Mitel MiContact Center Enterprise

TAS INTEGRATION – INSTALLATION INSTRUCTIONS

RELEASE 9.5 SP3

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

MiContact Center Enterprise TAS Integration – Installation Instructions
Release 9.5 SP3 – April 2022

INTRODUCTION

This document describes the installation and integration of Telephone Application Service (TAS) with MiContact Center (MiCC) Enterprise. TAS provides call control connectivity to call managers that support the SIP protocol. In this configuration, TAS is for call and media control used instead of Open Application Server (OAS).

When using TAS with MiCC Enterprise, the underlying call manager must support RFC3891, Replaces Header.

For a list of call managers supported for this configuration, please consult the Compatibility Matrix.

SYSTEM ARCHITECTURE

The following figures display a general overview of the system architecture when MiCC Enterprise is integrated with TAS, both in a single server configuration as well as multiple TAS servers.

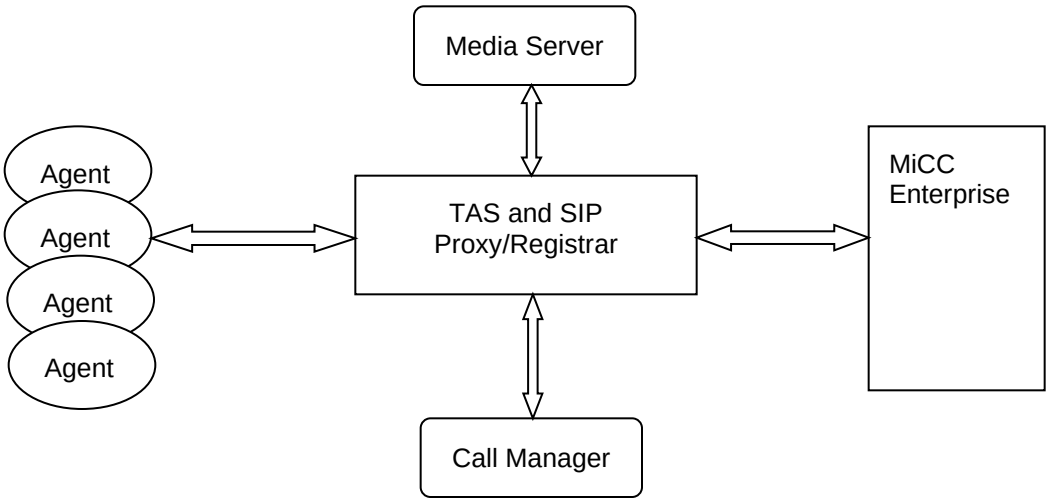


Figure 1: Overview of system components – single TAS server

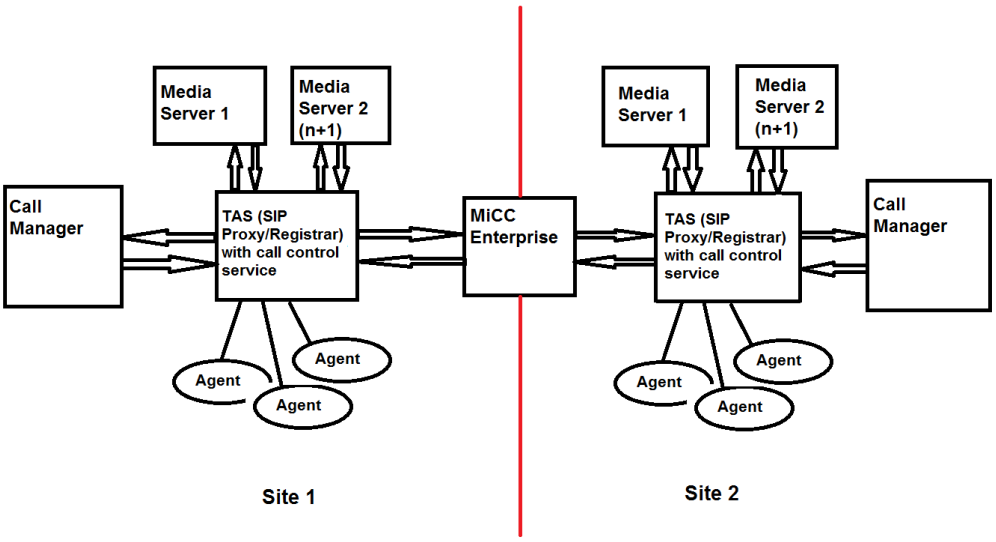


Figure 2: Multi-TAS configuration with single MiCC-E server connected to multiple TAS servers, each TAS server connects to its own call manager and Media Server(s).
Note that this configuration is only supported for systems where calls are isolated to one call manager. For example, a tenanted system, where each tenant has a separate associated call manager.

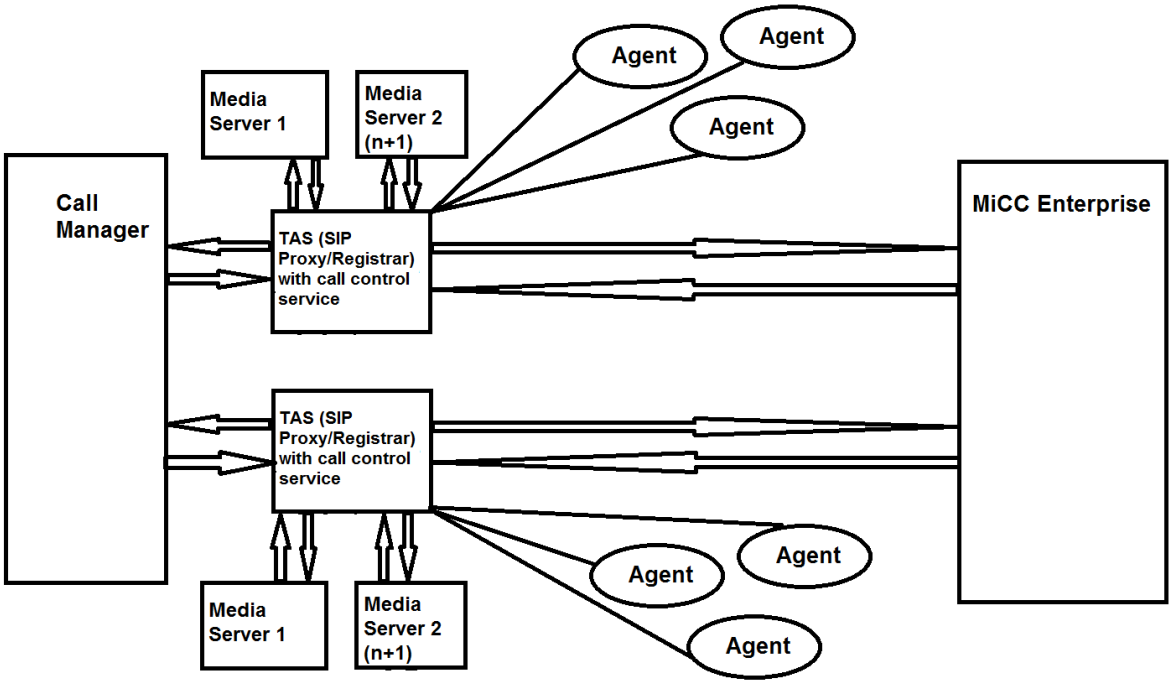


Figure 3: Multi-TAS configuration with single MiCC-E server connected to multiple TAS servers due to capacity and/or redundancy requirements, connected to one call manager

TAS AND SIP PROXY / REGISTRAR

The TAS and SIP proxy/registrar are contained within the same Windows service. TAS exposes a CSTA Phase III interface to connected CSTA clients, to make telephony requests and receive events.

The SIP Proxy/Registrar provides an endpoint for SIP clients to register toward, as well as to receive and send SIP events.

MEDIA SERVER

The Media Server provides media integration, such as playing messages, collecting DTMF digits, and conferencing multiple parties together.

Each Media Server can support up to 500 connection points. An active call for an agent using a desk phone requires 2 connection points (soft phone agents only use one connection point), and each queued call requires 1 connection point. The number of Media Servers added to the system should be based on the traffic handling required for the system.

MICONTACT CENTER AGENT AND WEB AGENT

MiCC Agents running as SIP softphone clients register as SIP clients toward the SIP Registrar in the TAS service. Web Agent does not support SIP softphone clients.

Agents using desktop phones are supported in MiCC Agent, Web Agent and as Phone Agents.

MICC ENTERPRISE

The MiCC Enterprise Call Control Service connects to the CSTA interface in TAS to send call and media requests and receive events. TAS provides a call control and media interface to the MiCC Enterprise Call Control Service.

Other MiCC Enterprise services requiring call and media control, such as the Router Service, Agent Service and Script Manager, connect to the Call Control Service.

CALL MANAGER

The call manager supports SIP trunks which are configured to route to TAS. This allows incoming service group calls to be routed to MiCC Agents via TAS.

In addition, the call manager can be configured with MiCC Agent extensions to route into TAS so that agents' extensions may be dialed directly from the other extensions in the call manager.

CAPACITY AND DIMENSIONING

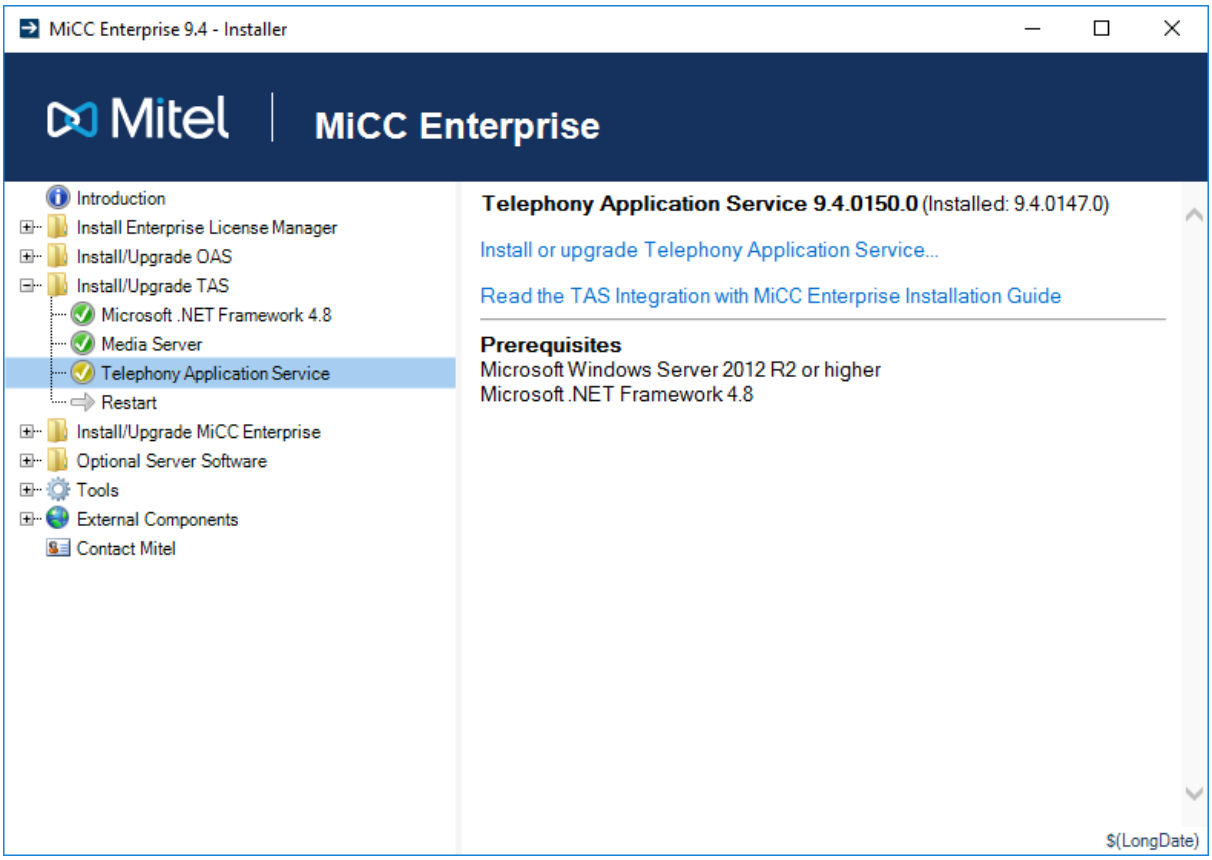
The capacities and dimensioning guidelines are documented in the MiCC Enterprise System Description (3/1551-LXA19154).

TAS AND MEDIA SERVER INSTALLATION

The following steps are required to install MiCC Enterprise with TAS:

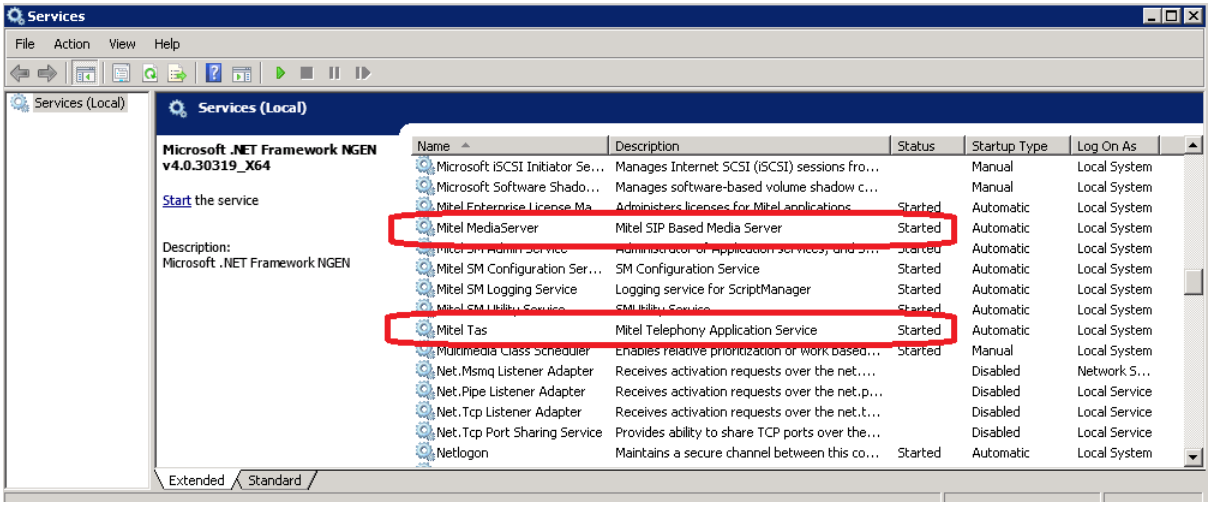
- Install Media Server
- Install TAS
- Configure Media Server and TAS components
- Install MiCC Enterprise
- Configure call manager data
- Configure call manager SIP trunks

The TAS, Media Server and MiCC Enterprise installations can be launched from the Mitel Package Browser.



Media Server and TAS installations are silent if initiated from the package browser.

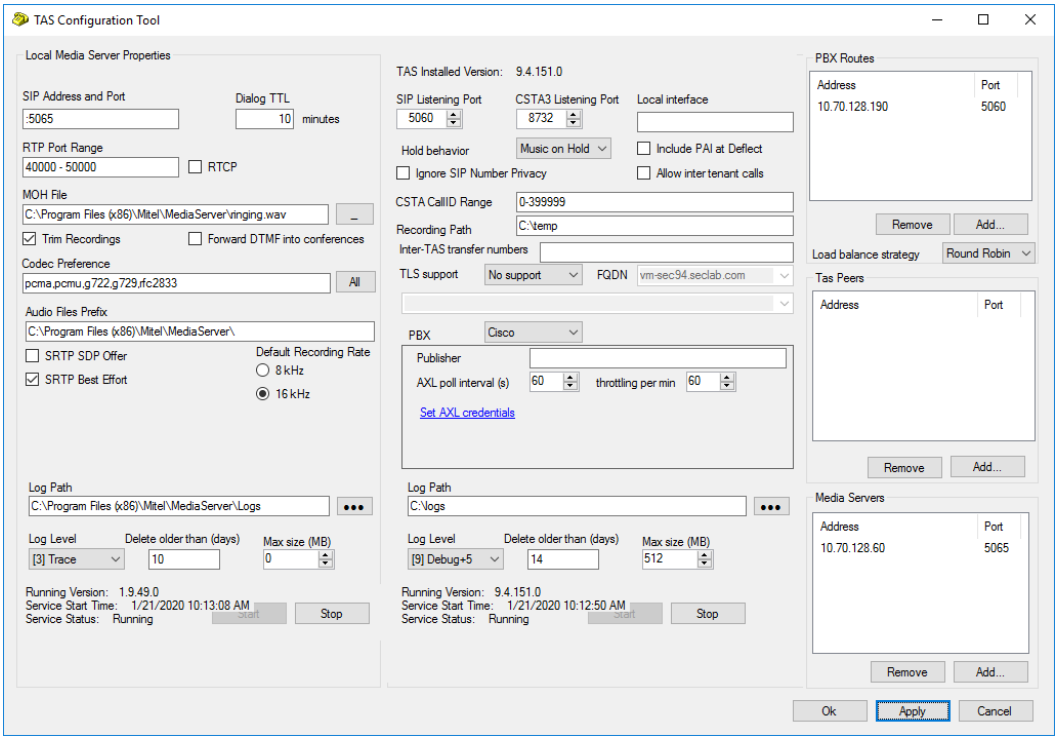
Once installed, you can stop and start TAS and the Media Server from the Services control panel applet or from the TAS Configuration tool described below.



TAS AND MEDIA SERVER CONFIGURATION

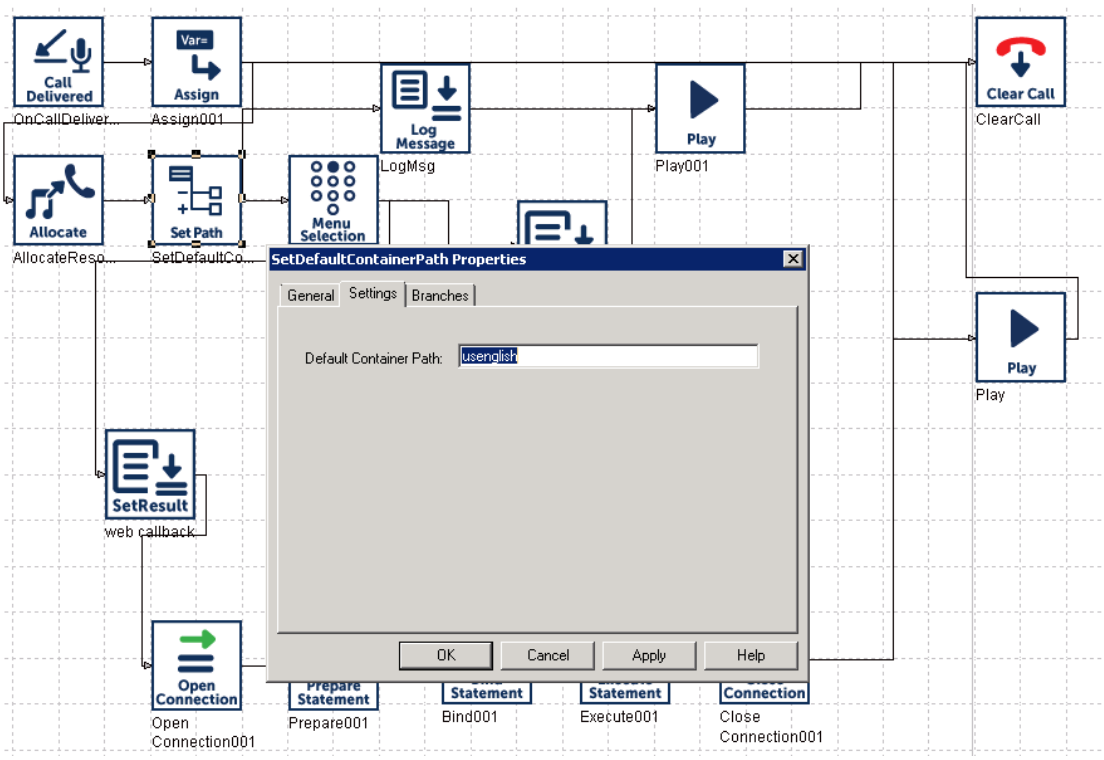
After the Media Server and TAS are installed, you must configure them. The TAS and Media Server configuration is enabled through the TAS Configuration Tool, which is available from the **Start** menu after TAS has been installed.

After installation, the Media Server configuration can be left at the default settings (except for the AudioFiles Prefix setting) unless there is a conflict with current ports in use. The following figure shows a sample Media Server configuration.

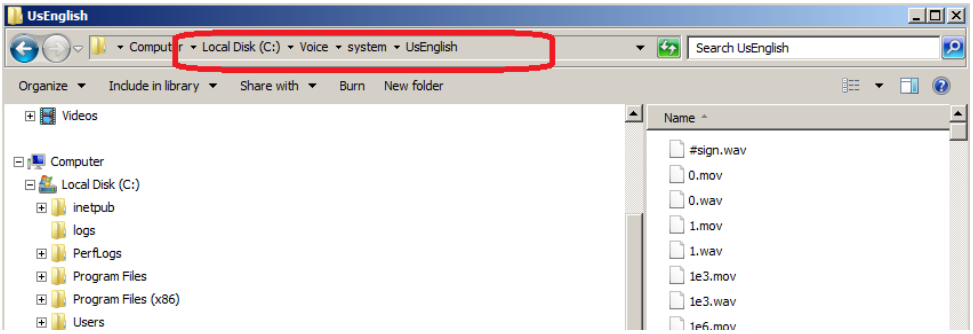


Note: You must use a backslash at the end of the Audio Files Prefix path. A "Set Default Container" block is used in Script Manager scripts, and the leading backslash is not accepted in that block. Be sure to test Router Service Accesses with this change to make sure the associated prompts are played correctly.

An example of a Script Manager script that uses the SetDefaultContainer block after a resource allocation and before a play message request is shown below.

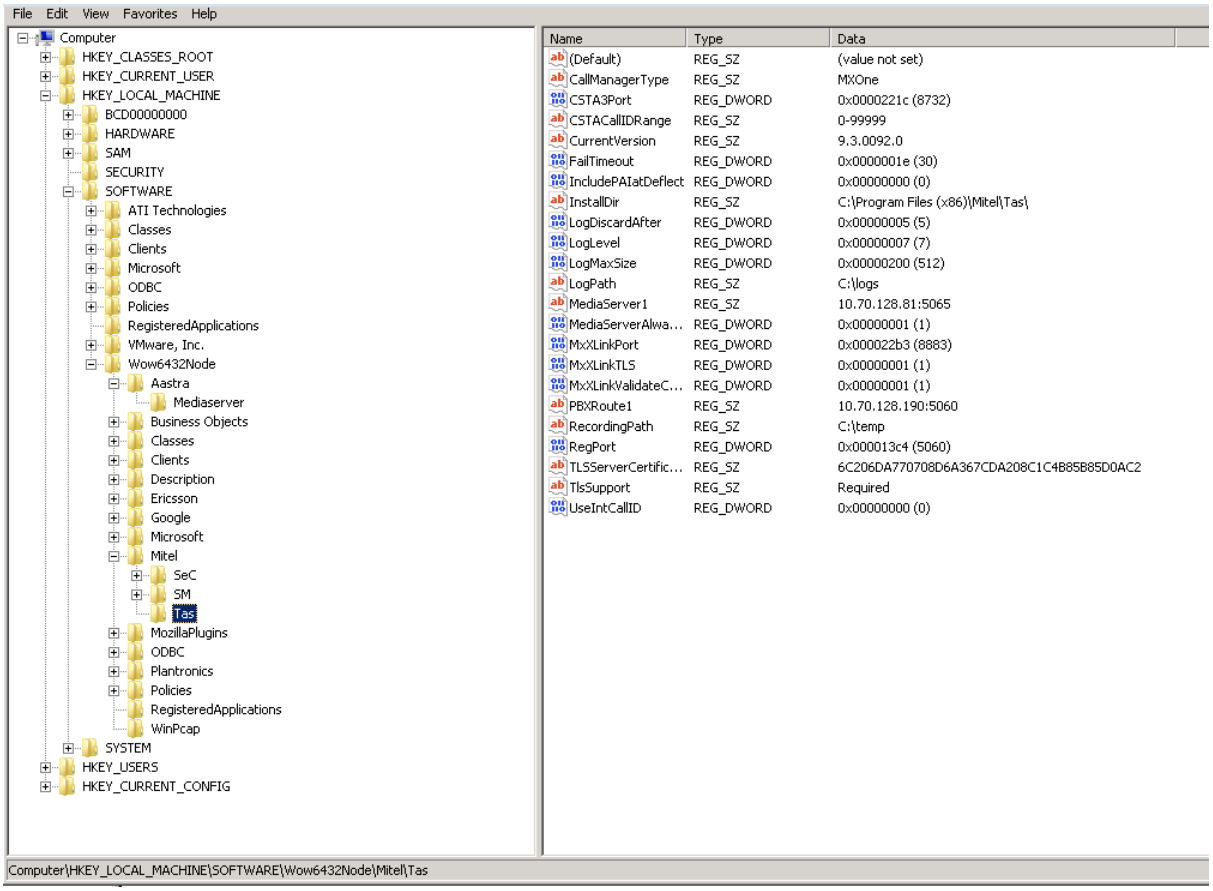


The following figure shows how the prompt files and folders are stored on the disk to support the script shown above.



TAS and Media Server configuration data location

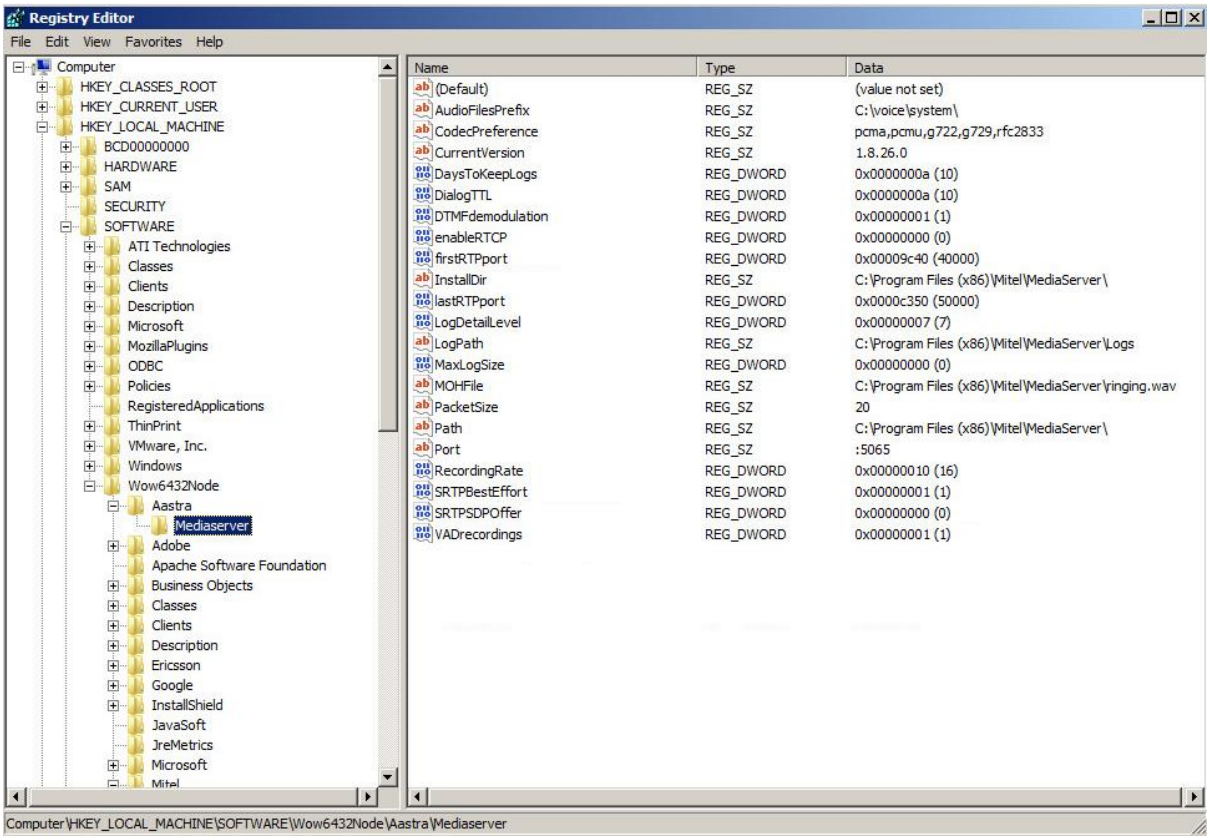
The TAS configuration is stored in the registry at **HKLM\Software\Wow6432Node\Mitel\Tas**.



