



MaxCS Release 8.6.1

All-Software Solution Deployment Guide

**Intended audience:
Altigen Authorized Partners**

May 26, 2020



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
Telephone: 888-Altigen (258-4436) | Fax: 408-597-9020
E-mail: info@altigen.com Web site: www.altigen.com

All product and company names herein may be trademarks of their registered owners.
Copyright © Altigen Communications, Inc. 2020. All rights reserved.

Contents

Introduction	5
Softswitch Small Business Deployment.....	5
Softswitch Standard Deployment	5
Additional Licenses Available	6
Licenses Not Available	7
Minimum Requirements	7
Before You Begin	8
Installation	8
Step 1: Install the HMCP Certification Tool	8
Step 2: Run the HMCP Certification Tool	10
Perform the DPC Latency Test – Pass/Fail	10
Determine Codec Maximum Quantities	12
Final Test with Codec Maximum Settings.....	13
Step 3: Install MaxCS	14
Step 4: Add the System Key.....	15
Step 5: Register Licenses.....	17
Step 6: Configure the HMCP Virtual Board	17
HMCP Resources Parameters	19
Parameters in IP Header	19
About Media Pass-Through Support	20
Step 7: Configure HMCP Codec Preferences for SIP Trunk Calls	20
Codec Preference - Incoming Calls.....	21
Codec Preference - Outgoing Calls, Third-Party IP Phones.....	21
Codec Preference - Outgoing Calls, IP Phones	22
Step 8: Configure the SIPSP Virtual Board	22
Step 9: Block Unauthorized SIP Invite Messages	25
Step 10: Configure the SIP Trunks.....	26
Step 11: Enable SIP Option (optional).....	31
Step 12: SIP Trunk Setting.....	32
Step 13: Configure a Codec Profile	33
Step 14: Assign the Codec Profile to the Two SIP Servers	34
Step 15: Configure NAT	35

Step 16: AltiGen SIP Trunk Configuration	35
Configure the First Server	36
Configure the Second Server	37
Enable Channels	38
Check Your Configuration	39
Step 17: Configure Inbound Routing	40
Step 18: Configure Out-Call Routing	40
Step 19: System Configuration	40
Step 20: Configure Polycom Phones	40
Step 21: Enforce TLS 1.2 (optional)	41
AltiGen Technical Support	41

Introduction

This document is provided for AltiGen partners who will be performing a fresh installation of MAX Communication Server (MaxCS) Release 8.6.1 All-Software Softswitch Solution for their clients.

A separate guide is provided for deploying AltiGen's Unified Communications service with MaxCS; refer to the *MaxCS UC Deployment Guide*.

IMPORTANT! These instructions are **only for new installations of MaxCS**. If you are upgrading from a previous release of MaxCS, follow the instructions in the *MaxCS Upgrade Guide*.

There are two types of Softswitch deployments for MaxCS:

- **Small Business Softswitch**
- **Standard Softswitch**

Some notes regarding this Softswitch installation:

- This is a software-only installation process.
- This installation does not support redundancy or gateway installation.
- All components must be installed on the same server.

Softswitch Small Business Deployment

The Softswitch Small Business system is capped at 24 users and cannot be expanded. It includes the following licenses:

- 1 ACM Base license
- 1 HMCP Media license
- 24 Combo Station licenses
- 24 SIP Trunk licenses
- 24 Compressed VoIP Channel licenses
- 12 Meet Me Conference Resources

Softswitch Standard Deployment

The Softswitch Standard bundle includes the following licenses:

- 1 ACM Base license
- 30 Port MeetMe Conference
- HMCP Media Server
- 1 AltiConsole license
- 1 Multilingual license
- 1 AltiEnterprise License
- 5 HMCP Combo Codecs
- 5 Agent Supervision

Note: These licenses can only be registered with the Softswitch system key.

Additional Licenses Available

The following additional license bundles are available for the Softswitch Standard deployment:

- The **Contact Center Combo license** bundle (ALTI-ACMCOMBO) includes the following licenses:
 - 5 Agent Combo licenses
 - 1 Supervisor Combo license
 - 1 AltiReport license
 - 1 MaxInsight license
 - 1 Advanced Call Router license
- The **Station Combo license** bundle (ALTI-COMBOSTATION-XX) includes the following licenses:
 - 1 Softswitch Station license
 - 1 MaxCommunicator/AltiView license
 - 1 IP Talk license
 - 1 Exchange integration license
 - 1 MaxMobile license
 - 1 HMCP Combo Codecs
- The **Agent Combo license** bundle (ACM-COMBOAGENT-XX) includes the following licenses:
 - 1 Softswitch Station license
 - 1 IP Talk license
 - 1 Exchange integration license
 - 1 MaxMobile license
 - 1 ACM Agent seat
 - 1 MaxAgent seat
 - 1 MaxCall seat
 - 1 HMCP Combo Codecs
- The **Supervisor Combo license** bundle (ACM-COMBOSUPVR-XX) includes the following licenses:
 - 1 Softswitch Station license
 - 1 IP Talk license
 - 1 Exchange integration license
 - 1 MaxMobile license
 - 1 ACM Agent seat
 - 1 MaxAgent seat
 - 1 MaxCall seat
 - 1 MaxSupervisor seat
 - 1 HMCP Combo Codecs
 - 1 Agent Supervision
- Other Softswitch-eligible licenses:
 - SSW ACM Agent Seat license
 - MaxAgent Session and Seat licenses
 - MaxSupervisor Session and Seat licenses

- AltConsole license
- CTI Integration Connector Seat license
- Call Recording Session and Seat licenses
- SIP Trunk license
- Third Party SIP Device license
- VRManager license
- MaxInsight Session license
- Client Application SDK Session license
- Trunk Control APC SDK Session license
- SightMax Integration license
- Polycom Advanced Features license
- Quality Management Feature and seat license

Licenses Not Available

The following licenses are not available for the MaxCS All-in-One Softswitch Solution.

- IP Gateway Expansion licenses (ALTI-GWEXP-01).
- AltStation licenses (you must use either an SSW-STATION stand-alone license or an SSW-BASECOMBO-STD license instead).
- ACM-SEAT500 (you must use either an SSW-ACMAGENT stand-alone license or an SSW-ACMCOMBOAGENT license instead).

Minimum Requirements

- Dedicated Windows Server 2019 64-bit, 2016 64-bit, Windows Server 2012 R2, Windows 7 64-bit SP1*, or Windows Server 2008 R2 SP1 Standard* running on a 64-bit, Quad-core Intel @ 2.5GHz, 4GB memory, 160GB hard drive, or, for a virtual environment, VMware ESXi 6.0/6.5/6.7 or Hyper-V 6.1; **at a minimum**, allocate 4 Intel cores @ 2.0GHz each, 4GB memory, and 160GB hard drive.

** After January 14, 2020, Microsoft will no longer provide security updates or support for Windows 7 and Windows Server 2008 R2.*

Strongly recommended, when installing a soft switch configured for 50 users or more, and/or systems processing in excess of 5K Trunk Calls per day*, are CPU's with overall Passmark Score of 10,000 or higher.

Required configurations for all Altigen Soft Switch installations running on a Virtual Machine:

- CPU Resources assigned to the VM where the Altigen Soft Switch Server is installed must be configured as **Dedicated** or **Reserved for MaxCS use**.
- Memory resources assigned to the VM where the Altigen Soft Switch Server is installed must be configured as **Dedicated** or **Reserved for MaxCS use**.
- ** These values are simply guidelines. In some cases, based on configurations, actual use, and types of Add-on applications installed and running, these values may be lower or higher than baselines noted above. If you are unsure, please open a case with Altigen Technical Support for guidance.*

- The server must pass the tests in the HMCP Certification Tool; see [Step 1: Run the HMCP Certification Tool](#) on page 8. **Do not proceed with installation** if the test results are not within the specified parameters.
- For on-premise deployments, we recommend that your system have an overall passmark score of 10,000 or greater.

IMPORTANT:

- Make sure that the server has the recommended Windows Service Pack and/or updates.
- The server must already be a member of the Active Directory Domain.

Before You Begin

We recommend that you take these steps before you begin the installation process:

- Make sure that TCP port 5061 is open on your firewall or router to the Altigen SIP Server addresses
- Have the System key and software license keys available
- Make sure you have your login information for the Partner portal

Installation

This section provides detailed instructions for installing MaxCS Softswitch Release 8.6.

Step 1: Install the HMCP Certification Tool

Before you install MaxCS, **you must run the DPC Latency test in the HMCP Certification Tool**. This tool can be automatically installed during MaxCS installation.

Note: You need to run HMCP only when you install MaxCS Softswitch; if you are installing MaxCS All-In-One, running HMCP is not required.

HMCP stands for *Host Media Control Processing*, a virtual component that uses an Intel CPU to provide the following functions:

Process VoIP media stream

- Encode, decode, and transcode voice streams
- Detect and generate tone for IP devices
- Play music when a device is on hold
- Process IP paging

Play and record voice files

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

Provide conferencing resources

- Barge-in/silent monitor/coaching

- Station conference and MeetMe conference

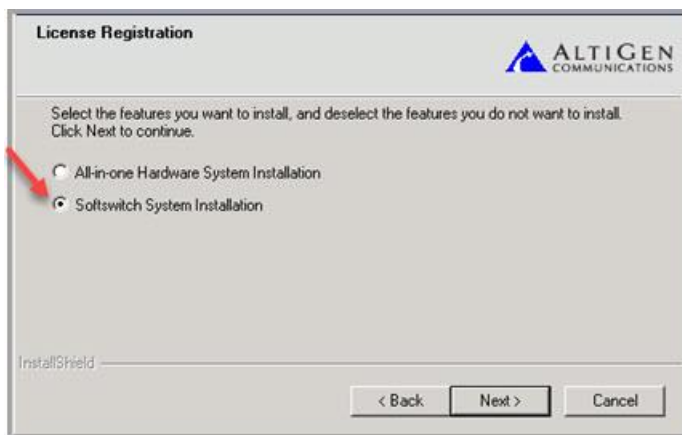
For a full explanation of HMCP and the roles it plays in the MaxCS All Software Solution, review the training presentation “What is HMCP?” in the AltiGen Communications Learning portal (<http://learn.altigen.com/login/index.php>). Log in with the same credentials that you use on the AltiGen Partner Portal.

You will run the AltiGen HMCP Certification tool before you begin the MaxCS installation. This tool helps measure how many channels can be simultaneously operated in certain conditions; you specify a threshold of CPU usage. It also measures DPC (Deferred Procedure Call) latency of Microsoft systems.

