# Mitel MiContact Center Enterprise

TAS INTEGRATION – INSTALLATION INSTRUCTIONS RELEASE 9.5



#### NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks<sup>™</sup> Corporation (MITEL<sup>®</sup>). 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.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

#### TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

MiContact Center Enterprise TAS Integration – Installation Instructions Release 9.5 – September 2020

> ®,™ Trademark of Mitel Networks Corporation
>  © Copyright 2020 Mitel Networks Corporation All rights reserved

# 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.

🖏 Services						_	
File Action View	Help						
	à 📑 🛛 📰 🕨 💷 🕕 🕨						
🤹 Services (Local)	🖏 Services (Local)						
	Microsoft .NET Framework NGEN	Name 🔺	Description	Status	Startup Type	Log On As	<b></b>
	v4.0.30319_X64	Microsoft iSCSI Initiator Se	Manages Internet SCSI (iSCSI) sessions fro		Manual	Local System	
	Chard the sure for	🍓 Microsoft Software Shado	Manages software-based volume shadow c		Manual	Local System	
	Start the service	Mitel Enternrise License Ma	Administers licenses for Mitel applications	Started	Automatic	Local System	
		🏩 Mitel MediaServer	Mitel SIP Based Media Server	Started	Automatic	Local System	
	Description:	Мисстон налитостисс	Hammiscrator of Application Services, and Services	Juanceu	Automatic	Local System	
	MICrosoft INET Framework NGEN	Mitel SM Configuration Ser	SM Configuration Service	Started	Automatic	Local System	
		Mitel SM Logging Service	Logging service for ScriptManager	Started	Automatic	Local System	
	-	O Mitol SM Likiliku Sovuico	CMI IFIIFU Consido	Started	Automatic	Local System	
		Altel Tas	Mitel Telephony Application Service	Started	Automatic	Local System	
		Multimedia Class Scheduler	Enables relative prioritization or work based	Started	Manual	Local System	
		🏩 Net. Msmq Listener Adapter	Receives activation requests over the net		Disabled	Network S	
		🏩 Net.Pipe Listener Adapter	Receives activation requests over the net.p		Disabled	Local Service	
		🏩 Net. Tcp Listener Adapter	Receives activation requests over the net.t		Disabled	Local Service	
		Net. Tcp Port Sharing Service	Provides ability to share TCP ports over the		Disabled	Local Service	
		Sector Netlogon	Maintains a secure channel between this co	Started	Automatic	Local System	-
	Extended Standard						

## 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.

2

ocal Media Server Properties		PBX Routes
IP Address and Port Dialog TTL 5065 10 minutes TP Port Range 10000 - 50000 RTCP	TAS Installed Version:       9.4.151.0         SIP Listening Port       CSTA3 Listening Port         5060       8732         Hold behavior       Music on Hold         Ignore SIP Number Privacy       Allow inter tenant calls	Address Port 10.70.128.190 5060
IOH File C:\Program Files (x86)\Mitel\MediaServer\ringing.wav	CSTA CallID Range 0-399999  C:\temp  C.\temp	Remove Add
Trim Recordings Forward DTMF into conferences	Inter-TAS transfer numbers	Load balance strategy Round Robin ~
Vuldio Files Prefix     valdio Files Prefix       C:\Program Files (x86)\Mtel\MediaServer\       SRTP SDP Offer     Default Recording Rate       SRTP Best Effort     8 kHz       Is RTP Best Effort     16 kHz	PBX Osco V Publisher AXL poll interval (s) 60 \$ throtting per min 60 \$ Set AXL credentials	Address Port
Log Path C: Program Files (x86)\Mtel\MediaServer\Logs  Log Level Delete older than (days) (3) Trace  10  0     Max size (MB) 0	Log Path C:Vogs Log Level Delete older than (days) Max size (MB) [9] Debug+5 V 14 512 V Running Version: 9.4.151.0 Running Version: 9.4.151.0	Remove         Add           Media Servers         Address           Address         Port           10.70.128.60         5065
ervice Status: Running Stop	Service Status: Running Stop	Remove Add

**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.

Call Delivered OnCallDeliver As	Var=       Assign       sign001       → <th>Log Message</th> <th>Play001</th> <th>y</th> <th>ClearCall</th>	Log Message	Play001	y	ClearCall
AllocateResoSe	tDefaultCo SetDefaultCo General Se	ntainerPath Properties Itings Branches		×	
	Default C	ontainer Path: usenglish			Play Play
SetResu					
¢	Open onnection Statemen	OK Cance	Apply	Help	
Op	en Prepare00 innection001		Executeool	Connection001	

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

📙 UsEnglish		_ 🗆 ×
🕞 🕞 🗸 🕨 🗸 Comput r 🔹 Local Disk (C:) 🔹 Voice 🔹 system 👻 UsEnglish	👻 🌆 Search UsEnglish	2
Organize ▼ Indude in library ▼ Share with ▼ Burn New folder	8==	- 🗌 🔞
🕑 🖬 Videos	▲ Name ^	<u> </u>
Computer Com	<ul> <li>≓sign.wav</li> <li>0.mov</li> <li>0.wav</li> <li>1.mov</li> <li>1.wav</li> <li>1e3.mov</li> <li>1e3.wav</li> <li>1e6.mov</li> </ul>	