The FailTimeout timer (shown above) is not exposed in the TAS Configuration Tool, and is used in conjunction with the Intrude function, where a third party wants to intrude on a call-in-progress. The third-party calls one of the call participants, but the call fails (participant is busy), leaving the connection in a failed state. If MiCC Enterprise designates the failed connection as an Intrude call, TAS puts the call through, resulting in a three-party call. If MiCC Enterprise does not recognize the failed connection as an Intrude call, the call is cleared when the FailTimeout interval has elapsed.

The InviteTimeout timer prevents hanging calls in TAS when there is no response to an INVITE within a certain period (default is 185 seconds). The InviteTimeout timer is not written to the registry by default but can be added and the default value changed.

The Media Server configuration data is stored in the registry at **HKLM\Software\Wow6432Node\Aastra\Mediaserver** (shown below).



Media Server settings

The following table describes Media Server settings.

SETTING	DESCRIPTION	DEFAULT VALUE
SIP port	The port TAS uses to connect to the Media Server. *:port* for the default Ethernet interface, *<interface>:port* for a specific Ethernet interface.	:5065
Dialog TTL	The interval for a simple “session timer” that uses OPTIONS SIP message to check if the call is still up	10 mins.
RTP port range	Ports used for RTP	40000-50000
RTCP	Indicates whether the media server sends RTCP Sender Reports and Receiver Reports	Unchecked
MOH file	File to be used for playing music on hold to callers when held, if configured in TAS configuration settings. **Note:** To configure a different music on hold file per MiCC-E tenant, add the following registry value to the	<InstallDir>\Ringing.wav

	MiCC-E server: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CCRouter\Parameters\TASMoHFiles Type = REG_SZ Data = <TenantID1>:<MoHFileName1>,<TenantID2>:<MoHFileName2>, etc. For example, to set c:\files\MoHTenant1.wav for Tenant 1 and c:\files\MoHTenant2.wav for Tenant2, configure the registry value as the following: 1:c:\files\MoHTenant1.wav, 2:c:\files\MoHTenant2.wav Note that a restart of the MiCC-E Router Service is required if this value is modified in order for it to take effect.	
Trim Recordings	Indicates whether the media server should remove trailing silence from recordings	Checked
Forward DTMF into conferences	When DTMF is sent from the call manager, the digits are received by the Media Server and reported to TAS. If the agent calls to an external IVR system, it is preferred to forward the DTMF signals from the Media Server to the call manager, which is achieved by checking this option.	Unchecked
Codec Preference	Codecs to be used, in order of preference.	pcma, pcmu, g.722, g.729, rfc2833
Audio Files Prefix	The location of the message prompt files.	C:\temp\
SRTP SDP Offer	Indicates whether the media server includes a crypto attribute (as described in RFC 4568) in the SDP offer generated.	Unchecked
SRTP Best Effort	Indicates whether SRTP Best Effort is used. If not checked, the “Strict SRTP” is used. If enabled, the SDP offer has the RTP/AVP profile; if unchecked, the RTP/SAVP profile is used. Best effort allows SRTP to be turned off through SIP negotiation; while strict does not allow SRTP to be turned off if the call has started with SRTP. ** See note below	Unchecked
Default Recording Rate	8kHz or 16kHz Configures the sample rate when TAS is recording wave files. The default is 16kHz, since that is the value used internally by the Media Server.	16kHz
Log Path	The location of the Media Server log files.	<InstallDir>\Logs
Log Level	Indicates the amount of detail to be logged. When a problem is experienced, it is preferred to have a log level of 7 or higher.	Trace
Max size	Maximum size of the log file. When the maximum size is reached, a new log is opened. Size is unrestricted if left	0

	at default and a new log is opened each day	
Delete older than (days)	Length of time the log file is maintained before it is discarded.	7 days

Note that for SRTP, there is no way to force it one way or the other. If an INVITE with (or without) crypto attribute is received, the media server always answers with (or without) crypto attribute regardless of the settings. For calls without SDP, SRTP is enforced if SRTP SDP Offer is selected and SRTP Best Effort is not selected.

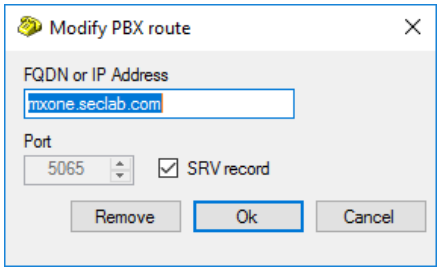
The media server picks up most configuration changes while running. However, if any changes are made to the SIP port configuration, the media server must be restarted.

TAS configuration settings

The following table describes TAS configuration settings.

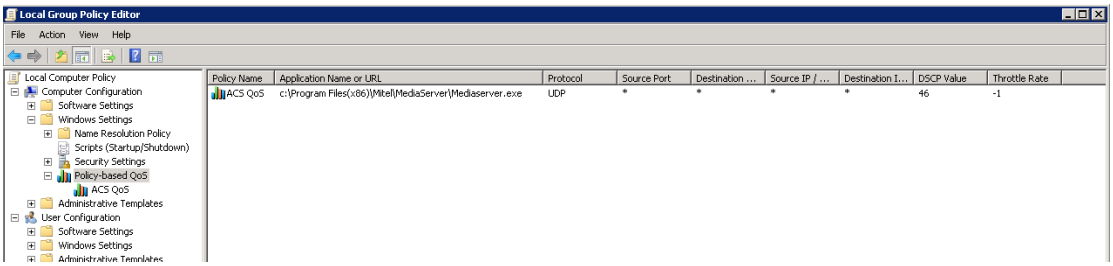
SETTING	DESCRIPTION	DEFAULT VALUE
SIP Listening Port	The port that TAS uses to listen for both TCP and UDP. If TLS is enabled, TAS listens to one port higher than the value entered, i.e. if 5060 is entered, TLS will use port 5061.	5060
CSTA3 Listening Port	The port the TAS CSTA3 Web Service listens to. By default, only TCP bindings are used.	8732
Local interface	By default, TAS sets the local IP address to the address set with the default gateway. To use a different interface, set the IP address in this field.	Empty
Hold Behavior	Determines whether Music on Hold is played while a call is on hold. Inactive = no music on hold provided; audio is set to inactive Music on Hold = music on hold played for held calls Send only = no music on hold provided; audio is set to send-only Note that TAS will only play Music on Hold for sessions which have a media session connected. Therefore, private calls made directly to an agent extension will not have Music on Hold when put on hold, even if this parameter is configured for Music on Hold.	Inactive
Include PAI at Deflect	Option to include the P-Asserted-Identity (PAI) header in the INVITE message sent to the receiving port. The PAI includes the number of the called Basic Virtual Device (BVD) number. When this option is enabled, the hard phone displays the originating Service Access number. Note, however, that	Unchecked

	the phone agent cannot call the original caller back with this option enabled. When disabled, the hard phone displays the number of the originating caller (making it possible for the agent to call the originating caller back).	
Ignore SIP Number Privacy	If SIP indicates that the number provided in the P-Asserted-Identity or Remote-Party-ID field is private, the number will not be displayed to the agent or recorded in the CDR data. Check this option to override this and always show the numbers regardless of the SIP privacy setting.	Unchecked
Allow inter tenant calls	By default, agents cannot call to or receive calls from a number associated with another MiCC-Enterprise tenant. The call will be rejected. If this option is checked, calls between tenants will be allowed.	Unchecked
CSTA CallID Range	Starting Number for CSTA CallID	300000-399999
Recording Path	The path on the media server where .wav files recorded with the Script Manager Record block are stored. If multiple media servers are configured, a directory synch mechanism must be deployed. Synchronization of media server folders is not automatically done by TAS or the Media Server.	C:\temp
Inter-TAS transfer numbers	For multi-TAS systems, this number is used by the TAS systems to communicate with each other. All TAS systems will subscribe to the Inter-TAS transfer numbers configured on peer TAS systems. When a call is sent to another TAS system, a SIP INFO message is sent to the target TAS system, and a SIP REFER is made for the call to the defined Inter-TAS number. The target TAS system is able to identify the call through the CSTA identifier in the SIP INVITE, as well as the SIP INFO message. Note that the Inter-TAS transfer numbers must also be configured in the call manager so that calls sent via SIP REFER to the Inter-TAS transfer number are routed to the correct TAS system. The number should include a trunk access code for the SIP trunk connected to the target TAS system, and in the same number range as the configured BVDs, but not used as a BVD in the system. Note: For Telepo systems, the entered value will be a range of numbers. For example, 100-109, 150, 180-189. A number from the Inter-TAS transfer number range will be selected when a call is sent via SIP REFER to another TAS when using Telepo. If an Inter-TAS transfer number is not available, a call will be blocked from being sent to another TAS until a number becomes available, so a sufficient number range should be configured to handle the number of simultaneous inter-TAS calls expected. Inter-TAS transfer numbers are only in use during the call setup process between TAS systems. Normally this takes less than 0.5 second. Once the target TAS receives the call, the number is deallocated and available for reuse.	Empty

TLS support	Whether TLS is not supported, supported or required	Not supported
FQDN	Enabled when TLS is selected, allowing entry of the host name with the fully qualified domain name. The name entered here is the value which TAS will use to identify itself when communicating with the call manager.	Host name with fully qualified domain name.
Certificate selection	Drop down list for selecting certificate for TLS support	Empty
PBX	Tabs for call manager specific configuration, including MX-One, Cisco, Telepo or Other. This determines which call manager specific features can be enabled in TAS.	Not selected, required to be selected at first configuration
Log Path	Path to TAS logs	C:\logs
Log Level	Verboseness of TAS log	Debug+3
Max Size	Maximum size of the log file. When the maximum size is reached, a new log is opened. Size is unrestricted if left at default and a new log is created each day.	512 MB
Delete older than (days)	Length of time the log file is maintained before it is discarded.	14 days
PBX Routes	Note that when adding or modifying a PBX Route, the following dialog is displayed:  Enter the fully qualified domain name or IP address and port of the call manager. A DNS domain name can also be entered, which contains one or more HOST records. Enable the SRV record option if DNS SRV records are used. If SIP SRV records are used, only 1 PBX route may be defined. Load balancing is determined by the priority and weight of the SIP SRV records defined in the DNS server.	<IP address>:<port>
TAS peers	The FQDN or IP address of other TAS servers in a multi-TAS system	<IP address>:<port>
Media Servers	The FQDN or IP address and port of the Media Server host.	<IP address>:<port>

QUALITY OF SERVICE POLICY FOR MEDIA SERVER

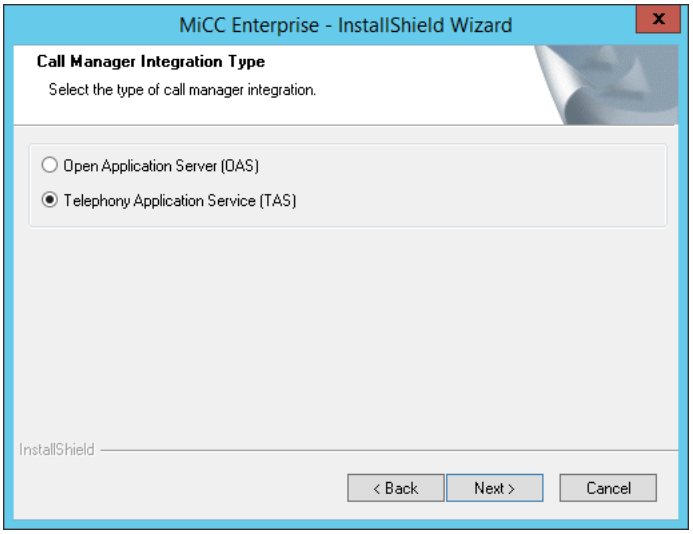
Use the Local Group Policy Editor to configure the Quality of Service (QoS) policy for the media servers by running gpedit.msc and configuring a policy as shown below. The QoS policy properly fills in the TOS field in the IP packets in the RTP stream and all RTP streams going to and from the media servers.



1. In the Local Group Policy Editor, navigate to **Local Computer Policy** > **Computer Configuration** > **Windows Settings**.
2. Right click on **Policy-based QoS and create new policy…** .
3. Specify a name for the QoS policy (e.g., TAS_QoS).
4. In the **DSCP Value** field, enter 46 and click **Next**.
5. Specify a specific application name as the path to the MediaServer.exe executable, and click **Next**.
6. On the page allowing to and from any source and destination IP address, click **Next**.
7. Select UDP as the protocol the policy applies to and click **Finish**.

INSTALLING MICC ENTERPRISE

During the installation of MiCC Enterprise 9.x, there is a call manager Integration option to use either an OAS or a TAS-based system. When prompted for the call manager type, select Telephony Application Service (TAS). It is not necessary to install OAS.



CALL MANAGER DATA CONFIGURATION

When MiCC Enterprise is integrated with TAS, call manager data must be configured in MiCC Enterprise Configuration Manager. The following sections describe the data that must be configured.

MESSAGE PROMPT FILES

Message prompt files should be copied from the MiCC Enterprise installation DVD to the location of the Media Server. The files should be copied into the directory specified as the Audio Files Prefix in the Media Server Configuration. For example, if c:\voice\system\ is configured as the Audio Files Prefix, the files should be copied into this directory under a subdirectory indicating the supported language. For example: c:\voice\system\USEnglish.

The system message prompt files that traditionally were installed by an OAS installation are now available from the MiCC Enterprise installation media.

If custom message files are defined, they should be added to the appropriate directory depending on the language. For example, if custom message files are used in a non-Script Manager Service Access or in a Service Group defined with the language US English, the files should be copied to the c:\voice\system\USEnglish directory so that they will be accessible to the system.

TAS SITE SETUP

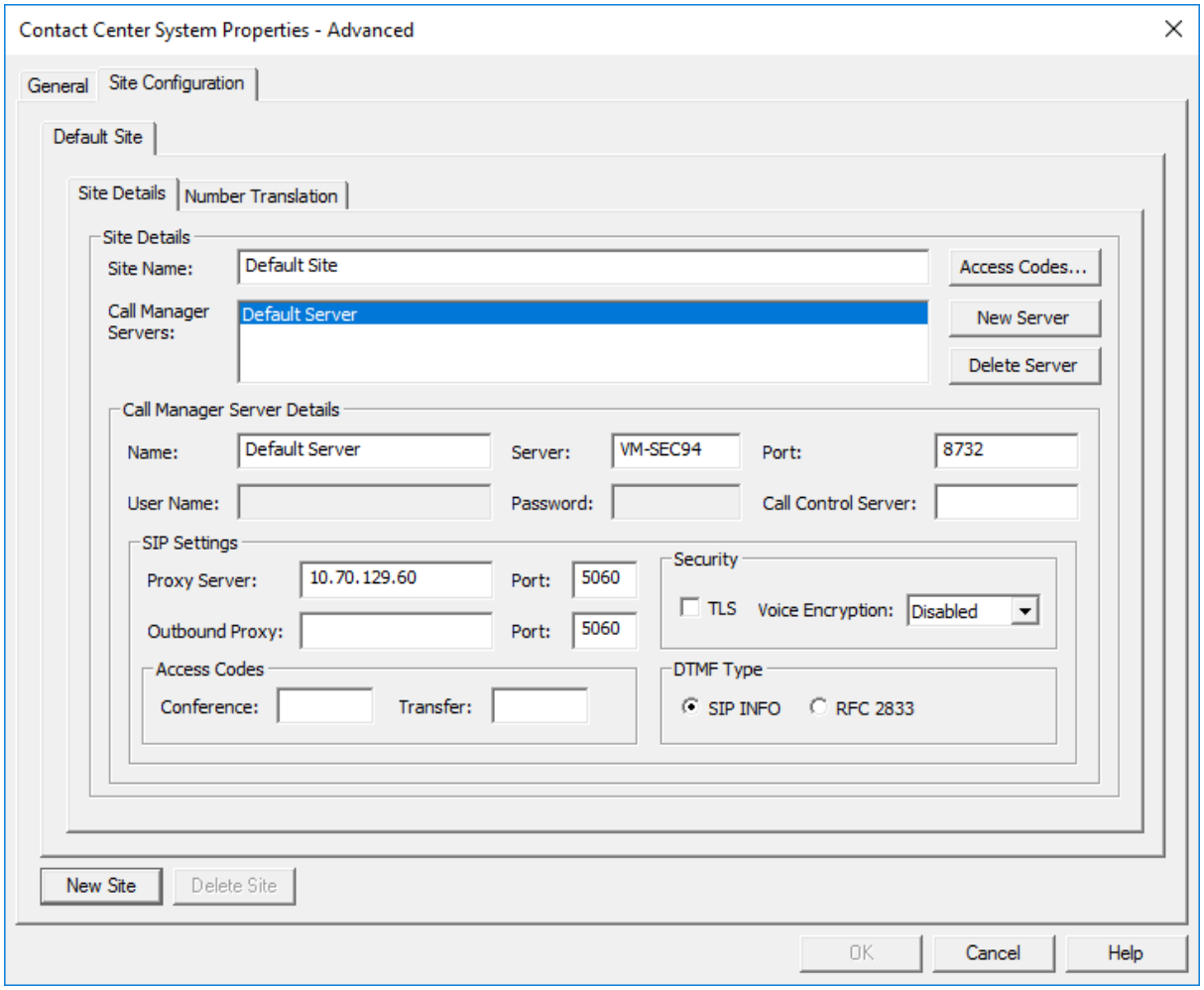
From Configuration Manager > System Properties > Advanced, add a site for the TAS Server.

On the **Site Details** tab, configure site information and details for the call manager server:

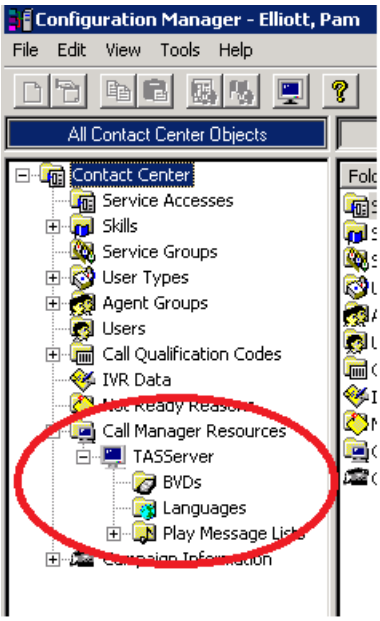
- **Name**: Name of the call manager server
- **Server**: indicates the machine where the TAS Service is installed. Note that it is recommended that the server name does not have the underscore character _ included in the host name, as this may cause softphone calls to be rejected.
- **Port**: the port configured for CSTA connections on the TAS Service
- **Call Control Server**: the machine hosting the MiCC-E Call Control Service. This can be left blank if it is the same as the server indicated in the **Server** field.
- **Proxy Server**: the IP address or hostname of the machine hosting the TAS Service
- **Port**: the port configured as the Registrar SIP Port on the TAS Server

  For TAS integration, do not configure any Access Code digits for Conference or Transfer. If present, MiCC Agent attempts to transfer using these access code digits instead of a SIP REFER method for conference and transfer.

For information on other settings, consult the *Configuration Manager Online Help*.



After the TAS site is added, Configuration Manager displays it under the Call Manager Resources folder.



You can now configure call manager data including BVDs, Languages and Play Messages. Below this is shown using the Configuration Manager application. It can also be done using Web Manager (see the Web Manager User Guide, 46/1553-LXA 119 154, for details).

BVD CONFIGURATION

Add the Basic Virtual Devices, or BVDs, which are used to route service group calls to MiCC Enterprise from the call manager. Each BVD number should correspond to the SIP trunk configured to route to from the call manager.

Note that a range of BVD numbers can also be assigned to one BVD name. In that case, any calls arriving to the configured numbers will be reported on the associated BVD name.

PLAY MESSAGE LISTS

Play Messages such as queue welcome messages and repeat queue messages are grouped together into a Play Message List. If your contact center is using multiple languages, it is recommended to add a separate Play Message for each language.

At least one Play Message List must be defined for the system.

LANGUAGES AND PLAY MESSAGE LISTS

The Languages and Play Message Lists are unique among tenants. There are no common languages or play message lists. If for example two tenants on a particular system wish to use the Spanish language, a unique Spanish language must be created for each tenant. The .rul files and the various subfolders for the “root container” are common between all tenants on the system and the relative path of the language specified media files are passed to the media server.

Play Messages

After the Play Message List is defined, Play Messages can be added to the list. The message prompt files provided with MiCC Enterprise can be utilized in the Play Messages, or it is possible to record new message files and use those.

On the General tab of the Play Message Properties, enter the Identification number for the Play Message. This number should be unique within the Play Message List.

Enter a description for the Play Message to help you identify its meaning.

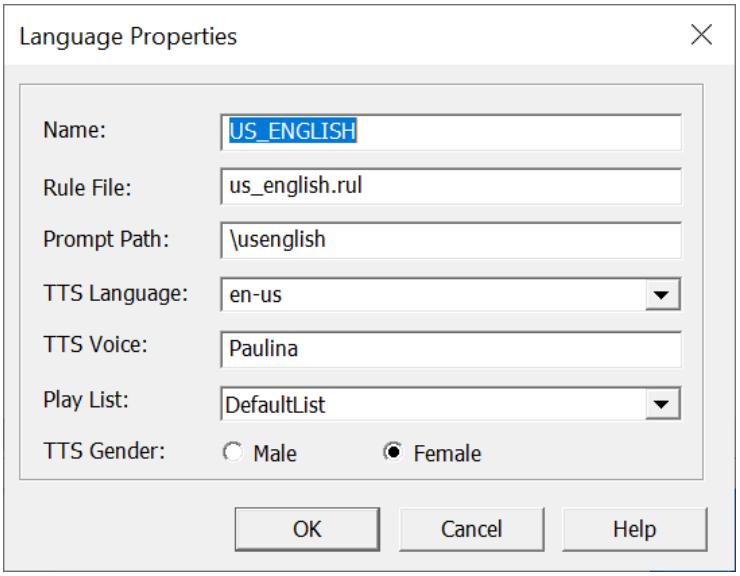
The Media Objects tab can be used to configure the content of the Play Message. For details on the various options available, consult the *Play Messages User Guide (4-1553 FAS10455)*.

Note: If Text to Speech (TTS) is used and a Play Message with a TtsMediaObject message object is defined, the Data field for the TtsMediaObject must contain the absolute file path for the file to be used. In addition, the file must exist on the Nuance server at the configured path.

In addition, ensure that the setting server.mrcp2.rsspeechsynth.rtpPacketSamples in the configuration file NSSServer.cfg on the Nuance server is set to 160. Otherwise, TTS messages will not play correctly.

Languages

After the Play Message List and Play Messages are defined, a Language can be configured. At least one Language is required.



Any descriptive name can be entered in the **Name** field.

The language Rule File designates the rules for how particular values, such as numbers, dates and time will be formatted. Enter the name of the rule file that should be applied for the language being defined.

Rule files are installed on the MiCC Enterprise Server at <InstallDir>\Services\Rule. The path does not need to be provided in the Rule File field, only the name of the rule file to be used.

In the Prompt Path, enter the relative location of the message prompt files to be used for this language. The value entered will be appended to the value defined as the Audio Files Prefix for the Media Server. In the example above, if the Audio Files Prefix is defined as c:\Voice\Files, the prompts for this language would be expected to be located at c:\Voice\Files\swedish. Ensure that the files exist at that location on the Media Server.

Note: The prompt path is only used when playing messages from the MiCC Enterprise Router Service, and not from Script Manager. When playing messages from Script Manager, the script must contain a Set Default Container block with the value set to the same value indicated in the Prompt Path field for the selected language. This will allow the system to find the message files by appending the value entered in the Set Default Container block to the path configured in the Audio Files Prefix for the Media Server.

If Text to Speech (TTS) is used, specify the language to be used. You can either select a language from the list or enter the language abbreviation. Note that the language abbreviation must match the available languages in the Nuance server. This language will be used for both TTS and Automatic Speech Recognition (ASR).

If TTS is used, the TTS Voice should also be entered, as well as the TTS Gender. Again, this must match the configured voice on the Nuance server.

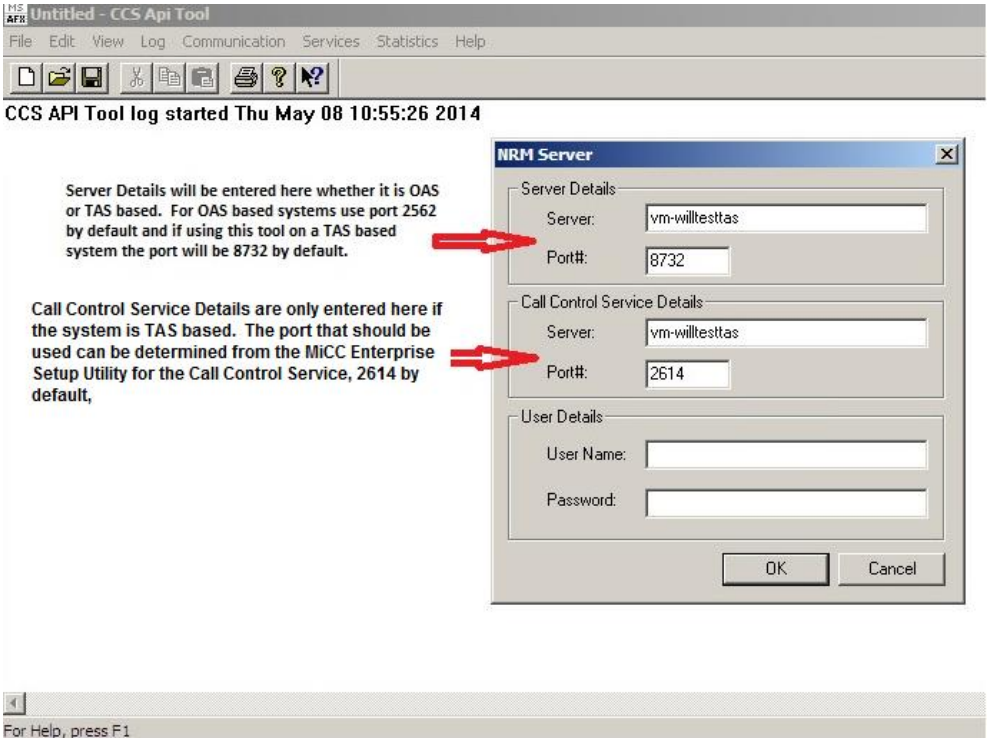
From the Play List drop-down list, select the Play Message List that will be used by this language.

Once the call manager data is defined, including the TAS Site, BVDs, Play Messages and Languages, other MiCC Enterprise data can be configured, including Service Groups, Service Accesses, Agent Groups, and Agents. For details on configuring this data, consult the *Configuration Manager Online Help*.

Note: Since Languages and Play Message Lists are defined on each MiCC Enterprise system, it is not possible to move a script from one MiCC Enterprise system to another without confirming that the selected Language and Play Message identifiers are correct in the Allocate Resources and other media script blocks.

CCS API TOOL

For users of OAS based systems there is a familiar tool called EtpApiTool that can be used to connect to NRM and monitor extensions, BVD's and do many other things with regards to troubleshooting. On a TAS based system there is an analogous tool called CCS Api Tool that connects to the MiCC Enterprise Call Control Service and is used for the same troubleshooting purposes. After MiCC Enterprise is installed this tool will be found in the ..\services\bin subfolder of the MiCC Enterprise directory structure.



SIP TRUNK CONFORMANCE VERIFICATION

Once a MiCC Enterprise/TAS-based system has been installed and configured for a particular call manager, the following set of test cases should be performed to verify system functionality.

For this set of test cases, a TAS Site is defined with one TAS-based MiCC Enterprise system. MiContact Center Agent, the MiCC Agent Service, the MiCC Enterprise Router Service, and the Script Manager AppMediaService communicate with TAS through the CallControlServiceLink.dll, which then sends the request to the MiCC Enterprise Call Control Service.

These test cases are designed to test call manager interaction with a TAS site, as well as call and media control through the TAS interface. The target call manager must have at least one SIP trunk configured towards the MiCC Enterprise/TAS system.

The access numbers for the trunk are used in the configuration of MiCC Enterprise service access' and system requeue device. The access numbers for the SIP trunk applications, as well as the agent device extension numbers, are defined and configured in the TAS Configuration tool on the MiCC Enterprise/TAS system.

TAS SERVICE START/RESTART/MONITORING TEST CASES

The following sections describe the test cases for verifying TAS service start and stop.

