **Queue Management** tab (and an Application Extension is already configured), use the list to select the desired Application Extension. For details on configuring an application extension, see “Application Extension Configuration” on page 83.



Queue Control

○ Basic

○ Advanced

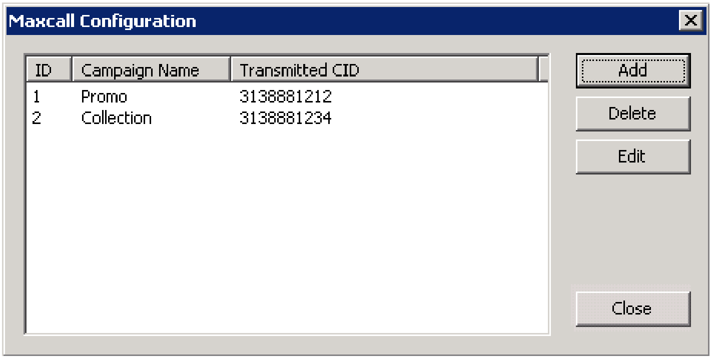
● Application Extension 5999

Figure 176. Workgroup Configuration, Queue Management tab, Application Extension Queue Control

MaxCall Configuration

The MaxCall Configuration screen is for entering Transmit CID numbers to be used when an agent uses the MaxCall application to play a phrase to a callee. The campaign names and transmit Caller IDs that you enter here appear in a list on the MaxCall tab in MaxAgent, MaxCommunicator, and MaxOutlook. The agent selects a CID by campaign name before handing a call off to MaxCS. Then MaxCS plays the phrase the agent selected.

To begin, select **Call Center** > **MaxCall Configuration**.



ID	Campaign Name	Transmitted CID
1	Promo	3138881212
2	Collection	3138881234

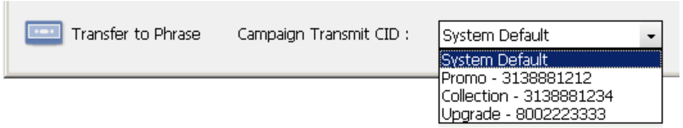
Figure 177. MaxCall Configuration screen

- **ID** – Campaign IDs are assigned sequentially by the MaxCS system.
- **Campaign Name** – The name you give to a calling campaign.
- **Transmitted CID** – The caller ID to transmit to the callee when an agent makes a call and uses MaxCall to play a phrase to the callee’s phone.

Adding a Transmitted CID

1. Click the **Add** button. The Campaign and Transmitted Caller ID dialog box opens:
2. Enter a campaign name and a caller ID to transmit when this campaign is chosen by the agent. Click **OK**.

The campaign names and caller IDs then appear in MaxAgent, MaxCommunicator, and MaxOutlook in the MaxCall tab list:



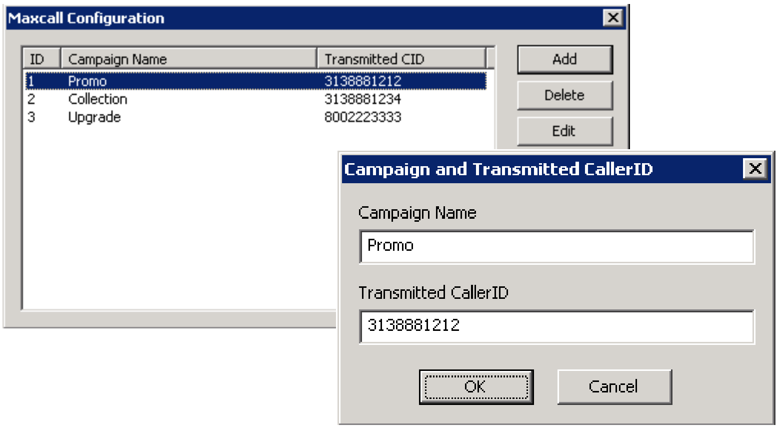
Campaign Transmit CID : System Default

System Default
Promo - 3138881212
Collection - 3138881234
Upgrade - 8002223333

Editing/Deleting Transmitted Caller IDs

To review a transmitted CID,

1. Select a campaign and click the **Edit** button.



ID	Campaign Name	Transmitted CID
1	Promo	3138881212
2	Collection	3138881234
3	Upgrade	8002223333

Campaign Name: Promo

Transmitted CallerID: 3138881212

Figure 178. Choosing a Caller ID Campaign

2. Make your changes, and click **OK**.

To remove a campaign, select it and click the **Delete** button. The entry is deleted.

Callback from Queue

The Callback feature lets you 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. Or 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 3 to remain on hold.
>
> Please say your name. When you have finished speaking, press the # key.
>
> Your name was recorded as <caller name>. Press 1 to continue or press 3 to re-record your name.
>
> You will be called at <incoming phone number>. Press 1 to confirm this number, or press 3 to be called at a different phone number.
>
> Please enter the 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 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.
>
> We are sorry that we are unable to reach <caller name>. We will try again later. Goodbye."

Types of Callbacks

There are two different types of Callback configurations:

- **Redirected Callback** - This type of callback was in earlier releases of MaxCS. With this configuration, one workgroup offers a callback option to callers in the queue, and a different workgroup actually handles the return calls.

- **Reserved Callback** - This is a new callback type offered beginning in Release 8.6.1. In this configuration, a single workgroup does it all - offers the callback option and places the return calls.

Callback 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.
- 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 from Queue 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 enabled for the Callback feature, the user must have either a seat license or must be using an available session license. If no session licenses are available, then the user 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 a separate Callback license for each workgroup.

Before You Begin

Perform these steps before you begin to configure workgroups for the callback feature.

1. Acquire the appropriate number of seat and/or session licenses, and assign any seat licenses to the appropriate agents.
2. If you will not be using the default phrases provided by Altigen, record custom phrases for the Callback Reconnect announcement and any Callback phrases. For instructions on recording phrases from your

Altigen phone or on using professionally recorded phrases, see the section *Phrase Management* on page 67. Callback phrases are stored in C:\PostOffice\phrases\LangCustom.

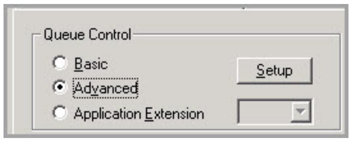
Following is a list of some of the phrases that are provided for the Callback feature:

Phrase #	Phrase
Callback1	This is a callback for...
Callback	You can also press 1 to schedule a callback.

Configuring a Single Workgroup for Reserved Callback

To configure a workgroup that both offers a return call and then handles those return calls,

1. On the Workgroups page, select the workgroup that you want to configure. Switch to the *Queue Management* tab.
2. In the *Queue Control* group, select **Advanced** and click the **Setup** button.



Queue Control

○ Basic
● Advanced
○ Application Extension

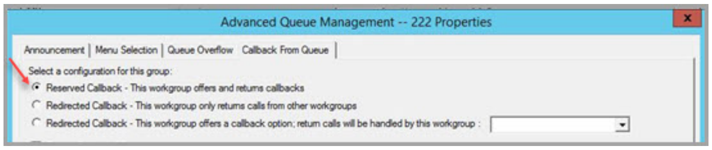
Figure 179. Click the Setup button on the Queue Management tab

3. On the *Announcement* tab, select the phrase for the *Callback Phrase* entry. This phrase will be played after each queue update for those calls that meet the callback criteria.

   You can select **Queue position**, **Expected Wait Time**, or both. See *Announcement Tab* on page 274 for details.
4. On the *Menu Selection* tab, add the action “Callback from Queue” to whichever key you've told them to press. See *Menu Selection Tab* on page 274 for details.

Important: If you do not specify an action here, the Callback from Queue feature will not be enabled.

5. On the *Callback from Queue* tab, select the first option: **Reserved Callback - This workgroup offers and returns callbacks.** Making your selection will enable the other fields that you must configure.



Advanced Queue Management -- 222 Properties

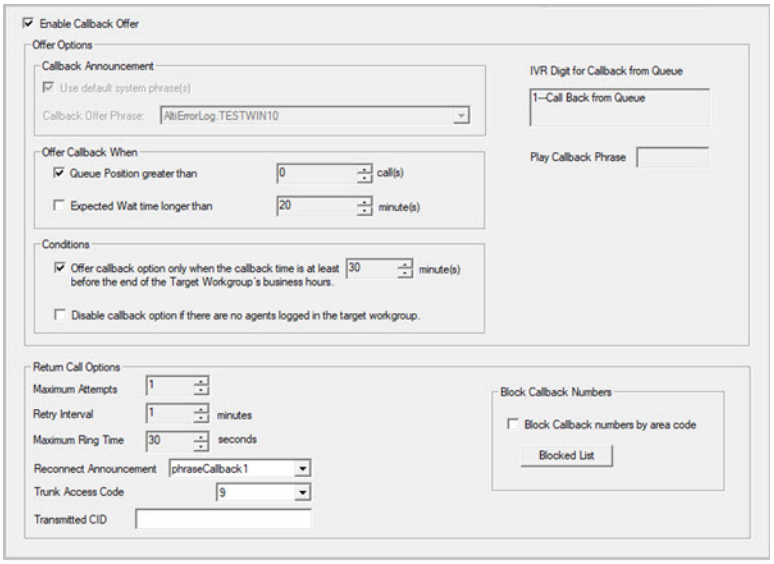
Select a configuration for this group:

● Reserved Callback - This workgroup offers and returns callbacks
○ Redirected Callback - This workgroup only returns calls from other workgroups
○ Redirected Callback - This workgroup offers a callback option; return calls will be handled by this workgroup :

Figure 180. Select the first callback type

6. Configure all options on that tab.

   The upper section has your “offer” options; the lower section is where you set the return call options. For explanations these options, see *Offer Options* on page 281 and *Return Call Options* on page 282.



☑ Enable Callback Offer

Offer Options

Callback Announcement

☑ Use default system phrase(s)

Callback Offer Phrase: AltiErrorLog.TESTWIN10

Offer Callback When

☑ Queue Position greater than 0 call(s)

□ Expected Wait time longer than 20 minute(s)

Conditions

☑ Offer callback option only when the callback time is at least 30 minute(s) before the end of the Target Workgroup's business hours.

□ Disable callback option if there are no agents logged in the target workgroup.

IVR Digit for Callback from Queue: 1--Call Back from Queue

Play Callback Phrase:

Return Call Options

Maximum Attempts: 1

Retry Interval: 1 minutes

Maximum Ring Time: 30 seconds

Reconnect Announcement: phraseCallback1

Trunk Access Code: 9

Transmitted CID:

Block Callback Numbers

□ Block Callback numbers by area code

Figure 181. The Offer and Callback options

7. If you are ready for that workgroup to begin offering callbacks, select the **Enable Callback Offer** option near the top of the tab.
8. Click **Save**.

Offer Options

Following are descriptions for the various callback offer options.

Offer Option	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 which workgroup will be handling the return calls. 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 option. This is because you've specified a minimum 20-minute buffer, but the return call would be placed 15 minutes before the end of the workday.

Offer Option	Description
Disable callback option if there are no agents logged into the target workgroup	This option disables the callback option if the system detects that there are no agents logged in to take the callback call.

Return Call Options

Following are descriptions for the various return call options.

Return Call Option	Description
Maximum Attempts	The number of times the system will attempt another call if the initial return call fails. 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 drop-ping the call.
Reconnect Announcement	The phrase that announces your company name; this phrase is used at the beginning of the return call, to identify the organization that is calling.
Trunk Access Code	The trunk access code that will be used when placing the return call.
Transmitted CID	The Caller ID that will be transmitted when placing the return call. This phone number is also logged in the Target Number field of the callback attempt CDR records.

Configuring Two Workgroups for Redirected Callback

Configuring *Redirected Callback* is a slightly different process from setting up a *Reserved Callback*, in that you must configure two different workgroups to each perform their role. One group will offer the return calls; the other group will handle the return calls.

Note: The workgroup offering the callback option and the workgroup that will handle the return calls must be on the same server. We recommend that you allocate a single workgroup to handle all callback calls, to simplify reporting of incoming and Callback calls.

You must configure the **target** workgroup before you can configure the workgroup that will be offering a callback option.

Note: Callback for international calls is not supported.

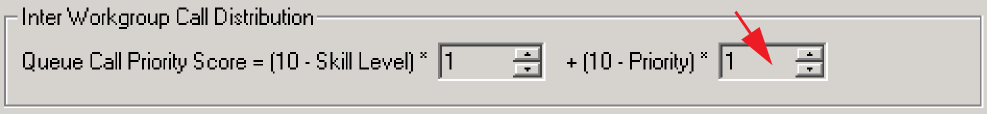
Step A: Configure the Target Workgroup to Handle Return Calls

Note that a target group can handle return calls from multiple workgroups.

1. On the Workgroups page, select the target workgroup - the group that will handle the return calls. Switch to the *Queue Management* tab.
2. In the *Queue Control* group, choose **Advanced** and click **Setup**.
3. If this workgroup has already been set up to handle the return calls for another group, skip ahead to Step B. Otherwise,
    a. On the *Callback from Queue* tab, select the second option, **Redirected Callback - This group only returns calls from other workgroups**. Making your selection will enable the other fields that you must configure.
    b. Configure the fields in the *Return Call Options* section. For explanations of each option, refer to *Return Call Options* on page 282.
4. Click **Save**.

Note: You will not enable the Callback feature yet; you will do this during Step B.

5. We recommend that you set the target 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, increase the value of the Inter Workgroup Call Distribution parameter.



Inter Workgroup Call Distribution

Queue Call Priority Score = (10 - Skill Level) * 1 + (10 - Priority) * 1

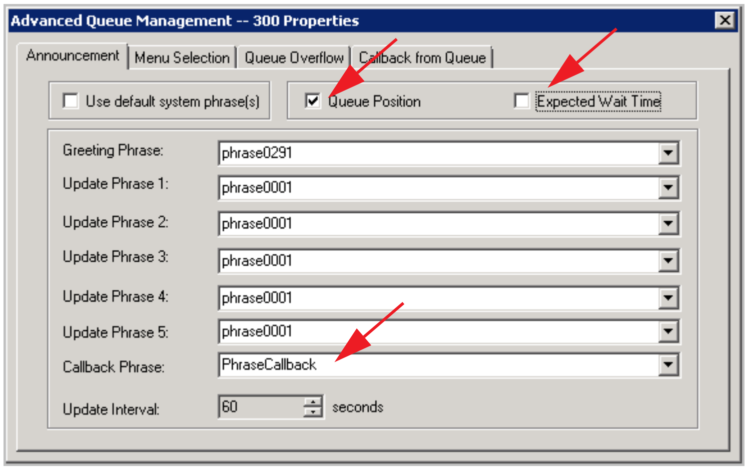
Figure 182. Inter-Workgroup Call Distribution options

Step B: Configure the Group that Will Offer the Callback Option

Next, configure the other workgroup, the one that will offer a callback option to callers waiting in the queue.

1. Select the offering workgroup in the list and switch to the *Queue Management* tab.
2. In the *Queue Control* group, select *Advanced* and click the **Setup** button.
3. On the *Announcement* tab, select the phrase for the *Callback Phrase* entry. This phrase will be played after each queue update for those calls that meet the callback criteria.

   You can select **Queue position**, **Expected Wait Time**, or both. See *Announcement Tab* on page 274 for details.



Advanced Queue Management -- 300 Properties

□ Use default system phrase(s)

☑ Queue Position

□ Expected Wait Time

Greeting Phrase: phrase0291

Update Phrase 1: phrase0001

Update Phrase 2: phrase0001

Update Phrase 3: phrase0001

Update Phrase 4: phrase0001

Update Phrase 5: phrase0001

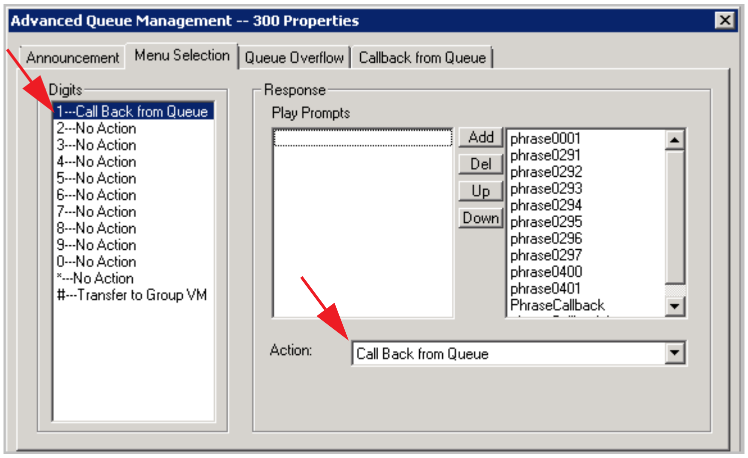
Callback Phrase: PhraseCallback

Update Interval: 60 seconds

Figure 183. The options on the Announcements tab

4. On the *Menu Selection* tab, add the action "Callback from Queue" to whichever key you've told them to press. See *Menu Selection Tab* on page 274 for details.

Important: If you do not specify an action here, the Callback from Queue feature will not be enabled.



Digits:

1---Call Back from Queue
2---No Action
3---No Action
4---No Action
5---No Action
6---No Action
7---No Action
8---No Action
9---No Action
0---No Action
*---No Action
#---Transfer to Group VM

Action: Call Back from Queue

Figure 184.   The Callback from Queue action on the Menu Selection tab

5. On the *Callback from Queue* tab, select the third option: **Redirected Callback - This workgroup offers a callback option; return calls will be handled by this workgroup:**
6. In the adjacent field, pull down the menu and choose the 'target' workgroup that you configured in *Step A: Configure the Target Workgroup to Handle Return Calls*. Only those workgroups that have already been configured to handle return calls will be included in this list.
7. Configure the options in the “Offer Options” group. See *Offer Options* on page 281.
8. (Optional) If you are ready for this group to begin offering return calls, select **Enable Callback Offer** near the top.
9. Click **Save**.

Enabling and Disabling the Callback Feature for a Workgroup

Once you have configured workgroups to offer and handle return calls, you can easily enable and disable the feature as needed.

To disable the Callback feature, clear the **Enable Callback Offer** option and click **Save**. For Redirected Callback configuration, this option is found on Callback from Queue tab of the *offering* workgroup.

Blocking Area Codes from the Callback Option

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

1. In the *Callback from Queue* tab, in the *Return Call Options* section, check the option **Block Callback Numbers by Area Code**, and then click **Blocked List**.

   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.

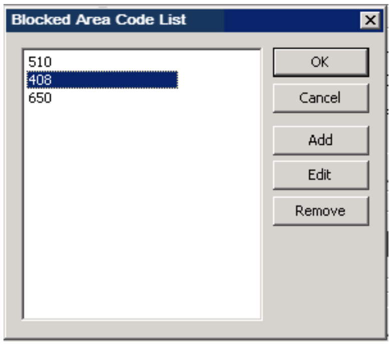


Figure 185. The Blocked Area Code list

Reserved Callback Reports

The following reports generate data on Reserved callback.

- (Agent) Reserve Agent Callback Summary Report (1207)
- (WG) Reserve Agent Callback Summary Report (2211)

Operational Notes for the Callback Feature

- Return calls to US Domestic and toll-free numbers are allowed.
- Return calls to International and 900 numbers **are not supported**.
- Note that callers can request a call back multiple times; for example, a caller can choose the callback option and leave a phone number, hang up, call in again, and request another return call.
- In some cases, the announcements may begin playing before the party answers the return call. The announcements will repeat, to make sure 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. The extension must be in Idle state to accept a return call.
- 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). When you enable callback, the *Busy Call Handling*, *No Answer Call Handling, Forward all calls*, and *Group RNA Handling* options will be disabled. The *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 queue control can only be set to *Basic*.

- If a return 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.
- Callback data can be found throughout the MaxCS product. Callback data appears in CDRs and in CDR Search, in various view in MaxAgent and MaxSupervisor, in reports 2206 and 2207 and a new report, *Callback Detail Report.*
- When you configure callback for a workgroup, then the Basic option on the *Queue Management* tab (in the *Queue Control* group) becomes disabled.
- In general, callback calls are handled in the order in which they entered the workgroup queue, regardless of how soon they chose the callback option. However, once a caller chooses the callback option and begins the process of leaving a name and phone number, that call will not be answered *even if it is the next call in the queue*. That call will be skipped, and the next call in the queue behind it will be answered.
- When the system is configured to use Account Codes, callback calls may not offer the agent a pop-up window to choose an account code for the call.
- If you have previously configured any Advanced mode queue options, and then later you attempt to switch back to Basic mode, you will be warned that you are disabling all advanced queue management features.

  In addition, if you have previously configured Callback from Queue for any workgroups, then you are prompted to disable the callback offer. When you click OK, the Advanced Queue Management Callback tab opens for you. Disable the callback feature and click OK; MaxAdmin will then switch the mode from Advanced back to Basic.
- Reserved Callback is not supported for the *Ring All Available Members* option (Intra Group Call Distribution).

CHAPTER

24

Reason Code Configuration

The Reason Code Configuration window is where you can configure various codes within MaxCS:

- Agent Logout Reason codes; see *Logout Reason Codes* on page 287
- Agent Not Ready Reason codes; see *Not Ready Reason Codes* on page 288
- Call Disposition codes; see *Call Disposition Codes* on page 290

To open this window, select **Call Center** > **Reason Code Configuration**.

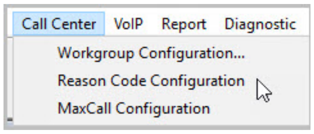


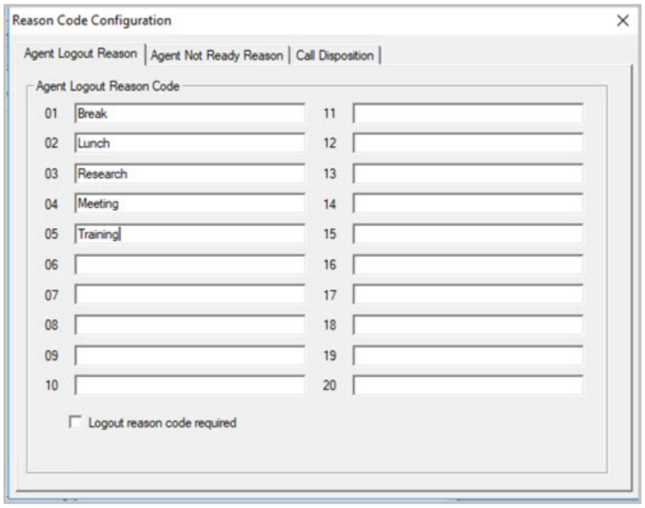
Figure 186. The Reason Code Configuration option

Logout Reason Codes

Logout reason codes allow agents to specify why they are signing off from the workgroup, and the manager can view that information. If logout reasons are required, the system requests a reason at logout from the phone set and from the Agent application.

The **Agent Logout Reason Configuration** window lets you require a logout reason, and it provides for defining up to 20 reason codes. A logout history can be tracked and stored for future analysis.

To access this window, select **Call Center** > **Reason Code Configuration**.



01	Break	11	
02	Lunch	12	
03	Research	13	
04	Meeting	14	
05	Training	15	
06		16	
07		17	
08		18	
09		19	
10		20	

☐ Logout reason code required

Figure 187.   Agent Logout Reason Code configuration window

To define reason codes, type the associated reason into the text box next to the code you want to associate with the reason.

To force agents to specify a reason code each time they log out, select the **Logout reason code required** check box. If you don’t want to require reason codes, deselect the check box.

The following logout codes are system codes:

- 00 - Either agents are not required to enter logout codes, or 00 indicates a logout code of ‘Other’
- 96 - The agent’s IP extension was logged out by the system due to a network error
- 97 - The agent’s IP or physical extension changed to a virtual extension, and the system logged the extension out of the workgroup
- 98 - The supervisor manually logged the agent out of the workgroup
- 99 - The system automatically logged the agent out of the workgroup based on the workgroup’s configuration for RNA (set on the Workgroup tabs).

Not Ready Reason Codes

Agent Not Ready codes allow agents to specify why they are changing their status to *Not Ready*.

You can make these codes mandatory or optional.

Creating a List of Not Ready Reason Codes

1. In MaxAdmin, choose **Call Center** > **Reason Code Configuration**.
2. Switch to the *Agent Not Ready Reason* tab.
3. In the table, enter the various reason codes that you want to present to your agents, one per field. For example, you might include terms such as *Research*, *Making Notes*, and so on.
4. (Optional) If you want to require agents to specify a Not Ready reason code, then check the option *Not Ready Reason Code Required*. To make entry of reason codes optional, leave the checkbox cleared. Click **OK**.

The following codes are system Not Ready Reason codes:

- 97 - Supervisor Override
- 98 - The system automatically set the agent to Not Ready based on the workgroup's configuration for RNA (set on the Workgroup tabs).
- 99 - The system automatically set the agent to Not Ready because the agent did not enter a required Call Disposition Code.

Not Ready Reason Codes in MaxAgent

If you select the option *Not Ready Reason Codes Required*, then agents will not be able to set their status to Not Ready until they enter a code. A pop-up will open if they click to change their status. If they click **Cancel**, they will see a warning message and will remain in Ready state.

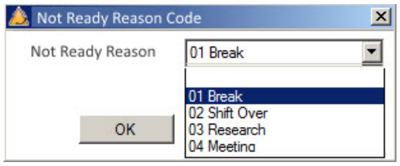


Figure 188. What the agent sees within MaxAgent

If you do not select the option *Not Ready Reason Codes Required*, then the pop-up will still open, but they will have a blank option in the pulldown menu that they can choose instead of a reason code.

The Not Ready Reason Code is a system wide option; if you force the entry of Not Ready Reason codes, then agents will no longer be able to use #91 (Not Ready) from their phones.

Not Ready Reason Codes in MaxSupervisor

In MaxSupervisor, users will see the Not Ready Reason code in the Agent State display. The code will also appear in the Agent View and Workgroup View > Agent State views.

Reports Which Include Not Ready Reason Codes

Not Ready Reason codes will appear in Report 1101.

- The state (Not Ready) will appear in an Activity Type column
- A new column shows the Not Ready Duration
- A new Reason column shows the reason for each Not Ready event.

Not Ready Code with #91 Feature Code

Beginning in Release 9.0.1, a change has been made to behavior when Not Ready Reason code Required is enabled.

After the agent enters #91, the agent is prompted to enter a code. While the agent is entering a Reason Code, the agent's status is Busy.

- If the agent enters two digits, then the reason code entry is processed immediately.
- If the agent does not enter any digits or only enters 1 digit, the system waits 7 seconds for input.

If the reason code is valid, the agent will hear "This extension will not receive workgroup calls. Enter #90 to start receiving workgroup calls again." The agent state is then set to Not Ready, and this call is disconnected.

Call Disposition Codes

Admins can now set up custom Call Disposition codes. These codes are typically descriptions of the final outcome of the call, and are a simple way to label or categorize calls.

For example, a Technical Support organization may choose to set up Call Disposition codes of Resolved, Researching, Feedback, Follow up, and so on. A service organization may set up Call Disposition codes such as Appointment Scheduled, Product Question, Service Inquiry, and so on.

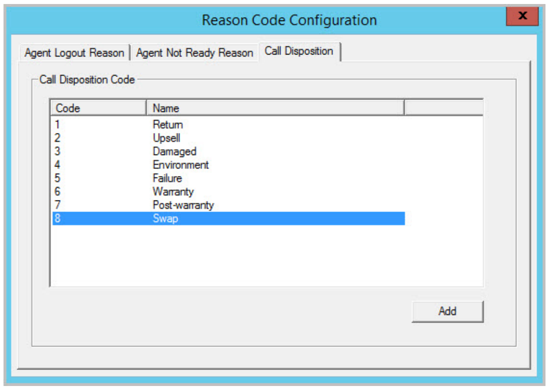
Please take the following behavior into account when designing and implementing Call Disposition Codes:

- Be aware that Disposition Codes **cannot be removed once they are configured**.
- We strongly recommend that you do not change Disposition Codes once they are configured, because this will skew any report data. You should add new codes rather than change existing codes.
- Call Disposition codes can be made mandatory or optional for individual workgroups.
- During a call, agents can change a Disposition Code if they have already specified one. The last code the agent chooses will be retained.
- For internal workgroup calls, if the agents enter different Disposition codes for the call, the code that was entered last will be stored. In other words, If Agent A calls Agent B, and Agent B enters a Disposition code **after** Agent A enters one, whichever code Agent B enters will be saved.

Creating Global Call Disposition Codes in MaxAdmin

Before you can assign Call Disposition codes to workgroups, you must add them into the MaxCS system.

1. In MaxAdmin, choose **Call Center** > **Reason Code Configuration**.
2. Switch to the *Call Disposition* tab.
3. In the table, click **Add**, and then enter the label for this disposition code. Click **OK**.



Code	Name
1	Return
2	Upsell
3	Damaged
4	Environment
5	Failure
6	Warranty
7	Post-warranty
8	Swap

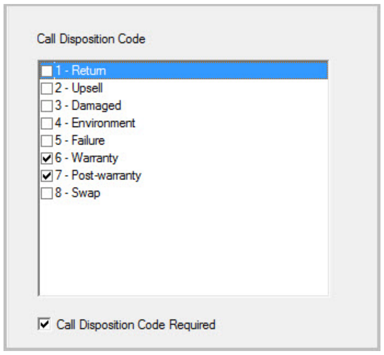
Figure 189. Creating a system list of Call Disposition Codes

Configuring Disposition Code Options for a Workgroup

You can specify which Call Disposition codes apply to each workgroup. You can also specify, for each workgroup, whether Disposition Codes are required or optional. If you want to require Disposition Codes, you can require them for inbound workgroup calls, for outbound workgroup calls, or for both.

1. Open the Workgroup Configuration panel. Select the workgroup.
2. Switch to the *Call Disposition* tab.
3. Select the codes that you want to make available for that workgroup (up to 64).

4. **I**f you want to enforce Disposition codes, first check the option **Call Disposition Code Required**. Then select whether you want to enforce codes for inbound, outbound, or both types of workgroup calls. Click **Ok**.



Call Disposition Code

- ☐ 1 - Return
- ☐ 2 - Upsell
- ☐ 3 - Damaged
- ☐ 4 - Environment
- ☐ 5 - Failure
- ☑ 6 - Warranty
- ☑ 7 - Post-warranty
- ☐ 8 - Swap

☑ Call Disposition Code Required

Figure 190. Selecting the specific Disposition Codes that apply to a workgroup

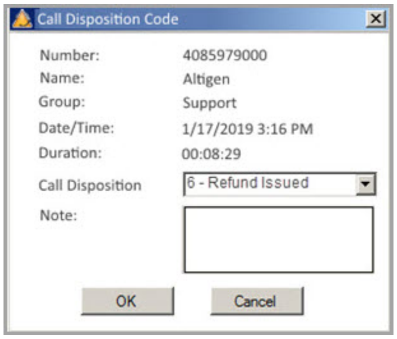
Considerations When Enforcing Call Disposition Codes

Before you enable the *Call Disposition Code Required* option, be aware of the following behavior.

- Agents who do not enter call a Disposition Code for a call will automatically be set to Not Ready. This will leave you with fewer agents available to handle incoming calls. For example, if you have 3 workgroup agents logged in and one of those agents has not entered a Disposition Code for a call and has been set to *Not Ready*, that leaves your workgroup with only two agents able to handle incoming calls.
- Agents can ignore the Disposition Code popup and place outgoing calls on physical extensions. (For IPTalk extensions, the system will prevent the agent from placing calls until the agent enters a code.) Note that you can run report 1305 to detect agent Not Ready status with a reason code of *Disposition Code*.
- Agents who have physical phones can answer an incoming workgroup call without opening the MaxAgent application. When the agent hangs up the call, the system sets this agent to *Not Ready* until a Disposition code is entered. However, if the agent does not have MaxAgent open, the agent will not be aware that a Disposition Code is required to return to *Ready* mode. Therefore, in order for this feature to work effectively, agents must have the MaxAgent application open - even those who take calls on a physical phone.

How Agents Enter Disposition Codes When Codes are Required

When a workgroup call is disconnected, the Disposition Code dialog opens in MaxAgent to allow the agent to select a code for this call.



Number: 4085979000
Name: Altigen
Group: Support
Date/Time: 1/17/2019 3:16 PM
Duration: 00:08:29
Call Disposition 6 - Refund Issued
Note:

Figure 191. The Disposition Code pop-up that is displayed to the agent

The agent can also enter any appropriate notes for this call.

Be aware of the following behavior within MaxAgent:

- The popup will remain in the foreground until the agent enters a code.
- The Cancel button in this popup will be disabled, because the agent must select a code.
- MaxCS will not present the agent with another workgroup call until a Disposition Code has been entered in MaxAgent. Personal calls to the agent will still come in, even while incoming workgroup calls are blocked.
- The agent cannot close MaxAgent normally if a Disposition Code popup remains open.
- If the agent state becomes available (after any wrap-up interval has passed), MaxCS sets the agent's state to Not Ready, with a Not Ready Reason Code of Disposition Code. This allows supervisors to determine whether agents are avoiding calls by not entering a required Disposition Code.
- If the MaxAgent application goes down mid-call for some reason, Disposition Codes for the interrupted call will no longer be required when the agent re-opens MaxAgent. The Call Disposition Codes feature requires that MaxAgent be running during calls.

How Agents Enter Disposition Codes When They are Not Required

Agents can still enter Disposition codes, even if the workgroup does not require codes to be entered. Agents can right-click the call and select Call Disposition Code from the menu.

Reports Which Include Call Disposition Codes

New reports have been added:

- Workgroup Call Disposition Code Summary report (2320)
- Call Disposition Code Summary Report by DNIS (3301)
- Call Disposition Code Summary Report by Agent (1305)

The following reports also include Disposition Code data:

- Agent Call Detail Report (1102)
- Workgroup Call Detail Report (2101)
- DNIS Call Detail Report (3101)

Call Disposition Code Data in CDRs

The following tables have been updated for Call Disposition Code data:

CDRMAIN Table

- DispositionCode (int, null): new column
- DispositionDescription (varchar(64), null): new column
- DispositionNote (varchar(256), null): new column

DISPOSITIONCODE: New Table

- Version (int, not null)
- NodeID (int, not null)
- Code (int, not null)
- Description (varchar(32), not null)
- StartTime (int, null)

- EndTime (int, null)
- StartTimeGMTOffset (int, null)
- EndTimeGMTOffset (int, null)
- RevisionID (int, not null)

CHAPTER

25

Location-Based E911

This feature is designed for roaming users who log into various IP phones at different locations, to use those phones as their extension.

E911 Caller ID (CID) information is sent to PSAPs (Public Safety Answering Point) when a user calls 911 from an IP phone. A new feature has been added to MaxCS that allows administrators to configure unique E911 Location IDs for specific locations. Each Altigen IP phone can then be assigned an appropriate E911 Location ID.

Configuring E911 Location IDs ensures that emergency calls placed from these IP phones:

- Will call the appropriate PSAP, based upon the phone's physical location.
- Will transmit the appropriate Caller ID information that will help emergency response teams find the right physical address.

E911 Location ID is supported by Polycom phones. Refer to the MaxCS Polycom Configuration Guide for details.

About E911 Location IDs

Each Location ID entry will contain the following information:

- The phone number of the local PSAP
- The E911 Caller ID (which is used by PSAPs to determine the correct street address) which is transmitted to emergency personnel when an emergency call is placed
- A default callback phone number (optional)

E911 Location ID information is associated with the IP phone itself, rather than being tied to a specific user or extension. This way, no matter who logs into an IP phone, the correct E911 Location ID will be transmitted during an emergency call.

Once these E911 Location IDs are configured within MaxAdministrator, administrators can either push the correct information to the Altigen IP phones or update the E911 information on each Altigen IP phone via the phone's menus.

Administrators can also configure whether users must enter a password in order to update an IP phone's assigned E911 Location ID themselves.

Note: When an IP phone is moved to a different location, the Administrator must update the phone's E911 Location ID accordingly, either by pushing it from within MaxAdministrator or by requesting that a user update the IP phone via the phone's menus.

Designing E911 Location IDs for Your Organization

Administrators can set up various E911 Location IDs (up to 10,000).

The strategy of how you implement E911 Location IDs will depend upon your unique business.

Some businesses may choose to set up location IDs for each building in a complex, something similar to this:

- Location ID 10 - Building 315 West
- Location ID 11 - Building 315 Warehouse
- Location ID 20 - Building 316
- Location ID 30 - Building 317

Or, if you have various branch offices, your Location ID schema may look more like this approach:

- Location ID 1 - San Jose
- Location ID 2 - Palo Alto
- Location ID 3 - Redwood City
- Location ID 4 - Sunnyvale

Another organization may choose to create different E911 Location IDs for each floor of a large office building, similar to this approach:

- Location ID 1 - Basement/garage
- Location ID 2 - Floor 1
- Location ID 3 - Floor 2
- Location ID 4 - Floor 3

Yet another schema could be to implement E911 Location IDs by the type of use of various building sections, by floor, similar to the following method. This convention uses the first digit as the floor and the second digit as an area within that floor.

- Location ID 11 - Warehouse
- Location ID 12 - Floor 1 Lab 1
- Location ID 13 - Floor 1 Lab 2
- Location ID 14 - Floor 1 Shipping/Receiving
- Location ID 15 - Floor 1 Manufacturing
- Location ID 21 - Floor 2 Test Lab
- Location ID 22 - Floor 2 Imaging

What's important is to come up with a set of entries that works for you, based upon your type of organization and your geographic specifics.

Altigen IP Phones Supporting E911 Location IDs

The following Altigen IP phones are supported:

- IP 705 (requires firmware version 22A6)
- IP 710 (requires firmware version 21A6)
- IP 720 (requires firmware version 23A6)
- IP 805 (requires firmware version 21, which will appear as “1121” in MaxAdministrator and on the phone itself)

If an IP phone does not have the correct firmware version, then you cannot configure an E911 Location ID for the phone until you upgrade its firmware.

New Altigen IP phones are shipped with the default E911 Location ID entry of 0.

The following phones are not supported:

- Altigen IP 600
- Analog phones connected to the MaxCS server
- Other 3rd party SIP phones

E911 Hierarchy

Beginning in Release 8.5 Update 1, MaxCS has a new option: *System E911 Caller ID*. Refer to *Setting General Parameters* on page 31.

The system follows this hierarchy to retrieve E911 information when a user places a 911 call from an IP phone:

1. If a Location ID has been assigned to the extension (**PBX** > **Location Based E911 Configuration** > **View E911 Assignments**), then the E911 CID associated with the assigned LID will be sent during an E911 call from the extension.
2. If no Location Based E911 LID has been configured for the extension, then the extension's configured E911 CID will be sent.
3. If there is no extension E911 CID configured for the extension, then the new **System E911 CID** will be sent.
4. If no System E911 CID has been configured, then the extension's Transmitted CID will be sent.
5. If the extension does not have a Transmitted CID configured, then the extension's DID number will be sent (if it is 10 digits or longer)
6. If there is no DID number associated with the extension, then the trunk's Transmitted CID will be sent set in the *Trunk Configuration* window)
7. If the area code and phone number have not been configured for the trunk, then the System Main number in the System Configuration window will be sent.

E911 Location ID Configuration Process

Following is an overview of how to configure E911 data for IP phones:

1. Administrators create a Location ID schema and plan various E911 Location IDs, one for each site, floor, or building.
2. Administrators configure password protection, so that changing the E911 information for a phone requires a user to enter a password (optional). See *Requiring a Password to Change E911 Location ID* on page 299 for details.
3. Administrators view (and update) the E911 assignments for IP phones. Administrators can either push the updated information to the phones or have users enter the appropriate information on the phone itself.

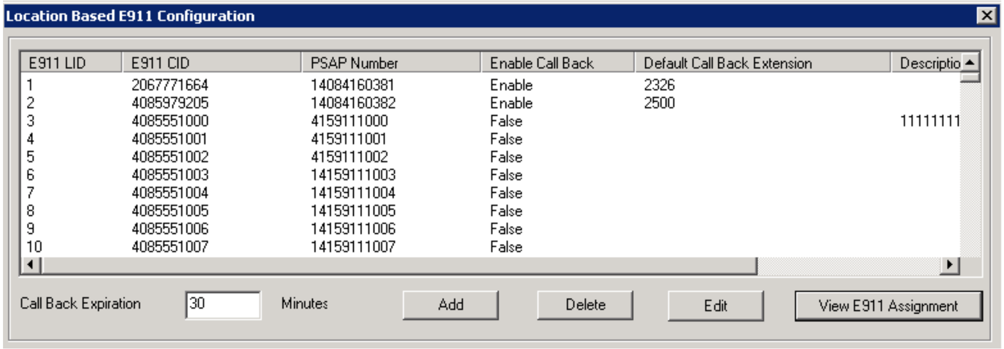
Creating the E911 Location ID Table

To configure location-based E911 information,

1. Select **PBX** > **Location Based E911 Configuration**.

Note: If you are a Basic Admin user or a Supervisor user, some menu choices and options may not be available for you. Only Full Admin user types will see all menu commands and options.

The panel shows the current E911 entries. To sort the table, click a column heading.



E911 LID	E911 CID	PSAP Number	Enable Call Back	Default Call Back Extension	Descriptio
1	2067771664	14084160381	Enable	2326	
2	4085979205	14084160382	Enable	2500	
3	4085551000	4159111000	False		11111111
4	4085551001	4159111001	False		
5	4085551002	4159111002	False		
6	4085551003	14159111003	False		
7	4085551004	14159111004	False		
8	4085551005	14159111005	False		
9	4085551006	14159111006	False		
10	4085551007	14159111007	False		

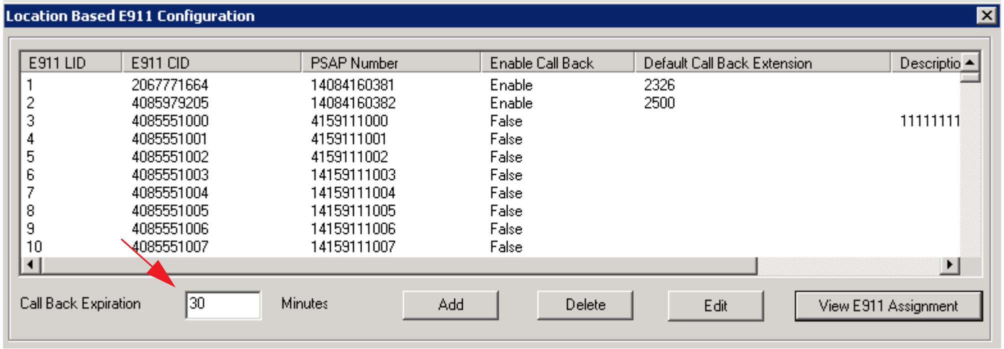
Call Back Expiration 30 Minutes

Figure 192. The Location Based E911 Configuration panel

The following table describes the information shown in this panel.

E911 Location Parameter	Description
E911 LID (Location ID)	1-10,000. Enter a unique number for this entry.
E911 CID (Caller ID)	The local E911 Caller ID which is used as a Caller ID when the extension places an emergency call. This field is also unique; each E911 LID must have a different E911 CID.
PSAP (Public Safety Answering Point) Number	When this extension makes a local E911 call, this is the PSAP number that will be called.
Enable Callback	This setting determines the routing for the call back from the PSAP center. • With Callback enabled, the callback call will route to the default callback extension defined in the E911 Location ID configuration. • With Callback disabled, call will be routed to the standard incoming call routing of MaxCS, regardless of the E911 call history. The default setting is **Disabled**.
Default callback extension	The default call back extension; this applies only if Callback is enabled. • If the DNIS number from the PSAP does not match the designated CID from the call history, then the response call will be routed to this callback extension. • If you do not enter a default callback extension, the response call goes through the standard incoming call routing.
Description	A brief description for this E911 LID entry.

2. Below the table, for the **Call Back Expiration Time xx Minutes** option, set the global expiration time for E911 response calls. The default interval is 30 minutes.



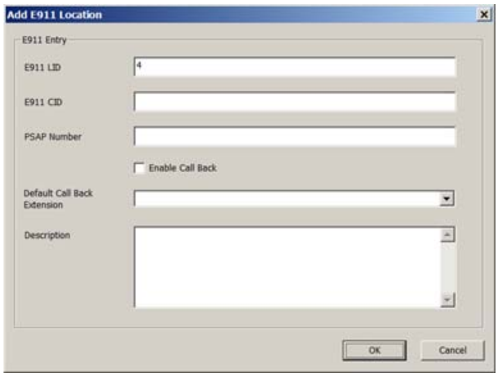
E911 LID	E911 CID	PSAP Number	Enable Call Back	Default Call Back Extension	Descriptio
1	2067771664	14084160381	Enable	2326	
2	4085979205	14084160382	Enable	2500	
3	4085551000	4159111000	False		11111111
4	4085551001	4159111001	False		
5	4085551002	4159111002	False		
6	4085551003	14159111003	False		
7	4085551004	14159111004	False		
8	4085551005	14159111005	False		
9	4085551006	14159111006	False		
10	4085551007	14159111007	False		

Call Back Expiration: 30 Minutes

Figure 193. The Call Back Expiration field

When *Enable Callback* is checked, this field sets the expiration time for the routing of response calls. Response calls will be routed to the last extension that placed an E911 call if the response arrives within that expiration time. After this interval has expired, response calls will be routed using the standard incoming call routing configured in MaxCS.

3. Click **Add**.



E911 LID: 4

E911 CID:

PSAP Number:

☐ Enable Call Back

Default Call Back Extension:

Description:

Figure 194. Add a new E911 Location entry

4. In the dialog box, complete each field and click **OK**. Refer to the table on page 298 for field descriptions.

Note: In order to support E911 LIDs across multiple servers, such that if one server fails the other will correctly handle E911 LID calls, we recommend that each server have an identical list of E911 Location IDs.

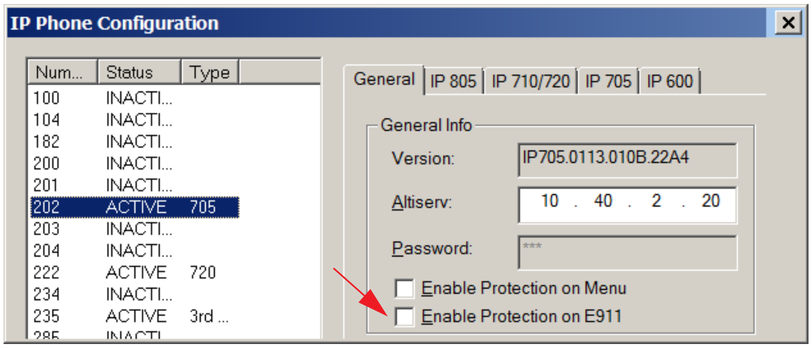
Note that you can change LIDs only for active phones.

Requiring a Password to Change E911 Location ID

Administrators can configure whether users must enter a password in order to update an Altigen IP phone's assigned E911 Location ID. This requirement can be enabled or disabled for each individual IP phone.

To enable password protection for a phone's E911 information,

1. Select **PBX** > **Altigen IP Phone Configuration**.
2. On the *General* tab, select the phone in the left panel and then check the **Enable Protection on E911** checkbox.



IP Phone Configuration

Num...	Status	Type
100	INACTI...	
104	INACTI...	
182	INACTI...	
200	INACTI...	
201	INACTI...	
202	ACTIVE	705
203	INACTI...	
204	INACTI...	
222	ACTIVE	720
234	INACTI...	
235	ACTIVE	3rd ...
285	INACTI...	