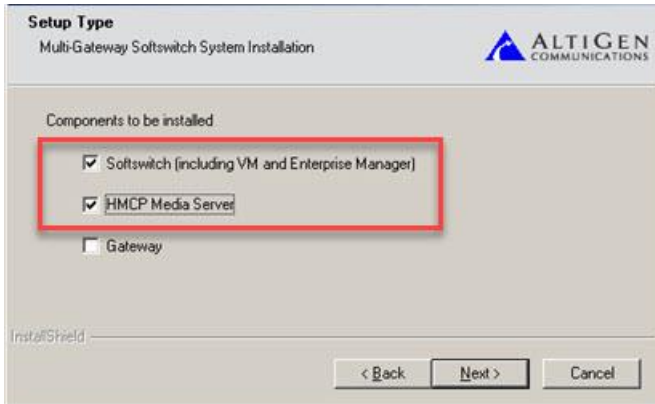
1. Log into the server as a user with administrative privileges. If the system is a stand-alone server, log in as a local administrator account. If you plan to run Exchange Integration, you must have domain administrator rights.
2. Stop all MaxCS services.
3. Load the installation media. Open and review the readme.txt file.
4. Navigate to the *MaxCS ACM* folder. Double-click **Setup**. The installation wizard starts.
5. On the Welcome panel, close all Windows applications and click **Next**.

For a new installation, the installation program will require a reboot after it installs the HMCP Certification tool. You will run the tool (step 2) and then start the wizard again to install the application.

6. In the *Setup Type* panel, select **Softswitch System Installation**. Click **Next**.



7. On the next panel, select only the first two options, **Softswitch (including VM and Enterprise Manager)** and **HMCP Media Server**. Click **Next**.



8. If you have not yet installed the MaxCS HMCP Certification tool, you are prompted to do so now. You must run the certification tool before you install MaxCS. Click **Yes** to install the tool now.
9. The HMCP Certification tool installation wizard starts. Click **Next**.
10. In the next panel, enter a user name and organization, and then click **Next**.
11. In the next panel, click **Next** to accept the default folder for the installation.
12. In the next panel, click **Install**.
13. After the files have been installed, click **Finish**.
14. Click **Yes** to restart the server.

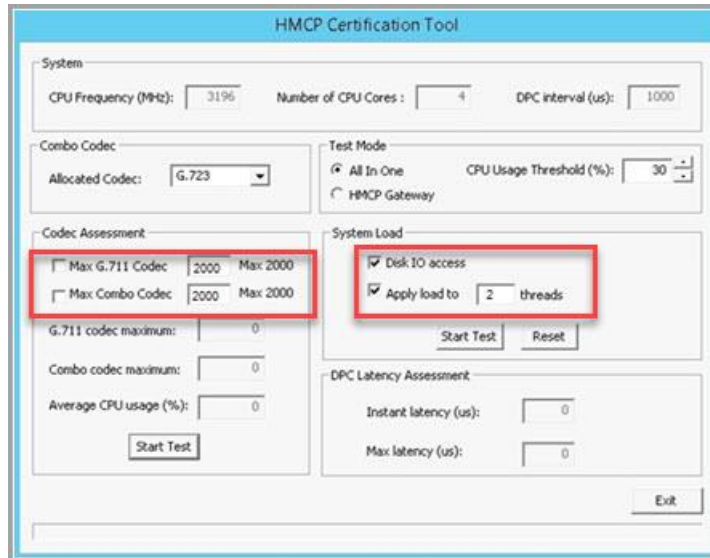
Step 2: Run the HMCP Certification Tool

You must determine if this system is appropriate for a Softswitch Deployment before you proceed with the full installation.

If the system has sufficient resources to pass the *DPC Latency* test, you will then perform a second assessment to determine the optimal codec maximum settings.

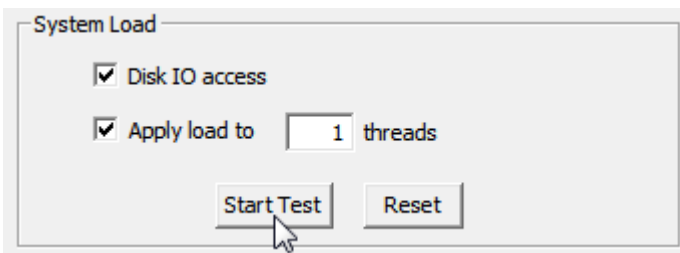
Perform the DPC Latency Test – Pass/Fail

1. After the system restarts, stop all AltiGen switching services.
2. In Windows, click **Start > All Programs**. Right-click **AltiGen HMCP Certification Tool** and select **Run as administrator**.



The screenshot shows the HMCP Certification Tool interface. The 'System' section at the top has fields for CPU Frequency (MHz) set to 3196, Number of CPU Cores set to 4, and DPC interval (us) set to 1000. The 'Combo Codec' section has 'Allocated Codec' set to G.723. The 'Test Mode' section has 'All In One' selected and 'CPU Usage Threshold (%)' set to 30. The 'Codec Assessment' section has two checkboxes: 'Max G.711 Codec' and 'Max Combo Codec', both with values of 2000 and 'Max 2000'. The 'System Load' section has 'Disk IO access' and 'Apply load to' checked, with 'Apply load to' set to 2 threads. The 'DPC Latency Assessment' section has 'Instant latency (us)' and 'Max latency (us)' both set to 0. There are 'Start Test' and 'Reset' buttons in the 'System Load' section, and an 'Exit' button at the bottom right.

3. Clear both of the checkboxes in the *Codec Assessment* section.
4. In the *Test Mode* section, select **All In One**.
5. In the *System Load* section:
 - a. Check the **Disk IO access** option.
 - b. Check the **Apply load to** option. For the number of threads parameter, enter a value that is half of the number of CPU cores on this virtual machine. (If the number of cores is an odd number, round up.)
6. Click **Start Test** in that section.



The screenshot shows the 'System Load' section of the tool. It has two checked checkboxes: 'Disk IO access' and 'Apply load to'. The 'Apply load to' field is set to 1 threads. There are 'Start Test' and 'Reset' buttons at the bottom. A mouse cursor is pointing at the 'Start Test' button.

7. Run the test for two minutes. While the test is running, watch the DPC Latency Assessment *Instant latency values*. The *Instant latency* values should remain less than 4000 us most of the time.



The screenshot shows the 'DPC Latency Assessment' section. It has two input fields: 'Instant latency (us)' with a value of 275 and 'Max latency (us)' with a value of 1483. The 'Instant latency (us)' field is highlighted with a red box.

8. After two minutes have passed, click **Stop Test**. Record the results for *Max latency*.

9. Leaving the threads value the same, click **Start Test** to run the test a second time, and observe the *Instant latency* values again to see if the values remain below 4000 us most of the time.
10. After two minutes have passed, click **Stop Test**. Record the *Max latency* results of the second test.
 - If *Max latency* in both tests is less than 8000 us, then the system passes the DPC Latency test.
 - If *Max latency* in both tests is greater than 8000 us, then the system fails this test.
 - If *Max latency* in **only one** of the tests is greater than 8000 us, and the majority of the *Instant latency* values were less than 4000 us, then the system has passed this test. Otherwise, it fails the test.

Note: You can also see the *Instant latency* results in the log file *CertLog.txt* under the folder where the HMCP test tool was installed.

In the following example of test results, the *Instant DPC Latency* value is highlighted in red:

2015-06-17 09:09:11.167 (14.562500) Average CPU usage:13 (235/17)

2015-06-17 09:09:11.167 Int DpcLatency: 6985us, Max: 7812us.

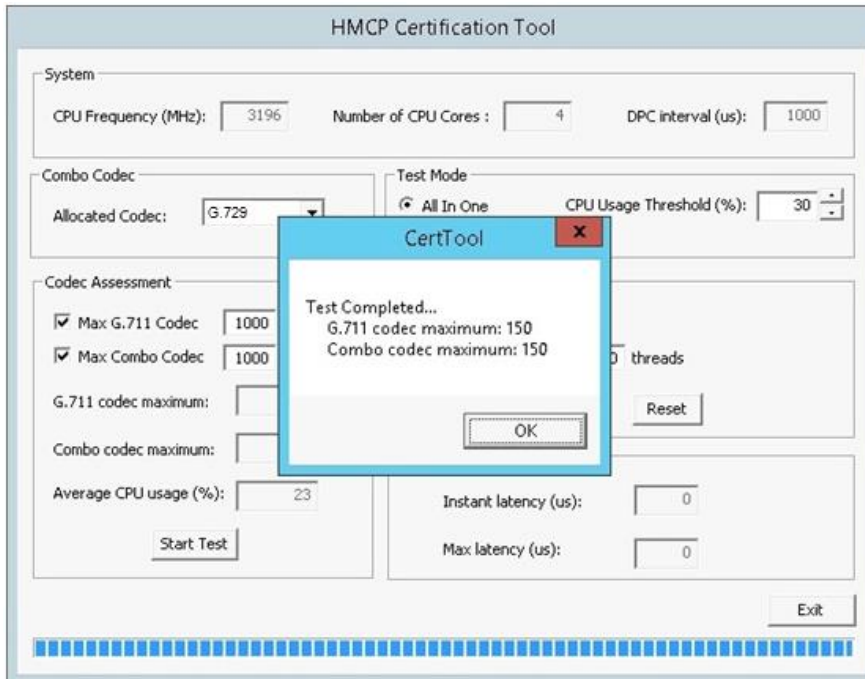
11. If the system has not passed the DPC Latency test, **do not proceed with the installation**. Restart the computer and contact your system administrator to optimize the DPC latency.
12. If the system passed the DPC Latency test, continue to the next section.

Determine Codec Maximum Quantities

Do not continue with these steps unless the system passed the *DPC Latency* tests.

1. In the *Codec Assessment* section, enter the maximum number of codecs in those two fields (enter 2000 for both Max G.711 and Max Combo)
2. In the *Test Mode* section, set *CPU Usage Threshold* to **30%**.
3. Click **Start Test** in the *Codec Assessment* section.
4. Record the number of supported G.711 and Combo codecs in the test results. Then enter those numbers in the *Max G.711 Codec* and *Max Combo Codec* fields (in the *Codec Assessment* section).
5. After the tool finishes this codec assessment, it shows the results. These values are the **maximum** quantities you should consider configuring. If you exceed these values, voice quality may start to degrade. Write down these values; you will need them on page 18, when you open MaxAdministrator and configure codec resources.

Example: If you enter G.729 for the *Combo Codec* and set the *CPU Usage Threshold* to 30%, the tool will determine the optimal combination of G.711_only and Combo channels in the HMCP server.



6. Click **OK** to close the results window.

Final Test with Codec Maximum Settings

Run a final test with the codec maximum values from the previous test.

1. In the *Test Mode* section, select **All In One**. Set *CPU Usage Threshold* to **60%**.
2. In the *System Load* section, use the settings that you tested with earlier:
 - Check the **Disk IO access** option.
 - Check the **Apply load to** option. For the number of threads parameter, enter a value that is half of the number of CPU cores on this virtual machine.
3. In the *Codec Assessment* section, check both options and enter the results for *Max. G.711 Codec* and *Max Combo Codec* from the previous test.
4. Click **Start Test** in the *System Load* section.
5. Just as you did on page 11, run the test for two minutes. While the test runs, closely monitor the *Instant latency* values, which should remain less than 4000 us most of the time.
6. After two minutes have passed, click **Stop Test**. Record the results for *Max latency*.
7. Click **Start Test** to run the test a second time, and observe the *Instant latency* values again to see if the values remain below 4000 us most of the time.
8. After two minutes have passed, click **Stop Test**. Record the *Max latency* results of the second test.

