



MAX Communication Server Server Release 9.0.1

New Features Guide

May 2021



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

www.altigen.com

Copyright © Altigen Communications, Inc. 2021. All rights reserved.



Contents

About This Guide	5
Requirements	5
Installation Procedures.....	5
MaxCS 9.0 Update1	5
MaxCommunicator Web	5
Service Hub	6
Standalone MeetMe Application.....	6
AltiReport Integrated with Service Hub.....	6
Update Management Studio (UMS)	6
Unassigned Extension Routing	6
DNIS Range	9
DNIS Routing.....	10
APC Activity Monitoring	11
IPTalk Custom Ring Tone	12
IPTalk Ring Tone When Non-Default Ring-Through Device Selected	12
IPTalk Incoming Call Popup.....	12
Password Security Policy	14
Busy Trunk Queuing.....	15
Displaying Agent Read/Not Ready State Time Duration	16
TRUSTID	16
New Extension Field: UPN	16
Workgroup Queue Management Changes.....	17
Custom User Activity Option	17
Change FROM Header to Local IP Address	17
MaxAgent IPTalk Hold Options.....	17
Workgroup Queue Hold Option	17
Double Hold Option	18
Call Answer Enhancements	18
Not Ready Reason Code With #91 Feature Code	19
Sending Extension's Transmitted CID When Calling Mobile Extension	19
Adjunct SIP Trunk	19



Disable Automatic Area Code Insertion for MaxClient.....	20
Regroup Abandoned to Voice Mail in MaxSupervisor and CDR Search	20
Added User Data Field in Call Entry in MaxCommunicator and MaxOutlook	20
Support “Apply” to Additional Extension Settings in MaxAdmin	20
AltiReport Enhancements.....	20
Polycom Firmware Support	20
SQL 2019.....	20
VMWare.....	20
Operational Notes and Limitations.....	21
Altigen Technical Support.....	21
Patch 8.6.1.216 Updates.....	21
New System Default Values.....	21
New Options for Extension Lockout Period.....	22
Extension Checker Updates in .216	23
Passwords Must Now Be Followed With #	23
Users Prompted to Change Password Upon Login	23
Transfer Calls over Tie-Trunks	24
Patch 8.6.1.215 Updates.....	25
Enhancements for the Trusted/Malicious SIP Device Lists.....	25
Password Configuration Enhancements.....	27
Patch 8.6.1.213 Updates.....	28
MaxSupervisor Updates	28
MaxAgent Updates	28

About This Guide

This guide is provided for the interim release of MaxCS Release 9.0.1.

It describes the enhancements that have been included since MaxCS Release 8.6.1. It documents changes that were included in various patches, builds, and QuickFix releases, including:

- [Patch 8.6.1.213 Updates](#)
- [Patch 8.6.1.215 Updates](#)
- [Patch 8.6.1.216 Updates](#)
- [MaxCS 9.0.1 Updates](#)

You should also refer to the various readme files to learn of any late-breaking changes or feature additions.

Requirements

MaxCS Release 9.0.1 is supported on Softswitch SaaS, Cloud, and on-premise; it is not supported on hardware chassis.

Notes:

- This release supports OpenJDK 8u262, Java 8 262b17, Tomcat 8.5.57.
- This release supports Polycom VVX firmware version 5.9.3.2489.
- This release supports SQL 2019.

Installation Procedures

Release 9.0 supports:

- A new installation of MaxCS
- An upgrade from an earlier release of MaxCS (refer to the *Upgrade Guide*)

MaxCS 9.0 Update1

The following enhancements were added in MaxCS 9.0 Update1.

MaxCommunicator Web

MaxCommunicator Web is a web-based version of MaxCommunicator that is available for cloud- and SaaS-based MaxCS servers. With this application, you can chat with other users, set your avatar and presence, perform most call actions, including transferring calls, forwarding calls, and other tasks available in MaxCommunicator. Some MaxCommunicator features are not available in this version.

Users can access MaxCommunicator Web from the Service Hub Home page or through a previously visited URL.



For detailed information about MaxCommunicator Web, see the *MaxCommunicator Web Guide* at www.altigen.com under the Support tab.

Service Hub

The Service Hub is a single-sign-on web application delivery platform that allows administrators to manage web-based applications and users to access web applications.

The MaxCommunicator Web, AltiReport, and Update Management Studio (UMS) cloud-based applications can be accessed through Altigen Service Hub (<https://servicehub.altigen.com>) in this release.

The Service Hub allows you to configure various aspects of your web application deployment, including user settings and service options. Web application users can update their profile and password in Service Hub, if you grant them appropriate permissions.

SaaS-based servers require installing MaxCS Service Hub and MaxCS WebApps on the MaxCS server for the MaxCommunicator Web application.

There are two versions of the *Service Hub* manual: Company Administrator and end users. You can find these manuals at www.altigen.com under the Support tab.

Standalone MeetMe Application

There is now a standalone MeetMe application to supplement MaxCommunicator Web. This application has the same MeetMe conferencing features as the Windows MaxCommunicator application.

AltiReport Integrated with Service Hub

AltiReport runs in standalone mode in prior releases. In addition to standalone mode, AltiReport supports integration with Service Hub for cloud servers where AltiReport administrator and application users can access the application through the Service Hub. On-premise MaxCS servers support standalone only.

See the *AltiReport* and *Service Hub* guides for details at www.altigen.com under the Support tab.

Update Management Studio (UMS)

An update management tool, available for resellers only, that is accessed through Altigen Service Hub. It allows administrators to update the image on a single or group of cloud-based MaxCS servers through scheduled tasks, and to deploy or update the MaxCommunicator Web application.

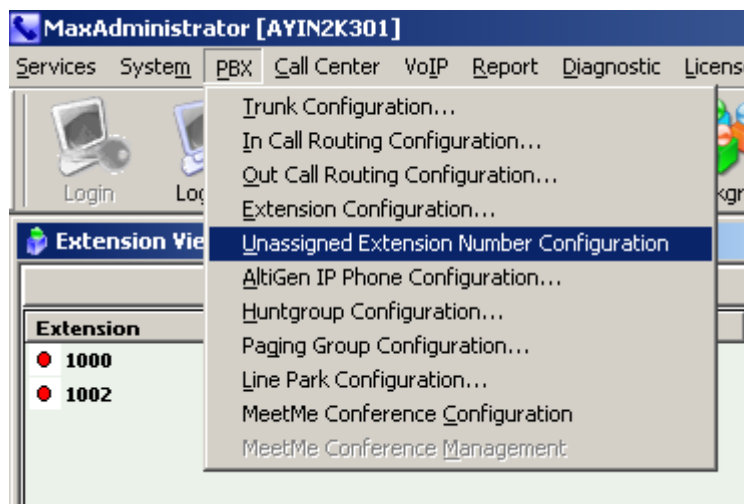
See the *UMS Guide for Resellers* for details at www.altigen.com under the Support tab.