Service Access Monitor Start and Stop from MiCC Enterprise

Configure a MiCC Enterprise SA using the SIP trunk access number as the number to monitor. Confirm in the TAS log that a monitor can be started when the SA is activated with a unique monitor cross reference ID generated. Confirm that this unique monitor cross reference ID is used to stop the monitor on the configured SA device when the SA is deactivated.

Service Access Monitor Start and Stop from Call Manager

Disrupt the SIP trunk connection from the call manager to MiCC Enterprise and confirm that the monitor is stopped and that it is restarted when the SIP connection from the call manager is re-established.

Requeue Device Monitor Start and Stop

Configure a requeue device in CM Contact Center properties on the Call tab using the access number of a SIP trunk coming from the target call manager. Confirm in the TAS log that a monitor is started on the device.

Restart Call Control Service

With connected SIP trunks, restart the Call Control service. Verify that the SA's lose the monitors and that upon restart of the Call Control service that the SA monitors are successfully restarted.

CALL CONTROL FUNCTIONALITY TEST CASES

MiCC Agent is using softphone connected to TAS in all the test cases below.

Start MiCC Agent with softphone

Verify MiCC Agent starts up properly, and the extension can be monitored via TAS.

Queued call

Place an incoming call to the SA via the SIP trunk access number and have it queue for a Service Group such that repeat queue messages defined for the group are heard repeatedly.

Incoming call via Router Service Access

Place an incoming call to a Router SA via the SIP trunk access number and have the call routed to MiCC Agent and answer. Verify that the agent enters Talking state and that an audio path is established between the caller and the MiCC Agent.

Incoming call via Script Manager service access

Place an incoming call to a Script Manager SA via the SIP trunk access number and have the call routed to MiCC Agent and answer. Verify that the agent enters Talking state and that an audio path is established between the caller and the MiCC Agent.

Outgoing call

Place an outbound call on the SIP trunk from MiCC Agent and answer at the far end. Verify that the agent enters Talking state and that an audio path is established between the MiCC Agent and the external endpoint.

Hold/Retrieve

Hold and retrieve incoming and outgoing SIP trunk calls call between MiCC Agent and the external endpoint. Verify the state is correct and that the audio path is correct for each state.

Clear call

Clear a call from MiCC Agent in various states: Calling, Talking, Conference. Verify that the call is removed from the SA and is seen as terminated from the perspective of the external call manager.

Consultation call

With an existing call in Talking state, place a new call over the SIP trunk to an endpoint on the external call manager. Verify that the new call can be answered and displays in Talking state, while the original call is in Held state.

Transfer incoming call

From MiCC Agent, transfer an existing incoming SIP trunk call to another MiCC Agent. Note that only transfer after answer is supported. Verify that original MiCC Agent is idle when the transfer is complete and that the audio path is established correctly between the other MiCC Agent and the incoming SIP trunk caller.

Transfer outgoing call

From MiCC Agent, make an outbound call over the SIP trunk to an extension on the call manager that is not monitored by TAS. This will be a call using the default route defined for TAS. Once this outbound call is established and speech path is confirmed, transfer the call to another MiCC Agent (repeat for both announced and blind transfers) and again confirm speech path with the connected parties. Verify that the call is torn down properly regardless of whether the MiCC Agent or the external caller disconnect first.

Conference incoming call

Receive an incoming SIP trunk call (i.e. a service group call) by MiCC Agent and then create a conference between MiCC Agent, the incoming SIP trunk caller and another extension defined on the call manager. Verify speech path and call window state display is correct for all parties.

Clear MiCC Agent from the conference and verify that the MiCC Agent call window shows as Idle and that the audio path is maintained between the two remaining parties. Clear the call between the two remaining parties.

Deflect call

From MiCC Agent, deflect an incoming SIP trunk call to another extension or destination defined on the call manager. Deflect is only supported from the connected state and is disabled when in the ringing state.

Be sure to verify that attempting a deflect to an invalid number will result in an entry in the TAS log about the deflect failing and the call state remaining unchanged. Also check that the call is undisturbed and remains at the MiCC Agent attempting the deflect.

DTMF digits

From MiCC Agent, enter DTMF digits for an existing call. Verify that the digits are sent to the opposite party. Various combinations of play message interruption by digits, inter digit timeout, termination digit, and flush buffer options in the Script Manager Collect Digits block are to be verified.

After-call handling

Configure After-Call handling for a service group, and configure to send the agent ID with the call. Place an incoming SIP trunk call to MiCC Agent and then send the call to the after-call handling destination. Confirm that the call is properly deflected, that correct call window states and displays are seen and that correct audio path is established between the SIP trunk caller and the After Agent Handing destination.

Deflect to Service Group

Deflect an incoming SIP trunk call to another service group. Verify that the call is correctly deflected and routed through the service group.

Reject Service Group call

Reject an incoming service group call, and verify that the call routes to the requeue destination, and it is routed to another agent.

Repeat allowing the call to timeout and be handled by the requeue device.

Associate data

Use a Script Manager Service Access and associated Script Designer script that utilizes an "Associate Data" block and configure the contents of the block to be a maximum length string of 512 digits (this block in Script Designer is limited to 100 characters). Confirm that the data is tagged to the call and displayed on another MiCC Agent when the call is transferred to another agent.

Assist

From a MiCC Agent, request Assist from another agent. Verify that the assisting agent is able to intrude on the call properly and the state display is correct on both agents, during the assist as well as after the assisting agent disconnects and when the incoming caller disconnects.

Single call monitoring

From a MiCC Agent, request to Monitor another MiCC Agent for a single call. Verify that the monitoring agent is able to intrude on the call properly and the state display is correct on both agents.

Continuous call monitoring

From a MiCC Agent, request to Continuously Monitor another MiCC Agent. Verify that the monitoring agent is able to intrude on the first call properly as well as all subsequent calls and the state display is correct on both agents.

Monitored agent consultation call

Monitoring of the agent should be re-established after the consultation call.

Callback handling

Configure a service group to ask for callbacks, and add a call to the queue that is changed to a callback. Verify that the agent is prompted to make the callback, and the callback can be initiated correctly from MiCC Agent.

Web callback handling

Add web callbacks to the system. Verify that the agent is prompted to make the web callback, and the callback can be initiated correctly from MiCC Agent.

Campaign call handling

Verify that campaign calls (regular and progressive) can be handled by MiCC Agent agents.

Dispatch call handling

Verify that an incoming call can be directed to a dispatch SG and that the call can be retrieved from the dispatch window.

Common hold call handling

Verify that a call can be placed on common hold and can then be retrieved.

MiCC Agent call recording

Verify that the “Record Calls” feature in MiCC Agent can be initiated and calls that were recorded can be played back successfully.

Music on Hold and Ringing

Verify that when calling a Service Access that the MOH file specified in the Media Server configuration utility is played (the default file is ringing.wav) while a call is in queue.

Verify that the MOH file play is stopped when the call is answered by an agent.

Verify that the MOH play is interrupted by play message prompts and that it resumes after the prompt is heard (for example, repeat queue messages).

Verify that if a repeat queue message is being played and an agent becomes available that the call will wait until the prompt completes and then route the call to the agent.

CISCO INTEGRATION WITH TAS / MICC ENTERPRISE

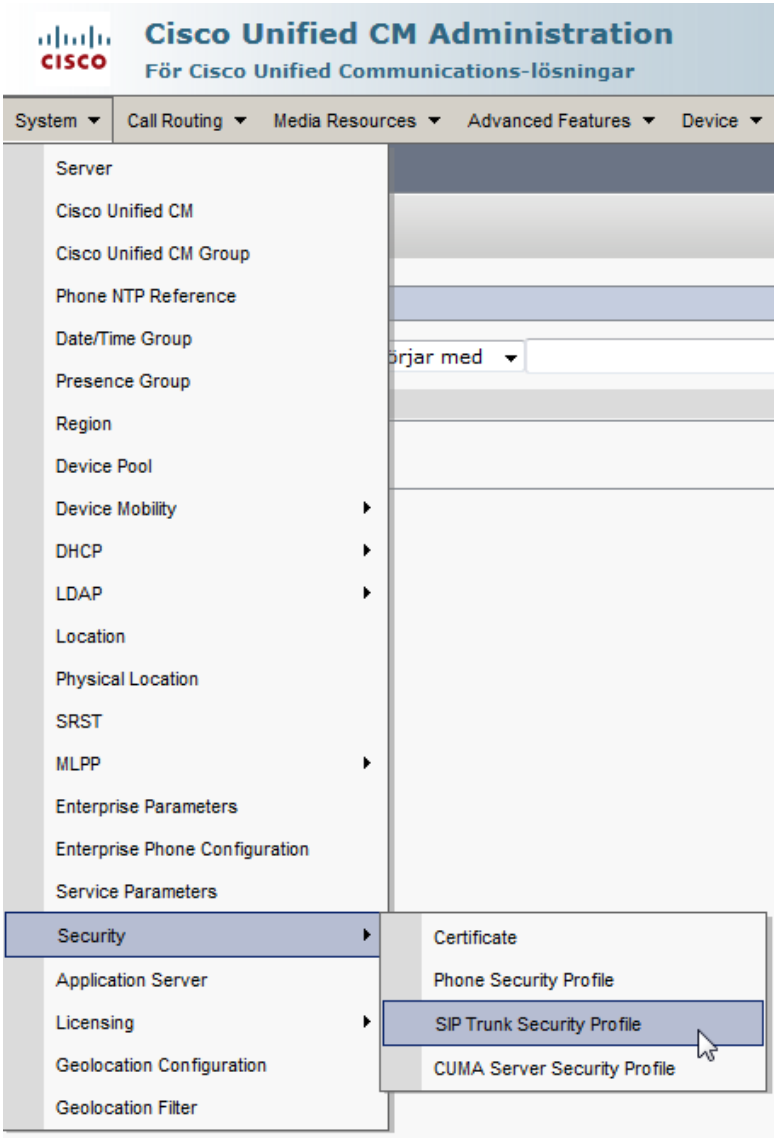
This section highlights the required configuration on the Cisco Unified Communications Manager for TAS / MiCC Enterprise integration. For detailed configuration instructions, please refer to the Cisco product documentation.

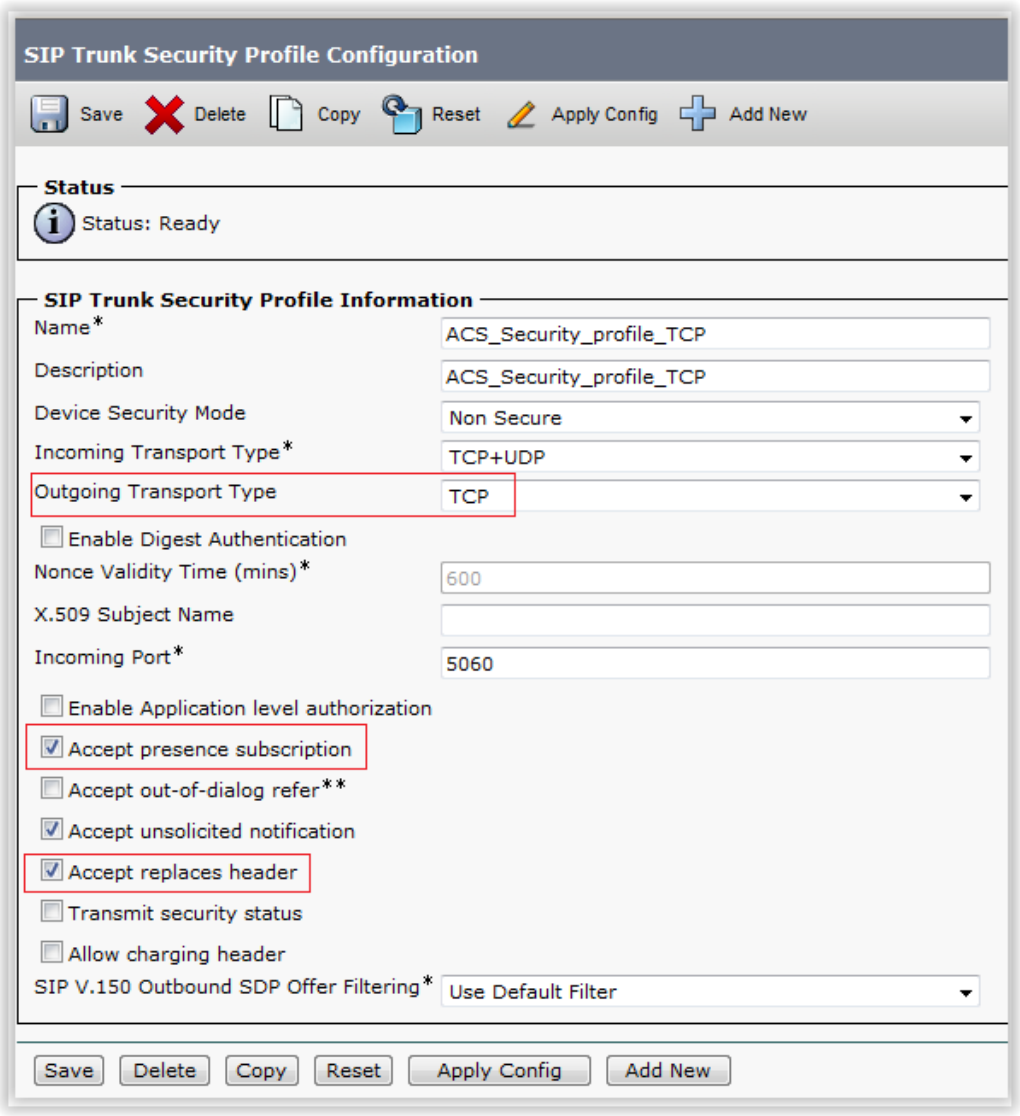
SIP TRUNK CHARACTERISTICS FOR CISCO UCM

The following configuration is required for CUCM:

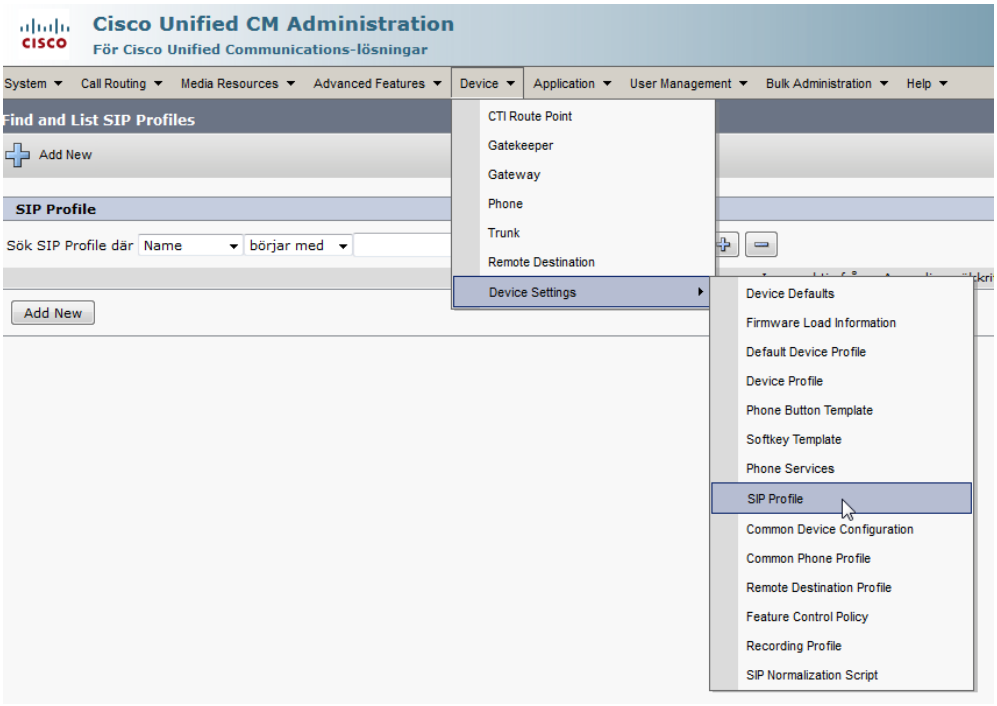
- Under SIP Trunk Security profile:
  - Check Accept Presence Subscription
  - Check Accept Replaces Header
- Under SIP Profile:
  - Check Redirect by Application
  - Reroute incoming request to new trunk based on **Contact Info Header**
- Under SIP Trunk:
  - Check Redirecting Diversion Header Delivery – Inbound
  - Check Redirecting Diversion Header Delivery – Outbound
  - Check Remote-Party-Id
  - Make sure SUBSCRIBE Calling Search Space and Rerouting Calling Search Space fit your number plan
  - Make sure Inbound **Calling Search Space** on the SIP trunk fits your number plan

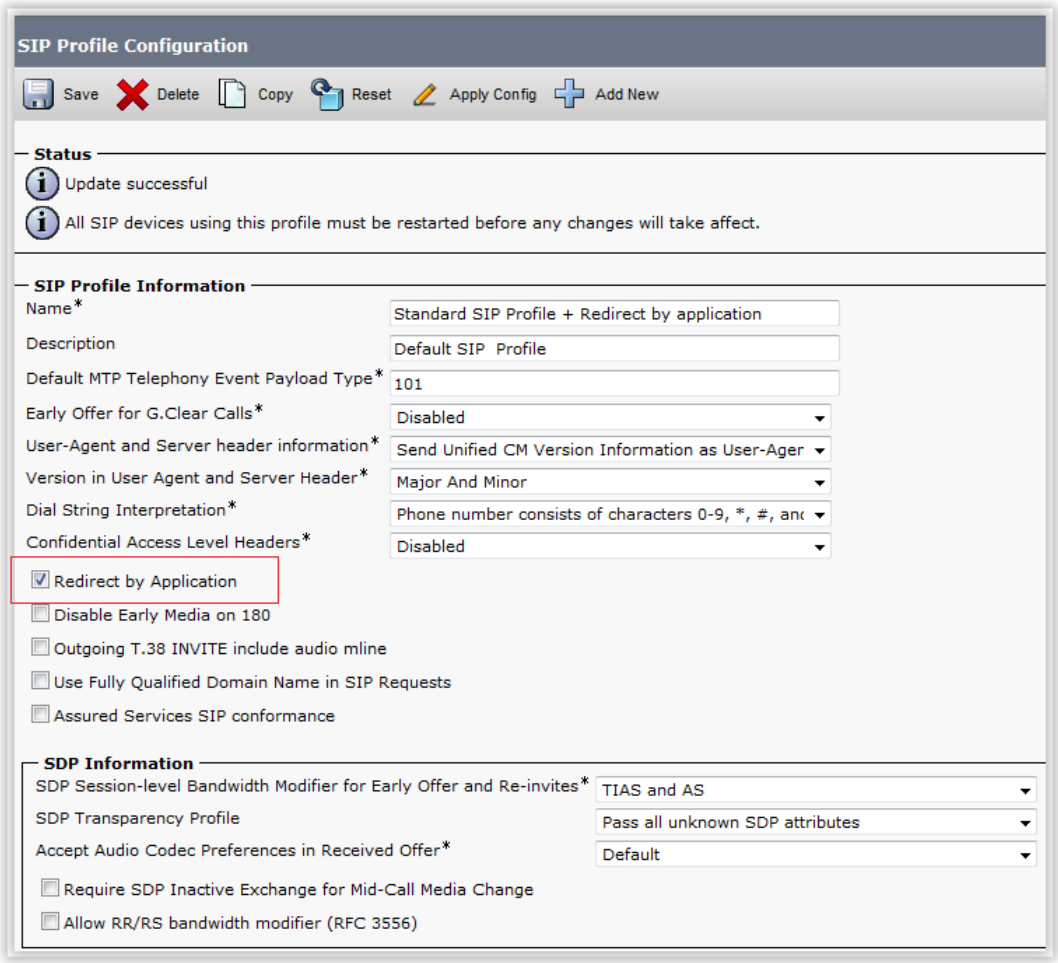
SIP trunk security profile

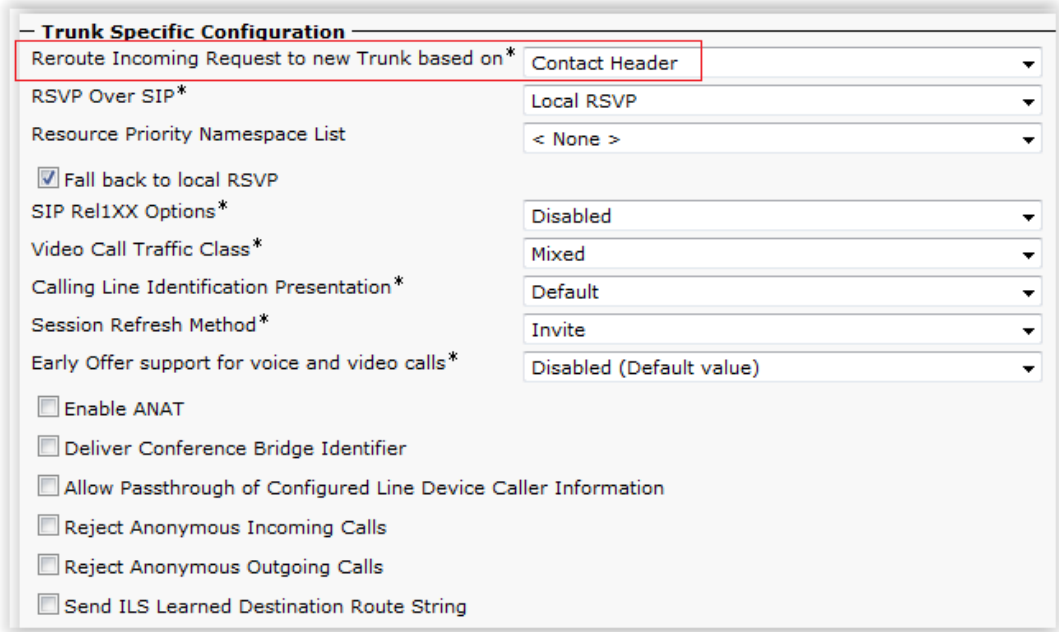



SIP Trunk Security Profile Configuration
Save
Delete
Copy
Reset
Apply Config
Add New
Status
Status: Ready
SIP Trunk Security Profile Information
Name*
ACS_Security_profile_TCP
Description
ACS_Security_profile_TCP
Device Security Mode
Non Secure
Incoming Transport Type*
TCP+UDP
Outgoing Transport Type
TCP
Enable Digest Authentication
Nonce Validity Time (mins)*
600
X.509 Subject Name
Incoming Port*
5060
Enable Application level authorization
Accept presence subscription
Accept out-of-dialog refer**
Accept unsolicited notification
Accept replaces header
Transmit security status
Allow charging header
SIP V.150 Outbound SDP Offer Filtering*
Use Default Filter
Save
Delete
Copy
Reset
Apply Config
Add New

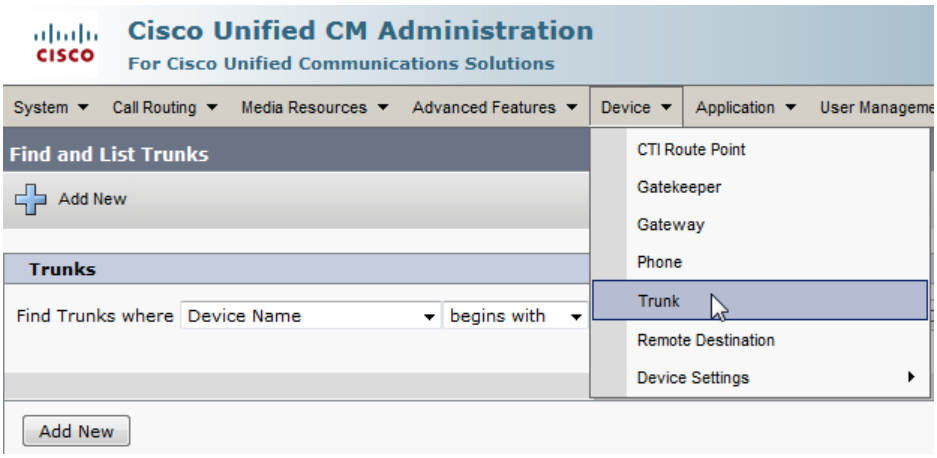
SIP profile

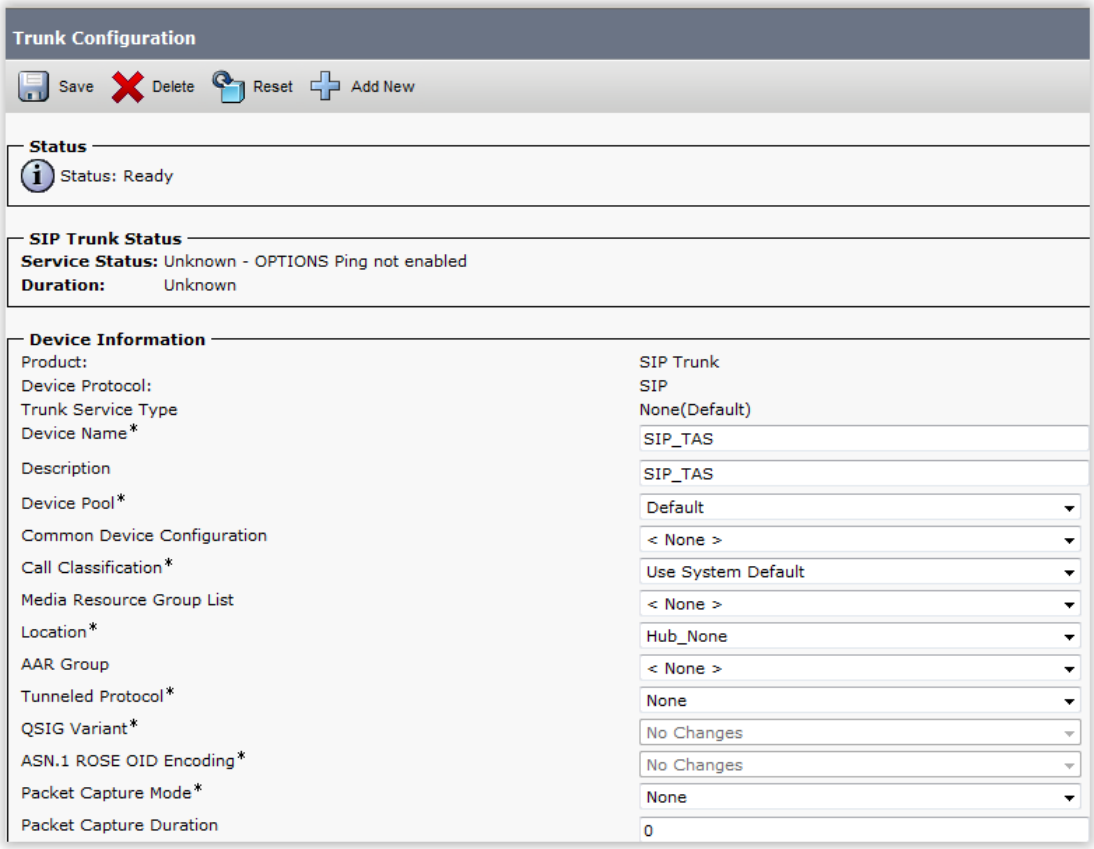

Cisco Unified CM Administration
För Cisco Unified Communications-lösningar
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help
Find and List SIP Profiles
Add New
SIP Profile
Sök SIP Profile där
Name
börjar med
Add New
CTI Route Point
Gatekeeper
Gateway
Phone
Trunk
Remote Destination
Device Settings
Device Defaults
Firmware Load Information
Default Device Profile
Device Profile
Phone Button Template
Softkey Template
Phone Services
SIP Profile
Common Device Configuration
Common Phone Profile
Remote Destination Profile
Feature Control Policy
Recording Profile
SIP Normalization Script