TAS and Media Server configuration data location

File Edit view Favorites Help			
⊡-1 <sup>1</sup> Computer	Name	Туре	Data
E	ab (Default)	REG_SZ	(value not set)
E HKEY_CURRENT_USER	ab CallManagerType	REG_SZ	MXOne
	8 CSTA3Port	REG_DWORD	0x0000221c (8732)
ECD00000000	ab CSTACallIDRange	REG SZ	0-99999
🗄 🤚 HARDWARE	ab CurrentVersion	REG SZ	9.3.0092.0
🗄 🚽 SAM	RailTimeout	REG DWORD	0x0000001e (30)
SECURITY	TocludePATatDeflect	REG DWORD	0×00000000 (0)
SOFTWARE	ab InstallDir	REG SZ	C:\Program Files (x86)\Mitel\Tas\
	BLogDiscardAfter	REG DWORD	0×00000005 (5)
	ind evel	REG DWORD	0×00000007 (7)
	100 LogMaxSize	REG DWORD	0×00000200 (512)
	ab LogPath	REG_S7	Cillions
	ab MediaServer1	DEC S7	10 70 128 81 5065
	MediaServerālwa	REG DWORD	0x00000001 (1)
	MyYLinkPort	PEG DWORD	0×000022b3 (8883)
Wow6432Node	MyYLinkTLS	PEG_DWORD	0×000002285 (0005)
Aastra	MyYLinkValidateC	REG_DWORD	0×00000001(1)
Mediaserver	ab DRVD outo1	REG_DWORD	10 70 128 100/E040
H-	ab DecordingDath	REG_DZ	Cultarra
	Recordingradi	REG_32	C:(Cemp 0~000013-4 (E060)
E Clients	TI SConverContifie	REG_DWORD	0200001304 (3060)
🕀 📲 Description	ab TicSupport	REG_52	Beguired
🕀 🔒 Ericsson	20 HastakCallTD	REG_32	
庄 🔒 Google		REG_DWORD	0x0000000 (0)
庄 📲 Microsoft			
🖻 🌗 Mitel			
E SeC			
i <u>B</u>			
Tas			
🕀 🕌 MozillaPlugins			
Plantronics			
. Policies			
RegisteredApplications			
J	1		
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mitel\Tas			

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-inprogress. 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.

Earc view ravorices ricip			
Computer	Name	Туре	Data
HKEY_CLASSES_ROOT	ab (Default)	REG_SZ	(value not set)
HKEY_CURRENT_USER	ab AudioFilesPrefix	REG_SZ	C:\voice\system\
HKEY_LOCAL_MACHINE	ab CodecPreference	REG_SZ	pcma,pcmu,g722,g729,rfc2833
ECD0000000	ab CurrentVersion	REG_SZ	1.8.26.0
HARDWARE	DaysToKeepLogs	REG_DWORD	0x0000000a (10)
E SAM	DialogTTL	REG_DWORD	0x0000000a (10)
SECURITY	DTMFdemodulation	REG_DWORD	0x00000001 (1)
	nableRTCP	REG_DWORD	0x00000000 (0)
H Glasse	10 firstRTPport	REG DWORD	0x00009c40 (40000)
Classes	ab InstallDir	REG SZ	C: Program Files (x86) Mitel MediaServer
E Description	10 lastRTPport	REG DWORD	0x0000c350 (50000)
E Microsoft		REG DWORD	0x00000007 (7)
HIG GLOTE MozillaPlugins	abLogPath	REG SZ	C: \Program Files (x86) Witel WediaServer Logs
THE ODBC	10 MaxLogSize	REG DWORD	0x00000000 (0)
F Policies	ab MOHFile	REG SZ	C: Program Files (x86) Witel WediaServer Vringing.w
RegisteredApplications	ab PacketSize	REG SZ	20
	ab Path	REG SZ	C:\Program Files (x86)\Mitel\MediaServer\
🗄 🔟 VMware, Inc.	ab Port	BEG SZ	:5065
	100 RecordingRate	REG DWORD	0x00000010 (16)
🖃 🛄 Wow6432Node	118 SRTPBestEffort	REG DWORD	0x0000001(1)
🖻 🍌 Aastra	SRTPSDPOffer	REG DWORD	
Mediaserver	200 VADrecordings	REG DWORD	0x00000001(1)
🗄 🌙 Adobe	leg moneconaligs	120_011010	0,0000001 (1)
Apache Software Foundation			
🗄 🦺 Business Objects			
🕀 🦺 Clients			
Ericsson			
Et Google			
Javason			
Microsoft			
	<b>T</b>		

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. : <i>port</i> for the default Ethernet interface, <i><interface>:port</interface></i> 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.	<installdir>\Ringing.wav</installdir>
Trim Recordings	Indicates whether the media server should remove	Checked

	trailing silence from recordings	
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</installdir>
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 at default and a new log is opened each day	0
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 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).	Unchecked
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, as 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 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
РВХ	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: Modify PBX route FQDN or IP Address Twone seclab com Port 5065 S SRV record Remove Ok Cancel 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></port></ip>
TAS peers	The FQDN or IP address of other TAS servers in a multi-TAS system	<ip address="">:<port></port></ip>
Media Servers	The FQDN or IP address and port of the Media Server host.	<ip address="">:<port></port></ip>