General Info

Version: IP705.0113.010B.22A4

Altiserv: 10 . 40 . 2 . 20

Password: ***

□ Enable Protection on Menu

□ Enable Protection on E911

Figure 195. Enable password protection for E911 entry

3. Once you check that checkbox, the **Password** field above it becomes active. Enter a password. Your entry will be the password that the user must enter in order to change the Location ID assigned to the phone. Click **OK**.

Note: You can use the *Apply To* feature to apply this requirement and the password to multiple phones.

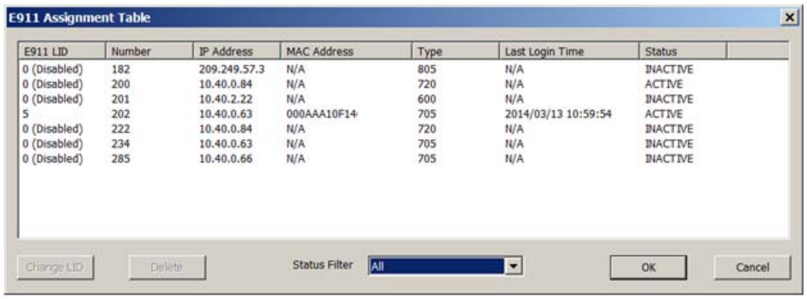
Assigning/Changing E911 Locations on Altigen IP Phones

Administrators can either push the correct E911 Location ID to an Altigen IP phone, or they can have users enter the correct ID manually on the IP phone itself.

To push an E911 Location ID assignment to an Altigen IP phone, follow these steps.

1. Select **PBX** > **Location Based E911 Configuration**.
2. Click **View E911 Assignments**.

   The table lists devices that have, at some point, registered with MaxCS.
3. Click a column to sort the table. You can also filter the data by choosing **All**, **Active**, or **Inactive** from the *Status Filter* pull-down menu.



E911 Assignment Table

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

Status Filter: All

Figure 196. The E911 Assignment table

The following table describes the fields in this panel.

E-911 Parameter	Description
E911 LID (Location ID)	The Location ID assigned to this IP phone. **Note:** A phone with a Location ID of "0 (Disabled)" either does not have the correct firmware or does not have any E911 Location ID assigned to it.
Number	The extension number of this IP phone.
IP Address	The IP address of this phone.

E-911 Parameter	Description
MAC Address	The MAC Address of this phone.
Type	The type of phone.
Last Login Time	The last time that this IP phone logged into the MaxCS system.
Status	The current state of this IP phone. You can filter the data in this list as needed. • **Active** - The IP phone is currently registered with the MaxCS system. • **Inactive** - The IP phone is not currently registered with the MaxCS system (the phone may have been unplugged or was logged out of the system).

4. To change the E911 Location ID for an IP phone, select the entry and click **Change LID**.

   Note: If you cannot click the **Change LID** button for that phone (in other words, if the button is disabled), this indicates that the phone does not have the correct firmware; you must upgrade the firmware on the Altigen IP phone before you can set the phone's E911 Location ID.

5. Make your changes and click **OK**. The data will be pushed to the phone, and the phone will automatically re-register to apply the updated configuration.
6. To remove an E911 LID assignment for an extension, select the entry and click **Delete**. (Note that you can delete assignments only for inactive Altigen IP phones.)

To have a user update the E911 Location ID on an IP phone, provide the user with the appropriate Location ID number. Instruct the user to open the phone's menu, choose **System** > **E911 LID**, and enter the Location ID number.

CHAPTER

26

Network Configuration Guidelines for VoIP

Real-time applications such as voice communications require a networking environment that meets certain requirements to deliver and maintain good voice quality. Follow these network configuration guidelines when using MAX Communication Server's VoIP features.

ISP/Intranet Quality of Service (QoS)

- If you subscribe to the public IP network or use your own Intranet, make sure the maximum network delay is less than 100 milliseconds.
- Also, the typical packet loss rate should be less than 1 percent.

Virtual LANs

MaxCS supports virtual LANs in accordance with IEEE 802.1Q. A virtual LAN (VLAN) segments an Ethernet-based network into different logical networks that provide different services such as data service and voice service. It also defines broadcast domains to reduce network traffic load. It provides a managed network environment to run voice and data together smoothly.

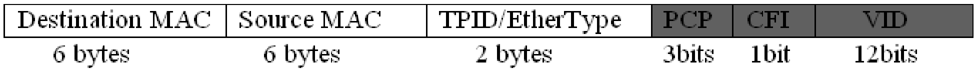
The IEEE 802.1Q header includes IEEE 802.1p, a standard method for assigning priority to packets traversing a network. It works with the Ethernet MAC (Media Access Control) header at the data link layer. The managed switches in a network are responsible for differentiating packets based on their priorities and processing them in different orders.

Requirements:

- MaxCS or above with two NICs for 802.1Q VLAN
- MaxCS or above for 802.1p
- NIC support 802.1p for 802.1p
- The following Altigen IP phone firmware:
  - VLAN: 2xA8 and boot code version 12 or above
  - 802.1p: 2xA8 (MaxCS firmware)
- Layer 2 managed switch

Ethernet II Framing Header

The Ethernet II framing header is defined as follows, with 802.1Q VLAN tag and 802.1p priority bits:

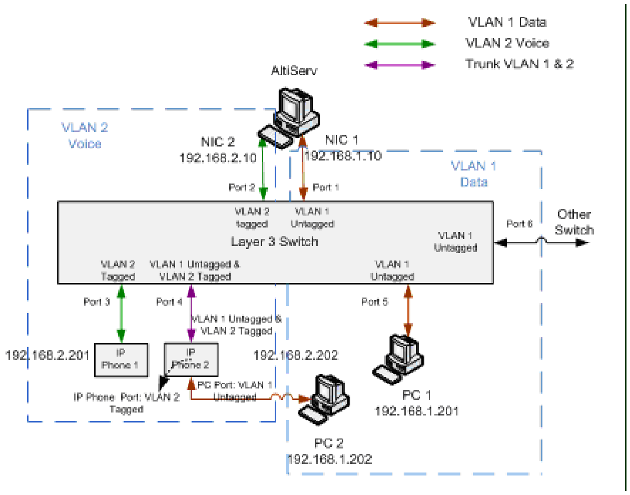


Destination MAC	Source MAC	TPID/EtherType	PCP	CFI	VID
6 bytes	6 bytes	2 bytes	3bits	1bit	12bits

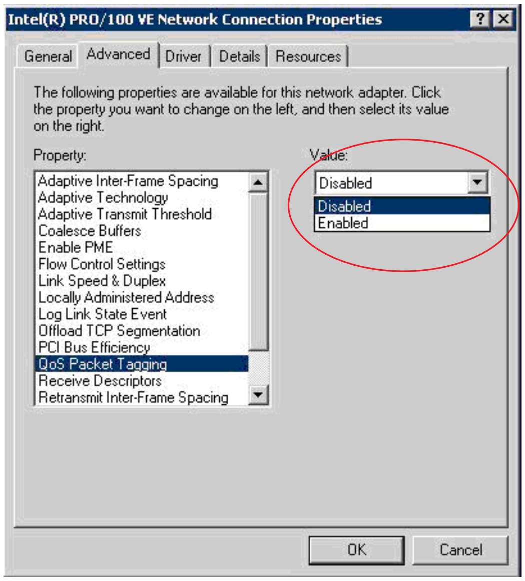
For 802.1Q VLAN-tagged Ethernet frame, the Tag Protocol Identifier (TPID) or Ethernet Type is set to 0x8100. The next 16 bits defines the VLAN and QoS bits:

- Priority Code Point (PCP): a 3-bit field which refers to the IEEE 802.1p priority. It indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, and so on).
- Canonical Format Indicator (CFI): a 1-bit field. If the value of this field is 1, the MAC address is in non-canonical format. If the value is 0, the MAC address is in canonical format. It is always set to zero for Ethernet switches.
- VLAN Identifier (VID): a 12-bit field specifying the VLAN to which the frame belongs. A value of 0 means that the frame doesn't belong to any VLAN; in this case the 802.1Q tag specifies only a priority and is referred to as a priority tag. A value of hex FFF is reserved for implementation use. All other values may be used as VLAN identifiers, allowing up to 4094 VLANs.

Only port-based VLAN is supported in MaxCS, which means the VLAN is assigned in the switch port and managed in the switch internally. The end device, like the MaxCS NIC and IP phone ARM MAC port, does not need to tag the packet with VLAN so there is no software implementation on the end device. MaxCS can use two NICs and connects them to the switch ports with a different VLAN assigned so the network traffic can be separated. However inside the IP phone, the firmware programs the Ethernet switch to assign and manage the different ports with different VLAN IDs. The IP phone user can configure the IP phone port with voice VLAN ID and PC port with data VLAN ID. Different VLANs use a different IP network. Below is a typical VLAN setup:



The NIC in both the MaxCS server and the IPTalk client (used with MaxCommunicator/MaxAgent) must support 802.1p. To see if the NIC supports the 802.1p feature, open the NIC's Properties dialog box and select the **Advanced** tab. See if the "QoS Packet Tagging" property is in the Property list. (Different NICs have different properties and may display a different property name for the 802.1p feature.) If the NIC supports the 802.1p feature, the default value is **Disabled** and you can change this value to enable 802.1p as seen in the following figure.



Intel(R) PRO/100 VE Network Connection Properties

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

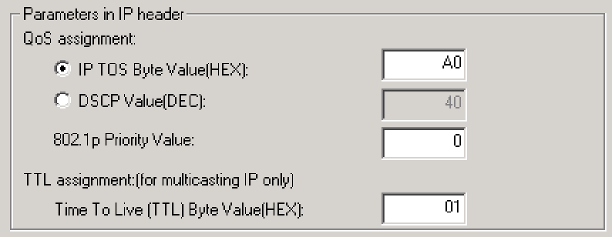
Property:

Value: Disabled

For 802.1p, eight different classes of service are available, expressed through the 3-bit user priority field in an IEEE 802.1Q header added to the frame. The IP phone tags the voice packet from the ARM processor with a user configured value.

Specifying the Priority Value

The server side configuration is located in the HMCP board's **Board Configuration** settings or the VoIP board’s **Board Configuration** > **Advanced setting**.



Parameters in IP header

QoS assignment:

● IP TOS Byte Value(HEX): A0

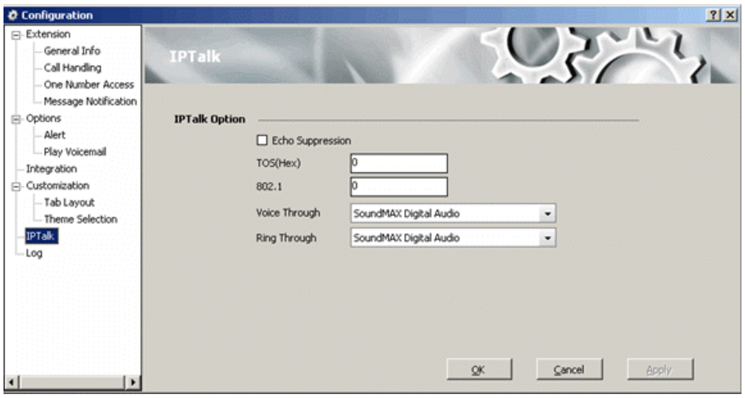
○ DSCP Value(DEC): 40

802.1p Priority Value: 0

TTL assignment:(for multicasting IP only)

Time To Live (TTL) Byte Value(HEX): 01

In MaxCommunicator/MaxAgent, the configuration is in the IPTalk configuration screen:



Configuration

IPTalk Option

□ Echo Suppression

TOS(Hex) 0

802.1 0

Voice Through SoundMAX Digital Audio

Ring Through SoundMAX Digital Audio

Enabling VLAN

VLAN can be enabled and configured in the Altigen IP phone: **Network** > **Enable VLAN** > **Yes**.

After enabling, set **VID:Phone** and **VID:PCPort** IDs.

It can also be configured in MaxAdministrator in the Altigen IP Phone Configuration screen, **General** tab.

WAN Bandwidth

Refer to the table on page 312 for bandwidth requirements for various transmission media with different codecs and frame sizes.

- The Jitter Buffer should be adjusted according to the bandwidth allocated to data traffic. For example, a long Ethernet packet (approximately 1500 bytes) traversing through a WAN which is allocated with 256 kbps of data traffic bandwidth will take about 50 milliseconds. The Jitter Buffer value should be set to this WAN link transmission delay plus the typical network jitter delay. To configure the Jitter Buffer, in Enterprise Manager (**VoIP > Enterprise Network Management**) click the **Codec** button.
- If you have heavier data applications running concurrently, the bandwidth reserved for data traffic should be increased.
- If your router supports multilink or TCP fragmentation, configure your WAN router to user smaller packet sizes, for example, 500 bytes.

WAN Router Configuration

- The router that connects your LAN and the WAN should support priority queuing.
- Configure the router so that the IP/UDP packets being sent to and from an IP station have higher priority than the packets generated by other stations on the same network. Consult your router manufacturer for more information on setting up this configuration.

Firewall Configuration

If a firewall is used to protect your network access security, reconfigure the firewall to open up TCP and UDP ports to the IP system’s IP address. The relevant ports are listed in the section Network Ports. This allows IP’s voice to pass through the firewall freely.

Network Using NAT

You are probably using NAT if *both* of the following conditions apply:

- Your MaxCS ACM server's IP address matches any of the following numbers (where x is any number from 0-255):
    - 10.x.x.x
    - 172.16.x.x to 172.32.x.x
    - 192.168.x.x
- You are able to connect to the Internet directly *without* using a proxy server.

- Contact your router/firewall vendor to obtain a software update for your networking equipment, or obtain routable address space from your Internet provider. If you are unsure whether or not you are using NAT, contact your router/firewall vendor or Internet provider.

Network Configuration Guidelines for Altigen IP Phones

The following guidelines (specific to Altigen IP phones) should be taken into consideration before you configure your network for use with NAT.

- DHCP is recommended to reduce the risks for duplicating IP addresses. MaxCS provides seamless support for Altigen IP phones using dynamic IP addresses. Select **Dynamic IP address** for IP Extensions in the Max Admin’s Extension Configuration window.
- A switch is required; VoIP quality can be adversely affected if a hub is used.

We recommend the following settings on the MaxCS server:

- Large Send Offload VZ (IPv4) – Disable
- Receive Side Scaling – Disable
- IP Security (IPSec) Offload – Disable
- TCP Checksum Offload IPv4 – Disable
- UDP Checksum Offload IPv4 – Disable

Configuration Guidelines for NAT

Note: This section applies only to Altigen IP phones or IPTalk integrated with MaxCommunicator or MaxAgent.

The section discusses the configuration guidelines when MaxCS is behind NAT (Network Address Translation) and communication to Altigen IP phones, IPTalk, or another MaxCS is over WAN. Altigen SIP phones support NAT traversal, which does not require special settings on the NAT router at the remote site.

Due to SIP protocol, which puts the IP address information in the TCP/IP payload, the NAT router requires some SIP protocol implementation to correctly handle the SIP traffic and translate the private IP address into a public IP address. Not all NAT routers have this kind of implementation, or have it implemented correctly (SIP ALG). If the NAT router does not support SIP ALG properly, you need to check **Enable SIP NAT Support** and **Enable SIP NAT Support** in Enterprise Manager on the *IP Networks* tab. Also, SIP ALG must be disabled in the NAT router to avoid the conflict between SIP ALG and SIP NAT support provided by MaxCS.

The following sections illustrate a private network configuration and a VPN configuration.

For information on setting up VoIP traffic forwarding for NAT and configuring MaxCS behind NAT, see “Configuring MaxCS Behind NAT” on page 325.

Private Network Configuration Example

(MaxCS with private IP address and behind NAT)

Only the private IP address is used in a private network. The public router will not route the packet that has a private IP address as its destination. (All IP addresses beginning with 192.168.x.x, 10.x.x.x, or 172.16.x.x to 172.32.x.x are private IP addresses.)

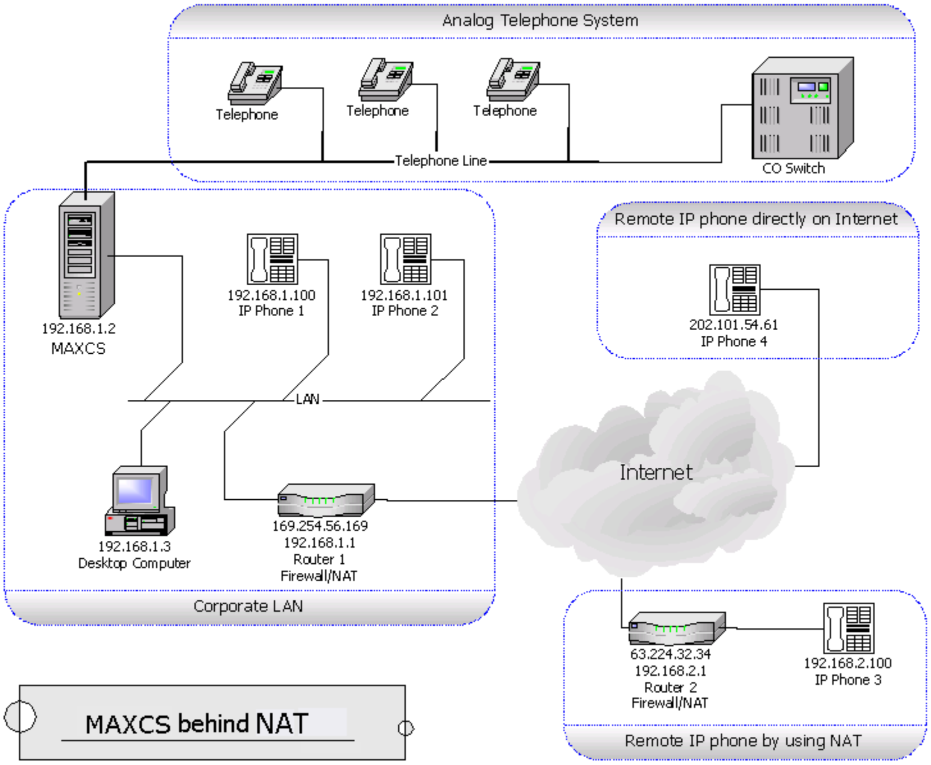


Figure 197. MaxCS behind NAT

This figure shows a private network, 192.168.1.0, where MaxCS is installed and running on a host with a private IP address 192.168.1.2.

Router 1 is a NAT router. The local IP phones – IP Phone 1 and IP Phone 2 – use the private IP addresses 192.168.1.100 and 192.168.1.101, respectively. There are two remote IP phones: IP Phone 3 with a private IP address 192.168.2.100 connects to the Internet via Router 2. Router 2 can also sit behind a DSL/Cable Modem.

Example Setup: Corporate LAN

- MaxCS – MaxCS is installed (private IP address 192.168.1.2). The public IP address of Router 2 should be configured as the IP address of this IP extension in MaxCS. If it is changed dynamically, then assign a dynamic IP address configuration for that extension.
- Router 1 – Router 1 is a NAT router. You need to set up the SIP port forwarding for this NAT router from 169.254.56.169 to the private IP address of MaxCS 192.168.1.2.

Example Setup: Remote IP Phone Using NAT

- IP Phone 3 – When configuring remote IP Phone 3, you should set up the MaxCS IP address to Router 1’s public IP address — 169.254.56.169.
- Router 2 – No special configuration is needed for Router 2. Also, more than one Altigen SIP phone can sit behind Router 2.

Example Setup: SIP IP Call from Another MaxCS on the Internet

Another MaxCS can make an SIP IP call to this MaxCS by calling the MaxCS's public IP address, which is 169.254.101.2.

VPN Network Configuration Example

(Connecting to MaxCS with VPN)

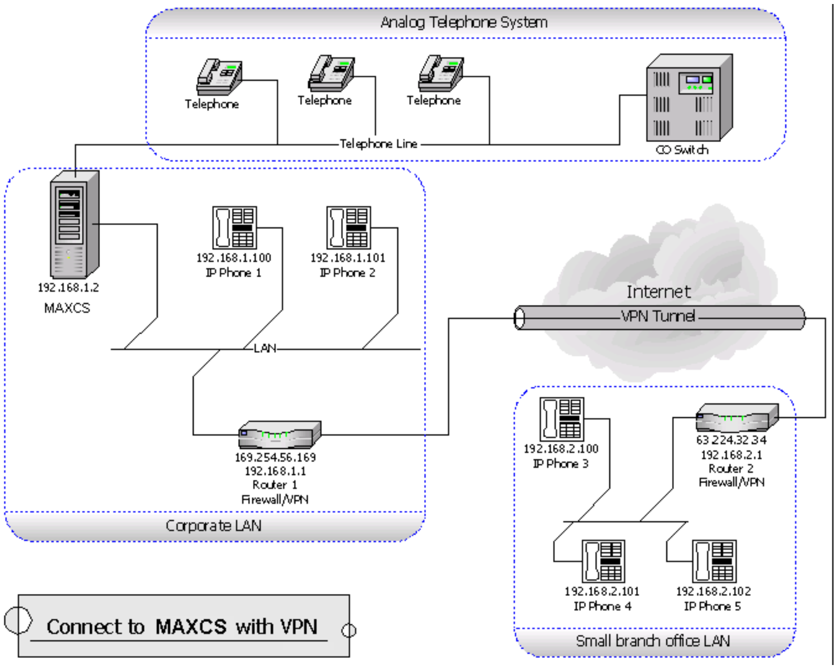


Figure 198. MaxCS with VPN

In a multi-site configuration, VPN can be used to provide a secured tunnel between the remote sites and the corporate site.

Figure 198, “MaxCS with VPN,” shows a network layout in which there are two private networks, the corporate LAN and branch office LAN. The VPN tunnel connects the two private networks such that the two networks access each other with a private IP address.

In the corporate network, MaxCS is installed on a host with private IP address 192.168.1.2.

Both Router 1 and Router 2 are VPN-capable and compatible with each other. (It is recommended that the routers come from same vendor.) A VPN tunnel exists between these two routers. The local IP phones – IP Phone 1 and IP Phone 2 – directly connect to the corporate network with private IP address 192.168.1.100 and 192.168.1.101. And the three remote IP phones – IP Phone 3, IP Phone 4 and IP Phone 5 – connect to the branch office network with private IP addresses 192.168.2.100, 192.168.2.101 and 192.168.2.102, respectively.

Example Setup: Branch office LAN

- IP Phone 3, IP Phone 4 and IP Phone 5

  When configuring the remote IP phones – IP Phone 3, IP Phone 4, and IP Phone 5 – you should set up the AW address to use the MaxCS IP address.

For the VPN Tunnel between the Two Private Networks:

You *must* set up a VPN tunnel to connect the two private networks. The VPN setup procedure may be complicated and is generally performed by a professional IT technician.

The following minimum guidelines need to be considered for setting up the VPN tunnel:

- **WAN Bandwidth –** Should be greater than the aggregate of maximum VoIP session bandwidth usage.

- **QoS –** If the IP WAN network provides QoS (Quality of Service), it should be configured to honor VoIP RTP packet transmission.

  An easy example for a VPN resolution is with the Linksys EtherFast VPN router[1]. Router 1 and Router 2 are routers supporting VPN. When configuring these VPN routers, the following information is needed. (Also, please refer to the Router's User Guide for more detailed information.)

Router 1's Settings

Local Secure Group: (specifies the local network which can access the VPN tunnel at the corporate network)	**Subnet IP**: 192.168.1.0 (Corporate Network)	**Subnet Mask**: 255.255.255.0
Remote Secure Group: (specifies the remote network which can access the VPN tunnel at the branch office network)	**Subnet IP**: 192.168.2.0 (Branch Office Network)	**Subnet Mask**: 255.255.255.0
Remote Security Gateway: (specifies the public IP address of the remote gateway which can access the VPN tunnel at the branch office)	63.224.32.34 (Router 2’s public IP Address	

Router 2's Setting

Router 2's public IP address should be a fixed IP address.

Local Secure Group: (specifies the local private network in the branch office, which can access the corporate network through VPN)	**Subnet IP**: 192.168.2.0 (Branch Office Network)	**Subnet Mask**: 255.255.255.0
Remote Secure Group: (specifies the corporate network, which can be accessed by stations in this local private network through the VPN tunnel)	**Subnet IP**: 192.168.1.0 (Corporate Network)	**Subnet Mask**: 255.255.255.0
Remote Security Gateway: (specifies the public IP address of the corporate VPN-enabled gateway)	169.254.56.159 (Router 1’s public IP Address	

[1] Linksys is for reference only. Altigen has not certified this product or any other router at this time.

CHAPTER

27

Enterprise VoIP Network Management

The VoIP-related aspects of both single-server systems and multi-site VoIP domains are configured in **Enterprise Manager**, available from the **VoIP** menu or the Windows **Start** menu.

In addition, multi-site VoIP domain management – including directory synchronization and routing – is handled here.

Notes

- With MaxCS Private Cloud systems, Enterprise Manager's domain-related features require a VPN or MPLS to the cloud service.
- A multi-site installation requires an Enterprise License.
- A security enhancement has been added for the Altigen Java Service Loader.

  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 Release 8.0 and later, however, the new Java Service Manager can connect only to the local system. Also, earlier versions of the MaxCS Altigen Java Service Manager will not be able to connect to the MaxCS Altigen Java Service loader.

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

For a *single-system installation*, only the following VoIP configuration elements in Enterprise Manager are relevant and are discussed in the first part of the chapter:

- **Codec Profile** – Create codec profiles that use different settings for jitter buffer size and packet length. Codec profiles can be assigned to different types of VoIP connections, as defined in the IP dialing table and IP codec assignment table.
- **VoIP Bandwidth Use** – Define the maximum VoIP sessions using different codecs on a public Internet or a private intranet data pipe.
- **NAT Support** – Configure VoIP NAT traversal when the server is behind NAT using a private IP address.
- **IP Dialing Table** – Define IP dialing digits and codec for VoIP dialing to other Altigen systems or certified third-party IP devices.
- **IP Codec Table** – Define the codec and data pipe for Altigen IP phones and SIP trunking service.

  Note: Altigen IP phones 705, 710, and 720 do not support G.722 or G.711 A-Law.

For a *multi-site installation*, you can manage the above configurations for *all* your VoIP domain servers from Enterprise Manager.

Along with the above configurations, the multi-site administrator will use Enterprise Manager and the **VoIP** menu in MaxAdministrator to do the following:

- Create the VoIP domain
- Define the VoIP domain Master
- Join servers to the VoIP domain
- Manage VoIP domain users
- Define global least cost routing

Understanding VoIP Bandwidth Requirements

Before starting VoIP related configurations, it is helpful to have some understanding of VoIP bandwidth requirements, so that you can plan your VoIP deployment properly. Also see **Network Configuration Guidelines for VoIP**.

The data network bandwidth required to carry VoIP depends on the following factors:

- **Codec and Compression** – This is the encoding of analog voice to digital form, decoding of digital form to analog wave form, and compression of digital form to a smaller size. MaxCS supports several type of codec: G.711, G.722, G.729, G.723.1.
- **Packet Length (Frame Size)** – The size of the voice frame data (payload) transmitted in a packet. For G.711, G.722, and G.729, you have choice of 10, 20, and 30 ms lengths. For G.723.1, the packet length is a fixed 30 ms. A larger packet length decreases the transmission overhead. However, it will increase the latency and have a negative effect on the voice quality if a packet is lost during transmission. For G.711, G.722, and G.729, 20 ms is efficient and recommended.
- **IP Header** – The IP/UDP/RTP header adds 40 octets per packet. With a packet length of 20 ms, the IP headers will require 16 kbps of bandwidth in addition to whatever codec is being used.
- **Transmission Medium** – In order to travel through the IP network, the IP packet is wrapped in another layer by the physical transmission medium. The transmission medium, such as Ethernet, will add its own header, checksums, and spacers to the packet. With a packet length of 20 ms, the transmission medium requires additional 15.2 kbps of bandwidth to carry the packets to their destination.
- **Silence Suppression** – You can suppress the transmission of data during periods of silence. This can reduce the demand for bandwidth by as much as 50 percent. However, it may have a negative impact on the voice quality. Some users may feel the conversation is not "natural" when artificial comfort noise is generated during periods of silence.

The following table lists bandwidth requirements for various transmission media with different codecs and frame sizes. It assumes silence suppression is not turned on.

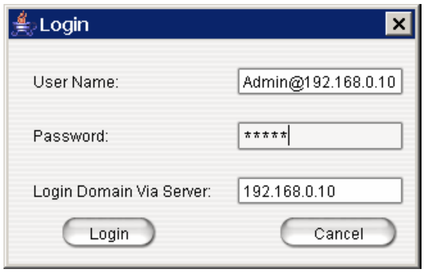
Codec	Voice Encoding (kbps)	Frame Size	PPP (kbps)	Frame Relay (kbps)	Ethernet (kbps)
G.711/G.722	64	10 ms	100.8	102.4	126.4
G.711/G.722	64	20 ms	82.4	83.2	95.2
G.711/G.722	64	30 ms	76.3	76.8	84.8
G.729	8	10 ms	44.8	46.4	70.4
G.729	8	20 ms	26.4	27.2	39.2
G.729	8	30 ms	20.3	20.8	28.8
G.723.1	6.4	30 ms	18.7	19.2	27.2

VoIP Bandwidth requirement for WAN connection varies depending on the type of WAN. Bandwidth requirement typically is less than Ethernet requirement.

Opening Enterprise Manager

To open Enterprise Manager, use one of the following methods:

- For a single-system installation without a Domain Master, this first method is recommended. From Max-Administrator, select **VoIP > Enterprise Network Management**. Enterprise Manager opens without a log-in dialog box.
- For multisite VoIP domain management, from the Windows **Start** menu, select **A MAX Communication Server ACM** > **Enterprise Manager**. A login screen opens. (With this method you can log in to the Domain Master from any member system or remote desktop.)



Login

User Name: Admin@192.168.0.10

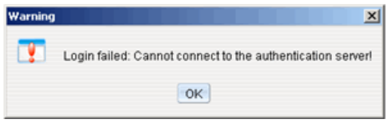
Password: *****

Login Domain Via Server: 192.168.0.10

Figure 199. The Login panel for Enterprise Manager

User name	Password	Login Domain Via Server
DomainAdmin (Logging in as DomainAdmin gives you rights to change the entire Enterprise Manager configuration.)	Default: 22222. You can change the password in Enterprise Manager. Note: This password is not the same as the MaxAdministrator password.	Enter the domain master's IP address
Admin@domain master IP address (A Site Admin who logs into the Domain Master in this way has the same rights as DomainAdmin.)	Enter MaxAdministrator password	Enter the domain master's IP address
Admin@member server IP address (A Site Admin who logs in this way can make changes on this member server only.)	Enter the MaxAdministrator password for the member server	Enter the member server's IP address

Warning! If your MaxCS system is using dynamic IP addressing, you will see the following warning message when launching Enterprise Manager. Please check the Internet Protocol (TCP/IP) Properties of your server NIC interface and assign a fixed IP address to this server.



Warning

Login failed: Cannot connect to the authentication server!

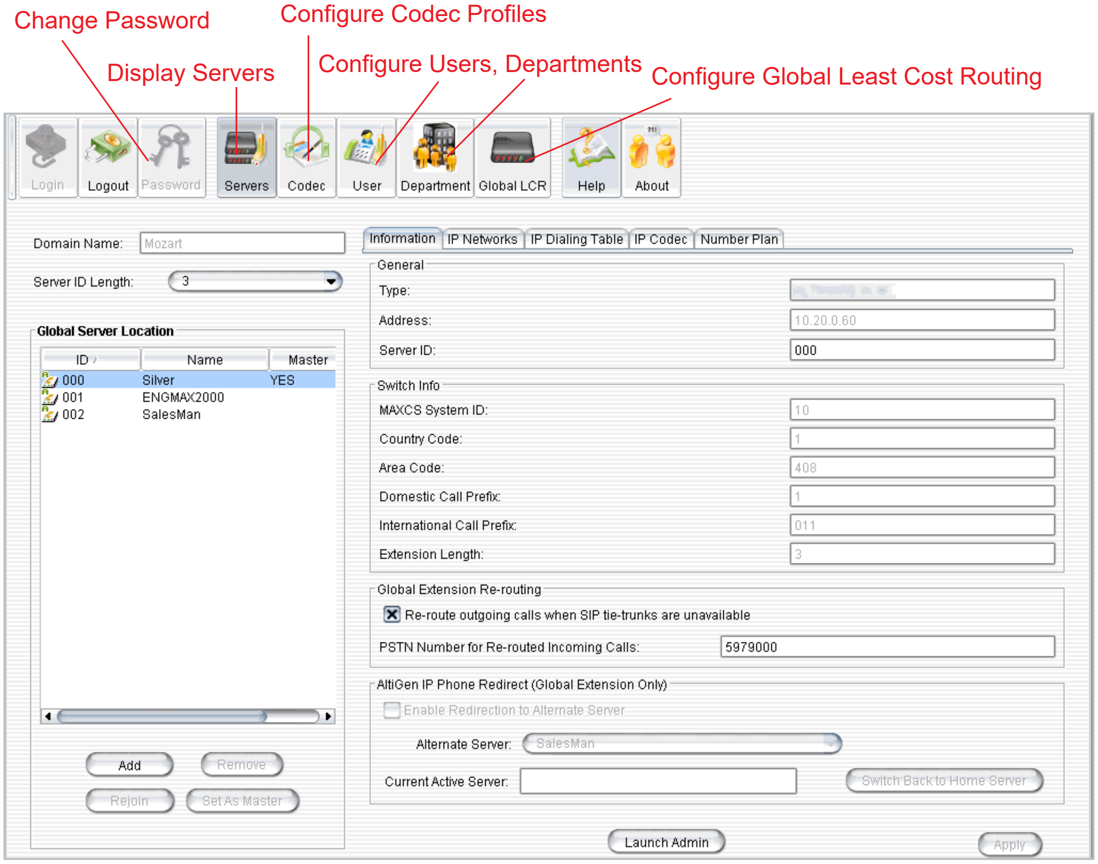
Figure 200. Example of a log-in error message

When multiple systems are added to the VoIP domain, all member systems need to have both **Route Access Code** and **IP Trunk Access Code** configured. If one or more member systems are not configured properly, a message opens.

Multisite routing may fail if **Route Access Code** and **IP Trunk Access Code** are not configured.

Overview of Enterprise Manager

After you log in, the Enterprise Manager window opens.



Domain Name: Mozart

Server ID Length: 3

Global Server Location

ID	Name	Master
000	Silver	YES
001	ENGMAX2000	
002	SalesMan	

General

Type: [illegible]

Address: 10.20.0.60

Server ID: 000

Switch Info

MAXCS System ID: 10

Country Code: 1

Area Code: 408

Domestic Call Prefix: 1

International Call Prefix: 011

Extension Length: 3

Global Extension Re-routing

☒ Re-route outgoing calls when SIP tie-trunks are unavailable

PSTN Number for Re-routed Incoming Calls: 5979000

AltiGen IP Phone Redirect (Global Extension Only)

☐ Enable Redirection to Alternate Server

Alternate Server: SalesMan

Current Active Server:

Figure 201. The Enterprise Manager window

Click a tab to view or configure settings on that tab. Information on a tab is related to the selected server. Click buttons in the toolbar to perform configuration tasks. Click a column heading to sort by that column.

Configuration Buttons

- **Servers** – Displays the VoIP domain name, servers in the system, and server ID length. Lets you add/remove servers and change the VoIP domain master. Lets you re-route outgoing calls of global extensions and redirect IP phones. Displays the configuration and informational tabs listed in the next section.
- **Codec** – button lets you configure individual codec profiles – silence suppression, codec, DTMF delivery, enable/disable SIP early media, SIP transport, jitter buffer range, and RTP packet length.
- **User** – Displays information about extensions in the VoIP domain and lets you change an extension to global or local and relocate an extension.

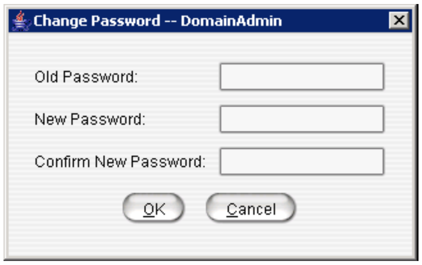
- **Department** – Lets you define departments in the VoIP domain and assign extensions to departments.
- **Global LCR** – Lets you add E.164 number patterns and specify source and target sites.

Tabs Displayed with the Servers Button

- **Information** tab displays information about the selected site and lets you configure a PSTN number for global extension rerouting as a failover when the TCP/IP network is down. You may also assign an alternate server to which to redirect global Altigen IP phones when their primary server is down.
- **IP Networks** tab defines IP networks and the bandwidth information for an MaxCS site. Bandwidth usage control for Internet and intranet can be set up here. If the bandwidth usage exceeds the maximum setting, the call will not be established.
- **IP Dialing Table** tab defines the IP dialing table for a MaxCS site. Specified information here includes a codec profile and a protocol (SIP) for the communication from this site to the selected site.
- **IP Codec** tab lets you specify an inter-gateway codec and define IP device ranges to which you can assign a codec profile.
- **Number Plan** tab displays the number plan information that is set up in MaxAdministrator, System Configuration window, **Number Plan** tab.

Changing the Enterprise Manager Password

Only a person with DomainAdmin rights can change the Enterprise Manager password. To change the password, click the **Password** button at the top of the Enterprise Manager window.


Change Password -- DomainAdmin

Old Password:

New Password:

Confirm New Password:

Figure 202. The Change Password panel

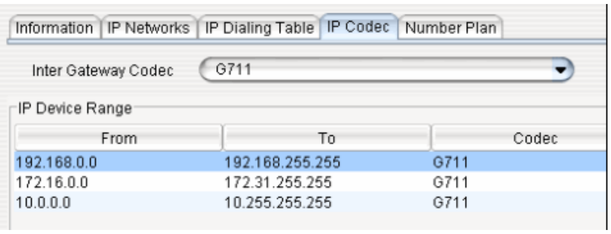
Enter the old password, and the new password. Confirm the password, and click **OK**.

Setting VoIP Codec Profiles

The codec setting is profile-based. For different IP addresses and protocols, a different preferred codec can be used. Each codec profile can have its own codec (G.711, G.722 on Softswitch or Cloud, G.723, G.729), packet length, and jitter buffer. The codec profile can be assigned to connectivity with a remote server, IP phone or other VoIP device.

By default, the following IP address ranges (private IP addresses) will use G.711 codec:

- 192.168.0.0 to 192.168.255.255
- 172.16.0.0 to 172.31.255.255
- 10.0.0.0 to 10.255.255.255



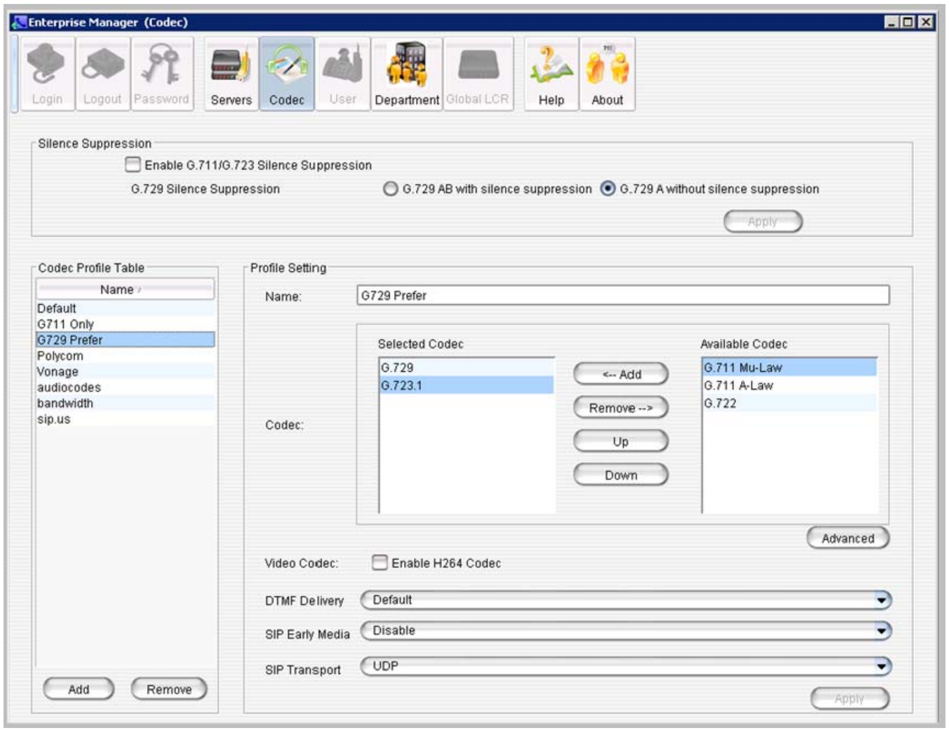
Inter Gateway Codec: G711

IP Device Range

From	To	Codec
192.168.0.0	192.168.255.255	G711
172.16.0.0	172.31.255.255	G711
10.0.0.0	10.255.255.255	G711

Figure 203. The IP Codec sub-tab showing devices and their assigned codecs

To open a window where you can set or modify codec profiles, click the **Codec** button in the Enterprise Manager toolbar.



Silence Suppression

☐ Enable G.711/G.723 Silence Suppression

G.729 Silence Suppression ○ G.729 AB with silence suppression ● G.729 A without silence suppression

Codec Profile Table

Name
Default
G711 Only
G729 Prefer
Polycom
Vonage
audiocodes
bandwidth
sip.us

Profile Setting

Name: G729 Prefer

Codec:

Selected Codec: G.729, G.723.1

Available Codec: G.711 Mu-Law, G.711 A-Law, G.722

Video Codec: ☐ Enable H264 Codec

DTMF Delivery: Default

SIP Early Media: Disable

SIP Transport: UDP

Figure 204. Codec profile setting window in Enterprise Manager

Named codec profiles are listed on the left.

To create a new profile,

1. Click the **Add** button.
2. Name the new profile and click **OK**. Make your changes, and then click **OK**.

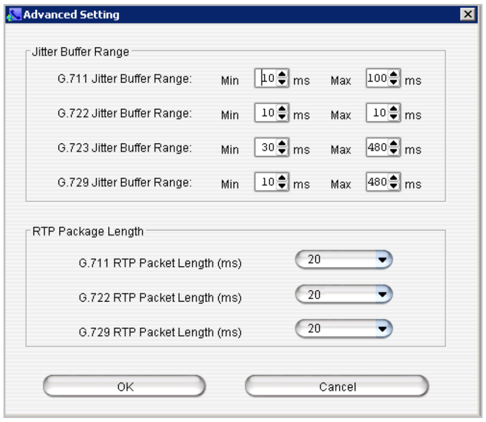
The next two tables describe the Codec parameters.

Codec Parameter	Description
Codec Profile Table	Lists codec profiles by name. Select a profile in the table to modify its settings, then click **Apply** in the panel where you made the changes. Click the **Add** button to add a codec profile. Click the **Remove** button to remove the selected profile. You cannot remove the Default profile.
Name	Name of the codec profile. You can modify the name, and click **Apply**. The Default profile name cannot be changed.

Codec Parameter	Description
Codec	There are several options: • G.711 Mu-Law • G.723.1 • G.729 • G.722 (supported on Softswitch and Cloud deployments only) G.711 provides toll quality digital voice encoding, and G.723 and G.729 use low rate audio encoding to provide near toll quality performance under clean channel conditions. G.722 is a wideband audio codec. It provides higher voice quality than more narrow-bandwidth codecs such as G.711. Use the **Add** and **Remove** buttons to move codecs between the *Available Codec* and the *Selected Codec* lists. Codecs you place into the Selected Codec list will appear in the *SDP Codec Capability* list for codec negotiation. Prioritize the selected codecs by using the **Up** and **Down** buttons. **Note:** While Polycom phones support G.722, Altigen IP phones 705, 710, and 720 do not support G.722 or G.711 A-Law. In mixed-phone environments, make sure you include G.711 Mu-Law, G.723-1,or G.729 in the Selected Codecs list.
G.711 / G.723 / G.729 Silence Suppression	When silence suppression is enabled, and silence is detected during a call, MaxCS stops sending packets to the other side. This decreases the bandwidth requirement, however the voice quality may be degraded slightly. These are system-wide settings.
Video Codec	Check the **Enable H.264 Codec** option to enable video support for P2P Polycom VVX phones. **Note:** MaxCS does not support video over SIP Tie trunks or SIP trunks. This option is only for Softswitch deployments.
DTMF Delivery (Applies to SIP protocol only)	SIP INFO is used to deliver DTMF. RFC 2833 – The DTMF pay load is embedded with RTP. Most 3rd-party SIP gateways support this standard. **Note:** The codec profile assigned to the SIP-TIE Trunk must use RFC 2833 (DTMF) in order to support Polycom phones. We recommend that you configure a single codec for SIP Trunk interfaces. In band – If DTMF tone is delivered over the voice band. It's not reliable over G.711 codec and will not work over G.729/G.723 codec
SIP Early Media (Applies to SIP protocol and SIP trunk only)	SIP Early Media allows two SIP devices to communicate before a SIP call is actually established. It is important for interoperability with the SIP trunk carrier's PSTN gateway. If SIP Early Media is not checked, the caller may not hear the exact ringback tone provided by the CO (the caller may not hear any ringback tone at all). When using a SIP trunk as a MaxMobile trunk, you must enable the **SIP Early Media** option for the SIP trunk.

Codec Parameter	Description
SIP Transport	There are several SIP Transport options. Note that security options can be configured for individual IP phone extensions in the IP Phone Configuration screen. (For more information on security settings, see “**SIP Transport**” on page 209.) Extension-level configuration takes precedence over a codec profile that is assigned in Enterprise Manager. See the next section. **UDP** – User Datagram Protocol is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). **Note:** All SIP trunks must use UDP. **TCP** – Transmission Control Protocol is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. **Note:** Altigen phones do not use TCP. **TLS/SRTP** – Adds Secure RTP to Transport Layer Security to secure SIP-associated media.

Click **Advanced** to access additional advanced parameters.



Advanced Setting

Jitter Buffer Range

G.711 Jitter Buffer Range: Min 10 ms Max 100 ms

G.722 Jitter Buffer Range: Min 10 ms Max 10 ms

G.723 Jitter Buffer Range: Min 30 ms Max 480 ms

G.729 Jitter Buffer Range: Min 10 ms Max 480 ms

RTP Package Length

G.711 RTP Packet Length (ms) 20

G.722 RTP Packet Length (ms) 20

G.729 RTP Packet Length (ms) 20

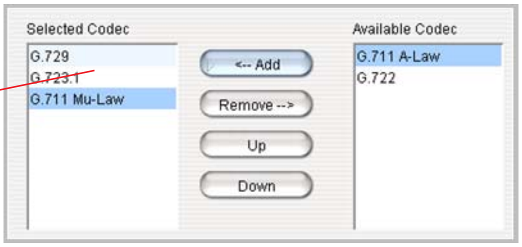
Figure 205. The Advanced Codec Profile Settings panel

Advanced Codec Parameter	Description
G.711 / G.722 / G.723 / G.729 Jitter Buffer Range (ms)	Indicates the delay, in milliseconds, used to buffer G.711, G.722, G.723, and G.729 voice packets received from the IP network. Voice packets sent over the IP network may incur different delays due to network load or congestion. The jitter buffer helps to smooth out the delay variation in the arriving voice packets and maintain voice quality at the receiving end. The default values for G.711 are 10 min. to 100 max milliseconds. The default values for G.722 are 10 min. to 100 max milliseconds. The default values for G.723 are 30 min. to 480 max milliseconds. The default values for G.729 are 10 min. to 480 max milliseconds.
G.711 / G.722 / G.729 RTP Packet Length (ms)	Lets you configure the length of the RTP packets for G.711, G.722, and G.729 in milliseconds. The RTP packet length can be set to 10, 20 or 30 milliseconds. The smaller the packet length, the larger the bandwidth required.