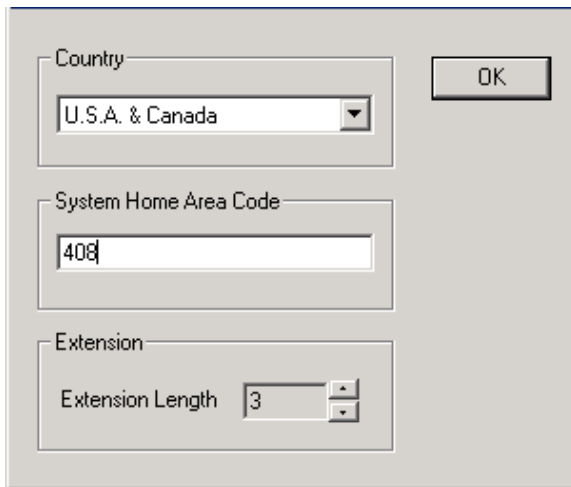
9. Click **OK** to close the results window.
 - If *Max latency* in both tests is less than 8000 us, then the system passes.
 - If *Max latency* in both tests is greater than 8000 us, then the system fails this test.
 - If *Max latency* in **only one** of the tests is greater than 8000 us, and the majority of the *Instant latency* values were less than 4000 us, then the system has passed this test. Otherwise, it fails the test.
10. If the system has not passed the DPC Latency test, **do not proceed with the installation**. Restart the computer and contact your system administrator to optimize the DPC latency.

If the system passed the DPC Latency test, click **Exit** to close the tool. Restart the system and continue to the next section, to install MaxCS.

Step 3: Install MaxCS

Next, you will re-run the MaxCS installation program.

1. Navigate to the *MaxCS ACM* folder. Double-click *Setup*. The installation wizard starts.
2. On the Welcome panel, close all Windows applications and click **Next**.
3. In the Setup Type panel, select **Softswitch System Installation**. Click **Next**.
4. On the next panel, select only the first two options, **Softswitch** (including VM and Enterprise Manager) and **HMCP Media Server**. Click **Next**.
5. The next few panels prompt you to accept the License Agreement, enter your user name and company, specify a password, and choose a folder for the installation. Provide the requested information and click **Next** in each panel.
6. When you are prompted about the registration file, choose **Register Later**.
7. When prompted, accept the default locations for the CDR database and the Post Office.
8. In the last panel, click **Install**.
9. If you are prompted to do so, install the software for KEYLOK, to support the soft system key: click **Install** and complete that installation process.
10. A warning indicates that you have not entered a system key. You will do this later; click **OK**.
11. When prompted, specify the country, the local area code for this server, and the number of digits you want for phone extensions. Click **OK**.



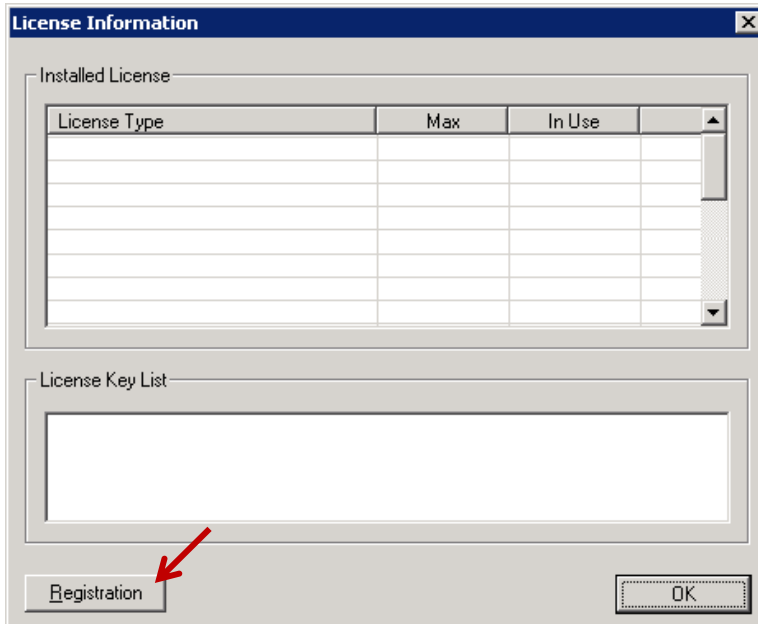
A screenshot of a configuration window. It has a light gray background and a thin border. On the right side, there is an 'OK' button. The main area contains three grouped input fields. The first group is labeled 'Country' and contains a dropdown menu with 'U.S.A. & Canada' selected. The second group is labeled 'System Home Area Code' and contains a text box with '408'. The third group is labeled 'Extension' and contains a text box with '3' and a small spinner control to its right.

12. A window shows you the password; click **OK**.
13. You are reminded to upgrade other components, click **OK**.
14. When you are prompted whether to restart the system, select **Yes, I want to restart my computer now**, and then click **Finish**. The server reboots.

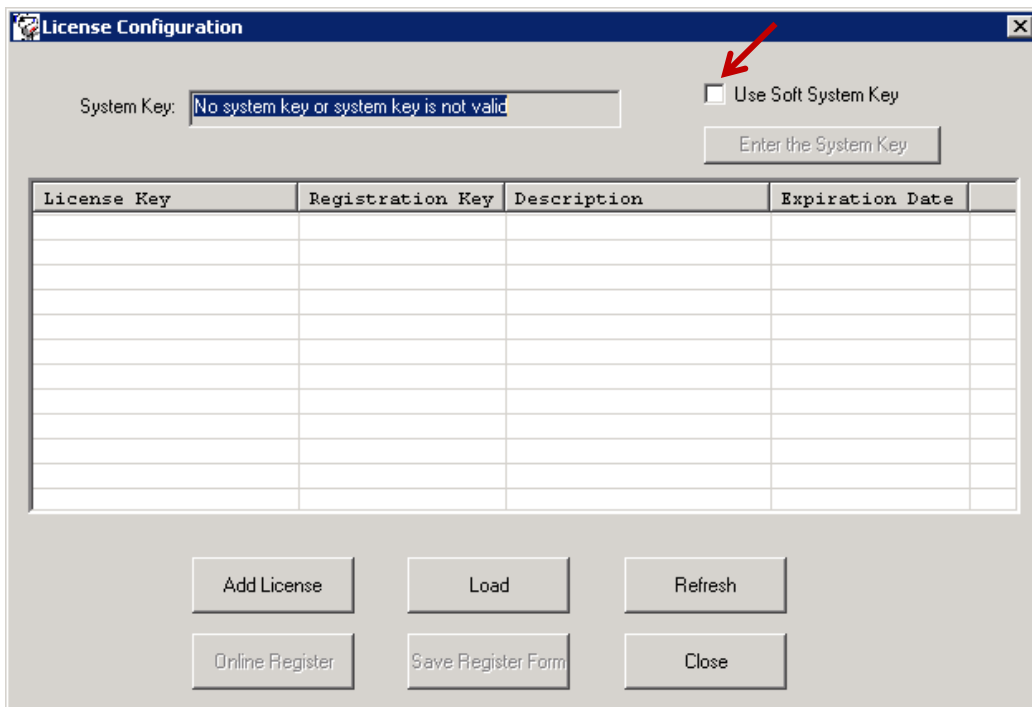
Step 4: Add the System Key

Next, you will add the client's System Key to MaxAdministrator.

1. In Windows, click **Start > All Programs > MaxCommunication Server > MaxAdministrator**.
2. In MaxAdministrator, choose the server.
3. When you are reminded that no system key has been provided, click **OK**.
4. Click the **Login** button and enter your password.
5. On the menu bar, choose **License > License Information**.
6. Click **Registration**.



7. In the License Configuration panel, check the option *Use Soft System Key*.
8. Click the **Enter the System Key** button.



9. Enter the System Key, which was provided by AltiGen. This string usually begins with the prefix “SS.” **You must enter this key in uppercase letters.** Click **OK**.
10. If you do not see the string in the field, click **Refresh**. The key will now appear in the System Key field.

Step 5: Register Licenses

Next, you will upload the license file(s) for this client.

1. In the License Configuration panel, click **Add License**.
2. Enter the **Softswitch Combo Base License** number and any other license numbers that you want to add.
3. If you have any Internet Explorer browsers windows open, close them at this point, and then click **Online Register**.
4. A new browser window opens. Click **Proceed to Online Registration**.
5. Log into the Partner site to view the *Assurance and Warranty* page.
6. On the first page, verify that the system configuration is correct. You can add more licenses here if you want to. Otherwise, click **Continue**.
7. On the next page, check **I have read and agree with the terms** to accept the **Assurance & warranty Agreement**, then click either **Continue With Price** or **Continue Without Price**.
8. Complete the contact information on the next page, and then click **Continue**.
9. View the *Assurance & Warranty Summary*, and then click **Continue Registration**.
10. On the final page, click **Download License Activation File** and save the EXCTL file somewhere on the server; you will load this file in step 13.
11. Close the web browser.
12. Return to the **License Configuration** window. In MaxAdministrator. Click **Load**.
13. Locate and load the EXCTL file that you downloaded in step 10.
14. The Softswitch Combo Base License should disappear, to be replaced by its component licenses.
15. Close the License Configuration window. Close the License Information window.
16. The licenses are now loaded; however, the virtual boards do not appear because the license files were not in place when switching was started. To force these boards to appear, restart switching. (Use Windows **Start > All Programs > MaxCommunication Server > Utilities > Start or Stop All AltiGen Services**.)

Step 6: Configure the HMCP Virtual Board

Next, you will configure the HMCP virtual board. An HMCP Media Server license is required to activate an HMCP virtual board.

License Type	Max	In Use
Gateway	8	1
HMCP Media Server	3	1
HMCP G.711/G.723/G.729 VPR	750	
HMCP MeetMe Conference	120	
HMCP Agent Supervision Session	60	
TAPI Seat	15	11

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.