Unassigned Extension Routing

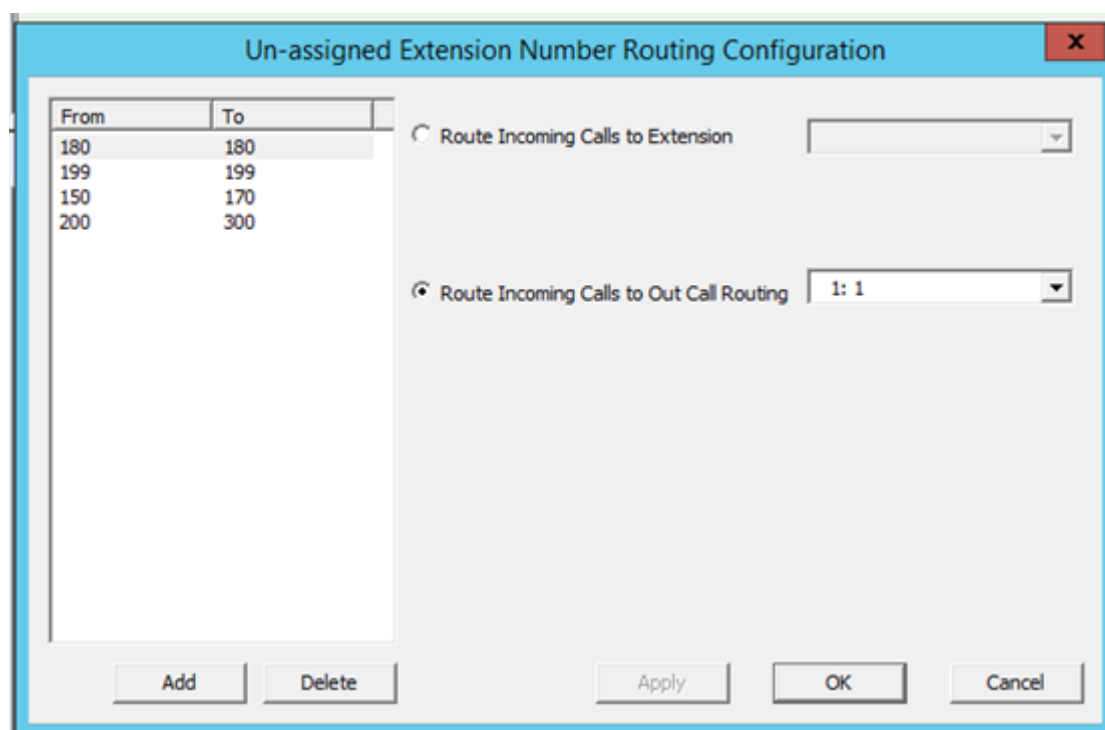
Call routing for unassigned extensions has been enhanced. You can now route these calls from unassigned extensions to an extension or group of third-party phone systems.

To configure how unassigned extension calls are routed, follow these steps:

1. In Max Administrator, choose **PBX > Unassigned Extension Number Configuration**.



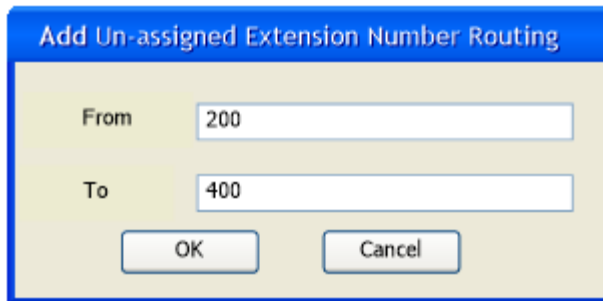
2. The Unassigned Extension Number Routing Configuration dialog appears.



The unassigned number range appears in the entry list. You can perform the following tasks: add a new range, delete the range, and specify the routing destination of a range.

Adding a range

To add a new range, click the Add button and specify the range in the dialog.



The dialog box has a blue title bar that reads "Add Un-assigned Extension Number Routing". It contains two text input fields: "From" with the value "200" and "To" with the value "400". Below the fields are two buttons: "OK" and "Cancel".

Here are the rules for entering a range:

- The length of an unassigned extension number must be the same as the system extension length or the system will not allow the administrator to add the route. You can find the system extension length under **MaxAdmin > System Configuration > Number Length**.
- An administrator cannot add a range that overlaps an existing unassigned extension routing entry.
- You can only enter digits to specify the range. Special characters are not allowed.
- The value for To cannot be less than the value for From.
- To enter a single entry, specify the same number in From and To.

Here are some examples of range entries:

- If the range is between 100 and 200, all 3-digit unassigned extension numbers from 100 to 200 will match this routing.
- If the range is between 2098 and 2102, and there's an extension 2099, the matched numbers are 2098, 2100, 2101 and 2102.
- Say you've already specified a range of: 1000~1600.
 - Range: 1600~1700 cannot be added because it overlaps with 1000~1600.
 - Range: 1601~1700 can be added because it is independent from 1000~1600.
 - Range: 1500~1600 cannot be added because it is nested within 1000~1600.
 - The single number, 1100, cannot be added because it falls within 1000~1600.

Deleting a range

To delete a range, select it from the list, and click Delete.

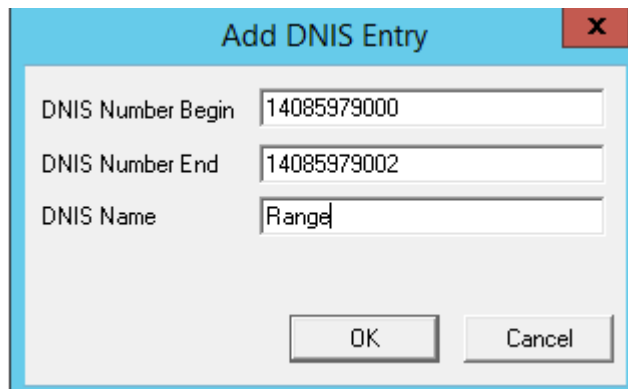
Routing unassigned extensions

Specify the routing destination after selecting an unassigned extension route in the list. Each call can only match one unassigned extension route. In other words, a call won't match multiple unassigned extension routes. The route can be one of the following:

- an extension/APC/WG
- an out call routing

DNIS Range

The DNIS Range feature lets you configure large numbers of DNIS extensions easily. You can specify a range of DNIS numbers, name the range, and configure it as you want. This version does not support overlapping or nested ranges. You can also specify a single entry by specifying the same number in the DNIS Number Begin and DNIS Number End fields.



The 'Add DNIS Entry' dialog box contains the following fields and buttons:

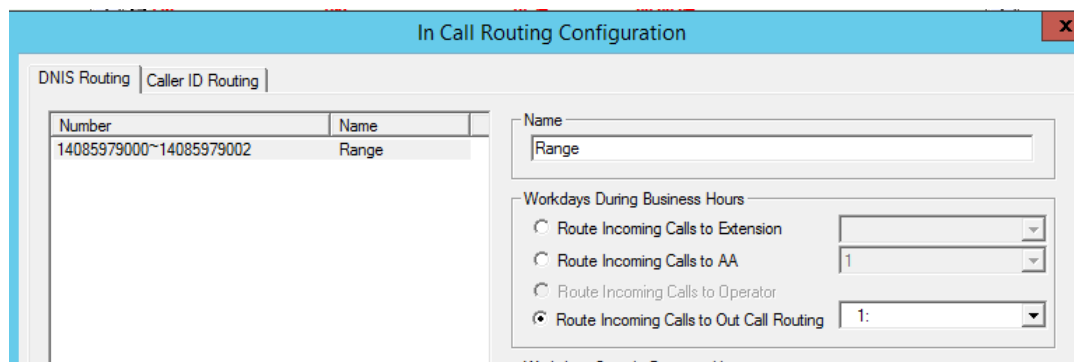
- DNIS Number Begin:** 14085979000
- DNIS Number End:** 14085979002
- DNIS Name:** Range
- Buttons:** OK, Cancel

You can also specify a wildcard entry that matches all the DNIS numbers that start with the same digits. For example, you can specify 14* to match all entries beginning with 14.

