# MAX Communication Server
# Release 8.6

## New Features Guide

July 30, 2019

# Contents

# About This Guide

This guide is provided for the release of MaxCS Release 8.6. It describes the enhancements that have been included since MaxCS Release 8.5.1.

# Requirements

For system requirements, refer to the *MaxCS All-in-One Deployment Guide*.

# Overview of MaxCS 8.6 Enhancements

The changes that are included in this release are listed in the table. Details for most features are included later in this guide.

| MaxCS 8.6 Enhancements | |
|---|---|
| **Polycom enhancements** | You now have better control over when your Polycom phones get new firmware when you install a new release of MaxCS.<br>MaxCS now supports Polycom VVX 201 phones. Note that this model does not support BLF or Line Park.<br>This release supports Polycom VVX firmware version 5.9.3.2489. |
| **Backup program changes** | The backup program no longer backs up the Polycom logs. |
| **MaxCS Client Upgrade enhancements** | When upgrading to a new release, MaxCS clients only upgrade when there are compatibility issues with the previous release. In addition, you now have the option to update MaxCS clients from an external source. |
| **Trace enhancements** | Logging has been made a more efficient process in this release. |
| **Midnight Task Schedule enhancements** | You can now set a custom schedule for nightly MaxCS tasks. |
| **Exception Routing Rules** | You can now create custom exception routing rules, for events such as company meetings that do not require a full day as a holiday typically does. |
| **OpenJDK Support** | AltiReport now supports OpenJDK to run Tomcat 8.5 (for AltiReport). |
| **Not Ready Reason Codes** | You now have customized codes that agents can enter when they switch their status to Not Ready. You can require these codes or make them optional. |
| **Call Disposition Codes** | You now have customized codes that agents can select to indicate the disposition of each workgroup call. You can require these codes or make them optional. |
| **Account Code enhancements** | You can now force agents to enter account codes for inbound workgroup calls, just as you can for outbound workgroup calls. |
| **Security update** | This release includes a security change which prevents a configuration file from being read remotely. As part of this change, MaxAdmin is initially |

| MaxCS 8.6 Enhancements | |
|---|---|
| | configured to accept only local access. See the section Security Update for instructions on updating the IP Dialing Table in Enterprise Manager to add IP addresses that you want to allow. |
| **VRM Pro update** | You can now disable Server Message Block signing (SMB) v1 on servers without obstructing the transfer of voice recordings to the VRM server. See VRM Pro Update for instructions. |
| **AltiSDK** | APIs have been added to AltiSDK for the Not Ready Reason Code, the Call Disposition Code, and Account Codes. |

# Installation Procedures

This release supports:

- A new installation of MaxCS; follow the steps in the *MaxCS SoftSwitch Deployment Guide* or the Readme file.
- An upgrade from an earlier release of MaxCS; follow the steps in the *MaxCS Upgrade Guide*.

# Polycom VVX Firmware Auto-Upgrade Enhancements

Unlike in earlier releases, you can now control firmware upgrades on individual VVX Polycom phones.

The individual VVX extension's **Update firmware to…** setting is no longer automatically disabled. You can choose to enable or disable each VVX phone's update option. (**PBX** > **AltiGen IP Phone Configuration** on the *Polycom* tab)

MaxCS now has an **Apply To** button, so that you can apply the enable/disable option to multiple Polycom VVX extensions.

# Backup Program Enhancements

For better performance and to reduce the amount of disk space used by backup logs, the Backup process no longer includes Polycom log files.

# MaxCS Client Upgrade Enhancements

This release includes two enhancements to the MaxCS client upgrade process:

- MaxCS clients now will require an upgrade to a new release only when the new version has known incompatibilities with the previous release.
- MaxCS clients can now be upgraded from an external URL. This lessens the impact on the bandwidth of the MaxCS server.

## Upgrading Clients via a URL

Administrators can now specify a location for the MaxCS client upgrade installation files, instead of having MaxCS clients retrieve upgrade files from the MaxCS Server. You will specify this download location within MaxAdmin.