1. In MaxAdministrator, open the Boards panel and double-click **HMCP**.

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

2. Click **Board Configuration**.

HMCP Resources <table border="1"> <thead> <tr> <th></th> <th>Licensed</th> <th>Total Assigned</th> <th>Assigned to This Board</th> </tr> </thead> <tbody> <tr> <td>Voice Processing Resource</td> <td></td> <td></td> <td></td> </tr> <tr> <td>G.711 only:</td> <td>200</td> <td>200</td> <td></td> </tr> <tr> <td>G.711 / G.722 / G.723 / G.729</td> <td>50</td> <td>50</td> <td>50</td> </tr> </tbody> </table>				Licensed	Total Assigned	Assigned to This Board	Voice Processing Resource				G.711 only:	200	200		G.711 / G.722 / G.723 / G.729	50	50	50	Parameters in IP header QoS assignment: IP TOS Byte Value(HEX): <input type="text" value="A0"/> DSCP Value(DEC): <input type="text" value="40"/> 802.1p Priority Value: <input type="text" value="0"/> TTL assignment:(for multicasting IP only) Time To Live (TTL) Byte Value(HEX): <input type="text" value="01"/>
	Licensed	Total Assigned	Assigned to This Board																
Voice Processing Resource																			
G.711 only:	200	200																	
G.711 / G.722 / G.723 / G.729	50	50	50																
Station Conference Maximum Bridge: 40 Members: <input type="text" value="40"/> <input type="text" value="40"/>			Codec Preference <input type="checkbox"/> Enable codec preference for all SIP trunk inbound and direct outbound calls Preferred Codec: <input type="text"/> Debug <input type="text"/> <input type="button" value="Send"/>																
MeetMe Conference Maximum Sessions: 20 Member: <input type="text" value="120"/> <input type="text" value="20"/> <input type="text" value="20"/>																			
Agent Supervision Bridge: <input type="text" value="50"/> <input type="text" value="20"/> <input type="text" value="20"/>																			
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>																			

3. In the **Assigned to This Board** fields, enter the codec values from the results of the HMCP Certification tool (refer back to page 12 as needed) and click **Apply**.

Note: Do not exceed the maximum numbers provided by the HMCP Certification Tool.

The next section describes the parameters in this dialog box.

4. After adjusting these values, you may need to reboot the system so that the changes can take effect.

HMCP Resources Parameters

This panel shows the total number licensed (if applicable), total currently assigned, and the number assigned to this HMCP board for Voice Processing Resources (VPR), station conference members, MeetMe conference members, and 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 - 200
- Station Conference Members - 120
- MeetMe Conference Members - 120
- Agent Supervision Bridges - 20

Important! When adding additional combo licenses, the system will 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. Please refer to the *MaxCS Administration Manual* Appendix "Network Ports" for instructions on how to identify these additional RTP ports.

- Codec G.722 is part of a combo codec and is controlled by license.
- 1,000 G.711 voice-processing resources will be licensed to the system when one HMCP Media Server license is registered.
- Do not assign more codecs than the system can support. Doing so can degrade system performance.
- The more VPRs you assign, the slower the system will be when it starts up. To calculate the optimized number of VPRs you need, use the following formula:
 - Total G.711 VPRs = Total number of local IP extensions
 - Total G.711/G.722/G.723/729 VPRs = Total number of remote IP phone users + Total Tie Trunk Channels that will use compressed codec

Parameters in IP Header

This panel is where you configure 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.

About Media Pass-Through Support

One enhancement that was provided beginning with MaxCS Release 8.5 for system performance and voice quality is the *Media Pass-through* feature.

While the Media Pass-through feature is enabled, the HMCP driver does not need to do encoding and decoding on both channels.

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.

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

Step 7: Configure HMCP Codec Preferences for SIP Trunk Calls

Note: An on-premise Softswitch deployment may not need this step unless the machine is low power.

MaxCS includes a feature designed to help you reduce the CPU consumption that occurs as 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.

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, the SIP device's codec configuration in *Enterprise Manager* will be ignored.

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

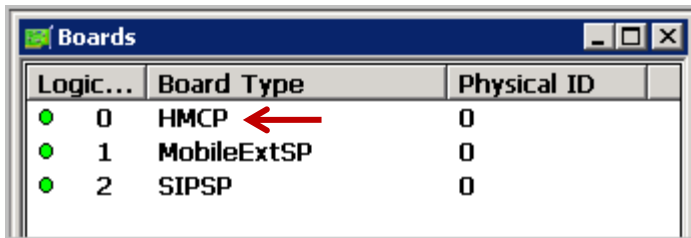
This codec preference applies to all SIP Trunk inbound calls and direct extension to SIP trunk outbound calls that are initiated from a phone or dialed via a MaxCS client.

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.

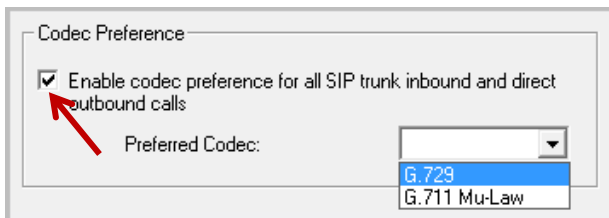
To configure this feature,

1. Log into MaxAdministrator with the superpassword. If you do not log in via the superpassword, then the feature will not be enabled.
2. Open the Boards panel and double-click **HMCP**.



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

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: G.729

G.711 Mu-Law

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.

Incoming Calls - 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.

Incoming Calls - 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.)

Outgoing Calls, 3 rd -Party IP Phones - 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.

Outgoing Calls, 3 rd -Party IP Phones - 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 the following logic for handling outgoing SIP trunk calls.

Outgoing Calls, IP Phones	
Preferred Codec	Codec Used for the Call
G.729	The system modifies the IP phone's codec in the RE-INVITE 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-INVITE 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.

Step 8: Configure the SIPSP Virtual Board

A VoIP connection typically consists of two parts.

Signal Channel – Sets up and tears down a call using protocol. SIP protocol is used in MaxCS to build a signal channel between the server and the IP phone.

Media Path – Encodes, transmits, and decodes voice for both parties.

The purpose of the virtual board 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.

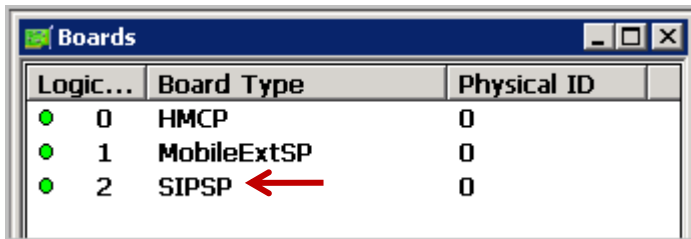
When an IP phone registers to the system, a channel ID will be assigned to the IP extension. However, these channels are only responsible for processing protocol and call control signals. They require a media path from a VoIP board or from the IP phone to establish a voice stream so that both sides can hear.

Notes

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

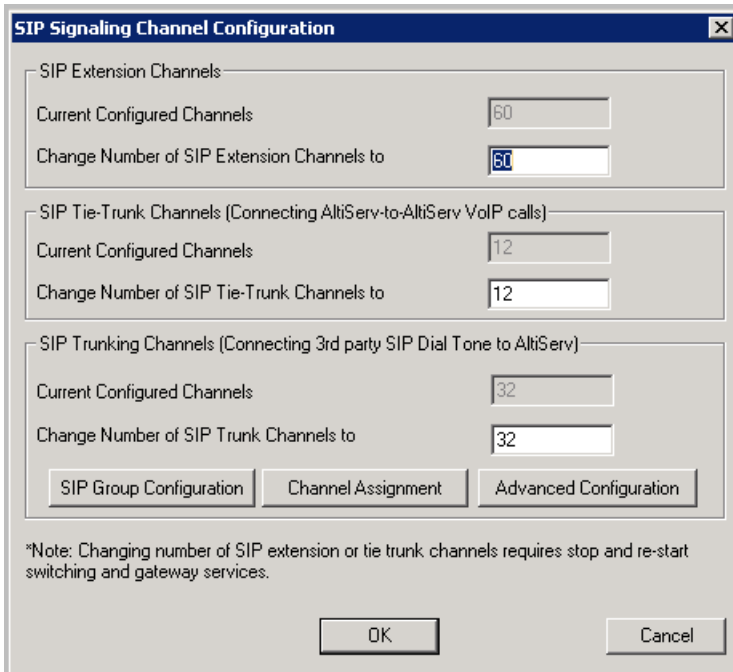
To configure the SIPSP board,

1. In MaxAdministrator, open the Boards panel and double-click **SIPSP**.



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

2. Click **Board Configuration**. The SIP Signaling Channel Configuration panel opens. This panel shows the number of configured channels and licensed channels.

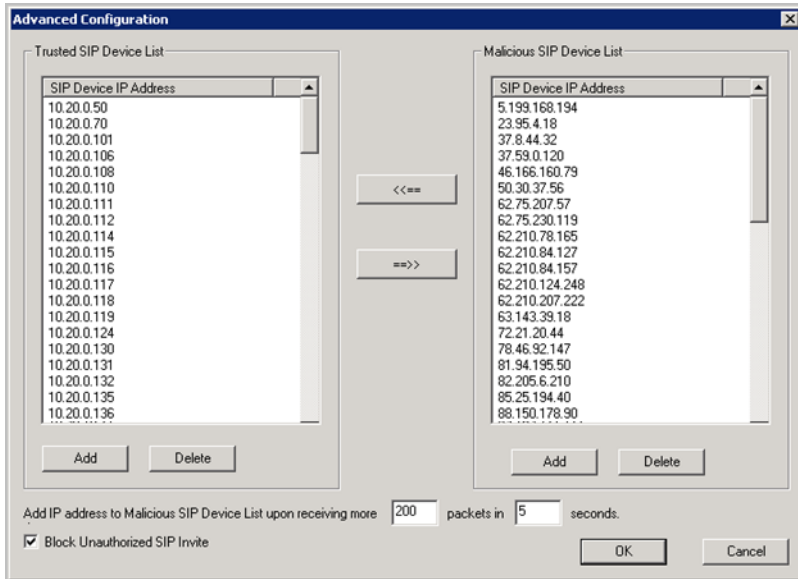


The dialog box is titled "SIP Signaling Channel Configuration". It contains three sections for configuring SIP channels:

- 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
 - Change Number of SIP Trunk Channels to: 32

At the bottom of the dialog, there are three buttons: "SIP Group Configuration", "Channel Assignment", and "Advanced Configuration". Below these buttons is a note: "*Note: Changing number of SIP extension or tie trunk channels requires stop and re-start switching and gateway services." At the very bottom are "OK" and "Cancel" buttons.

3. Adjust the number of SIP Extension channels, Tie-Trunk, and SIP Trunk channels as needed.
 By default, MaxCS is set to support 60 SIP extension channels. The maximum number possible depends of the system CPU performance, call volume, and usage.
 If you are using a high-performance machine as the Softswitch server, the number of channels can be more than 1000.
 Make sure that the system has enough voice processing resources. Calls can fail if there are not enough voice processing resources.
4. After you adjust these values, you must restart the switching and gateway services for this change to take effect. After the services restart, the new configuration will appear in the **Currently Configured Channels** fields.
5. After restarting the services, open MaxAdministrator, double-click **SIPSP** in the Boards panel and then click **Advanced Configuration** to manage the *Trusted SIP Device* list.
 To move an IP address from one list to the other, select the IP address and click either the right or left arrow button.