The DNIS matching priority rules for entries are in this priority order:

- Single number
- Range
- Wildcard

You can now route incoming calls to Out Call Routing



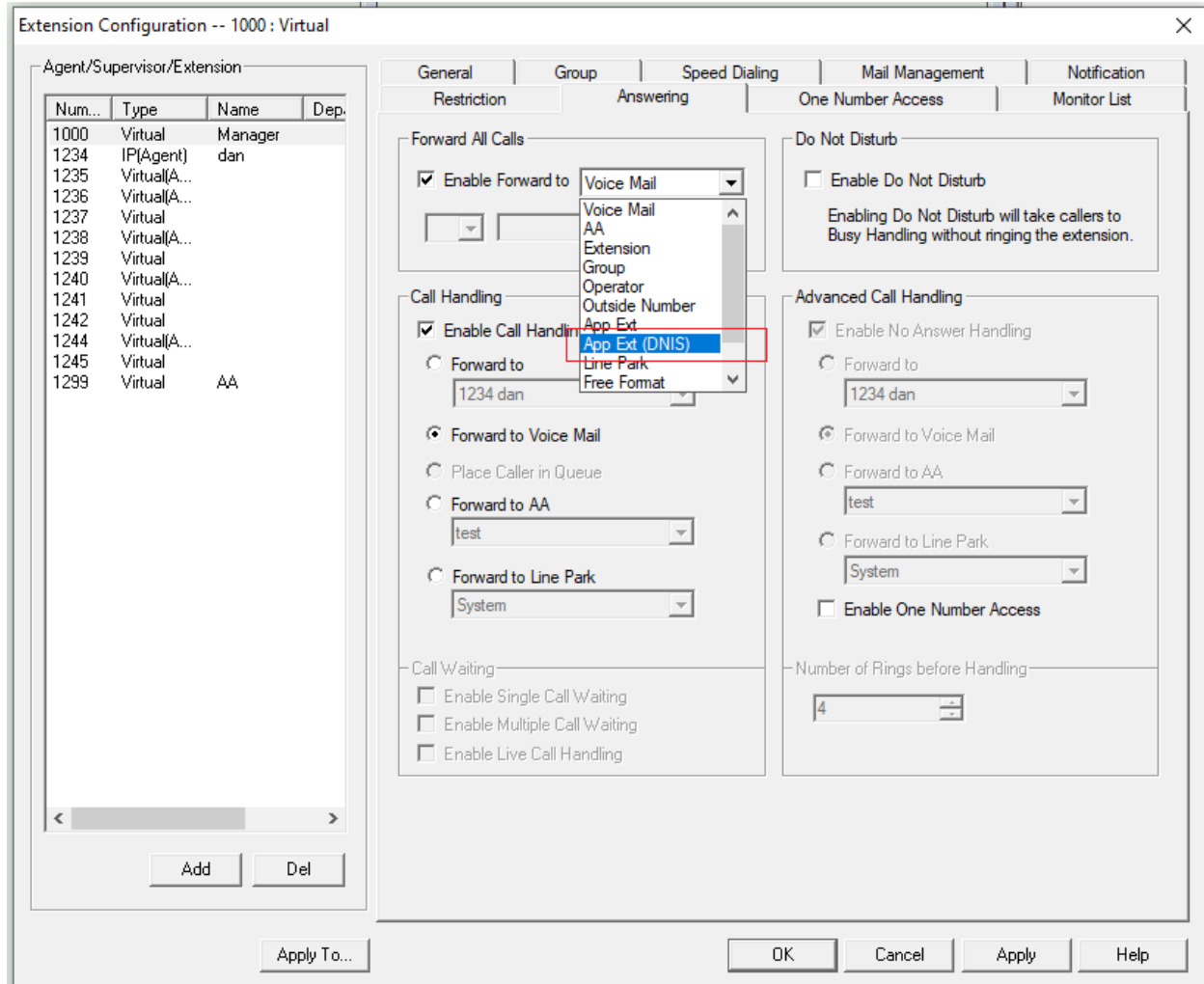
The 'In Call Routing Configuration' dialog box shows the following configuration:

- Tab:** DNIS Routing
- Table:**

Number	Name
14085979000~14085979002	Range
- Name:** Range
- Workdays During Business Hours:**
 - ☐ Route Incoming Calls to Extension
 - ☐ Route Incoming Calls to AA
 - ☐ Route Incoming Calls to Operator
 - ☒ Route Incoming Calls to Out Call Routing

DNIS Routing

When an incoming call connects to MaxCS, the initial DNIS number is associated with the call. If an agent answers this call and wants to route the user back to an application extension using a different DNIS number, they can now use App Ext (DNIS) in the Extension Configuration call forwarding options. If selected, calls to that extension get forwarded to an application extension that uses this configured virtual extension number as the DNIS number.



Extension Configuration -- 1000: Virtual

Num...	Type	Name	Dep.
1000	Virtual	Manager	
1234	IP(Agent)	dan	
1235	Virtual(A...		
1236	Virtual(A...		
1237	Virtual		
1238	Virtual(A...		
1239	Virtual		
1240	Virtual(A...		
1241	Virtual		
1242	Virtual		
1244	Virtual(A...		
1245	Virtual		
1299	Virtual	AA	

Buttons: Add, Del

Apply To...

OK, Cancel, Apply, Help

General | Group | Speed Dialing | Mail Management | Notification

Restriction | Answering | One Number Access | Monitor List

Forward All Calls

☒ Enable Forward to Voice Mail

Forward to: 1234 dan

Call Handling

☒ Enable Call Handling

Forward to: 1234 dan

Forward to Voice Mail

Place Caller in Queue

Forward to AA: test

Forward to Line Park: System

Call Waiting

☐ Enable Single Call Waiting

☐ Enable Multiple Call Waiting

☐ Enable Live Call Handling

Do Not Disturb

☐ Enable Do Not Disturb

Enabling Do Not Disturb will take callers to Busy Handling without ringing the extension.

Advanced Call Handling

☒ Enable No Answer Handling

Forward to: 1234 dan

Forward to Voice Mail

Forward to AA: test

Forward to Line Park: System

☐ Enable One Number Access

Number of Rings before Handling: 4

By default, this option is hidden. A registry key, “**EnabledDNISForwardToAppExt**” must be enabled to show this option. This registry key is located here:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Altigen Communications, Inc.\AltWare

The registry key does not appear automatically until **Extension > Answering** is selected.