Some considerations:

- If you configure the download URL in MaxAdmin, then you must manually sync the installation files on the web server that hosts that URL. This must be done with each future software upgrade. MaxCS will verify the version of the software, the system will push the correct version of installation files to the MaxCS client.
- If you do not configure a download URL in MaxAdmin, then the MaxCS clients will still download the installation flies from the MaxCS server.
- Administrators must log in under the “super admin” account in order to access this new field.

To configure this external download location,

1. In MaxAdmin, select **System** > **System Configuration** > **General**.
2. Enter the URL in the new field, **MaxCS Client Download URL**. Save your changes.

# Trace Enhancements

In this release, the log process has been streamlined to run more efficiently.traces In addition, several new traces have been added to the list of traces that you can run:

- SIP KeepAlive SP Log
- Polycom Phone Log
- QESL Log

You reach these trace settings by choosing **Diagnostics** > **Trace**.


Other notes:

- The *H323 SP log* has been removed; it is no longer relevant in the newer releases of MaxCS.
- The *IP Phone Service* log has been renamed to *Altigen IP Phone* log.

# Midnight Task Scheduling Enhancements

You can now set a custom schedule for nightly MaxCS tasks, through a registry entry.

To indicate what time you want the MaxCS nightly tasks to begin,

1. Open the registry on the MaxCS server.
2. Add a new entry:

   HKEY_LOCAL_MACHINE\software\Wow6432Node\AltiGen Communications, Inc.\AltiWare\MidnightTaskTime

3. The default time, 3:00 AM, is denoted as 03:00:00. This time will be used by default if you do not specify a different time, or if the value you enter is invalid.

   Enter the time you want the task to start and save the changes.

If you prefer, you can add this new registry entry via a command line. For example, to add an entry to this registry for the tasks to start at 2:15 AM, enter:

```
reg add "HKEY_LOCAL_MACHINE\software\Wow6432Node\AltiGen Communications, Inc.\AltiWare" /v MidnightTaskTime
/
t reg_sz /d 02:15:55
```

# Exception Routing

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

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

Considerations:

- You can add multiple exception routing rules, even for the same date and time.

- Exception routing rules can have one or more DNIS numbers.

## Routing Precedence

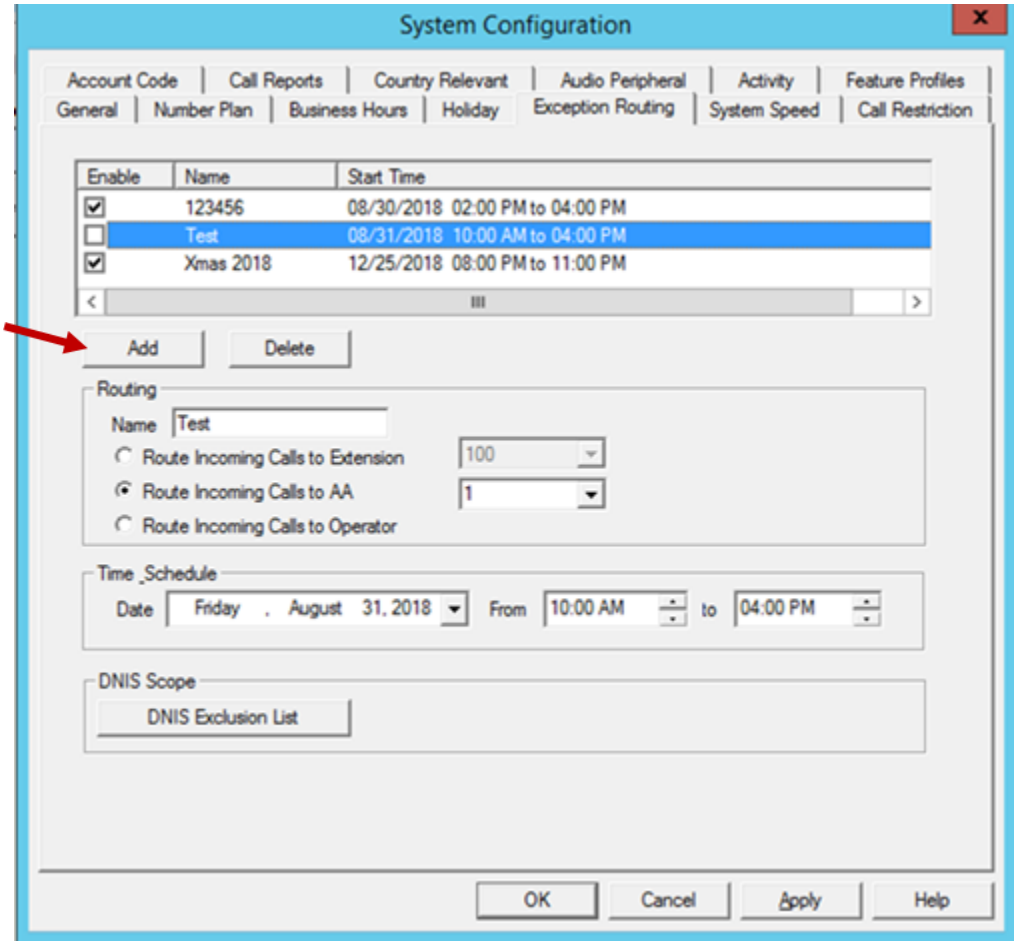
- Exception routing rules have precedence over Holiday Profile definitions.
- Holiday Profile definitions have precedence over Business Hours settings.