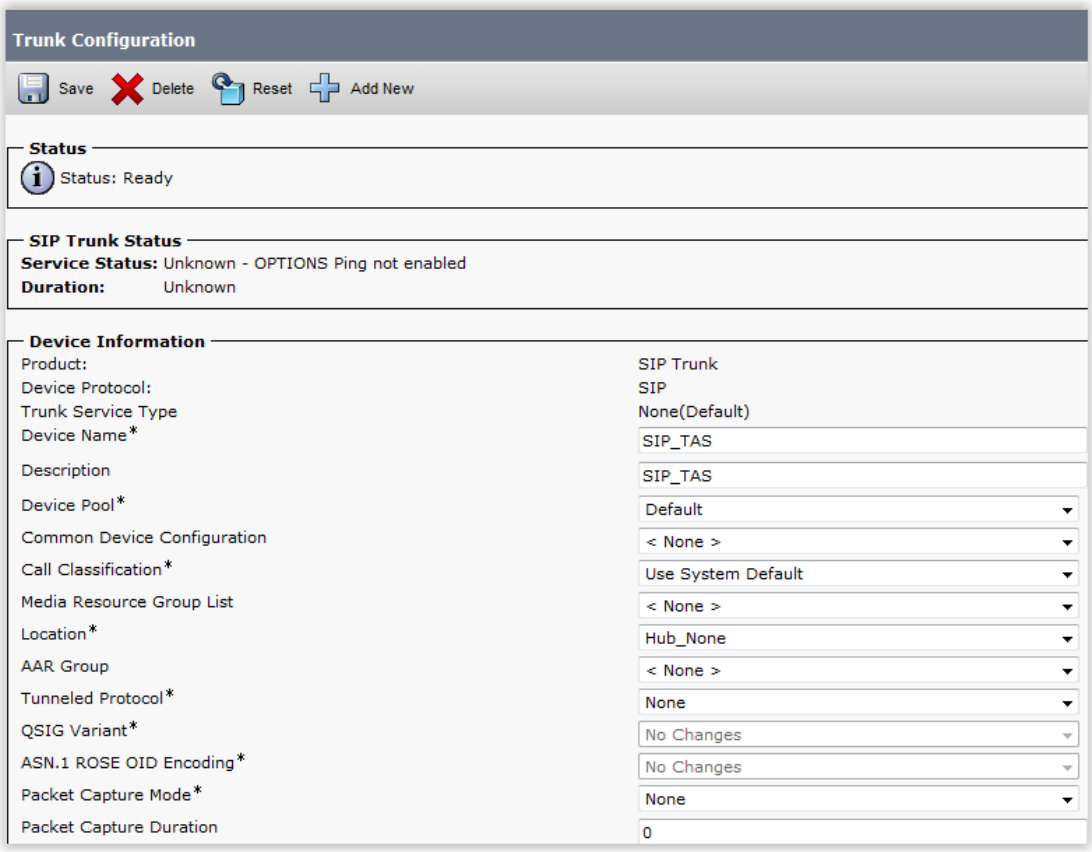

SIP Profile Configuration
Save
Delete
Copy
Reset
Apply Config
Add New
Status
Update successful
All SIP devices using this profile must be restarted before any changes will take affect.
SIP Profile Information
Name*
Standard SIP Profile + Redirect by application
Description
Default SIP Profile
Default MTP Telephony Event Payload Type*
101
Early Offer for G.Clear Calls*
Disabled
User-Agent and Server header information*
Send Unified CM Version Information as User-Ager
Version in User Agent and Server Header*
Major And Minor
Dial String Interpretation*
Phone number consists of characters 0-9, *, #, and
Confidential Access Level Headers*
Disabled
Redirect by Application
Disable Early Media on 180
Outgoing T.38 INVITE include audio mline
Use Fully Qualified Domain Name in SIP Requests
Assured Services SIP conformance
SDP Information
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*
TIAS and AS
SDP Transparency Profile
Pass all unknown SDP attributes
Accept Audio Codec Preferences in Received Offer*
Default
Require SDP Inactive Exchange for Mid-Call Media Change
Allow RR/RS bandwidth modifier (RFC 3556)

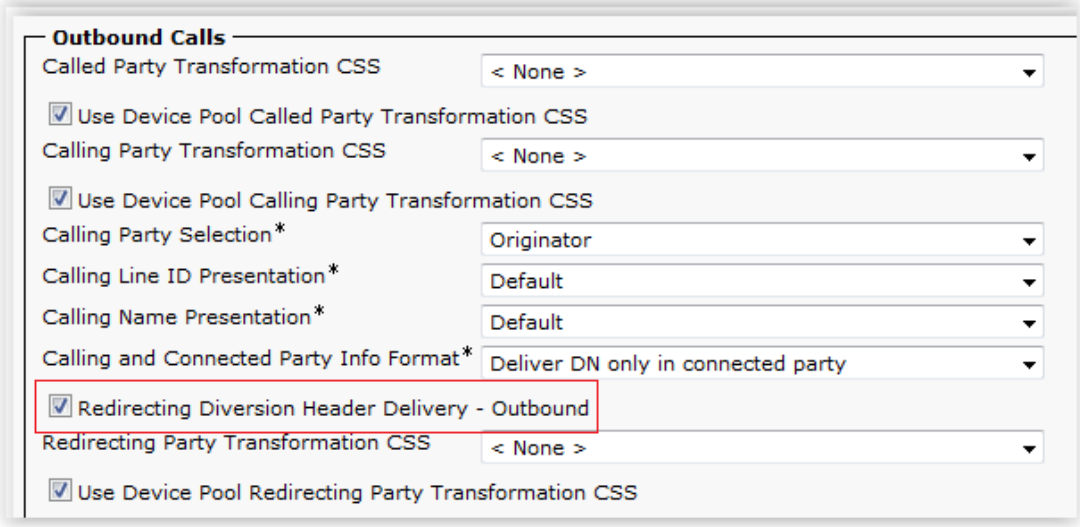

Trunk Specific Configuration
Reroute Incoming Request to new Trunk based on*
Contact Header
RSVP Over SIP*
Local RSVP
Resource Priority Namespace List
< None >
Fall back to local RSVP
SIP Rel1XX Options*
Disabled
Video Call Traffic Class*
Mixed
Calling Line Identification Presentation*
Default
Session Refresh Method*
Invite
Early Offer support for voice and video calls*
Disabled (Default value)
Enable ANAT
Deliver Conference Bridge Identifier
Allow Passthrough of Configured Line Device Caller Information
Reject Anonymous Incoming Calls
Reject Anonymous Outgoing Calls
Send ILS Learned Destination Route String

SIP trunk configuration



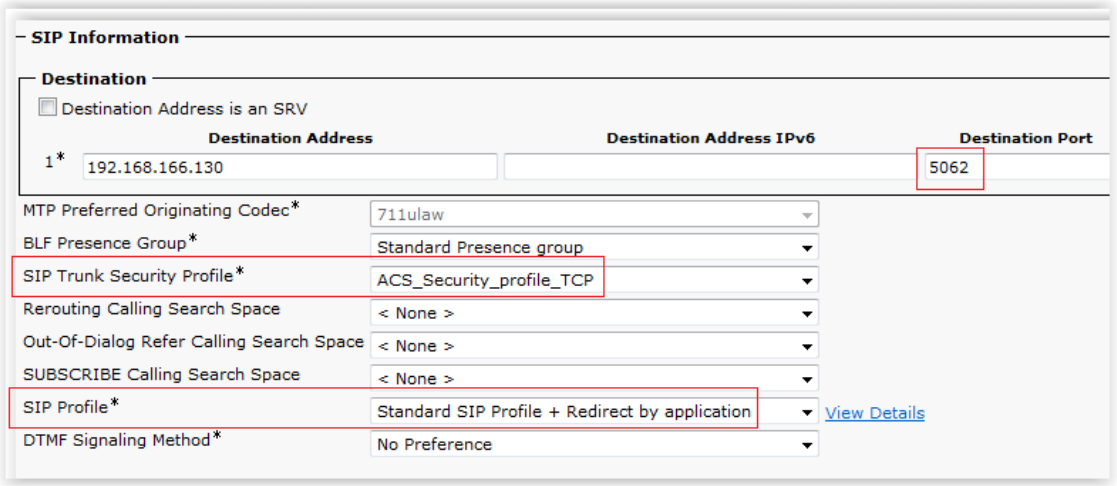



Trunk Configuration
Save
Delete
Reset
Add New
Status
Status: Ready
SIP Trunk Status
Service Status: Unknown - OPTIONS Ping not enabled
Duration: Unknown
Device Information
Product: SIP Trunk
Device Protocol: SIP
Trunk Service Type: None(Default)
Device Name* SIP_TAS
Description SIP_TAS
Device Pool* Default
Common Device Configuration < None >
Call Classification* Use System Default
Media Resource Group List < None >
Location* Hub_None
AAR Group < None >
Tunneled Protocol* None
QSIG Variant* No Changes
ASN.1 ROSE OID Encoding* No Changes
Packet Capture Mode* None
Packet Capture Duration 0


Outbound Calls
Called Party Transformation CSS < None >
Use Device Pool Called Party Transformation CSS
Calling Party Transformation CSS < None >
Use Device Pool Calling Party Transformation CSS
Calling Party Selection* Originator
Calling Line ID Presentation* Default
Calling Name Presentation* Default
Calling and Connected Party Info Format* Deliver DN only in connected party
Redirecting Diversion Header Delivery - Outbound
Redirecting Party Transformation CSS < None >
Use Device Pool Redirecting Party Transformation CSS


Call Routing Information
Remote-Party-Id
Asserted-Identity
Asserted-Type* Default
SIP Privacy* Default

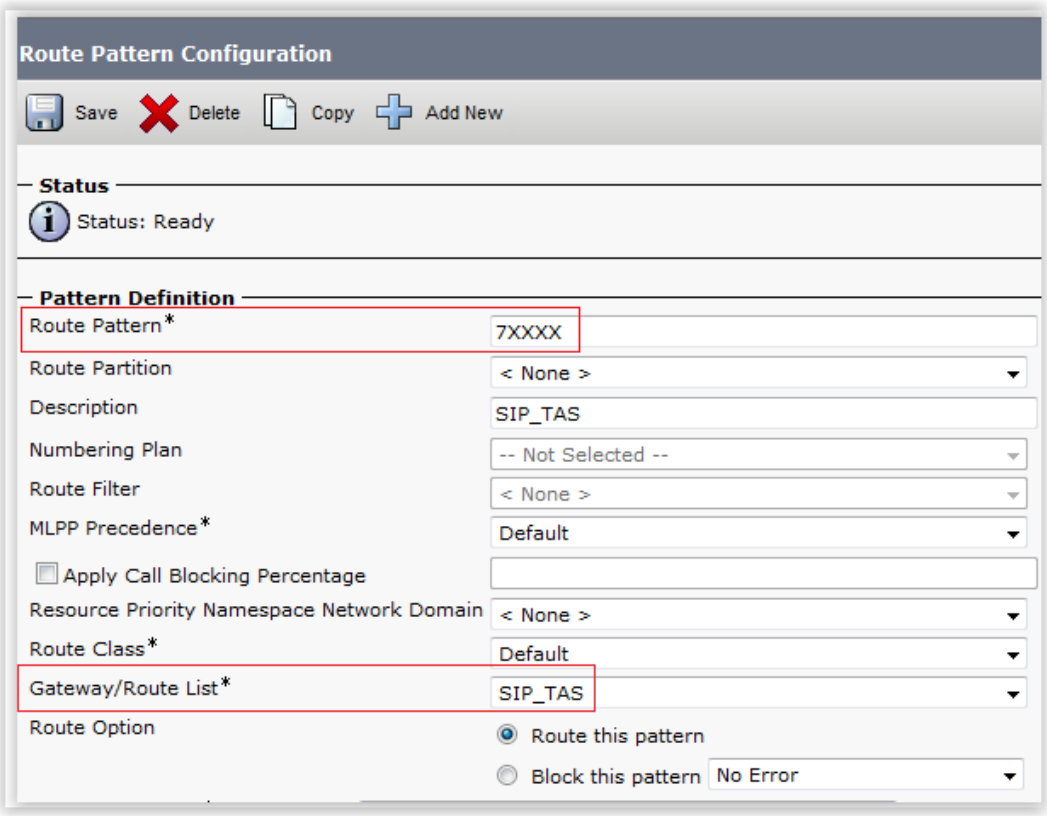
Note: You must match the destination port configured as seen below with the TAS SIP Listening Port configured on the TAS/MiCC Enterprise system. This configuration on the TAS/MiCC Enterprise system is done with the TAS Configuration Tool.



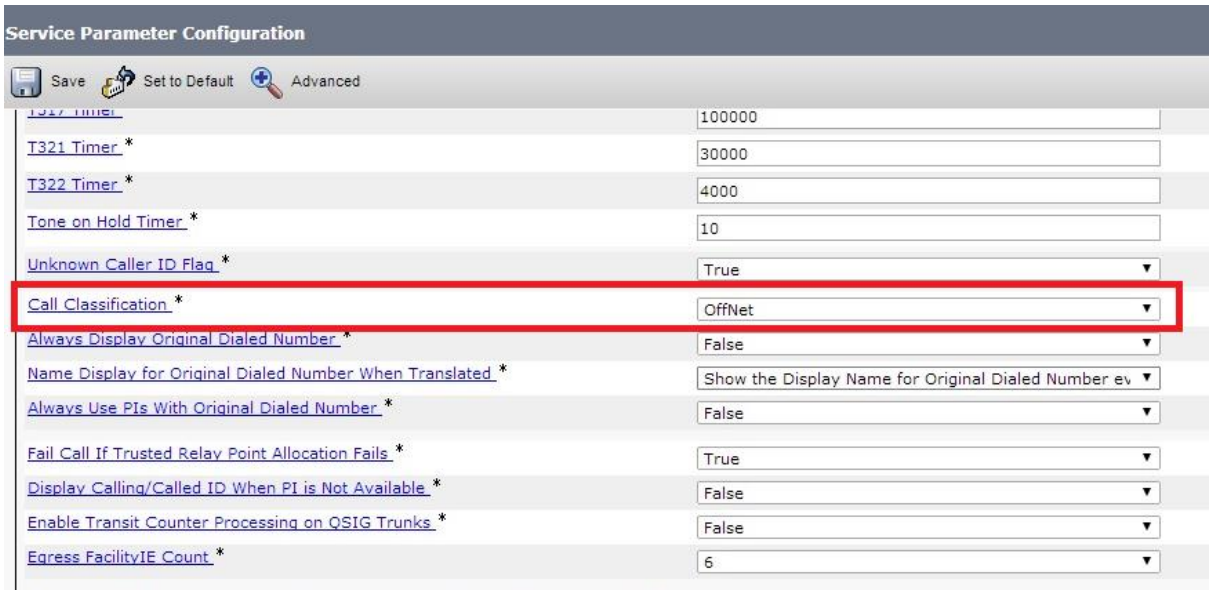
Note: The SUBSCRIBE setting for the trunk configured for call handling should match the SUBSCRIBE setting for the trunk configured for Line State.

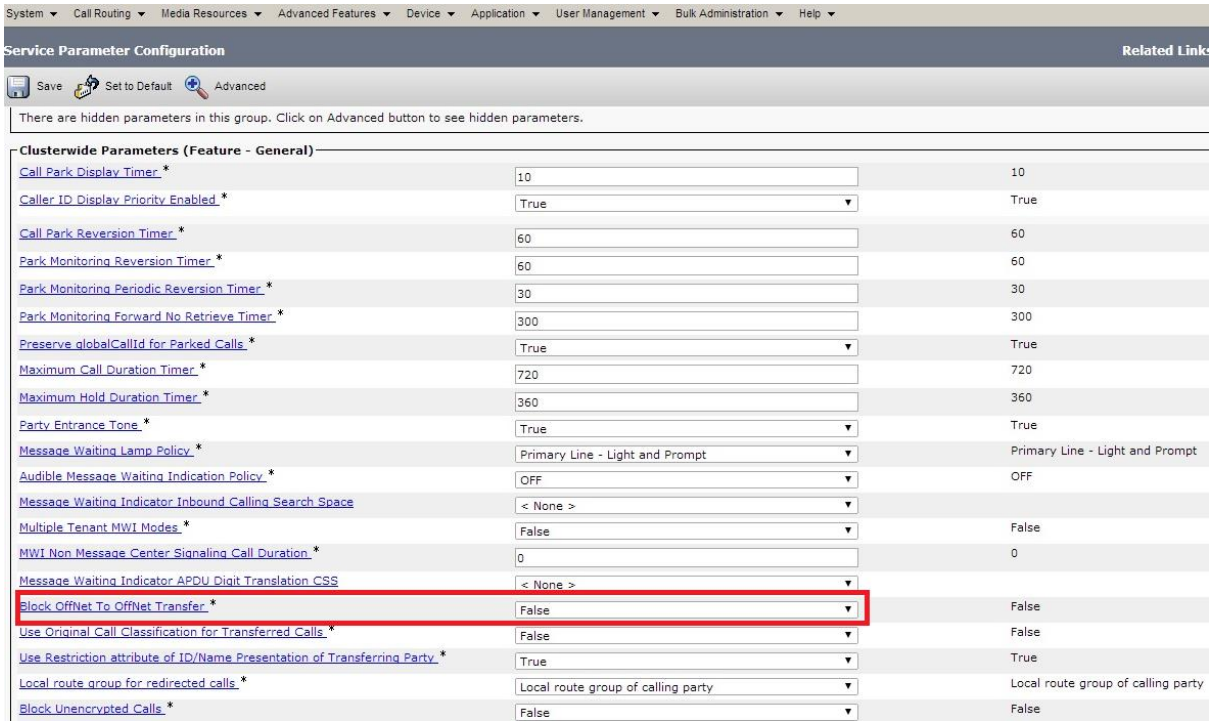
ROUTE NUMBERS TO THE SIP TRUNK

Be sure to set the Route Pattern as shown below to correspond to the BVDs configured in the MiCC Enterprise system.



CONFIGURATION FOR OFFNET TO OFFNET TRANSFERS





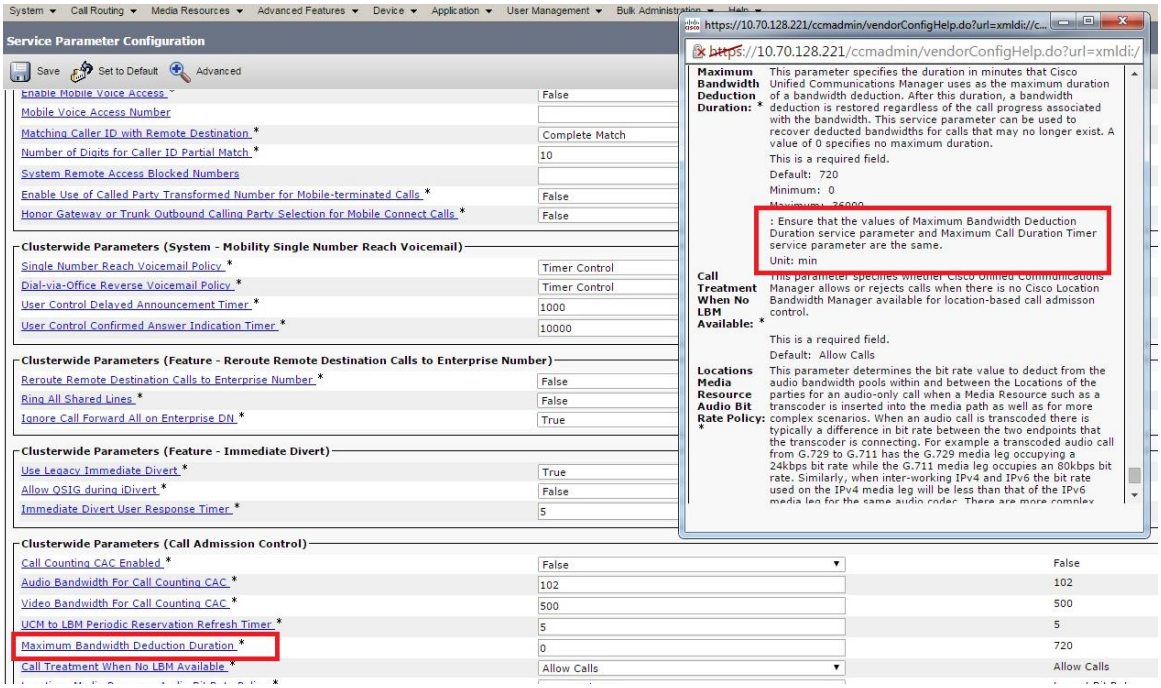
Cisco help about OffNet to OffNet Transfers

"The Cisco Unified Communications Manager clusterwide service parameter Block OffNet to OffNet Transfer allows administrators to prevent users from transferring external calls to another external number. This parameter specifies values as True or False. Setting the parameter to True blocks external calls from being transferred to another external device. The default value specifies False. You modify the Block OffNet to OffNet Transfer service parameter by using the Service Parameters Configuration window"

The recommendation is to set this parameter to the suggested value of False.

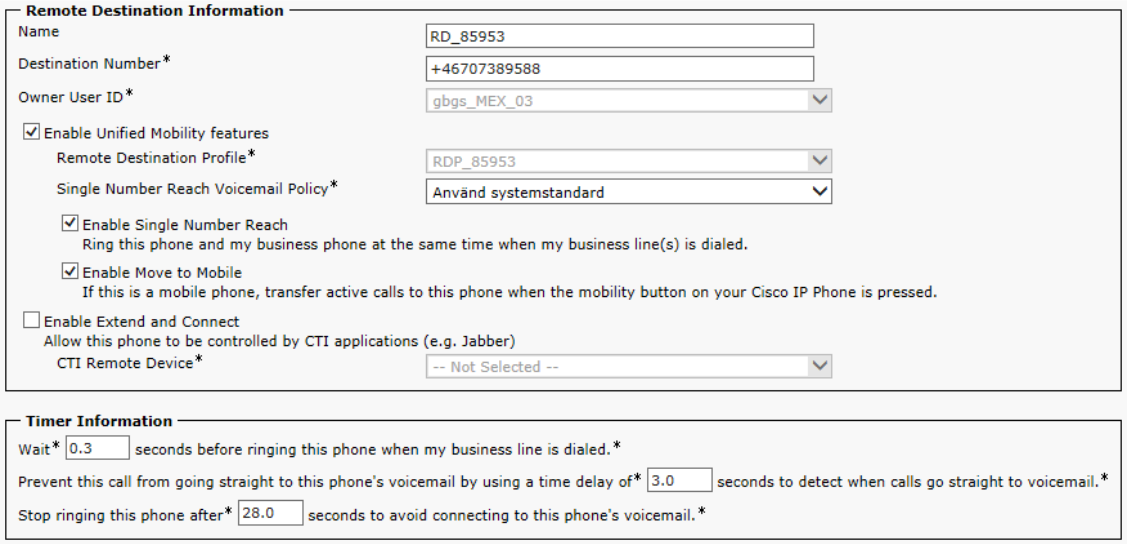
MAXIMUM BANDWIDTH DEDUCTION DURATION SERVICE PARAMETER

When setting the Maximum Call Duration Timer there is another setting that needs to be changed and that is the Maximum Bandwidth Deduction Duration service parameter. This should also be set to 0.


System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help
Service Parameter Configuration
Save
Set to Default
Advanced
Enable Mobile Voice Access
False
Mobile Voice Access Number
Matching Caller ID with Remote Destination *
Complete Match
Number of Digits for Caller ID Partial Match *
10
System Remote Access Blocked Numbers
Enable Use of Called Party Transformed Number for Mobile-terminated Calls *
False
Honor Gateway or Trunk Outbound Calling Party Selection for Mobile Connect Calls *
False
Clusterwide Parameters (System - Mobility Single Number Reach Voicemail)
Single Number Reach Voicemail Policy *
Timer Control
Dial-via-Office Reverse Voicemail Policy *
Timer Control
User Control Delayed Announcement Timer *
1000
User Control Confirmed Answer Indication Timer *
10000
Clusterwide Parameters (Feature - Reroute Remote Destination Calls to Enterprise Number)
Reroute Remote Destination Calls to Enterprise Number *
False
Ring All Shared Lines *
False
Ignore Call Forward All on Enterprise DN *
True
Clusterwide Parameters (Feature - Immediate Divert)
Use Legacy Immediate Divert *
True
Allow QSIG during iDivert *
False
Immediate Divert User Response Timer *
5
Clusterwide Parameters (Call Admission Control)
Call Counting CAC Enabled *
False
False
Audio Bandwidth For Call Counting CAC *
102
102
Video Bandwidth For Call Counting CAC *
500
500
UCM to LBM Periodic Reservation Refresh Timer *
5
5
Maximum Bandwidth Deduction Duration *
0
720
Call Treatment When No LBM Available *
Allow Calls
Allow Calls
https://10.70.128.221/ccmadmin/vendorConfigHelp.do?url=xmldi://c...
https://10.70.128.221/ccmadmin/vendorConfigHelp.do?url=xmldi:/
Maximum Bandwidth Deduction Duration: *
This parameter specifies the duration in minutes that Cisco Unified Communications Manager uses as the maximum duration of a bandwidth deduction. After this duration, a bandwidth deduction is restored regardless of the call progress associated with the bandwidth. This service parameter can be used to recover deducted bandwidths for calls that may no longer exist. A value of 0 specifies no maximum duration.
This is a required field.
Default: 720
Minimum: 0
: Ensure that the values of Maximum Bandwidth Deduction Duration service parameter and Maximum Call Duration Timer service parameter are the same.
Unit: min
Call Treatment When No LBM Available: *
Manager allows or rejects calls when there is no Cisco Location Bandwidth Manager available for location-based call admisson control.
This is a required field.
Default: Allow Calls
Locations Media Resource Audio Bit Rate Policy: *
This parameter determines the bit rate value to deduct from the audio bandwidth pools within and between the Locations of the parties for an audio-only call when a Media Resource such as a transcoder is inserted into the media path as well as for more complex scenarios. When an audio call is transcoded there is typically a difference in bit rate between the two endpoints that the transcoder is connecting. For example a transcoded audio call from G.729 to G.711 has the G.729 media leg occupying a 24kbps bit rate while the G.711 media leg occupies an 80kbps bit rate. Similarly, when inter-working IPv4 and IPv6 the bit rate used on the IPv4 media leg will be less than that of the IPv6

TIMER CONFIGURATION FOR REMOTE EXTENSIONS

If the Timer Information value is set to the Cisco Default of 0.0 then MiCC Enterprise doesn't get 180 ringing until Call Proceeded is received from the PSTN. By changing the delay to 0.1, ringing is received more or less directly after the Invite to PSTN.



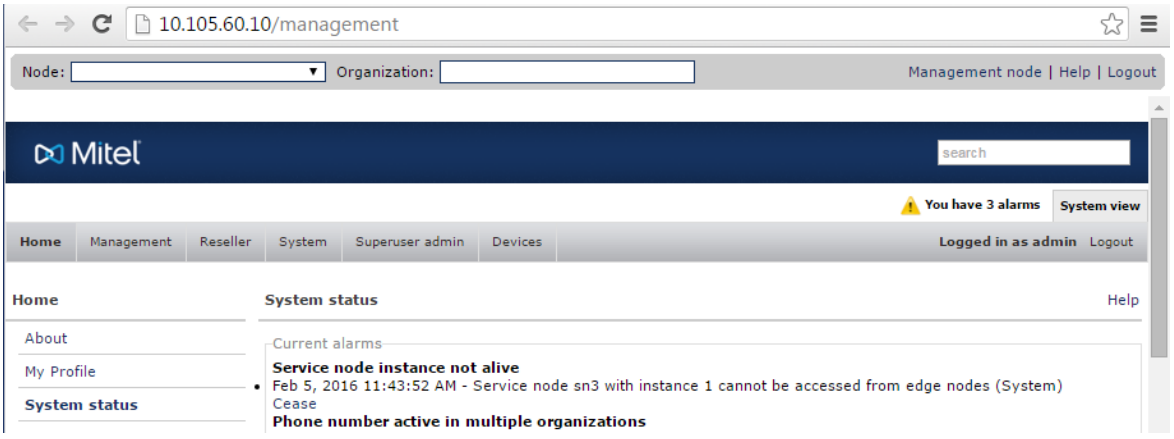
TAS Configuration Tool

For CISCO call managers, the **Media Server Always in Call** option must be enabled in the TAS Configuration Tool.

TELEPO INTEGRATION WITH TAS / MICC ENTERPRISE

This section describes the required configuration on the Telepo call manager for TAS / MiCC Enterprise integration. For detailed configuration instructions, please refer to the Telepo call manager product documentation.

You configure the Telepo call manager via the web portal hosted on the node (i.e., by typing the server address into a web browser).



SIP TRUNK CONFIGURATION

You can configure one or more SIP trunks between the MiCC Enterprise system and the Telepo call manager. When you configure a SIP trunk you:

- create a SIP trunk
- create a destination call tag
- create a trunk group for the SIP trunk(s)
- configure trunk group rewrites.