# 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.

🗐 Local Group Policy Editor										_ 🗆 🗙
File Action View Help										
🗢 🔿 🙎 🔐 🗟 🖬										
Local Computer Policy	Policy Name	Application Name or URL	Protocol	Source Port	Destination	Source IP /	Destination I	DSCP Value	Throttle Rate	
🖻 👰 Computer Configuration	ACS QoS	c:\Program Files(x86)\Mitel\MediaServer\Mediaserver.exe	UDP	•	•	*	*	46	-1	
📧 🚞 Software Settings										
🖃 🚞 Windows Settings										
Image: State Resolution Policy										
Scripts (Startup/Shutdown)										
📧 🚡 Security Settings										
Policy-based QoS										
ACS QoS										
Administrative Templates										
🖃 🕵 User Configuration										
🗉 🧮 Software Settings										
Windows Settings										
🕀 🧮 Administrative Templates										
Local Computer Policy     Congrueter Configuration     Computer Configuration     More Resolution Policy     Mane Resolution Policy     Sorpts (Startup/Shutdown)     Sorpts (Startup/Shutdown)     ACS QoS     ACS QoS     Configuration     Sortware Settings     Software Settings	Policy Name	Application Name or URL c:\program Files(v86) Mtel MediaServer(Mediaserver.exe	Protocol UDP	*	*	*	*	16 Value	Throttle Rate	

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.

Call Manager Server Details Name: Default Serv User Name: SIP Settings Proxy Server: 10.7 Outbound Proxy: Access Codes Conference:	er		Access Codes New Server Delete Server
New Site Delete Site	er Server: VM Password: Password: 0.129.60 Port: 5060 Port: 5060 Transfer: 0	Port: Call Control Server: Security TLS Voice Encryption: Di DTMF Type ( SIP INFO C RFC 2833	8732

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.

Language Proper	ties ×
Name:	US_ENGLISH
Rule File:	us_english.rul
Prompt Path:	\usenglish
TTS Language:	en-us 💌
TTS Voice:	Paulina
Play List:	DefaultList
TTS Gender:	C Male
	OK Cancel Help

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

1

2

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.

CS API Tool log started Thu May 08 10:55:26 201	4	
	NRM Server	2
Server Details will be entered here whether it is OAS or TAS based. For OAS based systems use port 2562 by default and if using this tool on a TAS based system the port will be 8732 by default.	Server Details Server: vm-willtesttas	
	Port#: 8732	
Call Control Service Details are only entered here if the system is TAS based. The port that should be	Call Control Service Details	
	Server: vm-willtesttas	
Setup Utility for the Call Control Service, 2614 by	Port#: 2614	
	User Details	
	User Name:	
	Password:	
	ОК Са	ncel

# 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

cisco	Cisco Unified CM Administration För Cisco Unified Communications-lösningar					
System 💌	Call Routing 🔻 🛛	ledia Resour	ces 🔻	Advanced Features 🔻	Device 🔻	
Server						
Cisco I	Unified CM					
Cisco I	Unified CM Group					
Phone	NTP Reference					
Date/Ti	ime Group			med -		
Presen	ice Group		Jai	meu 🔹		
Region			-			
Device	Pool					
Device	Mobility	•				
DHCP		•				
LDAP		•				
Locatio	n					
Physic	al Location					
SRST						
MLPP		•				
Enterp	rise Parameters					
Enterp	rise Phone Configura	tion				
Servic	e Parameters					
Securi	ty	•	C	Certificate		
Applica	ation Server		P	Phone Security Profile		
Licens	ing	۲	5	SIP Trunk Security Profile		
Geolog	ation Configuration		C	UMA Server Security Profile	N3	
Geolog	ation Filter					

SIP Trunk Security Profile Configuration					
🔚 Save 🗶 Delete 🖺 Copy 資 Reset 🧷 Apply Config 🕂 Add New					
- Status	- Status				
i Status: Ready					
- SIP Trunk Security Profile Informa	tion				
Name*	ACS_Security_profile_TCP				
Description	ACS_Security_profile_TCP				
Device Security Mode	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	Device  Application  User Manageme	nt ▼ Bulk Administration ▼ Helo ▼
System  Call Routing  Media Resources  Advanced Features  Find and List SIP Profiles SIP Profile Sök SIP Profile där Name  Korjar med  Add New	Device       Application       User Manageme         CTI Route Point       Gatekeeper         Gateway       Phone         Trunk       Remote Destination         Device Settings       •	nt   Bulk Administration  Help  Help
		Common Ponie Configuration Common Phone Profile Remote Destination Profile Feature Control Policy Recording Profile SIP Normalization Script

SIP Profile Configuration				
🔚 Save 🗙 Delete 📄 Copy 💁 Rese	t 🧷 Apply Config 🕂	Add New		
- Status (i) Update successful				
(i) All SIP devices using this profile must be	e restarted before any cha	inges will take affect.		
<u> </u>				
- SIP Profile Information Name*	Standard SIP Profile + Re	edirect 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 R	equests			
Assured Services SIP conformance				
SDP Session-level Bandwidth Modifier for Ea	arly Offer and Re-invites*	TIAS and AS		
SDP Transparency Profile		Pass all unknown SDP attributes		
Accept Audio Codec Preferences in Received	d Offer*	Default		
Require SDP Inactive Exchange for Mid-	Call Media Change			
Allow RR/RS bandwidth modifier (RFC 35	556)			
	,			

— Trunk Specific Configuration	
Reroute Incoming Request to new Trunk based on $^{st}$	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 Cal	ler Information
Reject Anonymous Incoming Calls	
Reject Anonymous Outgoing Calls	
Send ILS Learned Destination Route String	