Step 9: Block Unauthorized SIP Invite Messages

You can perform this step now, or return and configure these settings later.

You can block unauthorized SIP invite messages; this setting is disabled by default.

When you enable the setting, SIP Invite requests are ignored if the IP address is not configured in one of the following places:

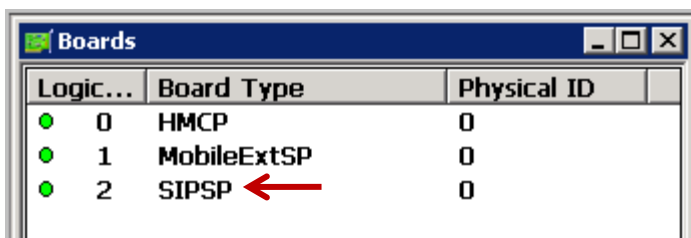
- SIP trunk
- IP dialing Table
- Trusted SIP Device List

IP extensions for the following devices are 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
- IPTalk

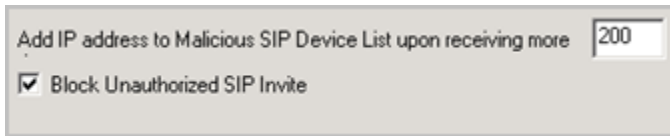
To enable protection,

1. In MaxAdministrator, open Boards view and double-click **SIPSP**.



2. Click **Board Configuration**, and then click **Advanced Configuration**.

3. Check *Block Unauthorized SIP Invite* and click **OK**.



Step 10: Configure the SIP Trunks

Next, you need to configure SIP trunk channels. Before you start, note the following:

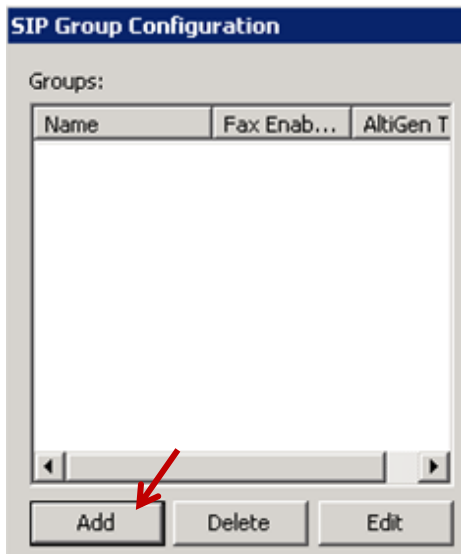
- If you are using AltiGen SIP Trunks, you may not need a license. For third-party SIP trunk providers, a SIP Trunk license is required for each SIP trunk.
- AltiGen does not guarantee the voice quality of the SIP dial tone coming from your service provider. You need to work with your data service and 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 SIP Trunk Configuration dialog box. Enter the service parameters for each SIP trunk channel configuration individually.

Note: Make sure that you have enough IP resource boards or that you configure enough HMCP voice processing resources to cover your needs.

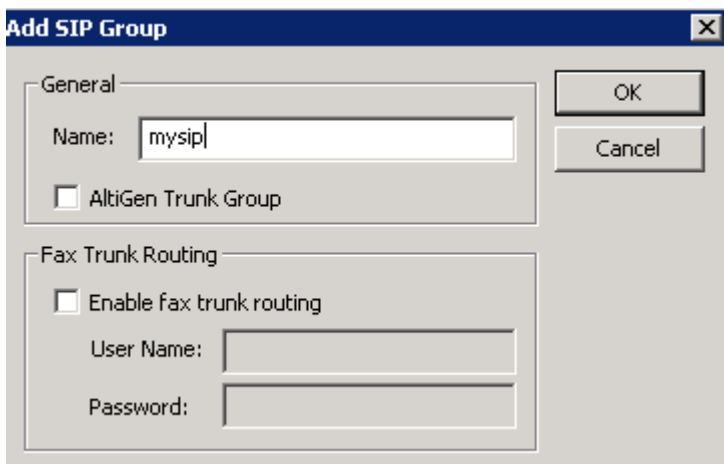
To configure a SIP trunk,

1. In MaxAdministrator, open the Boards panel and double-click **SIPSP**.
2. Click the **Board Configuration** button. Click the **SIP Group Configuration** button.
3. Under *SIP Group Configuration*, click the **Add** button to add a SIP group.

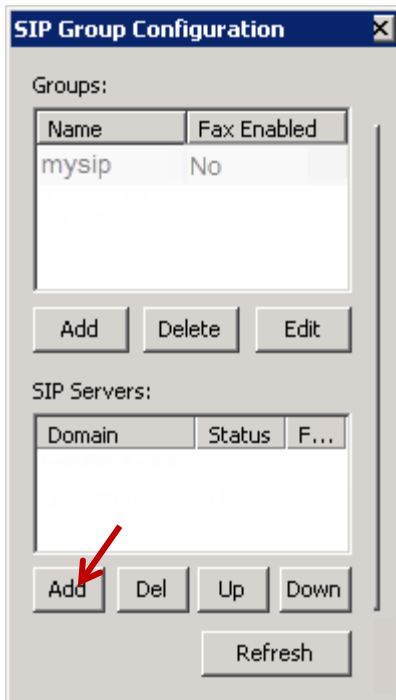


4. Enter a name for this SIP group.
5. If you are using Altigen SIP Trunks, check the **Altigen Trunk Group** option to waive the SIP trunk license requirement.

(If you check this option but are actually using a third-party SIP Trunk, the SIP Trunk will not work.)



6. Highlight the new SIP group (in our example, it is named *mysip*) and click the lower **Add** button (the one that is below the SIP Servers list) to add a sip server to the group. You can add one or more redundant SIP servers, if your service provider has redundant SIP servers.



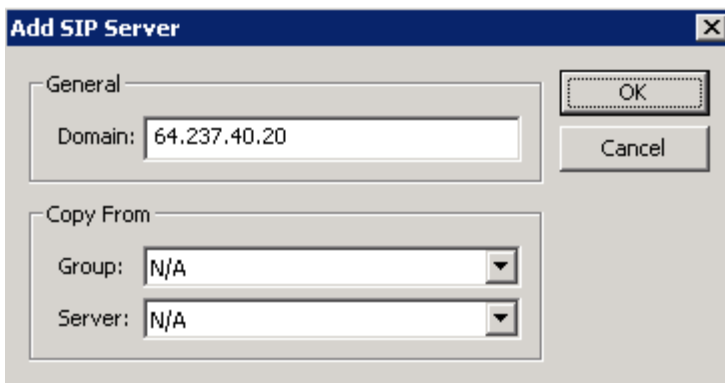
The SIP Group Configuration dialog box contains two main sections. The 'Groups' section has a table with columns 'Name' and 'Fax Enabled'. It lists a group named 'mysip' with 'Fax Enabled' set to 'No'. Below the table are 'Add', 'Delete', and 'Edit' buttons. The 'SIP Servers' section has a table with columns 'Domain', 'Status', and 'F...'. Below this table are 'Add', 'Del', 'Up', and 'Down' buttons, with a red arrow pointing to the 'Add' button. A 'Refresh' button is located at the bottom center.

Name	Fax Enabled
mysip	No

Domain	Status	F...
--------	--------	------

Buttons: Add, Delete, Edit, Refresh, Add, Del, Up, Down

7. Enter the URL for the domain. Click **OK**.



The Add SIP Server dialog box has two sections. The 'General' section contains a 'Domain' text field with the value '64.237.40.20'. The 'Copy From' section contains two dropdown menus: 'Group' with the value 'N/A' and 'Server' with the value 'N/A'. 'OK' and 'Cancel' buttons are on the right.

General

Domain: 64.237.40.20

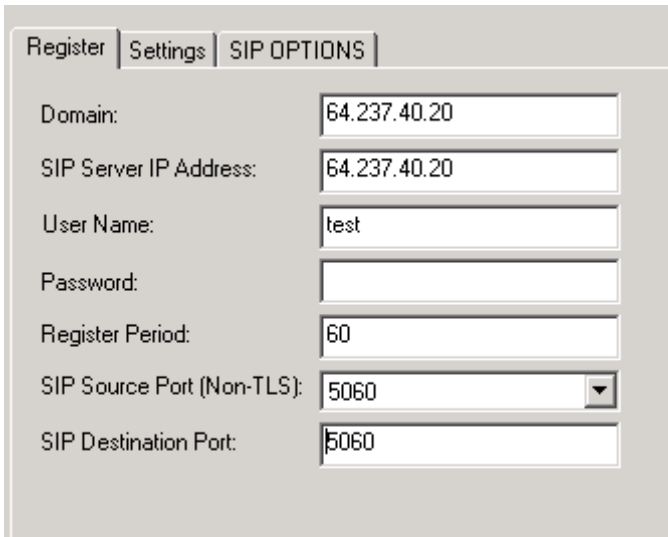
Copy From

Group: N/A

Server: N/A

Buttons: OK, Cancel

8. Highlight the SIP group and then highlight the SIP server that you just added.

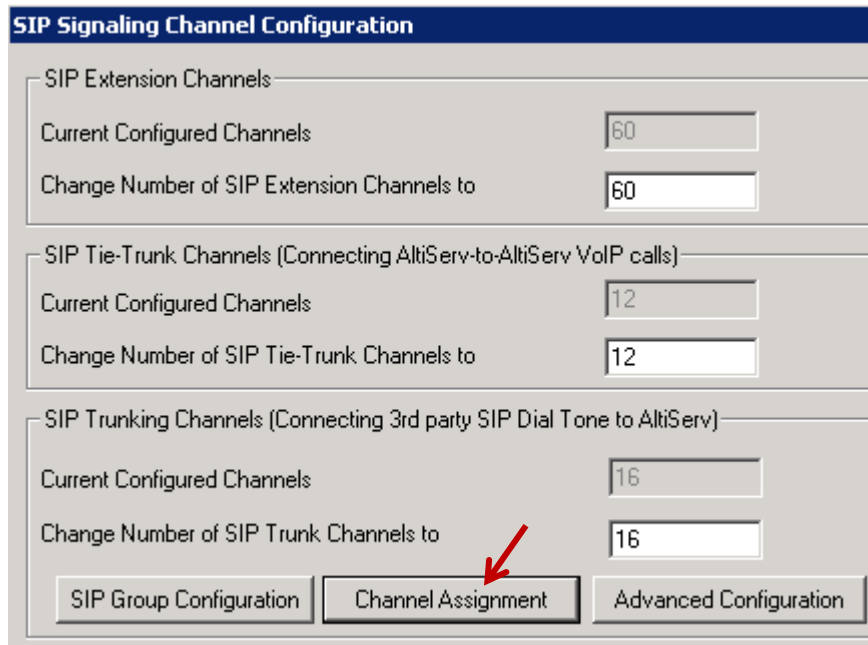


Field	Value
Domain:	64.237.40.20
SIP Server IP Address:	64.237.40.20
User Name:	test
Password:	
Register Period:	60
SIP Source Port (Non-TLS):	5060
SIP Destination Port:	5060

9. On the *Register* tab, enter the parameters as follows.

- Domain – The Domain Name of the SIP Trunk service provider. For some service provider, it can be the same as SIP Server IP Address.
- SIP Server IP Address – The SIP Trunk service provider's server IP address.
- User Name – Assigned by the SIP Trunk service provider.
- Password – Assigned by the SIP Trunk service provider.
- SIP Register Period – How frequently the Altigen system needs to send SIP registration packets to the service provider or the SIP gateway. 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 – 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. Port 10060 is recommended, if the service provider supports it.
- SIP Destination Port – A SIP Trunk can have different source port and destination port.