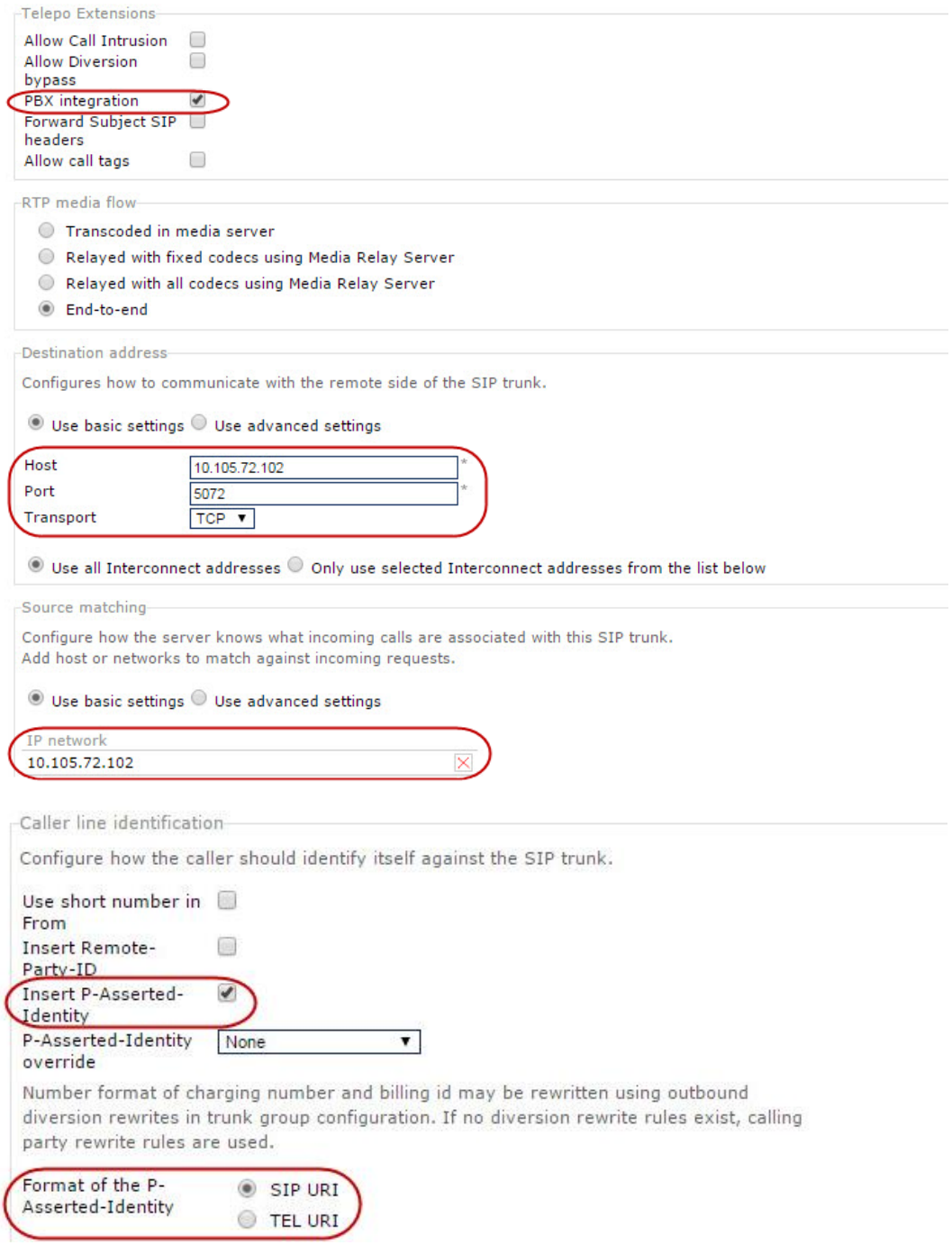
Create a SIP trunk

You can configure one or more SIP trunks between the Telepo call manager and the MiCC Enterprise system. You create the SIP trunk on the Telepo management node.

As system administrator on the management node, do the following:

1. Click on the **Devices** menu and select the **SIP trunks** option.
2. On the **SIP trunks** page, click **New SIP trunk**.
3. On the **SIP trunk configuration** page, create a new SIP trunk with the following characteristics:
    - Under Telepo Extensions, enable the PBX integration option.

- Under **Destination address**, specify the TAS IP address and port.
- Under **Source matching**, add the MiCC Enterprise system address for the IP network.
- Under Caller line identification, enable the Insert P-Asserted-Identity option and set the Format of the P–Asserted Identity to SIP URI.



4. Click **Save** to apply your changes.

Create a destination call tag

You must create a destination call tag to enable the Telepo call manager to route calls to the MiCC Enterprise SIP trunk.

As system administrator on the management node, do the following:

1. Click on the **System** menu and select the **Call tags** option.
2. On the **Call tags** page, specify the name of the MiCC Enterprise SIP trunk you created, select the type from the drop-down menu, and click **Add**.

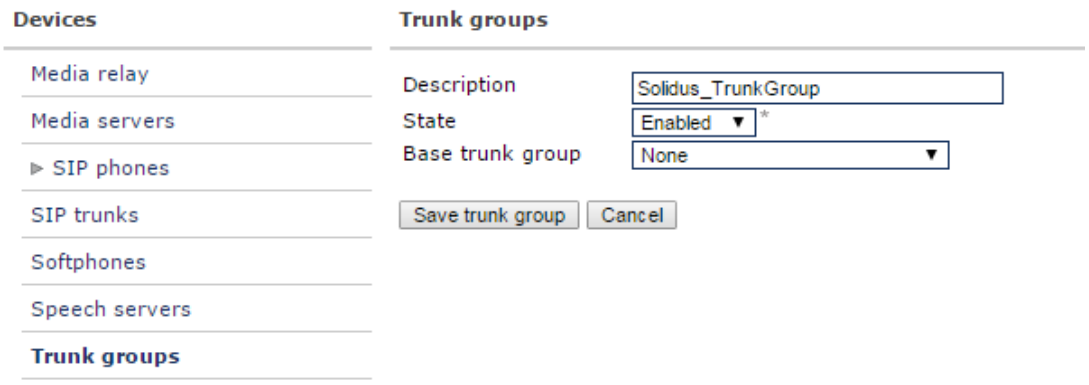
3. Click **Apply** to save your changes.

Create a trunk group

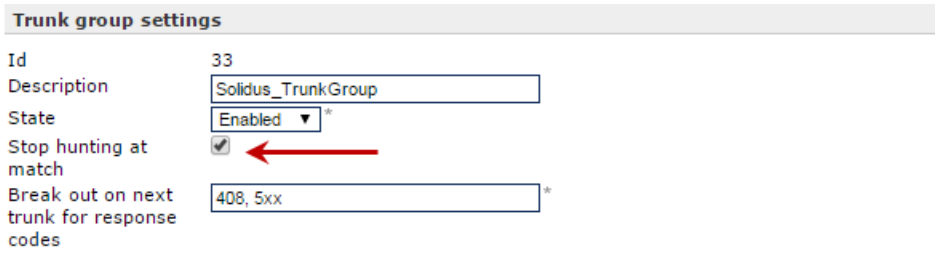
You must create a trunk group for the MiCC Enterprise SIP trunk.

As system administrator on the management node, do the following:

1. Click on the **Devices** menu and select the **Trunk groups** option.
2. On the **Trunk groups** page, click New trunk group.
3. On the new trunk group page, do the following:
   a. Specify a name for the trunk group.
   b. Select a state for the trunk group from the pull-down menu (enabled or disabled)/
   c. Optionally, select another trunk group to use as a base for configuration.
   d. Click **Save trunk group** to apply your changes.



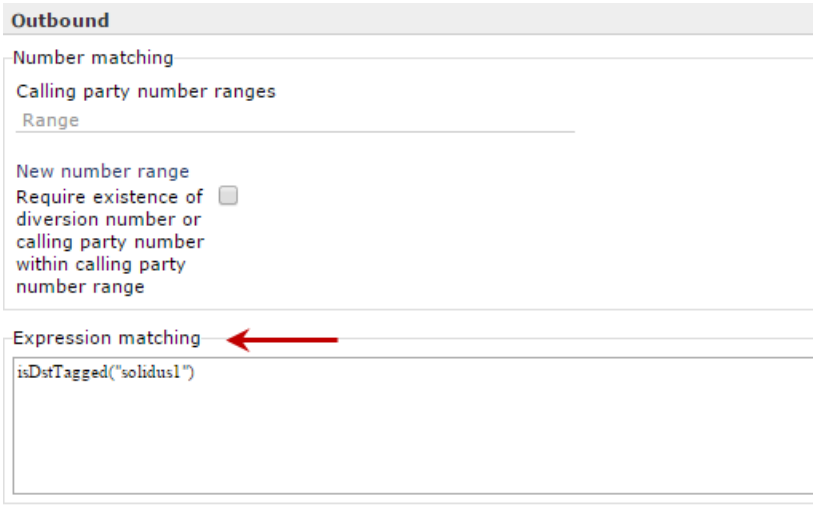
4. On the **Trunk groups** page, select the new trunk group from the list to edit the settings.
5. On the page for your new trunk group, specify the following parameters:
   a. Under Trunk group settings, enable the Stop hunting at match parameter.



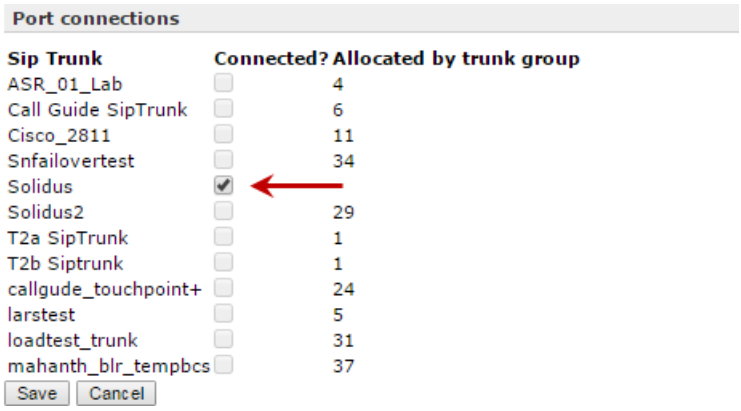
b. Under Outbound, add the following entry to the **Expression matching** field:

```
isDstTagged ("<call-tag>”)
```

where <call-tag> is the destination call tag you created for the MiCC Enterprise SIP trunk.



c. Under **Port connections**, select the SIP trunk you created for the MiCC Enterprise system.



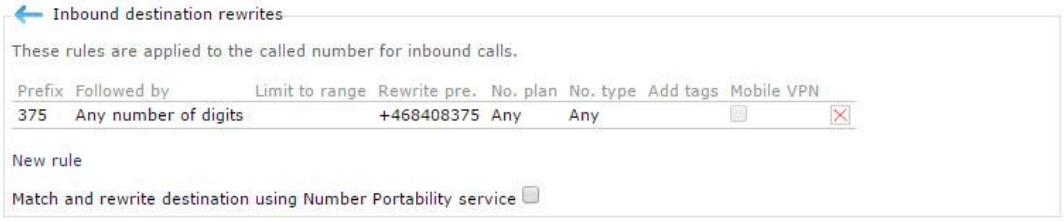
6. Click **Save** to apply your changes.

Configure trunk group rewrites

TAS supports E.164 numbers; however, if it is preferred to use shorter numbers in the system configuration, the Trunk Group Rewrites function can be used. Only the system administrator can configure this feature.

As system administrator on the management mode, do the following:

1. Click on the **Devices** menu and select the **Trunk groups** option.
2. On the **Trunk groups** page, select the SIP trunk group you created for MiCC Enterprise.
3. On the **Trunk group** page, do the following:
   - Under **Inbound**, use the **Inbound destination rewrites** function to expand the numbers from TAS to the agent hard phone (i.e., to allow for the use of short numbers for agents on hard phones). If the whole agent number is +468561000, you can configure a rule that expands the prefix “61” to “+468561”. You can then use a number like 61000 in the agent extension.


Inbound destination rewrites

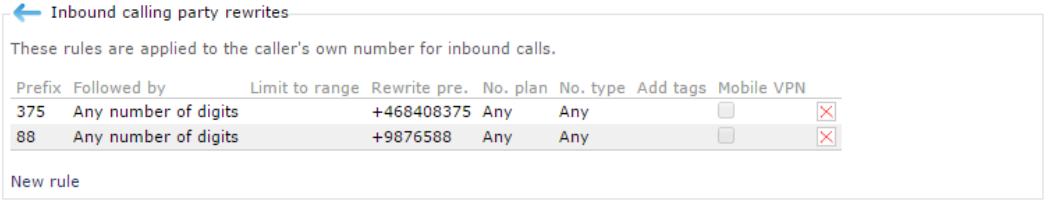
These rules are applied to the called number for inbound calls.

Prefix	Followed by	Limit to range	Rewrite pre.	No. plan	No. type	Add tags	Mobile VPN	
375	Any number of digits		+468408375	Any	Any			

New rule

Match and rewrite destination using Number Portability service

   - Under **Inbound**, use the **Inbound calling party rewrites** function to enable the Telepo call manager to identify the source of the call (otherwise all calls appear to come from "anonymous"). For example, to identify an incoming call from 61000, add a rule that expands the prefix “61” to “+468561”.

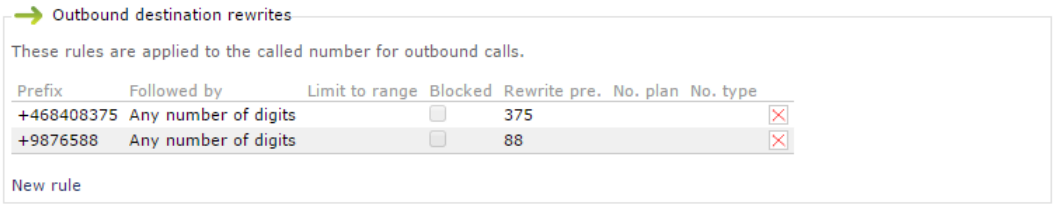

Inbound calling party rewrites

These rules are applied to the caller's own number for inbound calls.

Prefix	Followed by	Limit to range	Rewrite pre.	No. plan	No. type	Add tags	Mobile VPN	
375	Any number of digits		+468408375	Any	Any			
88	Any number of digits		+9876588	Any	Any			

New rule

   - Under **Outbound**, use the **Outbound destination rewrites** function to shorten the number towards the TAS. If the whole BVD number is +468552000, you can configure the rule to rewrite the prefix “+468552” to “52”. You can then configure TAS to use 52000 as the start of the BVD range.


Outbound destination rewrites

These rules are applied to the called number for outbound calls.

Prefix	Followed by	Limit to range	Blocked	Rewrite pre.	No. plan	No. type	
+468408375	Any number of digits			375			
+9876588	Any number of digits			88			

New rule

4. Click **Save** to apply your changes.

USER AND EXTENSION CONFIGURATION

In addition to configuring a SIP trunk for Telepo and MiCC Enterprise integration, you must configure MiCC Enterprise extensions on the Telepo call manager, and an organization to contain them.

To configure MiCC Enterprise users and extensions you:

- create an organization
- create a number range for the organization
- create users and assign them to the organization
- provision 68XXX SIP phones
- create an external system number for the Basic Virtual Device (BVD)

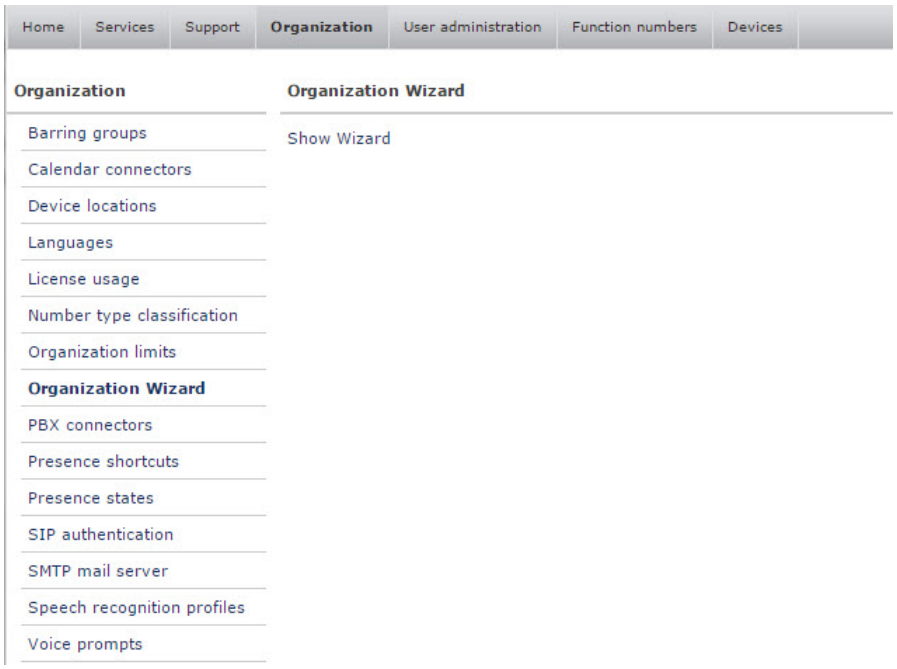
Create an organization

An Organization represents a customer or tenant. Both the Telepo call manager and MiCC Enterprise support multiple tenants. The Organization is used to isolate the customer-specific configuration (e.g., the Welcome message for each organization is different, a user in one organization can only search for numbers in the local organization).

You must create an organization that includes the MiCC Enterprise extensions.

As System Administrator on the service node, do the following:

1. Click on the **Organizations** menu and select the **Organization Wizard** option.
2. On the **Organization Wizard** page, click **Show Wizard**.



The Organization Wizard launches to guide you through the creation of a new organization component.

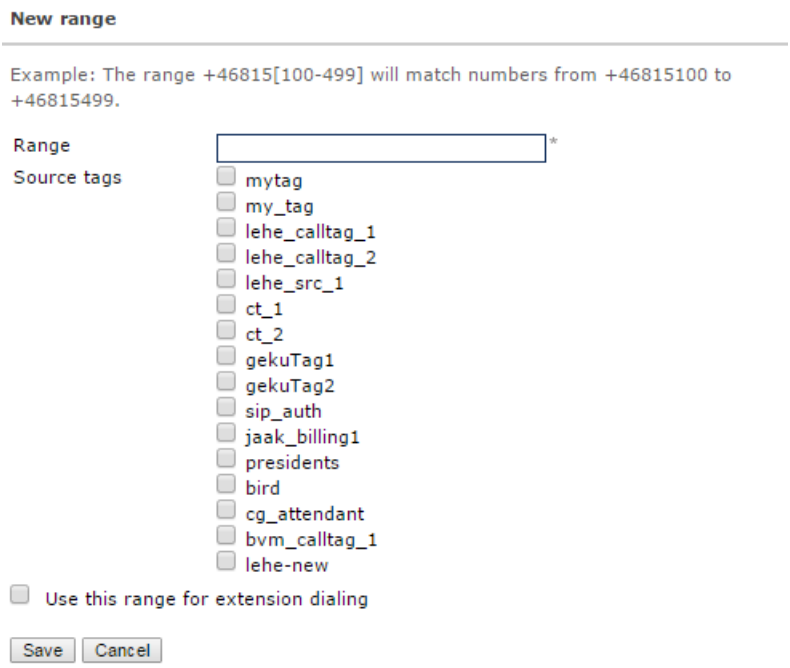
3. Follow the instructions in the Organization Wizard to create your organization.

Create a number range

When you have created your organization, you can configure a number range for the MiCC Enterprise extensions.

As System Administrator on the management node, do the following:

1. Enter the name of your new organization in the Search box.
2. On the home page, click on the **Organization** menu and select the **Number ranges** option.
3. On the **Number ranges** page, click **New range**.
4. On the **New range** page, create a number range for the MiCC Enterprise extensions.



5. Repeat step 4 to create a number range for the desk phones.
6. Click **Save** to apply your changes.

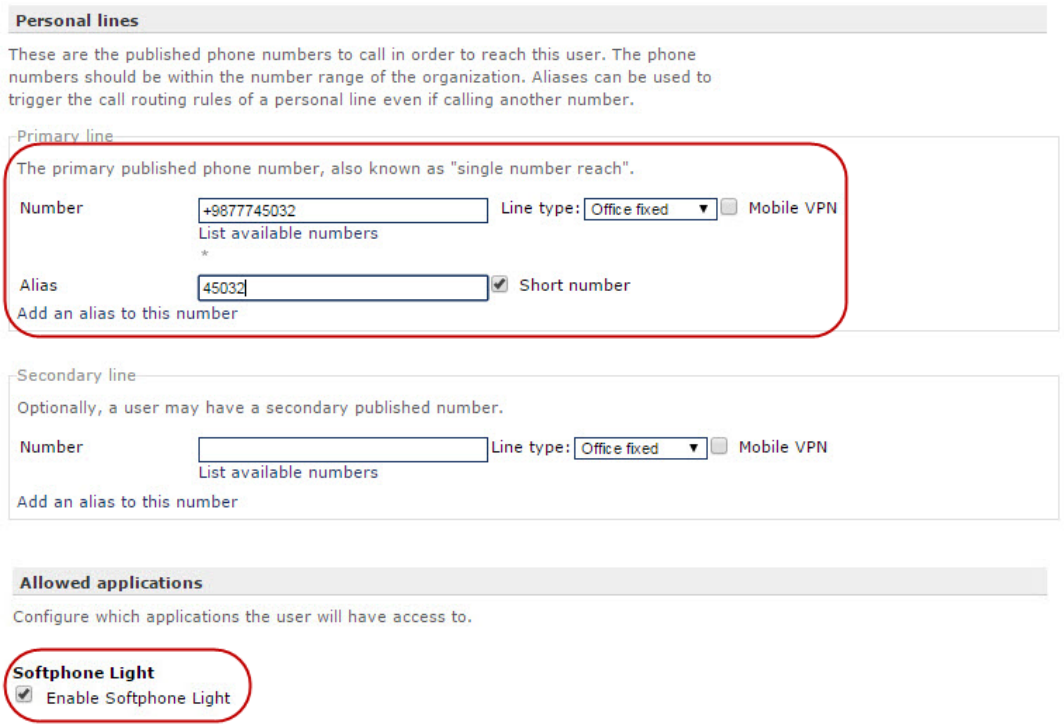
Create users

You create users in the Telepo call manager for each MiContact Center agent.

As Organization Administrator on the service node, do the following:

1. Click on the **User Administration** menu and select the **Users** option.
2. On the **Users** page, click **Create new user**.
3. On the **New user** page, specify the information for the user. In particular:

- Under **Personal lines**, assign an alias for the extension and enable the **Short number** parameter for the phone number
- Under Allowed applications, check the Enable Softphone Light option.



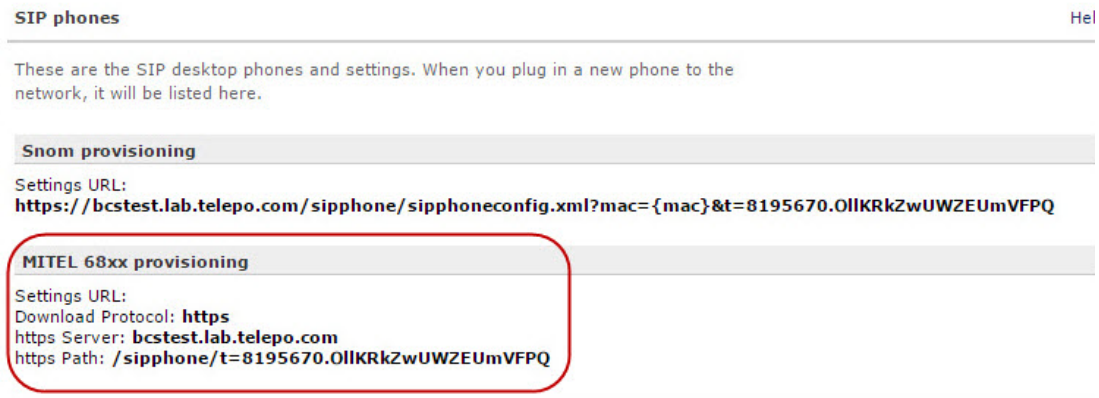
4. Click **Save** to apply your changes.
5. Repeat for each MiContact Center agent in the MiCC Enterprise system.

Provision 68XXX SIP phones

Mitel 68xxx series SIP phones must be provisioned before they can be assigned to a user. The steps below must be performed for every SIP phone in the system.

As Organization Administrator on the service node, do the following:

1. Click on the **Devices** menu and select the **SIP phones** option.
2. On the **SIP phones** page, under **Mitel 68xxx provisioning** note the Configuration Server settings that must be entered on the SIP phone for provisioning (in the **https Serve**r and **https Path** fields).



3. Obtain the IP address of the SIP phone.

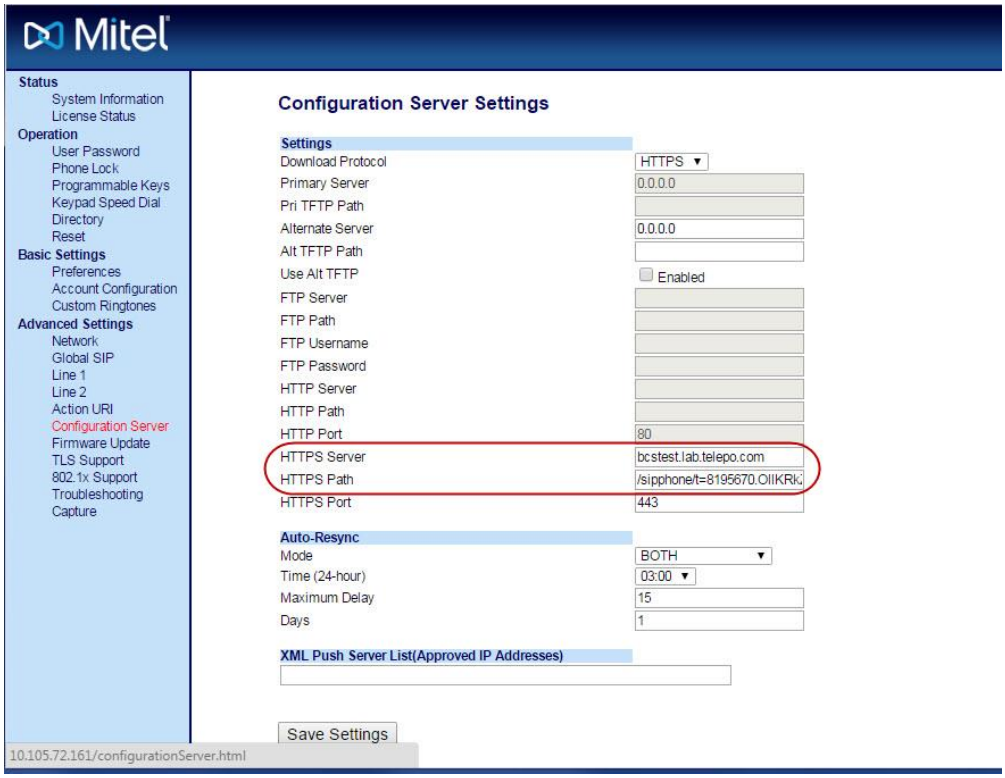
   On the SIP phone, select **Options List** > **3 Phone Status** > **IP & MAC Addresses** > **IP Address**.

4. Open a browser and connect to the SIP phone using its IP address.

5. Login in with the following credentials: **User** = admin, **Password** = 22222.

6. In the SIP phone administration interface, click on **Configuration Server** in the left navigation pane (under **Advanced Settings**).

7. Enter the values for **HTTPS Path** and **HTTPS Server** (noted above).



8. Click **Save Settings**.

9. Restart the SIP phone.

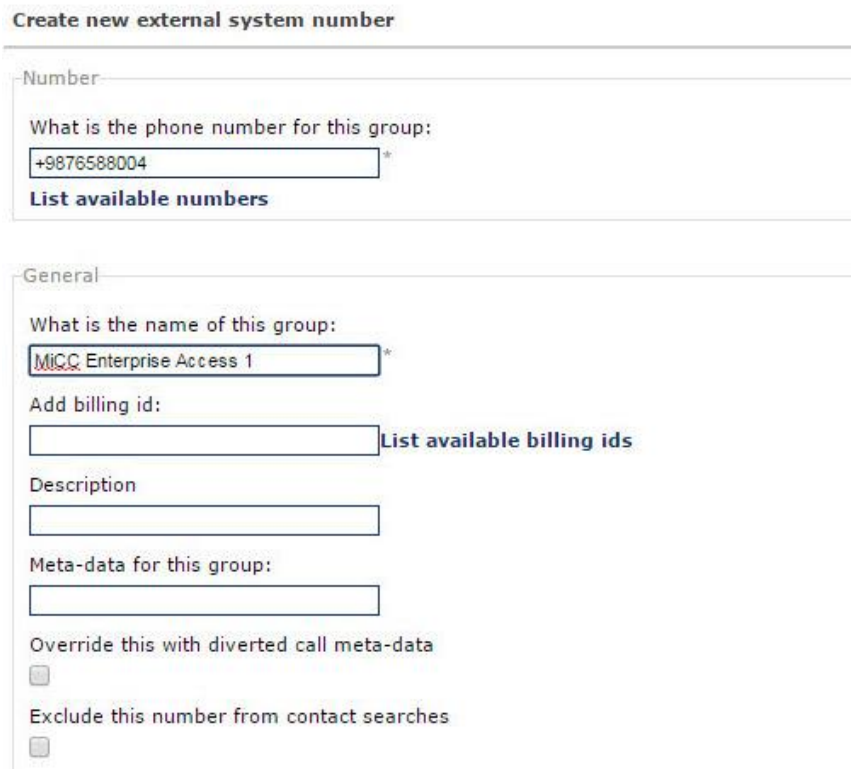
The SIP phone registers with the Configuration Server and appears in the system's SIP phone list (under Devices->SIP Phones). The SIP phone can now be assigned to a user.