## Creating Exception Routing Rules

To create a new routing rule,

1. In MaxAdmin, select **System** > **System Configuration** > **Exception Routing**.
2. This tab shows you routing rules that have already been configured.

   To add a new rule, click the **Add** button below the list of rules.
3. In the *Routing* section below the table, enter a name for this rule. We recommend that you use a unique and descriptive name that will make it easy to identify among other rules.




4. Choose a routing option:
   - Route Incoming Calls to Extension – Enter or select the extension for calls during this period.

- Route Incoming Calls to AA – Select the AA for calls during this period
- Route Incoming Calls to Operator – Routes calls to the Operator during this period.

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

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

# OpenJDK Support

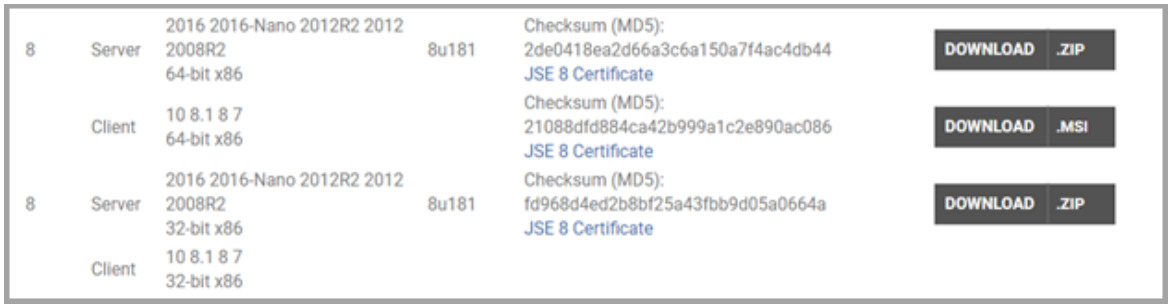
Currently, MaxCS AltiReport relies on 32- or 64-bit Oracle 8u101 JREs for Tomcat 8.5. However, since this is an old version of Java JRE, you may want to use an updated JRE. Because JDK 8 may not be supported after January 2019, you can download an OpenJDK JRE to run Tomcat 8.5.