Setting Codec Priority

You can set codec priorities for each Codec Profile.

During codec negotiation, the highest-priority codec that the receiving end supports will be used. Therefore, you should sort the *Selected Codec* list by priority, from top to bottom. Use the **Up** and **Down** buttons to do this.



Selected Codec: G.729, G.723.1, G.711 Mu-Law

Available Codec: G.711 A-Law, G.722

Prioritize this profile's codecs by arranging codecs top (highest priority) to bottom (lowest priority)

Figure 206. Codecs in the Selected Codec and Available Codec lists

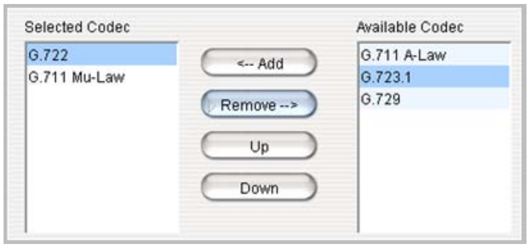
Codec Negotiation

The logic for negotiating codec capabilities varies for various types of connection.

Negotiation - Server to Client

With a server-to-client connection, the highest priority codec in the server's codec list that is supported by the client will be assigned.

Following is an example of a typical setting for SIP devices on a LAN: G.722, then G.711 Mu-Law. This hierarchy allows Polycom phones and the Altigen IP-805 phone to connect via G.722. Altigen IP phones will connect with G.711.

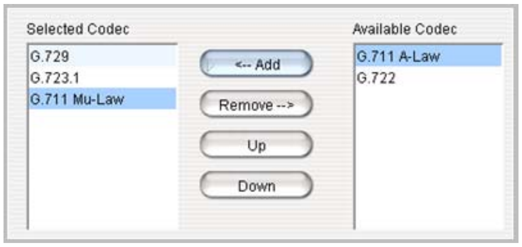


Selected Codec: G.722, G.711 Mu-Law

Available Codec: G.711 A-Law, G.723.1, G.729

Figure 207. Codec negotiation example: SIP devices on a LAN

The next example shows a typical setting for SIP devices on a WAN: First G.729, the G.723.1, and then G.711 u-Law. This hierarchy allows remote SIP devices to use the compressed codec G.729. Remote IPTalk instances use G.723.1, and G.711 is used for other remote devices that do not support the other two codecs.



Selected Codec: G.729, G.723.1, G.711 Mu-Law

Available Codec: G.711 A-Law, G.722

Figure 208. Codec negotiation example: SIP devices on a WAN

Negotiation - Server to Server

With server-to-server connections, the responding device determines the codec from the common codecs that both of the devices accept. Usually, the responding device selects the first preferred codec from among the common list. We recommend that you assign a preferred codec on both servers, so that both incoming and outgoing events use the same codec.

If you are not sure of the codecs supported by your SIP Trunk provider, then we recommend that you configure a single codec (your preferred codec) for SIP Trunks.

About the G.722 Codec

MaxCS supports the G.722 codec on Softswitch and on Cloud deployments. G.722 is a wideband audio codec. The G.722 codec provides higher voice quality than more narrow-bandwidth codecs such as G.711. MaxCS supports G.722 64 kbps only.

The CPU processing requirement for G.722 is similar to G.723 and G.729. It is designed to use the same combo codec resources as G.723 and G.729.

The G.722 codec is supported in HMCP media servers only. Altigen's telephony boards, including the Triton and Vision boards and the Max1000 and Max2000 boards, do not support the G.722 codec.

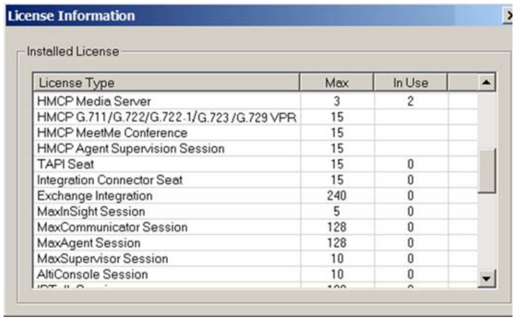
G.722 is supported by the following devices:

- Altigen IP 805 phone - G.722 64 kbps ONLY
- Polycom phones
  - SoundPoint IP-335, IP-550, IP-560, IP-650, IP-670
  - SoundStation IP-6000, IP-7000
  - VVX 300, VVX 310, VVX 400, VVX 410, VVX500, VVX 600
- SIP tie trunks

The G.722 codec is part of combo codec and is controlled by license.

Note: When adding additional combo licenses, the system will also increase the RTP ports it uses and will use these new ports. If these additional ports are not added to the firewall, then calls will not have audio.

The number of total codecs is shown in the License Information panel.



License Type	Max	In Use
HMCP Media Server	3	2
HMCP G.711/G.722/G.722-1/G.723 /G.729 VPR	15	
HMCP MeetMe Conference	15	
HMCP Agent Supervision Session	15	
TAPI Seat	15	0
Integration Connector Seat	15	0
Exchange Integration	240	0
MaxInSight Session	5	0
MaxCommunicator Session	128	0
MaxAgent Session	128	0
MaxSupervisor Session	10	0
AltiConsole Session	10	0

Figure 209. The License Information panel

Assigning Codec Profiles to IP Addresses

You can specify what codec profile to use when connecting to the following VoIP devices:

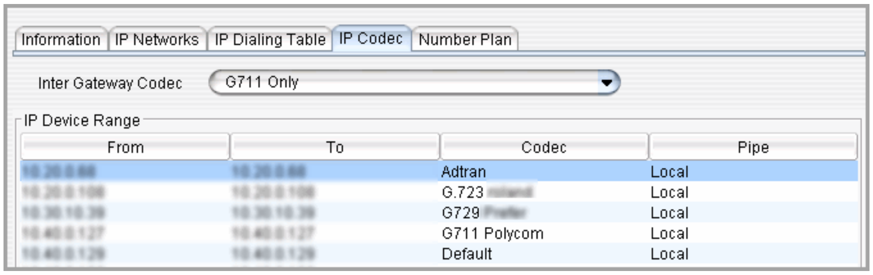
- IP phones on the LAN
- a remote IP phone over WAN
- a remote Altigen system over WAN
- SIP Trunk service provider over WAN
- multiple gateways on the LAN

The codec profile assigned in the IP Device Range table (shown below) supersedes the codec profile defined in the IP dialing table if the IP address is duplicated in both tables.

The SIP transport assigned to an extension in the IP Phone Configuration screen takes precedence over a codec profile with a different SIP transport assigned in Enterprise Manager. If the IP extension supports TLS and the codec profile does not, then the IP extension policy holds. That way you can configure a range of IP addresses in the IP dialing table or IP codec, and have only a few IP addresses/extensions support TLS.

If the IP extension has not configured TLS as its transport, and the codec profile supports it, then the codec profile policy holds.

To set IP address ranges and assign codec profiles to them, in Enterprise Manager, on the *Servers* tab, click the **IP Codec** sub-tab.



Inter Gateway Codec: G711 Only

IP Device Range

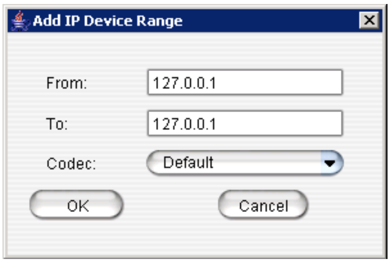
From	To	Codec	Pipe
[redacted]	[redacted]	Adtran	Local
[redacted]	[redacted]	G.723 [redacted]	Local
[redacted]	[redacted]	G729 [redacted]	Local
[redacted]	[redacted]	G711 Polycom	Local
[redacted]	[redacted]	Default	Local

Figure 210. The IP Codec sub-tab

By default, all private addresses are set to G.711 codec only. You can add individual IP addresses and address ranges and assign a codec to each.

Add IP Addresses and Address Ranges and Assign a Codec

1. Click the **Add** button in the IP Device Range panel (the panel on the right).



From: 127.0.0.1

To: 127.0.0.1

Codec: Default

2. Enter an IP address range (for dynamic IP addressing), or enter the same address in each field if this is a static address. You cannot use the minimum and maximum values (0.0.0.0. and 255.255.255.255).
3. Click **OK**.

If you have multiple gateways controlled by a MaxCS host system, you need to configure an Inter Gateway Codec profile.

Set the Codec for a Connection among Gateways in the Same MaxCS Server

1. Select a server in the *Global Server Location* list on the left side of the window.
2. In the *Codec* field, select the codec to use for a connection to this server from the list.

Managing IP Networks

In MaxCS, Instead of specifying the maximum number of sessions per each codec, as in previous releases, you specify the maximum number of sessions per *bandwidth range*.

The actual network bandwidth required for the bit rate range is used for the bandwidth calculation. 33 to 64 Kbps bit rate is translated into 100 Kbps network bandwidth, which includes LAN and IP/UDP/RTP header overhead. 16 to 32 Kbps and under 16 Kbps are translated into 65 Kbps and 40 Kbps, respectively.

The maximum number of allowed G.711 and G.722 codecs appears by default. You can lower these numbers by clicking the down arrow until you reach the desired amount.

After the maximum number of sessions has been reached, the call negotiated with this codec bit rate will be rejected. Also, after the total bandwidth utilization of all the codecs exceeds the value specified in Bandwidth for VOIP parameter, new calls cannot be established.

You configure this on the **IP Networks** sub-tab in Enterprise Manager.

The tab allows you to specify the following limits:

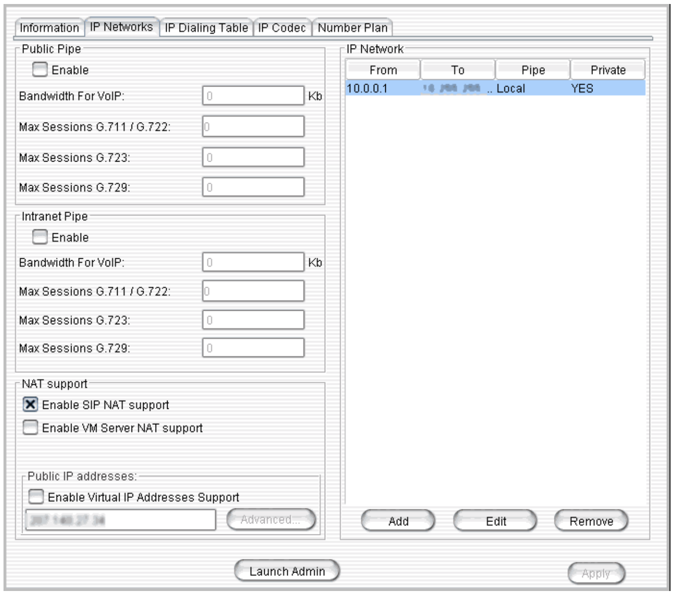
- Bandwidth for VoIP sessions in the *Public Pipe*

- Bandwidth for VoIP sessions in the *Intranet Pipe*
- NAT support when the server is behind a NAT router

The **Public Pipe** is the WAN connection to the public Internet, including IP-VPN over WAN.

The **Intranet Pipe** is the enterprise WAN connection, for example, Frame Relay.

Note: The VoIP connections through public or enterprise WAN will work without configuring the **IP Networks** tab. However, if the total number of VoIP connections exceeds the WAN bandwidth, the voice quality will be affected for all connections. It is recommended that you set a limit based on the WAN bandwidth to ensure the voice quality.



Public Pipe

□ Enable

Bandwidth For VoIP: 0 Kb

Max Sessions G.711 / G.722: 0

Max Sessions G.723: 0

Max Sessions G.729: 0

Intranet Pipe

□ Enable

Bandwidth For VoIP: 0 Kb

Max Sessions G.711 / G.722: 0

Max Sessions G.723: 0

Max Sessions G.729: 0

NAT support

☒ Enable SIP NAT support

□ Enable VM Server NAT support

Public IP addresses:

□ Enable Virtual IP Addresses Support

[redacted]

IP Network

From	To	Pipe	Private
10.0.0.1	[redacted] ..	Local	YES

Figure 211. The IP Networks sub-tab

Defining Your Network

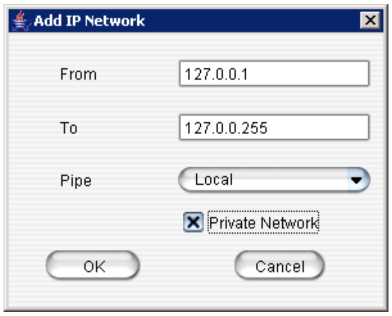
If you need to configure either bandwidth control or NAT support, you have to define your network first. These are the guidelines:

- You must define your LOCAL network IP address range. When a Pipe is defined as **Local**, it tells the system that the configured IP address range is not subject to bandwidth control. If the Altigen system and this Local Network are behind the same NAT router, you need to check the **Private Network** check box. This tells the system that VoIP connection to this address range does not require IP address translation, which is replacing the system's private IP address with a public address when sending VoIP packets to outside devices.
- If you have an intranet linking multiple locations, you must enter the IP address range and define the Pipe as **Intranet**. If the Altigen system and this intranet are behind the same NAT router, you need to check the **Private Network** check box.
- If you have VPN service over public WAN, you must enter the VPN IP address range and define the Pipe as **Public**. If the Altigen system and this VPN IP addresses are behind the same NAT router, you need to check the **Private Network** check box.
- All undefined IP addresses fall into the Public Pipe range and are subject to bandwidth control if the public pipe bandwidth control is enabled.

Note: When MaxCS is behind a NAT router, and you do not check the **Private Network** check box, IP phones may not function.

Define an Address Range

1. Click the **Add** button in the IP Network panel.



Add IP Network

From: 127.0.0.1

To: 127.0.0.255

Pipe: Local

☒ Private Network

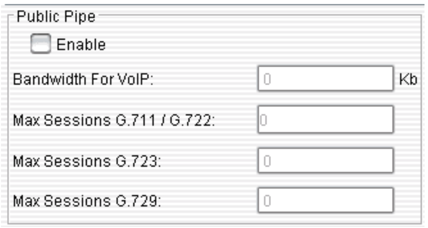
2. Fill in a range of IP addresses.
3. Select the pipe for this IP address range.
4. If this is a private network, check the **Private Network** check box. Click **OK**.

To edit a network you've added, select it and click the **Edit** button. To remove it, select it and click the **Remove** button.

Configuring a Public or Intranet Pipe

If you want to regulate how many VoIP sessions can be connected to the server through a Public or Intranet Pipe,

1. In the Public Pipe panel, check the **Enable** box.
2. Enter the maximum WAN bandwidth you want to allocate to VoIP connections.
3. Specify the maximum sessions for one of the codecs. The system will calculate the maximum sessions for the other codecs automatically.
4. You can change the G.711 sessions by using the Up/Down arrow button.



Public Pipe

□ Enable

Bandwidth For VoIP: 0 Kb

Max Sessions G.711 / G.722: 0

Max Sessions G.723: 0

Max Sessions G.729: 0

Figure 212. The Public Pipe options

Notes

- When calculating the maximum sessions for each codec, the system uses the following bandwidth requirement to ensure that each session has some safety margin:

  G.711 / G.722 – 90 kbps

  G.723 – 24 kbps

  G.729 – 30 kbps

- It is recommended that you use 20 ms frame size for G.711, G.722, and G.729 when configuring a Codec Profile.

- When different IP devices using various codecs connect to the server through a Public Pipe, the system will aggregate the total bandwidth of all connections. If the total bandwidth exceeds that specified in the **Bandwidth for VoIP** box, the system will reject additional connection requests.

Configuration example

Suppose your company has a T1 line configured as half voice PRI and half data service. There are 12 remote employees using IP phones connecting to the Altigen system. Because bandwidth is limited, you would like to regulate the bandwidth used by VoIP. You have set up remote IP phones using G.729 with 20 ms frame, and you want to limit the number of concurrent VoIP sessions to 6. If you enter 180 in the **Bandwidth for VoIP** field, the system will show that 6 G.729 sessions are allowed.

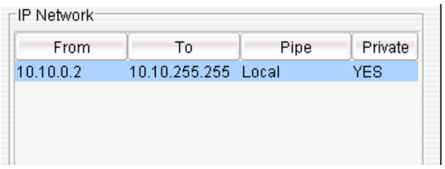
Configuring MaxCS Behind NAT

Your MaxCS system should be inside a firewall/NAT router. If your MaxCS is supporting remote IP phones, IPTalk or AltiClients, you need to configure MaxCS and the NAT router to make MaxCS work properly behind NAT. Port forwarding configuration on the firewall/NAT router is required. If you're not sure how to configure your firewall/NAT router, please consult your firewall/NAT router manual or vendor. Altigen Technical Support will not be able to help with this.

Important: If your firewall/NAT router supports SIP, you need to FULLY disable this feature on the firewall/NAT router, or conflicts may occur between MaxCS and the firewall/NAT router. In this case, remote IP phones might not work or might behave strangely. Again, please consult the firewall/NAT manual to find out how to do this.

Take the following steps:

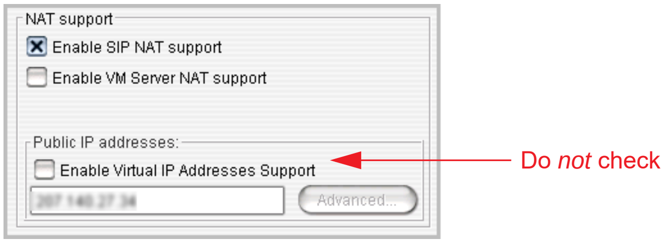
1. Make sure the MaxCS system uses a private *static* IP address, for example, 10.10.0.8. Do *not* use DHCP on the MaxCS system.
2. Define the range of the local IP addresses (see “Define an Address Range” on page 324). Make sure the MaxCS system is included in the range. If the range is not defined correctly, all the IP phones will not work.



From	To	Pipe	Private
10.10.0.2	10.10.255.255	Local	YES

Figure 213. The range of local IP addresses

3. Set local IP network ranges to private. Multiple private networks can be added.
4. On the **IP Networks** tab, in the NAT Support panel, check **Enable SIP NAT support**.



☒ Enable SIP NAT support

☐ Enable VM Server NAT support

☐ Enable Virtual IP Addresses Support

[redacted]

Do *not* check

Figure 214. The NAT Support options

Enter the Public IP address of the router in the Public IP Addresses panel. Do ***not*** check **Enable Virtual IP Addresses Support**.

5. Configure the NAT/firewall to forward TCP ports 10025, 10027, 10032, 10037, 10050, 10064, 1720 and UDP ports 69, 5060, 10060 to MaxCS.

6. Configure the NAT router to forward to MaxCS UDP ports 49152 + gwid * 512 ~ 49152 + (gwid * 512 + ipresno * 2) where *gwid* is the gateway id and *ipres* number is the number of the IP resource channels in the system. (See note below for an easier way to figure the port ranges.)

   For the MAX1000 system, it would be UDP ports, from 49152~49211 (30 IP resource channels).

   Note: An easy way to find out the RTP/TCP port range(s) for SIP is to look in the Current Resource Statistics window in MaxAdministrator (**View** > **Current Resource Statistics**). All the ports are listed in the **Local Ports** column.

Implementation details

After you complete the NAT configurations, the system will translate the sending party's IP address with the defined public IP address instead of the system's private IP address. When the remote IP device sends VoIP packets to the defined public address, all packets will be routed to the system's provided IP address by the NAT router.

Defining the IP Dialing Table

The IP Dialing Table is used for creating location-based VoIP routing in the enterprise.

To use a MaxCS-to-MaxCS connection for VoIP, you need to configure the routing in the IP Dialing Table for each MaxCS system.

Considerations

- The IP Dialing Table is disabled unless there is a VoIP board installed.
- You must assign an IP Trunk Access code (**System Configuration** > **Number Plan** tab)
- You must set the VoIP codec profiles.

Security Update in Release 8.6.1

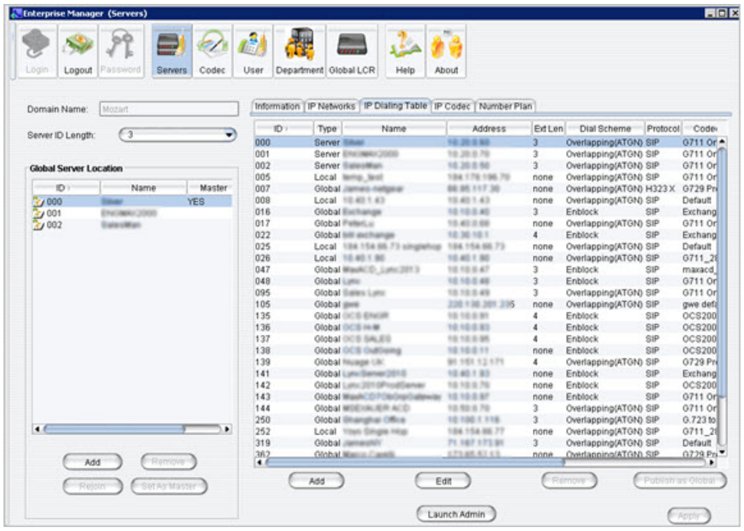
Release 8.6.1 included a security change which prevents a configuration file from being read remotely. As part of this change, MaxAdmin is initially configured to accept only local access.

This means that you must update the IP Dialing Table, to add any IP addresses that you need to allow.

1. Clear your browser cache.
2. Try to open *http://:10043/..%2f..%2fwindows/win.ini* remotely. Confirm that the system will not allow you to access this file.
3. To allow access to an IP Address, add an IP address entry to the IP Dialing Table in Enterprise Manager and publish this as a 'Global' type.
4. Try to access the IP address from step 2 remotely again. The system should now allow you to access that file now.

The IP Dialing Table Tab

To manage the IP dialing table, click the **IP Dialing Table** sub-tab in Enterprise Manager:



Domain Name: Mozart

Server ID Length: 3

Global Server Location

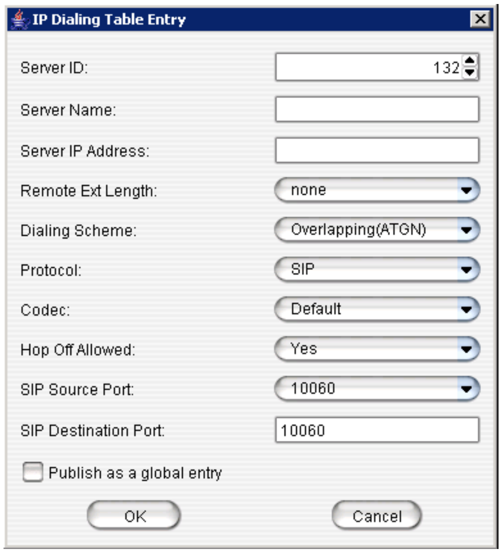
ID	Name	Master
000	[redacted]	YES
001	[redacted]	
002	[redacted]	

ID	Type	Name	Address	Ext Len	Dial Scheme	Protocol	Code
000	Server	[redacted]	[redacted]	3	Overlapping(ATGN)	SIP	G711 Or
001	Server	[redacted]	[redacted]	3	Overlapping(ATGN)	SIP	G711 Or
002	Server	[redacted]	[redacted]	3	Overlapping(ATGN)	SIP	G711 Or
005	Local	[redacted]	[redacted]	none	Overlapping(ATGN)	SIP	G711 Or
007	Global	[redacted]	[redacted]	none	Overlapping(ATGN)	H323 X	G729 Pr
008	Local	[redacted]	[redacted]	none	Overlapping(ATGN)	SIP	Default
016	Global	[redacted]	[redacted]	3	Enblock	SIP	Exchang
017	Global	[redacted]	[redacted]	none	Overlapping(ATGN)	SIP	G711 Or
022	Global	[redacted]	[redacted]	4	Enblock	SIP	Exchang
025	Local	[redacted]	[redacted]	none	Overlapping(ATGN)	SIP	Default
026	Local	[redacted]	[redacted]	none	Overlapping(ATGN)	SIP	G711_2
047	Global	[redacted]	[redacted]	3	Enblock	SIP	maxacd_
048	Global	[redacted]	[redacted]	3	Enblock	SIP	G711 Or
095	Global	[redacted]	[redacted]	3	Overlapping(ATGN)	SIP	G711 Or
105	Global	[redacted]	[redacted]	none	Overlapping(ATGN)	SIP	gwe defa
135	Global	[redacted]	[redacted]	4	Enblock	SIP	OCS200
136	Global	[redacted]	[redacted]	4	Enblock	SIP	OCS200
137	Global	[redacted]	[redacted]	4	Enblock	SIP	OCS200
138	Global	[redacted]	[redacted]	none	Enblock	SIP	OCS200
139	Global	[redacted]	[redacted]	4	Overlapping(ATGN)	SIP	G729 Pr
141	Global	[redacted]	[redacted]	none	Enblock	SIP	Exchang
142	Global	[redacted]	[redacted]	none	Enblock	SIP	OCS200
143	Global	[redacted]	[redacted]	none	Enblock	SIP	G711 Or
144	Global	[redacted]	[redacted]	3	Overlapping(ATGN)	SIP	G711 Or
250	Global	[redacted]	[redacted]	3	Overlapping(ATGN)	SIP	G.723 to
252	Local	[redacted]	[redacted]	none	Overlapping(ATGN)	SIP	G711_2
319	Global	[redacted]	[redacted]	3	Overlapping(ATGN)	SIP	Default
362	Global	[redacted]	[redacted]	none	Overlapping(ATGN)	SIP	G729 Pr

Figure 215. IP Dialing Table tab in Enterprise Manager

The left side of the window displays the VoIP domain name, the server ID length, and the name, ID and statuses of the global servers in this Domain.

To add an entry to the IP Dialing Table, click the **Add** button below the table (in the panel on the right).



Server ID:	132
Server Name:	
Server IP Address:	
Remote Ext Length:	none
Dialing Scheme:	Overlapping(ATGN)
Protocol:	SIP
Codec:	Default
Hop Off Allowed:	Yes
SIP Source Port:	10060
SIP Destination Port:	10060

☐ Publish as a global entry

Define the attributes for the entry:

Dialing Entry Parameter	Description
Server ID	A unique dialing number to connect to the remote server. The server could be MaxCS, a 3rd-party VoIP gateway, or an Altigen-certified 3rd-party VoIP device.
Server Name	A descriptive name of up to 15 characters to identify the server. This name may be used by Caller ID.
Server IP Address	The remote server's address. If the server has multiple IP addresses, enter the one that other servers will use to communicate to this system. This IP address format is recommended over DNS names, since with the IP address, the application does not need to resolve the name. DNS name is also posted in this field.
Remote Ext. Length	The length of extension digits at the remote location. Valid entries are None – 7, with "None" meaning not specified. Specifying the remote extension length is optional but highly recommended, since this information tells the system how long to wait for another entry before sending the digits.
Dialing Scheme	Overlapping (ATGN) allows the terminal to omit part of the digits required to complete a call while buffering the remaining digits. This results in faster response time, but it only works if the other end is also a MaxCS system. Enbloc allows the system to buffer all of the digits required to complete a call.
Protocol	SIP - Select if the destination supports SIP protocol.
Codec	Select which codec profile to use. If the selected profile is incompatible with the remote end, the call will not go through. If you create two items that point to the same IP address, they must use the same codec. Specifying a different codec is an invalid configuration. MaxCS will always use the codec defined in the first item.
Hop Off Allowed	Choosing Yes allows calls from this remote system to hop off to the PSTN by using the trunks in this system. Hop-off capability can be enabled or disabled on a per IP Dialing Table Location basis.
SIP Source Port	Used by UDP only. Choose the SIP source port.
SIP Destination Port	Used by UDP only. Is 10060, by default.
Publish as a global entry	If you are adding a system or 3rd-party VoIP device that is not part of the VoIP domain, but you want it to be seen by all servers in the domain, check this box. (The entry will appear as "Global" in the Type column.) You can also globalize it later by selecting the entry in the IP Dialing Table and clicking the Publish as Global button below the table.

The Multi-site VoIP Domain

Note: This feature is not applicable to the MaxCS Private Cloud service.

A group of Altigen systems can form a *VoIP domain* where they share the same global extension directory and call routing rules. The VoIP domain is based on VoIP framework and uses IP tie-trunks to interconnect among different sites.

A domain is created in MaxAdministrator. Here, a system is designated as the domain Master. Other Altigen systems can then be added to a VoIP domain.

The VoIP domain Master maintains global configurations and propagates the configurations to all the members belonging to this domain automatically. Any changes in the global configuration are propagated in real time to the other members in the VoIP domain.

Note: A multi-site installation requires an Altigen Enterprise license.

Multi-Domain Enterprise Management Features

This section lists the PBX features supported under the context of multi-domain Enterprise Management in this release.

Global Extension Features - Those features supporting global extension transparently

- Global extension Dialing (Phones and Clients)
  - Direct Dial (video not supported)
  - Conference
  - Transfer (Blind and Supervise)
  - Hold/Resume
  - System/Station/Phone Speed Dial
- Global BLF
  - Global Extension status monitoring (Idle/Ringing/Busy status)
  - Users can call Global extensions by pressing the assigned BLF softkey
  - Call pick-up is not supported
- Call a Global WG/Hunt Group (the agent must have a local extension)
- View Global Paging Group
- Global extension Forwarding/Routing
  - Trunk In Call Routing
  - DNIS Routing
  - Caller ID Routing
  - Extension forwarding options
  - Workgroup/Hunt Group forwarding options
  - Holidays routing
- AA
  - IVR Call to Ext/Group
  - VM Record Message
  - Dial-by-Name
- Other Call Features
  - Message Notification
  - Reminder Call
  - ONA
  - MeetMe
  - Emergency Notification
  - Return call from VM

    - Dialing from VM
    - Monitoring List
- MaxCommunicator/MaxAgent/MaxOutlook
    - Directory
    - Monitoring
        - State (Idle/Busy/Ringing)
        - Name
        - DND/Forward
        - Location
        - Department
        - Activity
- #93 (Intercom) a Global extension
- Advanced Call Router - call routing target

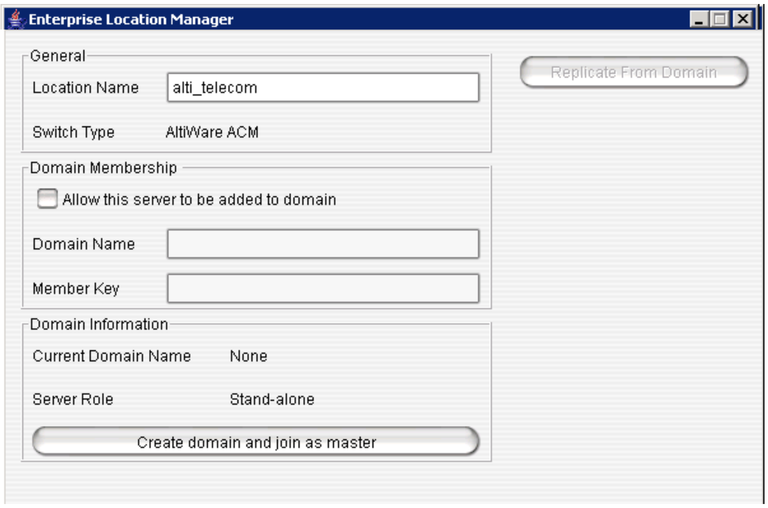
Enterprise Management Related Features

- Global Extension User Management
    - Changing/resolving Extension/Group Scope
    - Relocate Global Extension
    - Relocate VM
    - Redirect (Altigen phone and IPTalk)
    - #27 and #17 Global Relocation (#17 is not included in the "Relocating Global Extension for an IP Phone" section)
- Global LCR
- Global DID Routing
- Global Directory
- Global Dial-by-Name
- Greeting Synchronization
- Hop-on and Hop-off calls
- Data Transport between servers
    - ANI
    - DNIS
    - Caller Name
    - User Data
    - IVR Data
    - Tenant ID (not supported in 8.0 and later releases)
- PSTN Re-Routing

Creating a Multi-site VoIP Domain

To create a multi-site VoIP domain and designate a system as the domain Master:

1. Select **VoIP** > **Multi-Site Domain Configuration**. The Enterprise Location Manager window opens.



Enterprise Location Manager

General

Location Name: alti_telecom

Switch Type: AltiWare ACM

Domain Membership

☐ Allow this server to be added to domain

Domain Name:

Member Key:

Domain Information

Current Domain Name: None

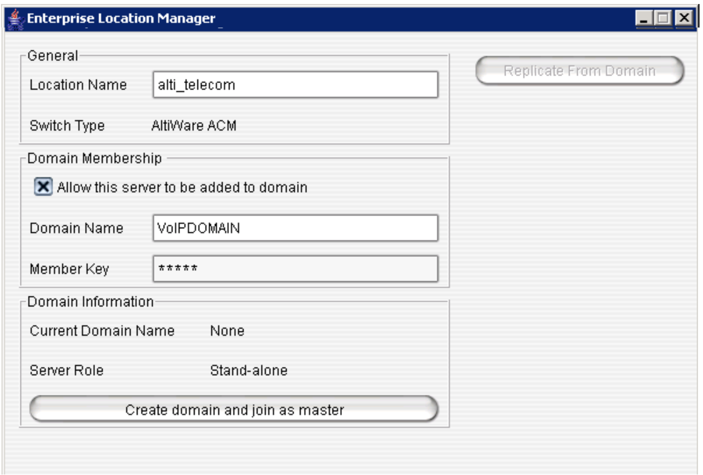
Server Role: Stand-alone

The name of the server appears in the **Location Name** field, and the name of your Altigen product appears in the **Switch Type** field (MaxCS ACC or MaxCS ACM). The domain name is blank, and the server role is currently **Stand-alone**.

2. Check the **Allow this server to be added to domain** check box.
3. Enter a Domain Name and a Member Key.

The Member Key will be the security password when the Domain Admin adds this location into the domain. To reduce the complexity of administration, you can use the same key for all member systems.

The Enterprise Location Manager window will look similar to the next figure.



Enterprise Location Manager

General

Location Name: alti_telecom

Switch Type: AltiWare ACM

Domain Membership

☒ Allow this server to be added to domain

Domain Name: VoIPDOMAIN

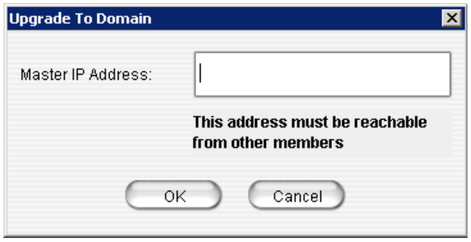
Member Key: *****

Domain Information

Current Domain Name: None

Server Role: Stand-alone

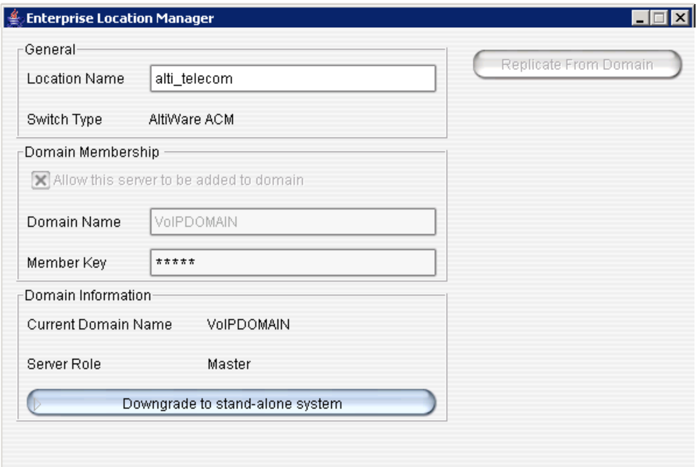
4. Click **Create domain and join as master**.



Master IP Address:

This address must be reachable from other members

5. Enter the IP address of this system. If this system has multiple IP addresses, enter the one that can communicate with other member servers.
6. Click **OK** and wait for 5 to 60 seconds, depending on the size and configuration of the system. The display in the Enterprise Location Manager window changes to show the name of the VoIP domain and this server as Master.



Location Name alti_telecom

Switch Type AltiWare ACM

☒ Allow this server to be added to domain

Domain Name VoIPDOMAIN

Member Key *****

Current Domain Name VoIPDOMAIN

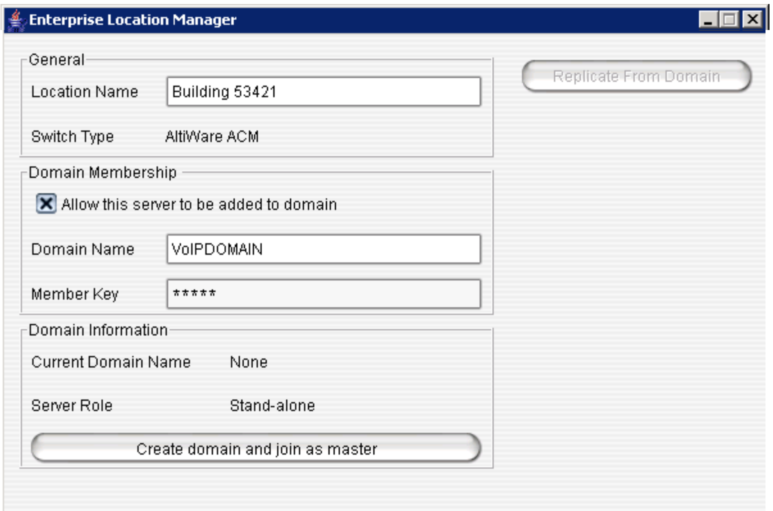
Server Role Master

Declaring Additional Servers for the VoIP Domain

Additional servers are added to the VoIP domain in Enterprise Manager, but first you must “declare” these servers and assign them a member key in MaxAdministrator. To do so:

1. Log on to the member server you want to declare.
2. Select **VoIP** > **Multi-Site Domain Configuration**. The Enterprise Location Manager window opens.

   The name of the server and the name of the Altigen product appear in the top box.
3. Check the **Allow this server to be added to domain** check box.
4. Enter the name of the VoIP domain that you want this server to be a part of.
5. Enter a member key for this server. The Member Key is the security password when the Domain Admin adds this server into the domain. To reduce the complexity of administration, you can use the same key for all member systems.



Enterprise Location Manager

General

Location Name: Building 53421

Switch Type: AltiWare ACM

Domain Membership

☒ Allow this server to be added to domain

Domain Name: VoIPDOMAIN

Member Key: *****

Domain Information

Current Domain Name: None

Server Role: Stand-alone

6. Click **Apply**, then click **Close**.

Repeat these steps for each server you want to make available to the VoIP domain. To actually add a server to the domain using Enterprise Manager, see “Adding a Server to a VoIP Domain” on page 334.

Working with Servers in the Domain

In the Global Server Location panel in Enterprise Manager, you can add a server to the VoIP domain by using the **Add** button in the panel, remove a selected server from the VoIP domain by using the **Remove** button, and you can set the master server, by selecting a server and clicking the **Set as Master** button. Before you can add a server to the VoIP domain, you must have declared it in MaxAdministrator (see “Declaring Additional Servers for the VoIP Domain” on page 332). These are the fields in the Global Server Location panel:

Server Parameter	Description
Domain Name	The name of the VoIP domain.
Server ID Length	Length is from 1-3. See ““Changing the Server ID Length” on page 333 for detailed information.
Global Server Location	Displays the ID, Name, and Status (active/inactive) of the servers in the VoIP domain. Master – One Domain system must be assigned as Domain Master to propagate configuration data to member MaxCS systems. The master acts as a central server to accept the connection, synchronize change from one site to the other sites, and authenticate users.

Changing the Server ID Length

The Server ID is used for the following two purposes:

- Identifying member systems in the VoIP domain
- Mapping to a remote system's IP address in the IP dialing table for system-to-system dialing

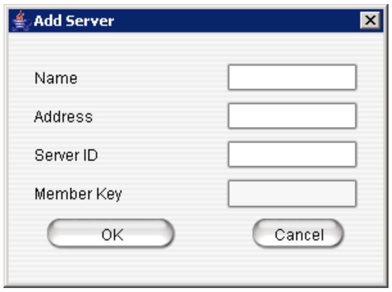
Depending on the number of systems that will be added to the VoIP domain and the number of entries in the IP dialing table, the **Server ID Length** can be set to 1, 2, or 3 digits.

Caution! The **Server ID Length** can be changed. However, if this number is changed, the server IDs are all altered. If you increase the length, the number 0 is added to the front of the server IDs. For example, if you change the length from 2 to 3, original ID 02 and 27 will become 002 and 027 respectively. If you change the length from 3 to 2, the original IDs 112 and 311 will become 12 and 11. It is advisable to keep the original length. If you are not sure about future expansion, using a 3-digit length is advised.

Adding a Server to a VoIP Domain

Important: Before you add a server to the domain, you need to make sure that the **System ID** (specified in MaxAdministrator, System Configuration tab) is not the same as another member server's **System ID**. Enterprise Manager will use the **System ID** to build a unique identifier in the multisite database. Once a server is joined to a domain, you cannot change the **System ID** in MaxAdministrator.

1. Click the **Add** button in the Global Server Location panel.

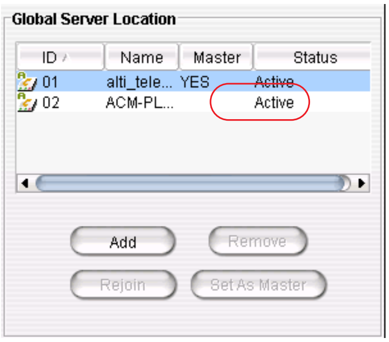


2. Define the attributes for the server, and click **OK**:

Server Parameter	Definition
Name	Enter the name of the server.
Address	Enter the IP address of the server.
Server ID	A unique dialing number to connect to this server.
Member Key	Enter this server's member key. (Configured in this server's Enterprise Location Manager: VoIP > MultiSite Domain Configuration).

After you add a member server to the Domain, an entry is also added to the IP dialing table and propagated to all members automatically.

In the Global Server Location panel, the status will show "Active" if the Domain master communicates to the member successfully.


Global Server Location

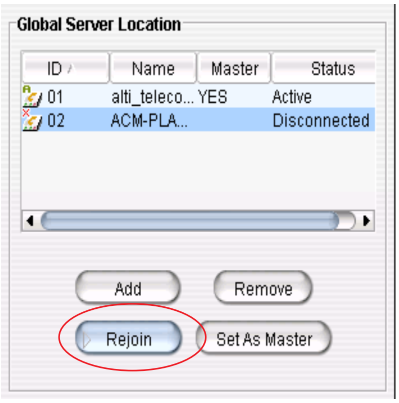
ID	Name	Master	Status
01	alti_tele...	YES	Active
02	ACM-PL...		Active

In the event that you need to shut down the Domain Master for a period of time, you can change the Master role to another member system by selecting one of the member systems and clicking the **Set as Master** button.

Rejoining a Server to the VoIP Domain

If a slave server crashes, or for some other reason disconnects and never returns by itself into the domain, you will have to manually rejoin it to the VoIP domain:

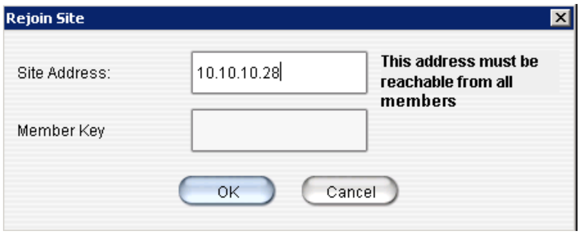
1. Rebuild the slave, if necessary.
2. In the **VoIP** > **Multi-Site Domain Configuration** window, make sure the slave's Server Role is **Standalone** and that the domain name is correct.
3. The **System ID** of this slave should be the same as it was before it became disconnected from the domain. (This ID is set in MaxAdministrator: in **System Configuration** > **General** tab.)
4. In Enterprise Manager, Global Server Location panel, select the slave and click the **Rejoin** button to synchronize the slave with the domain.



Global Server Location

ID	Name	Master	Status
01	alti_teleco...	YES	Active
02	ACM-PLA...		Disconnected

A dialog box opens.



Rejoin Site

Site Address: 10.10.10.28

This address must be reachable from all members

Member Key

5. Input the address and member key, and click **OK**.

Setting an Alternate Server for Altigen IP Phones

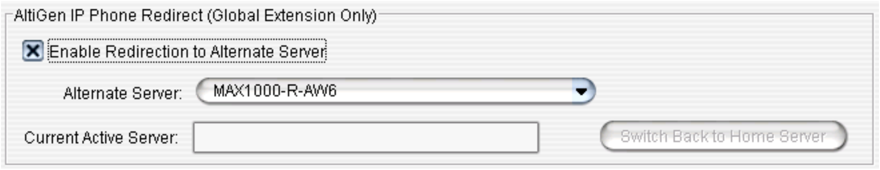
In a VoIP domain, you can set an alternate server to which global Altigen IP phones will be registered when their own server (primary server) experiences a problem that interrupts phone service. The IP phones will register to the alternate server. This applies to a workgroup, as well. Switchover must be enabled for the individual IP phones/groups in Enterprise Manager (**User** button > **Resolve** tab). But before you can do this, you must set an alternate server.

Notes:

- Because of its role in the domain, the domain master cannot use this feature.
- This feature does not apply to extensions using IPTalk.
- Make sure the alternate server has enough licenses, such as agent licenses, station licenses, and so on.

To set an alternate server,

1. Click the **Servers** button, and then the **Information** tab.
2. In the Altigen IP Phone Redirect panel at the bottom of the tab, check **Enable Switchover to Alternate Server.**



AltiGen IP Phone Redirect (Global Extension Only)

☒ Enable Redirection to Alternate Server

Alternate Server: MAX1000-R-AW6

Current Active Server:

3. Select an alternate server from the list.
4. Click **Apply**.

   (After you click **Apply**, the current active server name will appear in the **Current Active Server** box. This name is not editable.)

With the alternate server assigned, you can now configure individual extensions/groups for redirection. See “Redirecting Altigen IP Phones When a Server Is Down” on page 343.

Note: If the alternate server assignment is removed from the configuration above, the redirection configuration is removed from all extensions and workgroups to which you assigned this feature (**User** button > **Resolve** tab).

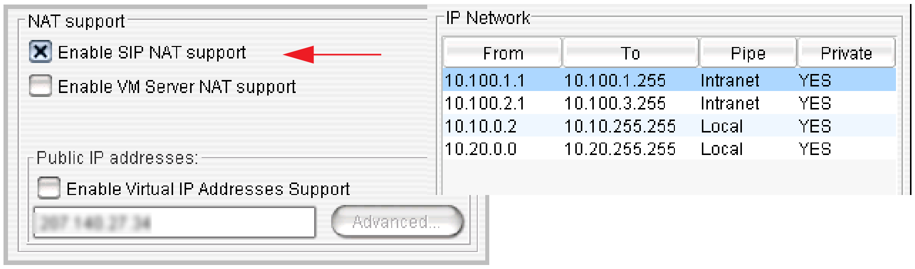
Note: If Native VM Integration with Microsoft Exchange is also configured, then both the primary and alternate servers need to have the *same dial plan* configured in the Microsoft Exchange server, so that users who have extensions flagged for redirection can access their voice messages from both the primary and alternate servers.