10. Click **Channel Assignment** to assign channels to the SIP Group that you just configured.



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

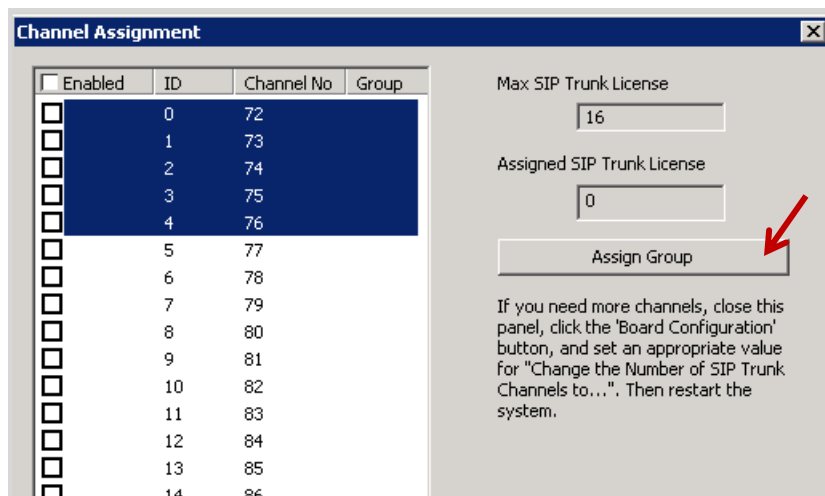
SIP Trunking Channels (Connecting 3rd party SIP Dial Tone to Altiserv)

Current Configured Channels: 16

Change Number of SIP Trunk Channels to: 16

SIP Group Configuration | **Channel Assignment** | Advanced Configuration

11. Highlight the trunk channels and press **Assign Group** to assign them to the SIP Trunk group. License usage will be automatically updated. SIP trunk service provided by Altigen does not require license when Altigen SIP trunk group is checked.



Channel Assignment

Enabled	ID	Channel No	Group
<input type="checkbox"/>	0	72	
<input type="checkbox"/>	1	73	
<input type="checkbox"/>	2	74	
<input type="checkbox"/>	3	75	
<input type="checkbox"/>	4	76	
<input type="checkbox"/>	5	77	
<input type="checkbox"/>	6	78	
<input type="checkbox"/>	7	79	
<input type="checkbox"/>	8	80	
<input type="checkbox"/>	9	81	
<input type="checkbox"/>	10	82	
<input type="checkbox"/>	11	83	
<input type="checkbox"/>	12	84	
<input type="checkbox"/>	13	85	
<input type="checkbox"/>	14	86	

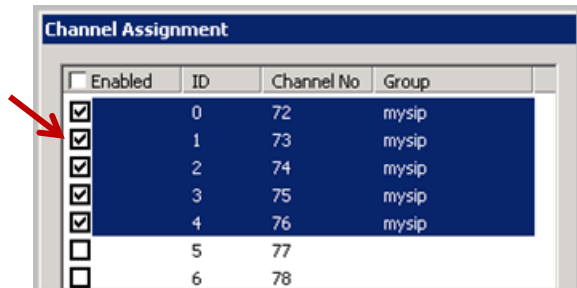
Max SIP Trunk License: 16

Assigned SIP Trunk License: 0

Assign Group

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.

12. Highlight these SIP trunk channels and check their boxes to enable them.



Enabled	ID	Channel No	Group
<input checked="" type="checkbox"/>	0	72	mysip
<input checked="" type="checkbox"/>	1	73	mysip
<input checked="" type="checkbox"/>	2	74	mysip
<input checked="" type="checkbox"/>	3	75	mysip
<input checked="" type="checkbox"/>	4	76	mysip
<input type="checkbox"/>	5	77	
<input type="checkbox"/>	6	78	

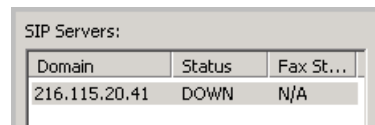
13. In Enterprise Manager, add the SIP Trunk service provider's IP address to the IP Device Range (on the **Servers** > **IP codec** tab) and select the proper codec profile for this service.

If you omit this step, then calls may have no audio even if the SIP Trunk channel shows the call is connected.

Step 11: Enable SIP Option (optional)

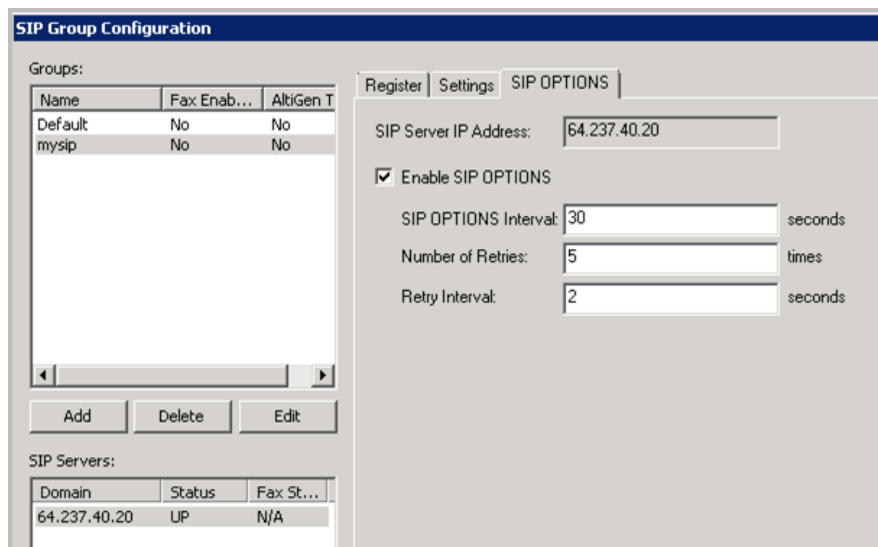
SIP Option is a keepalive message to check the SIP server's availability.

If the server or network between the SIP server and MaxCS is down. MaxCS will mark the server as down if either SIP registration or SIP Option fails. If all SIP servers with in the same SIP group are down, the all the trunks associated with the SIP group will become not ready and the status in the list will show as DOWN.



Domain	Status	Fax St...
216.115.20.41	DOWN	N/A

1. Highlight the SIP Group and then highlight the SIP Server.
2. Switch to the *SIP OPTIONS* tab.



Name	Fax Enab...	Altigen T
Default	No	No
mysip	No	No

Register Settings **SIP OPTIONS**

SIP Server IP Address: 64.237.40.20

☒ Enable SIP OPTIONS

SIP OPTIONS Interval: 30 seconds

Number of Retries: 5 times

Retry Interval: 2 seconds

Add Delete Edit

Domain	Status	Fax St...
64.237.40.20	UP	N/A

You can enable or disable *SIP OPTIONS* independently for each SIP Server. By default, the *SIP Options* feature is disabled.

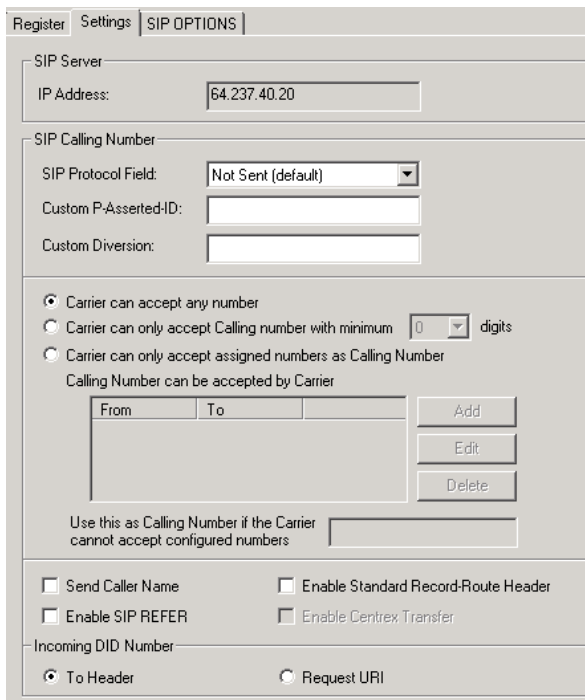
3. Configure the parameters as follows, and click **OK**.

- SIP Server IP Address – The IP address for this SIP Server.
- Enable SIP OPTIONS – Enable or disable this feature for the selected SIP Trunk group.
- 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 MaxCS 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 MaxCS 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.

Step 12: SIP Trunk Setting

Different SIP service providers may have different settings such as supporting different ways of sending a caller ID and so on. These options are found in the SIP server's *Settings* tab.

1. Highlight the SIP group and then highlight the SIP server in that group (this allows you to configure the server).



The screenshot shows the 'SIP OPTIONS' configuration window. It has tabs for 'Register', 'Settings', and 'SIP OPTIONS'. The 'SIP OPTIONS' tab is active. The window contains the following sections:

- SIP Server:** IP Address: 64.237.40.20
- SIP Calling Number:**
 - SIP Protocol Field: Not Sent (default)
 - Custom P-Asserted-ID:
 - Custom Diversion:
- Carrier can accept any number:**
 - ☒ 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: Add Edit Delete
- Use this as Calling Number if the Carrier cannot accept configured numbers:**
- Checkboxes:**
 - ☐ Send Caller Name
 - ☐ Enable Standard Record-Route Header
 - ☐ Enable SIP REFER
 - ☐ Enable Centrex Transfer
- Incoming DID Number:**
 - ☒ To Header
 - ☐ Request URI

2. Edit the fields as necessary and click **OK**. (Refer to the following table for descriptions of these fields).

SIP Trunk Profile Field	Description
SIP Protocol Field	<p>Not Sent (default) – Do not send transmitted caller ID</p> <p>FROM Header – Send the caller ID using the SIP FROM header</p> <p>P-Preferred Identity – Send the caller ID using the SIP P-Preferred Identity header</p> <p>P-Asserted Identity – Send the caller ID using the SIP P-Asserted Identity header</p>
Carrier can accept any number	This is the default.
Carrier can only accept Calling Number with minimum x digits	Enter the number of digits, and 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 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 the 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]
Incoming DID Number Field	When a call comes in, the SIP trunk uses To Header or Request URI as the DID/DNIS number
Enable Fax Trunk Routing	<p>This feature is supported on Altigen SIP trunks only.</p> <p>If the extension is a fax extension and <i>Fax Trunk routing</i> is checked, that means the SIPSP should use the Fax Username and Fax password of SIP Trunk profile instead of regular username and password of SIP Trunk to negotiate with the SIP Trunk.</p> <p>If the extension is a fax extension but <i>Fax Trunk routing</i> is unchecked, that means the SIPSP should use the regular username and password of the SIP Trunk to negotiate with the SIP Trunk side.</p> <p>Fax User Name – The user name for fax routing</p> <p>Fax Password – The password for fax routing</p>