Create an external system number

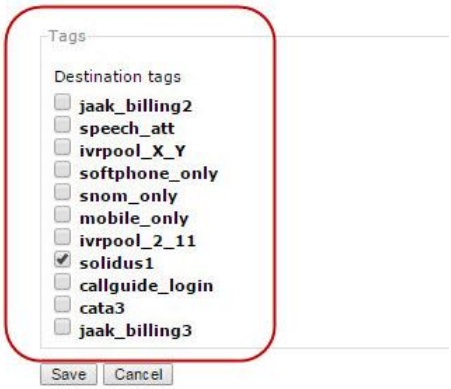
You must configure an external number for each Basic Virtual Device (BVD) number in MiCC Enterprise. The BVD is the access number used to reach the call center. There is a one-to-one mapping between function numbers and BVDs.

As Organization Administrator on the service node, do the following:

1. Click on the **Function numbers** menu and select the **External systems** option.
2. On the **External systems** page, click on **Create a new external system number**.
3. On the **Create new external system number** page, specify the settings for the MiCC Enterprise access number.



Make sure you select the destination call tag you created for the MiCC Enterprise system (under **Tags**).



4. Click **Save** to confirm your changes.

Note: MiCC Enterprise soft clients connect to the MiCC Enterprise system (and not the Telepo call manager). If you want the MiCC soft clients to be reachable from the outside world, you must configure external numbers for each softphone as well, so that the Telepo call manager can route them to the MiCC Enterprise system.

Configure number conversions

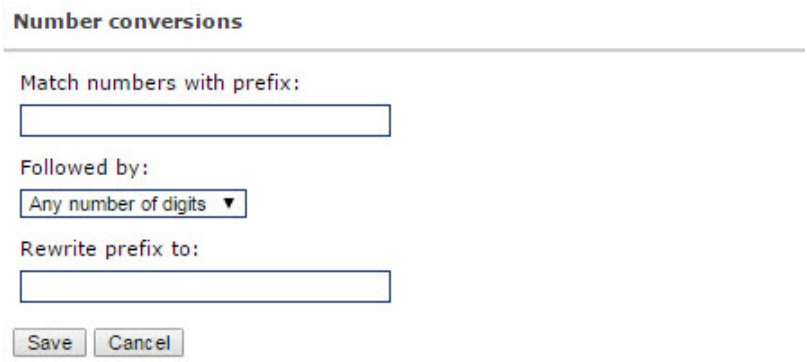
A number conversion is a rule used to map numbers to other numbers. You configure number conversions to allow users to use shorter numbers to call BVDs from their telephones.

As Organization Administrator on the service node, do the following:

1. On the management node, click on the **Services** menu and select the **Number conversions** option.
2. On the **Number conversions** page, click **Configure for all users in the organization**.

3. On the next page, click **New rule**.
4. On the next page, configure a number conversion rule for the BVD.

   For example, if the full number to a BVD is +468552000, you can configure "52" to expand to +468552. This conversion rule allows users to use 52000 to call the BVD.



5. Click **Save** to confirm you changes.

CONFIGURE TELEPO LINESTATE MONITORING

You can monitor line state presence for numbers configured on the Telepo call server. Telepo line state monitoring requires configuration in the Telepo system nodes and the TAS Configuration Tool.

Telepo system configuration

TAS uses a Dialog Info subscription to obtain line state information for a Telepo extension. The Dialog Info message must be sent to the Edge Node, which requires a user name and password for authentication.

In addition, when line state monitoring is initiated, TAS only has the phone number of the extension being monitored. Since Dialog Info subscription is not possible with only a phone number, TAS must access a Telepo API on the Management Node to look up the user associated with the number. The Telepo API requires a Token and Secret for authentication.

Create a user group

You must create a user group for the user account used to access the Edge Node and request line state information.

As Organization Administrator on the service node, do the following:

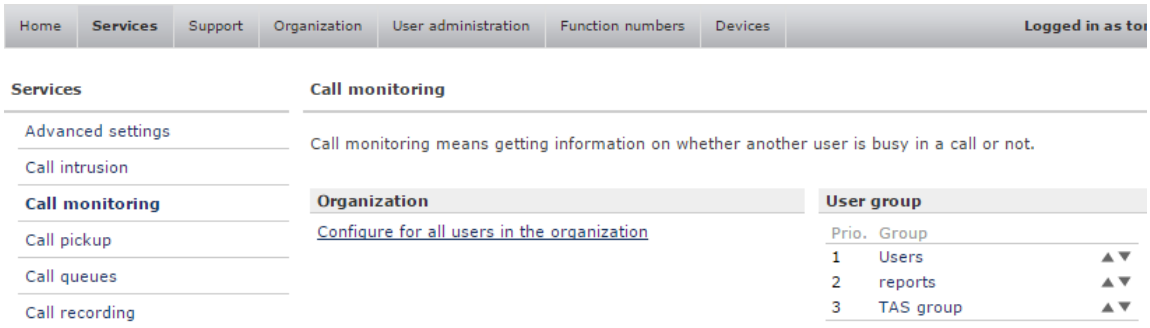
1. Click on the **User Administration** menu and select the **User Groups** option.
2. On the **User groups** page, click **New**.
3. Specify a name for the new user group.
4. Click **Save** to apply your changes.

Assign Call Monitoring permission to user group

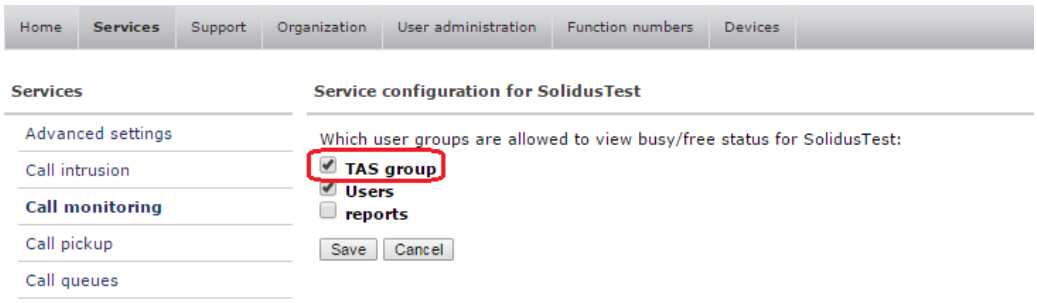
Call monitoring permissions are assigned at the user group level.

To authorize the new user group for call monitoring, do the following:

1. Click on the **Services** menu and select the **Call Monitoring** option.
2. On the **Call monitoring** page, click **Configure for all users in the organization**.



3. On the **Service configuration for <organization name>** page, check the box beside in the new user group to allow the user to see busy/free status.

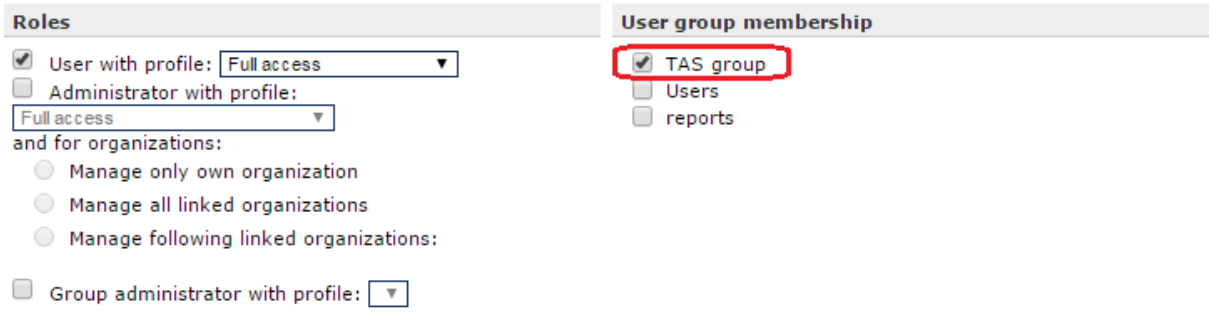


4. Click **Save** to apply your changes.

Create a user account for Dialog Info subscription

To create the new user account, do the following:

1. Click on the **User Administration** menu and select the **Users** option.
   - On the **Users** page, click **Create new user**. Note the user name and password. This information must be configured in the TAS Configuration Tool.
2. On the **New user** page, specify the information for the user. Under **User group membership**, select the newly-created user group (with call monitoring permissions).



3. Under **Personal lines**, assign a primary line number.
4. Under **Personal phones**, check the **Enable Softphone** option.
5. Click **Save** to apply your changes.

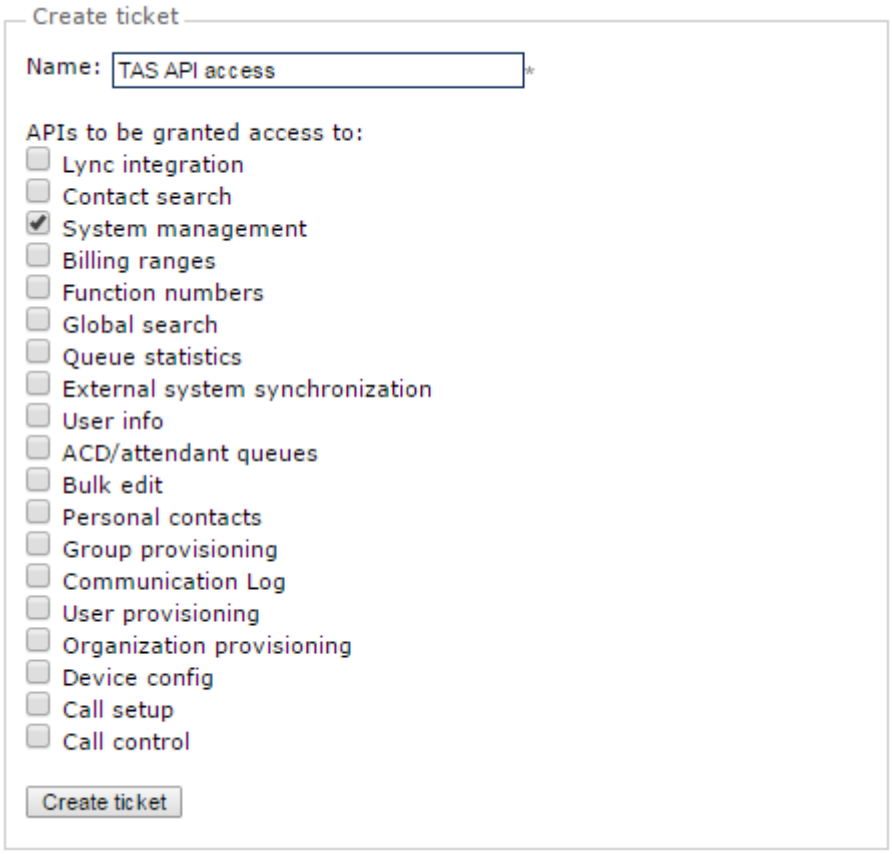
Generate a token and secret for the System Management API

TAS requires a token and secret to access the System Management API on the Management Node.

As system administrator on the management node, do the following:

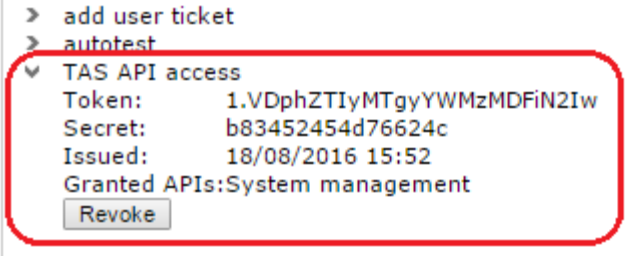
1. Click on the **Systems** menu and select the **Tickets** option.

   The **Tickets** page has two sections: **Granted tickets** and **Create ticket**.
2. Scroll to the Create ticket pane.
3. Specify a name for the new ticket in the **Name** field.
4. Select **System management** from the list of APIs.



5. Click **Create ticket** to apply your changes.

   The new ticket appears in the Granted tickets section.
6. Locate the entry for the new ticket and expand the entry (by clicking on **>**).



Note the token and secret values. This information must be configured in the TAS Configuration Tool.

TAS configuration for Telepo line state

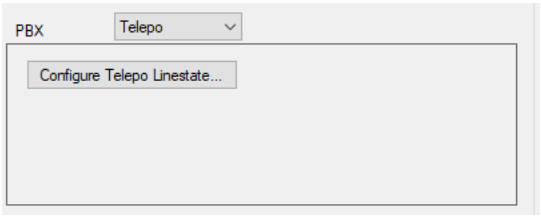
To configure line state monitoring for Telepo extensions, TAS must be able to connect to the Telepo edge node (for Dialog Info subscription) and the management node (to access the System Management API for phone number lookup).

In this procedure, you configure the following information:

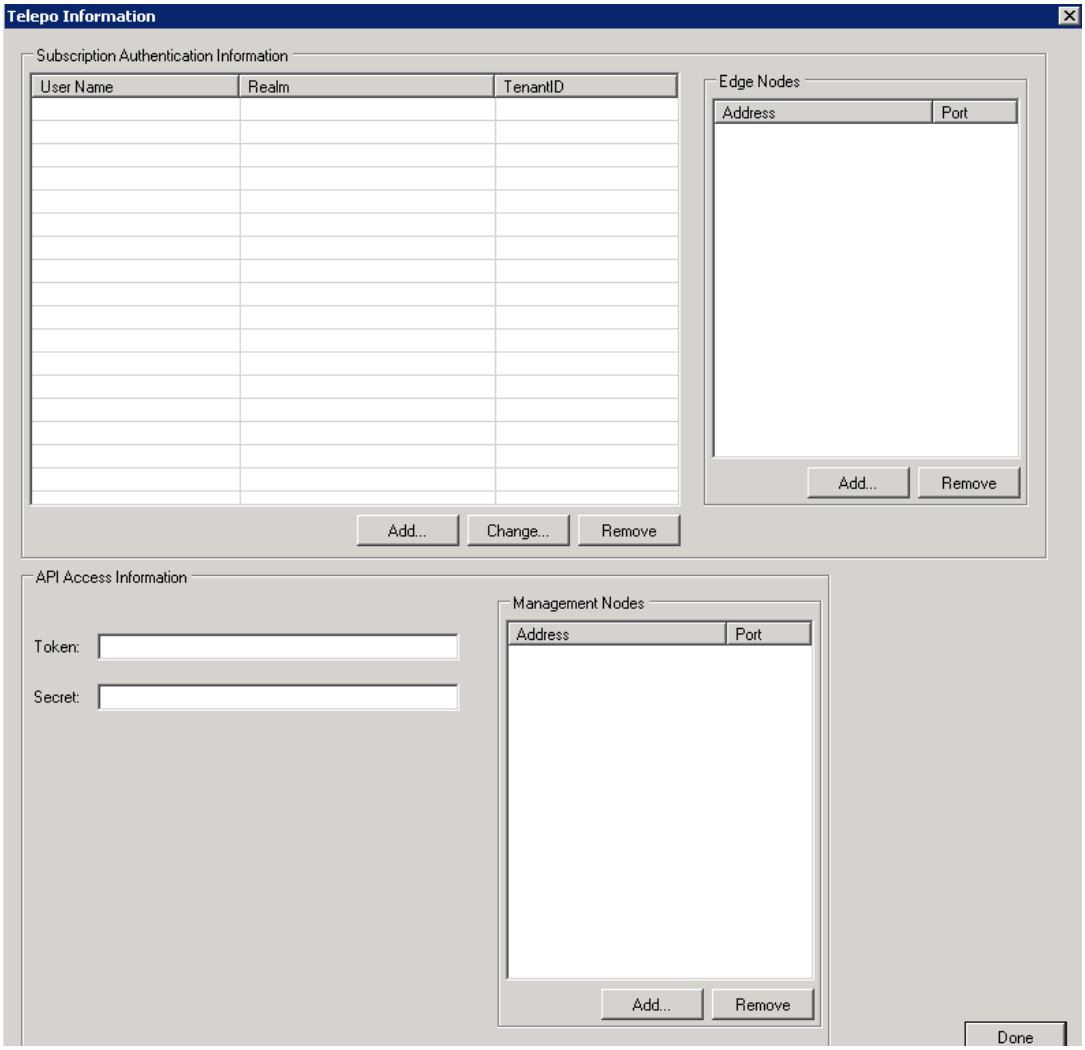
- the user account used to authenticate on the Telepo edge node for Dialog Info subscription
- the IP address of the Telepo edge node
- the token and secret pair to access the System Management API on the Telepo management node
- the IP address of the Telepo management node

In the TAS Configuration Tool, do the following:

1. Under **TAS Properties**, click on **Configure Telepo Linestate**. Note that this option will be displayed when **Telepo** is selected as the PBX.



The system opens the **Telepo Information** window.



2. Add the user account you created on the Telepo edge node.

a. Under the **Subscription Authentication Information** section, click **Add**.

b. In the **Add Credentials** dialog, enter the following information for the user account:

- **User name**: name of the user account
- **Realm**: the domain for the user's organization (on the Telepo node)
- **Tenant ID**: the number that the MiCC Enterprise system uses to identify the tenant to which the user belongs (available in the Configuration Manager on the **Contact Center System Properties** > **Configuration** tab)
- **Password**: password for the user account

c. Click **Ok** to save your changes.

3. Add an entry for the Telepo edge node.

a. Under the **Edge Nodes** section, click **Add**.

b. In the **Add Edge Node** dialog, enter the following information:

- **FQDN or IP address**: name or IP address of the Telepo edge node
- **Port**: port on the edge node (default is 5060)

c. Click **Ok** to save your changes.

4. Add the token/secret information required to access the System Management API on the management node.

   a. Under the **API Access Information**, enter the following information:

   - **Token**: value of the token in the token/secret pair generated on the management node for System Management API access
   - **Secret**: value of the secret in the token/secret pair generated on the management node for System Management API access

5. Add an entry for the Telepo management node.

   b. Under the **Management Nodes** section, click **Add**.

   c. In the **Add Management Node** dialog, enter the following information:

   - **FQDN or IP address**: name or IP address of the Telepo management node
   - **Port**: port on the management node (default is 5060)

   d. Click **Ok** to save your changes.

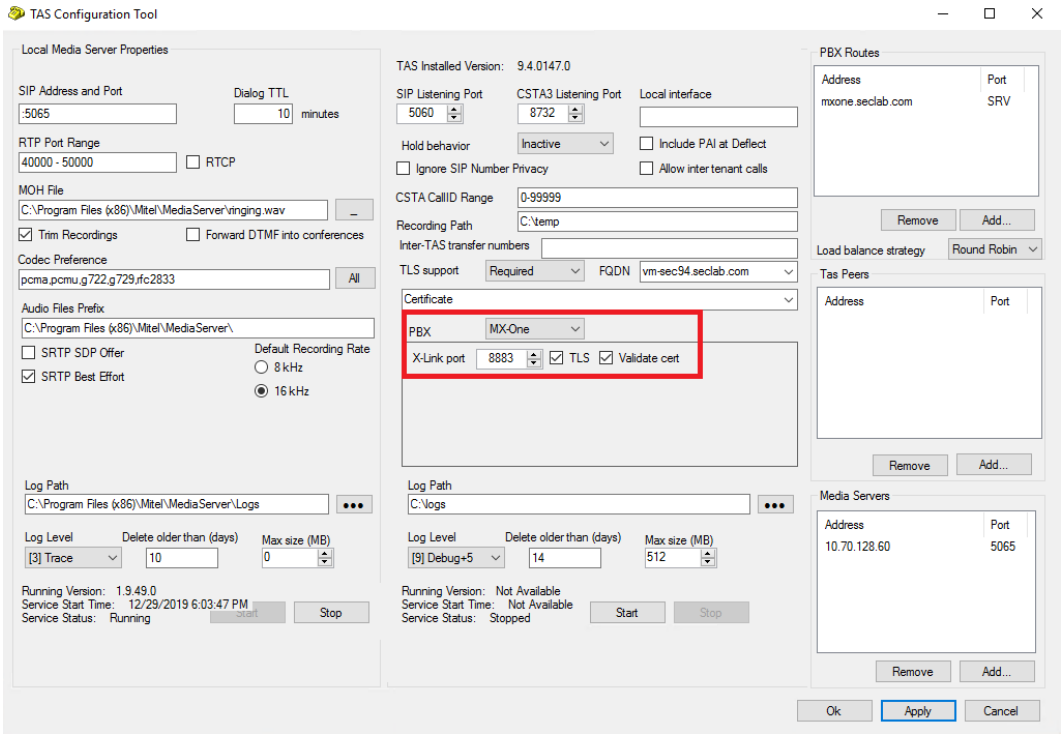
6. Click **Done** at the bottom of the Telepo Information window to save your changes.

MX-ONE INTEGRATION WITH TAS / MICC ENTERPRISE

Communication between TAS and the MX-ONE call manager is via X-link for hard phone support. If TLS is to be used the csta server is initiated on the MX-ONE at port 8883. If TLS is not used the default is 8882.

Example:

csta -i --lim 1 --port 8883 --csta-serv 000000000



In this case please note that TLS support is required. In TAS Configuration, port 5060 will be entered, and then TAS will assume that TLS is supported on one port higher, i.e. on port 5061.

Note: MiCC Enterprise soft clients connect to the MiCC Enterprise system (and not the MX-ONE call manager). If you want the MiCC soft clients to be reachable from the outside world, you must configure external numbers for each softphone as well, so that the MX-ONE call manager can route them to the MiCC Enterprise system.

HOST NAME IN CONTACT FIELD

If the MX-ONE sets the host name in the Contact header, TAS must be able to resolve the host name. This is the case for MX-ONE 7.1 HF01 or higher. There are two possible methods for resolving the host name if it cannot be added to the DNS lookup for the network:

1. Modify the hosts file on the TAS machine to include an entry for the MX-ONE host name as follows:
   192.168.145.10 lim1.MX-ONE
2. Modify the SIP trunk profile used for the TAS SIP trunk to not use the FQDN (Fully Qualified Domain Name) in the Contact header as follows:
   TrunkProfile:MiCC_Tas:SipUseFqdnInContact: no

MX-ONE SIP TRUNK PROFILE

A SIP trunk profile named MiCC_Tas is available when initiating the SIP trunk from the MX-ONE to the TAS server. Depending on whether plaintext or TLS is desired, the protocol variable will be different.

Example:

sip_route -set -profile MiCC_Tas -remoteport 5061 -route 8 -uristring0 'sip:?@10.70.128.81' -accept REMOTE_IP -match 10.70.128.81 -protocol tls

```
MDSH> sip_route -print -route 8 -short
Route data for SIP destination

route : 8
  protocol        = tls
  profile         = MiCC_Tas
  service         = PRIVATE_SERVICES
  uristring0      = sip:?@10.70.128.81
  remoteport      = 5061
  accept          = REMOTE_IP
  match           = 10.70.128.81
  register        = SET_BY_PROFILE
  trusted         = TRUST_BY_PROFILE
  supervise       = ACTIVE_SUPERVISION
  supervisetime   = 30
```

Refer to MX-ONE CPI documents with regards to TLS, encryption and Certificate Management:

CSTA Server (Phase III) Operational Directions: 130_15431_ANF90114.pdf

Certificate Management Operational Directions: 132_15431_ANF90114.pdf

MX-ONE SIP EXTENSION PROFILE

If SIP desktop phone extensions are used with TAS with the per-call option, the following parameter must be set in the extension profile:

```
Common Service Profile
Csp Cust  Traf       Serv                           Cdiv            Roc    Npres   Offered Forced          CnnLog Csp Name
                                                                                    Time    DisconnectTime
0   0     0000151515 00000300000000000000000000000000 000000000000000 000001 0000000 0       0               0      CSP 0
```

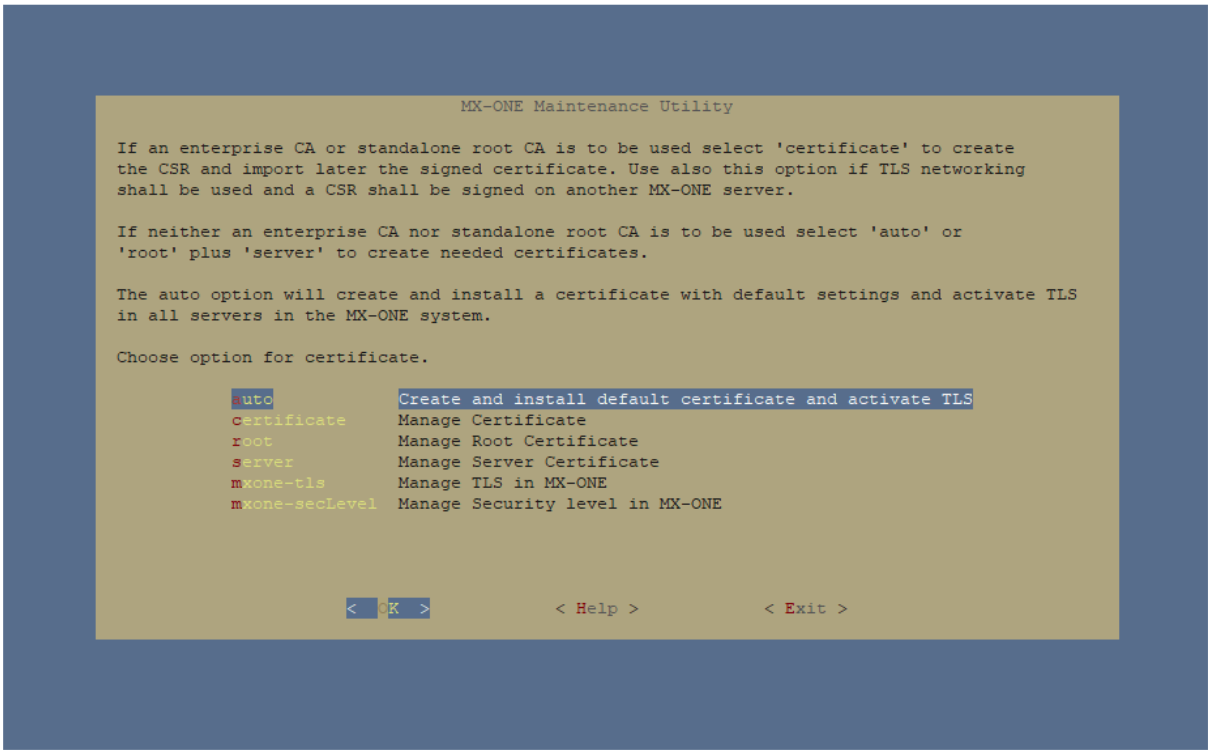
Note that digit 29 must be set to 0 as shown above.

CREATING SIGNED CERTIFICATES FOR TLS IN THE MX-ONE

The following instructions apply to MX-ONE version 7.0.0.2.5 with a single LIM. This allows the user to create a Certificate Authority (CA) and sign server certificates using the created CA.

Follow the steps below to configure the MX-ONE:

1. As root, run mxone_certificate. The following screen will be displayed:



Select **auto**. This will create a Certificate Authority (CA), a server certificate for the MX-ONE, and enable TLS in the MX-ONE.