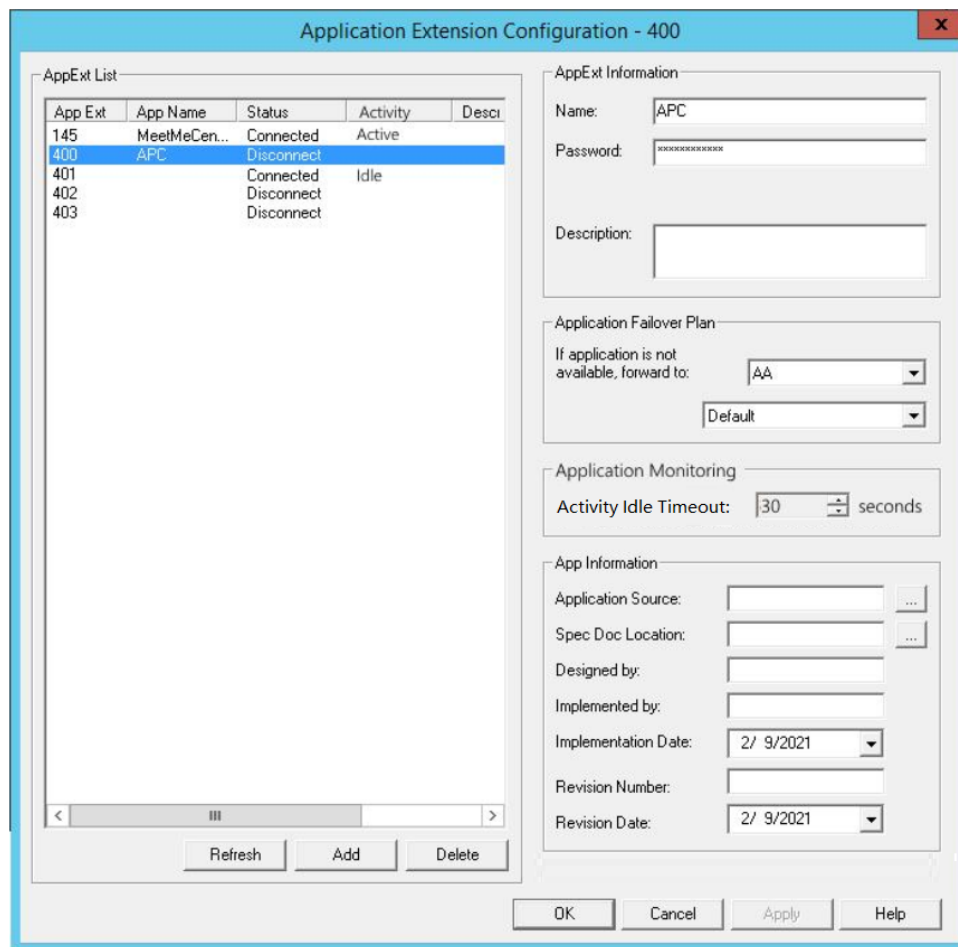
APC Activity Monitoring

MaxCS has been enhanced to monitor APC application activities so that unhealthy application status can be detected. Note that the Frontstage server runs as an APC application and will send CTI commands as keepalive to MaxCS.

The Activity Idle Timeout setting has been added under Application Extension Configuration for application activity monitoring. If there are CTI activities detected within the specified timeout duration, its status shows Active, otherwise its status is Idle.

The TCP connection status for each application extension is displayed in the Application Extension List. The APC application's Activity Status is added to this list to display the activity for each connected APC extension.

The TCP connection state change along with its APC extension number will be recorded in a trace log file. Activity state changes with the APC extension number will also be logged



Application Extension Configuration - 400

App Ext	App Name	Status	Activity	Descr
145	MeetMeCen...	Connected	Active	
400	APC	Disconnect		
401		Connected	Idle	
402		Disconnect		
403		Disconnect		

AppExt Information

Name:

Password:

Description:

Application Failover Plan

If application is not available, forward to:

Application Monitoring

Activity Idle Timeout: seconds

App Information

Application Source:

Spec Doc Location:

Designed by:

Implemented by:

Implementation Date:

Revision Number:

Revision Date:

IPTalk Custom Ring Tone

In MaxCommunicator and MaxAgent, you can now upload a custom ring tone to play when receiving an incoming call.

To upload the custom ring tone, click Upload and specify the PCM WAV file to use as a ring tone. To reset the ring tone back to the default, click Reset to Default.



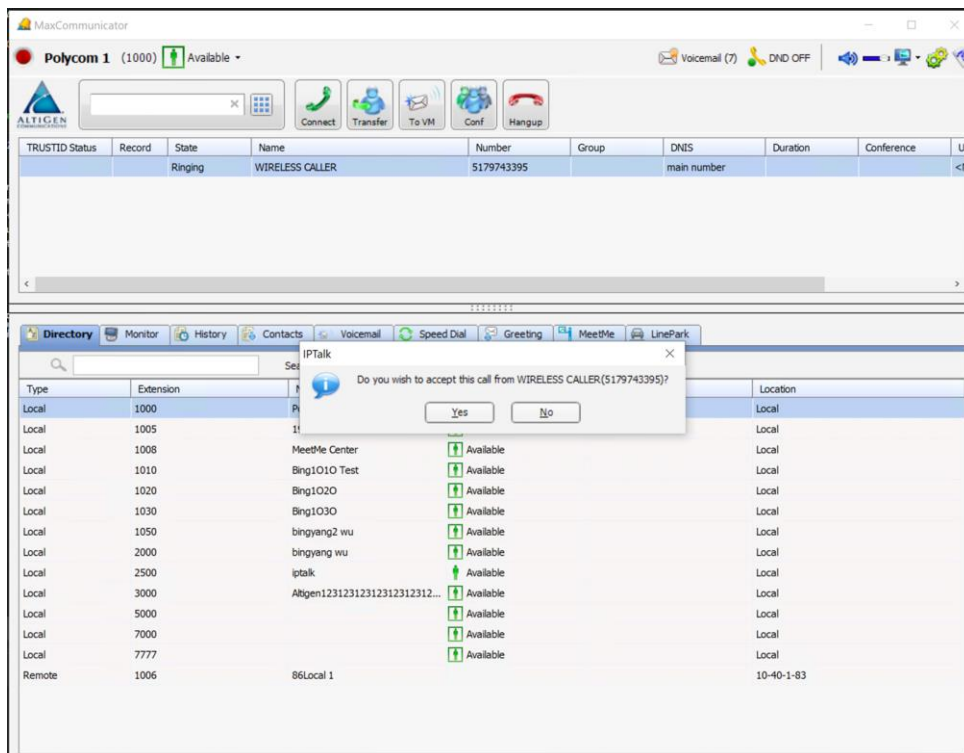
IPTalk Ring Tone When Non-Default Ring-Through Device Selected

Currently when a non-default speaker device is selected for the Ring-Through Device setting, the IPTalk user hears a mono ring tone when receiving an incoming call. This enhancement will play the system default ringer or custom ringer when a non-default speaker device is selected.

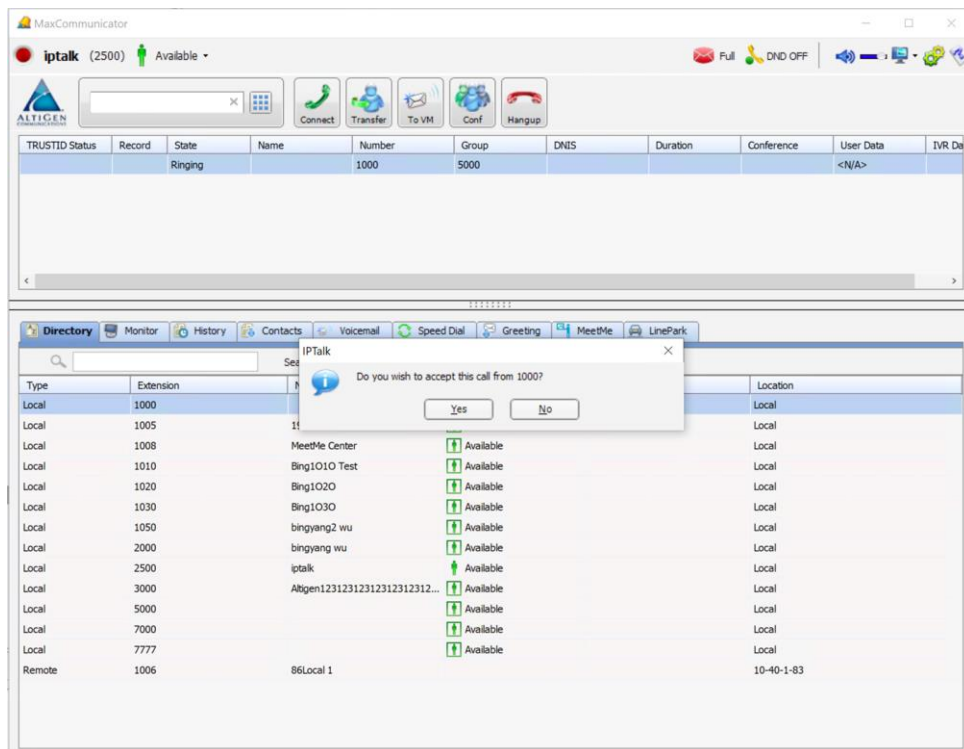
IPTalk Incoming Call Popup

There is now an incoming call pop-up window for MaxCommunicator. It displays the Caller Name and Number when a call comes in. If the name is not available, only the Caller Number is shown.