Step 13: Configure a Codec Profile

Next, configure a Codec Profile for the SIP trunks in Enterprise Manager:

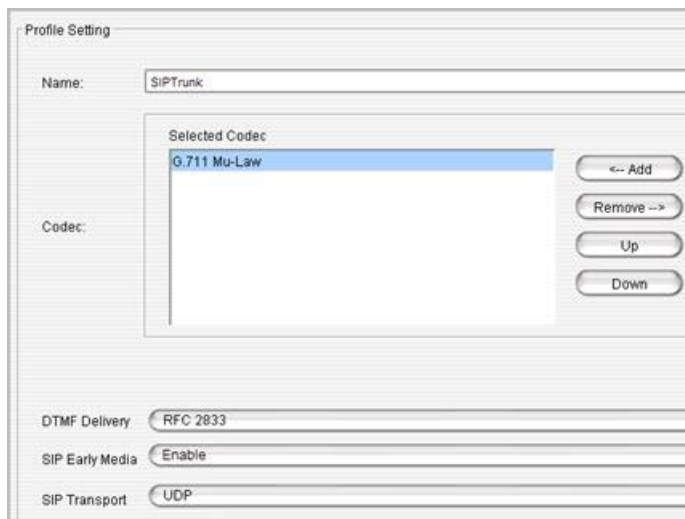
1. In MaxAdministrator, select **VoIP > Enterprise Network Manager**.

2. Click the **Codec** button on the *Quick Launch* bar (this is different from the *IP Codec* tab).
3. Check whether a profile named *SIPTrunk* has been preconfigured for you.

If it has already been configured, confirm that the settings are correct.

If this profile was not preconfigured, click **Add** and create a profile with the following parameters:

- For the name, enter **SIPTrunk**.
- Set the *Selected Codec* to **G.711 Mu-Law** (use the **Add** and **Remove** buttons as needed)
- Set *DTMF Delivery* to **RFC 2833**
- Set *SIP Early Media* to **Enable**
- Set *SIP Transport* to **UDP**
- Click **Advanced** and set both packet lengths to **20 ms**



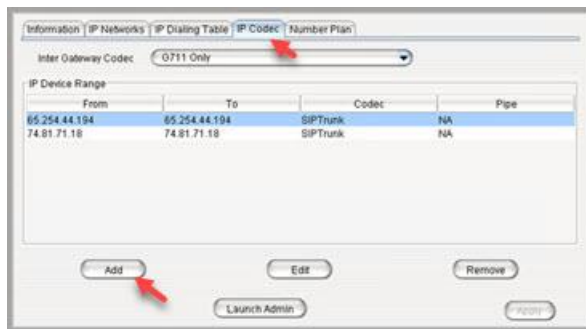
The screenshot shows the 'Profile Setting' dialog box. The 'Name' field is filled with 'SIPTrunk'. Below it, the 'Selected Codec' list contains 'G.711 Mu-Law'. To the right of the list are buttons for '<-- Add', 'Remove -->', 'Up', and 'Down'. At the bottom, there are three rows of settings: 'DTMF Delivery' set to 'RFC 2833', 'SIP Early Media' set to 'Enable', and 'SIP Transport' set to 'UDP'.

Step 14: Assign the Codec Profile to the Two SIP Servers

Next, assign the *SIPTrunk* Codec Profile to the two SIP trunk servers.

1. In Enterprise Manager, click the **Servers** button on the Quick Launch bar.
2. Open the **IP Codec** tab.
3. Determine whether the following servers were preconfigured for you:
 - 65.254.44.194
 - 74.81.71.18
4. If these servers were preconfigured for you, confirm that each server is assigned to the Codec Profile *SIPTrunk*.

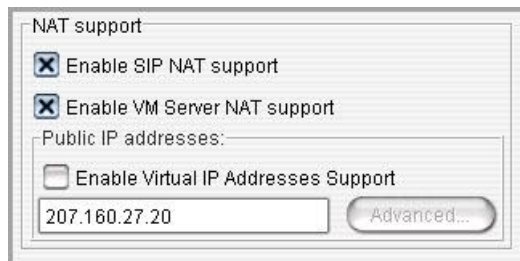
If they were not preconfigured for you, click **Add**, add the first server, and set the Codec Profile to *SIPTrunk*. Repeat for the second server.



Step 15: Configure NAT

To confirm that NAT support has been configured,

1. Click the **IP Networks** tab and confirm that both of the NAT support checkboxes are selected. If they have not been selected, check both boxes.



2. Close *Enterprise Manager*.

Step 16: AltiGen SIP Trunk Configuration

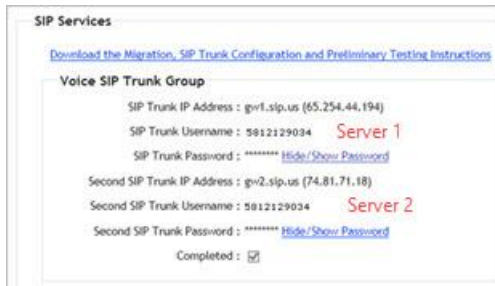
Note: These steps apply **only** to deployments that are using AltiGen SIP Trunks. Before you begin, retrieve the configuration details from the MaxCS Private Cloud portal, in the *SIP Services* section of the *General* tab of your account.

If your deployment uses SIP services from another AltiGen-certified SIP Trunk carrier, you will need to get the specific configuration details from that provider. Configuration details will vary from one provider to another.

You will begin by configuring the *first* server.

Configure the First Server

1. Log into the MaxCS Cloud portal and retrieve the details on the *General* tab of your account.



SIP Services

[Download the Migration, SIP Trunk Configuration and Preliminary Testing Instructions](#)

Voice SIP Trunk Group

SIP Trunk IP Address : gvl1.sip.us (65.254.44.194)

SIP Trunk Username : 5812129034 **Server 1**

SIP Trunk Password : ***** [Hide/Show Password](#)

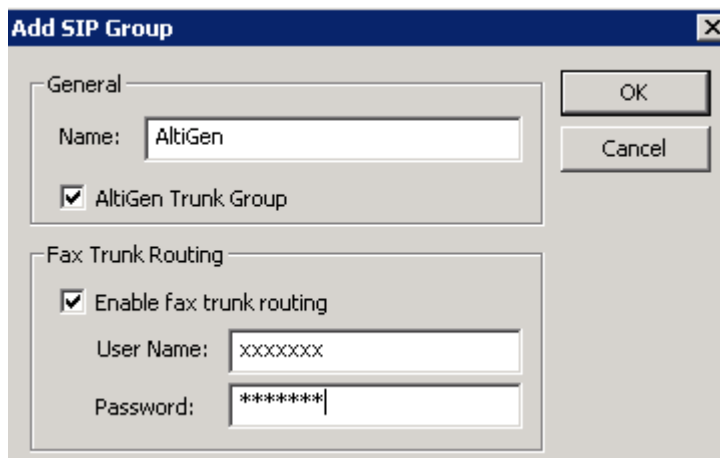
Second SIP Trunk IP Address : gv2.sip.us (74.81.71.18)

Second SIP Trunk Username : 5812129034 **Server 2**

Second SIP Trunk Password : ***** [Hide/Show Password](#)

Completed : ☒

2. Switch back to MaxAdministrator. You should be in the *SIP Group Configuration* page. If not, open it now.
3. Add a SIP Group for the AltiGen SIP trunk. In our example, it is named it *AltiGen*.
 - Check the option **AltiGen Trunk Group**.
 - If you also have a Fax Trunk account, check the **Enable fax trunk routing** option and enter the user name and password. (If you do not have a Fax Trunk account, or if you are not sure, leave this option unchecked. You can configure it later as needed.)



Add SIP Group

General

Name:

☒ AltiGen Trunk Group

Fax Trunk Routing

☒ Enable fax trunk routing

User Name:

Password:

OK

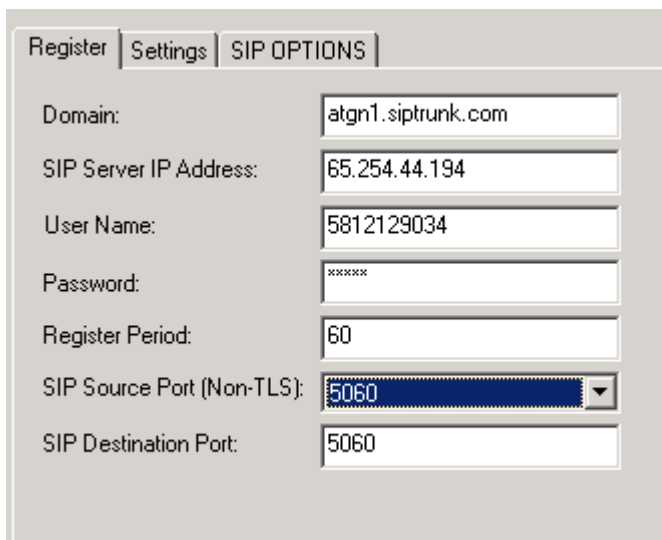
Cancel

4. Highlight the SIP group that you just created and add the first AltiGen SIP server (Server 1). The domain is *atgn1.siptrunk.com*.



The 'Add SIP Server' dialog box has a title bar with a close button. It contains two sections: 'General' and 'Copy From'. The 'General' section has a 'Domain' text field with the value 'atgn1.siptrunk.com'. The 'Copy From' section has two dropdown menus: 'Group' and 'Server', both showing 'N/A'. To the right of these sections are 'OK' and 'Cancel' buttons.

5. After you add this server, switch to the Register tab on the right and configure the parameters as follows:



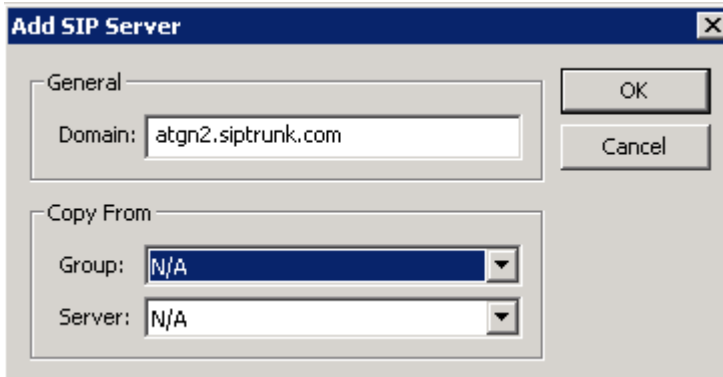
The 'Register' tab configuration form has three tabs: 'Register', 'Settings', and 'SIP OPTIONS'. The 'Register' tab is active. It contains the following fields: 'Domain' (atgn1.siptrunk.com), 'SIP Server IP Address' (65.254.44.194), 'User Name' (5812129034), 'Password' (masked with asterisks), 'Register Period' (60), 'SIP Source Port (Non-TLS)' (5060), and 'SIP Destination Port' (5060).