Cisco Unified CM Administration For Cisco Unified Communications Solutions	I			
System ▼ Call Routing ▼ Media Resources ▼ Advanced Features ▼	Dev	vice 🔻	Application -	User Manageme
Find and List Trunks		CTI Ro	ute Point	
Add New		Gateke Gatew	eeper /ay	
Trunks		Phone		
Find Trunks where Device Name		Trunk Remot	e Destination	
Add New		2.57100		

Trunk Configuration		
🔚 Save 🗙 Delete 省 Reset 🕂 Add New		
🖵 Status —		
i 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)	
	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	<b>•</b>
QSIG Variant*	No Changes	
ASN.1 ROSE OID Encoding*	No Changes	
Packet Capture Mode*	None	
Packet Capture Duration	0	

# SIP trunk configuration

Trunk Configuration		
🔚 Save 🗙 Delete 省 Reset 🕂 Add New		
Status Status: Ready		
SIP Trunk Status Service Status: Unknown - OPTIONS Ping not enabled Duration: Unknown		
Device Information	OID Truck	
Product:	SIP Trunk	
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	<b>.</b>
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 >		
Vse Device Pool Called Party Transformation CSS			
Calling Party Transformation CSS	< None >		
Vse 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 Trans	sformation CSS		

Call Routing Inf	ormation	
Remote-Party	-Id	
Asserted-Ide	ntity	
Asserted-Type*	Default	
SIP Privacy*	Default	•

2

**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.

– SIP Information						
Destination						
Destination Address is an SRV						
Destination Address	•	Destination Addres	s IPv6	r	De	stination Port
1* 192.168.166.130					5062	
MTP Preferred Originating Codec*	711ulaw		Ŧ	]		•
BLF Presence Group*	Standard Presence grou	р	-	]		
SIP Trunk Security Profile*	ACS_Security_profile_T	CP	-	j		
Rerouting Calling Search Space	< None >		-	]		
Out-Of-Dialog Refer Calling Search Space	< None >		•	]		
SUBSCRIBE Calling Search Space	< None >		-	]		
SIP Profile*	Standard SIP Profile + F	edirect by application	•	View Details	2	
DTMF Signaling Method*	No Preference		•	]		

2

**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.

Route Pattern Configuration	
Save 🗶 Delete 🗋 Copy 🕂 Add Ne	w
- Status	
(1) Status: Ready	
- Pattern Definition	
Route Pattern*	7XXXX
Route Partition	< None >
Description	SIP_TAS
Numbering Plan	Not Selected 👻
Route Filter	< None > v
MLPP Precedence*	Default 🔹
Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	SIP_TAS 🗸
Route Option	Route this pattern
	Block this pattern No Error

# CONFIGURATION FOR OFFNET TO OFFNET TRANSFERS

rvice Parameter Configuration	
🕽 Save 🧬 Set to Default 🍕 Advanced	
<u>317 1000</u>	100000
321 Timer *	30000
<u>322 Timer</u> *	4000
one on Hold Timer_*	10
Inknown Caller ID Flag *	True
Call Classification *	OffNet T
lways Display Original Dialed Number *	False
ame Display for Original Dialed Number When Translated *	Show the Display Name for Original Dialed Number ev 🔻
ways Use PIs With Original Dialed Number *	False
ail Call If Trusted Relay Point Allocation Fails.*	True
isplay Calling/Called ID When PI is Not Available *	False
nable Transit Counter Processing on QSIG Trunks *	False T
igress FacilityIE Count.*	6

System 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 A	pplication 👻 User Management 👻 Bulk Administration 👻 Help 👻	
Service Parameter Configuration		Related Links
📊 Save 🧬 Set to Default 🔍 Advanced		
There are hidden parameters in this group. Click on Advanced button to see hi	dden parameters.	
Clusterwide Parameters (Feature - General)		
Call Park Display Timer.*	10	10
Caller ID Display Priority Enabled *	True	True
Call Park Reversion Timer *	60	60
Park Monitoring Reversion Timer *	60	60
Park Monitoring Periodic Reversion Timer.*	30	30
Park Monitoring Forward No Retrieve Timer *	300	300
Preserve globalCallId for Parked Calls *	True	True
Maximum Call Duration Timer_*	720	720
Maximum Hold Duration Timer *	360	360
Party Entrance Tone *	True	True
Message Waiting Lamp Policy *	Primary Line - Light and Prompt	Primary Line - Light and Prompt
Audible Message Waiting Indication Policy *	OFF	OFF
Message Waiting Indicator Inbound Calling Search Space	< None >	
Multiple Tenant MWI Modes *	False	False
MWI Non Message Center Signaling Call Duration *	0	0
Message Waiting Indicator APDU Digit Translation CSS	< None >	
Block OffNet To OffNet Transfer.*	False	False
Use Original Call Classification for Transferred Calls *	False	False
Use Restriction attribute of ID/Name Presentation of Transferring Party.*	True	True
Local route group for redirected calls *	Local route group of calling party	Local route group of calling party
Block Unencrypted Calls *	False	False