2. The system will prompt you to enter a password for the CA and for the server certificate. Note that in this example, the passwords for both the CA and certificate are set to **Mitel#123.**

3. Reload the necessary MX-ONE program units as instructed. Note that this will affect ongoing traffic.

4. Change the directory to **/etc/opt/eri_sn/certs** and verify that the files **CA.pem** and **mxone.pem** have been created

5. Ensure that the protocol of the SIP Trunk Profile MiCC_Tas created in the MX-ONE is set to TLS using the following command:

   sip_route -set -route 4 -protocol tls

6. Enable TLS on the CSTServer using the SERV parameter. In the following example, TCP is running on port 8882 and TLS is enabled on port 8883.

```
ts1:/tmp/certs # csta -p --lim 1
Lim  Port    Serv       IP Address
1    8882    0000000000 10.105.79.150
1    8883    0000000100 10.105.79.150
```

The next step is to create the server certificate to be used by TAS for TLS. Follow the steps below:

1. Change the directory to /tmp

2. Create a new directory called **certs**

3. Change the directory to certs

4. Create a 2048-bit private key using the following command:

   openssl genrsa -out private.key 2048

5. Create a new Certificate Signing Request (CSR) using the following command:

openssl req -new -sha256 -key private.key -subj "**/C=SE/ST=SE/O=MiCC Enterprise TAS/CN=solidus.lab.se**" **-out solidus.lab.se.csr**

Note: The value following **CN=** must be the fully qualified domain name of the Windows server that is running TAS. In this example, it is **solidus.lab.se**.

Important Note:
Since the FQDN is used in the CN when creating the CSR, the value of **-uristring0** must be entered as the FQDN of the TAS server as well when creating the SIP trunk inside the MX-ONE.

Example: -uristring0 "sip:?@solidus.lab.se"

Also, ensure that DNS is configured correctly on the MX-ONE so it can resolve the name of the TAS server.

To read more about the C, ST and O parameters, please refer to the OpenSSL documentation for the MX-ONE.

6. Create the server certificate using the following command:

openssl x509 -req -in solidus.lab.se.csr -CA /etc/opt/eri_sn/certs/root/CA.pem -CAkey /etc/opt/eri_sn/certs/root/private_key.pem -CAcreateserial -out solidus.lab.se.crt -days 365 -sha256 -passin pass:Mitel#123

Replace the password **Mitel#123** with the password for your certificate. This request will apply for most systems using the **auto** settings in the MX-ONE. The paths may need to be adjusted if your system differs.

If you increase the number of days, make sure the value does not extend beyond the number of days specified for the Certificate Authority (CA) to expire.

7. Create a server certificate and private key combination for the TAS Windows server using the following command:

openssl pkcs12 -export -out solidus.lab.se.pfx -inkey private.key -in solidus.lab.se.crt -password pass:Mitel#123

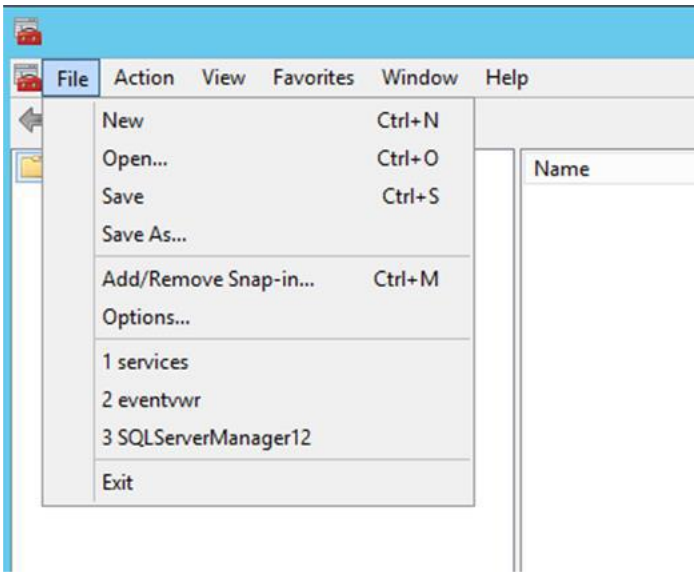
Replace the password **Mitel#123** with the password for your certificate.

Follow the steps below to install the certificate on the Windows server running TAS.

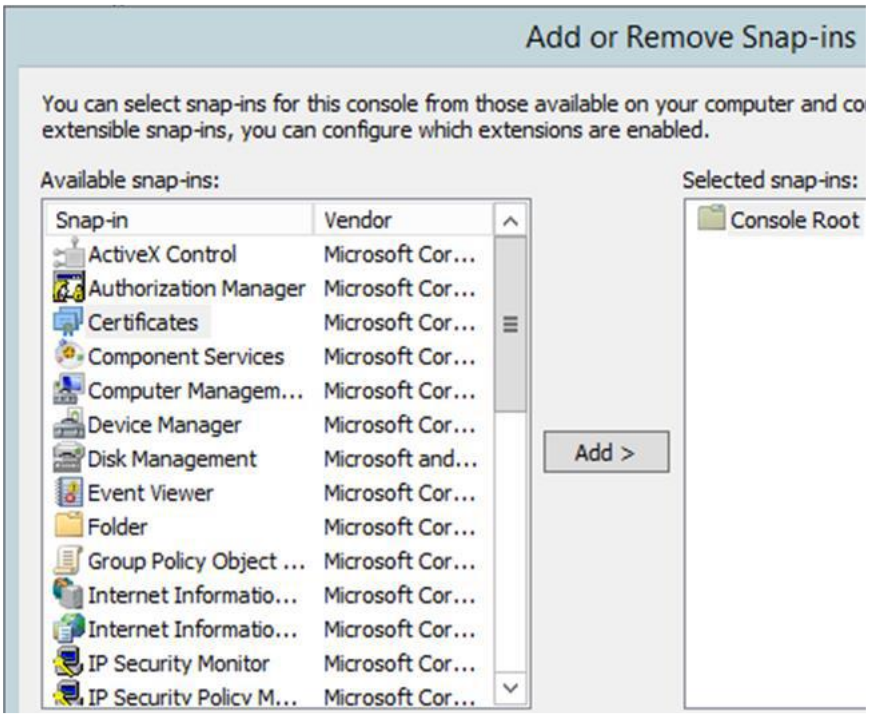
1. Copy the CA.pem file and the newly created .pfx file to the Windows server running TAS.

2. Enter **mmc** to open the Microsoft Management Console.

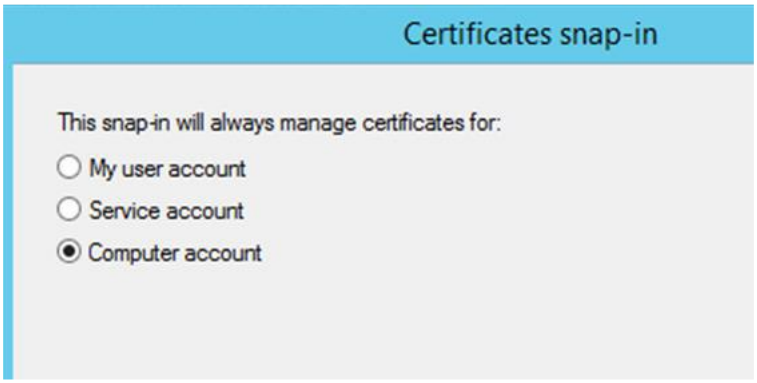
3. Add the snap-in module for Certificates by selecting **Add/Remove Snap-in** from the menu.



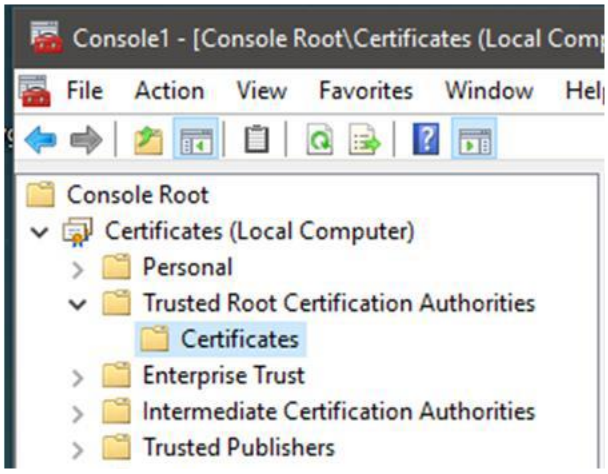
4. Select **Certificates** from the list and press the **Add >** button to add the snap-in.



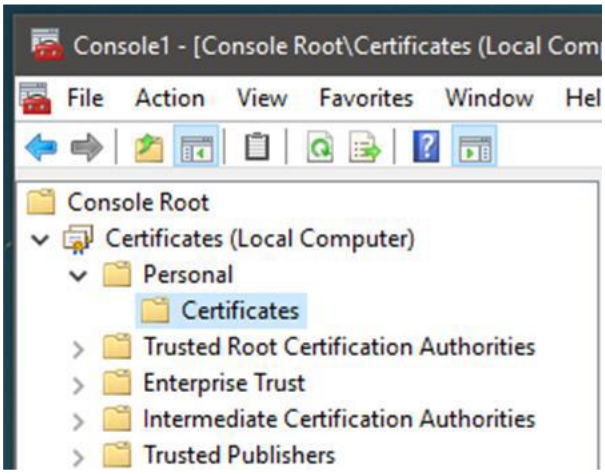
5. When prompted, select **Computer account**



6. The CA.pem file should be installed in the directory shown below:



7. The server certificate (.pfx file) should be installed in the directory shown below:



Refer to the Windows documentation for further information regarding importing a trusted root certificate and a server certificate:

https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate

8. Open the TAS Configuration tool, set TLS support to **Required** and select the newly imported certificate from the drop-down list.

DESKTOP PHONE SUPPORT

MiCC Agents and Web Agents can use desktop phone devices on a SIP-enabled call manager. CTI integration for private calls is enabled if X-Link is connected for the MX-ONE call manager.

Note: Line state monitoring is applicable only for Cisco and Telepo call managers.

The agent's desktop phone will be called when a call is routed to the agent. If CTI integration is available, the phone will be automatically answered. After the call is answered, the customer call will be connected to the agent's desktop phone. This allows the agent to receive MiCC Enterprise calls via the desktop phone and still receive personal calls directly to the agent's desktop phone extension.

FEATURES SUPPORTED WITH DESKTOP PHONE

The table below lists the features supported in MiCC Agent and Web Agent when desktop phones are used for MiCC Agents.

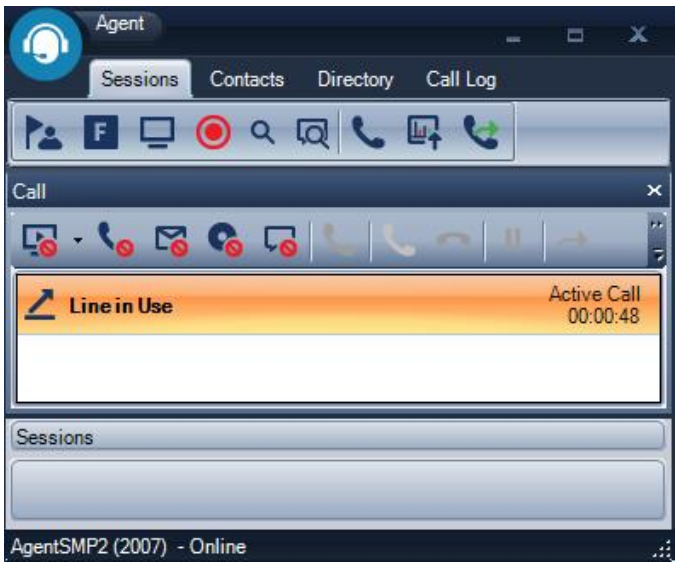
FEATURE	MX-ONE with X-Link	Other Call Managers
Make Call[Note 1]	✓ (Agent's phone is called first and then the call is initiated)	✓ (Agent's phone is called first and then the call is initiated)
Answer Call	✓ Note 1	✗ (calls must be answered from the phone)
Hangup Call	✓ Note 1	✓ Note 1
Hold Call	✓	✓
Retrieve Call	✓	✓
Transfer Call	✓	✓
Conference Call	✓	✓
Divert to Service Group	✓ (if call is connected)	✓ (if call is connected)
Divert to Agent	✓ (if call is connected or a service group call)	✓ (if call is connected or a service group call)
Assist	✓	✓
Monitor	✓	✓

Record Calls	✖	✖
Enter DTMF Digits	✖	✖
Reject Service Calls	✓	✓
Consultation Call	✓	✓
Handle Callback Calls	✓	✓
Participate in a Call Campaign	✓	✓

Note 1: These features are available if the device type supports the feature. For example, if the desktop phone is an analog device, Make Call and Answer Call are not supported due to limitations with the analog device.

LINE STATE MONITORING

When using desktop phones, the MiCC Agent or Web Agent can initiate call activities with the physical phone, but the MiCC Enterprise Router does not know about the device unless Line State Monitoring is configured. This configuration is performed in the Cisco or Telepo call manager. When Line State monitoring is configured, a MiCC Agent or Web Agent who makes or receives a non MiCC Enterprise call will display “Line in Use, Active Call” as the call status in the Agent call window and thus the Router will know that the extension is not available for Service Call distribution. In addition, all call control through Agent or Web Agent will be disabled until the call is cleared from the phone.



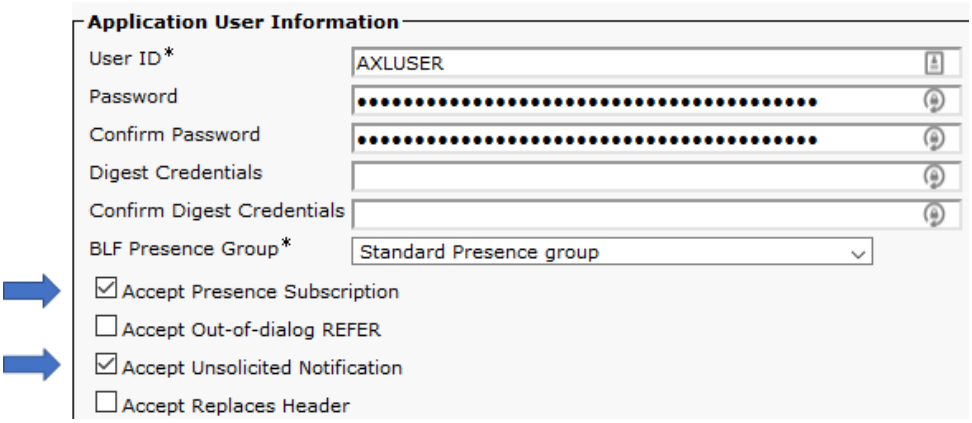
When TAS is connected to a Cisco call manager, it can communicate via both the SIP trunk and the AXL web service. The web service communicates with the Cisco publisher machine.

To access the AXL web service, it is necessary to create an Application User account on the Cisco call manager. It is recommended to create a new dedicated user for this role, as shown in the example below.

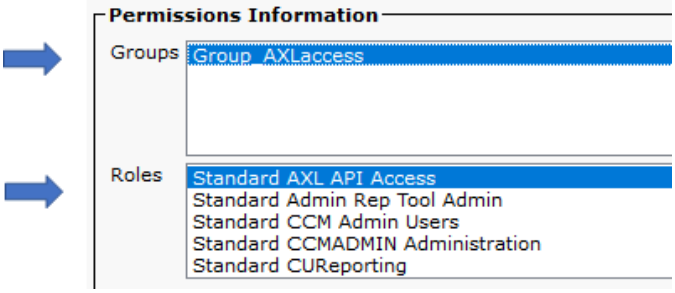
The AXL web service is used to obtain the forwarding status of the monitored extensions. To limit the load on the Cisco call manager, the number of AXL requests can be limited. It is recommended to keep the default value of 60. A single query is used from TAS toward the AXL web service for the forward status of all monitored devices, which limits the number of queries required.

It is not necessary to configure a SIP trunk for line state on the Cisco call manager, or to configure a security profile for the SIP trunk.

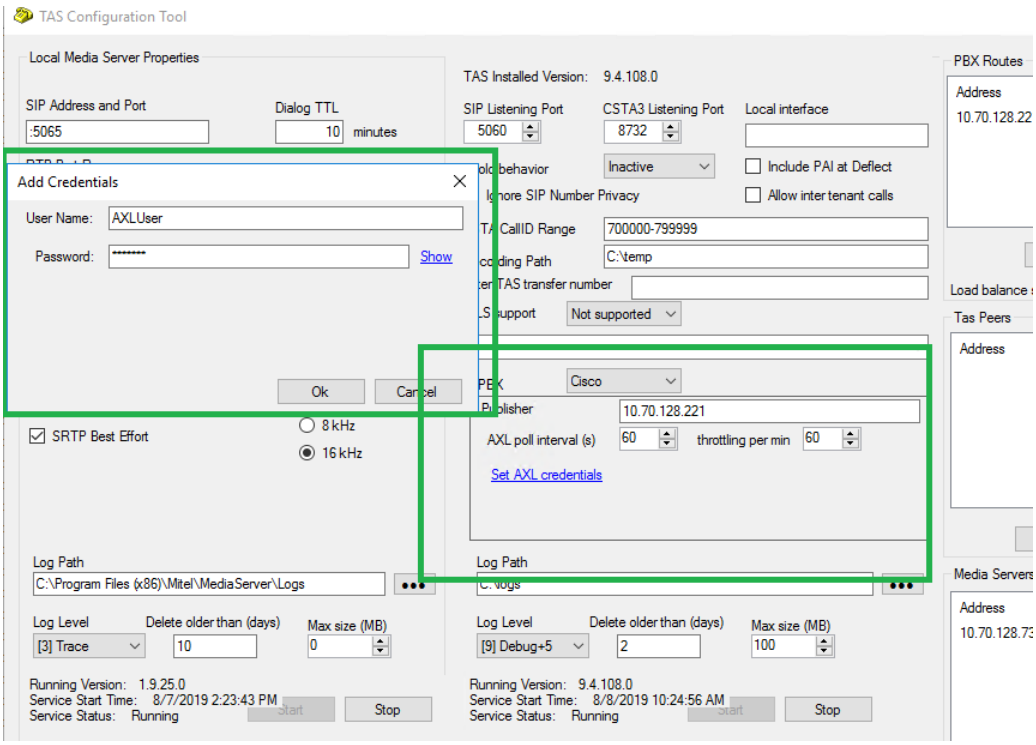
The following example shows configuration of the AXL web service user account. Note that "Accept Presence Subscription" and "Accept Unsolicited Notification" must be selected.



The permissions for the user should be set as follows:



In TAS Configuration, enter the location of the AXL web service in the Publisher text box. Select the "Set AXL credentials" link to enter the user name and password of the account to be used to access the AXL web service, as configured on the Cisco call manager.



MULTI-TAS SETUP

Note: If your system is setup with multiple sites but a single TAS server, the Call Manager in each site must have a unique name so that when clients connect to the MiCC-E Call Control Service, they can indicate the Call Manager to which they wish to connect. To accommodate this, define a unique DNS entry for the Call Manager Server Name for each site, where all the names reference the same server, where TAS is running. In addition, the following registry value must be added to the MiCC-E Call Control Service registry (HKLM\System\CurrentControlSet\Services\CCCallControl\Parameters):

Name: CompareServerIPAddresses
Type: DWORD
Value: 0

When this value exists and is set to 0, the MiCC-E Call Control Service will only compare the provided Call Manager Server Name and not try to resolve the IP address. This will allow unique Call Manager Server Names for each site when there is a single TAS server.

If the MiCC Enterprise system is configured to use multiple TAS servers, ensure that the following items are configured properly:

- The Requeue Call Manager is set in Configuration Manager system properties on the Call tab to be “Same as the Agent”. This will reduce the number of connections to the Media Server when the call is requeued by the agent.
- Languages defined on each TAS system must have the same Language ID configured. This can be modified in MiCC-E Configuration Manager as follows:
    - In the Properties dialog when defining a language, the ID may be specified by appending it to the language name separated by a colon. For example, to set the ID to 100 for English, specify the name as:

      ENGLISH:100

      The ID may be specified when adding a new language or it may be modified for an existing language. If the ID is not specified when adding a new language, a generated ID will be used. If the ID is not specified when modifying an existing language, the ID will not be changed.
- Play Message Lists and Play Message IDs must be the same for each TAS system. The Play Message IDs are configured in MiCC-E Configuration Manager when defining the message for each TAS system.
- For optimal performance, it is recommended that the MiCC-E Call Control Service and at least one Media Server are configured for each TAS system. Please refer to Media Server for information on the traffic handling capacity for each Media Server.

LOAD BALANCING INCOMING CALLS

Load balancing traffic to multiple TAS servers can be achieved in many ways:

- Using DNS (multiple HOST records)
- Using DNS SRV record
- Cisco
    - Configure multiple destination IP addresses in SIP trunk configuration
    - Use a Trunk Group

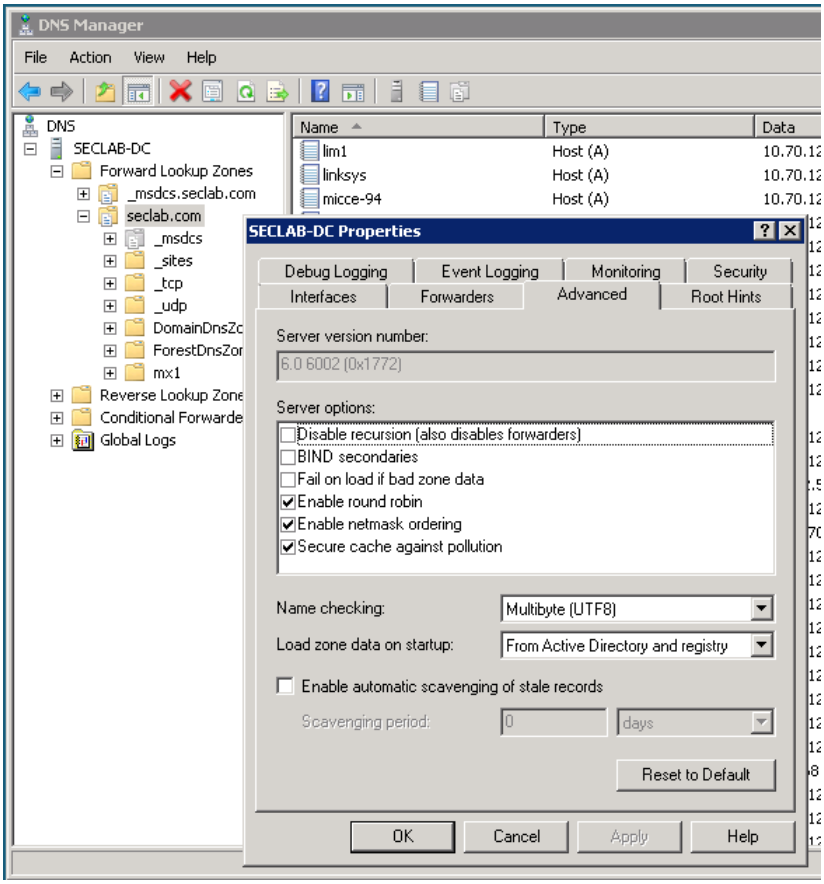
Example: Configure Windows DNS with multiple HOST records

Sample environment

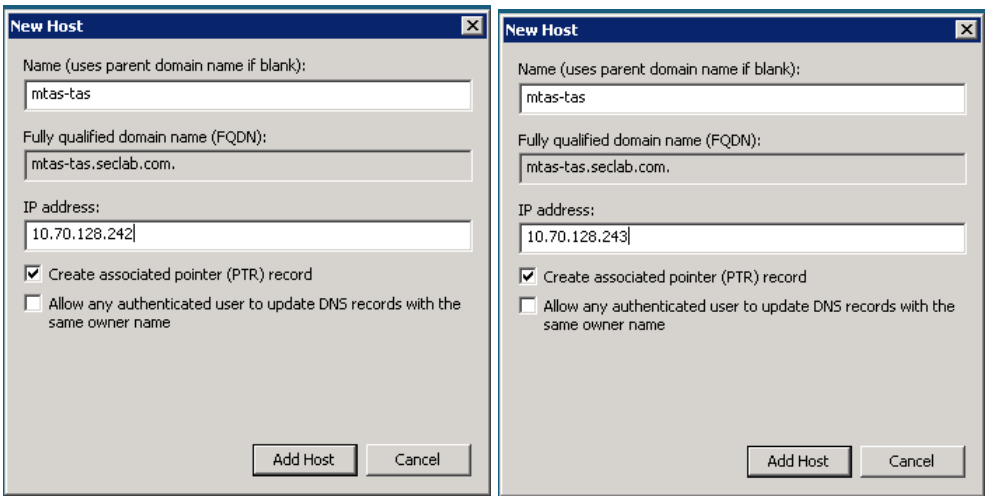
Windows domain: seclab.com

MiCC-E server:	mtas-micce.seclab.com	IP: 10.70.128.241
TAS 1:	mtas-tas1.seclab.com	IP: 10.70.128.242
TAS 2:	mtas-tas2.seclab.com	IP: 10.70.128.243
MX-ONE:	mxone7.mxone.seclab.com	IP: 10.70.128.177
DNS server	seclab-dc.seclab.com	IP: 10.70.128.101

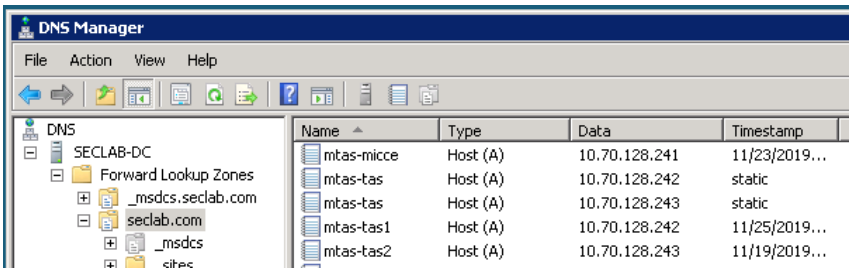
On the DNS server for seclab.com, enable Round Robin:



Create multiple HOST records for a new entry (mtas-tas):



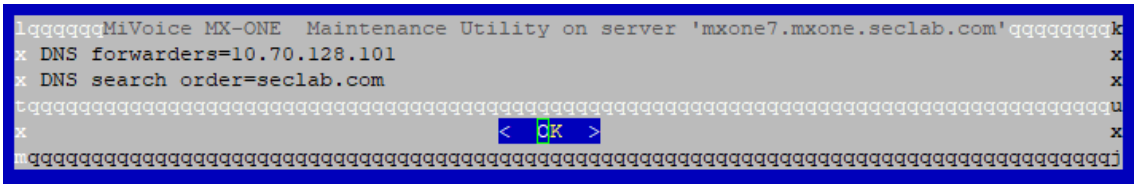
Now the DNS for mtas-tas will look like this:



The DNS server will now alternate giving out address 10.70.128.242 and 10.70.128.243 when a DNS lookup is done for mtas-tas.seclab.com.

Configuring MX-ONE

Use the mx-one maintenance tool to set DNS forwarder to the Windows DNS server:

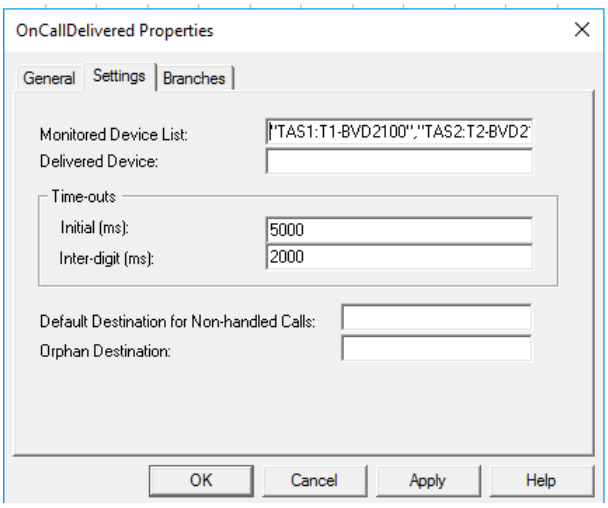


Configure the SIP route to the TAS servers. Note that the *match* parameter should contain the IP addresses of both TAS servers:

Configure the trunk access code to reach the BVDs in TAS. In this example trunk access code 21 will be used to reach the BVDs in TAS 1 and 2 that use number 2100:

roddi:dest=21,route=20,adc= 05050000000002500050010100000,srt=1;

In Configuration Manager, create a BVD in each TAS for number 2100. For instance, create a BVD called T1-BVD2100 in TAS 1 and a BVD called T2-BVD2100 in TAS 2. Configure your IVR script to use both these BVDs as Monitored device in the onCallDeliverd block:



Now calls to 2100 in MX-ONE will be evenly distributed between TAS 1 and TAS 2. If one of the TAS servers is not available then all calls will be sent to the working TAS.

Note: If the Monitored Device List is defined using variables, a separate variable should be created for each BVD. For example, variable bvd1 = “TAS1:T1-BVD2100”, variable bvd2 = “TAS2:T2-BVD2100”, etc. Enter the variables names in the Monitored Device List as @bvd1, @bvd2, …

This will allow editing of the variables in the Configuration Manager Service Access Properties dialog.