If the Primary or Alternate Server Is Behind NAT

When you configure the redirection feature for Altigen IP phones, the primary server sends the IP address of the primary and alternate servers to the IP phone. The IP phone may run on the public or local network, and the primary server or alternate server may run behind NAT. So to support a server behind NAT, the primary server sends the NAT IP address or local private address according to the IP phone's IP address. If the IP phone's IP address is in a local network for the server, the primary server sends the private address, otherwise it sends the NAT address.

To configure for NAT,

1. In Enterprise Manager, click the **Servers** button > **IP Networks** tab.
2. In the NAT Support panel, check **Enable SIP NAT Support**.



NAT support

☒ Enable SIP NAT support

☐ Enable VM Server NAT support

Public IP addresses:

☐ Enable Virtual IP Addresses Support

[redacted]

IP Network

From	To	Pipe	Private
10.100.1.1	10.100.1.255	Intranet	YES
10.100.2.1	10.100.3.255	Intranet	YES
10.10.0.2	10.10.255.255	Local	YES
10.20.0.0	10.20.255.255	Local	YES

3. Configure the NAT address.
4. In the IP Network panel, configure the IP range of the local network or public network.

When Will Switchover Happen?

If the current active system is the primary server, switchover will happen under one of the following conditions:

- Network error on the primary server or the primary server is down. IP phones cannot connect to the primary server. After one minute of retrying, the IP phones will register to the alternate server. At that time, the status of the primary server is "Disconnected" or "Softswitch Offline".
- Softswitch service on the primary server is down. The status of the primary server is "Softswitch Offline".
- IP phone service on the primary server is down. IP phones cannot register to the primary server. After one minute of retrying, the IP phones will register to the alternate server. At that time, the status of the primary server is "Fail".
- Default gateway on the primary server is down. The status of the primary server is "Fail".
- Manual switch from Enterprise Manager. The status of the primary server is "Standby".

When the primary server is recovered, the status is "Standby".

If the current active system is the alternate server, only clicking the **Switch Back to Home Server** button in Enterprise Manager can switch the control from the alternate server back to the primary server. Before manually switching back, the status of the primary server should be "Standby". After you have manually switched back, the status of the primary server changes to "Active".

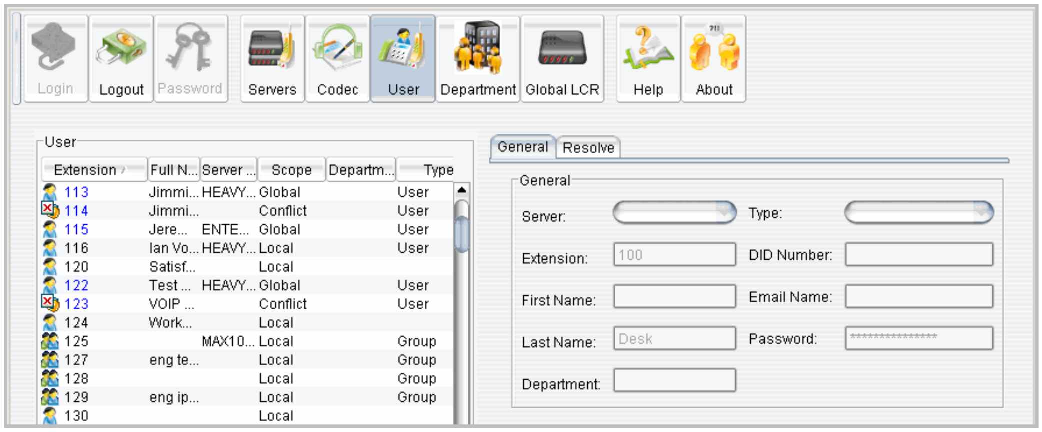
Note: Unlike normal relocation, redirect can be executed only on the destination site.

Managing Domain Users

Click the **User** button in the toolbar to:

- Display all extensions from all VoIP domain member systems: extension number, name, type, home server, and scope. The *scope* of an extension is discussed in the following section.
- Resolve conflicting extensions and groups to global user or back to local user (on the **Resolve** tab).
- Relocate an extension from one location to another location with optional voice mail (on the **Resolve** tab).

The **General** tab displays read-only information about the selected extension.



User

Extension	Full N...	Server ...	Scope	Departm...	Type
113	Jimmi...	HEAVY...	Global		User
114	Jimmi...		Conflict		User
115	Jere...	ENTE...	Global		User
116	Ian Vo...	HEAVY...	Local		User
120	Satisf...		Local		
122	Test ...	HEAVY...	Global		User
123	VOIP ...		Conflict		User
124	Work...		Local		
125		MAX10...	Local		Group
127	eng te...		Local		Group
128			Local		Group
129	eng ip...		Local		Group
130			Local		

General

Server:
Type:
Extension: 100
DID Number:
First Name:
Email Name:
Last Name: Desk
Password: ***************
Department:

Figure 216. The User sub-tab

When a global extension is added to a member system, this extension can be propagated to other networked systems in the VoIP domain automatically. This extension is recognized as a *remote* extension by other systems. When a call is made to a remote extension, it is redirected to the remote system over IP automatically.

Note: No virtual extension configuration is needed to forward the call. The Enterprise VoIP domain uses the User directory combined with the IP dialing table to resolve multi-site routing.

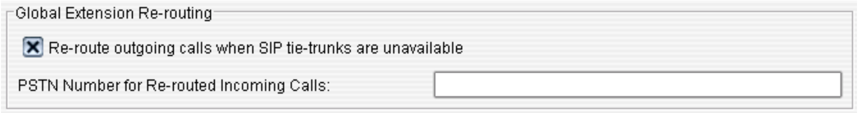
An extension can call a remote extension when invoking basic features such as an extension-to-extension call, call transfer, conference, Zoomerang, and so on. Advanced features, such as silent monitoring and barge-in, between sites are NOT supported.

PSTN Failover When the TCP/IP Network is Down

Enterprise call routing works with a SIP-tie trunk, but at times the TCP/IP network may be down. To provide failover for these times, you can assign a PSTN number to each MaxCS in Enterprise Manager. The default PSTN number is the main number of each MaxCS site.

To enable global extension rerouting,

1. In Enterprise Manager click the **Servers** button, and then the **Information** tab.
2. In the Global Extension Re-Routing panel, check **Re-route outgoing calls when SIP tie-trunks are unavailable**.
3. Enter a PSTN number in the **PSTN Number for Re-routed Incoming Calls** field, if different from the main number of the MaxCS site. If nothing is entered in this field, the main number of the MaxCS site is used. If you enter a number, use the E.164 format.



Global Extension Re-routing

☒ Re-route outgoing calls when SIP tie-trunks are unavailable

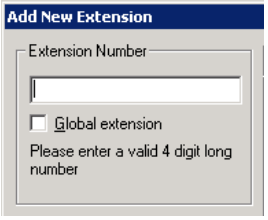
PSTN Number for Re-routed Incoming Calls:

When failover is needed, MaxCS dials the destination site number with the proper call prefix and area code or country code. On the call destination site, the call comes into the AA. The AA receives the extension number the call is directed to and rings the extension.

Note: The rerouted call may hear 1 or 2 seconds of auto-attendant announcement before the call is sent to the extension.

The Scope of an Extension in the VoIP Domain

When an extension is added to a system in MaxAdministrator, Extension Configuration window, it can be defined as *Global* by checking the **Global extension** box. If this box is not checked, the newly added extension is a local extension.



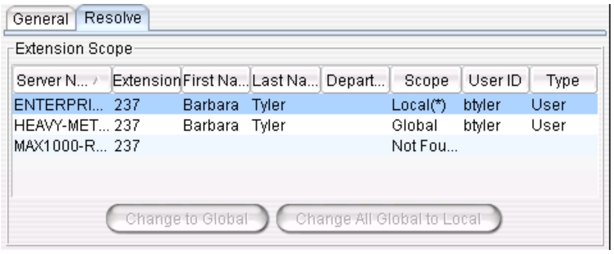
Add New Extension

Extension Number

☐ Global extension

Please enter a valid 4 digit long number

The scope of an extension shows the relationship of the extension to other member systems. In Enterprise Manager, a selected extension's scope appears on the **Resolve** tab.



Extension Scope

Server N...	Extension	First Na...	Last Na...	Depart...	Scope	User ID	Type
ENTERPRI...	237	Barbara	Tyler		Local(*)	btyler	User
HEAVY-MET...	237	Barbara	Tyler		Global	btyler	User
MAX1000-R...	237				Not Fou...		

You may see any of the following in the **Scope** column:

- **Global** – The extension has been published to all member systems within the same VoIP domain. Every extension in the domain can dial and ring this number.

- **Local** – The extension has not been published to the VoIP domain. Only extensions in the same system can dial and ring this number.
- **Not Found –** The extension is not a **Global** extension and is not created in the selected system as **Local**. The extension number is used by other member systems as a local extension.
- **Remote** – The word *Remote* in the **Scope** column shows that the selected system maintains this extension in the extension list because it is a **Global** extension of another member system. If you see an extension whose Type is **Remote** in the Extension Scope window, you can only see the extension information. You cannot configure any tabs because it is created in another system.
- **Conflict** – Conflict happens when one of the following situations has occurred:

- The same extension number exists as a **Global** extension in one member system and as a **Local** extension in other systems.
- The same extension number was created as a **Global** extension in different systems before the VoIP domain was formed.

The following example may help you conceptualize the multi-site extension scope.

Suppose you have three systems in different locations connected over the IP network. The numbering for System A is 1xx; System B is 2xx, and System C is 3xx.

System A is configured as the VoIP domain Master. Assuming there is no conflict , the following table shows the Scope relationship of **Global** vs. **Remote**:

Ext	System A (Domain Master)	System B	System C
100	Global	Remote	Remote
200	Remote	Global	Remote
300	Remote	Remote	Global

In the event that multiple systems have a same extension or group number created, the following situations may occur:

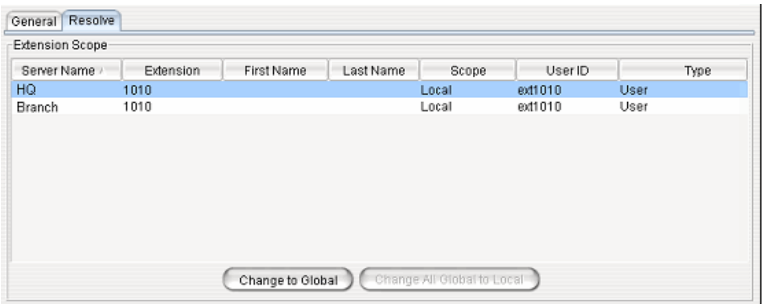
Ext	System A	System B	System C	Scope	Note
401	Local	Not Found	Not Found	Local	1
402	Local	Local	Not Found	Local	2
403	Global	Local	Local	Conflict	3
404	Global	Global	Local	Conflict	4

1. Extension 401 is created in System A for local purposes. Users in Systems B and C cannot dial and ring extension 401.
2. Extension 402 is created in both Systems A and B. You may intentionally set it up this way so that System A and B users can dial 402 for their local purposes. Ext. 402 may be used for connecting to a paging device, for example.
3. Extension 403 is created in all systems. It is defined as Global when created in System A and not defined as Global when created in Systems B and C. This conflict requires resolution, or else System B and C users cannot dial to the Global extension in System A.
4. Extension 404 is created in Systems A and B as Global prior to the creation of the VoIP domain. This conflict also requires resolution to determine which system will host the Global extension.

Changing an Extension's Scope from Local to Global

If you need to resolve a conflict by making a Local extension into a Global extension, follow these steps:

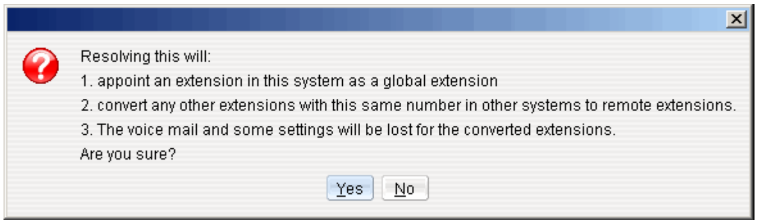
1. Select the extension in the User panel, and click the **Resolve** tab.



Server Name	Extension	First Name	Last Name	Scope	User ID	Type
HQ	1010			Local	ext1010	User
Branch	1010			Local	ext1010	User

2. Select the server name/extension where you would like the Global extension to reside.
3. Click the **Change to Global** button.

Note: You must take the voice mail box and extension configuration into consideration when you change an extension to Global. In making this change, you will be deleting the voice mail box and extension settings on the home system of the "other" Local extension. A warning box will prompt you for confirmation.


Resolving this will:

1. appoint an extension in this system as a global extension
2. convert any other extensions with this same number in other systems to remote extensions.
3. The voice mail and some settings will be lost for the converted extensions.

Are you sure?

Changing an Extension's Scope from Global to Local

If you want to change an extension's scope from Global to Local, you can highlight the extension and click the **Change All Global to Local** button. This extension's scope in other member systems will be impacted after Global is changed to Local. Using the previous case as an example, you may encounter one of the following situations when changing an extension's scope from Global to Local.

Situation 1: One Global and no conflict

Before you make the change, extension 100's scope is as follows:

Ext.	System A	System B	System C
100	Global	Remote	Remote

After you change extension 100 to Local, the scope of 100 will be:

Ext.	System A	System B	System C
100	Local	Not Found	Not Found

Note: After you make the change, users in Systems B and C cannot dial and ring extension 100. Only System A users can call local extension 100.

Situation 2: One or more Global with conflict

Before you make the change, the scope of extensions 403 and 404 is as follows:

Ext.	System A	System B	System C
403	Global	Local	Local
404	Global	Global	Local

After you change the two extensions to Local, their scope will be:

Ext.	System A	System B	System C
403	Local	Local	Local
404	Local	Local	Local

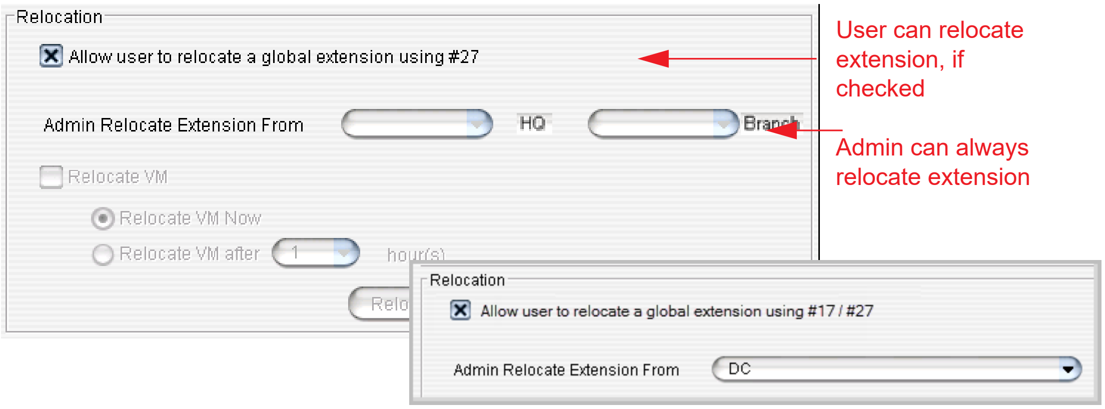
Note: After you make the change, extensions 403 and 404 can be dialed only by the users in their own system.

Relocating a Global Extension for an IP Phone

The administrator can relocate a global extension from one system to another. In addition, a *user* may be allowed to relocate a global extension by using the feature code #27. To allow a user to use this feature, check the appropriate check box in the Relocation panel on the **Resolve** tab. The behavior of this feature differs, depending on whether an analog or an Altigen IP phone is being used. (See “Relocating a Global Extension Using #27 on Analog Phone vs Altigen IP Phone” on page 342..)

As of Release 8.0, Polycom users can also relocate extensions. Refer to the *MaxCS Polycom Configuration Guide* for requirements and instructions.

Note: The check box is available only if a global extension is selected and that extension has no conflict.



Relocation

☒ Allow user to relocate a global extension using #27

Admin Relocate Extension From HQ Branch

□ Relocate VM

● Relocate VM Now

○ Relocate VM after 1 hour(s)

Relocation

☒ Allow user to relocate a global extension using #17 / #27

Admin Relocate Extension From DC

User can relocate extension, if checked

Admin can always relocate extension

When a global extension (1001, in this example) is moved from site A to site B, this is what happens:

- The following configurations are replicated from site A to site B:
  - First Name
  - Last Name
  - Password
  - Extension Number
  - DID Number

  - Dial by Name
  - Disable Mailbox option (Extension Configuration, **Mail Management** tab)
- Site A marks extension 1001 as removed and adds it to a Relocated Extension List (REL). The configuration of extension 1001 is still remembered in site A, even though it appears to be removed.
- Site B creates extension 1001. If extension 1001 is found in site B's REL, the extension 1001 will be restored in site B. However, the fields listed above will be overwritten with the settings of site A's extension 1001. If extension 1001 is not found in site B's REL, a new extension 1001 will be created in site B. The fields listed above will be set with site A's extension 1001 settings. The remaining fields of extension 1001 in site B are set with default values.

For the administrator to relocate a global extension,

1. Select the extension in the **User** list. The Relocation panel shows where the extension is located.
2. From the **To** box, select a different system for the extension.
3. To move the extension's voice mail along with the extension, check the **Relocate VM** check box. Then select either **Relocate VM Now** or **Relocate VM after x hour(s)**.

   Note: Because moving the voice mail requires network bandwidth, you may want it to move when system usage is low. The first time the voice mail is moved to a specific location, it can take hours for all the voice mails to be moved. Thereafter, only new voice mails are moved (because the old ones are still there, backed up), so subsequent moves take a shorter time.

   VM files are transferred by HTTP protocol using TCP port 10043. The administrator can configure the firewall/router to limit the bandwidth on port 10043, so that the voice mail transferring will not impact the voice quality over IP.

   Note: If you do not move the voice mail, the VM files will be deleted and cannot be recovered. (When the *user* relocates an extension using #27, the voice mail is moved also. The user cannot choose whether or not to move the voice mail.)
4. Click **Relocate**.

Notes on Relocating a Global Extension

- The phone user can start using the voice mail during VM relocation, but the voice mail count will keep increasing until the relocation is complete.
- If extension 1001 is relocated from site A to site B, and the administrator creates a local extension 1001 in site A, the extension 1001 will be removed from the REL. Later, if the administrator removes the local extension 1001 and relocates global extension 1001 back to site A, this extension cannot be restored to its original settings.
- When an extension is relocated to site B for the first time, the administrator or the user should configure the Call Restriction, Speed Dial list, and so on, for one time in site B. These configurations will be stored on site B. Later, if the extension is relocated to site B again, no additional configuration is needed, as the previous configuration will be restored.
- If multiple systems in the VoIP domain have a PRI interface, it's possible that DID numbers could be duplicated. For example, say the DID number for extension 1001 is configured as 250. In this case, the DID number 5102520*250* and 4087899*250* will ring extension 1001. To ensure that this doesn't happen, you can do one of two things: (1) Make sure the DID numbers are not duplicated; (2) Ask the CO to send more digits (to decrease the likelihood of identical DID numbers).

Relocating a Global Extension Using #27 on Analog Phone vs Altigen IP Phone

- Analog phone: The phone must be off hook. The user presses #27 and follows the voice prompts. User must press # after inputting the password.
- IP phone: The IP phone must be on hook. The user presses #27, and then inputs the global extension number and password. The global extension is then relocated to this IP phone.

If system B does not have a prior record of this extension, it will create a new extension with known information and the following settings:

- **Enable IP Extension** and **Dynamic IP Address** settings will be selected automatically (in MaxAdministrator, Extension Configuration window).
- The newly created extension will use the *default* voice mail, mail forwarding, notification, call handling, restriction, and monitor list settings (MaxAdministrator, Extension Configuration window).

  Note: The administrator needs to make the proper changes for this user when the global extension is relocated by the user.
- When this Global extension user returns to his home office, all settings are stored in the REL database. The administrator does not need to change these settings when the user presses #27 to relocate the extension the next time.

Relocating More Than One Global Extension

When more than one global extension is being relocated at the same time, and voice mail is also being relocated, the voice mail of the extension that was relocated first will be copied over completely to the relocation site, before copying begins for the voice mail of the second extension, and so on.

The extension, itself, is relocated immediately.

Redirecting Altigen IP Phones When a Server Is Down

Relocating a global extension, described in the preceding section, is intended to serve employees who are physically relocating to another office for a time. Administrators can also configure global IP phones to register to another server in the VoIP domain when their primary server goes down for some reason. All configured phones switch over at the same time. When their primary server returns to service, the administrator can switch the phones back to their primary server by clicking the **Switch Back to Home Server** button in the **Servers** > **Information** tab. For more complete information, see “Setting an Alternate Server for Altigen IP Phones” on page 335.

Notes:

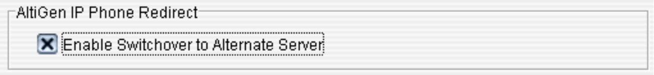
- When you redirect Altigen IP phones, voice mail is not moved. Otherwise, the extension configuration changes of the redirect feature are the same as they are with normal relocation.
- If Native VM Integration with Microsoft Exchange is also configured, users can access their voice messages from both the primary and alternate servers, if both have the *same dial plan* configured in the Microsoft Exchange server.
- Redirection does not work when an extension user is using IPTalk.

Before configuring individual IP phones to redirect from their primary server to an alternate server, an alternate server must be assigned in **Servers > Information** tab **> Altigen IP Phone Redirect** panel. The Redirect option is not available until an alternate server is assigned. Only Altigen IP phones that are global and have no conflict with the extensions of other sites can be configured to redirect.

To configure an IP phone to redirect,

1. In Enterprise Manager click **Users** button > **Resolve** tab.
2. Select a global IP phone whose server has an alternate server assigned.

   Note: The Altigen IP extension may need to be pre-configured on the alternate server to match its configuration on the home server, so that it works as expected. (For example, the alternate server may have a different call restriction policy. The extension on the alternate server may belong to a different workgroup. The greetings may be different even if the extension number is the same.)
3. Check the **Enable Switchover to Alternate Server** check box.



AltiGen IP Phone Redirect

☒ Enable Switchover to Alternate Server

Note: If an extension configured with the redirection feature is manually relocated (by the system administrator in Enterprise Manager or by the user pressing #27), the redirection configuration is dropped on the new site. If the extension is manually relocated back to its original site, the feature is recovered.

Changes to Altigen IP Phone When Redirect Is Configured

After the redirection feature is configured, the IP phone will receive the configuration of the primary and alternate server address, and store them in its local flash memory. Once it has been configured for redirection, the IP phone's "AW Server" address will be that of the primary server. The user can view the address on the IP phone (**Menu > System > AW Server**) but cannot configure it. When redirect is enabled, "Primary Server" and "Alternate Server" are added to the phone's **System** menu. They are read-only.

IPTalk Redirect

The Redirect feature, if enabled , 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

Enable IPTalk Redirect

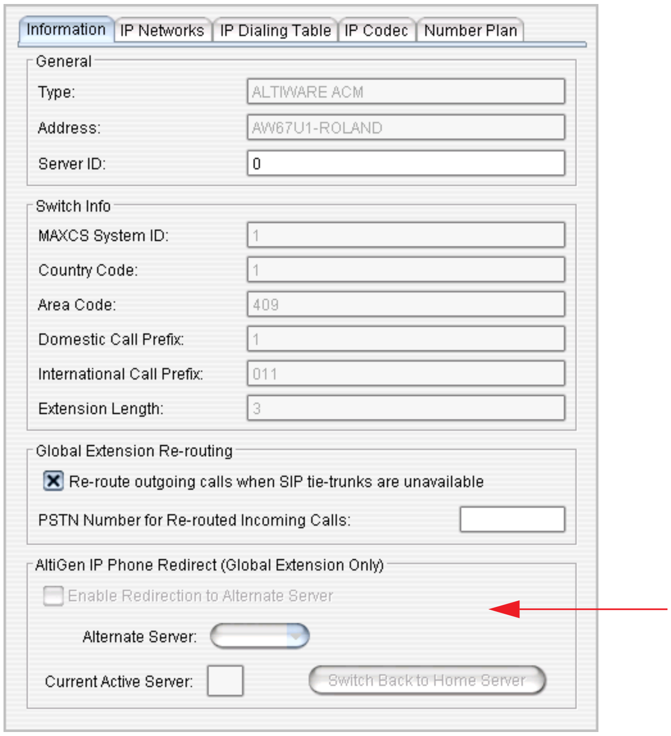
The Redirect feature, if enabled, will prompt users to connect to a backup server if their client application loses its connection with the primary server. This has been implemented in MaxAgent, MaxCommunicator, and MaxOutlook.

To enable this feature, Administrators perform two steps:

1. Enable the Redirect feature for MaxCS.
2. Enable the Redirect ability for specific user extensions.

To enable the Redirect feature ,

1. In MaxCS Administrator, enable the Redirect feature for MaxCS. Select **VoIP** > **Enterprise Network Management**.
2. Click the **Servers** button on the Toolbar. Select the **Information** subtab.
3. Check the option **Enable Redirection to Alternate Server**.



General

Type: ALTIWARE ACM

Address: AW67U1-ROLAND

Server ID: 0

Switch Info

MAXCS System ID: 1

Country Code: 1

Area Code: 409

Domestic Call Prefix: 1

International Call Prefix: 011

Extension Length: 3

Global Extension Re-routing

☒ Re-route outgoing calls when SIP tie-trunks are unavailable

PSTN Number for Re-routed Incoming Calls:

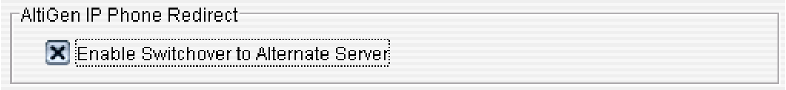
AltiGen IP Phone Redirect (Global Extension Only)

☐ Enable Redirection to Alternate Server

Alternate Server:

Current Active Server:

4. For *Alternate Server*, select the server that you want to use as the alternate server. Click **Apply**.
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**.



AltiGen IP Phone Redirect

☒ Enable Switchover to Alternate Server

Figure 217. Enable switchover for a user

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.

Switch Users Back to the Main Server

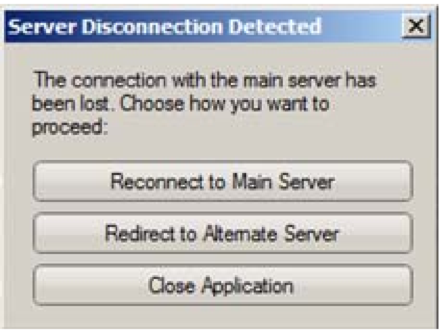
In the event that the main server goes down or is otherwise unavailable, you can ask users to switch client applications from the alternate server back to the main server by following these steps:

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

MaxAgent and MaxCommunicator Switchback Behavior

For MaxCommunicator and MaxAgent, when you enable this feature for MaxCS, users that have been assigned the switchover ability will experience the following behavior if their client loses its connection with the MaxCS server.

1. When the 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.



The connection with the main server has been lost. Choose how you want to proceed:

Figure 218. The client application prompts the user to reconnect or switch servers

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.

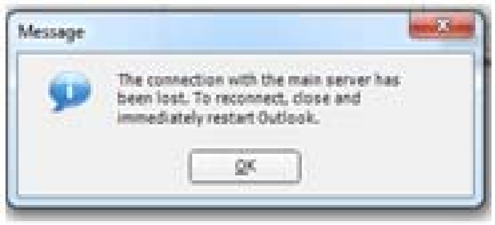
   If the user chooses **Redirect to Alternate Server**, then the client will establish a connection with the alternate server.

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 Switchback Behavior

Users that have been assigned the switchover ability will experience the following behavior if MaxOutlook loses its connection with the MaxCS server.

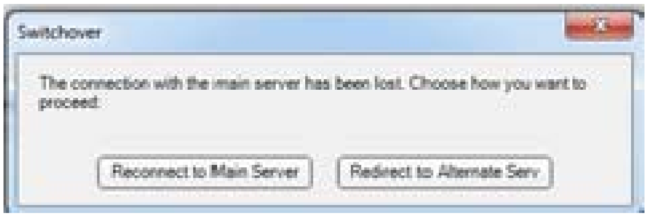
1. When the connection with the main server is lost, a message opens.



The connection with the main server has been lost. To reconnect, close and immediately restart Outlook.

Figure 219. MaxOutlook prompts the user to close and restart the application

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



The connection with the main server has been lost. Choose how you want to proceed:

Figure 220. MaxOutlook prompts the user to either reconnect or redirect

3. 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.

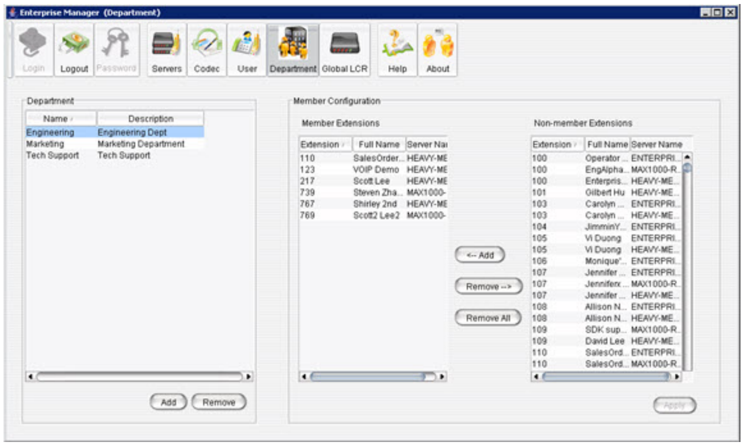
Once you have brought the main server back up and clicked **Switch Back to Home Server** within Enterprise Manager, the user will be prompted to switch the client's connection back to the main server.

Configuring Departments in a Multi-site VoIP Domain

In a VoIP domain, departments can be defined and added to extensions. An extension in one MaxCS system can be assigned to only one department. However, the same extension number in different MaxCS systems can be assigned to different departments. A department can also be assigned to a global extension and can be seen across the Enterprise domain.

In MaxAdministrator, the department field can be seen on the Extension **General** tab. In MaxCommunicator, the department is displayed on the **Directory** and **Monitor** tabs. In Enterprise Manager, the department is displayed in the **User** list. Departments can also be seen in CDR Search.

To define a department and assign or remove members from a department, click the **Department** button.



Name	Description
Engineering	Engineering Dept
Marketing	Marketing Department
Tech Support	Tech Support

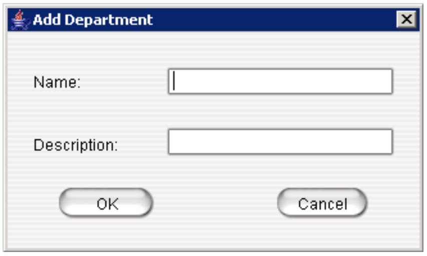
Extension	Full Name	Server Nai
110	SalesOrder...	HEAVY-ME
123	VOIP Demo	HEAVY-ME
217	Scott Lee	HEAVY-ME
739	Steven Zha...	MAX1000-
767	Shirley 2nd	HEAVY-ME
769	Scott2 Lee2	MAX1000-

Extension	Full Name	Server Name
100	Operator ...	ENTERPRI...
100	EngAlpha...	MAX1000-R...
100	Enterpris...	HEAVY-ME...
101	Gilbert Hu	HEAVY-ME...
103	Carolyn ...	ENTERPRI...
103	Carolyn ...	HEAVY-ME...
104	JimminY...	ENTERPRI...
105	Vi Duong	ENTERPRI...
105	Vi Duong	HEAVY-ME...
106	Monique'...	ENTERPRI...
107	Jennifer ...	ENTERPRI...
107	Jenniferx ...	MAX1000-R...
107	Jennifer ...	HEAVY-ME...
108	Allison N...	ENTERPRI...
108	Allison N...	HEAVY-ME...
109	SDK sup...	MAX1000-R...
109	David Lee	HEAVY-ME...
110	SalesOrd...	ENTERPRI...
110	SalesOrd...	MAX1000-R...

Figure 221. Department configuration

To define a department,

1. Click the **Add** button at the bottom of the Department panel.



2. Enter a department name and a description, if desired, and click **OK**.

To configure extensions for departments,

1. Select a department in the Department list.
2. To add non-member extensions to the department, select the extensions and click **Add**.
3. To delete extensions from the Member Extensions list, select the extensions, and click **Remove**. To remove all member extensions from a department, click **Remove All**.

Configuring Global Least Cost Routing

Global LCR allows you to save on toll charges by making long distance or international calls through a VoIP domain member system. The target system will function like a PSTN gateway for other member systems to hop-off. For example, suppose you have two systems in the U.S. and one system in the U.K. configured as VoIP domains. When users in the U.S. dial country code 44, you want the call to be dialed though the system in the U.K. to its PSTN network.

Global LCR has higher priority than local outcall routing. The system will check the Global LCR entries first before the call is handled by the local system's outcall routing rules.

Before you configure Global LCR, you need to evaluate the following conditions:

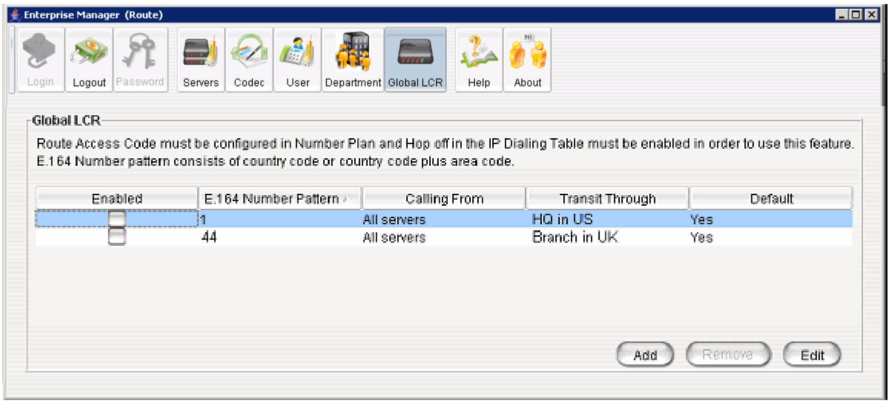
- How many concurrent calls will be routed through the target system?
- Does the target system have enough PSTN trunks to support the entire VoIP domain?
- Does the target system have enough WAN bandwidth to support system-to-system and PSTN hop-off calls?

Before you configure Global LCR, you need to make sure the following settings are properly configured in Max-Administrator:

- Both systems need to have the route access code configured on the **Number Plan** tab in System Configuration. (The user has to dial the route access code + the phone number to use Global LCR.)
- The target system needs to have the hop-off restriction reference properly configured. The reference extension is set on the **Call Restriction** tab in System Configuration, and then that reference extension cannot have **Internal Calls Only** checked on the **Restriction** tab of Extension Configuration.

To configure Global Least Cost routing,

1. Click the **Global LCR Button**.

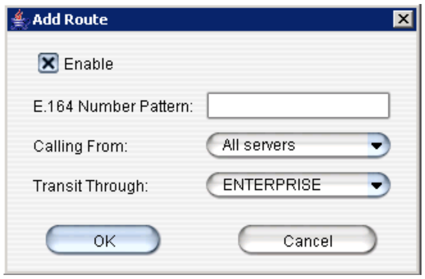


Global LCR

Route Access Code must be configured in Number Plan and Hop off in the IP Dialing Table must be enabled in order to use this feature.
E.164 Number pattern consists of country code or country code plus area code.

Enabled	E.164 Number Pattern	Calling From	Transit Through	Default
☐	1	All servers	HQ in US	Yes
☐	44	All servers	Branch in UK	Yes

2. On the Global LCR screen, click the **Add** button.



☒ Enable

E.164 Number Pattern:

Calling From: All servers

Transit Through: ENTERPRISE

3. Fill in the dialog box, and click **OK**.

Parameter	Description
Enable	Check this check box to enable the configuration.
E.164 Number Pattern	E.164 is the ITU standard format for international telephone numbers. Enter a country code and area code. For example, the number pattern for a site in Fremont, Calif., would be 1510 (the country code 1, followed by the Fremont area code 510).
Calling From	Select the server from which the call originates, or select All Servers.
Transit Through	Select the server that receives the call.

4. After adding a route, click **Edit**, check the **Enable** check box, and click **OK** to activate the Global LCR route.

To edit an entry made to the Global Least Cost Routing table, select the entry you want to change, and click the **Edit** button. Make your changes, and click **OK**.

When Information May Be Out of Sync

If a server is down for any length of time, such that changes may have been made in the VoIP domain and the server is now out of sync with the Master, you need to update the server manually. In the server's MaxAdministrator, select **VoIP** > **Multi-Site Domain Configuration**, and click the **Replicate from Domain** button. This brings the server up-to-date with the Master.

If the server is still not seeing all the information it should (this would be rare), click **VoIP** > **Refresh Enterprise Configuration**.

CHAPTER

28

System Report Management

This information has been removed from the MaxCS Administration Manual and moved into a separate document. You can find this document on the Altigen web site, at https://www.altigen.com/support/, on the MaxCS Manuals tab.

29

Microsoft Exchange Integration

This chapter provides step-by-step instructions for configuring Microsoft Exchange and MAX Communication Server (MaxCS) to work together.

Important Notes:

- Exchange Integration in MaxCS Release 8.5 is significantly different than in earlier releases. We recommend that you carefully review this information, especially if you are upgrading from an earlier release.
- Configuring Exchange Integration on networks that require **TLS 1.2 security** requires additional steps, including changes to the registry. Refer to the section *Configuration Steps for Environments That Require TLS 1.2*.

MaxCS supports the following versions of Exchange:

- Exchange 2010
- Exchange 2013 - requires Windows Server 2008 R2 or later
- Exchange 2016
- Exchange 2019
- Office 365 Exchange Online

Note that Office 365 Exchange Online supports only Synchronized mode. It does not support either Bridge mode or Native mode.

MaxCS Private Cloud supports Office 365 Exchange Online.

Exchange Integration Options

Three integration options are possible, and are covered in this chapter:

- **Synchronize with Exchange –** Synchronize voice messages between the Altigen voice mailbox and Exchange mailbox. Works with Exchange 2010, 2013, 2016, 2019, and Office 365 Exchange Online.
- **Bridged Access to Exchange** – An option is provided in the Altigen Voice Mail System menu to log in to the Exchange mailbox (option **7** in the main menu). To synchronize voice mail between the Altigen mail box and the Exchange server, check the **Enable Synchronization** check box. If you don't check this, voice mail is not synchronized between the two message stores.

  Bridged Access is not supported with Office 365 Exchange Online.

- **Native VM Integration with Exchange –** In this mode, Altigen voice mailboxes are replaced by Exchange mailboxes. Each user in MaxCS needs to have a mailbox in the Exchange server and each mailbox must be Unified Messaging (UM) enabled, or the user will not be able to receive any voice mail.

  Native VM Integration is not supported with Office 365 Exchange Online

You can choose any of these options while installing MaxCS, and later you can switch options from MaxAdministrator. When you switch options, service restart is required.

Note: If Exchange integration was used in the previous version of MaxCS server, you must uninstall the Outlook client before you install MaxCS 8.5.

Before You Begin

Make sure the following items are ready before Exchange integration is configured. Note that Altigen is not responsible for, and cannot support, installation of Microsoft Exchange Server.

- You must have an Altigen Exchange Integration license for each extension using Exchange integration
- You must have one Windows server for MaxCS, loaded with:
  - Windows Server or Windows 7
  - The MAX Communication Server ACM software
- You must have a second Windows server for Exchange, loaded with Exchange Server software. It should be installed on 64-bit system(s) with Windows 64-bit or above OS. Unified Messaging, Client Access, and Mailbox Server roles should be installed with Exchange Server. (Requirement does not apply to Exchange Online.)

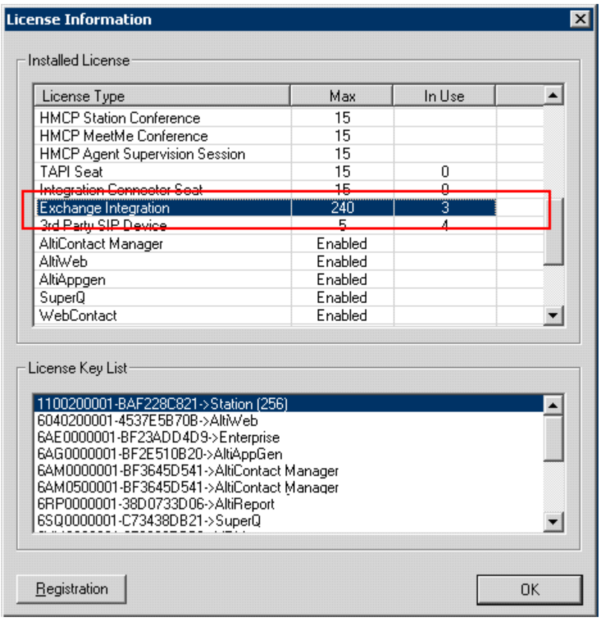
  Note: When you install both the Exchange Server and MAXCS, you must log in with an account with local administrator privileges. For Exchange Integration deployment, you should have Exchange Admin privileges and Domain Admin privileges.

  The MaxCS system and the Exchange Server system must belong to the *same* domain, with a network throughput rate of no less than 100Mbps and without any Web proxies in between.
- Altigen Services must be installed and started with the user account <*Domainname.com*>\Altigen_<AltiServ*SystemName*> or <*AltiServSystemName*>@<*Domainname.com*>. Make sure that you include the *.com* or *.net* part of the domain name in the entry.
- Exchange Server Services must be started.
- You must be able to successfully ping from the Exchange Server to MaxCS 8.5, and vice versa. (For Exchange Online, the MaxCS server must be able to connect with the Exchange Online server.)

Exchange Integration Configuration Steps

This section describes how to configure integration with Exchange. The steps may vary, depending upon which version of Exchange you are configuring.

1. Add your *Exchange Integration* licenses to MaxCS (see Figure 222).

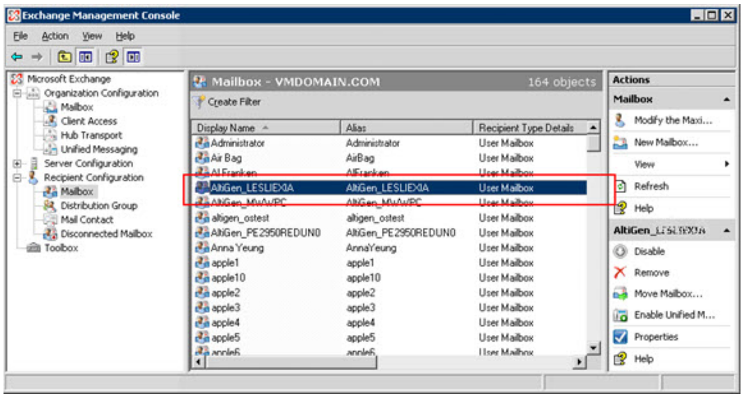


License Type	Max	In Use
HMCP Station Conference	15	
HMCP MeetMe Conference	15	
HMCP Agent Supervision Session	15	
TAPI Seat	15	0
Integration Connector Seat	15	0
Exchange Integration	240	3
3rd Party SIP Device	5	4
AltiContact Manager	Enabled	
AltiWeb	Enabled	
AltiAppgen	Enabled	
SuperQ	Enabled	
WebContact	Enabled	

```
1100200001-BAF228C821->Station (256)
6040200001-4537E5B70B->AltiWeb
6AE0000001-BF23ADD4D9->Enterprise
6AG0000001-BF2E510B20->AltiAppGen
6AM0000001-BF3645D541->AltiContact Manager
6AM0500001-BF3645D541->AltiContact Manager
6RP0000001-38D0733D06->AltiReport
6SQ0000001-C73438DB21->SuperQ
```

Figure 222. Adding Exchange Integration licenses in MaxCS

2. In the Exchange Management Console, create a mailbox for the service account that was created during installation. This account will be used for the integration service.



Display Name	Alias	Recipient Type Details
Administrator	Administrator	User Mailbox
Air Bag	AirBag	User Mailbox
Al Franken	AlFranken	User Mailbox
AltiGen_LESLIEXIA	AltiGen_LESLIEXIA	User Mailbox
AltiGen_MWVPC	AltiGen_MWVPC	User Mailbox
altigen_ostest	altigen_ostest	User Mailbox
AltiGen_PE2950REDUN0	AltiGen_PE2950REDUN0	User Mailbox
Anna Yeung	AnnaYeung	User Mailbox
apple1	apple1	User Mailbox
apple10	apple10	User Mailbox
apple2	apple2	User Mailbox
apple3	apple3	User Mailbox
apple4	apple4	User Mailbox
apple5	apple5	User Mailbox
apple6	apple6	User Mailbox

Figure 223. Creating a mailbox for the service account

(To do this in Exchange 2013 or 2016, choose **recipients** > **mailboxes**; click the **Plus** sign and choose **user mailbox**.)

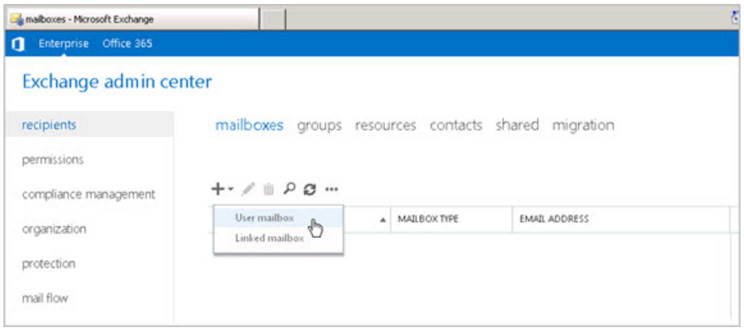
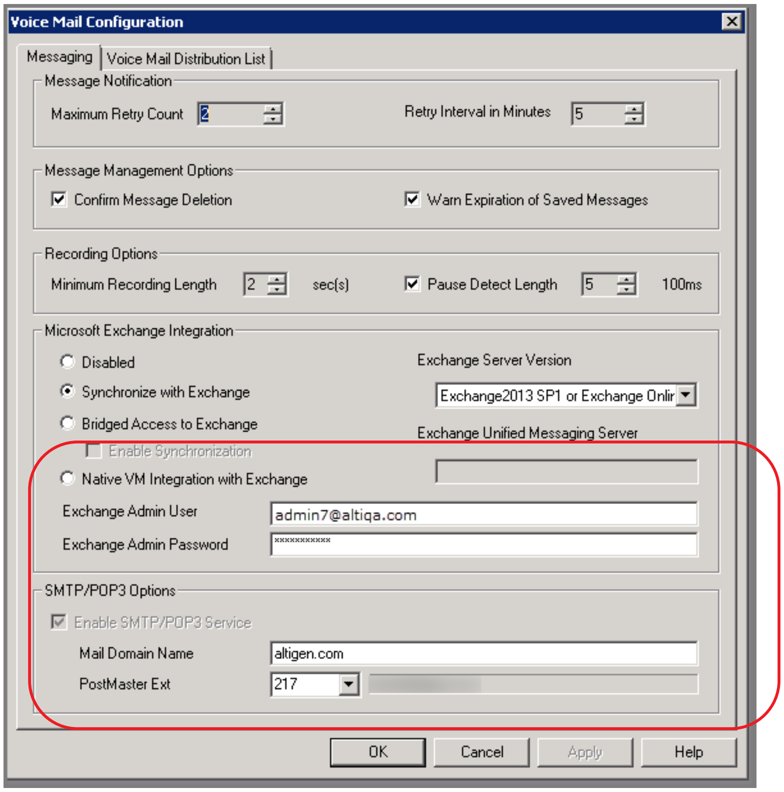


Figure 224. Creating a mailbox in Exchange 2013

3. In MaxAdministrator, choose **System** > **Voice Mail Configuration**.

   Select the Exchange Integration mode you want to use, the exchange server version, and enter the Admin User name and password.