### 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.
## TAS Integration – Installation Instructions

ervice Parameter Configuration		Bx https://10	70 128 221/ccmadmin/venc	lorConfigHelp.do?url=xmld
Save 🧬 Set to Default 🍳 Advanced	15-1	Maximum T Bandwidth U	his parameter specifies the durati nified Communications Manager u	on in minutes that Cisco uses as the maximum duration
Mobile Voice Access Number	False	Deduction of Duration: * d	a bandwidth deduction. After this eduction is restored regardless of	s duration, a bandwidth the call progress associated
Matching Caller ID with Remote Destination *	Complete Match		ith the bandwidth. This service pa cover deducted bandwidths for c	arameter can be used to alls that may no longer exist. A
Number of Digits for Caller ID Partial Match *	10	vi T	alue of 0 specifies no maximum d	luration.
System Remote Access Blocked Numbers		D D	efault: 720	
Enable Use of Called Party Transformed Number for Mobile-terminated Calls *	Falce	м	inimum: 0	
Honor Gateway or Trunk Outbound Calling Party Selection for Mobile Connect Calls *	False	_	avimum, 26000	
	1000		Ensure that the values of Maximu uration service parameter and Ma	im Bandwidth Deduction aximum Call Duration Timer
Clusterwide Parameters (System - Mobility Single Number Reach Voicemail) ———		s	ervice parameter are the same.	
Single Number Reach Voicemail Policy_*	Timer Control	- U	nit: min	
Dial-via-Office Reverse Voicemail Policy.*	Timer Control	Treatment M	anager allows or rejects calls whe	en there is no Cisco Location
User Control Delayed Announcement Timer *	1000	When No B	andwidth Manager available for lo ontrol.	ocation-based call admisson
User Control Confirmed Answer Indication Timer *	10000	Available: *	nic is a required field	
Clusterwide Parameters (Feature - Reroute Remote Destination Calls to Enterprise	Number)	D	efault: Allow Calls	
Reroute Remote Destination Calls to Enterprise Number *	False	Locations T	his parameter determines the bit udio bandwidth pools within and b	rate value to deduct from the
Ring All Shared Lines.*	False	Resource p	arties for an audio-only call when	a Media Resource such as a
Ignore Call Forward All on Enterprise DN.*	True	Rate Policy: co	anscoder is inserted into the med omplex scenarios. When an audio	call is transcoded there is
Clusterwide Parameters (Feature - Immediate Divert)			e transcoder is connecting. For e	xample a transcoded audio call
Use Legacy Immediate Divert *	True	24	4kbps bit rate while the G.711 me	dia leg occupies an 80kbps bit
Allow OSIG during iDivert *	Falce	ra	ite. Similarly, when inter-working sed on the IPv4 media leg will be	IPv4 and IPv6 the bit rate less than that of the IPv6
Immediate Divert User Response Timer.*	5		edia len for the same audio code	c. There are more complex
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
JCM to LBM Periodic Reservation Refresh Timer *	5			5
Aximum Bandwidth Deduction Duration *	0			720
Call Transformer Million Ma L DM Association				Allen Celle
Jan freathent when no Lom Avanable	Allow Calls		•	Allow Calls

# 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.

— Remote Destination Information		
Name	RD_85953	
Destination Number*	+46707389588	
Owner User ID*	gbgs_MEX_03	~
Enable Unified Mobility features		
Remote Destination Profile*	RDP_85953	$\checkmark$
Single Number Reach Voicemail Policy*	Använd systemstandard	✓
<ul> <li>Enable Single Number Reach Ring this phone and my business phone at the s</li> <li>Enable Move to Mobile If this is a mobile phone, transfer active calls to</li> <li>Enable Extend and Connect Allow this phone to be controlled by CTI applications CTI Remote Device*</li> </ul>	same time when my business line(s) is dialed. this phone when the mobility button on your Cisco IP (e.g. Jabber) Not Selected	Phone is pressed.
Timer Information         Wait* 0.3       seconds before ringing this phone when         Prevent this call from going straight to this phone's voice         Stop ringing this phone after* 28.0	my business line is dialed.* email by using a time delay of* 3.0 seconds to de d connecting to this phone's voicemail.*	tect when calls go straight to voicemail.*

# **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).

$\leftarrow \rightarrow$	C 🗋 10.	105.60.1	<b>0</b> /manag	ement								\$	≡
Node:			•	Organization:						Management r	node	Help   Lo	gout
	Mitel									search			1
										🚹 You have 3 al:	arms	System vie	w
Home	Management	Reseller	System	Superuser admin	Devices					Logged in	as adn	nin Logou	t
Home			System st	tatus								He	lp
About My Pro Syster	file n status	•	Current a Service n Feb 5, 20 Cease Phone n	larms node instance not 16 11:43:52 AM - 9 umber active in m	alive Service nod ultiple or	le sn3 with instanc ganizations	ce 1 cann	ot be access	ed from	edge nodes (S	ystem)	)	

# 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.

Teleno Extensions	
relepo Extensions	
Allow Call Intrusion	
Allow Diversion	
bypass	
PBX integration	
Forward Subject SIP	
Allow cell to co	
Allow call tags	
RTP media flow	
0 -	
I ranscoded in n	hedia server
Relayed with fix	ed codecs using Media Relay Server
Relayed with all	codecs using Media Relay Server
End-to-end	
end to end	
-Destination address-	
Configures how to cor	nonunicate with the remote side of the SIP trunk
configures now to con	Innunicate with the remote side of the SIP trunk.
Ilse hasis settings	O lise advanced settings
<ul> <li>Ose basic settings</li> </ul>	o use auvanced setungs
Host	10.105.72.102
Port	*
-	30/2
Transport	
Use basic settings     IP network     10.105.72.102     Caller line identific	Use advanced settings
Configure how the	caller should identify itself against the SIP trunk.
Use short number	in 🛄
From	
Insert Remote-	
Party-ID	
Insert P-Asserted-	
Identity	
P-Accerted-Identit	N Nego
override	y None
Number format of	charging number and billing id may be rewritten using outbound
diversion rewrites	in trunk aroun configuration. If no diversion rewrite rules exist calling
uiversion rewrites	in dank group comparation. If no unversion rewrite rules exist, caming
party rewrite rules	are used.
Enmah al the D	
Format of the P-	I SIP URI
Asserted-Identity	TEL URI
	The only

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**.