To run Tomcat using the OpenJDK JRE,

1. Download the latest Zulu build for OpenJDK 8. The website can be found here:

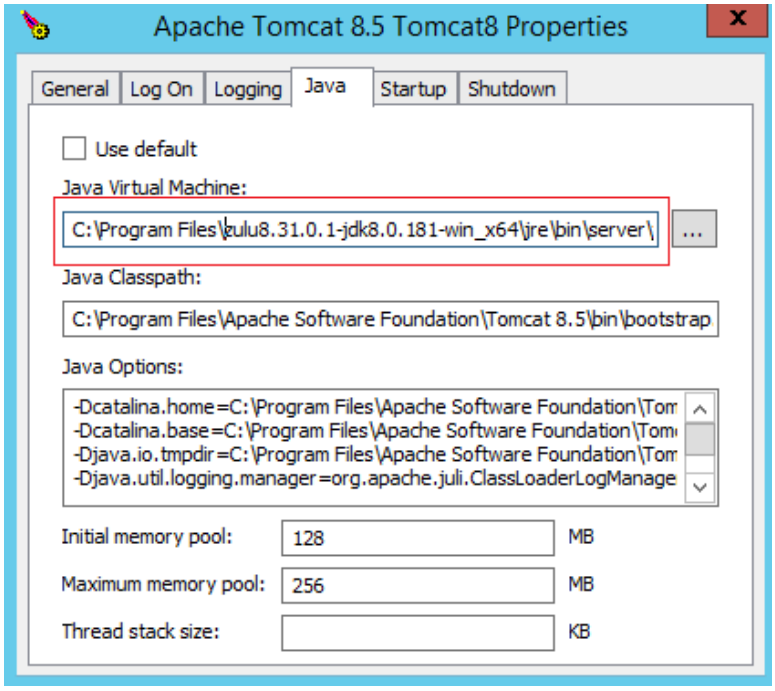
   https://www.azul.com/downloads/zulu/zulu-windows/

2. Depending on the system, you will need to either download the most up-to-date 32-bit x86 or 64-bit x86 version of Java Version 8. Download the .zip and unzip the JDK to a folder.




If Tomcat and AltiReport are already installed on the server, follow these steps:

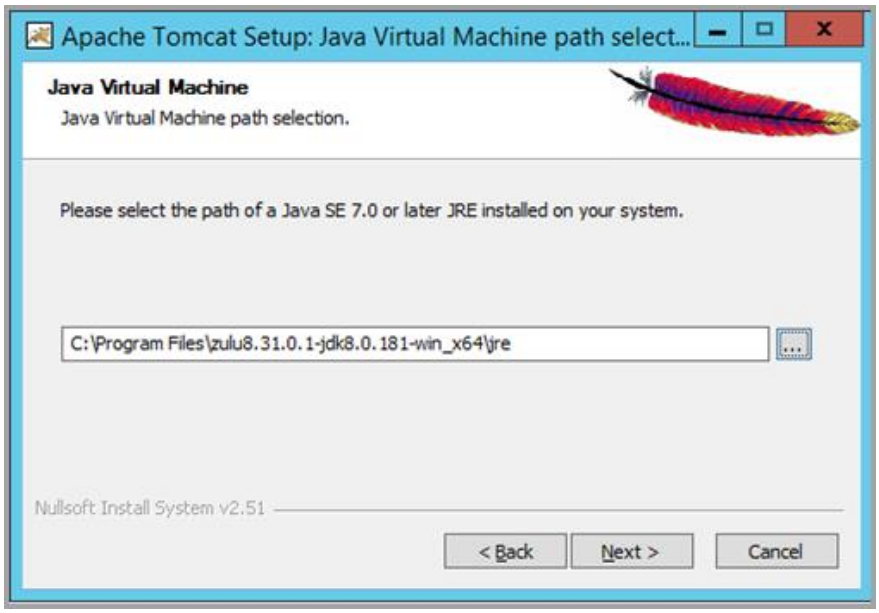
1. Open the Tomcat configuration. Switch to the *Java* tab.




2. Change the *Java Virtual Machine* entry to point to the jvm.dll file in the OpenJDK folder that was unzipped. The jvm.dll file can be found in \jre\bin\server\jvm.dll.
3. Apply the change and restart the Tomcat services.

If Tomcat and AltiReport have not been installed on the server, follow these steps:

1. In the Tomcat installation, proceed with a normal installation until you reach the *Java Virtual Machine path* selection.




2. It will default to any Oracle JRE installations on the system. Change the directory to the JRE directory inside the OpenJDK folder.