Message Notification

Maximum Retry Count: 2

Retry Interval in Minutes: 5

Message Management Options

☑ Confirm Message Deletion

☑ Warn Expiration of Saved Messages

Recording Options

Minimum Recording Length: 2 sec(s)

☑ Pause Detect Length: 5 100ms

Microsoft Exchange Integration

○ Disabled

● Synchronize with Exchange

○ Bridged Access to Exchange

☐ Enable Synchronization

○ Native VM Integration with Exchange

Exchange Server Version: Exchange2013 SP1 or Exchange Onlir

Exchange Unified Messaging Server:

Exchange Admin User: admin7@altiqa.com

Exchange Admin Password: ***********

SMTP/POP3 Options

☑ Enable SMTP/POP3 Service

Mail Domain Name: altigen.com

PostMaster Ext: 217

Select the Exchange Integration mode you are going to use.

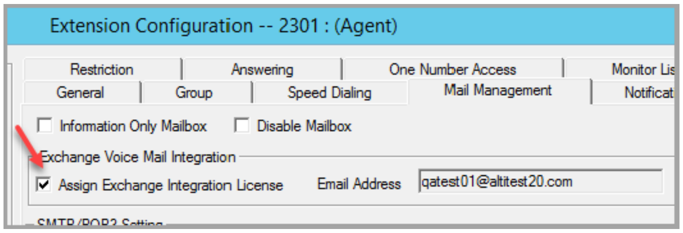
Figure 225. Choosing the **Synchronize** Exchange Integration mode in MaxCS

4. Configure the names of each extension user such that the first and last names are the same as the user’s matching mailbox on the Exchange Server. MaxCS matches the email address.

   Note: Exchange Native VM integration uses the extension number and the extension’s first and last names to link between MaxCS and Exchange.

5. In order to synchronize voicemail in *Bridged Access to Exchange* mode, check the **Enable Synchronization** box below that option.

6. For each user whose voice mail messages will be integrated with Exchange, open the extension's **Mail Management** tab and check the **Assign Exchange Integration License** option.



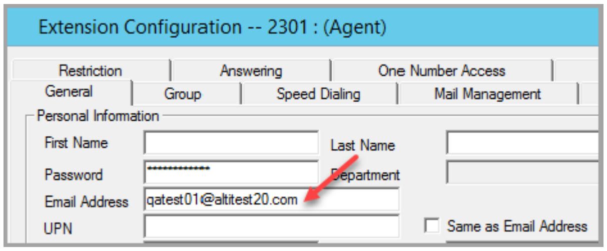
☐ Information Only Mailbox ☐ Disable Mailbox

Exchange Voice Mail Integration

☑ Assign Exchange Integration License Email Address qatest01@altitest20.com

SMTP/POP3 Setting

7. Then switch to the **General** tab and enter the user's email address. Beginning in Release 9.0.1, the Email Address field on the Mail Management tab became read-only.



Personal Information

First Name

Last Name

Password ************

Department

Email Address qatest01@altitest20.com

UPN

☐ Same as Email Address

Figure 226. Assigning the Exchange Integration license to a user

Note: Each user needs to access their mailbox once via an e-mail client (Outlook, Outlook Express, Outlook Web Access) before synchronization will start working for that user. A unique e-mail address is required for each user.

This is all you need to do if you selected the **Synchronize with Exchange** option in the Voice Mail Configuration Screen.

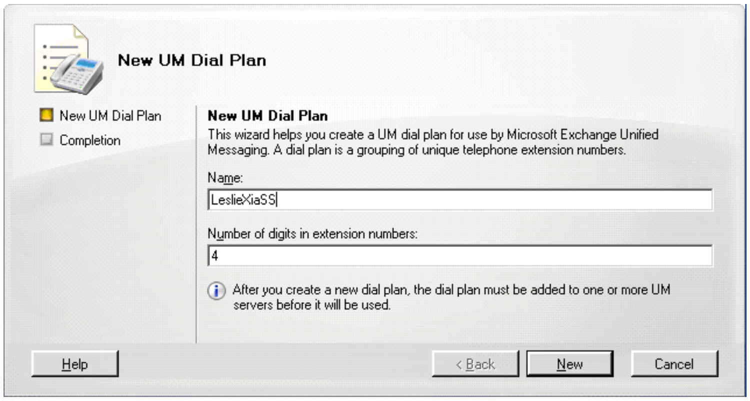
Configuring Bridged Access and Native VM Integration with Exchange

Note that the *Bridged Access to Exchange* and the *Native VM Integration with Exchange* options are not supported for Office 365 Exchange Online.

In addition to the steps given thus far in this chapter, follow these additional steps for *Bridged Access to Exchange* and *Native VM Integration with Exchange* options. As with the earlier section, these steps will vary from one version of Exchange to another.

1. Create a new dial plan.

   To do this in Exchange Management Console for 2010, go to **Organization Configuration > Unified Messaging**, and click **New UM Dial Plan**.



New UM Dial Plan

☐ New UM Dial Plan
☐ Completion

New UM Dial Plan

This wizard helps you create a UM dial plan for use by Microsoft Exchange Unified Messaging. A dial plan is a grouping of unique telephone extension numbers.

Name: LeslieXiaSS

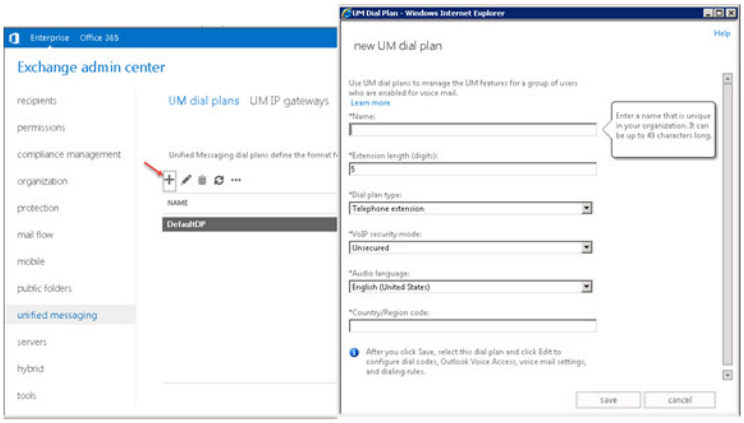
Number of digits in extension numbers: 4

After you create a new dial plan, the dial plan must be added to one or more UM servers before it will be used.

The digit length you enter must match the digit length of extensions in MaxCS

Figure 227. Creating a new UM dial plan in Exchange 2010

(In Exchange 2013 or 2016, select **unified messaging** > **UM dial plans** and click the Plus sign.)



Unified Messaging dial plans define the format f

NAME
DefaultDP

new UM dial plan

Use UM dial plans to manage the UM features for a group of users who are enabled for voice mail.
Learn more

*Name:

Enter a name that is unique in your organization. It can be up to 49 characters long.

*Extension length (digits): 5

*Dial plan type: Telephone extension

*VoIP security mode: Unsecured

*Audio language: English (United States)

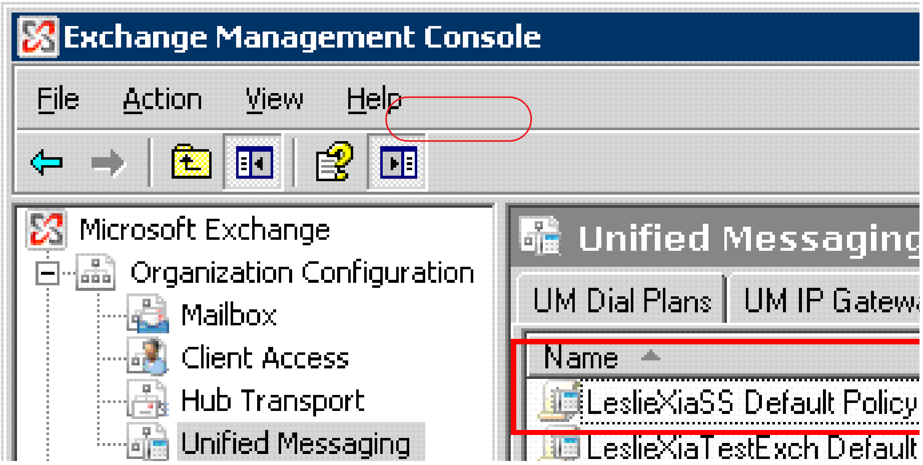
*Country/Region code:

After you click Save, select this dial plan and click Edit to configure dial codes, Outlook Voice Access, voice mail settings, and dialing rules.

Figure 228. Creating a new UM dial plan in Exchange 2013

2. Enter a name for the dial plan, specify the length of the extension numbers, and enter a country or region code. The extension length must be the same as the extension number length in MaxCS.

   A default UM Mailbox Policy is created automatically and is associated with the dial plan.

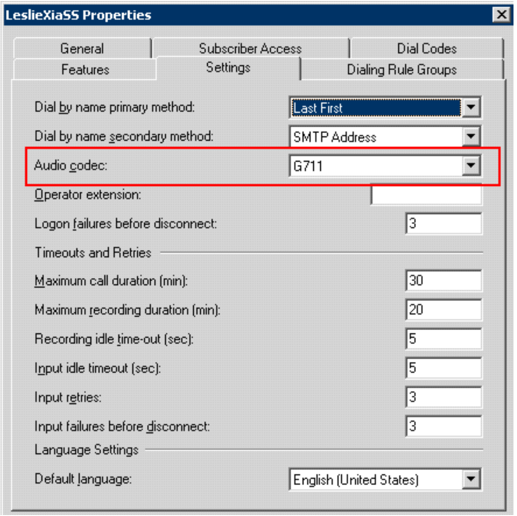


Name ▲
LeslieXiaSS Default Policy
LeslieXiaTestExch Default

Figure 229. A Default UM Mailbox Policy is created when you create a new dial plan

3. Change the codec for the new dial plan to G.711.

   To do this In Exchange 2010, open the dial plan’s Properties dialog box, select the **Settings** tab, and change **Audio Codec** to G.711.



LeslieXiaSS Properties

Dial by name primary method: Last First

Dial by name secondary method: SMTP Address

Audio codec: G711

Operator extension:

Logon failures before disconnect: 3

Timeouts and Retries

Maximum call duration (min): 30

Maximum recording duration (min): 20

Recording idle time-out (sec): 5

Input idle timeout (sec): 5

Input retries: 3

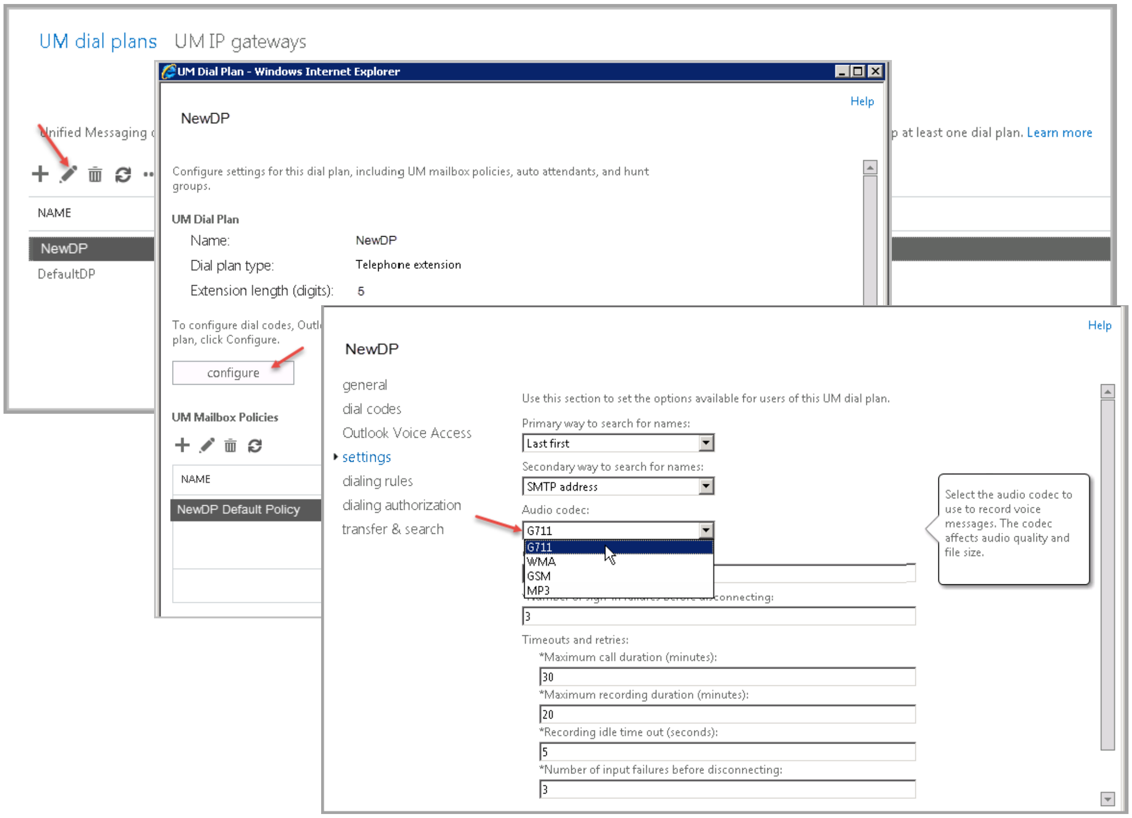
Input failures before disconnect: 3

Language Settings

Default language: English (United States)

Figure 230.   Changing the Dial Plan’s Audio Codec to G711 in Exchange 2010

To do this in Exchange 2013/2016, select the dial plan and click the Pencil icon to edit it. Then click **configure**, select **settings** (on the left) and choose **G.711 f**or the Audio codec option. Save your work and close the window.



UM dial plans UM IP gateways

Unified Messaging ... p at least one dial plan. Learn more

NAME

NewDP

DefaultDP

UM Dial Plan - Windows Internet Explorer

Help

NewDP

Configure settings for this dial plan, including UM mailbox policies, auto attendants, and hunt groups.

UM Dial Plan

Name: NewDP

Dial plan type: Telephone extension

Extension length (digits): 5

To configure dial codes, Outl... plan, click Configure.

configure

UM Mailbox Policies

NAME

NewDP Default Policy

Help

NewDP

Use this section to set the options available for users of this UM dial plan.

Primary way to search for names: Last first

Secondary way to search for names: SMTP address

Audio codec: G711

Select the audio codec to use to record voice messages. The codec affects audio quality and file size.

...connecting: 3

Timeouts and retries:

*Maximum call duration (minutes): 30

*Maximum recording duration (minutes): 20

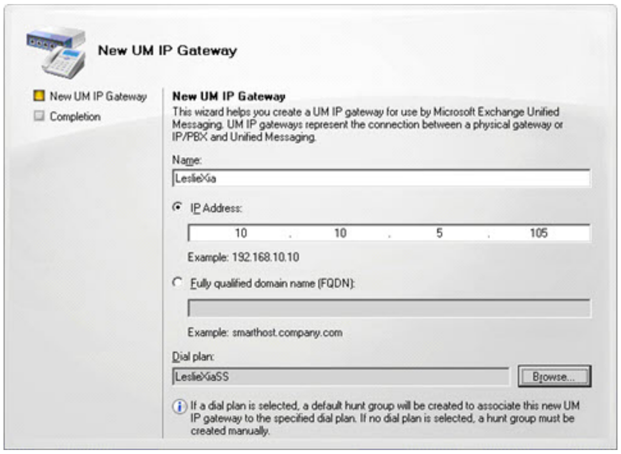
*Recording idle time out (seconds): 5

*Number of input failures before disconnecting: 3

Figure 231.   Changing the Dial Plan’s Audio Codec to G711 in Exchange 2013

4. Add your MaxCS server as a UM Gateway.

   To do this in Exchange 2010, select **Organization Configuration** > **Unified Messaging** > **UM IP Gateways** > **New UM IP Gateway**. Enter the name of the gateway and the IP address of your MaxCS server. Browse for and select the dial plan you just created. and click **New**.



New UM IP Gateway

New UM IP Gateway

This wizard helps you create a UM IP gateway for use by Microsoft Exchange Unified Messaging. UM IP gateways represent the connection between a physical gateway or IP/PBX and Unified Messaging.

Name: LeslieXia

● IP Address: 10 . 10 . 5 . 105

Example: 192.168.10.10

○ Fully qualified domain name (FQDN):

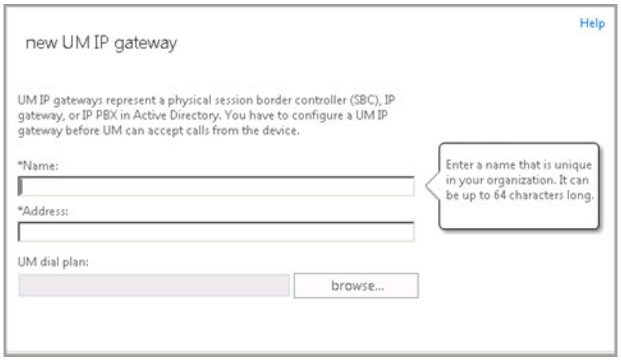
Example: smarthost.company.com

Dial plan: LeslieXiaSS Browse...

If a dial plan is selected, a default hunt group will be created to associate this new UM IP gateway to the specified dial plan. If no dial plan is selected, a hunt group must be created manually.

Figure 232.   Add the MaxCS server as a gateway, in Exchange 2010

To do this in Exchange 2013/2016, select **unified messaging** > **UM IP gateways**, click the Plus sign, enter the name of the gateway, the IP address of the MaxCS server, and browse to the dial plan that you just created.



new UM IP gateway

UM IP gateways represent a physical session border controller (SBC), IP gateway, or IP PBX in Active Directory. You have to configure a UM IP gateway before UM can accept calls from the device.

Enter a name that is unique in your organization. It can be up to 64 characters long.

Figure 233. *Add the MaxCS server as a gateway, in Exchange 2013*

5. If your system has multiple gateways, repeat step 4 to add each gateway as a UM gateway.
6. Associate your dial plan to the Exchange Server UM.

   To do this in Exchange 2010, go to **Server Configuration** > **Unified Messaging**, select the server and click **Properties**. Click the **UM Settings** tab, click **Add**, and add your dial plan to the list of associated dial plans.

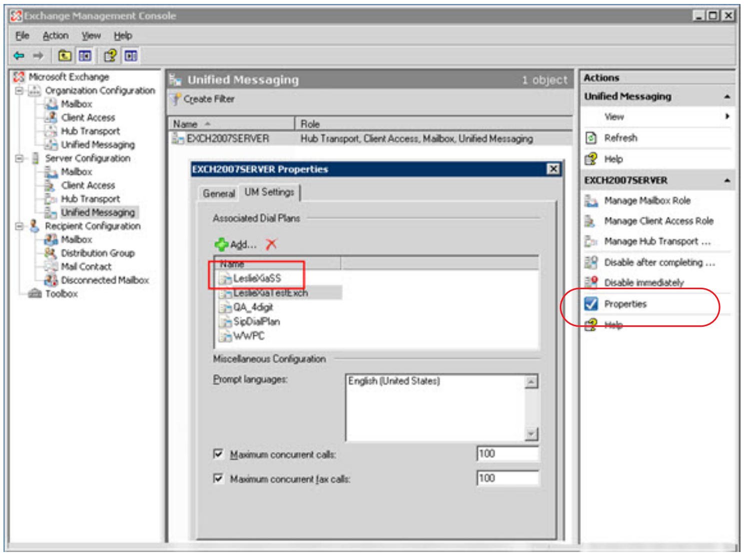
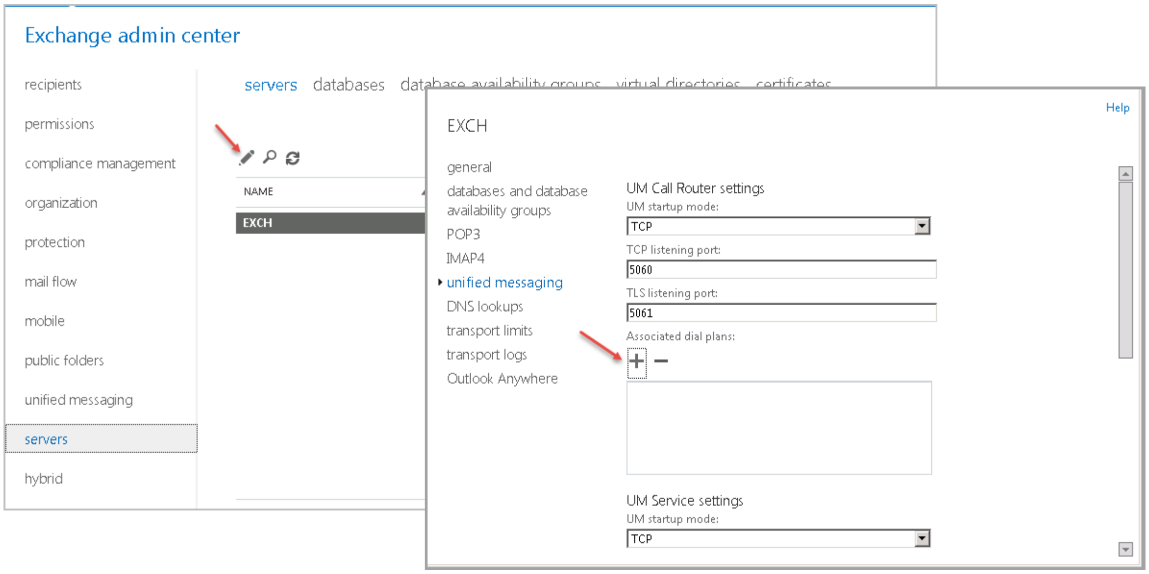


Figure 234. *Add the new dial plan to the list of associated dial plans*

To do this in Exchange 2013/2016, select **server** > **servers**, select the name of the Exchange server and click the Pencil icon. Select **unified messaging** on the left**.** Below *Associated dial plans*, click the Plus sign. Select the new dial plan and click **add**. Click **OK**.



UM Call Router settings

UM startup mode: TCP

TCP listening port: 5060

TLS listening port: 5061

Associated dial plans:

UM Service settings

UM startup mode: TCP

This completes all system-wide settings in Exchange Server.

Configuring UM Settings for Each User

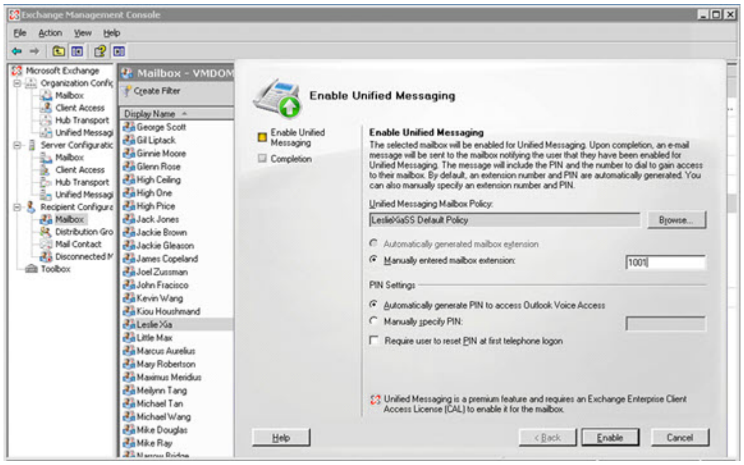
With all system-wide settings in Exchange Server complete, configure the UM settings for each user.

- *Configure User UM Settings in Exchange 2010* on page 362
- *Configure User UM Settings in Exchange 2013/2016* on page 363

Configure User UM Settings in Exchange 2010

To do this in Exchange 2010:

1. In **Recipient Configuration > Mailbox**, select the user and select **Enable Unified Messaging** from the Actions pane.



Enable Unified Messaging

The selected mailbox will be enabled for Unified Messaging. Upon completion, an e-mail message will be sent to the mailbox notifying the user that they have been enabled for Unified Messaging. The message will include the PIN and the number to dial to gain access to their mailbox. By default, an extension number and PIN are automatically generated. You can also manually specify an extension number and PIN.

Unified Messaging Mailbox Policy: LeslieXiaSS Default Policy [Browse...]

○ Automatically generated mailbox extension

● Manually entered mailbox extension: 1001

PIN Settings

● Automatically generate PIN to access Outlook Voice Access

○ Manually specify PIN:

□ Require user to reset PIN at first telephone logon

Unified Messaging is a premium feature and requires an Exchange Enterprise Client Access License (CAL) to enable it for the mailbox.

Figure 235. Here, Leslie Xia is an individual IP phone user with a mailbox

2. Click **Browse**, select the policy associated with the dialing plan you created, then click **OK**.

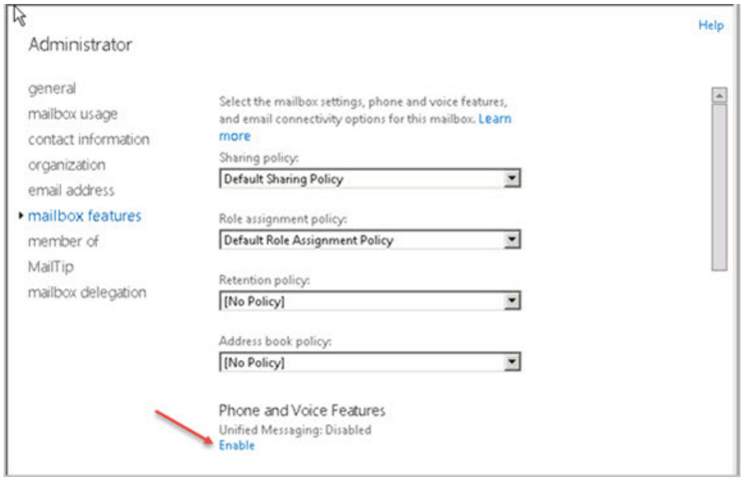
3. Enter the user’s MaxCS extension number in the **Manually entered mailbox extension** field (make sure the extension number is the same in MaxAdministrator and the Exchange User Mailbox).
4. Select PIN setting(s), and click **Next**. (If you select **Automatically Generate**, the Exchange Server will send the user an e-mail with the PIN.)
5. Click **Enable**.

Repeat steps 1-5 for each user you want to enable.

Configure User UM Settings in Exchange 2013/2016

To do this in Exchange 2013 or 2016,

1. Select **recipients** > **mailboxes**. Select the user and click the Pencil icon.
2. Select **mailbox features**. Below *Phone and Voice Features*, click **Enable**.



Administrator

Help

- general
- mailbox usage
- contact information
- organization
- email address
- mailbox features
- member of
- MailTip
- mailbox delegation

Select the mailbox settings, phone and voice features, and email connectivity options for this mailbox. Learn more

Sharing policy:
Default Sharing Policy

Role assignment policy:
Default Role Assignment Policy

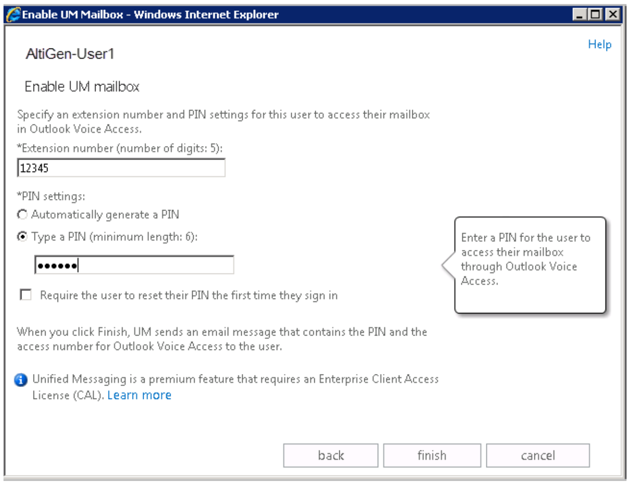
Retention policy:
[No Policy]

Address book policy:
[No Policy]

Phone and Voice Features
Unified Messaging: Disabled
Enable

Figure 236. Enable Unified Messaging

3. Browse to the policy associated with the dialing plan that you just created. Click **Ok**. Click **Next**.
4. Enter the extension number for the user to access the mailbox through Outlook Voice Access, and specify the PIN options. Click **Finish**.



Enable UM Mailbox - Windows Internet Explorer

AltiGen-User1

Help

Enable UM mailbox

Specify an extension number and PIN settings for this user to access their mailbox in Outlook Voice Access.

*Extension number (number of digits: 5):
12345

*PIN settings:
○ Automatically generate a PIN
● Type a PIN (minimum length: 6):
••••••

□ Require the user to reset their PIN the first time they sign in

Enter a PIN for the user to access their mailbox through Outlook Voice Access.

When you click Finish, UM sends an email message that contains the PIN and the access number for Outlook Voice Access to the user.

Unified Messaging is a premium feature that requires an Enterprise Client Access License (CAL). Learn more

Figure 237. Enter the extension number and PIN

Repeat these steps for each user.

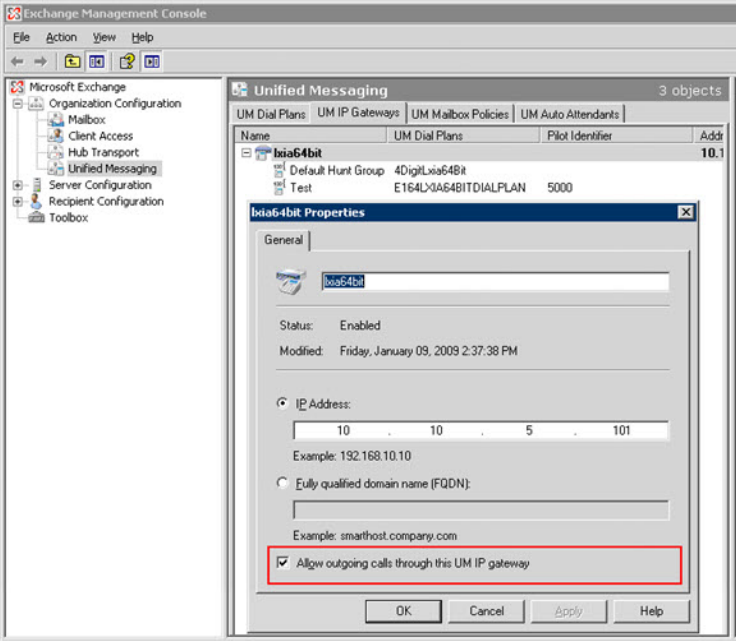
Configuring Out Calling from UM

This process enables extensions that are integrated with Exchange in *Native* or *Bridged* mode to call personal contacts or contacts from the database and to return calls from an Exchange voicemail message.

Configure Out Calling in Exchange 2010

To configure out call routing in Exchange 2010,

1. Open the Exchange Management console. Select **Unified Messaging** and switch to the *UM IP Gateways* tab.
2. Open the Properties panel and select the option **Allow outgoing calls through this UM IP gateway**.



Name	UM Dial Plans	Pilot Identifier	Addr
lxia64bit			**10.1**
Default Hunt Group	4DigitLxia64Bit		
Test	E164LXIA64BITDIALPLAN	5000	

lxia64bit

Status: Enabled

Modified: Friday, January 09, 2009 2:37:38 PM

● IP Address: 10 . 10 . 5 . 101

Example: 192.168.10.10

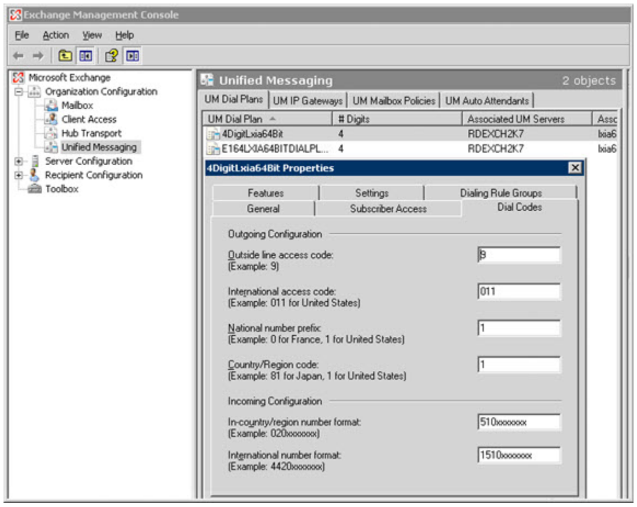
○ Fully qualified domain name (FQDN):

Example: smarthost.company.com

☑ Allow outgoing calls through this UM IP gateway

Figure 238. Allowing outgoing calls through the UM IP gateway in Exchange 2010

3. Set the Dial Code in your dial plan.



UM Dial Plan	# Digits	Associated UM Servers	Asso
4DigitLxia64Bit	4	RDEXCH2K7	lxia6
E164LXIA64BITDIALPL...	4	RDEXCH2K7	lxia6

Outgoing Configuration

Outside line access code: (Example: 9) 9

International access code: (Example: 011 for United States) 011

National number prefix: (Example: 0 for France, 1 for United States) 1

Country/Region code: (Example: 81 for Japan, 1 for United States) 1

Incoming Configuration

In-country/region number format: (Example: 020xxxxxxx) 510xxxxxxx

International number format: (Example: 4420xxxxxxx) 1510xxxxxxx

Figure 239. Setting the Dial Code in Exchange 2010

Outgoing Configuration

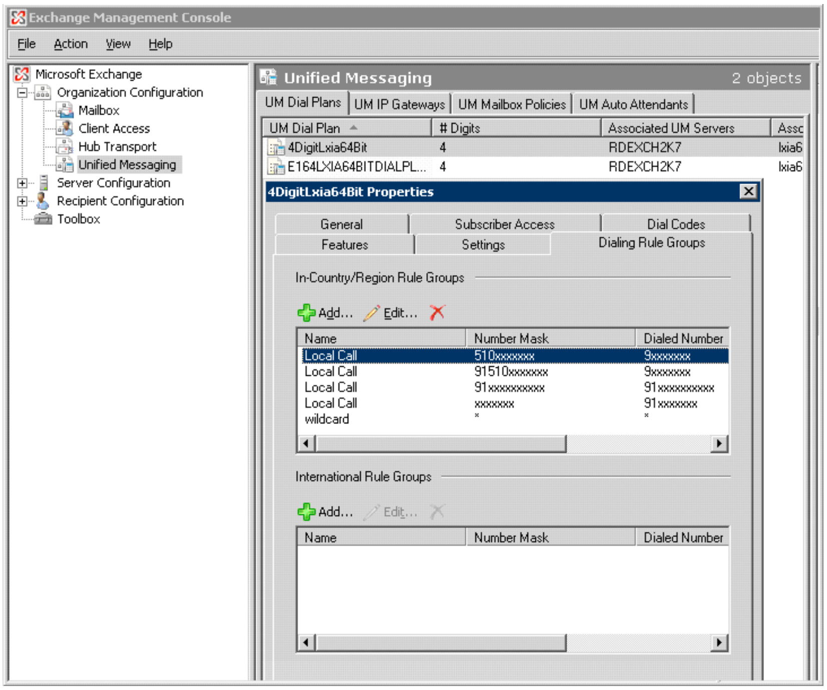
- **Outside line access code** – The trunk access code of your Softswitch
- **International access code** – Toll call prefix for international calls. For the U.S., it is "011"
- **National number prefix** – Toll call prefix for domestic calls, always set as "1"
- **Country/Region code** – Country code. For the U.S., it is "1"

Incoming Configuration

- **In-country/region number format**
  - Use this field to specify how a user's telephone number should be dialed by the UM Server in a different dial plan, but having the same country code. This is used by an auto attendant and when an Outlook Voice Access subscriber searches and tries to call the user in the directory.
  - This entry consists of a number prefix and n number of x characters (for example, 020xxxxxxx).
  - To determine the telephone number, UM will append the last n-digits from the telephone number that is specified in the directory to the prefix that is specified.
- **International number format**
  - Use this field to specify how a user's telephone number should be dialed by the UM Server in a different dial plan, and having a different country code. This is used by an auto attendant and when an Outlook Voice Access subscriber searches and tries to call the user in the directory.
  - This entry consists of a number prefix and n number of x characters (for example, 4420xxxxxxx).
  - To determine the telephone number, UM will append the last n-digits from the telephone number that is specified in the directory to the prefix that is specified.

4. Switch to the *Dialing Rule Groups* tab. Add dial rules for in-country/region and international calls that will be placed by UM-enabled users.

   Each dialing rule entry that is defined on the dial rule group determines the types of calls that users within a specific dial rule group can make.



Exchange Management Console

File Action View Help

- Microsoft Exchange
  - Organization Configuration
    - Mailbox
    - Client Access
    - Hub Transport
    - Unified Messaging
  - Server Configuration
  - Recipient Configuration
  - Toolbox

Unified Messaging — 2 objects

UM Dial Plans | UM IP Gateways | UM Mailbox Policies | UM Auto Attendants

UM Dial Plan	# Digits	Associated UM Servers	Assc
4DigitLxia64Bit	4	RDEXCH2K7	lxia6
E164LXIA64BITDIALPL...	4	RDEXCH2K7	lxia6

4DigitLxia64Bit Properties

General | Subscriber Access | Dial Codes | Features | Settings | Dialing Rule Groups

In-Country/Region Rule Groups

Add... Edit...

Name	Number Mask	Dialed Number
Local Call	510xxxxxxx	9xxxxxxx
Local Call	91510xxxxxxx	9xxxxxxx
Local Call	91xxxxxxxxxx	91xxxxxxxxxx
Local Call	xxxxxxx	91xxxxxxx
wildcard	*	*

International Rule Groups

Add... Edit...

Name	Number Mask	Dialed Number

Figure 240. Adding Dial Rule entries in the Dialing Rule Groups tab

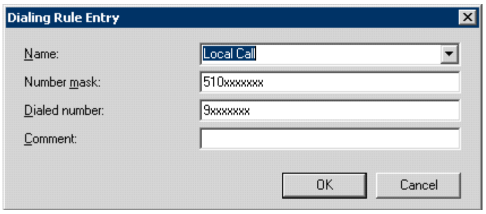
For a Dialing Rule Entry (see Figure 240), the following are required:

Name – Select a name of an existing dialing rule or, if you want to create a dialing rule, type the name of the dialing rule (up to 32 characters, text characters only). This is the display name for the dialing rule that will be displayed in the Exchange Management Console.

Number Mask – Define the number mask for the dialing rule. A number mask is used to define the telephone number format that a Unified Messaging server will use to determine what outgoing telephone number it will dial for a user. When an outgoing call is made to a number that is matched by the number mask on the dialing rule, the UM server will substitute the digits that are matched into the dialed number. It will then use the digit string from this match to make the outgoing call. An example of a valid number mask is 91425xxxxxxx. This field can contain only numbers and the letter 'x'.

Dialed Number – Define the dialed number for the dialing rule. The dialed number is used to determine the actual dial string that is sent to the IP gateway. This number can be different from the number that is obtained by Unified Messaging for the outgoing call. However, your PBX can also be configured to omit the area code for local calls and can be configured for private voice numbering plans. Any wildcard (x) characters in the dial string are substituted with the digits from the original number that were matched by the number mask on the dialing rule. An example valid dialed number is 9xxxxxxx. This field can contain only numbers and the character "x".

Comment – Use this text box to input a comment or description for the dialing rule that you are adding.



Dialing Rule Entry

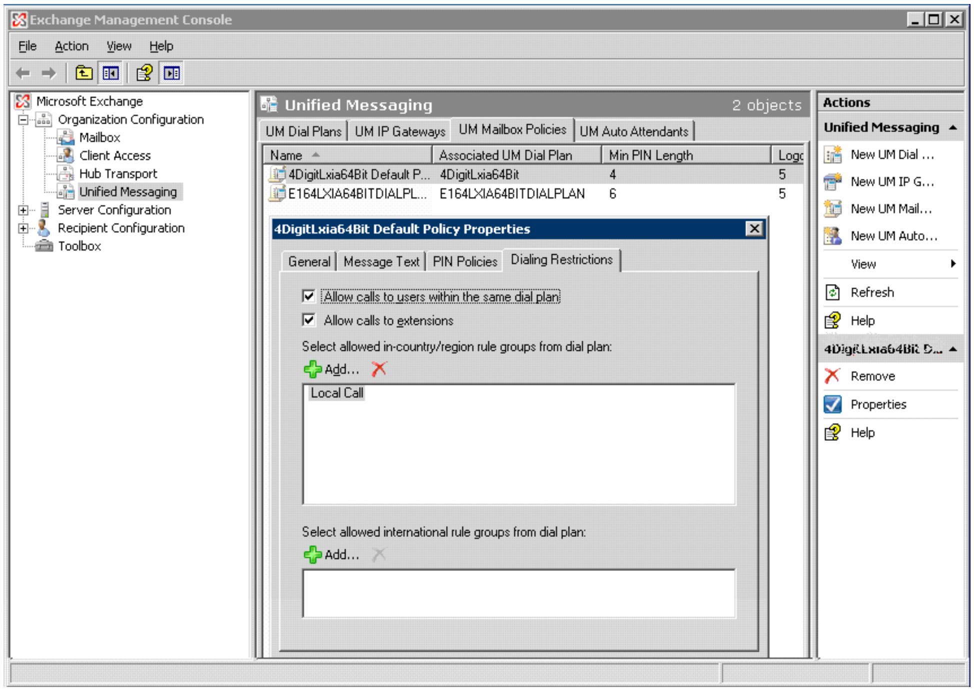
Name:	Local Call
Number mask:	510xxxxxxx
Dialed number:	9xxxxxxx
Comment:	

Figure 241. Creating a dialing rule

For example, if the business number of a personal contact is 5102529712, then the number mask should be set as "91510xxxxxxx", because UM will add "91" automatically, and the Dialed Number is "9xxxxxxx", so that the final dialed number will be "92529712".

You can use the wild card "*" to handle any length of digits.

5. Assign the Dial Entry to mailbox Policies: Go to UM Mailbox Policies, select the mailbox that users belong to, open the Dialing Restrictions tab, and assign the rule group you just created.



Name	Associated UM Dial Plan	Min PIN Length	Logo
4DigitLxia64Bit Default P...	4DigitLxia64Bit	4	5
E164LXIA64BITDIALPL...	E164LXIA64BITDIALPLAN	6	5

4DigitLxia64Bit Default Policy Properties

General | Message Text | PIN Policies | Dialing Restrictions

☑ Allow calls to users within the same dial plan

☑ Allow calls to extensions

Select allowed in-country/region rule groups from dial plan:

Add...

Local Call

Select allowed international rule groups from dial plan:

Add...

Figure 242. Assigning dial plan to mailbox policy

After you configure the UM mailbox to use a dialing rule group, the dialing restrictions that are configured apply to all UM-enabled users who are associated with the UM mailbox policy. For example, you can configure a dialing rule group that does not require users who are associated with the dial plan to dial an outside line access code when they place a call to an in-country/region telephone number.

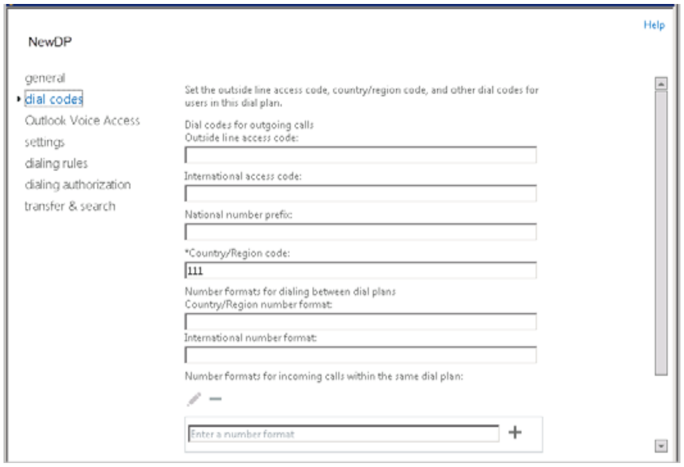
Note: If you need help in configuring dialing rules, see http://technet.microsoft.com/en-us/library/bb629580.aspx. That will put you in the general location of what you need. Much of this information came from that Microsoft site.

6. Next, complete the steps in the section *Configuring MaxAdministrator* on page 368.

Configure Out Calling in Exchange 2013/2016

To configure out call routing in Exchange 2013 or 2016,

1. Open the Exchange Management console.
2. Select **unified messaging** > **UM IP gateways**.
3. Select the gateway. Click the Pencil icon.
4. Select the option **Allow outgoing calls through this UM IP gateway**.
5. Select **unified messaging** > **UM dial plans**. Click the dial plan and click the Pencil icon.
6. Click **configure**. Select **dial codes** (on the left).



Set the outside line access code, country/region code, and other dial codes for users in this dial plan.

Dial codes for outgoing calls

Outside line access code:

International access code:

National number prefix:

*Country/Region code: 111

Number formats for dialing between dial plans

Country/Region number format:

International number format:

Number formats for incoming calls within the same dial plan:

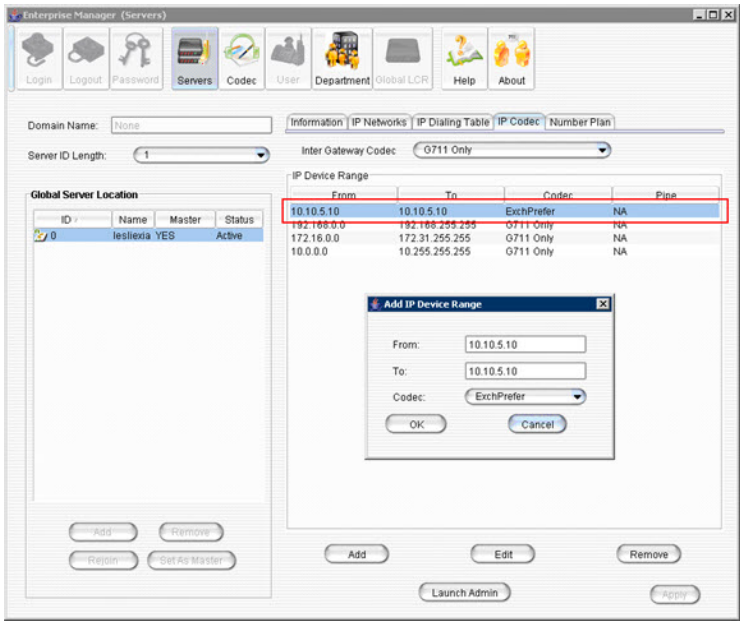
Figure 243. Open the Dial Codes panel

7. Refer to the section *Configure Out Calling in Exchange 2010* on page 364 to specify dial code options. Create rules for in-country/region and international calls that will be placed by your UM-enabled users.
8. Complete the steps in the next section, *Configuring MaxAdministrator*.

Configuring MaxAdministrator

Complete the configuration in MaxAdministrator.