Name	Туре	
MiCC Enterprise	Destination V Add	
Apply		

- **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.

Devices	Trunk groups	
Media relay	Description Solidus TrunkGroup	
Media servers	State Enabled ▼*	
▶ SIP phones	Base trunk group None 🔻	
SIP trunks	Save trunk group Cancel	
Softphones		
Speech servers		
Trunk groups		

- 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.

Trunk group settin	gs
Id	33
Description	Solidus_TrunkGroup
State	Enabled V *
Stop hunting at match	< ← ← ← ← ← ← ← ← ← ← ← ← ← ← ← ← ← ← ←
Break out on next trunk for response codes	408, 5xx *

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.

Outbound
Number matching
Calling party number ranges
Range
New number range
Require existence of
calling party number
within calling party number range
Expression matching
isDstTagged("solidus1")

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

Port connections		
Sip Trunk	Connected	Allocated by trunk group?
ASR_01_Lab		4
Call Guide SipTrunk		6
Cisco_2811		11
Snfailovertest		34
Solidus	Image:	-
Solidus2		29
T2a SipTrunk		1
T2b Siptrunk		1
callgude_touchpoint+		24
larstest		5
loadtest_trunk		31
mahanth_blr_tempbcs	s 📃	37
Save Cancel		

6. Click Save to apply your changes.

Configure trunk group rewrites

TAS does not support E.164 numbers. Since it preferable to use shorter numbers, you can use the Trunk Group Rewrites function to ensure that the correct numbers are 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.

ules are applied to the	e called number	for inbound o	alls.				
Followed by	Limit to range	Rewrite pre.	No. plan	No. type	Add tags	Mobile VPN	
Any number of digits		+468408375	Any	Any			$\times$
	ules are applied to the Followed by Any number of digits	ules are applied to the called number Followed by Limit to range Any number of digits	ules are applied to the called number for inbound of Followed by Limit to range Rewrite pre. Any number of digits +468408375	ules are applied to the called number for inbound calls. Followed by Limit to range Rewrite pre. No. plan Any number of digits +468408375 Any	ules are applied to the called number for inbound calls. Followed by Limit to range Rewrite pre. No. plan No. type Any number of digits +468408375 Any Any	ules are applied to the called number for inbound calls. Followed by Limit to range Rewrite pre. No. plan No. type Add tags Any number of digits +468408375 Any Any	ules are applied to the called number for inbound calls. Followed by Limit to range Rewrite pre. No. plan No. type Add tags Mobile VPN Any number of digits +468408375 Any Any

• 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".

🔶 In	bound calling party re-	writes						
These r	rules are applied to the	e caller's own n	umber for inbo	ound calls				
Prefix	Followed by	Limit to range	Rewrite pre.	No. plan	No. type	Add tags	Mobile VPN	1
375	Any number of digits		+468408375	Any	Any			×
88	Any number of digits		+9876588	Any	Any			×
New	-							
New ru	le							

• 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.

Home Services Support	Organization	User administration	Function numbers	Devices
Organization	Organizatio	n Wizard		
Barring groups	Show Wizard	ł		
Calendar connectors				
Device locations				
Languages				
License usage				
Number type classification				
Organization limits				
Organization Wizard				
PBX connectors				
Presence shortcuts				
Presence states				
SIP authentication				
SMTP mail server				
Speech recognition profiles				
Voice prompts				

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

New 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.

Range	*
Source tags	mytag my_tag lehe_calltag_1 lehe_calltag_2 lehe_src_1 ct_1 ct_2 gekuTag1 gekuTag2 sip_auth jaak_billing1 presidents bird cg_attendant bvm_calltag_1 lehe-new

- 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.

nese are the p numbers should rigger the call r	ublished phone numbers to call i be within the number range of i outing rules of a personal line e	in order to reach this user. The phone the organization. Aliases can be used to wen if calling another number.
Primary line		
The primary pu	ublished phone number, also kno	own as "single number reach".
Number	+9877745032	Line type: Office fixed 🔻 📃 Mobile VPN
	List available numbers *	
Alias	45032	Short number
Secondary line Optionally, a us	ser may have a secondary publi	ished number.
Secondary line Optionally, a u Number	ser may have a secondary publi List available numbers	ished number. Line type: Office fixed ▼
Secondary line Optionally, a us Number Add an alias to	ser may have a secondary publi List available numbers this number	ished number. Line type: Office fixed ▼  Mobile VPN
Secondary line Optionally, a u Number Add an alias to	ser may have a secondary publi List available numbers this number	Line type: Office fixed ▼  Mobile VPN
Secondary line Optionally, a u Number Add an alias to Allowed appl	ser may have a secondary publi List available numbers this number ications	ished number. Line type: Office fixed ▼  Mobile VPN
Secondary line Optionally, a us Number Add an alias to Allowed appl Configure which	ser may have a secondary publi List available numbers this number ications a applications the user will have	ished number. Line type: Office fixed ▼ Mobile VPN access to.