3. Proceed with the rest of the installation. The Tomcat Java Virtual Machine will be set to run using the OpenJDK jvm.dll as part of the installation process.

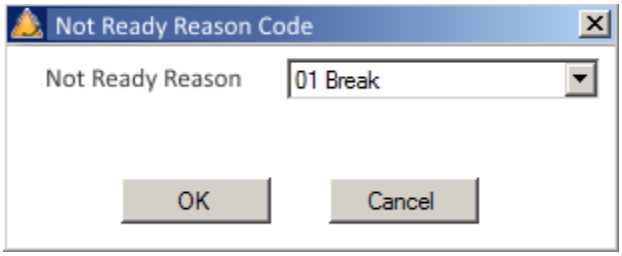
# Not Ready Reason Codes

You can now configure various codes that agents can use to specify why they are switching to *Not Ready* status. You can make reason codes mandatory or optional.

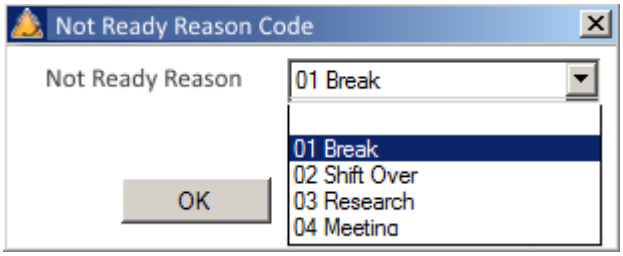
1. In MaxAdmin, choose **Call Center** > **Reason Code Configuration**.
2. Click the **Agent Not Ready Reason** tab.
3. In the table, enter the various reason codes that you want to present to your agents, one per field. For example, you might include terms such as Break, Shift Over, Meeting, Research, Training.
4. If you want to require agents to specify reason codes, then check the option *Not Ready Reason Code Required*. To make entry of reason codes optional, leave the checkbox cleared. Click **OK**.

## Not Ready Reason Codes in MaxAgent

If you select the option *Not Ready Reason Codes Required*, then agents will not be able to set their status to *Not Ready* until they enter a code. A pop-up will open if they click to change their status. If they click **Cancel**, they will see a warning message and will remain in *Ready* state.




If you do not select the option *Not Ready Reason Codes Required,* then the pop-up will still open, but they will have a blank option in the pulldown menu that they can choose instead of a reason code.




The Not Ready Reason Code is a system wide option so if the required box is check (which is optional) you will no longer be able to use the #91 (Not Ready) from your phone.

## Not Ready Reason Codes in MaxSupervisor

In MaxSupervisor, users will see the *Not Ready Reason Code* in the Agent State display. The code will also appear in the Agent View and Worgroup View > Agent State views.

## Reports Which Include Not Ready Reason Codes

Not Ready Reason codes will appear in the Agent Activity Event Report.

- The state (Not Ready) will appear in an Activity Type column
- A new column shows the Not Ready Duration
- A new Reason column shows the reason for each Not Ready event.

# Call Disposition Codes

Admins can now set up custom Call Disposition codes. These codes are typically descriptions of the final outcome of the call, and are a simple way to label or categorize calls.

For example, a Technical Support organization may choose to set up Call Disposition codes of *Resolved*, *Researching*, *Feedback*, *Follow up*, and so on. A service organization may set up Call Disposition codes such as *Appointment Scheduled*, *Product Question*, *Service Inquiry*, and so on.

Please take the following behavior into account when designing and implementing Call Disposition Codes:

- Be aware that Disposition Codes **cannot be removed once they are configured**.
- We strongly recommend that you do not change Disposition Codes once they are configured, because this will skew any report data. You should add new codes rather than change existing codes.
- Call Disposition codes can be made mandatory or optional for individual workgroups.
- During a call, agents can change a Disposition Code if they have already specified one. The last code the agent chooses will be retained.