This screen shows the display when the Caller Name exists:

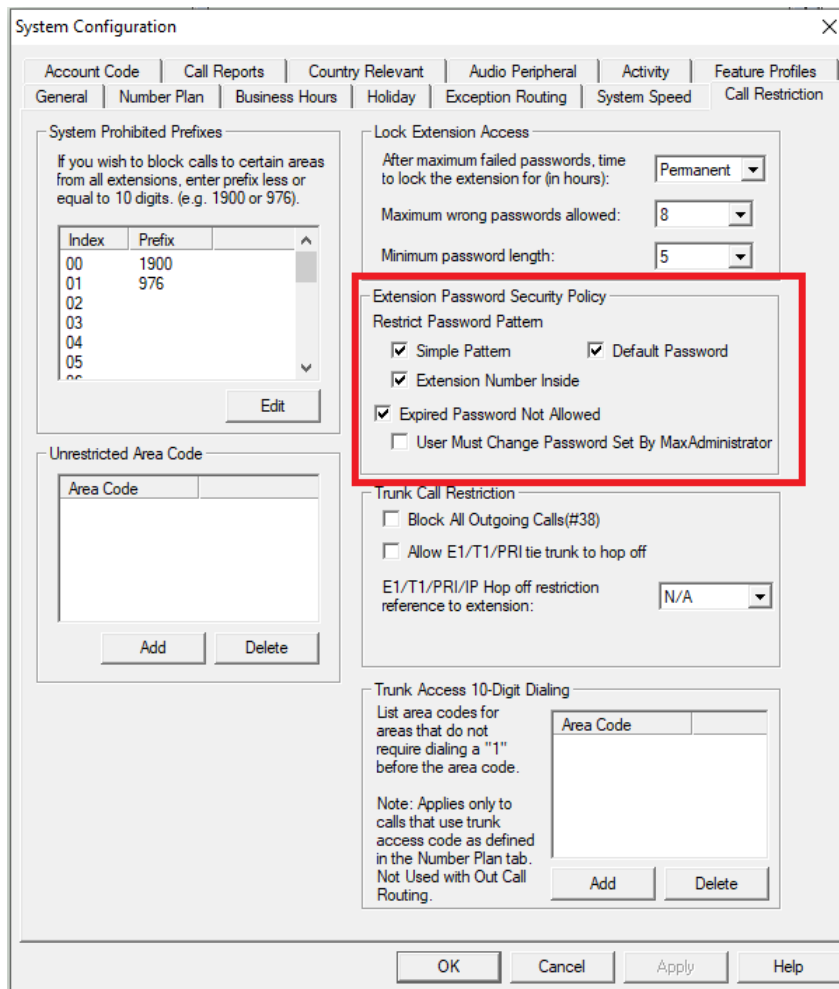


This is the pop-up window when the Caller Name does not exist:



Password Security Policy

Some password security related settings currently available in ExtChecker tool are added to this release.



System Configuration

Account Code | Call Reports | Country Relevant | Audio Peripheral | Activity | Feature Profiles
 General | Number Plan | Business Hours | Holiday | Exception Routing | System Speed | **Call Restriction**

System Prohibited Prefixes
 If you wish to block calls to certain areas from all extensions, enter prefix less or equal to 10 digits. (e.g. 1900 or 976).

Index	Prefix
00	1900
01	976
02	
03	
04	
05	
...	

Edit

Unrestricted Area Code

Area Code

Add Delete

Lock Extension Access
 After maximum failed passwords, time to lock the extension for (in hours): Permanent
 Maximum wrong passwords allowed: 8
 Minimum password length: 5

Extension Password Security Policy
 Restrict Password Pattern
☒ Simple Pattern ☒ Default Password
☒ Extension Number Inside
☒ Expired Password Not Allowed
☐ User Must Change Password Set By MaxAdministrator

Trunk Call Restriction
☐ Block All Outgoing Calls(#38)
☐ Allow E1/T1/PRI tie trunk to hop off
 E1/T1/PRI/IP Hop off restriction reference to extension: N/A

Trunk Access 10-Digit Dialing
 List area codes for areas that do not require dialing a "1" before the area code.
 Note: Applies only to calls that use trunk access code as defined in the Number Plan tab. Not Used with Out Call Routing.

Area Code

Add Delete

OK Cancel Apply Help

Restrict Password Pattern

Simple Pattern – Disallow password entry if the digits are all the same or if it is a sequence of sequential digits.

Default Password – Disallow password entry if the password is the system default password.

Extension Number Inside – Disallow password entry if the password contains the extension number

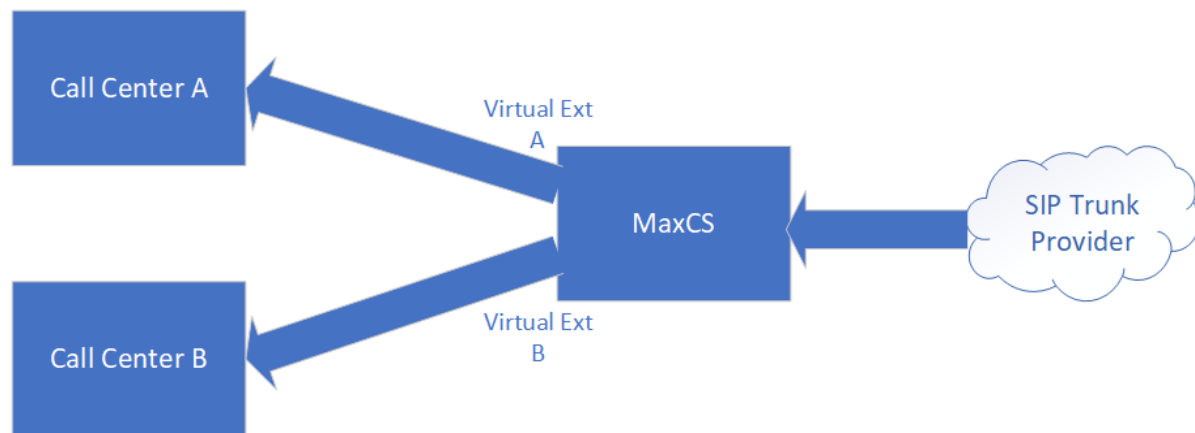
Expired Password Not Allowed – When enabled, if a password is expired, users are prompted to change the password when they login.

User must change password set by MaxAdmin – After setting an extension's password from MaxAdministrator, the password will be marked as expired, and the user will have to set a new password when logging in.

Busy Trunk Queuing

In this release, MaxCS can be configured to queue and distribute the calls to multiple call centers. A virtual extension can be configured to route the call to a target call center. The incoming trunk calls can be routed using DNIS Routing, Auto Attendant or some other means available in MaxCS.

One SIP Group can be configured to route calls to each target call center with the desired number of SIP trunk channels. When a virtual extension is called and there are no available trunk channels to the target call center, the call gets put into a trunk busy queue (specific to each virtual extension) until a trunk channel frees up.



Calls will be distributed to the target call center in the order that they come in.

Record greetings

If a personal standard greeting has been recorded, it will play followed by hold music. If not, the system standard greeting is played. In either case, the recording repeats every 30 seconds.

Note: The system standard greeting mentions pressing # to leave a voicemail. This feature does not support DTMF options, so it is highly recommended that you record a custom personal standard greeting.