LIMITATIONS AND FEATURE DIFFERENCES

Note the following limitations in a TAS-based MiCC Enterprise system:

- VoiceXML is not supported with the TAS solution.
- In TAS based systems, only one Site is supported. This site can however contain multiple TAS servers for capacity and redundancy.
- TAS and OAS cannot be run simultaneously.
- Tone Generator resources are not supported with the TAS solution.
- Deflection of a private call before it is answered by an agent is not supported in MiCC Agent.
- Answering of an incoming call via MiCC Agent when using a hard phone is not supported except when X-Link is enabled on the MX-ONE call manager.
- Private data associated with the call, such as through an Associate Data Script Manager block, does not persist once the call is transferred to a non-agent. Private data is displayed for service group calls transferred to another MiCC Agent.

- If a MiCC Agent supervisor is monitoring a MiCC Agent, and the agent puts the call on hold, the supervisor remains monitoring the agent until the agent drops from the call.
- Transfer of a service group call by a MiCC Agent to another service group through a consultation call and transfer is not supported. It is possible to use the Service Group Transfer feature to directly divert the call from the agent to another service group.
- Conference calls between MiCC Agents, and other call manager extensions are not supported unless there is an incoming Service Group call involved in the call. This is supported when X-Link is enabled on the MX-ONE call manager.
- Conferences between an agent and a BVD are not supported. A conference cannot be created until the call is routed to an agent.
- If a conference is created with a private call and another softphone agent (via private or Service Group call), the softphone agent will not display “Conference” state since it cannot be monitored through X-Link. The agent creating the conference will display “Conference” in the Agent call window.
- Supervisor monitoring is not supported for calls that are not Service Group related
- Bypass Diversion is not supported with the Cisco call manager. This refers both to the Attendant Agent Bypass Diversion feature as well as when an agent performs an Attendant Transfer to a diverted extension. In this case, the call will forward to the diverted extension.
- Set Diversion is not supported with the Cisco call manager.
- Call lists defined on agent extensions with direct or follow-me diversion are not supported. Call lists may be defined with no answer diversion, but the no answer time out period must be greater than the ring time supervision time out defined in MiCC Enterprise.
- The following call scenario is not supported when using call lists: Agent has a held call, then makes a call to an extension that has a call list which is diverted to a BVD. The agent transfers the held call.
- Extension service codes such as Account Codes are not supported when making calls through TAS.
- When creating a conference call in a multi-TAS environment, if the added conference member is monitored on a different TAS server than the conference leader, the conference member will display Talking state instead of Conference state.
- To support Attendant Transfer to voice mail using TAS, ensure that the registry value HashStarHashMeaning is set to Diversion as explained in the TAS Registry Settings section.
- If a Media Server fails while a queued call is connected to the Media Server, there will be no further media for the call unless it is directed to an agent or requeued. New media requests will avoid the failed Media Server.

SCRIPT MANAGER RECORD BLOCK VS OAS-BASED SYSTEM

There are a number of differences and some limitations in the Script Manager Recording function when TAS is used vs OAS, most of them due to differences in how the recording function in the TAS Media Server is implemented.

- MiCC Enterprise uses the existing capabilities in the TAS Media Server for recording. What is added is the capability of MiCC Enterprise to instruct the Media Server (via TAS) to start the recording and to implement functionality in TAS to pass on recording requests to the TAS Media Server via SIP. TAS receives SIP events for recording progress and

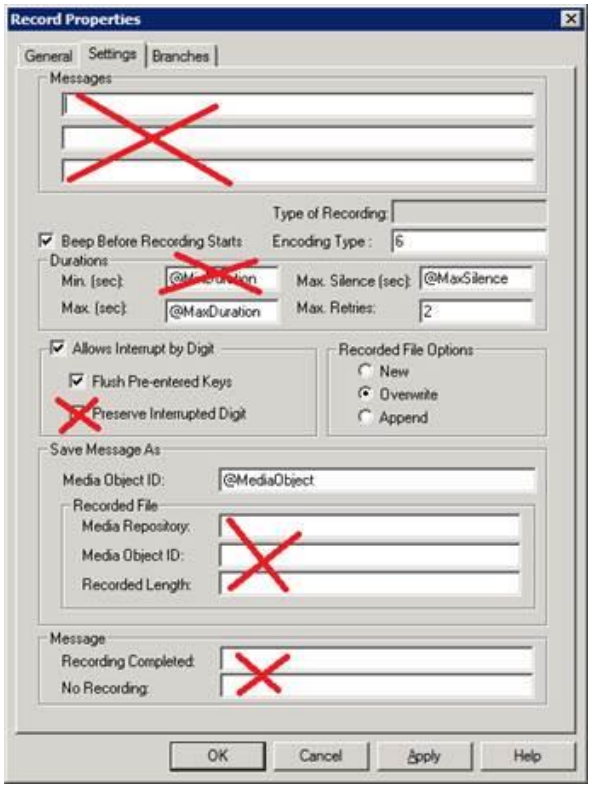
generates CSTA events (Recording Started, Recording Ended, etc.) to MiCC Enterprise. Limitations in the Script Manager Record block are that Minimum Duration and Preserving the DTMF digit that interrupted the recording are not implemented when using TAS.

- Message fields in the record block are not implemented when using TAS. The limitation of not being able to play a message in the record block can be overcome by playing any necessary intro messages (or trailing messages) before entering the Record block in SM.

As for where to store the recordings, you can include the sub-folder structure as part of the Media Object ID. For example, if the configured recording path is set to C:\Recordings, then if your Media Object ID is set to \VoiceMail\User\bstenlund\greeting.wav, the recording is stored in C:\Recordings\VoiceMail\User\bstenlund\greeting.wav

If multiple media servers are configured a directory synchronization mechanism must be deployed. Synchronization of media server folders is not automatically done by TAS or the Media Server.

The following figure indicates which fields are supported when TAS is used:



LIMITATIONS WITH TELEPO

The following limitations exist when integrating MiCC-Enterprise with Telepo:

- Same Keyword Search not supported for Attendant Agent
- Same Department Search not supported for Attendant Agent

- Custom User Defined Field Search not supported for Attendant Agent
- Add/Display/Manage Activities for users not supported for Attendant Agent
- Diversion Bypass not supported for Attendant Agent
- Send call to Voice Mailbox not supported for Attendant Agent
- Busy Lamp Field with Line State in Personal Contacts not supported for Attendant Agent

PROGRESSIVE CALL CAMPAIGNS

- To use a progressive dialing call campaign with TAS, the Dialing Device must be configured as a BVD, since virtual extension dialing is not supported. Note that the number of the BVD should be entered in the Device Start/Device End fields.

WINDOWS EVENT LOG

The following Event IDs will be logged to the Windows Event Log by TAS for the condition indicated:

EVENT ID	EVENT NAME	TYPE	DESCRIPTION
1000	DnsLookupFail	Warning	Lookup of remote host name fails.
1001	PbxNodesUnreachable	Warning	TAS is unable to connect to any of the configured PBX nodes.
1002	MediaServersUnreachable	Warning	TAS is unable to connect to any of the configured media servers.
1003	CpuLoadHigh	Warning	New INVITE request rejected since current CPU load exceeds the configured value which defaults to 95%. The default value can be changed through the registry value CPUAcceptLimit.
1004	TooManyPendingCalls	Warning	New session rejected due to pending calls reaching the default limit of 500. The default value can be changed through the registry value MaxPendingCalls.
1005	TransportTooSlow	Warning	New session rejected due to time required to process the session through the transport layer exceeded 7 seconds. The default value can be changed through the registry value MaxTransportLayerQueueTimeMS.
2000	UnknownNumber	Information	New session rejected due to targeted

			number is unknown to TAS.
2001	TenantToTenantBlocked	Information	New session, deflected call, or initiated call blocked since it is targeting another tenant and calls between tenants are prohibited. Calls between tenants can be allowed by checking the option “Allow inter tenant calls” in TAS Configuration.

TAS REGISTRY SETTINGS

The following table lists registry settings supported in TAS to customize the behavior of TAS for particular call situations. All values are located at HKLM\Software\WOW6432Node\Mitel\Tas.

Most settings are not changed from the default in most installations. In some cases, updates are required to improve interoperability with Call Managers and other components.

VALUE	DESCRIPTION	DEFAULT VALUE
AfterDivertAbortDelay	Number of milliseconds to delay following a Divert request.	0
AgentBusyRetryGrace	If an agent is busy when a call attempts to deflect to the agent, amount of time TAS should wait to allow currently terminating calls to terminate.	2000 (msec)
AgentDivertedIgnoreList	Defines a list of number ranges. If a diversion to one of these number occurs, the remote user change is hidden from MiCC-E. Syntax is 2000-2003;2006;2008-2009	Empty
AgentDivertedWhiteList	When diverting a call to an agent, if values are defined in this list, only diversions to the defined number ranges are allowed. Syntax is 2000-2003;2006;2008-2009	Empty
AgentDivertedBlackList	When diverting a call to an agent, if values are defined in this list, diversions to the defined number ranges are not allowed. Syntax is 2000-2003;2006;2008-2009	Empty
AgentMakeCallRemoteOverride	If this is set for SMP agents, the static number configured in this registry value will be set as the From party in the call to the desktop phone. This makes it possible to hide the caller	Empty, indicating that the caller number is displayed.

	identity for SMP Agents.	
AllowCallsBetweenTenants	Set in TAS Configuration utility using “Allow inter tenant calls”	0 (False)
AllowPlaintextSoftphone	If TAS is set to TLS-only, setting this value to 1 (True) will allow softphones to talk clear text with TAS.	0 (False)
AnonymousHostname	Host name provided for anonymous dialog.	@anonymous.invalid
AnonymousUserName	User name provided for anonymous dialing	anonymous
BusyTones	Indicates what will be played as the busy tone. Syntax is hz:ms,hz:ms where hz indicates the hertz level (use 0 for silence) and ms is the duration of the tone in milliseconds.	425:250,0:250
CiscoLinestateReportEstablishedDelay	When busy is received Cisco in the SIP NOTIFY, this indicates how long to wait for the same event to be signaled through the SIP INVITE before displaying Agent busy for a private call.	500 (msec)
ClearFailedDelay	If an outbound call fails to be made from Agent, indicates how long to play busy tone before clearing the call.	5 (seconds)
ClearWholeCallIfAgentPhoneDiverted	If a call is being a deflected to an agent and it is further diverted to a disallowed destination, this indicates whether the inbound caller should be terminated.	1 (True)
ClearWholeCallIfAgentPhoneDiverted_FaultToneDelay	If a call is cleared while being diverted, indicates how long to play a fault tone for the caller before clearing the call.	7 (seconds)
ConferenceLocalized	By default “Conference” is the text displayed for a conference call. If another text string is preferred, it can be entered in this registry value.	Empty string
ConnectionTimeToLiveSeconds	Indicates how long to keep idle SIP-TCP connections.	
CPUAcceptLimit	When the machine CPU usage reaches the defined percent TAS will refuse to accept new sessions.	95
DeflectWaitForRemoteUserChange	If the deflect target is already in the call when the Deflect request is received, it is assumed that a remote-user-change operation is in progress, so TAS will wait for that to complete. This indicates how long to wait for that to complete. If the deflect target remains in the call after this duration, the Deflect	3 (seconds)

	request will fail.	
DelayAfterTransferBeforeReferRelaces	When transferring, TAS first establishes direct media between the two parties, and then it requests REFER + replaces. This value indicates how long TAS will wait after the re-INVITE before sending REFER, which gives time for the call manager to complete any internal operations.	640 (msec)
DeviceStateCacheTTL	Indicates how long to maintain terminated calls in the cache before clearing them.	30 (seconds)
DisplayAnonymousNumbersAs	Refer to ReWriteAnonymousFromTas	anonymous
DisplayPrivateNumbersAs	Display string for numbers listed as private.	Empty string
DivByPassSMP	When calling out to a hard phone on the MX-One, indicates whether diversion bypass should be used to ignore forwarding of the phone.	0 (False)
DivertFailClearTargetDelay	Wait time before reporting Connection Cleared event to client after a failed divert.	1000 (msec)
DivertFailFaultToneDelay	Wait time before playing fault tone (tre-klang/reorder tone) after a divert failure.	200 (msec)
DivertFailTerminateAfter	If deflection of a non-TAS caller fails, indicates how long to wait before terminating the call.	5400 (msec) Set to 0 to avoid terminating the call.
DnsLookupFrequencySeconds	Set to avoid re-running failed DNS queries too often.	270 (seconds)
DnsRefresh	Indicates how often DNS cache is refreshed	300 (seconds)
DumpTransactionsSeconds	Indicates how often ongoing SIP transactions are logged	15 (seconds)
EarlyMediaForSoftphone	Indicates whether softphone should have early media played, when the call manager supports early media. If this is set to 0 (False), then the Agent will only hear the locally generated ringback tones, regardless of what is sent by the network.	1 (True)
EdgeNodePingInterval	Indicates how often a keep-alive signal is sent to Telepo Edge nodes	Same as the PingInterval setting
EnsureHostpartNotIntraForHeaders	When sending requests from the TAS Core via Proxy to a destination outside of TAS, indicates which headers should have the host-part rewritten to match the TAS external	P-Asserted-Identity, Remote-User, Remote-Party-ID, Contact

	hostname	
FailedReferLeavesTrombone	If TAS fails to transfer the call with REFER + replaces, indicates whether the call should remain trombone, which consumes 2 SIP sessions in the call manager.	1 (True)
FailTimeout	Amount of time before a failed call times out and is cleared.	30 (seconds)
FaultTones	Indicates what will be played as the failure/fault tone. Syntax is hz:ms,hz:ms where hz indicates the hertz level (use 0 for silence) and ms is the duration of the tone in milliseconds.	950:333:-17,0:30,1400:330:-17,0:30,1800:330:-17,0:1000
GraceFailSafeCallCleared	Indicates how long to wait before clearing a call from the internal storage in TAS after all connections on a call have been cleared.	1500 (msec)
HashStarHashMeaning	To support Attendant Agent Transfer to Voice Mail, set this value to Diversion. This allows TAS to divert calls to the voice mail system with the proper SIP header so that the call is sent to the user's mailbox.	Empty
HoldIsSendOnly	Determines whether hold sends a=sendonly or a=inactive in the SDP when a call is placed on hold.	1 (True)
HoldOtherSessions	When call is placed on hold, indicates whether other sessions should be held as well	1 (True)
HTTP Allow	TAS normally answers HTTP requests to port 5060 with a statistics page. Set to 0 to disable this.	1 (True)
IfCstaClientDown_StopAllMonitors	If the connected WCF client (i.e. MiCC-E Call Control Service) sets SystemStatus of TAS to disabled, indicates whether all ongoing monitors should be stopped automatically.	0 (False)
IfCstaClientDown_ReferQueuedCallsToPbxCode	If the connected WCF client (i.e. MiCC-E Call Control Service) sets SystemStatus of TAS to disabled, indicates whether TAS should REFER all calls back to the BVD number so the call manager can handle them.	1 (True)
IfCstaClientDown_PbxCode	If the connected WCF client (i.e. MiCC-E Call Control Service) sets SystemStatus of TAS to disabled, indicates the reason code TAS will use to reject incoming calls.	503
IgnoreNumberChangePrefix	When the remote user is changed, indicates the number of ending digits that are significant when determining if the change is	0 (compare entire number)

	relevant. For example, if this value is set to 9, +46856867000 and 000856867000 will be considered as the same number since the last 9 digits are the same.	
IgnoreNumberPrivacy	Set to force TAS to ignore any privacy requests in received SIP messages and display the number information to agents.	0 (False)
IgnoreOutgoingNumberChange	Set to disable remote number changes from being handled so that the number change will not be passed on to agents.	0 (False)
IgnoreUserChangesInResponse	If the remote-user changes in some response codes are unreliable (such as for 183), specify a comma separated list of response codes for which to ignore changes.	Empty
IncludePAIatDeflect	When deflecting a call, indicates whether the local number should be included in the P-Asserted-Identity field. This is used for billing by some customers.	0 (False)
InformPeerMaxDelay	Indicates how long TAS will wait for a response when sending SIP INFO to a peer.	4500 (msec)
Initial180Delay	When receiving an incoming INVITE, indicates how long TAS should wait before sending 180 Ringing.	0 (msec, indicates send immediately without delay)
InitialPingGrace	At startup, TAS will assume all call managers and media servers are up for the configured period of time, allowing time for initial communication. After this time period, the call managers and media servers will be considered as down if no communication has been received and an Event Viewer message will be generated.	30 (seconds)
InterTas_DontAnswerFromAgentPeer	When TAS receives an inter-TAS call originating from an agent, this indicates whether the receiving TAS should wait for the target number to answer and not answer the call immediately.	1 (True)
InterTasReservationTimeout	For Telepo systems, an inter-tas-number-pool is used and freed once TAS is done using it. This setting indicates how long to wait before freeing the number if something fails.	12 (seconds)
InviteTimeout	If outgoing INVITEs don't receive a final response within this timeout period, the call is cleared.	185 (seconds)

LateResponsesInterpretAsReject	This indicates for which SIP/Q.850 codes TAS should treat the calls as rejected.	486, 21, 29
LateResponsesInterpretAsReject Timeout	If a called party rejects the call, TAS expects to receive a 603 Declined message, but in some cases a 486 Busy is received. If a response is received after the time configured in this value, TAS will treat the call as rejected.	1500 (msec)
LinestateEventMaxWaitMs		5000 (msec)
LinestateIgnoreEmptyNotifies		0 (False)
LoadBalancing	In the case of multiple PBX nodes, indicates the method TAS will use for load balancing: firstWorking, random, roundRobin, dns_srv	firstWorking
LogDnsFailureToEventViewer		1 (True)
LSSUser	Indicates the user name for line state SUBSCRIBE messages	TAS-LSS-client
MaxLogSameEvent	Set this value to avoid logging the same message to the Windows Event Viewer after the configured number of times.	0 (no limit)
MaxPendingCalls	Max number of simultaneous calls before incoming sessions are rejected	500
MaxTimeoutOutboundAlertingMillisec	When making an outbound call, indicates the maximum amount of time to wait for a SIP response of 180 or greater. If a response is not received within the configured time, the call attempt is aborted.	7000 (msec)
MaxTransportLayerQueueTimeMS	This option is used to reject incoming calls when TAS is overloaded. If received TCP packets are not handled within the configured time, TAS will start rejecting new calls/OPTIONS.	7000 (msec)
MaxWaitAbortRequets	This option indicates how long to wait for an abort request of a Media Server command to complete.	730 (msec)
MaxWaitStopPlaying	This option indicates how long to wait for an abort request of a Media Server play to complete.	650 (msec)
MediaServerLoadBalancing	By default, the Media Server to be used for a call is selected in a “round-robin” manner, with TAS cycling through the available Media Servers. Create this registry value and set it to “random” to override this behavior and randomly select a Media Server for a call instead of using the round-robin method.	Empty

MediaServer_OptionsExpires	This option indicates the amount of time to wait for the Media Server to answer a SIP OPTIONS message.	7 (seconds)
MediaServerPingInterval	This indicates how often to send OPTIONS-ping to the Media Server(s).	Uses the value in PingInterval
MediaServerTimeoutMs	Indicates how long to wait for a response from the Media Server to an INVITE request before switching to the next Media Server. Note that the last Media Server will allow longer before timing out.	3 (seconds)
MinSessionExpires	See SessionExpires	90 (seconds)
MxXLinkDisableAnswerSMP	Set to 1 to disable answering calls for agents using hard phones through X-Link. This requires the agent to answer the call with the physical phone.	0 (False)
OptionsFailiuesTreatedAsAlive	When sending SIP OPTIONS to a server, it should respond with 200 OK. In some cases, an error is received indicating that the server doesn't support OPTIONS. If any of the configured errors are received, the server is considered as alive.	403, 404, 405, 501
PbxSupport302	If the Call Manager supports 302 Moved Temporarily, TAS can use that option when deflecting unanswered calls.	0 (False)
PbxSupportReferReplaces	For an unknown call manager, indicates whether sending Refer with Replaces is supported. By default, this is supported for Cisco, MX-ONE and Telepo call managers, but can be overridden with this registry value.	1 (True)
PingInterval	How often to send OPTIONS message to call manager nodes/Media Servers as a keep-alive	60 (seconds)
PrivacyUser_SetPAI	If TAS rewrites the From field due to privacy settings, indicates whether the original From value should be sent in the P-Asserted-Identity.	1 (True)
PrivacyValue	When privacy is requested for an outbound call, this setting indicates which SIP level of privacy will be used. Set to one of the following values: none history user id	id

	header session critical	
ProxyRewriteUnknownCstIdAsDiversion	If the call is diverted from an external number to a BVD on an MX-ONE system, the original diverted-from number can be obtained in the Last Redirection Device field of the Delivered and Established events by setting this option to 1.	0 (False)
ReferFailed404_RetrySwapped	If a transfer using REFER+replaces fails from A to B, indicates whether TAS should retry transferring B to A.	1 (True)
ReferFailedWaitBeforeRetrySwapped	If a retry is attempted, indicates how long to wait before sending the retry REFER+replaces.	95 (msec)
ReferReplaceDiverted	When diverting a call from an external number to another external number, REFER + replaces occurs after call completion.	1 (True)
ReferReplaceDiverted_WaitBefore	Indicates how long to wait before REFER + replaces is sent to allow re-INVITEs from the remote party to complete.	450 (msec)
ReferReplacesTimeout	Max time allowed for a REFER + replaces to complete	3 (seconds)
RegistrarMaxExpires	This is the maximum value TAS will allow for the expires field when a softphone registers. It can be used to force the softphone to register more frequently.	600 (seconds)
RegistrarMinExpires	This is the minimum value TAS will allow for the expires field when a softphone registers. It can be used to prevent the softphone from registering too frequently.	60 (seconds)
RemoveSensitiveDataFromTrace	Indicates whether sensitive data such as DTMF digits is removed from the trace log file or traced normally.	0 (False)
ReplaceCallingNumberWithOriginallyCalledNumber	Set to override the calling number with the originally called number instead of the BVD number when the option "Replace Calling Number with Called Number for Service Group Calls" is set in the Phone Agent tab of the Tenant System Properties of MiCC Enterprise. Instead of replacing the ANI with the BVD number, TAS will replace the ANI with the originally called number. This is useful when the customer calls a number which is diverted to the BVD.	0 (False)
ReportAllXLinkTransferred	Set to False to ignore all XLink Transferred	1 (True)

	events.	
ReportRemoteUserChangeAs	When the remote user changes on SIP, this must be reported as a CSTA Diverted or Transferred event. Normally, TAS will select the best option based on the change, but it is possible to force one of the events to always be used as follows: Deduce = 0 Use Diverted event = 1 Use Transferred event = 2	0 (deduce)
RequirePrackInterTas	When TAS receives an inter-TAS call from the call manager, it is expected to receive a PRACK on the 180 Ringing. Set this to 0 (False) to not require a PRACK.	1 (True)
ReWriteAnonymousFromTas	When privacy is requested, indicates whether TAS should change the From header to the string in the registry value "DisplayAnonymousNumbersAs" (which defaults to anonymous). If this option is set to 0 (False), the From header is unchanged but the Privacy-header will indicate privacy.	1 (True)
RingbackTones	Indicates what will be played as the ringback tone. Syntax is hz:ms,hz:ms where hz indicates the hertz level (use 0 for silence) and ms is the duration of the tone in milliseconds.	440:990,0:4710
RingbackWhenDeflecting	Indicates whether ring back tone should be played while a call is being diverted to another destination	1 (True)
RingbackWhenEarlyTransfer	If a consultation call is transferred when the target is early (i.e. not answered), this setting indicates whether the ringback tone should being to be played to the consultation call.	1 (True)
SessionExpires	TAS suggestion for Session-Expires value.	1800 (seconds)
SessionMaxWaitForAckWhenTerminate	If a non-established SIP session is terminated, indicates how long to wait for an ACK before sending BYE and terminating the internal session object	10 (seconds)
SessionRefresher	Indicates whether TAS or the call manager should be responsible for refreshing SIP sessions that are long duration calls. TAS refreshes = local PBX refreshes = remote Caller refreshes = uac Called party refreshes = uas	local

SetDivHeaderOnDivertToExternal	When a call is diverted to a non-TAS number (i.e. not a BVD or Agent), this setting indicates whether information should be added indicating from which device (Agent) the call was diverted.	0 (False), since this avoids revealing agents' numbers
SetUserEqualsPhone	When making outbound calls, indicates whether the From header should contain user=phone	0 (False)
ShowRemoteUserInTransfer	When agent transfers caller A to party B, indicates whether B should view A's number	1 (True)
SipCred	Credentials for Telepo-SUBSCRIBE. This is set via TAS Configuration application.	
SipFailiures	Indicates which Nuance SIP failure responses will be considered as indicating that the Nuance server is alive.	403, 404, 405, 501
SipGlobalFinalCauses	When TAS has several PBX nodes, this indicates which responses will cause TAS to abort the call attempt. Otherwise, TAS will attempt to use the next node to make the call.	400, 404, 410, 486, 488, 603
SmpMaxWaitForCall	Number of milliseconds to wait for a call to a hard phone agent's extension number to be answered after requesting to answer the call.	1500 (msec)
SnapshotMaxWait	When an MX-One hardphone agent logs in, a Snapshot request is made via XLink to find out if there are any existing calls. This indicates the maximum wait time for the response, since this is a blocking call.	2000 (msec)
StopMonitorWhenUnRegister	Indicates whether the agent monitor will be stopped automatically when the SIP softphone unregisters.	0 (False)
SubscribeExpires	Indicates the length of the expires time for Peer subscriptions.	300 (seconds)
SupportPRACK	By default, TAS considers PRACK to be supported. It can be disabled by setting this value to 'none' or forced to be supported by setting this value to 'required'.	supported
TcpConnectTimeout	Max time to wait for the TCP connection to be established toward the call manager or Media Server	3200 (msec)
TelepoAPISecret	This is set by the TAS Configuration application.	Empty string
TelepoAPIToken	This is set by the TAS Configuration application.	Empty string

TimeBeforeSending100Trying	Normally TAS doesn't send 100 Trying immediately after receiving a request. If no other response has been sent within the timeout configured, 100 Trying will be sent. This can be changed to force TAS to always send 100 Trying by setting the value to 0, or to never send 100 Trying by setting the value to a high number.	250 (msec)
TlsFQDN	Value to use as the local FQDN for TLS	Hostname.<name of Windows domain>
TraceCurrentCallsFreqSeconds	Configures how frequently to log the trace of ongoing calls.	60 (seconds)
TransactionAddResendCound	When TAS resends a SIP request, it adds the header X-TAS-Resend-Count. To disable this, set this value to 0.	1 (True)
TreatAs180	Indicates which SIP responses should be treated the same as a 180 Ringing.	180, 182
TrunkGroup	For outbound calls, if this value is set, the tgrp parameter in the request URI will be set to the configured value.	Empty string
UserUpdateHeader	When TAS transfers a call, it sends a SIP UPDATE to indicate that the remote user has changed. This indicates which SIP header will contain the updated value.	P-Asserted-Identity
WaitAfterAnswerBeforeRefer	If TAS is answering in order to REFER a call (such as when a Deflect request is made before the call is answered), this value indicates how long TAS will wait between the ACK and the REFER in order to allow any re-INVITE to occur.	800 (msec)
WaitAfterFailBeforeClear	If a call enters Failed state, such as after a deflect to an external number, this indicates how long to play fault tones before clearing the call.	4000 (msec)
WaitBeforeClearingOnphanCalls	When an agent hangs up on a call, indicates how long to wait before clearing the orphaned call.	5000 (msec)
WaitForAllConnectionsBeforeReportUserChange	TAS may have connections not yet reported to the MiCC-E core yet. For example, when an outgoing SIP INVITE has been sent, but 180 Ringing has not yet been received. If a remote-user change occurs before the 180 Ringing, this setting indicates how long to wait for the 180 Ringing before reporting the remote user change.	2400 (msec)

XLinkDelayBeforeReportDiverted	When a Diverted event is received from XLink, this value indicates how long to wait for the same event to be signalled via SIP first.	0 (msec)
XLinkDelayBeforeReportTransfer	When a Transferred event is received from XLink, this value indicates how long to wait for the same event to be signalled via SIP first.	200 (msec)
X_Mxone_Endpoint_Disabled	Indicates whether the SIP header X-Mxone-Endpoint should be ignored when detecting the remote user name	0 (False)