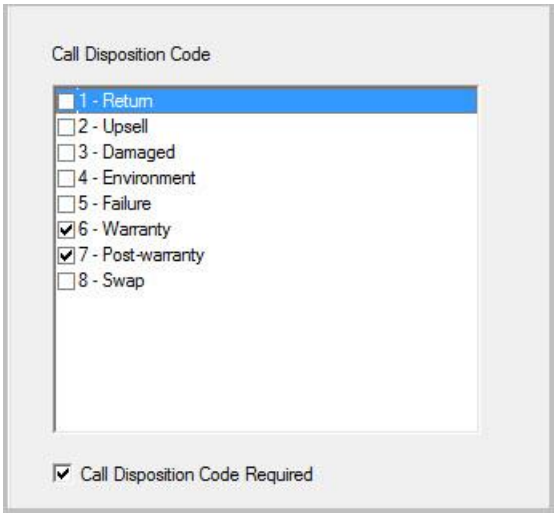
## Creating Call Disposition Codes in MaxAdmin

1. In MaxAdmin, choose **Call Center** > **Reason Code Configuration**.
2. Click the **Call Disposition** tab.
3. In the table, click **Add**, and then enter the label for this disposition code. Click **OK**.

## Configuring Call Disposition Code Options for a Workgroup

You can specify which Call Disposition codes apply to each workgroup. You can also specify, for each workgroup, whether Disposition Codes are required or optional. If you want to require Disposition Codes, you can require them for inbound workgroup calls, for outbound workgroup calls, or for both.

1. Open the Workgroup Configuration panel. Select the workgroup.
2. Click the *Call Disposition* tab.
3. Select the codes that you want to make available for that workgroup (up to 64).
4. If you want to enforce Disposition codes, first check the option **Call Disposition Code Required**. Then select whether you want to enforce codes for inbound, outbound, or both types of workgroup calls. Click **Ok**.



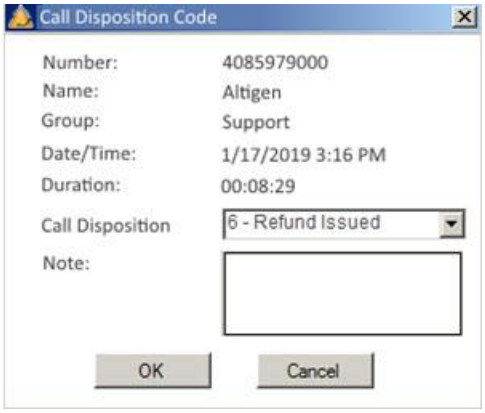

## Considerations

Before you enable the *Call Disposition Code Required* option, be aware of the following behavior.

- Agents who do not enter call a Disposition Code for a call **will automatically be set to *Not Ready***. This will leave you with fewer agents available to handle incoming calls. For example, if you have 3 workgroup agents logged in and one of those agents has not entered a Disposition Code for a call and has been set to *Not Ready*, that leaves your workgroup with only two agents able to handle incoming calls.
- Note that agents can ignore the Disposition Code popup and **place outgoing calls on physical extensions**. (For IPTalk extensions, the system will prevent the agent from placing calls until the agent enters a code.) Note that you can run report 1305 to detect agent *Not Ready* status with a reason code of *Disposition Code*.
- Be aware that agents who have physical phones can answer an incoming workgroup call *without opening the MaxAgent application*. When the agent hangs up the call, the system sets this agent to *Not Ready* until a Disposition Code is entered. However, if the agent does not have MaxAgent open, the agent will not be aware that a Disposition Code is required to return to *Ready* mode. Therefore, in order for this feature to work effectively, **agents must have the MaxAgent application open** – even those who take calls on a physical phone.

# How Agents Enter Disposition Codes in MaxAgent When Codes are Required

When a workgroup call is disconnected, the *Disposition Code* dialog opens to allow the agent to select a code for this call.




The agent can also enter any appropriate notes for this call.