Enabling the registry key

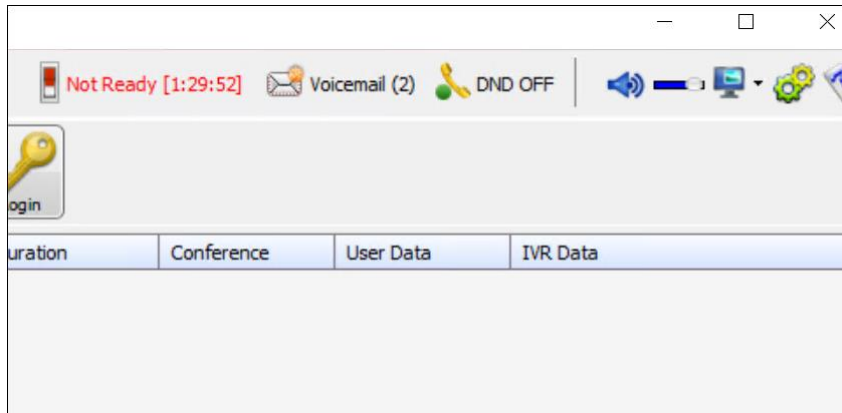
By default, this functionality is disabled. A registry key **"EnableTrunkBusyQueue"** needs to be enabled to show this option. This registry key can be found in

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Altigen Communications, Inc.\AltWare.

After enabling the key, Minute Task must be run from **MaxAdmin >Diagnostic->Trace**.

Displaying Agent Read/Not Ready State Time Duration

In MaxAgent, the duration for agent's Ready/Not Ready state is displayed.



TRUSTID

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.

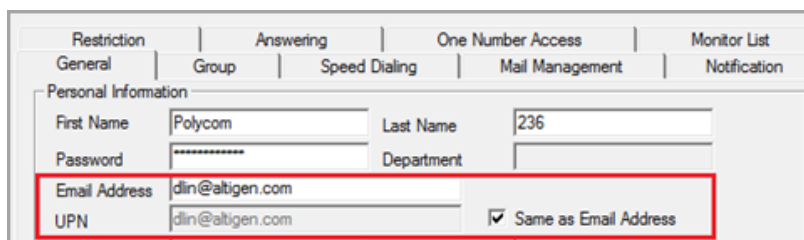
The primary benefit of call authentication is to let credentialed calls be routed in your system swiftly and be noted to agents as valid calls, thus reducing the need for extensive scrutiny by your agents. This way, your agents spend more time helping your callers and less time verifying their identities. A secondary benefit of call authentication is to identify and flag uncredentialed calls and, if desired, route them to different teams for further scrutiny.

Refer to the separate manual, the *TRUSTID Guide*, for details.

New Extension Field: UPN

A new field, UPN, has been added to the **Extension Configuration > General** tab. You can set this UPN field to be the same as the user's email address by checking the option "Same as Email Address."

The *Email Address* field in the **Extension Configuration > Mail Management** tab is now read-only. A configurable field has been added to the **Extension Configuration > General** tab.



The screenshot shows the 'Extension Configuration > General' tab. The 'Personal Information' section contains fields for 'First Name', 'Last Name', 'Password', and 'Department'. Below these is the 'Email Address' field, which is highlighted with a red box. The 'UPN' field is also highlighted with a red box and contains the value 'dlin@altigen.com'. A checkbox labeled 'Same as Email Address' is checked.

Workgroup Queue Management Changes

In Release 9.0, the Workgroup Queue Management feature has been changed.

- When *Basic* mode is selected, the **Setup** option is disabled.
- 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*.

Custom User Activity Option

In this release, MaxCS Presence has a new user Activity: **Busy**. There is a corresponding voicemail greeting, which will play when the user has selected the Busy activity.

Change FROM Header to Local IP Address

A new option has been added for SIP Trunks. There is a new checkbox in the SIP Group Settings panel named *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.

MaxAgent IP Talk Hold Options

Two new options are introduced in Release 9.0. These options apply to IP Talk users.

- **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.

Workgroup Queue Hold Option

In prior releases, when an agent took a call, then made a separate call to a workgroup and was placed into the workgroup queue, the agent could not continue to speak with the caller until the agent's call was picked up by a workgroup member.

In Release 9.0.1, agents can now continue their conversations with callers even while agents are waiting in a workgroup queue.

This agent must be on IP Talk in order for this feature to be supported.

Following is an example of how this works.

1. An IP Talk agent takes an incoming call.
2. After talking with the caller, the agent needs to transfer the call to a different workgroup. However, the agent needs to first call the workgroup and speak with a member of that workgroup before handing over the call, due to internal policies.

3. The agent places the caller on hold and makes a separate call to the target workgroup. But because the other workgroup is busy, the agent is put into the workgroup queue.
4. While the agent's call is in the workgroup queue, the agent can now switch between the two calls (the call to the other workgroup and the original call) by placing one call on hold and picking up the other call. In other words, agents can now place a workgroup queue call on hold.

Note that agents cannot join or initiate a conference call while the workgroup queue call is on hold.

CDR data should reflect no hold duration time for the workgroup hold time.

Double Hold Option

If an agent has been placed on hold by a caller, the agent can now place that caller on hold as well. This is referred to as a "Double Hold." While that call is on hold, the agent can make other calls.

Following is an example of how this works.

1. You are an agent on IPTalk. You get a call from extension 123.
2. The caller at extension 123 places you on hold. The call entry in your MaxAgent window is now in *OnHold* status.
3. You can now place that call on hold yourself – MaxAgent will now show the call in *Hold* status.
4. You can make other calls as needed. You cannot, however, join or initiate a conference call during this 'double hold' period.
5. When you switch back to the call from extension 123, MaxAgent will change the call status to either *Connected* (meaning that the caller removed you from their hold) or *OnHold* (the caller at extension 123 still has you on hold).

The agent who is making the double-hold must have IPTalk. The other extension, which initiates the initial hold, does not need to have IPTalk.

CDR data should reflect hold duration time for the double hold.

Call Answer Enhancements

There are two updates for call answering.

Automatically Answer Ring-back Calls

With MaxAgent or MaxCommunicator, ring-back calls are now automatically answered. This includes the following ring-back call scenarios:

- Making outbound calls
- Playing voicemail
- Recording and reviewing greetings
- Playing an introductory message when forwarding voicemail messages

In MaxSupervisor, these types of ring-back calls are automatically answered:

- Listen
- Barge-in



- Coach

Auto-answer applies to Altigen IP phones, Polycom phones, and to IPTalk.

Click to Answer Calls

When a user of MaxAgent or MaxCommunicator 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.

Not Ready Reason Code With #91 Feature Code

The following changes have been applied 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.

Sending Extension's Transmitted CID When Calling Mobile Extension

If the call to the mobile extension is from a trunk caller, the admin can choose to send either trunk caller's "In-bound Caller ID" or a specified number as the Transmitted Caller ID.

If the call to the mobile extension is from an extension caller, the admin can choose to send one of the following as the Transmitted Caller ID:

- Caller's Extension Number
- Caller Extension's TCID or System Main Number
- System Main Number
- SIP Guest ID
- A specified number

Adjunct SIP Trunk

- Enabled through registry and configuration at SIP trunk channel
- Main use case is when MaxCS is connected to a 3rd party PBX and functions as an adjunct call center
- Support send extension number as caller ID when making a SIP trunk call
- Support hop-off dialing through 3rd party PBX with dialing digits allowed by PBX
- Support calling extension number from incoming SIP trunk calls



Disable Automatic Area Code Insertion for MaxClient

Administrators can configure this option in the MaxAdmin > System > Country Relevant page to disable automatically inserting area code when a MaxClient user dials a 7-digit number or an 8-digit number with a leading access code. This feature applies to Windows MaxCommunicator, MaxAgent and MaxOutlook only when "Auto Format" is enabled in the client. MaxCommunicator Web also supports this feature.

Regroup Abandoned to Voice Mail in MaxSupervisor and CDR Search

"Abandoned to Voice Mail" calls are now counted as Redirected/Overflowed calls, and hence removed from the Abandoned Calls category. A separate "Calls to Voice Mail" statistics section is displayed in MaxSupervisor and CDR Search.