- For Domain, enter *atgn1.siptrun.com*.
- For *SIP Server IP Address*, enter the SIP Trunk IP address of the first SIP trunk server: 65.254.44.194.
- For *User Name*, enter the *SIP Trunk Username* number (from the order in the MaxCS Private Cloud portal). In our example, this username is 5812129034.
- For *Password*, enter the *SIP Trunk Password* (from the order in the Cloud Services portal). Click **Hide/Show Password** to see it.
- Set the *Register Period* to 60.
- Set *SIP Source Port (Non-TLS)* to **5060**.
- Set *SIP Destination Port* to **5060**.

Configure the Second Server

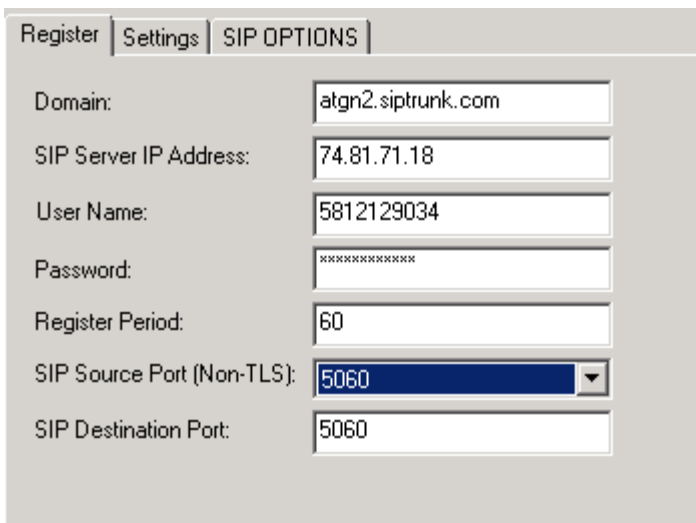
Next, configure the second server.

1. Highlight the SIP group Altigen, and add the first Altigen SIP server (Server 2). The domain is *atgn2.siptrunk.com*.



The 'Add SIP Server' dialog box has a title bar with a close button. It contains two sections: 'General' and 'Copy From'. In the 'General' section, the 'Domain' field is populated with 'atgn2.siptrunk.com'. To the right of this section are 'OK' and 'Cancel' buttons. The 'Copy From' section contains two dropdown menus: 'Group' and 'Server', both of which are currently set to 'N/A'.

2. In the *Register* tab, configure these parameters for this second server:



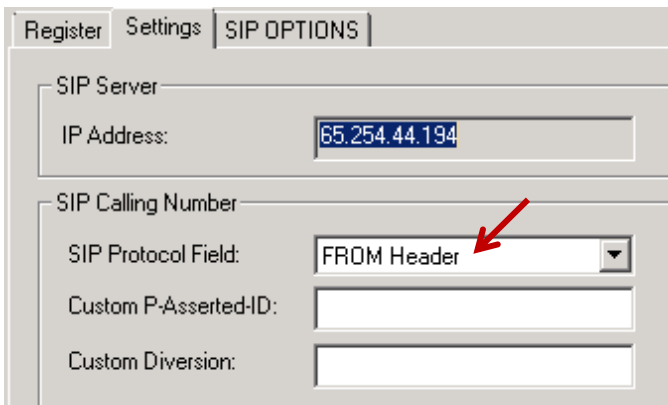
The 'Register' tab configuration form has three tabs: 'Register', 'Settings', and 'SIP OPTIONS'. The 'Register' tab is active. It contains the following fields: 'Domain' (atgn2.siptrunk.com), 'SIP Server IP Address' (74.81.71.18), 'User Name' (5812129034), 'Password' (masked with asterisks), 'Register Period' (60), 'SIP Source Port (Non-TLS)' (5060), and 'SIP Destination Port' (5060).

- For Domain, enter *atgn2.siptrunk.com*.
- For *SIP Server IP Address*, enter the SIP Trunk IP address of the second SIP trunk server: 74.81.71.18.
- For *User Name*, enter the *SIP Trunk Username* number (from the order in the MaxCS Private Cloud portal). In our example, this username is 5812129034.
- For *Password*, enter the *SIP Trunk Password* (from the order in the Cloud Services portal). Click **Hide/Show Password** to see it.
- Set the *SIP Register Period* to 60.
- Set *SIP Source Port* to **5060**.
- Set *SIP Destination Port* to **5060**.

Enable Channels

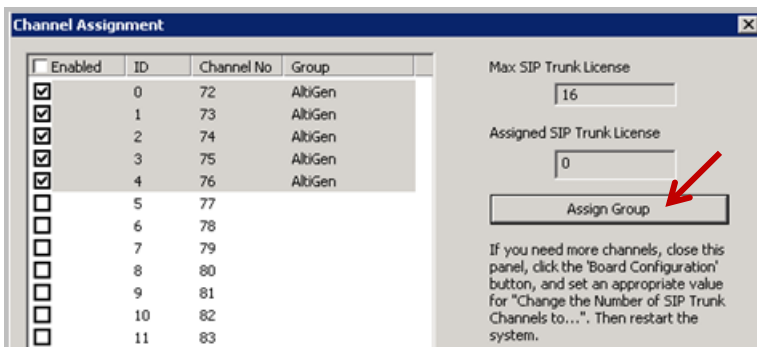
1. For **Server 1**, open the *Settings* tab and change *SIP Protocol Field* to **From Header**.

2. Repeat this step for **Server 2**, setting *SIP Protocol Field* to **From Header**.



The image shows the 'SIP OPTIONS' tab in a configuration window. The 'SIP Server' section has an 'IP Address' field with the value '65.254.44.194'. The 'SIP Calling Number' section has a 'SIP Protocol Field' dropdown menu set to 'FROM Header', indicated by a red arrow. Below it are empty text boxes for 'Custom P-Asserted-ID' and 'Custom Diversion'.

3. Open the *Channel Assignment* window.
4. Highlight multiple SIP trunk channels and then click **Assign Group**. Assign them to the AltiGen SIP Group. Make sure that those channels remain highlighted, and check one of their check boxes. This should enable all of the selected channels.



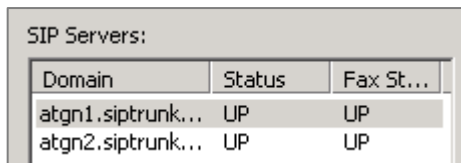
The image shows the 'Channel Assignment' window. On the left is a table with columns: Enabled, ID, Channel No, and Group. The first four rows (ID 0-4) are highlighted, and the 'Enabled' checkbox for ID 0 is checked. On the right, the 'Max SIP Trunk License' is set to 16 and the 'Assigned SIP Trunk License' is set to 0. A red arrow points to the 'Assign Group' button. Below the button is a note: '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.'

Enabled	ID	Channel No	Group
<input checked="" type="checkbox"/>	0	72	AltiGen
<input checked="" type="checkbox"/>	1	73	AltiGen
<input checked="" type="checkbox"/>	2	74	AltiGen
<input checked="" type="checkbox"/>	3	75	AltiGen
<input checked="" type="checkbox"/>	4	76	AltiGen
<input type="checkbox"/>	5	77	
<input type="checkbox"/>	6	78	
<input type="checkbox"/>	7	79	
<input type="checkbox"/>	8	80	
<input type="checkbox"/>	9	81	
<input type="checkbox"/>	10	82	
<input type="checkbox"/>	11	83	

Check Your Configuration

To confirm that your configuration is correct,

1. Look in the SIP Group Configuration window. The status for both servers should show as UP.



The image shows the 'SIP Servers' section of a configuration window. It contains a table with columns: Domain, Status, and Fax St... (likely Fax Status).

Domain	Status	Fax St...
atgn1.siptrunk...	UP	UP
atgn2.siptrunk...	UP	UP

2. In Trunk view, these trunks should show as Idle.

Trunk View		
Reset		
Location	Type	Status
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-AltiGen	idle
02:0073	SIP-AltiGen	idle
02:0074	SIP-AltiGen	idle
02:0075	SIP-AltiGen	idle
02:0076	SIP-AltiGen	idle

Step 17: Configure Inbound Routing

Carriers send 11 digits as DNIS; configure your inbound routing rules accordingly.

Step 18: Configure Out-Call Routing

Configure out-call routing as appropriate for your system. Refer to the *MaxCS Administration Manual* for details and instructions.

Step 19: System Configuration

At this point, calls should come into the system. Your next steps are to configure out-call routing and other internal processing rules.

Refer to the *MaxCS Administration Manual* for instructions:

- Chapter 4, System Configuration
- Chapter 26, Enterprise Manager

Step 20: Configure Polycom Phones

If the organization has Polycom phones, refer to the *MaxCS Polycom Phone Configuration Guide* for instructions on how to configure those IP phones. This document is available in the AltiGen Knowledge Base.

Note: Beginning with MaxCS Release 8.5, the process of configuring Polycom phones is very different from the process that was used in earlier releases.

Step 21: Enforce TLS 1.2 (optional)

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*.

This option only enables TLS 1.2 *on the SIP/TLS layer*. If you also want to enforce TLS 1.2 on Windows Server, you must get a public certificate and import it via MaxAdministrator (**System > Import Certificate**).

Note: 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 in your environment 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:

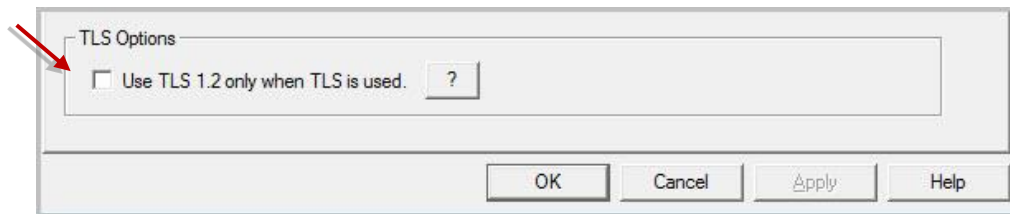
- Third-party gateways
- SIP trunk service providers (Note that Altigen SIP trunks support TLS1.2; if you require TLS/SRTP on Altigen SIP trunks, contact Altigen Support to coordinate that configuration change)

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**.



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.

Altigen Technical Support

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



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

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

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

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

Please be ready to supply the following information:

- Partner ID
- AltiGen Certified Engineer ID
- AltiWare or MaxCS version number
- Server model
- The telephone number where you can be reached