Notes:

- The popup will remain in the foreground until the agent enters a code.
- The **Cancel** button in this popup will be disabled, because the agent must select a code.
- **MaxCS will not present the agent with another workgroup call until a Disposition Code has been entered in MaxAgent**. Personal calls to the agent will still come in, even while incoming workgroup calls are blocked.
- The agent cannot close MaxAgent normally if a Disposition Code popup remains open.
- If the agent state becomes available (after any wrap-up interval has passed), MaxCS sets the agent's state to *Not Ready*, with a Not Ready Reason Code of *Disposition Code*. This allows supervisors to determine whether agents are avoiding calls by not entering a required Disposition Code.
- If the MaxAgent application goes down mid-call for some reason, Disposition Codes for the interrupted call will no longer be required when the agent re-opens MaxAgent. The Call Disposition Codes feature requires that MaxAgent be running during calls.

## How Agents Enter Disposition Codes When They are Not Required

Agents can still enter Disposition codes, even if the workgroup does not require codes to be entered. Agents can right-click the call and select Call Disposition Code from the menu.

## Reports That Include Call Disposition Code Data

New reports have been added:

- Workgroup Call Disposition Code Summary report (2320)
- Call Disposition Code Summary Report by DNIS (3301)
- Call Disposition Code Summary Report by Agent (1305)

The following reports also include Disposition Code data:

- The Agent Call Detail Report (1102)
- Workgroup Call Detail Report (2101)
- DNIS Call Detail Report (3101)

## Call Disposition Code Data in CDRs

The following tables have been updated for Call Disposition Code data:

### CDRMAIN Table

- DispositionCode (int, null): new column
- DispositionDescription (varchar(64), null): new column
- DispositionNote (varchar(256), null): new column

### DISPOSITIONCODE: New Table

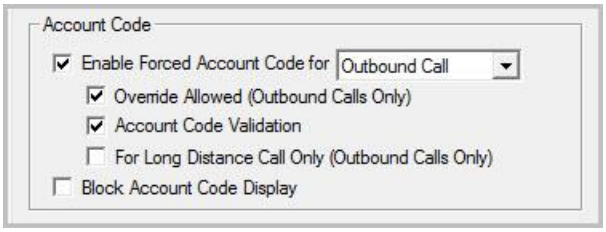
- Version (int, not null)
- NodeID (int, not null)
- Code (int, not null)
- Description (varchar(32), not null)
- StartTime (int, null)
- EndTime (int, null)
- StartTimeGMTOffset (int, null)
- EndTimeGMTOffset (int, null)
- RevisionID (int, not null)

# Account Code Enhancements

You can now require account codes for inbound calls in addition to outbound calls. You configure this on an extension basis.

To configure the account code settings,

1. Open the *Extension Configuration* panel and switch to the *Restriction* tab.
2. For the *Enable Forced Account Code* setting, select an option:
   - Outbound Call (which is the default setting)
   - Inbound Call
   - Both – this option forces agents to enter account codes for both incoming and outbound calls
3. Select any of the other options:
   - Override Allowed – allows the agent to override account code entry for outbound calls
   - Account Code Validation – validates the account code entered
   - For Long Distance Calls Only – forces account code entry only for long-distance outbound calls
   - Block Account Code Display – hides the account code list; the agent must enter the code manually
4. After selecting all options, click **OK**. You can also use the **Apply To** button to apply this setting to other extensions.




When account codes are required, agents will see the Account Code pop-up for incoming calls.

When account codes are not required, agents can still enter a code for a call by right-clicking the call and selecting Account Codes.

### Account Codes in Reports

In the Agent Call Detail Report (1102) and the Workgroup Call Details (2101) report, you can now search by Account Code.

## Security Update

This release includes a security change which prevents a configuration file from being read remotely. As part of this change, MaxAdmin is initially configured to accept only local access.