Added User Data Field in Call Entry in MaxCommunicator and MaxOutlook

Support "Apply" to Additional Extension Settings in MaxAdmin

Support Apply to for "Non-Workgroup call", "Recording tone" and "Number of Rings before Handling" in MaxAdmin Extension configuration

AltiReport Enhancements

- The AltiReport configuration backup file is now encrypted.
- Two operation modes are now supported: Standalone AltiReport and AltiReport integrated with Service Hub (available for cloud only)

Polycom Firmware Support

Polycom VVX phones now support firmware version 5.9.6.2327.

SQL 2019

Release 9.0 now supports SQL 2019.

VMWare

Release 9.0 supports VMWare 7.0

Operational Notes and Limitations

This section mentions operational limitations and provides workarounds to any known issues. In addition to this section, you should refer to the Readme files on your installation media for any other known limitations with this release.

- No known operational limits in this release.

Altigen Technical Support

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

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

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

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

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

Please be ready to supply the following information:

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

Patch 8.6.1.216 Updates

The following changes were introduced in build .216.

New System Default Values

There are new default values included in this build; these default values apply to new systems.

- **Default Extension Lockout Period**
The default lockout period for extension password retries (Lock Extension Access group) is now 23 hours.

If a user reaches the maximum number of password attempts, the extension will be locked out for 23 hours (unless you manually change this value). Also see a related change, in [New Options for Extension Lockout Period](#).

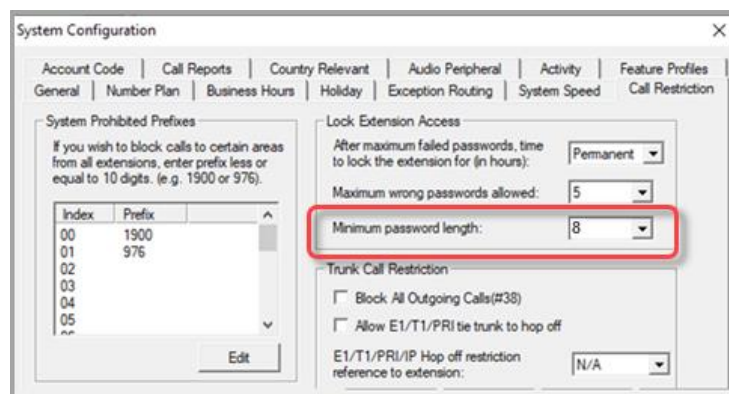
This option is found in the **System > System Configuration > Call Restriction** tab.

- **Default Minimum Password Length**

The default minimum length for both extension passwords and SIP registration passwords is now 8 digits. (Note that this option was moved into MaxAdministrator in build .215.)

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 into voicemail the system will indicate that the password has expired and will prompt the user to change it.

This option is found in the **System > System Configuration > Call Restriction** tab.



The screenshot shows the 'System Configuration' window with the 'Call Restriction' tab selected. The 'Lock Extension Access' section is highlighted with a red box. It contains the following options:

- After maximum failed passwords, time to lock the extension for (in hours): Permanent
- Maximum wrong passwords allowed: 5
- Minimum password length: 8

The 'Trunk Call Restriction' section is also visible, with options for blocking outgoing calls and allowing E1/T1/PRI tie trunk to hop off.

- **Default Action for the # Symbol in AA**

The default value for the # symbol in AA trees has changed from *Mailbox Access* to *No Action*. This will apply to any new deployments or to any new AA trees that you create after upgrading to build .216.

New Options for Extension Lockout Period

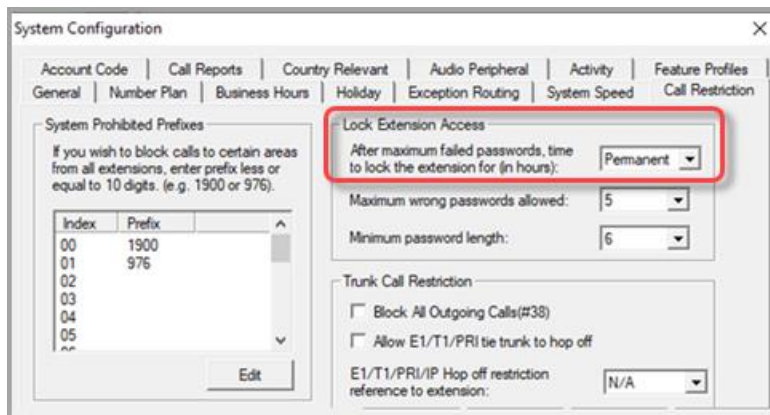
Your options for the Extension Lockout period (Lock Extension Access group) have been expanded. These options are found in the **System > System Configuration > Call Restriction** tab. You can now choose:

- **Lock the extension for a specific number of hours (1-72 hours)**

In earlier releases, you could specify the duration in hours:minutes:seconds. As of Release .216, any durations for this field that included minutes and seconds will be rounded up to the nearest hour. For example, if you previously had this option set to lock the account for 2:30:00, in Release .216 this will be reset to 3 hours.

- **Lock the extension as *Permanent***

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. For details on using this tool, refer to the *MaxCS Administration Manual*.)



Extension Checker Updates in .216

MaxCS Admin & Extension Security Checker is a separate tool provided with MaxCS. Several changes to this tool are introduced in this build.

- **Login Requirements**

In order to log into the tool, you must now have Super Admin, Full Admin, or Basic Admin login credentials. For details on these types of admin users, refer to the *Admin User Configuration* chapter in the *MaxCS Administration Manual*.

- **Remote Support**

You can now run this tool remotely.

There were also Extension Checker changes in build .215; see the section [Extension Checker Updates in .215](#).

Passwords Must Now Be Followed With

In earlier releases, users could just press the digits of their voicemail passwords and the system would log them in.

Beginning with Release 8.6.1.216, users must now press the # key to indicate the end of the password entry process. The system will play a prompt stating that they need to press the # key after entering their password.

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

Users Prompted to Change Password Upon Login

Beginning with Release 8.6.1.216, when a user logs into one of the client applications the system will check to see if the current password meets the password requirements. It will make sure the password is not the system default password or has patterns in the digits, among other security checks.

This change applies to MaxAgent, MaxCommunicator, and MaxOutlook. It does not apply for MaxSupervisor or MaxInsight.

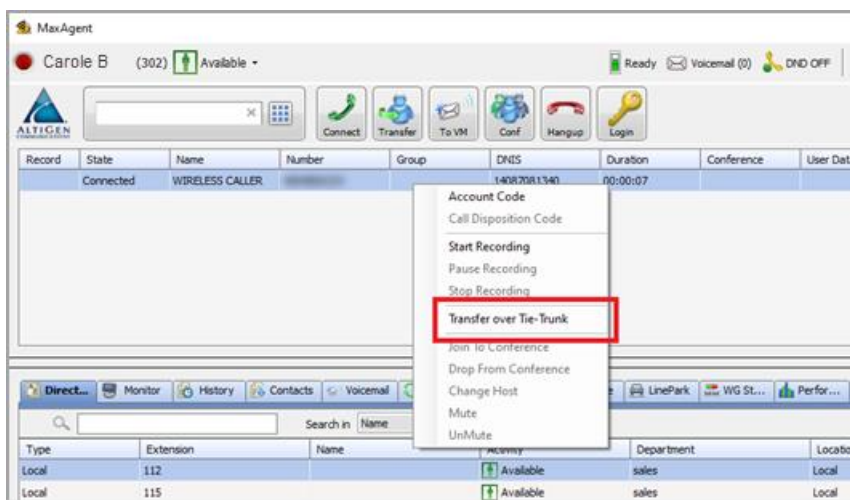


If the user's password fails to meet the requirements, the system will inform the user that the password is unsafe and must be changed. When the user clicks OK, the system will automatically open a dialog box where the user must change the password to a safer one that meets the requirements.

Transfer Calls over Tie-Trunks

Some customers need to transfer calls to other extensions over Tie-Trunk. IP Talk in the client applications has been enhanced to make it easier to transfer calls over Tie-Trunks.