1. Go to **System** > **System Configuration** > **Number Plan** tab. In the First Digit Assignment panel, assign one of the digits (for example, digit 8) to IP Trunk Access.
2. Go to the Trunk Configuration screen, and assign the digit selected in step 1 to all the SIP-Tie entries. (Click the first SIP-Tie entry, and assign the digit, then use the **Apply** button to apply the assignment to all the other SIP-Tie entries.) This allows calls in either bridged or native mode to access the Exchange Server.
3. Go to **VoIP** > **Enterprise Network Management** to open Enterprise Manager.
4. Click **Codec** to create a new codec profile only for the Exchange connection.
    a. In the **Name** field, enter a name for the new codec profile.
    b. In the **Codec** field, select **G.711 Mu-Law**.
    c. In the **DTMF Delivery** field, select **RFC2833**
    d. In the **SIP Early Media** field, select **Enable**.
    e. In the **SIP Transport** field, select **TCP**.
5. Associate this new codec profile to the IP address of Exchange Server (and *only* Exchange Server):
    a. Click the **Servers** button, then click the **IP Codec** tab.
    b. Add a new IP Device Range for the Exchange Server:



Domain Name: None

Server ID Length: 1

Global Server Location

ID	Name	Master	Status
0	lesliexia	YES	Active

Inter Gateway Codec: G711 Only

IP Device Range

From	To	Codec	Pipe
10.10.5.10	10.10.5.10	ExchPrefer	NA
192.168.0.0	192.168.255.255	G711 Only	NA
172.16.0.0	172.31.255.255	G711 Only	NA
10.0.0.0	10.255.255.255	G711 Only	NA

From: 10.10.5.10

To: 10.10.5.10

Codec: ExchPrefer

Figure 244. Associating your “Exchange” codec profile to the IP address of Exchange Server

6. Click the **Add** button in the IP Device Range panel.
7. Select the codec profile you just created specifically for Exchange.
8. Enter the IP address of the Exchange Server in both the **From** and **To** fields. Be sure that this IP address does not fall into any other device range. (Check the **IP Codec** tab and the **IP Dialing Table** tab.) If it does, reset that range into two ranges: one that ends just before the Exchange Server’s IP address, and one that starts just after the Exchange Server’s IP address.
9. In MaxAdministrator, go to **System** > **Voice Mail Configuration**. In the Microsoft Exchange Integration panel, select **Bridged Access to Exchange** or **Native VM Integration with Exchange**. Click **OK**.
10. Restart all Altigen services.

Note: After all Altigen services are restarted, voice mail access may be unavailable for 1-2 minutes.

Configuring Exchange Online Impersonation

For full discussions on situations where you may want to configure Application Impersonation, read the following Microsoft articles:

- https://msdn.microsoft.com/en-us/library/office/dn722377(v=exchg.150).aspx
- https://msdn.microsoft.com/en-us/library/office/dn722376(v=exchg.150).aspx

1. Set the Exchange administrator as MaxCS Exchange Integration service admin.

   a. Log into the Exchange portal as the Exchange administrator. Click **permissions** on the left.

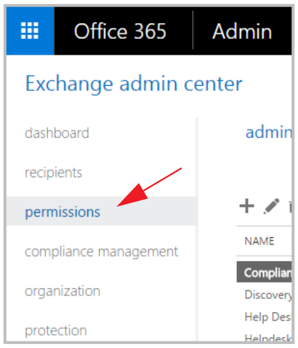
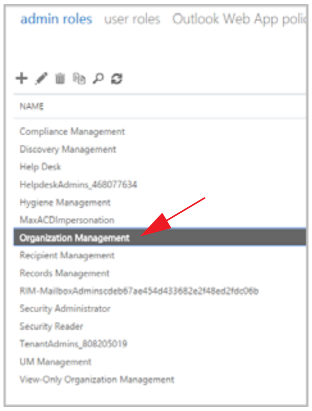


Figure 245. Click “permissions” in the left panel in the Exchange portal

   b. In the middle panel, click the **admin role** tab, select **Organization Management** and then click the Pencil icon.

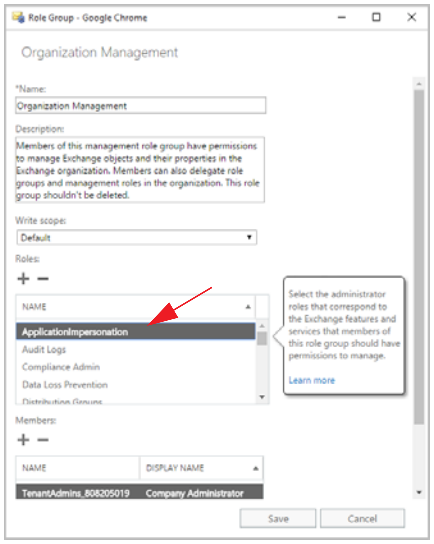


NAME
Compliance Management
Discovery Management
Help Desk
HelpdeskAdmins_468077634
Hygiene Management
MaxACDImpersonation
Organization Management
Recipient Management
Records Management
RIM-MailboxAdminscdeb67ae454d433682e2f48ed2fdc06b
Security Administrator
Security Reader
TenantAdmins_808205019
UM Management
View-Only Organization Management

Figure 246. Click “Organization Management”

   c. In the *Role Group* popup window, click the add button (the Plus sign) under *Roles*.

   d. In the *Select a Role* popup window, select **ApplicationImpersonation** and click the **add ->** button. Then click **OK** to return to the previous window.



Role Group - Google Chrome

Organization Management

*Name: Organization Management

Description: Members of this management role group have permissions to manage Exchange objects and their properties in the Exchange organization. Members can also delegate role groups and management roles in the organization. This role group shouldn't be deleted.

Write scope: Default

Roles:

NAME
ApplicationImpersonation
Audit Logs
Compliance Admin
Data Loss Prevention
Distribution Groups

Select the administrator roles that correspond to the Exchange features and services that members of this role group should have permissions to manage.

Learn more

Members:

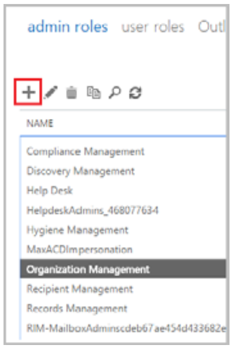
NAME	DISPLAY NAME
TenantAdmins_808205019	Company Administrator

e. In the *Role Group* window, you should see ApplicationImpersonation in the Roles list. Click **Save**.

2. Set another user as the MaxCS Exchange Integration service admin.

   a. Log into the Exchange portal as the Exchange administrator. Click **permissions** in the left panel.

   b. In the middle panel, click the *admin role* tab, click the **Add** (Plus sign) button to create a new role.

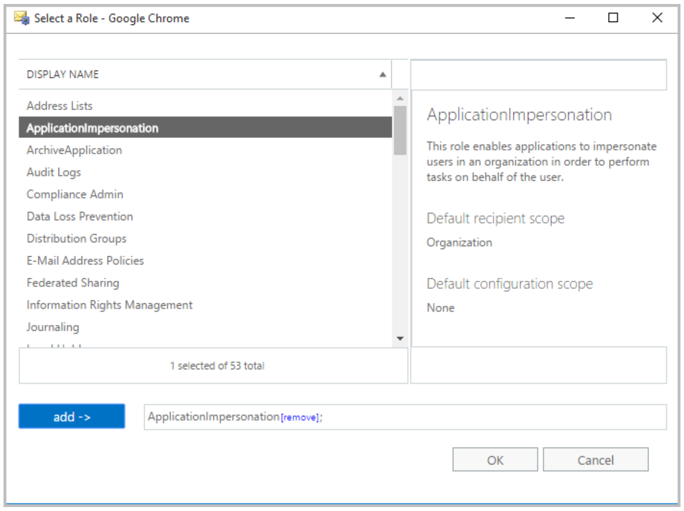


NAME
Compliance Management
Discovery Management
Help Desk
HelpdeskAdmins_468077634
Hygiene Management
MaxACDImpersonation
Organization Management
Recipient Management
Records Management
RIM-MailboxAdminscdeb67ae454d433682e

Figure 247. Click the Plus sign to add a new role

   c. In the *Role Group* window, provide a meaningful name and enter a brief description.

   d. In the same window, click the **Add** (Plus sign) button under *Roles* to add a new role. In the *Select a Role* popup window, select **ApplicationImpersonation** and click the **add ->** button. Click **OK** return to the previous window.



ApplicationImpersonation

This role enables applications to impersonate users in an organization in order to perform tasks on behalf of the user.

Default recipient scope

Organization

Default configuration scope

None

1 selected of 53 total

ApplicationImpersonation[remove];

Figure 248. Select “applicationimpersonation” and click “add”

e. In the *Role Group* window, click the **Add** (Plus sign) button under *Members*. In the *Select Members* window, select the user you want to use as the MaxCS Exchange Integration Service administrator and click the **add ->** button. Click **OK** to return to the previous window.

f. Make sure that **ApplicationImpersonation** appears on the roles list, and confirm that the MaxCS Exchange Integration administrator is in the members list. Click **Save**.

When You Create New Mailbox Users

If you are using Synchronize mode, Bridged Access mode with synchronization, or Native VM Integration mode, and you create a new mailbox user in Exchange Server and a new extension in MaxCS, in order to associate them, you must restart the Altigen Exchange Integration Service.

Testing for Synchronization

You can use some simple procedures to make sure that the **Synchronize with Exchange** integration is working correctly.

To test the integration, set up an extension in MaxCS (for example, extension 100) and its corresponding mailbox in Exchange Server. Also, set up a computer with Outlook configured for this user.

Test Message Delivery to Exchange

1. Leave a voice mail for extension 100. The message light illuminates.
2. Log on to the Exchange Mailbox from Outlook and check for the message in the inbox. The message should be titled **Voice-mail from *xxx*** and include the voice mail as a `.wav` attachment.

Check Message State Change Notification

1. Log in to extension 100’s voice mail from a phone. The message you left in the preceding step should be there as a new message.
2. Save the message by pressing 3. Within approximately a minute, the message in Outlook will become a saved message as well – it will no longer appear in **bold**.

Listen to VM in Outlook

Open the message in Outlook, and open the `.wav` attachment. It should be the same message.

Check deletion notification

1. Delete this message from Outlook.
2. Wait a few minutes, and then log on to extension 100’s voice mail from a phone. The voice mail should no longer be there.

If any of these tests fail, consult the “Troubleshooting Tips” section.

Troubleshooting Tips

To check the profile for the service account

1. Log on to the MaxCS system as the *Altigen service account* (for example, **Altigen_telesystem**). You will need the password you set up when you installed MaxCS.
2. Select **Control Panel** > **Mail**. (In Windows, right-click **Microsoft Office** on the **Start** menu, and select **Properties**.)
3. Click **Show Profiles**. In MaxCS 8.5, there is only one profile there, which is for the service account, so that name should be AltiExch<*ServerName*><*AccountName*> (for example, AltiExchMAILSERVERAltigen_telesystem).

   If you don’t see any such profile, make sure that \altiserv\exe folder does not contain the files **`mapi32.dll`** or **`gapi32.dll`**. If these files exist, delete them, then stop and start the Exchange Integration Service.

To delete the profile for the service account

If an error occurred while MaxCS was creating the service account profile, the damaged profile would remain there until removed manually. After the re-configuration, the new profile can't be created, because the old one still exists.

You can remedy this in the following way:

1. Log on as Altigen Service Account.
2. Shut down Altigen Exchange Integration Service from **Control Panel** > **Administrative Tools** > **Services**, then open **Control Panel** > **Mail** (or **Mail and Fax**) and click **Show Profiles**. Remove the service profile.
3. Start the **Altigen Exchange Integration Service** from **Control Panel** > **Administrative Tools** > **Services**.

If this doesn’t work, contact Altigen Technical Support.

To gather trace files

1. Log in to Admin.
2. Select **Turn AltiTrace On**, and click **Apply**.
3. Select **VM and SP Log Dump**.
4. To view logs, go to AltiServ\Log\VM\ExchIntg.

To avoid “extension in use” message

When synchronizing with Exchange Server, the mailbox needs to be locked. If the extension has a lot of messages, it could take some time, but shouldn’t take as long as 2-3 minutes. In normal cases, it should take just 10-20 seconds. You may adjust a registry key to change the synchronization interval:

HKEY_LOCAL_MACHINE\SOFTWARE\Altigen Communications, Inc.\AltiWare\ExchIntg\Polling Interval

The value is in ms. 60000 = 60 seconds. You may change it to 300000 for 5 minutes. After changing the value, restart Exchange integration service for the change to take effect.

Exchange Integration service synchronizes voice messages on the Exchange server with those on the MaxCS system by polling the two servers periodically. This polling interval can be adjusted by creating a DWORD value called “Polling Interval” under the key

HKEY_LOCAL_MACHINE\SOFTWARE\AltiGen Communications, Inc.\AltiWare\ExchIntg

This DWORD value should contain the number of milliseconds between polling. If this value is not present in the registry, a default value of 60000 (1 minute) is used by the system. For performance reasons, you should not set this value to below 60000.

To avoid “Access Deny” errors while sending messages

If you have applied Microsoft patch ms06-029, when an Altigen PBX phone user attempts to send a message, the user receives an “Access Deny” error. This is because the patch changes the grant for the permission of **Send As**.

After applying the patch, the **Send As** permission of each user needs to be granted to the account of “altigen service” explicitly.

You may have to restart the Exchange Server and MaxCS.

Configuration Steps for Environments That Require TLS 1.2

If your Exchange server or network environment is upgraded to where your minimum security level requires TLS 1.2, your Exchange Integration configuration may fail.

One example of a change that would cause Exchange Integration to fail is if you reconfigured your service to route Exchange traffic through a network element such as an F5 load balancer. This configuration would restrict exchange traffic to TLS 1.2.

In such a case, you would notice the following errors in the *ExchIntLog* log file:

```
Connect to exchange server failed!
Cannot initialize EWS admin login
The Autodiscover service couldn't be located.
Exchange Integration Service is shutting down!
```

To account for this, you would need to change some registry entries on the MaxCS server.

1. Add (or modify) the following Registry keys to these values on the MaxCS server:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]

"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]

"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.2\Client]

"Enabled"=dword:00000001

2. After making these changes, reboot the server.
3. Check the status of the synchronization application.

Notes

- Prevent attempts by the Exchange Administrator/Manager to use the existing service account for the Altigen Exchange Integration Service. Using the Altigen service account will provide you an audit trail that is invaluable while troubleshooting.

- Depending on the number of voice mails you have on the Altigen server, the initial mailbox synchronization may take a long time.

  For example, if you have 10GB of voice mails on the Altigen server and are enabling Exchange integration for all the mailboxes, it may take up to 24 hours to initialize the Exchange integration service.

  On the other hand, if you have less than 100MB of voice mails on the Altigen server, the initialization will take less than 5 minutes.
- If users experience a problem making calls to the Exchange server, make sure the MSXML 6.0 Parser has not been deleted from the server. Without it, the speech engine services cannot play voice prompts.

CHAPTER

30

Fax-over-IP Configuration

This section describes how to configure MaxCS for Fax-over-IP (FoIP).

MaxCS supports FoIP, leveraging T-38 pass-through. (T.38 pass-through is only supported on Altigen SIP Trunks.)

Both voice calls and fax calls can be made through a FoIP extension; both incoming and outgoing calls on the extension will use G.711 codec.

Fax extension-to-extension is supported; the SIP endpoints must be a supported ATA device.

Limited FoIP extension parameters are supported:

- First/Last Name, Password, Description, Department
- DID Number, Transmitted Caller ID, E911 CID
- IP Extension parameters, except Enable Fallback to Mobile Extension
- Out Call Restrictions
- Forward All Calls - forwarding target must be an FoIP extension or FoIP hunt group
- Busy Call Handling - forwarding target must be an FoIP extension or FoIP hunt group

FoIP Limitations

Sending and receiving faxes over IP service has known limitations. Altigen, along with many other companies, uses the T.38 industry standard for FoIP configuration. The T.38 standard contains minor variations in how it can be implemented. Because of these variations, one provider's FoIP handling can vary from another's, thus introducing the possibility of incompatibilities. As the standard continues to evolve, it is reasonable to expect these variations to diminish over time.

If your organization typically sends frequent faxes that are lengthy multiple page documents, consider retaining a few analog lines and traditional fax machines as a backup option.

FoIP Requirements

In order to implement FoIP, your system must meet the following requirements:

- Your SIP Service provider must be Altigen.
- You FoIP gateway must be an Altigen-certified ATA device. Supported devices include various AudioCodes gateways; see the Altigen Knowledge Base (https://know.altigen.com/) for device configuration guides.

Overview

MaxCS supports T.38 pass-through, which is a protocol for real-time fax transmission over IP networks. There are three common scenarios for sending faxes to/from MaxCS.

One scenario is an On-premise installation of MaxCS with users sending faxes within the facility.

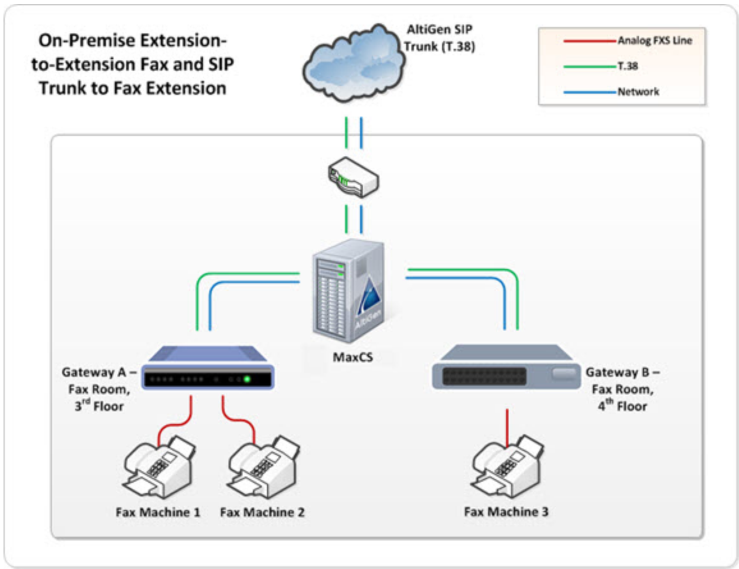

On-Premise Extension-to-Extension Fax and SIP Trunk to Fax Extension
AltiGen SIP Trunk (T.38)
Analog FXS Line
T.38
Network
MaxCS
Gateway A – Fax Room, 3rd Floor
Gateway B – Fax Room, 4th Floor
Fax Machine 1
Fax Machine 2
Fax Machine 3

Figure 249. Example of internal fax configuration in an on-premise MaxCS deployment

In this scenario, faxes are connected to VoIP gateways via analog FXS. The gateways all connect to MaxCS via network connections with T.38 pass-through.

Another scenario is an On-premise installation with users sending faxes to, and receiving faxes from, an external fax machine outside of the organization.

In this scenario, the faxes connect to the VoIP gateway, which connects to MaxCS. MaxCS connects to a router which sends faxes through (and receives faxes from) the cloud. The remote location will have a router receiving the fax, sending it to the VoIP gateway which is connected to the target fax machine.

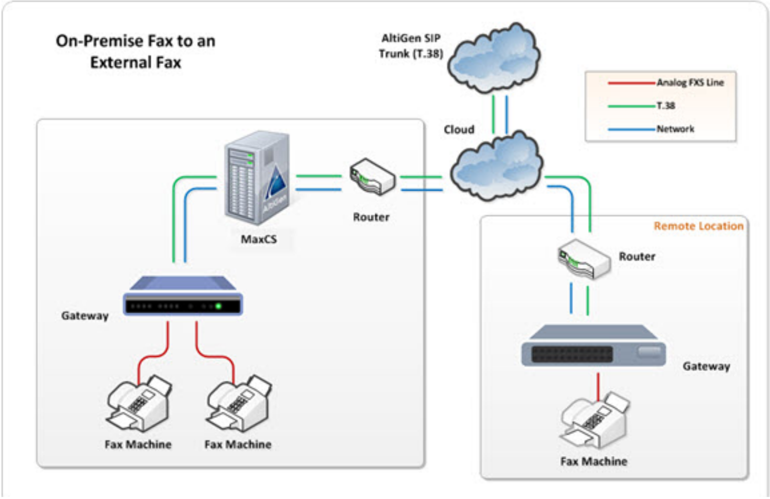


Figure 250. Example of sending faxes from internal fax devices to external fax machines

A third scenario illustrates fax flow with MaxCS Cloud deployments. The gateway connects to the cloud, connecting to MaxCS, and faxes are sent through to the router, gateway, and fax device at an external location.

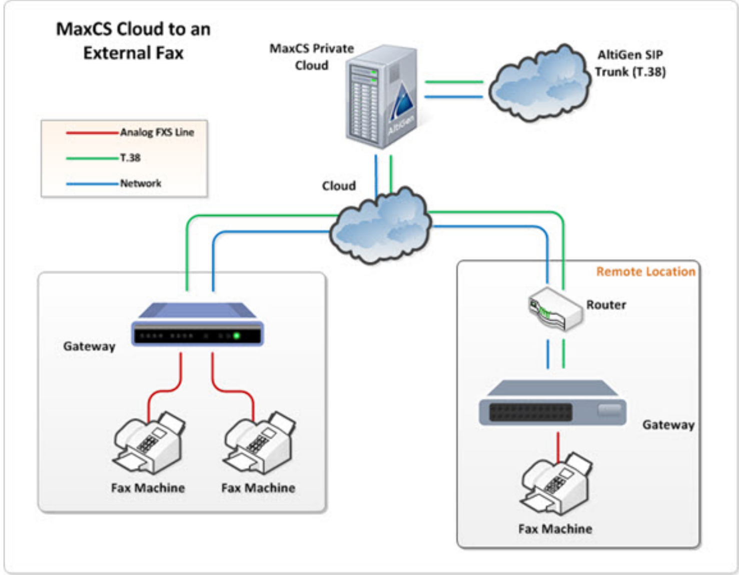
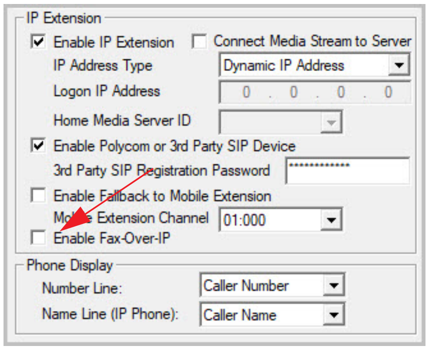


Figure 251. Example of sending and receiving faxes in a MaxCS Cloud deployment

Configure an IP Extension for FoIP

To configure an IP extension to support FoIP,

1. Select **PBX** > **Extension Configuration**.
2. Select the extension on the left.
3. On the right, in the IP Extension group, check **Enable Fax-Over-IP**.



IP Extension

☑ Enable IP Extension ☐ Connect Media Stream to Server

IP Address Type: Dynamic IP Address

Logon IP Address: 0 . 0 . 0 . 0

Home Media Server ID:

☑ Enable Polycom or 3rd Party SIP Device

3rd Party SIP Registration Password: ************

☐ Enable Fallback to Mobile Extension

Mobile Extension Channel: 01:000

☐ Enable Fax-Over-IP

Phone Display

Number Line: Caller Number

Name Line (IP Phone): Caller Name

Figure 252. Configuring Fax-over-IP for an IP extension

Enabling this setting changes the configuration for this extension as follows:

- All outbound calls from this IP extension will use the G.711 codec
- All incoming DID routing calls to this extension will use the G.711 codec

Configure In Call Routing for FoIP

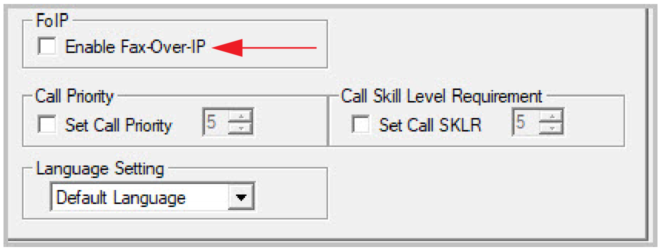
MaxCS supports support two different In Call routing methods for fax numbers:

- DNIS In Call Routing
- FoIP Extension DID number

Routing supports T.38 UDPTL (UDP packets) using the same RTP port range.

To enable FoIP DNIS In Call routing,

1. Select **PBX** > **In Call Routing Configuration**.
2. Select the DNIS number.
3. On the *DNIS Routing* tab, check **Enable Fax-Over-IP** and click **OK**.



FoIP

☐ Enable Fax-Over-IP

Call Priority

☐ Set Call Priority 5

Call Skill Level Requirement

☐ Set Call SKLR 5

Language Setting

Default Language

Figure 253. The Enable Fax-Over-IP checkbox

Enabling this setting forces incoming calls that match this entry to use G.711 codec. If this checkbox is not checked but the destination is a fax extension, then G.711 codec will still be used.

Create a SIP Group for Fax Routing

You can allow voice and fax calls to run on the same SIP trunk channel. The trunks must be configured to support both voice and fax. The SIP trunk uses the same SIP server IP address, but different authentication credentials for voice trunk versus a fax trunk.

To configure fax routing,

1. Log into the MaxCS Cloud Services portal and retrieve the Fax details on the *General* tab of your account You will need this information in steps 6 and 7.
2. In MaxAdministrator, open *Trunk* view.
3. Double-click an unconfigured SIP Trunk. In the *Trunk Configuration* panel, click **Trunk Properties**.
4. In the next dialog box, click **SIP Group Configuration**.

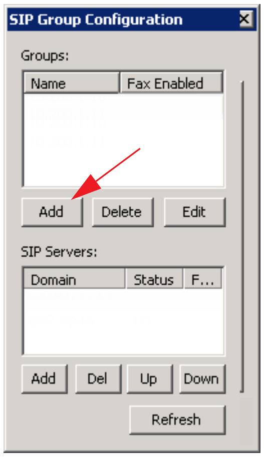
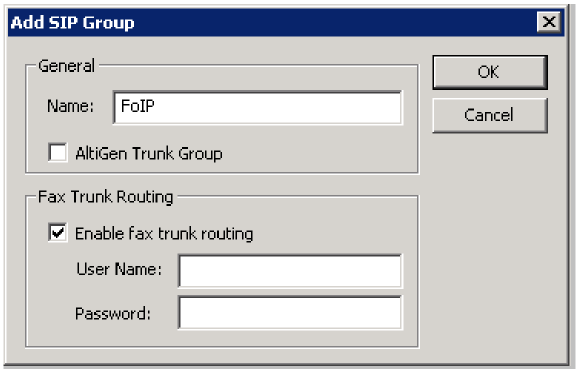


Figure 254. The SIP Groups and SIP Servers lists

5. Add a new SIP Group:
   a. Click **Add** (just below the *Groups* list) to add a new SIP Group:
   b. Enter a name (for example, *FoIP*) and check the option **Fax Trunk Routing**.
   c. Enter the fax trunk's user name and password (from the *Fax SIP Trunk Group* section on the *General* tab of the order in the Cloud Services portal) and click **OK**.



General

Name: FoIP

□ AltiGen Trunk Group

Fax Trunk Routing

☑ Enable fax trunk routing

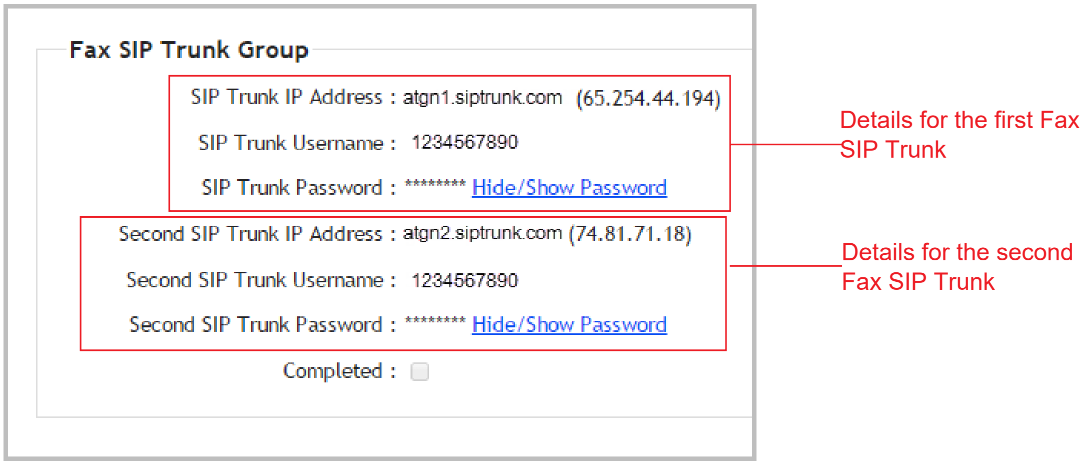
User Name:

Password:

Figure 255. Adding a new SIP Group for FoIP

6. Add two servers to this new SIP Group:
   a. In the *Groups* list, select the SIP Group that you just created.
   b. To create the first server, click the **Add** button that is just below the *SIP Servers* list.
   c. Copy and paste the first domain (from the *Fax SIP Trunk Group* section on the *General* tab of the order in the Cloud Services portal) and click **OK**.
   d. Repeat this process to create the second server; click **Add** (below the *SIP Servers* list), paste the second domain, and click **OK**.
7. You now have two SIP servers in this SIP Group. Next, configure these two servers:
   a. In the *SIP Servers* list, highlight the first server that you added.
   b. Specify the following parameters on the *Register* tab:
      - For *SIP Server IP Address*, copy and paste the IP address of the first trunk server (from the *Fax SIP Trunk Group* section on the *General* tab of the order in the Cloud Services portal (for example, **65.254.44.194**)

- For *User Name*, copy and paste the fax username from the portal
- For *Password*, copy and paste the fax password (click **Hide/Show Password** to see it)
- Set the *SIP Register Period* to **60**
- Set the *SIP Source Port* to **5060**
- Set the *SIP Destination Port* to **5060**



Fax SIP Trunk Group

SIP Trunk IP Address : atgn1.siptrunk.com (65.254.44.194)

SIP Trunk Username : 1234567890

SIP Trunk Password : ******** Hide/Show Password

Second SIP Trunk IP Address : atgn2.siptrunk.com (74.81.71.18)

Second SIP Trunk Username : 1234567890

Second SIP Trunk Password : ******** Hide/Show Password

Completed : □

Details for the first Fax SIP Trunk

Details for the second Fax SIP Trunk

Figure 256. Fax SIP Trunk details on the General tab of the order in the Cloud Services portal

c. Switch to the *Settings* tab and specify the following parameters:

- Set the *SIP Protocol Field* to **FROM Header**.
- Select *Carrier can only accept assigned numbers as Calling Number*.
- Enter the range of DID numbers that you want to assign to this trunk in the Calling Number can be accepted by the Carrier box. These must be valid DIDs that are on the trunk; each entry must be 10 digits.
- For the *Use this Calling Number if the Carrier cannot accept configured numbers* field, enter the main phone number. The phone number that you enter must be included among the Calling Number can be accepted by the Carrier entries.
- Select **Send Caller Name**. (Do NOT select Enable Standard Record-Route Header.)
- Set the *Incoming DID Number* field to **To Header**.

d. Repeat steps a through c for the second server, but this time specify the IP address as the ***second*** SIP trunk address from the portal.

8. Assign channels to the SIP Group and enable those channels:

a. Close the *SIP Group Configuration* window to return to the *SIP Signaling Channel Configuration* window.

b. Click **Channel Assignment**.

c. Select the channels to apply to this fax SIP Group. (You can use **Ctrl-click** to select multiple channels.)

d. Click **Assign Group**. In the list, select the group that you just created and click **OK**.

e. In the channel list, check the checkboxes for those channels to enable them. Click **OK**.

Considerations:

- Outbound calls that are made through SIP channels that have been configured for fax channels are for fax only. Therefore, they should **not** be assigned trunk access codes or be included in the out call routing for voice calls.

- Do not add these two SIP Trunk servers to any out call routing tables
- Do not assign trunk access codes to these two fax SIP Trunk servers
- These two fax SIP Trunk servers can receive either voice or fax trunk calls

Configure Gateway Devices

MaxCS works with several gateways, including the following devices:

- AudioCodes MP-202
- AudioCodes MP-118 and MP-124

For instructions on configuring these devices, and any other new devices that may have been certified after this manual was released, search the Altigen Knowledge Base (https://know.altigen.com/) for articles on your specific hardware.

FoIP Hunt Groups

For instructions on how to configure FoIP Hunt groups, see the discussion in *About Fax-over-IP Hunt Groups* on page 237.

CHAPTER

31

Tools and Applications

MaxCS comes with the following tools and applications for testing, diagnosing and configuring your system. They are available from the Windows **Start** menu.

- Backup and Restore Utility
- MaxAdministrator and Extension Security Checker
- Start and Stop All Altigen Services
- Trace Filter
- Trace Collector
- Voice File Converter
- Read Config

In addition, on the **Services > Utilities** menu in MaxAdministrator:

- Work/Hunt Group Converter utility
- Export and Import extensions utilities

If you installed Altigen's Custom Phrase Manager, it is available from the Windows **Start** menu. You can use this tool only if you have an Altigen SDK license.

Altigen Board Test

This is an Altigen hardware test tool for system hang and other hardware-related problems. It tests the following on all Altigen boards:

- Board memory from host or from both host and DSP
- DSP internal memory from host or from both host and DSP
- FMIC connection and data memory from host
- NVRAM from host
- PMC chip from host and DSP if T1/E1 board

You have the option of testing a single board or testing all boards at the same time.

The installation program for this tool is found in the \altiserv\exe folder in the installation media.

CT-Bus Test Tool

The CT-Bus Test Tool is a tool that detects one-way connection, cross talk, bad MVIP cable and static noise problems.

To run the CT-Bus test tool,

1. Stop Altigen Switching Services before running this utility.
2. Launch CT-Bus Test Tool.
3. Click **Start** to begin the test.
4. At the end of the test, the utility provides pass or fail results.

The installation program for this tool is found in the \altiserv\exe folder in the installation media.

Backup and Restore Utility

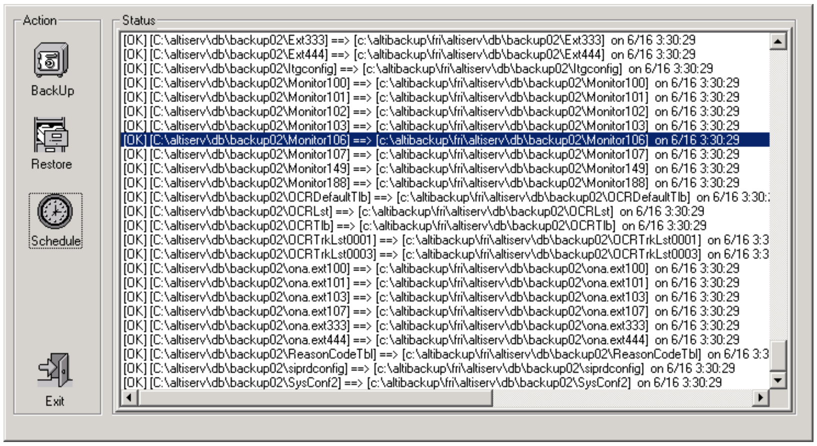
Note: The configuration backup option is turned on by default.

Backups do not include CDRs.

As of MaxCS Release 8.6.1, the backup utility no longer backs up the Polycom logs.

To back up or restore data, select either

- From MaxAdministrator: **Services > Utilities > Backup and Restore**, or
- From the Windows Start menu: **Max Communication Server ACM** > **Backup and Restore**.



```
[OK] [C:\altiserv\db\backup02\Ext333] ==> [c:\altibackup\fri\altiserv\db\backup02\Ext333]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\Ext444] ==> [c:\altibackup\fri\altiserv\db\backup02\Ext444]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\ltgconfig] ==> [c:\altibackup\fri\altiserv\db\backup02\ltgconfig]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\Monitor100] ==> [c:\altibackup\fri\altiserv\db\backup02\Monitor100]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\Monitor101] ==> [c:\altibackup\fri\altiserv\db\backup02\Monitor101]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\Monitor102] ==> [c:\altibackup\fri\altiserv\db\backup02\Monitor102]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\Monitor103] ==> [c:\altibackup\fri\altiserv\db\backup02\Monitor103]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\Monitor106] ==> [c:\altibackup\fri\altiserv\db\backup02\Monitor106]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\Monitor107] ==> [c:\altibackup\fri\altiserv\db\backup02\Monitor107]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\Monitor149] ==> [c:\altibackup\fri\altiserv\db\backup02\Monitor149]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\Monitor188] ==> [c:\altibackup\fri\altiserv\db\backup02\Monitor188]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\OCRDefaultTlb] ==> [c:\altibackup\fri\altiserv\db\backup02\OCRDefaultTlb]  on 6/16 3:30:
[OK] [C:\altiserv\db\backup02\OCRLst] ==> [c:\altibackup\fri\altiserv\db\backup02\OCRLst]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\OCRTlb] ==> [c:\altibackup\fri\altiserv\db\backup02\OCRTlb]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\OCRTrkLst0001] ==> [c:\altibackup\fri\altiserv\db\backup02\OCRTrkLst0001]  on 6/16 3:3
[OK] [C:\altiserv\db\backup02\OCRTrkLst0003] ==> [c:\altibackup\fri\altiserv\db\backup02\OCRTrkLst0003]  on 6/16 3:3
[OK] [C:\altiserv\db\backup02\ona.ext100] ==> [c:\altibackup\fri\altiserv\db\backup02\ona.ext100]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\ona.ext101] ==> [c:\altibackup\fri\altiserv\db\backup02\ona.ext101]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\ona.ext103] ==> [c:\altibackup\fri\altiserv\db\backup02\ona.ext103]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\ona.ext107] ==> [c:\altibackup\fri\altiserv\db\backup02\ona.ext107]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\ona.ext333] ==> [c:\altibackup\fri\altiserv\db\backup02\ona.ext333]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\ona.ext444] ==> [c:\altibackup\fri\altiserv\db\backup02\ona.ext444]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\ReasonCodeTbl] ==> [c:\altibackup\fri\altiserv\db\backup02\ReasonCodeTbl]  on 6/16 3:3
[OK] [C:\altiserv\db\backup02\siprdconfig] ==> [c:\altibackup\fri\altiserv\db\backup02\siprdconfig]  on 6/16 3:30:29
[OK] [C:\altiserv\db\backup02\SysConf2] ==> [c:\altibackup\fri\altiserv\db\backup02\SysConf2]  on 6/16 3:30:29
```

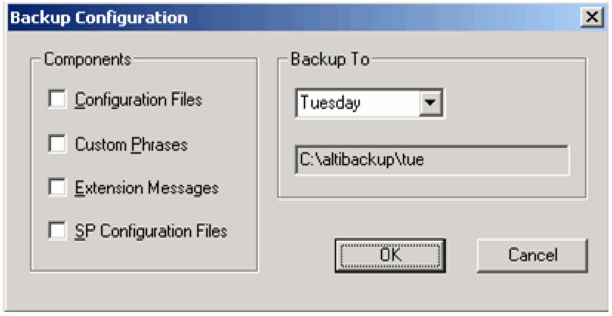
Figure 257. Backup and Restore window

Note: The Backup and Restore window can only be accessed at the primary MaxCS system; it is *not* available from a remote MaxAdministrator client.

Backing Up Files

Note: The backup utility does not back up internal CDR database. You must back up the internal CDR database from \AltiDB\InternalDB\Internal.mdb manually.

1. Click the **Backup** icon.



Backup Configuration

Components

□ Configuration Files

□ Custom Phrases

□ Extension Messages

□ SP Configuration Files

Backup To

Tuesday

C:\altibackup\tue

Figure 258. Backup Configuration dialog box

2. In the **Components** panel, select the files you want to back up.
3. In the **Backup To** list, select the day of the week (each day has its own folder in C:\altibackup for backing up files to), or select **Advanced** to change the drive or select a different folder.

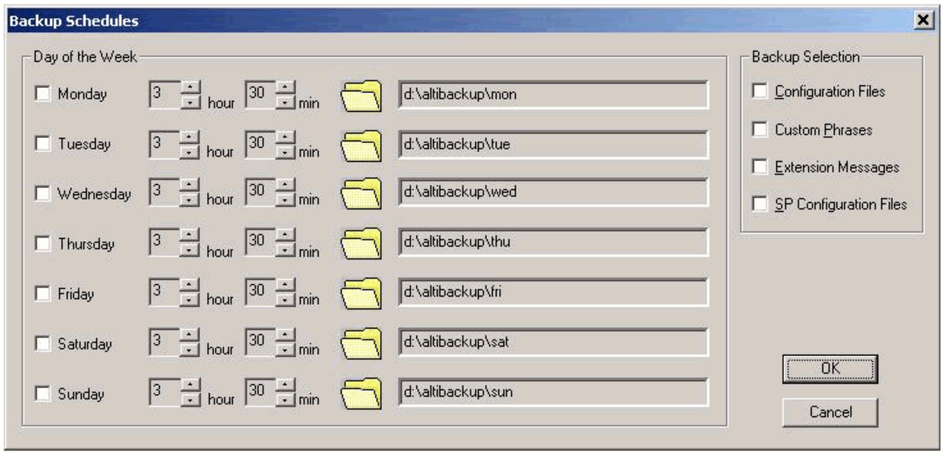
   Selecting **Advanced** displays a folder icon. Click the folder icon to open a browse dialog box that lets you select the folder to back up to. When you click **OK** in the dialog box, the selected drive or directory is displayed in the field below the **Backup To** list.
4. Click **OK** to start the backup. The panel shows the progress of the backup.

Scheduling Backups

You can set up automated backup on a schedule, and you can select the days, the times, and the target drives and folders for the backups.

To set backup schedules,

1. In the Backup and Restore window, click the **Schedule** button.



Backup Schedules

Day of the Week

□ Monday	3 hour	30 min	d:\altibackup\mon
□ Tuesday	3 hour	30 min	d:\altibackup\tue
□ Wednesday	3 hour	30 min	d:\altibackup\wed
□ Thursday	3 hour	30 min	d:\altibackup\thu
□ Friday	3 hour	30 min	d:\altibackup\fri
□ Saturday	3 hour	30 min	d:\altibackup\sat
□ Sunday	3 hour	30 min	d:\altibackup\sun

Backup Selection

□ Configuration Files

□ Custom Phrases

□ Extension Messages

□ SP Configuration Files

Figure 259. Backup Schedules dialog box

2. Set the options:
   - Check the box for each day of the week you want run the backup.
   - For each day, use the lists to specify the time. These time settings use a 24-hour clock.
   - You can accept the default target directories, or you can click the **Folder** icon to open the **Browse for Folder** dialog box to select the destination for the backup files.

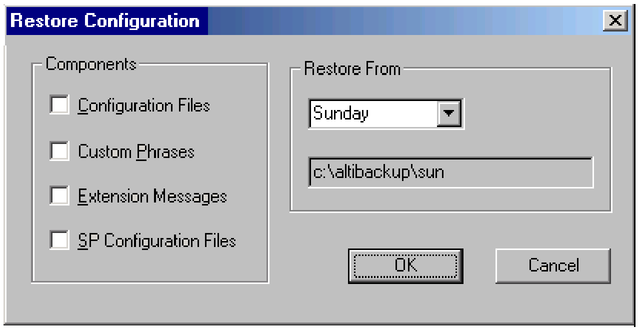
- Under **Backup Selection**, select the file components you want to back up: Configuration files, Custom Phrases, Extension Messages, SP Configuration files.

3. Click **OK**.

Restoring Backed up Files

To restore backed up files,

1. Stop the Altigen switching services.
2. In the Backup and Restore window, click the **Restore** button.



Components

□ Configuration Files

□ Custom Phrases

□ Extension Messages

□ SP Configuration Files

Restore From: Sunday

c:\altibackup\sun

Figure 260. Restore Configuration dialog box

3. Under **Components**, select the file groups you want to restore.
4. Using the **Restore From** list, select the day you want to restore from, or select **Advanced** to choose the restore folder.

   Clicking **Advanced** displays a folder icon that you can click to open a dialog box that allows you to select the directory you want to restore from.

   Select a day of the week or manually choose the restore directory. The specified directory appears in the text box below the list.

   Note: The components you select for restore must have been backed up into the directory you selected. For example, if you didn’t back up configuration files on Thursday, you won’t be able to restore them from the Thursday directory.

Important: Make sure the version you restore the database files from is compatible with the current MaxCS version. If incompatible files are restored, the phone system will fail to restart!

5. Click **OK** to start the restore process.
6. When you are finished restoring backed up files, restart the Altigen switching services.

MaxCS Admin & Extension Security Checker

MaxCS Admin & Extension Security Checker is a tool that

- Checks the security status of every extension in your MaxCS system and displays the security characteristics of each extension. From an extension’s right-click menu, you can lock and unlock the extension, force the user to change the password, clear an attacked record, and reset the status.
- Shows how many MaxCS Admins are currently connected to the system. By clicking **Disconnect All**, you can disconnect all MaxCS Admins from the local MaxCS system.

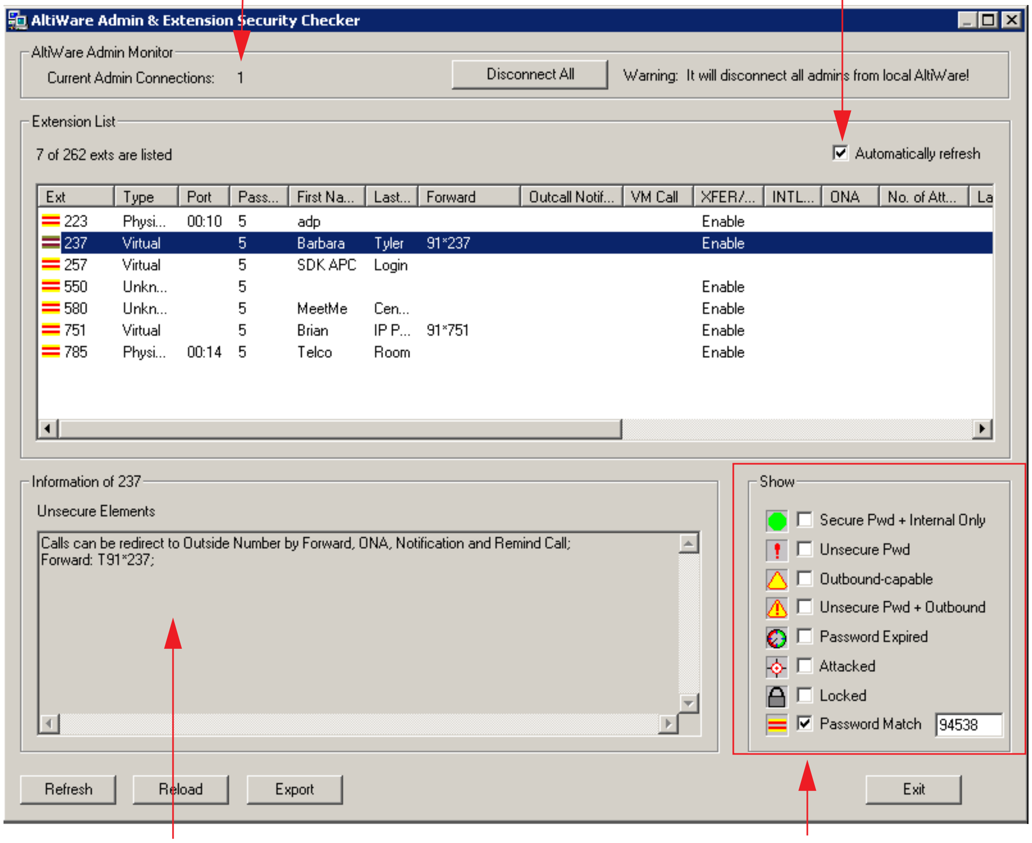
Changes as of Release 9.0.1:

- You must have Super Admin, Full Admin, or Basic admin login credentials to open Extension Checker.
- You can now run this tool remotely.