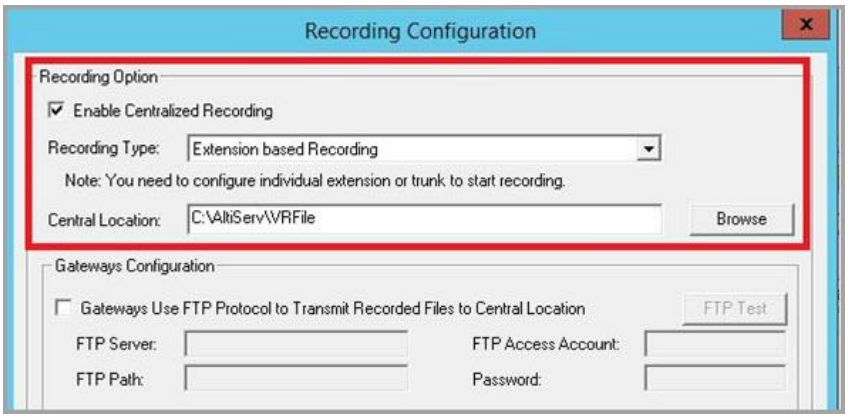
This means that you must update the IP Dialing Table in Enterprise Manager, to add any IP addresses that you need to allow.

1. Clear your browser cache.
2. Try to open http://:10043/..%2f..%2fwindows/win.ini remotely. Confirm that the system will not allow you to access this file.
3. To allow access to an IP Address, add an IP address entry to the IP Dialing Table in Enterprise Manager and publish this as a 'Global' type.
4. Try to access the IP address from step 3 remotely. The system should allow you to access that address now because it is listed in the IP Dialing table.

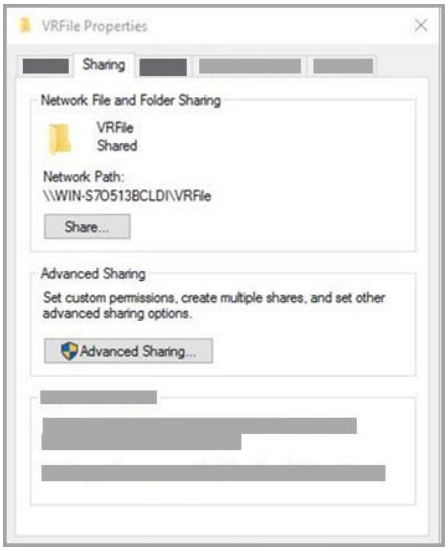
# VRM Pro Update

To disable Server Message Block signing (SMB) v1 on servers without obstructing the transfer of voice recordings to the VRM server,

1. Set up the recording configuration on MaxAdministrator.




2. Whichever folder you specified in step 1, edit its properties and make it a shared folder.




3. In VRM Pro Admin, open the MaxCS ACM tab. Specify the email address based upon which SMB version you are testing (refer to the next figure):

   3.1 For testing SMB2, add ";use_winnet" at the end of the user email account field. For example:

   a. administrator;use_winnet

   b. alti2013;administrator;use_winnet

   c. administrator@alti2013.com;use_winne

   3.2 For testing SMB1, do not add ";use_winnet" at the end of user email account field. For example:

   a. administrator

   b. alti2013;administrator

   c. administrator@alti2013.com


4. Make a call. MaxCS will generate the recording files.
5. Check the protocol when VRM Pro tries to transfer the recording file(s) from the MaxCS shared folder:
   5.1 Install Wireshark to monitor the network packet.
   5.2 Try to add a filter ip.addr == MaxCS_IP_Address
   5.3 For testing step 3.1, you will see the SMB2 packet when VRM Pro is moving the recording files. For testing step 3.2, you will see the SMB1 packet when VRM Pro is moving the recording files.
6. If you want to ensure that the SMB1 was not running during the testing procedure, you can use the following power shell script to disable SMB1 on your MaxCS machine.
   6.1 Detect the SMB1 feature:
   Get-WindowsFeature FS-SMB1
   6.2 Disable the SMB1 feature:
   Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
   6.3 Enable the SMB1 feature:
   Enable-WindowsOptionalFeature -Online -FeatureName smb1protocol

# 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 know limitations with this release.

- MaxOutlook display issues – If the main MaxOutlook window does not appear, the issue may be a result of some Microsoft API changes. To fix this issue, in Outlook choose **File** > **Options** > **General**. In the User Interface settings, choose the *Optimize for compatibility* option. Restart the application and it should now use the old Windows API.
- For the Callback from Queue feature, note that callers can request a callback multiple times.

# 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