1. Right-click a call entry and choose **Transfer over Tie-Trunk** from the menu.



2. In the pop-up, enter the target extension number and click **Transfer**.

Depending upon where you are transferring the call, the following will happen:

Target Type	Behavior
Target is a physical extension	<p>You will hear the call ring.</p> <ul style="list-style-type: none"> • If the target party answers, the trunk call will be held while you speak with that person. When you hang up, the held call will be connected to the target party. • If the target party does not answer and your call is directed to the target party's voicemail mailbox, you will hear a prompt. You

	<p>have two options:</p> <ul style="list-style-type: none"> ○ To send the call to the target party's voicemail, hang up. ○ To reconnect to the caller, press the Flash and Star buttons.
Target is an APC extension	MaxAgent hangs up your call automatically and connects the trunk call to the target APC extension.
Target is a workgroup number	<p>You will hear the call ring.</p> <ul style="list-style-type: none"> • If a workgroup member answers, the trunk call will be held while you speak with that person. When you hang up, the held call will be connected to the workgroup member. • If the workgroup is sending the call to voicemail or placing the call in the call queue, you have two options: <ul style="list-style-type: none"> ○ To complete the transfer, hang up. ○ To reconnect to the caller, press the Flash and Star buttons.
Target extension does not exist	You will hear a prompt, "The extension you are calling is invalid; press the Flash and the Star button to reconnect to the calling party."
Target extension is a virtual extension that is forwarded to IVR or voicemail	<p>You will hear a prompt, "The extension you are calling is not available at the moment." You have two options:</p> <ul style="list-style-type: none"> ○ To complete the transfer, hang up. ○ To reconnect to the caller, press the Flash and Star buttons.

Patch 8.6.1.215 Updates

The following enhancements were added in the .213 build of MaxCS 8.6.1.

Enhancements for the Trusted/Malicious SIP Device Lists

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.

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,

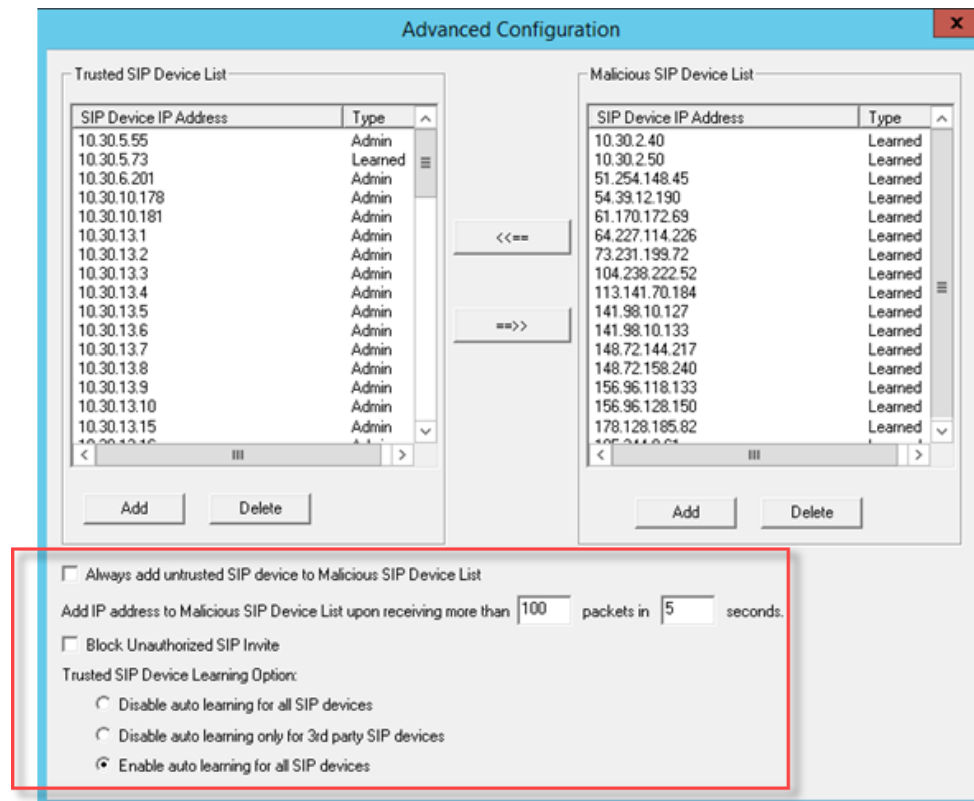
- If a packet comes in and the device's IP address is listed in the Malicious SIP Device list, then no traffic is allowed from that device.
- If the device's IP address is listed in the Trusted SIP Device list, then traffic is allowed but the device still needs the correct password to register to the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



Trusted SIP Device Learning Options

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 administrators 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

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 automatically be added **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.
- User **Shift-Click** to select the beginning and ending IP addresses, to select a contiguous range.

Password Configuration Enhancements

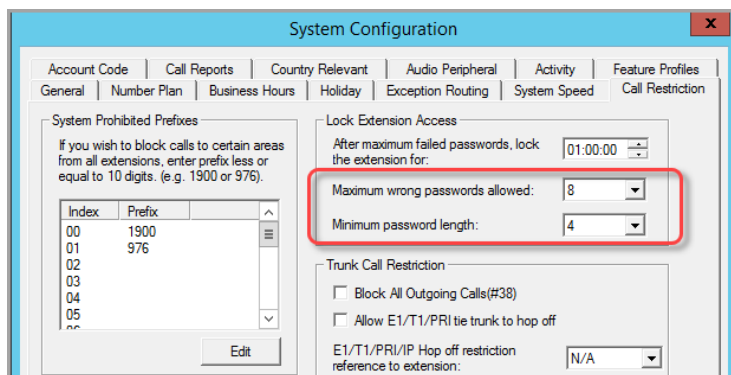
The following enhancements to password options are included in MaxCS 8.6.1.215.

Options That Are Now in MaxAdministrator

The following options have been moved from Extension Checker into MaxAdministrator:

- Maximum wrong passwords allowed
- Minimum password length (this option applies to both extension passwords and to SIP Registration passwords)

These options are now in **System Configuration > Call Restrictions** tab.





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 MaxAdministrator installations, there will be an ExtChecker.exe located in C:\Program Files (x86)\Altigen\AltWare Administrator.

Refer to the *MaxCS Administration Manual* for a discussion of using Extension Checker.

Patch 8.6.1.213 Updates

The following enhancements were added in the .213 build of MaxCS 8.6.1.

MaxSupervisor Updates

Following are descriptions of changes to the MaxSupervisor client.

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 increased 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.

If this column is not visible, then you will need to unhide it by right clicking the column to open the Column Chooser, and then selecting "Current Time in Not Ready Reason" to display the column.

This duration will increment as long as the agent is not ready, even when taking personal calls. The duration will reset if the agent changes the 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

Following are descriptions of changes to the MaxAgent client application.



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.

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:

1. Right-click the *Not Ready* icon to see a drop-down list of valid Not Ready reason codes.
2. Select the new Not Ready reason code to switch.

(This option is not available if the agent is set to *Ready*.)

Note that changing the reason code will reset the "Time in Not Ready Reason" duration shown in MaxSupervisor.

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.

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 "EnableIPTalkRejectLogOutRNA" key. Change its value from 0 to 1. Save your changes.
3. 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 the workgroup's configuration. That result will be reflected in the AltiReport Activity Report (1101).



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.

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 "EnableAgentLoginAutoReady" key. Change its value from 1 to 0. Save your changes.
3. In MaxAdmin, select **Diagnostic > Trace**. Locate and run **Minute Task** (NOT Midnight Task)

After applying these changes, agents will no longer be set to Ready when they log into a workgroup (via MaxAgent or via #54). Agents will need to set their state to *Ready* manually.

To reverse this change, set the registry value from 0 to 1 and run **Minute Task** again.