Launch the MaxAdministrator & Extension Security Checker from the Windows Start menu **MAX Communication Server ACM** > **MAXCS Admin & Extension Security Checker**.

Number of Admin connections

Automatically refreshes the display



AltiWare Admin & Extension Security Checker

AltiWare Admin Monitor

Current Admin Connections: 1

Warning: It will disconnect all admins from local AltiWare!

Extension List

7 of 262 exts are listed

☑ Automatically refresh

Ext	Type	Port	Pass...	First Na...	Last...	Forward	Outcall Notif...	VM Call	XFER/...	INTL...	ONA	No. of Att...	La
223	Physi...	00:10	5	adp					Enable				
237	Virtual		5	Barbara	Tyler	91*237			Enable				
257	Virtual		5	SDK APC	Login								
550	Unkn...		5						Enable				
580	Unkn...		5	MeetMe	Cen...				Enable				
751	Virtual		5	Brian	IP P...	91*751			Enable				
785	Physi...	00:14	5	Telco	Room				Enable				

Information of 237

Unsecure Elements

Calls can be redirect to Outside Number by Forward, ONA, Notification and Remind Call;
Forward: T91*237;

Show

- 🟢 □ Secure Pwd + Internal Only
- ❗ □ Unsecure Pwd
- ⚠ □ Outbound-capable
- ⚠ □ Unsecure Pwd + Outbound
- □ Password Expired
- □ Attacked
- 🔒 □ Locked
- ☑ Password Match 94538

Information on the selected extension

Security characteristics to check

Figure 261. MaxAdministrator & Extension Security Checker

Checking Extension Security

Generally, an extension is considered secure if its password meets the following conditions:

- It meets your password requirements
- Is different from the extension
- Is different from the default system password
- Does not consist of consecutive numbers
- Does not consist of a repetition of the same digit

To check extension security,

1. Select the security characteristics you want to check in the **Show** field group.

Status	Description
Secure Pwd + Internal Only	Has secure password and cannot make outbound trunk calls
Unsecure Pwd	Password has unsecure elements described in the Unsecure Elements window
Outbound-capable	Can make outbound trunk calls
Unsecure Pwd + Outbound	Password has unsecure elements described in Unsecure Elements window AND can make outbound trunk calls
Password Expired	Password is expired
Attacked	8 consecutive false password attempts have been made
Locked	Extension has been locked by system due to attack or by System Administrator
Password Match	To detect if an extension uses a specific trivial password, such as street address, zip code, phone number, enter that string here.

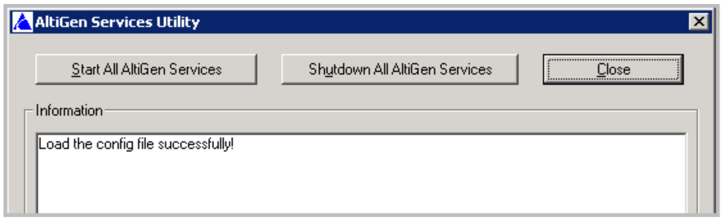
2. Click **Refresh.** Extensions with the selected insecure characteristics will appear in the Extension List.
3. Make changes to extensions from the right-click menus, or advise extension user(s) to make changes.
4. After changes have been made (for example in MaxAdministrator, MaxCommunicator, or with right-click commands in this tool), click **Reload** to fetch the new settings from MaxCS.

   Security characteristics for extensions you select in the Extension List display in the Unsecure Elements panel.
5. (Optional) Click **Export** to export the data in the Extension List to a text file.

Note: You are advised to run this security check periodically and remind extension users to use secure passwords.

Start & Stop All Altigen Services

You can start or stop all Altigen services from the Windows **Start** menu: **Max Communication Server ACM** > **Start & Stop All Altigen Services**.



Load the config file successfully!

Figure 262. The Altigen Services Utility

To shut down all Altigen services, click the **Shutdown All Altigen Services** button. Some examples of when you might want to do this are before you upgrade, before running some utilities and tools, and to apply certain configuration changes.

To start all Altigen services, click the **Start All Altigen Services** button.

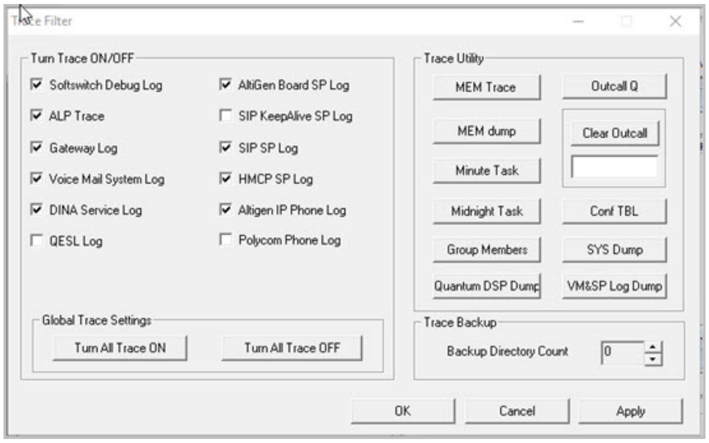
Trace Filter

You use the Trace Filter as a troubleshooting tool when working with Altigen Technical Support.

Several new traces were added in Release 8.6.1:

- SIP KeepAlive SP Log
- Polycom Phone Log
- QESL Log

You reach these trace settings by choosing **Diagnostics** > **Trace**.



☑ Softswitch Debug Log
☑ ALP Trace
☑ Gateway Log
☑ Voice Mail System Log
☑ DINA Service Log
☐ QESL Log
☑ AltiGen Board SP Log
☐ SIP KeepAlive SP Log
☑ SIP SP Log
☑ HMCP SP Log
☑ Altigen IP Phone Log
☐ Polycom Phone Log

Backup Directory Count: 0

Figure 263. Trace Filter panel

Other notes:

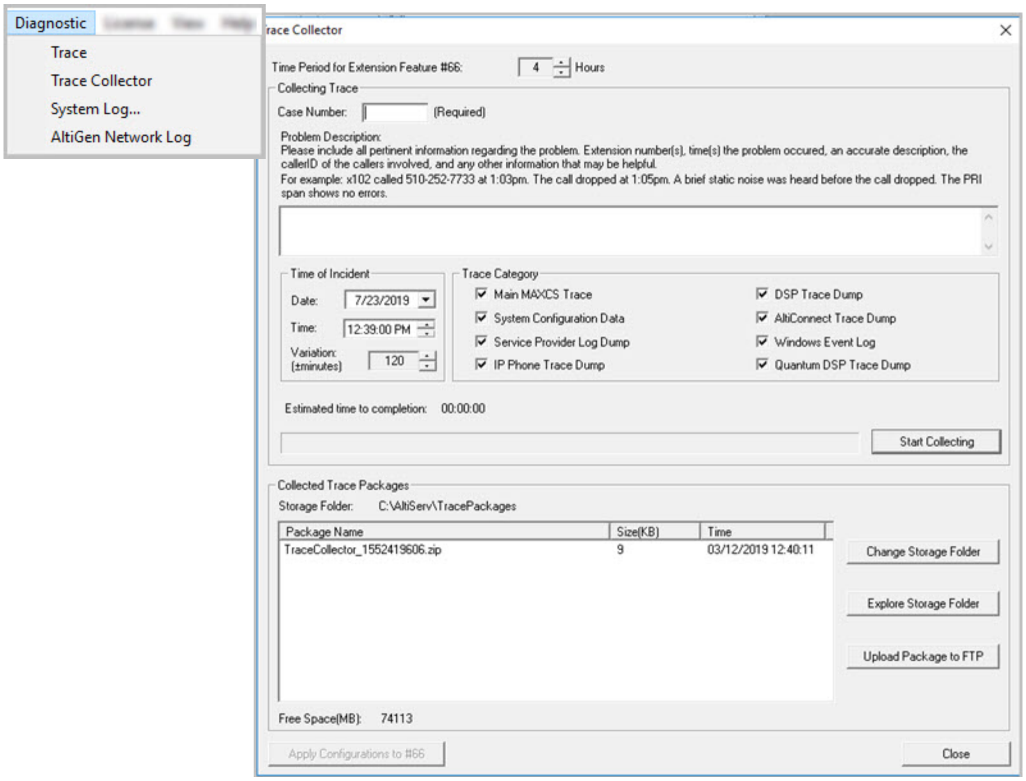
- The H323 SP log has been removed; it is no longer relevant in the newer releases of MaxCS.
- The *IP Phone Service* log has been renamed to *Altigen IP Phone log*.

Trace Collector

The Trace Collector collects trace for diagnostic purposes, and lets you upload the results to Altigen Technical Support directly from the Trace Collector dialog box. You can run the Trace Collector tool from the Windows **Start** menu, and also from MaxAdmin’s **Diagnostic** menu.

Note: Trace Collector is not available from an MaxAdministrator installed in a remote machine.

The Trace Collector first examines the running status of MaxCS and the gateway, and then checks whether each trace status is on or off. If a trace status is turned off, the Altigen system will not produce those traces. A message box pops up if MaxCS and the gateway are not running or an important trace status is off.



Time Period for Extension Feature #66: 4 Hours

Collecting Trace

Case Number: (Required)

Problem Description:
Please include all pertinent information regarding the problem. Extension number(s), time(s) the problem occured, an accurate description, the callerID of the callers involved, and any other information that may be helpful.
For example: x102 called 510-252-7733 at 1:03pm. The call dropped at 1:05pm. A brief static noise was heard before the call dropped. The PRI span shows no errors.

Time of Incident

Date: 7/23/2019

Time: 12:39:00 PM

Variation: (±minutes) 120

Trace Category

☑ Main MAXCS Trace
☑ System Configuration Data
☑ Service Provider Log Dump
☑ IP Phone Trace Dump
☑ DSP Trace Dump
☑ AltiConnect Trace Dump
☑ Windows Event Log
☑ Quantum DSP Trace Dump

Estimated time to completion: 00:00:00

Collected Trace Packages

Storage Folder: C:\AltiServ\TracePackages

Package Name	Size(KB)	Time
TraceCollector_1552419606.zip	9	03/12/2019 12:40:11

Free Space(MB): 74113

Figure 264. Trace Collector panel

Parameters for Trace Collector

Customize traces by choosing from the following parameters:

Time Period for Extension Feature #66 – Defines how many hours you want to go back to collect trace, starting from the time you press **#66**. The default value is 2 hours.

Case Number – Enter the Altigen case number associated with this trace collection activity. The case number will comprise the first part of the file name of the collected trace package.

Problem Description – Enter a description of the problem, including the extension number involved, the time when the problem happened, how to reproduce the problem, and so on.

Time of Incident – The tool collects the trace between the time ranges. The range covers before *and* after the defined Date and Time. The default Date and Time is one hour before the current date and time, and the default variation is 60 minutes. This setting is not applicable when **#66** is performed.

Trace Category – By default, all options are selected.

- **Main MaxCS Trace** (\AltiServ\log)

  Collects the following files, and extracts the trace records that fall in the specified time range:

actrace.log	AlpErrLog.txt	SIPlog.txt
ALPxxx.txt	\atps\threadID.txtl	SIPMan.txt
altiserv.txt	\atps\cmdlog.txt	SIPPstnReg.txt
AltiBack_XXX.trc	AdvQOverflow.log	SipExtChanTbl.log
AltiKeep_XXX.trc	Ac2AppPathHdlTbl.txt	SIPKeepALive.txt

AnnouceRunLog.txt	FeatServ.txt	QESLLog.txt
AssertLog.txt	DbUpdateTrdLog.txt	Qtmlog.txt
AW_AstrCpyErrLog.txt	HGwGenLog.txt	Loggservice_Mutex.txt
CallQManLog.txt	HGwMsgLog.txt	MEMORYTRACE.txt
CDRLogDLL.txt	threadid.txt	NewCDRExt.txt
CDRLogTrace.txt	MidNightLog.txt	TritonSPLog.txt
ConfigLog.txt	\logservice\Internal.txt	pathlog.txt
MsgOCLog.txt	ConfigServiceLog.txt	rsrclog.txt
MSRunLog.txt	CDRLogTrace.txt	RtpPortRangeTbl.txt
mviperr.txt	CDRLogDLL_EXCEPTION.txt	StartupLog.txt
Postman.txt	CSH323log.txt	Swxx_xxxx.txt
ProcInfoLog.txt	ExceptionLog.txt	GWMsgLog.txt

- **System Configuration Data** – Collects system configuration data, including System, Extension, Trunk, AA configurations, and Read OE files.
- **Service Provider Log Dump** – Runs SPDump.exe to dump the SP log into files and then collects the trace.
- **IP Phone Trace Dump** – Collects the Altigen IP Phone dump log in \AltiServ\Log\IPP (except for IP-805 models).
- **Stand-alone Gateway Trace** – Collects the trace on the stand-alone gateway machine. If AltiServ Services are shut down, the option is disabled. If Trace Collector is running on the stand-alone gateway machine, this option is hidden (because Trace Collector just needs to collect the trace locally).
- **DSP Trace Dump** – Collects the Triton DSP dump log in \AltiServ\SP\Triton\. Runs TritionDSPDebug.exe to dump Triton DSP binary log data, runs TATraceDecode.exe to convert binary log to text files, and then collects the text files.
- **AltiConnect Trace Dump** – Runs acdump.exe to dump the AltiConnect Trace, and then collects the trace. If Trace Collector is running on the stand-alone gateway machine, this option is hidden.
- **Windows Event log** – Extracts the system and application event log from the Windows system.

Start Collecting – Click this button to begin the trace collection, according to the time range and trace categories you chose. All collected files will be zipped to a single file, which will be listed in the Collected Trace Packages list box. The progress bar will display the progress of the whole process.

Storage Folder – The collected trace package is saved in this folder. The format of the file name is CaseNumber_Year_Month_Day_Hour_Minute_Second _ComputerName.zip. If the trace package is collected by **#66**, the format of the file name is #66_Year_ Month_Day_Hour_Minute_Second _ExtensionNumber.zip.

Free Space – Displays the free space of the drive where the storage folder is located. The folder must be in a local drive.

Change Storage Folder – Opens a folder browser window to select another storage folder. After the change, **Storage Folder**, **Free Space**, and the package list are refreshed to reflect the status of the new storage folder.

Explore Storage Folder – Opens the storage folder in a new explorer window.

Upload Package to FTP – Opens an FTP configuration dialog box. After you complete the required configuration, Trace Collector uploads the selected package to the Altigen Tech Support FTP site.

Apply Configurations to #66 – Apply time period, trace category, and storage folder to feature code #66 (Trace Collecting).

Limitations

If you run Trace Collector on MaxCS installed machine, note the following limitations:

- If MaxCS is not running, Trace Collector can only collect the trace of this machine. The traces in memory, such as “AltiConnect Trace Dump” and “Service Provide Log Dump”, and “Stand-alone Gateway Trace” will not be collected.
- If the default gateway is not running, the traces for "Triton DSP Trace Dump" will not be collected.
- If AltiServ is running, and an attached remote gateway is not running, or a remote gateway is detached, the trace for this gateway will not be collected even if that "Stand-alone Gateway Trace" is selected. If an attached gateway has the status of "Out of Service", the trace for this gateway will be collected.

If you run Trace Collector on a gateway MaxCS machine, note the following limitations:

- It can only collect the trace of this machine.
- If the stand-alone gateway is not running, the trace for “Triton DSP Trace Dump” will not be collected.

MaxCS Nightly Maintenance Tasks

The MaxCS system runs various maintenance and cleanup tasks every night. By default, these tasks begin at 3:00 AM local server time, to occur at non-peak time.

You can now adjust the start time of these tasks, by adding a registry entry. We recommend that you back up your registry before you make any changes to it.

To indicate what time you want the MaxCS nightly tasks to begin,

1. Open the registry on the MaxCS server.
2. Add a new entry:

```
HKEY_LOCAL_MACHINE\software\Wow6432Node\AltiGen Communications,
Inc.\AltiWare\MidnightTaskTime
```

3. The default time, 3:00 AM, is denoted as 03:00:00. This time will be used by default if you do not specify a different time, or if the value you enter is invalid.

   Enter the time you want the task to start and save the changes.

If you prefer, you can add this new registry entry via a command line. For example, to add an entry to this registry for the tasks to start at 2:15 AM, enter:

```
reg add "HKEY_LOCAL_MACHINE\software\Wow6432Node\AltiGen Communications,
Inc.\AltiWare" /v MidnightTaskTime /
t reg_sz /d 02:15:55
```

Change Log

As of Release 8.5 update 1, you can run a report showing changes that Administrators have made through the MaxAdministrator application.

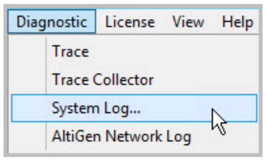


Figure 265. The options on the Diagnostics menu

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

The record contains information such as the following:

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

Administrators generate Change Log Reports by clicking a button within MaxAdministrator and specifying criteria such as a date range, a user, or an action pattern match. The query request is sent to Altiserv; Altiserv queries the logs through the Log Service and returns the matching results to the administrator. From there, the report can be exported to a PDF file as needed.

Change Log Report Requirements

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

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

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

About the Change Log Records

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

This table consists of the following columns.

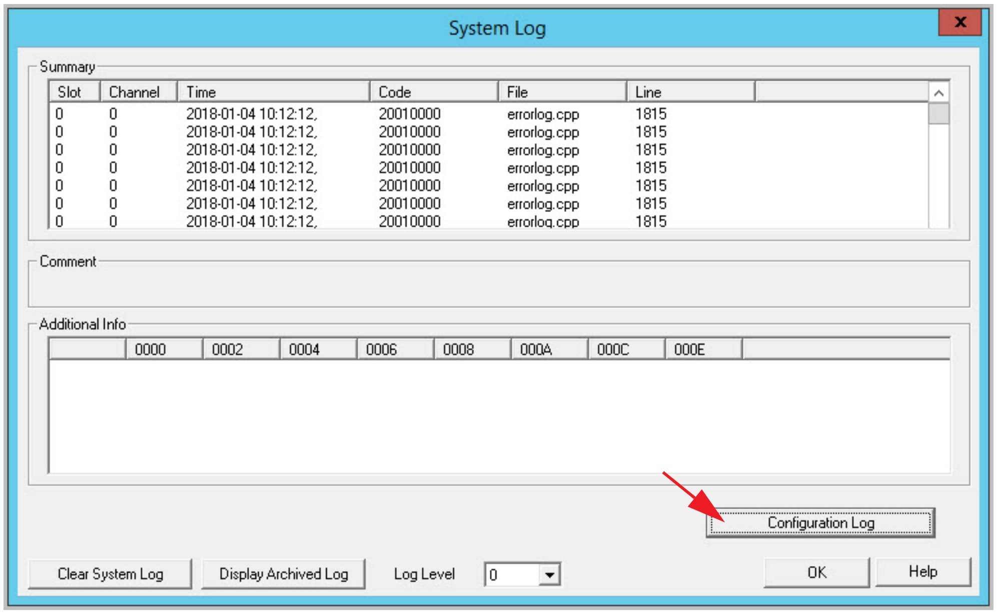
- [GUID] - The GUID of the transaction; all records generated by this user's change will share the same GUID
- [SeqID] - The sequence number of the records
- [date] - The date and time that the change was made
- [user] - The login name of the Admin user who made the change
- [description] - A description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

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

Generating a Change Log Report

To generate a Change Log Report,

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



System Log

Summary

Slot	Channel	Time	Code	File	Line
0	0	2018-01-04 10:12:12,	20010000	errorlog.cpp	1815
0	0	2018-01-04 10:12:12,	20010000	errorlog.cpp	1815
0	0	2018-01-04 10:12:12,	20010000	errorlog.cpp	1815
0	0	2018-01-04 10:12:12,	20010000	errorlog.cpp	1815
0	0	2018-01-04 10:12:12,	20010000	errorlog.cpp	1815
0	0	2018-01-04 10:12:12,	20010000	errorlog.cpp	1815
0	0	2018-01-04 10:12:12,	20010000	errorlog.cpp	1815

Comment

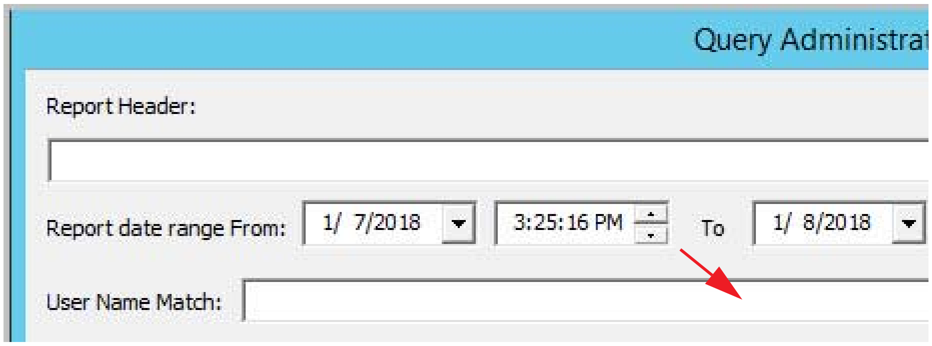
Additional Info

	0000	0002	0004	0006	0008	000A	000C	000E

Log Level 0

Figure 266. The System Log panel

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



Query Administrat

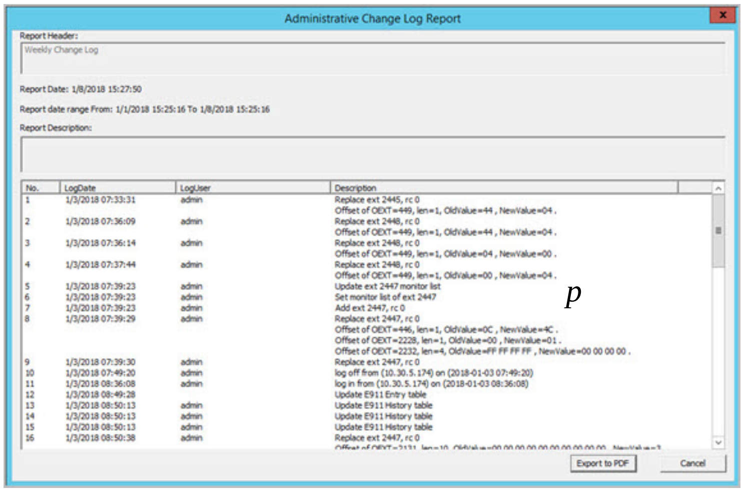
Report Header:

Report date range From: 1/ 7/2018 3:25:16 PM To 1/ 8/2018

User Name Match:

Figure 267. Enter criteria for the Change Log Report

6. Click **Query**. A panel shows you the configuration changes that meet your report criteria.



Report Header:

Weekly Change Log

Report Date: 1/8/2018 15:27:50

Report date range From: 1/1/2018 15:25:16 To 1/8/2018 15:25:16

Report Description:

No.	LogDate	LogUser	Description
1	1/3/2018 07:33:31	admin	Replace ext 2445, rc 0 Offset of OEXT=449, len=1, OldValue=44 , NewValue=04 .
2	1/3/2018 07:36:09	admin	Replace ext 2448, rc 0 Offset of OEXT=449, len=1, OldValue=44 , NewValue=04 .
3	1/3/2018 07:36:14	admin	Replace ext 2448, rc 0 Offset of OEXT=449, len=1, OldValue=04 , NewValue=00 .
4	1/3/2018 07:37:44	admin	Replace ext 2448, rc 0 Offset of OEXT=449, len=1, OldValue=00 , NewValue=04 .
5	1/3/2018 07:39:23	admin	Update ext 2447 monitor list
6	1/3/2018 07:39:23	admin	Set monitor list of ext 2447
7	1/3/2018 07:39:23	admin	Add ext 2447, rc 0
8	1/3/2018 07:39:29	admin	Replace ext 2447, rc 0 Offset of OEXT=446, len=1, OldValue=0C , NewValue=4C . Offset of OEXT=2228, len=1, OldValue=00 , NewValue=01 . Offset of OEXT=2232, len=4, OldValue=FF FF FF FF , NewValue=00 00 00 00 .
9	1/3/2018 07:39:30	admin	Replace ext 2447, rc 0
10	1/3/2018 07:49:20	admin	log off from (10.30.5.174) on (2018-01-03 07:49:20)
11	1/3/2018 08:36:08	admin	log in from (10.30.5.174) on (2018-01-03 08:36:08)
12	1/3/2018 08:49:28		Update E911 Entry table
13	1/3/2018 08:50:13	admin	Update E911 History table
14	1/3/2018 08:50:13	admin	Update E911 History table
15	1/3/2018 08:50:13	admin	Update E911 History table
16	1/3/2018 08:50:38	admin	Replace ext 2447, rc 0 Offset of OEXT=2131, len=10, OldValue=00 00 00 00 00 00 00 00 00 00 , NewValue=3

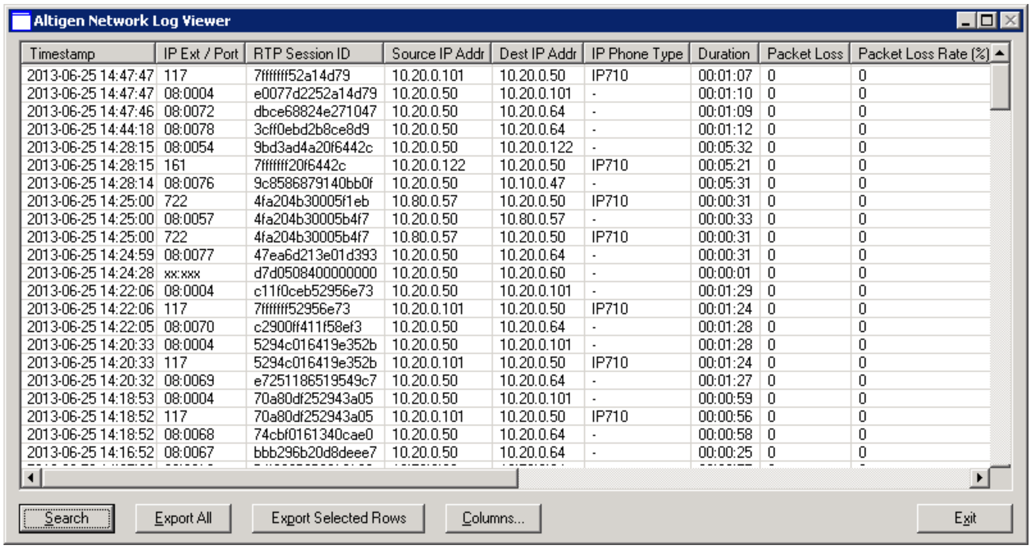
Figure 268. The generated Change Log Report

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

Network Log for Altigen IP Phones

The Altigen Network log shows traffic between the IP phones and the server. The information in this log is helpful when troubleshooting voice quality issues.

To view the log, from MaxAdministrator select **Diagnostic** > **Altigen Network Log**.



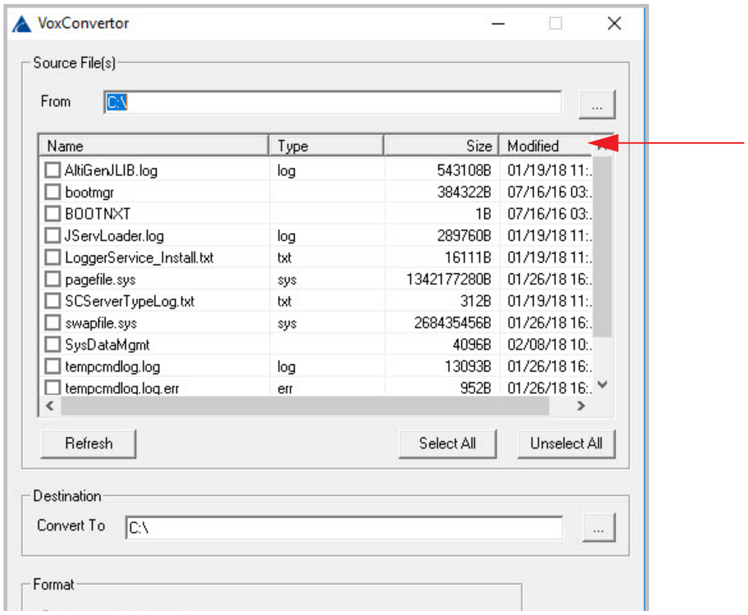
Timestamp	IP Ext / Port	RTP Session ID	Source IP Addr	Dest IP Addr	IP Phone Type	Duration	Packet Loss	Packet Loss Rate (%)
2013-06-25 14:47:47	117	7fffffff52a14d79	10.20.0.101	10.20.0.50	IP710	00:01:07	0	0
2013-06-25 14:47:47	08:0004	e0077d2252a14d79	10.20.0.50	10.20.0.101	-	00:01:10	0	0
2013-06-25 14:47:46	08:0072	dbce68824e271047	10.20.0.50	10.20.0.64	-	00:01:09	0	0
2013-06-25 14:44:18	08:0078	3cff0ebd2b8ce8d9	10.20.0.50	10.20.0.64	-	00:01:12	0	0
2013-06-25 14:28:15	08:0054	9bd3ad4a20f6442c	10.20.0.50	10.20.0.122	-	00:05:32	0	0
2013-06-25 14:28:15	161	7fffffff20f6442c	10.20.0.122	10.20.0.50	IP710	00:05:21	0	0
2013-06-25 14:28:14	08:0076	9c8586879140bb0f	10.20.0.50	10.10.0.47	-	00:05:31	0	0
2013-06-25 14:25:00	722	4fa204b30005f1eb	10.80.0.57	10.20.0.50	IP710	00:00:31	0	0
2013-06-25 14:25:00	08:0057	4fa204b30005b4f7	10.20.0.50	10.80.0.57	-	00:00:33	0	0
2013-06-25 14:25:00	722	4fa204b30005b4f7	10.80.0.57	10.20.0.50	IP710	00:00:31	0	0
2013-06-25 14:24:59	08:0077	47ea6d213e01d393	10.20.0.50	10.20.0.64	-	00:00:31	0	0
2013-06-25 14:24:28	xx:xxx	d7d0508400000000	10.20.0.50	10.20.0.60	-	00:00:01	0	0
2013-06-25 14:22:06	08:0004	c11f0ceb52956e73	10.20.0.50	10.20.0.101	-	00:01:29	0	0
2013-06-25 14:22:06	117	7fffffff52956e73	10.20.0.101	10.20.0.50	IP710	00:01:24	0	0
2013-06-25 14:22:05	08:0070	c2900ff411f58ef3	10.20.0.50	10.20.0.64	-	00:01:28	0	0
2013-06-25 14:20:33	08:0004	5294c016419e352b	10.20.0.50	10.20.0.101	-	00:01:28	0	0
2013-06-25 14:20:33	117	5294c016419e352b	10.20.0.101	10.20.0.50	IP710	00:01:24	0	0
2013-06-25 14:20:32	08:0069	e7251186519549c7	10.20.0.50	10.20.0.64	-	00:01:27	0	0
2013-06-25 14:18:53	08:0004	70a80df252943a05	10.20.0.50	10.20.0.101	-	00:00:59	0	0
2013-06-25 14:18:52	117	70a80df252943a05	10.20.0.101	10.20.0.50	IP710	00:00:56	0	0
2013-06-25 14:18:52	08:0068	74cbf0161340cae0	10.20.0.50	10.20.0.64	-	00:00:58	0	0
2013-06-25 14:16:52	08:0067	bbb296b20d8deee7	10.20.0.50	10.20.0.64	-	00:00:25	0	0

Figure 269. Altigen Network Log

Voice File Converter

This tool converts phrase, greeting, and music files from .wav to Altigen format and vice versa. To open the tool, from the Windows **Start** menu, select **Max Communication Server ACM** > **Voice File Converter**.

Note: The source .wav file must be in 8k/8bit/mono/mu-law format.



From: C:\

Name	Type	Size	Modified
□ AltiGenJLIB.log	log	543108B	01/19/18 11:.
□ bootmgr		384322B	07/16/16 03:.
□ BOOTNXT		1B	07/16/16 03:.
□ JServLoader.log	log	289760B	01/19/18 11:.
□ LoggerService_Install.txt	txt	16111B	01/19/18 11:.
□ pagefile.sys	sys	1342177280B	01/26/18 16:.
□ SCServerTypeLog.txt	txt	312B	01/19/18 11:.
□ swapfile.sys	sys	268435456B	01/26/18 16:.
□ SysDataMgmt		4096B	02/08/18 10:.
□ tempcmdlog.log	log	13093B	01/26/18 16:.
□ tempcmdlog.log.err	err	952B	01/26/18 16:.

Convert To: C:\

You can sort by clicking a column head

Figure 270. The Voice File Converter panel

To use the Voice File Converter,

1. Beside the **From** field, click the Browse button to select the folder that contains the files you want to convert.
2. Beside the **Convert To** field, click the Browse button to select the destination folder for the converted files. If they are prompts, they should be placed in the **C:\PostOffice\phrases\LangCustom** directory on the gateway that is running MaxCS. If the files are music files, they should be placed in the **C:\PostOffice\Phrases\Music** directory. A file that you want to use for music on hold must be named MusicOnWaiting. To save the Altigen system MusicOnWaiting file, rename it before replacing it.
3. Check the files you want to convert.
4. In the Format panel, select a format.
5. Click **Convert**.

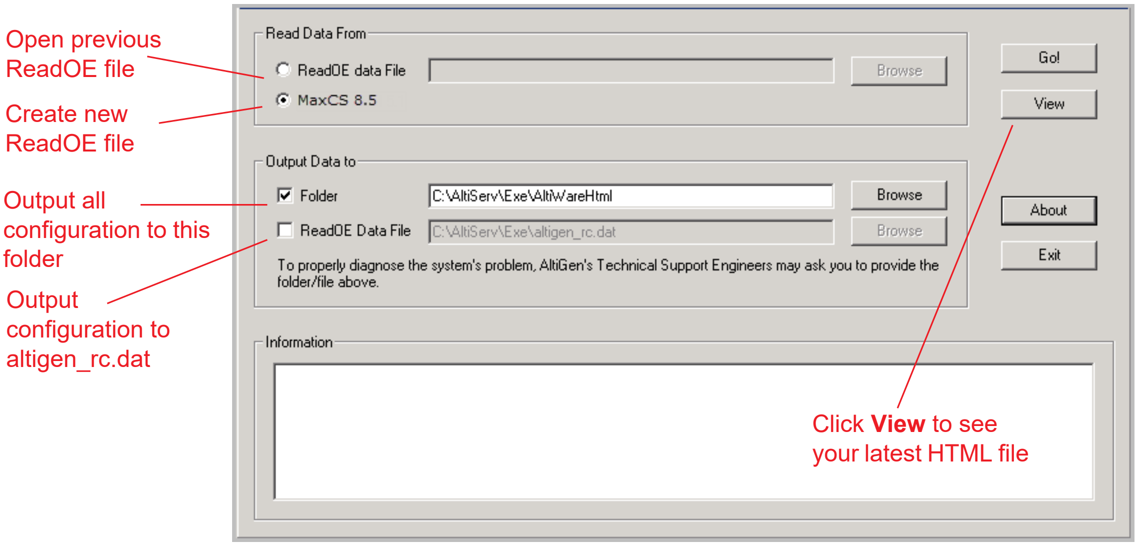
If a file format is incorrect, an error message pops up.

Read Config

Read Config (or Configuration Reader) is a tool that creates a subdirectory in \altiserv\EXE\AltiWareHtml\ of HTML files showing details of your MaxCS configuration.

To use Configuration Reader,

1. Launch Configuration Reader from the Windows **Start** menu, **Max Communication Server ACM** > **Read Config**.



Open previous ReadOE file

Create new ReadOE file

Output all configuration to this folder

Output configuration to altigen_rc.dat

Click **View** to see your latest HTML file

Read Data From

○ ReadOE data File

● MaxCS 8.5

Output Data to

☑ Folder: C:\AltiServ\Exe\AltiWareHtml

☐ ReadOE Data File: C:\AltiServ\Exe\altigen_rc.dat

To properly diagnose the system's problem, AltiGen's Technical Support Engineers may ask you to provide the folder/file above.

Information

Figure 271. The Read Config panel

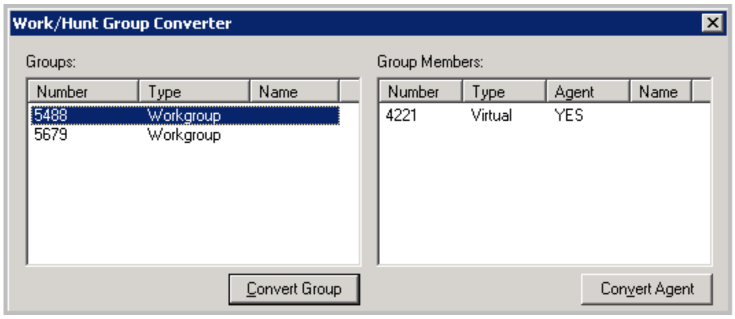
2. Make selections in the dialog box. If you will be sending a configuration file to Altigen Technical Support, check **ReadOE Data File**, and select a folder for the .dat file.
3. Click **Go**. A processing bar indicates the progress of configuration reading.
4. When the status window is complete, you can click the **View** button to view the HTML files showing your configuration.

Columns across the top of the opening page let you view statistics on different components of your configuration.

Work/Hunt Group Converter

The MaxCS Work/Hunt Group Converter allows you to convert workgroups to hunt groups or hunt groups to workgroups.

To launch the Work/Hunt Group Converter, select **Services** > **Utilities** > **Convert Work/Hunt Group**.



Work/Hunt Group Converter

Groups:

Number	Type	Name
5488	Workgroup	
5679	Workgroup	

Group Members:

Number	Type	Agent	Name
4221	Virtual	YES	

Figure 272. Work/Hunt Group Converter

Workgroups and hunt groups are listed on the left side of the window, member agents and non-agents are listed on the right side.

The **Work/Hunt Group Converter** can be used to convert:

- **Agent to Non-Agent –** If an agent belongs to any workgroup, it cannot be converted to a non-agent. When an agent is converted to a non-agent, all workgroup-related parameters will be cleared, including wrap-up time, inter-call delay, and outgoing workgroup number.

  To convert, select the agent (indicated by YES in the **Agent** field) and click the **Convert Agent** button or double-click the agent.
- **Non-Agent to Agent –** To convert, select the non-agent (indicated by NO in the **Agent** field) and click the **Convert Agent** button or double-click the non-agent. Make sure you have enough agent licenses.
- **Convert Workgroup to Hunt Group –** When a workgroup is converted to a hunt group, its members are not changed, but the following parameters are cleared, including:
  - voice recording setting
  - queue time threshold
  - queue overflow settings
  - queue announcement
  - agent announcement
  - queue quit forward (returns to default value – *to voice mail*)
  - call distribution (if previously configured to *Ring First Available Member*, *Ring Next Member* or *Ring All*, the setting is not changed. If configured to any other settings, the setting is configured to *Ring First Available Member*.)

  To convert, select the workgroup (indicated in the *Type* field) and click the **Convert Group** button or double-click the workgroup.
- **Convert Hunt group to Workgroup –** A hunt group cannot be converted if it contains at least one non-agent. You must first change the extension from non-agent to agent (by selecting the agent and clicking the **Convert Agent** button or by checking the **Agent** check box in the Extension Configuration window before converting).

  To convert, select the hunt group (indicated in the *Type* field) and click the **Convert Group** button or double-click the hunt group.

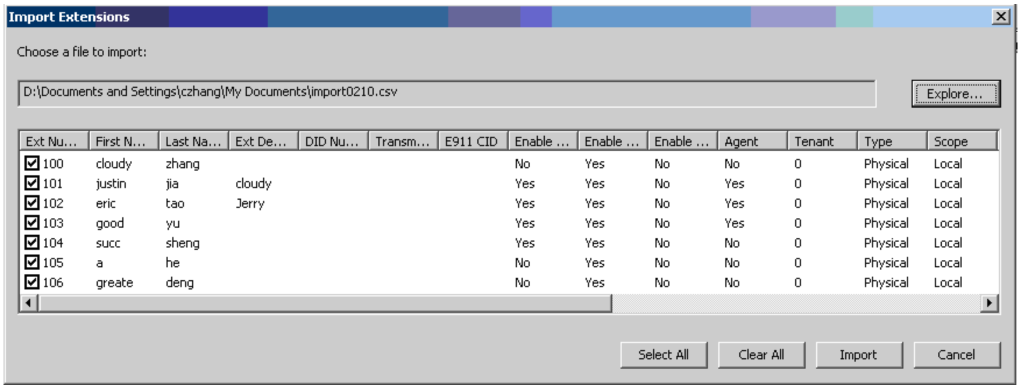
Exporting and Importing Extensions

You can import and export extensions in a .csv file and you can import extensions from the active directory.

Importing Extensions from a .csv File

1. First, back up your system configurations, using Altigen’s Backup and Restore tool (**Services** > **Utilities** > **Backup and Restore**).
2. Go to **Services** > **Utilities** > **Import Extensions**.
3. In the Import Extensions dialog box, click the **Explore** button to select a .csv file to import, and click **OK**.

   All the extension records in the .csv file are added to the Import Extensions list.



Choose a file to import:

D:\Documents and Settings\czhang\My Documents\import0210.csv

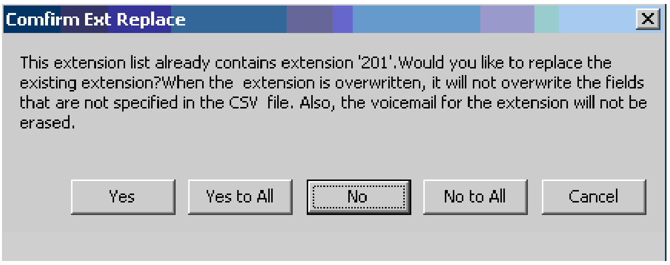
Ext Nu...	First N...	Last Na...	Ext De...	DID Nu...	Transm...	E911 CID	Enable ...	Enable ...	Enable ...	Agent	Tenant	Type	Scope
☑ 100	cloudy	zhang					No	Yes	No	No	0	Physical	Local
☑ 101	justin	jia	cloudy				Yes	Yes	No	Yes	0	Physical	Local
☑ 102	eric	tao	Jerry				Yes	Yes	No	Yes	0	Physical	Local
☑ 103	good	yu					Yes	Yes	No	Yes	0	Physical	Local
☑ 104	succ	sheng					Yes	Yes	No	No	0	Physical	Local
☑ 105	a	he					No	Yes	No	No	0	Physical	Local
☑ 106	greate	deng					No	Yes	No	No	0	Physical	Local

Figure 273. Choose a file to import

4. Check the records you want to import. Click the **Select All** and **Clear All** buttons to select or clear all the check boxes.)

Note: In release 8.5 Update 1, there are additional fields that you can import. See the section *Exporting and Importing Extensions* on page 400 for details.

5. Click **Import**. A progress bar shows you the progress of the import. When the import is finished, a message indicates how many extensions were imported, how many extensions were skipped and how many extensions failed.
6. If an extension already exists, you are prompted whether to replace the extension:



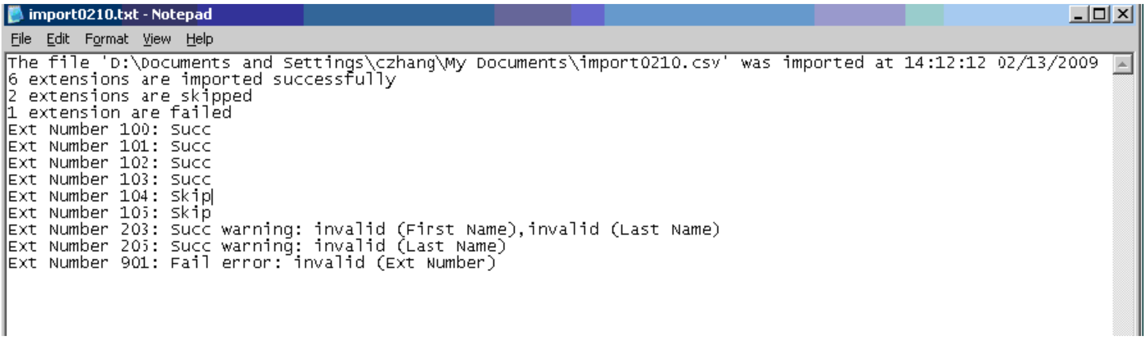
This extension list already contains extension '201'.Would you like to replace the existing extension?When the extension is overwritten, it will not overwrite the fields that are not specified in the CSV file. Also, the voicemail for the extension will not be erased.

Figure 274. Choose whether to replace the extension

If you overwrite an extension, fields that are not specified in the .csv file are not overwritten with default values or blank values. For example, if the column **Department** is not included in the .csv file, but is configured in the extension that you overwrote, the **Department** field is not reset to the default value when the extension is overwritten.

When the import is finished, a report file opens showing detailed information for every extension you attempted to import. If some fields are invalid, the system replaces them with a default value, except for the extension number field.

Note: The Department column doesnot support being modified after being imported from aCSV file.



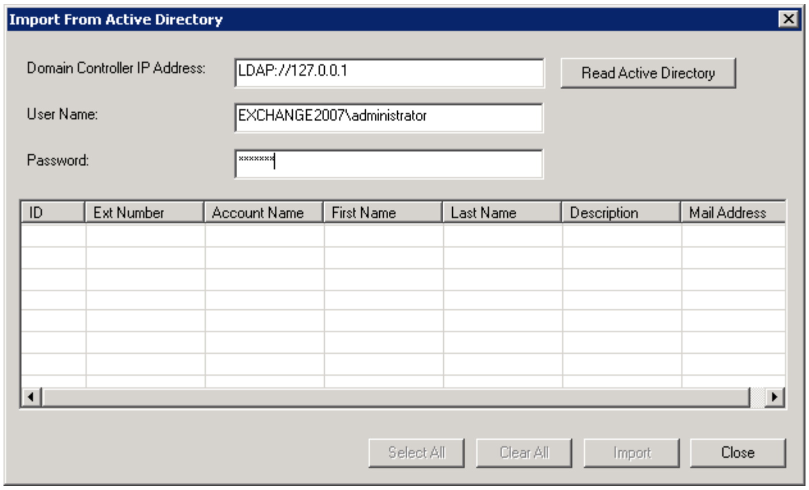
```
The file 'D:\Documents and Settings\czhang\My Documents\import0210.csv' was imported at 14:12:12 02/13/2009
6 extensions are imported successfully
2 extensions are skipped
1 extension are failed
Ext Number 100: Succ
Ext Number 101: Succ
Ext Number 102: Succ
Ext Number 103: Succ
Ext Number 104: Skip
Ext Number 105: Skip
Ext Number 203: Succ warning: invalid (First Name),invalid (Last Name)
Ext Number 205: Succ warning: invalid (Last Name)
Ext Number 901: Fail error: invalid (Ext Number)
```

Figure 275. The results of the import process

The name of the text file is the same as the .csv file, except that the file extension is .txt.

Importing Extensions from the Active Directory

1. First, back up your system configurations, using the Backup and Restore tool (**Services** > **Utilities** > **Backup and Restore**).
2. Go to **Services** > **Utilities** > **Import Extensions from Active Directory**.



Domain Controller IP Address: LDAP://127.0.0.1

User Name: EXCHANGE2007\administrator

Password: *******

ID	Ext Number	Account Name	First Name	Last Name	Description	Mail Address

Figure 276. Import from the Active Directory

3. Enter the server path, user name and password.
4. Click the **Read Active Directory** button.

   All user information is displayed in the table. (A record must have either an Ext Number or First Name or Last Name or Mail Address, otherwise it will not be not listed in the table.)
5. Select the extensions you want to import. You can use the **Select All** button, but only records that have an extension number can be selected. If an extension number is empty, a warning pops up.

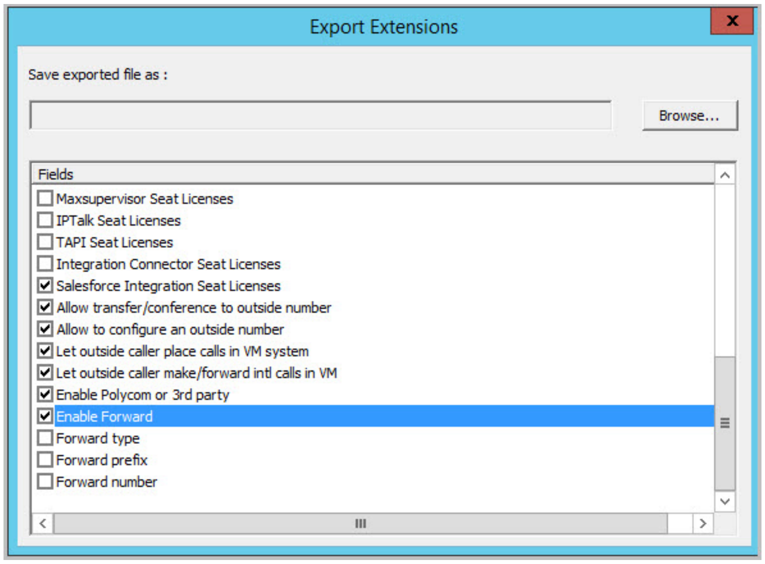
Note: Beginning with release 8.5 Update 1, there are additional fields that you can import. See the section *Exporting and Importing Extensions* on page 400 for details.

6. You can use the **Clear All** button to clear all check marks.
7. Click the **Import** button. A progress bar tells you the progress of importing.
8. If an extension already exists in the destination list, a dialog box opens.

9. Choose whether to replace the existing extension. If you decide to overwrite the extension, other fields not in the Active Directory are kept.

After finishing importing, a dialog box pops up to tell you how many extensions were imported successfully. When you click **OK**, an error report file is opened automatically to tell you the detailed information on every extension. If some fields are invalid, the system replaces them with a default value (except for the extension number). (The report file's name is “ReportImportAD.txt”. It is in the \altiserv\exe directory.)

1. Go to **Services > Utilities > Export Extensions**.



Export Extensions

Save exported file as :

Fields

- □ Maxsupervisor Seat Licenses
- □ IPTalk Seat Licenses
- □ TAPI Seat Licenses
- □ Integration Connector Seat Licenses
- ☑ Salesforce Integration Seat Licenses
- ☑ Allow transfer/conference to outside number
- ☑ Allow to configure an outside number
- ☑ Let outside caller place calls in VM system
- ☑ Let outside caller make/forward intl calls in VM
- ☑ Enable Polycom or 3rd party
- ☑ Enable Forward
- □ Forward type
- □ Forward prefix
- □ Forward number

Figure 277. Exporting extensions to a file

2. Click the **Explore** button and specify a name and location for the .csv file you’re about to create.
3. Check the fields you want to export. Use the **Select All** and **Clear All** buttons to select or clear all the check boxes.

   Note: You must export the extension number field.
4. Click the **Export** button to save the extension configurations to a .csv file.

   A progress bar shows you the progress of the export. When the export is complete, a dialog box indicates how many extensions were exported.

Editing a .csv File

If you edit a .csv file,

- All fields must be separated by a "," and all the records must be divided by pressing the **Enter** key.
- The first line must be a pre-defined field name, such as “First Name”. If the field name doesn’t match a pre-defined field name, the field is skipped during an import operation.
- The sequence of the columns doesn’t matter.

Altigen Custom Phrase Manager

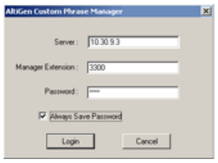
The Altigen Custom Phrase Manager is a Windows-based application that makes managing custom phrases easy. It displays all custom phrases in a graphical user interface. You can add or delete a phrase by clicking a button. You also can rename an existing phrase to a meaningful name, rather than pressing digits on the telephone.

The installation program for this tool is found in the Add-on Application folder in the installation media.

Note: The Altigen Custom Phrase Manager requires a Client SDK license.

To use the Altigen Custom Phrase Manager,

1. Open the tool from the Windows **Start** > **Max Communication Server ACM** menu. You'll see the login screen:



AltiGen Custom Phrase Manager

Server : 10.30.9.3

Manager Extension : 3300

Password : ****

☑ Always Save Password

Figure 278. Phrase Manager login panel

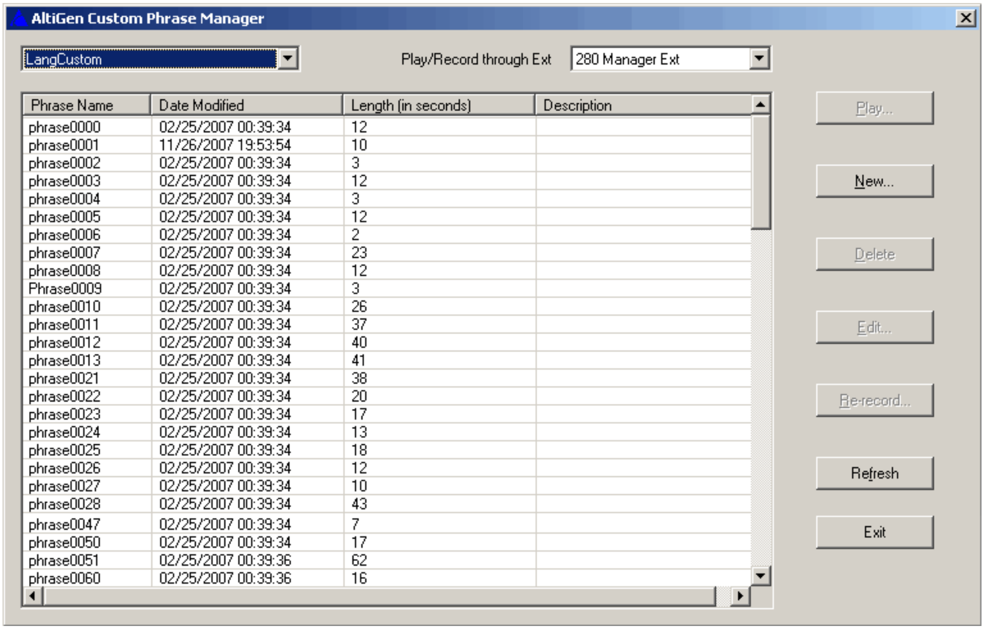
Enter the following:

- MaxCS server address
- Manager Extension
- Manager Extension password.

If you want to save the password for this application, check the **Always Save Password** check box.

Note: The server address and the extension number will be written to the windows registry. If you choose **Always Save Password**, the password will be encrypted and also saved in the registry. The tool will automatically reload the server address, manager extension number and the password from the registry when it starts next time.

2. Click **Login**. The main window opens.



AltiGen Custom Phrase Manager

LangCustom

Play/Record through Ext: 280 Manager Ext

Phrase Name	Date Modified	Length (in seconds)	Description
phrase0000	02/25/2007 00:39:34	12	
phrase0001	11/26/2007 19:53:54	10	
phrase0002	02/25/2007 00:39:34	3	
phrase0003	02/25/2007 00:39:34	12	
phrase0004	02/25/2007 00:39:34	3	
phrase0005	02/25/2007 00:39:34	12	
phrase0006	02/25/2007 00:39:34	2	
phrase0007	02/25/2007 00:39:34	23	
phrase0008	02/25/2007 00:39:34	12	
Phrase0009	02/25/2007 00:39:34	3	
phrase0010	02/25/2007 00:39:34	26	
phrase0011	02/25/2007 00:39:34	37	
phrase0012	02/25/2007 00:39:34	40	
phrase0013	02/25/2007 00:39:34	41	
phrase0021	02/25/2007 00:39:34	38	
phrase0022	02/25/2007 00:39:34	20	
phrase0023	02/25/2007 00:39:34	17	
phrase0024	02/25/2007 00:39:34	13	
phrase0025	02/25/2007 00:39:34	18	
phrase0026	02/25/2007 00:39:34	12	
phrase0027	02/25/2007 00:39:34	10	
phrase0028	02/25/2007 00:39:34	43	
phrase0047	02/25/2007 00:39:34	7	
phrase0050	02/25/2007 00:39:34	17	
phrase0051	02/25/2007 00:39:36	62	
phrase0060	02/25/2007 00:39:36	16	

Figure 279. Phrase Manager main window

- The list at the top left displays all the directories of custom phrases under your MaxCS system's PostOffice\phrases\ directory, such as LangCustom, LangCustom_Chinese, Tenant1Custom.
- The list at the top right lets you select an extension through which to record or listen to a phrase.

- The table shows all custom phrases under the selected directory, including:
  - Phrase name
  - Date and time the phrase was created or last modified
  - Phrase length
  - A column for a description of the phrase

  Data can be sorted in ascending or descending order by clicking a column heading.
- Buttons let you play, create and edit phrases.

Creating a New Phrase

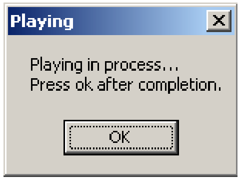
To create a new phrase,

1. Select the extension you will be using to record the phrase.
2. Click the **New** button.
3. Enter a name for the phrase.
4. Click **Start Recording**.
5. When finished recording, press **#** on the phone and follow the instructions you hear. Also click **OK** in the dialog box when done.

Playing a Phrase

To play a phrase,

1. Select the extension you will be using to listen to the phrase.
2. Click the **Play** button. The extension will ring.
3. Answer the ring, and a voice announces the phrase before playing it.



Playing in process...
Press ok after completion.

Figure 280. Playing a phrase

4. When you are finished listening, hang up the phone and click the **OK** button in the Altigen Custom Phrase Manager.

Editing a Phrase Name or Description

To edit the name of a phrase or its description,

1. Select the phrase you want to edit.
2. Click the **Edit** button.
3. Make your changes to the name and description. Click **OK**.

Deleting Phrases

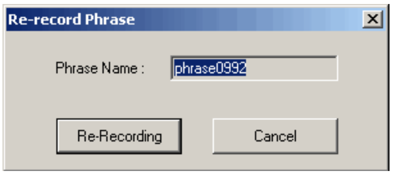
To delete a phrase,

1. Select the phrase you want to delete.
2. Click the **Delete** button. A confirmation dialog box opens.
3. To delete the phrase, click **Yes**. The phrase is deleted from the directory and from the table in Altigen Custom Phrase Manager.

Re-recording Phrases

To re-record a phrase,

1. Select the extension you will be using to re-record the phrase.
2. Select the phrase, and click the **Re-record** button.


Re-record Phrase

Phrase Name : phrase0992

3. When you have finished recording, press **#** on the phone and follow the instructions you hear. Click **OK** in the dialog box when you are done.

HMCP Certification Test Tool

The HMCP Certification tool helps you measure how many channels can be simultaneously operated in an HMCP system, based upon a threshold of CPU usage. The tool can also be used to measure DPC (Deferred Procedure Call) latency of a Microsoft system.

For instructions on installing this tool and running the various HMCP tests, refer to the detailed steps in the *Softswitch Deployment Guide*, found in the Altigen Knowledgebase. You will need to first install the tool, and then run it.

CHAPTER

32

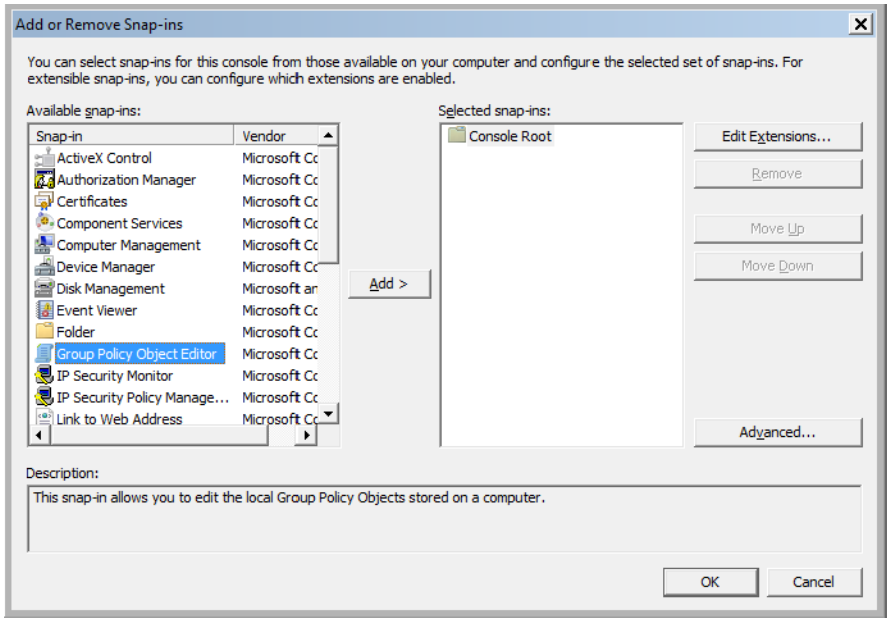
Quality of Service (QOS) Configuration

This section describes how to add QoS tags for MaxCS RTP packets.

- *Configure the MaxCS Server* on page 407
- *Configure Each MaxAgent Client System* on page 411

Configure the MaxCS Server

1. Open the Local Group Policy Editor on the MaxCS server: In Windows, click Start. In the Search box, enter ***gpedit.msc*** and press **Enter**.
2. Open MMC: In Windows, click **Start**. In the Search box, enter **mmc** and press **Enter**.
3. On the File menu, click **Add/Remove Snap-in**. In the dialog box, click **Group Policy Object Editor** and click **Add**.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cc
Authorization Manager	Microsoft Cc
Certificates	Microsoft Cc
Component Services	Microsoft Cc
Computer Management	Microsoft Cc
Device Manager	Microsoft Cc
Disk Management	Microsoft ar
Event Viewer	Microsoft Cc
Folder	Microsoft Cc
Group Policy Object Editor	Microsoft Cc
IP Security Monitor	Microsoft Cc
IP Security Policy Manage...	Microsoft Cc
Link to Web Address	Microsoft Cc

Selected snap-ins:

Console Root

Description:

This snap-in allows you to edit the local Group Policy Objects stored on a computer.

Figure 281. The Add or Remove Snap-ins dialog box

4. In the next dialog box, click **Browse**.

5. You can click either **This computer** to edit the Local Group Policy object, or click **Users** to edit Administrator, Non-Administrator, or per-user Local Group Policy objects.
6. Click **Ok**. Click **Finish**.
7. Switch back to the Local Group Policy Editor. In the left pane, expand **Local Computer Policy** > **Computer Configuration** > **Windows Settings**.
8. Right-click **Policy-based QoS** and select **Create new policy**.

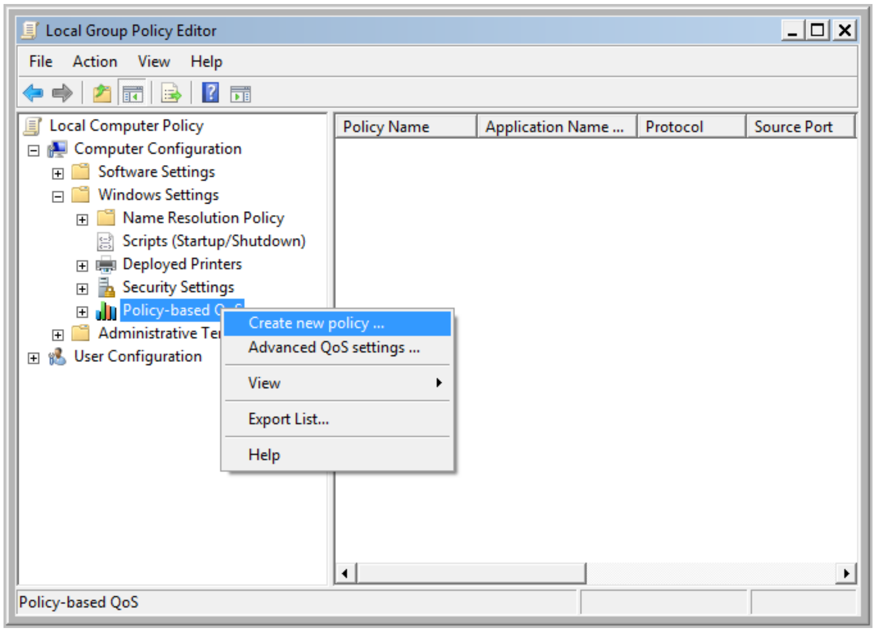
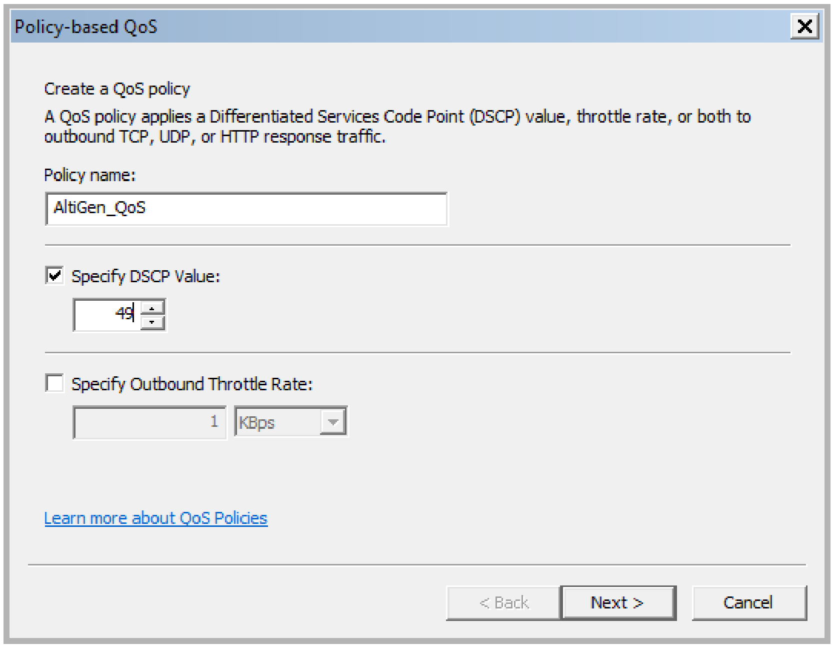


Figure 282. The Local Group Policy Editor window

9. In the new window, enter a policy name and specify a DSCP value from 0-63. Click **Next**.



Policy-based QoS

Create a QoS policy

A QoS policy applies a Differentiated Services Code Point (DSCP) value, throttle rate, or both to outbound TCP, UDP, or HTTP response traffic.

Policy name:

AltiGen_QoS

☑ Specify DSCP Value:

49

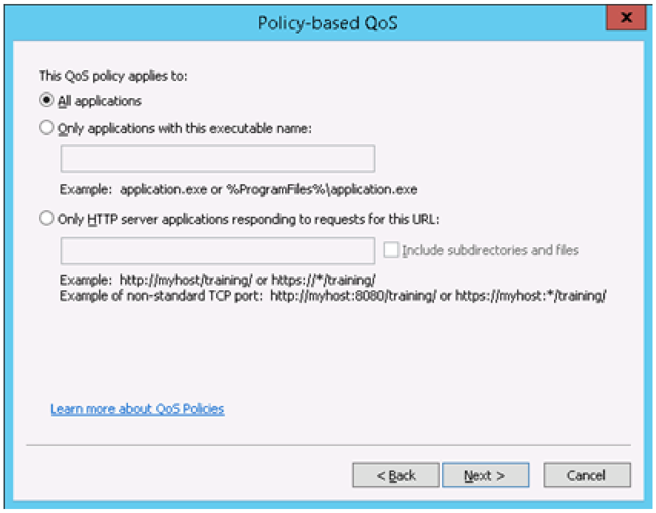
☐ Specify Outbound Throttle Rate:

1 KBps

Learn more about QoS Policies

Figure 283. Enter a name for the policy and a DSCP value

10. Select **All applications** and then click **Next**.



Policy-based QoS

This QoS policy applies to:

● All applications

○ Only applications with this executable name:

Example: application.exe or %ProgramFiles%\application.exe

○ Only HTTP server applications responding to requests for this URL:

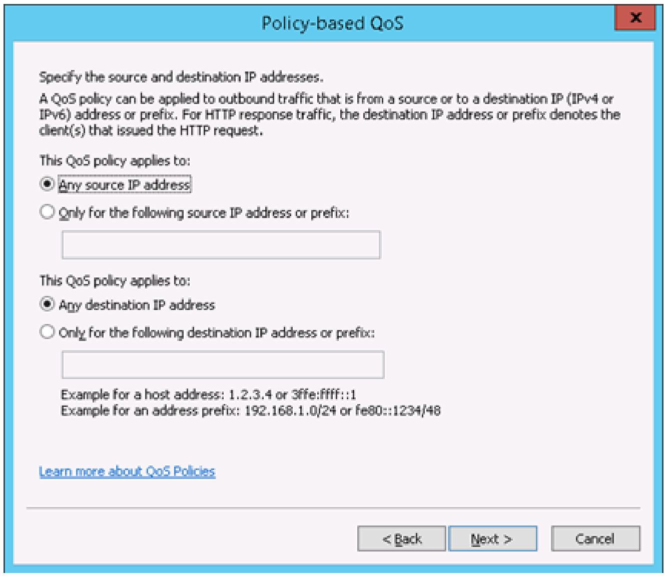
☐ Include subdirectories and files

Example: http://myhost/training/ or https://*/training/
Example of non-standard TCP port: http://myhost:8080/training/ or https://myhost:*/training/

Learn more about QoS Policies

Figure 284. Specify that the policy applies to all applications

11. Select **Any source IP address** and **Any destination IP address** in this panel and click **Next**.



Policy-based QoS

Specify the source and destination IP addresses.

A QoS policy can be applied to outbound traffic that is from a source or to a destination IP (IPv4 or IPv6) address or prefix. For HTTP response traffic, the destination IP address or prefix denotes the client(s) that issued the HTTP request.

This QoS policy applies to:

● Any source IP address

○ Only for the following source IP address or prefix:

This QoS policy applies to:

● Any destination IP address

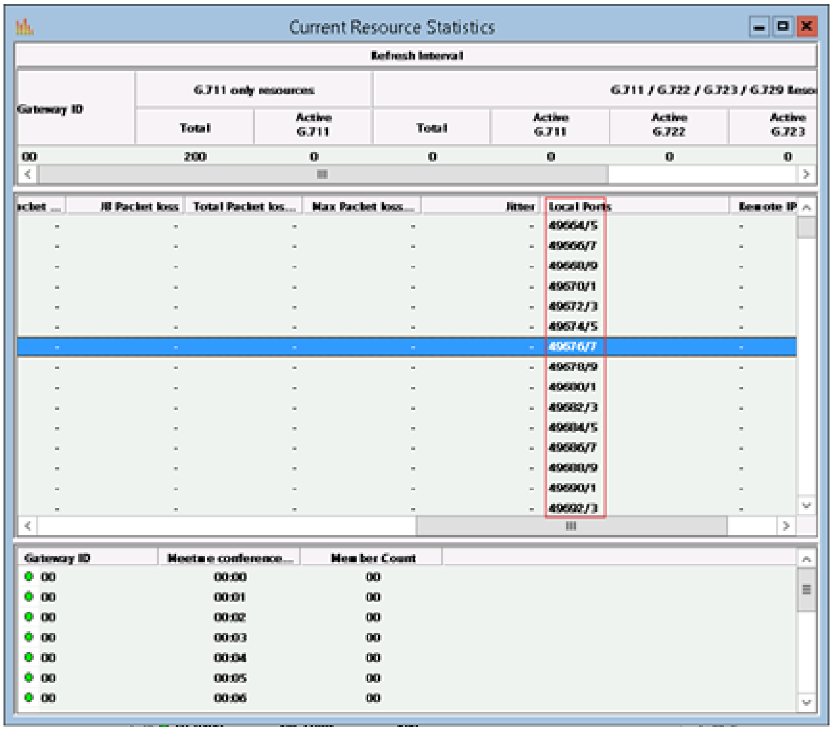
○ Only for the following destination IP address or prefix:

Example for a host address: 1.2.3.4 or 3ffe:ffff::1
Example for an address prefix: 192.168.1.0/24 or fe80::1234/48

Learn more about QoS Policies

Figure 285. Specify source and destination IP addresses

12. Open MaxCS Administrator. Obtain the port range (in the Local Ports column) in the *Current Resource Statistics* window.



Current Resource Statistics

Refresh Interval

Gateway ID	G.711 only resources		G.711 / G.722 / G.723 / G.729 Reso			
	Total	Active G.711	Total	Active G.711	Active G.722	Active G.723
00	200	0	0	0	0	0

cket ...	JB Packet loss	Total Packet los...	Max Packet loss...	Jitter	Local Ports	Remote IP
-	-	-	-	-	49664/5	-
-	-	-	-	-	49666/7	-
-	-	-	-	-	49668/9	-
-	-	-	-	-	49670/1	-
-	-	-	-	-	49672/3	-
-	-	-	-	-	49674/5	-
-	-	-	-	-	49676/7	-
-	-	-	-	-	49678/9	-
-	-	-	-	-	49680/1	-
-	-	-	-	-	49682/3	-
-	-	-	-	-	49684/5	-
-	-	-	-	-	49686/7	-
-	-	-	-	-	49688/9	-
-	-	-	-	-	49690/1	-
-	-	-	-	-	49692/3	-

Gateway ID	Meetme conference...	Member Count
● 00	00:00	00
● 00	00:01	00
● 00	00:02	00
● 00	00:03	00
● 00	00:04	00
● 00	00:05	00
● 00	00:06	00

Figure 286. MaxAdministrator Current Resource Statistics

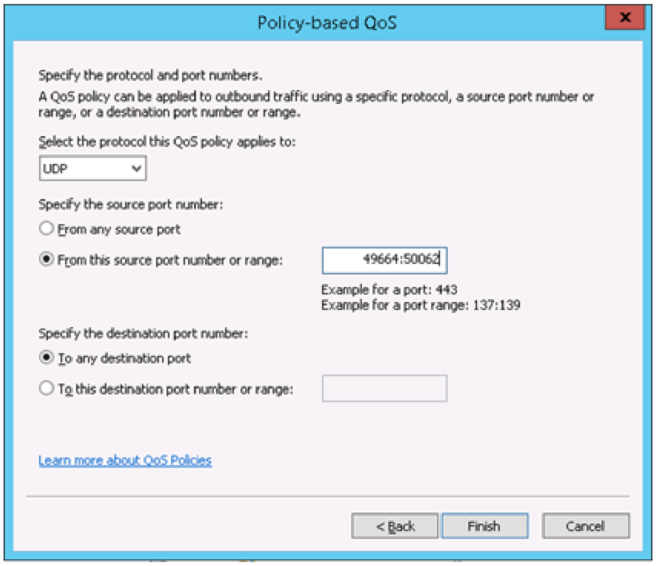
13. Switch back to the QoS policy window.

a. Select **UDP** for the protocol.

b. Select **From this source port number or range** and enter the port range from step 12.

c. Select To **any destination port**.

d. Click **Finish**.



Policy-based QoS

Specify the protocol and port numbers.

A QoS policy can be applied to outbound traffic using a specific protocol, a source port number or range, or a destination port number or range.

Select the protocol this QoS policy applies to: UDP

Specify the source port number:

○ From any source port

● From this source port number or range: 49664:50062

Example for a port: 443
Example for a port range: 137:139

Specify the destination port number:

● To any destination port

○ To this destination port number or range:

Figure 287. Figure 7: Set QOS options

Configure Each MaxAgent Client System

Repeat the steps listed in the previous section on each MaxAgent client system: add the policy with the same steps, but use port number 30000.

QoS Notes

If you had a Windows client machine on which you are pushing Policy Based QoS, and you noticed in a subsequent network trace that the DSCP value is 0x00, perform these steps:

1. If you need to make DSCP values to take effect on the adapter which does not have Domain access, you need to add the following registry on the system:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\QoS

   Type: REG_SZ

   Name: Do not use NLA

   Value: 1

   Create the key "QoS" if it does not exist.

   After you create the QoS registry key, reboot the computer.

2. If step 1 does not work, create an additional registry entry:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters] "Disable-UserTOSSetting"=dword:00000000

   Reboot the server and check the behavior.

If the system belongs to a domain, log in as a domain user; logging in as the local administrator or a user will not work.

CHAPTER

33

TLS 1.2 Configuration

Beginning with release 8.5.1, MaxCS includes several security enhancements:

- MaxCS now supports TLS 1.2, and includes an option to use only version 1.2 when TLS is used

  TLS 1.2 is now supported on IPTalk on MaxAgent, MaxCommunicator, and MaxOutlook.
- MaxCS now supports public certificates, and includes a new SNMP trap, to alert administrators when a certificate is approaching its expiration date (OID 1.3.6.1.4.1.13679.38.1)
- For enhanced security, MaxCS now supports firmware release F6.6.0A.336.004 on the AudioCodes MP1xx and Mediant devices. SIP UDP and SIP TLS 1.0 and 1.2 are supported. Both Altigen Enterprise certificates and public certificates are supported

Public Certificate Support

Public certificates are optional in MaxCS.

MaxCS now supports the following types of public certificates:

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

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

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

Certificate Details

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

- When you are creating a certificate request in Windows and must choose a Cryptographic Service Provider, select Microsoft RSASChannel, 2048 bit). The steps on this web page may be helpful to you: https://www.digicert.com/csr-ssl-installation/iis-7.htm
- Complete the certificate signing on the IIS server where you initially generated the Certificate Signing Request (CSR).

- Use Windows MMC (Microsoft Management Console) to export the file to a .pfx file. You may find the instructions in this web page helpful: https://www.sslsupportdesk.com/export-ssl-certificate-private-key-pfx-using-mmc-windows/
- You must enable TLS 1.2 on the server in order to use a public certificate.

Certificate Format

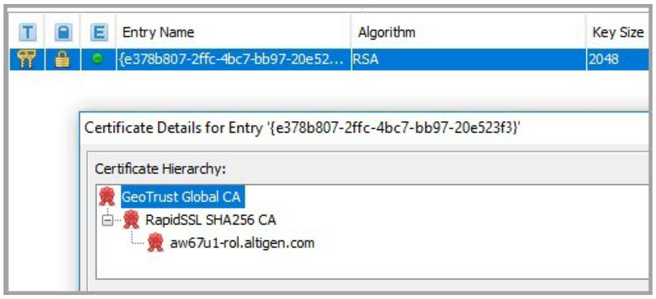
The certificate format that MaxCS supports is the .pfx format, which is used by Microsoft IIS.

The key pairs in the .pfx file must contain the full certificate chain; otherwise, Polycom phones may reject it.

To confirm that a .pfx file contains a full certificate chain:

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

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



T		E	Entry Name	Algorithm	Key Size
		●	{e378b807-2ffc-4bc7-bb97-20e52...	RSA	2048

Certificate Details for Entry '{e378b807-2ffc-4bc7-bb97-20e523f3}'

Certificate Hierarchy:

GeoTrust Global CA
RapidSSL SHA256 CA
aw67u1-rol.altigen.com

Figure 288. Public certificate format

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

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

Importing a Public Certificate

To import a public certificate into MaxAdministrator:

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

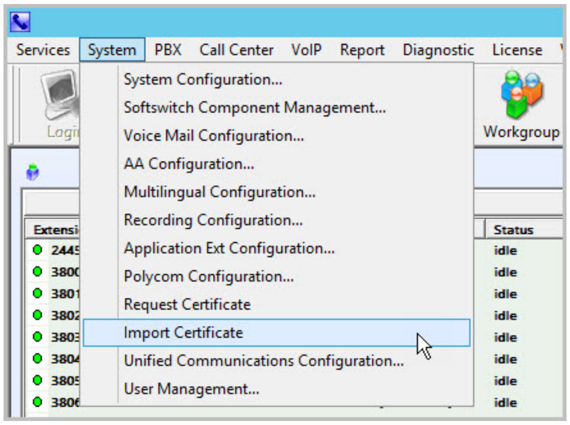


Figure 289. The Import Certificate option on the System menu

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

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

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

Limiting TLS to Version 1.2 Only

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

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

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

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

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

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

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

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

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

To enable this feature,

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

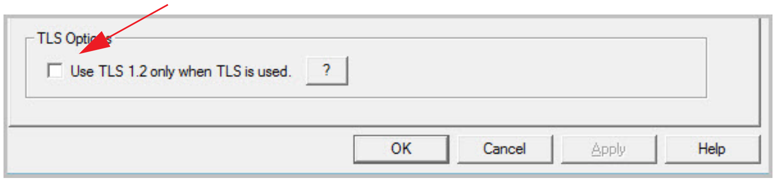


Figure 290. Enabling the Use TLS 1.2 only... option

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

TLS 1.2 Support on Altigen Phones

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

This firmware can be applied to the following Altigen phones: IP 705, IP710, IP 720. and IP 720a.

Altigen IP phones do not need to use public certificates.

Configuring IP-805 Phones in a TLS 1.2 Environment

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

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

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

Registry Entries to Enable TLS 1.2 Support

Depending upon whether you upgraded to 8.6.1 or performed a new installation, you may need to update some registry entries in order to enable TLS 1.2.

Scenario 1: You performed a clean (new) installation of MaxCS 8.6 or later

If you did not perform an upgrade from an earlier release of MaxCS such as 8.0, 8.5, or 8.5.1, then you do not need to make any registry changes in order to enable TLS 1.2.

Scenario 2: You upgraded from MaxCS Release 8.0, 8.5, or 8.5.1

If you upgraded from an earlier release, check your registry settings. Look for the following two entries:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.2\Client]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\
Protocols\TLS 1.2\Server]
```

If you do not see these entries, then you do not need to make any registry changes to enable TLS 1.2.

If you do see these entries, you have two choices. You can either edit those entries (and reboot) or you can remove those entries.

The registry entries should have these values:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]

"DisabledByDefault"=dword:00000000

"Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]

"DisabledByDefault"=dword:00000000

"Enabled"=dword:00000001
```

Reboot the server in order for the changes to take affect.

After you edit or remove those registry entries, if you are not using a public certificate then you should re-request a new certificate from MaxAdmin.

APPENDIX

A

E1-R2 and E1 ISDN PRI Installations

This information has been removed from the MaxCS Administration Manual and moved into a separate document. You can find this document on the Altigen web site, at https://www.altigen.com/support/, on the MaxCS Manuals tab.

B

Required Service Parameters

This section identifies the recommended and supported parameters for T1, PRI, and E1 service and provides you with the information needed when you make your service request.

Service Parameters/Request Information for T1

To subscribe to T1 service, certain parameters are required to establish service. The information provided below identifies the recommended and supported parameters for T1 service. When ordering T1 service, provide the following service request information:

Equipment Information

- PBX Manufacturer – Altigen Communications, Inc.
- CSU/DSU – ADTRAN T1 ACE (recommended) or other CSU/DSU

Technical Information for T1 with Voice

Signaling Protocol:

- E&M Wink Start (recommended)
- E&M Immediate Start
- Ground Start
- Loop Start (not recommended)

Trunk Type:

- DID
- 2-Way DID (recommended)
- DOD

Framing:

- Super Frame (SF)/D4
- Extended Super Frame (ESF) (recommended)

Line Coding:

- Alternate Mark Inversion (AMI)
- B8ZS (recommended)

DNIS, Caller ID:

- DTMF (Dual Tone Multi-Frequency)

Physical Termination:

- RJ-48X or RJ-48C

Wire:

- 4 wires

800 Service:

- You decide

Termination Impedance:

- 100 ohms

Type of Registered Services Provided

- BN 1.544 Mbps SF without power
- DN 1.544 Mbps SF B8ZS without power
- 1KN 1.544 Mbps ANSI ESF without power
- 1SN 1.544 Mbps ANSI ESF, B8ZS without power (recommended)

Service Order Code

SOC 6.0P AS.2

T1 Channel Assignment

- Trunk Type – In, Out, or 2-Way (recommended)
- Channels Assigned – 24 (Enter partial channels if you wish to subscribe to both voice and data service.)
- Hunting – Most Idle, Least Idle, Ascend, Descend
- DNIS Digits/Signal – 3/DTMF (can be 3 to 10 digits)
- Caller ID Signal – DTMF, if available (Not every service provider provides Caller ID over T1 lines.)

CSU/DSU Requirements

The CSU (channel service unit) is a device used to connect a digital trunk line coming in from the phone company to the PBX. A CSU can terminate signals, repeat signals and respond to loopback commands sent from the central office.

Service Parameters/Request Information for PRI

To subscribe to PRI service, certain parameters are required to establish service. The information provided below identifies the recommended and supported parameters for PRI service. When ordering PRI service, provide the following service request information:

Equipment Information

- PBX Manufacturer – Altigen Communications, Inc.
- CSU/DSU – ADTRAN T1 ACE (recommended) or other CSU/DSU

Technical Information for PRI with Voice

Switch Type:

- 5ESS (recommended)
- DMS (recommended)
- NI-2 (recommended)
- 4ESS

Framing:

- Super Frame (SF)/D4
- Extended Super Frame (ESF) (recommended)

Line Coding:

- Alternate Mark Inversion (AMI)
- B8ZS (recommended)

Physical Termination:

- RJ-48X or RJ-48C

Wire:

- 4 wires

PRI Channel Assignment

D Channels Assignment – 24th channel (the channel ID 23)

> **Note:** MaxCS can configure any channel in a PRI span to be the D channel. The default setting is the last channel. Every span should select a D channel within the span. Shared D channel (NFAS) or back up D channel is not supported.

Hunting – Most Idle, Least Idle, Ascend, Descend

DNIS Digits – can be 3 to 10 digits

CSU/DSU Requirements

The CSU (channel service unit) is a device used to connect a digital trunk line coming in from the phone company to the PBX. A CSU can terminate signals, repeat signals, and respond to loopback commands sent from the central office.

Service Parameters/Request Information for E1

To subscribe to E1 service, certain parameters are required to establish service. The information provided below identifies the recommended and supported parameters for E1 service. When ordering E1 service, provide the following service request information:

Equipment Information

- PBX Manufacturer – Altigen Communications, Inc.
- CSU/DSU – ADTRAN T1 ACE (recommended) or other CSU/DSU

Technical Information for E1 with Voice

Switch Type:

- Austel TS014
- ETSI NET5 (recommended)
- NT DMS-100

Framing:

- No CRC (recommended)
- CRC4

Line Coding:

- Alternate Mark Inversion (AMI)
- HDB3 (recommended)

Physical Termination:

- RJ-48X or RJ-48C

Wire:

- 4 wires

E1 Channel Assignment

- Data Channels Assignment – 1st channel (the channel ID 0)
- Channels Assignment – 17th channel (the channel ID 16)
- Hunting – Most Idle, Least Idle, Ascend, Descend
- DNIS Digits – can be 3 to 10 digits

CSU/DSU Requirements

The CSU (channel service unit) is a device used to connect a digital trunk line coming in from the phone company to the PBX. A CSU can terminate signals, repeat signals, and respond to loopback commands sent from the central office.

Appendix C

Network Ports

If MaxCS is installed behind a firewall/NAT router, you must open TCP and UDP ports according to this table:

For external VoIP connection through a firewall	TCP	UDP
Remote IP phone/IPTalk to phone service	10032 10064 5061	10060
TLS Support on Altigen SIP Trunks (ensure that TCP port 5061 is open on your firewall or router to the Altigen SIP Server addresses)	5061	
Remote Altigen IP phone firmware download (TFTP)		69
Extension global appearance	10066	
VoIP RTP Port (Voice Stream) for SIP		From X to Y (See note below)
SIP Tie Trunk from other Altigen systems		10060
SIP Trunking Service from carrier		5060
Polycom phone service	80 443	
With MaxCS Release 8.5.0.215 and later, TCP port 10078 is used for secured MaxAdministrator connection. Please make sure TCP port 10078 is opened on server side firewall for remote MaxAdministrator connection and the internet facing firewall appliance/router Port 10068 should be replaced with 10078 on the internet facing firewall appliance/router, if port 10068 is currently being used.	10078	

For external VoIP connection through a firewall	TCP	UDP
If you deploy on-premise MaxCS Service Hub and MaxCS WebApps applications you will need to open the following firewall ports for public Internet access: MaxCS Service Hub – TCP port configured on IIS during MaxCS Service Hub deployment MaxCommunicator Web & Web CT Proxy – TCP port 443 WebRTC control for IPTalk - TCP Port 7443 WebRTC media for IPTalk – UDP Ports 16384~32768 Chat – TCP port 8065		

When adding additional combo licenses, the system will also increase the RTP ports it uses and will use these new ports. If these additional ports are not added to the firewall, then calls will not have audio.

Note: An easy way to find out the RTP/TCP port ranges for SIP is to look in the MaxAdministrator **View > Current Resource Statistics** window. All the ports are listed in the **Local Ports** column.

When MaxCS or Softswitch is running on a non-Windows 2008/2012 system, BasePort = 49152.

When MaxCS or Softswitch is running on a Windows 2008/2012 system, BasePort = 49664 (This is because Windows 2008/2012 has some system services use ports in the 49152 range).

For a *single* chassis system:

X = BasePort

Y = BasePort + Total IP codec channels x 2

For a *multi*-chassis system, you need to enter multiple ranges:

Gateway ID = 0

X0 = BasePort

Y0 = BasePort + Total IP codec channels in GW0 x 2

Gateway ID = 1

X1 = BasePort + 512 x 1

Y1 = X1 + Total IP codec channels in GW1 x 2

Gateway ID = 2

X2 = BasePort + 512 x 2

Y2 = X2 + Total IP codec channels in GW2 x 2

Gateway ID=n

X(n)=BasePort + 512 x n

Y(n)=X(n) + Total IP codec channels in GW(n) x 2

To connect the following applications through a firewall	TCP
AltiConsole	10025
AltiReport	10025 10037

To connect the following applications through a firewall	TCP
MaxCommunicator/MaxAgent/IPTalk VM service for MaxCommunicator/MaxAgent	10025 10026 10028
MaxCommunicator/MaxAgent MeetMe Conference	10040
MaxSupervisor	10025 10027 10028 10029 10050
MaxMobile Communicator	10080 10081
Client Applications Auto Update	10050
CDR Search	10025
Remote MaxAdministrator	10078
VRManager Pro	10040
MaxInSight	10029
Network Assessment Tool	10010
Remote CT Proxy	10037

MaxCS connects the following application through a firewall	TCP
External CDR Logger Service	10027

MaxCS 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.

To help to avoid the potential RTP port use conflict with other Windows applications, you can use Windows commands to shift the dynamic port range out of the Altigen use. Following is an example, as 50663 is the highest RTP port for Altigen:

```
netsh int ipv4 set dynamicport udp start=50664 num=10000
```

Remote IP Phones Behind NAT

For remote IP phones behind NAT, you don’t need to do any configuration. However, if the remote firewall/NAT router blocks outgoing traffic, then you will need to open the following ports on the remote firewall/NAT router:

- UDP 10060
- UDP 30,000~31,000

- TCP 10064

APPENDIX

D

Technical Support & Product Repair Services

This section describes:

- Altigen technical support policy and procedures
- Product repair
- Technical training for administrators

Technical Support Eligibility

Eligibility: Altigen provides technical support to Authorized Altigen Partners and distributors only.

End user customers, please contact your Authorized Altigen Partner for technical support.

How To Reach Altigen 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, and 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
- A brief description of the problem and the procedure to reproduce the problem

Having this information ready will help us to better assist you.

End users who have problems unresolved by their Altigen Authorized Partner, and Partners who have problems unresolved by Altigen Technical Support may send an e-mail to Altigen’s CEO at ceo@altigen.com.

Product Repair

You may send defective Altigen-manufactured hardware products (in or out of warranty) to our factory for prompt authorized repairs. For information on Altigen repair services and return policies and the Altigen warranty, visit the Altigen Partner portal at https://partner.altigen.com.

APPENDIX

E

Troubleshooting

This section describes some common problems you may encounter, and provides steps you can take to try to resolve them.

Polycom Phone Cannot Register

If a Polycom IP phone cannot register, try the following:

1. Check LAN connectivity
2. Check that the firewalls have ports 80 and 443 unblocked
3. Reset the Polycom phone to the manufacturer's default and then reboot it. For instructions, see the *MaxCS Polycom Configuration Guide*.

Poor Voice Quality

When voice quality is poor, try the following:

1. **Perform a Loop-Back Test**. Call yourself by dialing out and dialing back into yourself. If you don't have any problems performing this test, the problem is most likely in the network or at the remote site.
2. **Check Traffic Between MaxCS IP Stations**. Open the Current Resource Statistics window (on the **View** menu) and the IP Cumulative Traffic Statistics window (on the **Report** menu) in MaxAdministrator to view network traffic.
3. **Check the RTP and RTCP Settings**. RTP/RTCP stands for Real-Time Transport (Control) Protocol, a transport protocol for real-time applications used to transport packetized voice packets over the IP network. Make sure UDP port numbers (49152 + n*512) ~ (49152 + n*512+p*2), where "n" is the gateway ID and "p" is the number of IP resource channels, are not assigned to other applications.

   Note: You can find this range displayed in the Current Resource Statistics window in the **Local Ports** column.
4. **Check Network Configurations**. Follow all network configuration guidelines provided under "Network Configuration Guidelines for VoIP" on page 303. Make sure the router, WAN bandwidth, and Jitter Buffer are configured properly.

Cannot Make a Connection

If a connection cannot be made, check the following:

1. Check network connectivity using “ping.”
2. Check network firewall settings. See “Network Configuration Guidelines for VoIP” on page 303 for details.
3. Check the IP address of the destination system.
4. Check the RTP and RTCP settings. Make sure UDP port numbers 49152-49199 are not assigned to other applications. RTP/RTCP stands for Real-Time Transport (Control) Protocol, a transport protocol for real-time applications used to transport packetized voice packets over the IP network.
5. Check the IP Dialing Table in Enterprise Manager for **Server ID Length**. Refer to “Defining the IP Dialing Table” on page 326.
6. Check if **Called Extension** is a **Workgroup** or has **Multiple Call Waiting Enabled**. When the called party is a workgroup pilot number or has Multiple Call Waiting enabled, the caller is placed on hold and hears ringback or music.

Incoming Calls with No Audio

If you have TLS turned on for your Altigen SIP trunks and an incoming call connects with no audio then drops, check that TCP port **5061** is open to the Alitgen SIP server addresses.

IP Resource Does Not Appear in Current Resource Statistics

When an IP resource doesn’t appear in the **Current Resource Statistics** window, there are two possible causes:

- **Device Driver is Not Running**. Check the device driver. Make sure it’s installed and working properly.
- **Triton VoIP Board is Not Installed Properly**. Refer to the *Quick Installation Guide* for details on proper installation of the Triton VoIP board.

Index