- 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 Server and https Path fields).

SIP phones	Hel
These are the SIP desktop phones and settings. When you plug in a new phone to the network, it will be listed here.	
Snom provisioning	
Settings URL: https://bcstest.lab.teleno.com/cinnbone/cinnboneconfig.xml2mac={macl&t=81956	
אוגעינער איז	70.0IIIIIIIII
MITEL 68xx provisioning	
Settings URL: Download Protocol: https https Server: bcstest.lab.telepo.com https Path: /sipphone/t=8195670.0llKRkZwUWZEUmVFPQ	

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).

System Information License Status	Configuration Server Setti	ngs
ration User Password Phone Lock	Settings Download Protocol	HTTPS V
Programmable Keys Keypad Speed Dial	Primary Server Pri TFTP Path	0.0.0
Directory Reset	Alternate Server Alt TETP Path	0.0.0
Preferences Account Configuration	Use Alt TFTP	Enabled
Custom Ringtones anced Settings	FTP Path	
Global SIP Line 1	FTP Deservante	
Line 2 Action URI	HTTP Server HTTP Path	
Firmware Update TLS Support	HTTP Port HTTPS Server	80 bcstest.lab.telepo.com
802.1x Support Troubleshooting	HTTPS Path HTTPS Port	/sipphone/t=8195670.OIIKRK
Сарине	Auto-Resync	
	Mode Time (24-bour)	BOIH •
	Maximum Delay	15
	Days	1
	XML Push Server List(Approved IP Ad	dresses)

- 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.

Create new external system nu	ımber	
Number		
What is the phone number for t	his group:	
+9876588004	de la	
List available numbers		
General		
What is the name of this group:		
MiCC Enterprise Access 1	*	
Add billing id:		
	List available billing ids	
Description		
Meta-data for this group:		
Override this with diverted call	meta-data	
Exclude this number from conta	act searches	

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.

number conversion rule is used to map numbers to umbers to international numbers or rules that map in	other numbers. You can for example set up rules that map r iternal short numbers to external numbers.	nationa
Organization	User group	
Configure for all users in the organization )	Group	
Configure for all users in the organization	Users	

- 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.

Match numbers with prefix:		
Followed by:		
Any number of digits <b>v</b>		
Rewrite prefix to:		

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.

Home	Services	Support	Organization	User administration	Function numbers	Devices			Logged in as to
Service	s		Call mo	nitoring					
Advan	ced settings		Call mo	nitoring means getting	n information on wh	ether anoth	er user i	s busy in a call or i	not.
Call in	trusion			into ing incuns getting					
Call n	nonitoring		Organi	zation			Use	r group	
Call pi	ckup		Configu	ire for all users in the	organization		Pric	. Group	
Coll or							1	Users	A <b>V</b>
Call qu	ieues						2	reports	▲ ▼
Call re	cording						3	TAS group	▲▼

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.

Home	Services	Support	Organization	User administration	Function numbers	Devices		
Service	5		Service	configuration for S	olidusTest			
Advan	ced settings		Which u	ser groups are allow	ed to view busy/fre	status for SolidusTest:		
Call intrusion			🗹 TAS	TAS group				
Call monitoring			User repo	✓ Users reports				
Call pickup			Save	Save Cancel				
Call qu	ieues							

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).

Roles	User group membership			
User with profile: Full access  Administrator with profile: Full access	TAS group Users reports			
and for organizations:				
Manage only own organization				
Manage all linked organizations				
Manage following linked organizations:				
Group administrator with profile:				

- 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 >).

```
    add user ticket
    autotest
    TAS API access
Token: 1.VDphZTIyMTgyYWMzMDFiN2Iw
Secret: b83452454d76624c
Issued: 18/08/2016 15:52
Granted APIs:System management
Revoke
```

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.

PBX	Telepo	~
Configure T	eleno Linestate	
Configure 1	ciepo Encolato.	

The system opens the Telepo Information window.

	Realm	TenantID	Edge Nodes	
			Address	Port
				Add Remove
PI Access Informatio	n	r Management Nodes		
		Address	Port	
oken:				
ken:				
ken:				
iken:				
ken:				
iken:				

- 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:

🧇 TAS Configuration Tool		- 🗆 X
Local Media Server Properties SIP Address and Port Dialog TTL [5065 10 minutes RTP Port Range [40000 - 50000 C RTCP	TAS Installed Version:       9.4.0147.0         SIP Listening Port       CSTA3 Listening Port       Local Interface         5060	PBX Routes Address Port mxone.seclab.com SRV
MOH File C:\Program Files (x86)\Mitel\MediaServer\tinging wav Trim RecordingsForward DTMF into conferences Codec Preference pcma.pcmu.g.722.g.729.rfc2833All	CSTA CallD Range 0-99999 Recording Path C:\temp Inter-TAS transfer numbers TLS support Required V FQDN \vm-sec94.seclab.com V	Remove Add Load balance strategy Round Robin ~ Tas Peers
Audio Files Prefix C:\Program Files (k86)\Mitel\MediaServer\ SRTP SDP Offer Default Recording Rate SRTP Best Effort ( 16 kHz) Default Recording Rate ( 16 kHz) Defaul	Certificate V PBX MX-One V X-Link port 8883  TLS Validate cert	Address Port
Log Path     C.\Program Files (x86)\Mitel\MediaServer\Logs     ●●●       Log Level     Delete older than (days)     Max size (MB)       [3] Trace     10     0       Punning Version:     1.9.49.0       Service Start Time:     12/29/2019 6-03.47 PM       Service Status:     Running	Log Path C.Vogs  Log Level Delete older than (days) Max size (MB) [9] Debug+5 14 512 \$ Running Version: Not Available Service Start Time: Not Available Service Starts: Stopped	Remove     Add       Media Servers     Address       Address     Port       10.70.128.60     5065
		Remove Add Ok Apply Cancel

csta -i --lim 1 --port 8883 --csta-serv 00000000

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:

- 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
- 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 ·	-pı	rint -route 8 -short
Route data for S	ΙP	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:

Comn	ommon Service Profile										
Csp	Cust	Traf	Serv	Cdiv	Roc	Npres	Offered	Forced	CnnLog	Csp	Name
							Time	DisconnectTime			
0	0	0000151515	0000030000000000000000000000 <b>0</b> 0	000000000000000000000000000000000000000	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:

		MX-ONE Maintenance Utility
If an ent the CSR a shall be	erprise CA or sta nd import later t used and a CSR sh	andalone root CA is to be used select 'certificate' to create the signed certificate. Use also this option if TLS networking hall be signed on another MX-ONE server.
If neithe 'root' pl	r an enterprise ( us 'server' to ci	CA nor standalone root CA is to be used select 'auto' or reate needed certificates.
The auto in all se	option will creat rvers in the MX-(	te and install a certificate with default settings and activate TLS DNE system.
Choose op	tion for certific	cate.
	uto Certificate root server m xone-tls m xone-secLevel	Create and install default certificate and activate TLS Manage Certificate Manage Root Certificate Manage Server Certificate Manage TLS in MX-ONE Manage Security level in MX-ONE
	K	K > < Help > < Exit >

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.

	MX-ONE Maintenance Utility
Root and MX-ONE 1	d server certificate successfully created and installed in the system. MLS successfully configured.
Check me	edia encryption settings.
Complete	the activation of MX-ONE TLS by reloading the following program units:
reload -	-u SIPLP, IPLP, TLP65, CSTServer, ConfigServer
	< <u>x</u> >

- 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 000000000 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.
- 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.

vailable snap-ins:				Selected snap-ins
Snap-in	Vendor	^		Console Roo
ActiveX Control	Microsoft Cor			
Authorization Manager	Microsoft Cor			
Certificates	Microsoft Cor	≡		
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Bevice Manager	Microsoft Cor			-
Disk Management	Microsoft and		Add >	
8 Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor			
Internet Informatio	Microsoft Cor			
Internet Informatio	Microsoft Cor			
IP Security Monitor	Microsoft Cor			
IP Security Policy M	Microsoft Cor	~		

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

FEATURE	MX-ONE with X-Link	Other Call Managers
Make Call <sup>Note 1</sup>	<ul> <li>✓ (Agent's phone is called first and then the call is initiated)</li> </ul>	<ul> <li>✓ (Agent's phone is called first and then the call is initiated)</li> </ul>
Answer Call	✔ Note 1	<ul> <li>(calls must be answered from the phone)</li> </ul>
Hangup Call	✓ Note 1	✓ Note 1
Hold Call	$\checkmark$	4
Retrieve Call	$\checkmark$	4
Transfer Call	$\checkmark$	4
Conference Call	$\checkmark$	$\checkmark$
Divert to Service Group	✓ (if call is connected)	✓ (if call is connected)
Divert to Agent	<ul> <li>✓ (if call is connected or a service group call)</li> </ul>	<ul> <li>✓ (if call is connected or a service group call)</li> </ul>
Assist	✓	×

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

Monitor	$\checkmark$	$\checkmark$
Record Calls	×	×
Enter DTMF Digits	×	×
Reject Service Calls	4	✓
Consultation Call	$\checkmark$	✓
Handle Callback Calls	✓	✓
Participate in a Call Campaign	4	✓

**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.

-Application User Informa	ation	
User ID*	AXLUSER	Å
Password	•••••	9
Confirm Password	•••••	9
Digest Credentials		9
Confirm Digest Credentials		9
BLF Presence Group*	Standard Presence group 🗸	
Accept Presence Subscr	iption	
Accept Out-of-dialog RE	FER	
Accept Unsolicited Notifi	cation	
Accept Replaces Header		

The permissions for the user should be set as follows:

Permis	sions Information
Groups	Group AXLaccess
Roles	Standard AXL API Access Standard Admin Rep Tool Admin Standard CCM Admin Users Standard CCMADMIN Administration Standard CUReporting

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.

TAS Configuration Tool		
Local Media Server Properties	TAS Installed Version: 9.4.108.0	PBX Routes
SIP Address and Port Dialog TTL :5065 10 minutes	SIP Listening Port CSTA3 Listening Port Local interface	Address 10.70.128.22
Add Credentials	old behavior         Inactive         □ Include PAI at Deflect           k nore SIP Number Privacy         □ Allow inter tenant calls	
Password: Short	T/ Call/D Range 700000-799999      co ding Path     C:\temp     C:\temp	
	ter TAS transfer number	Load balance :
	-5 support Not supported V	Tas Peers
Ok Car 2el ☑ SRTP Best Effort ④ 8 kHz ④ 16 kHz	PE Cisco	Address
Log Path	Log Path	Media Servers
C:\Program Files (x8b)\Mitel\MediaServer\Logs       Log Level     Delete older than (days)       [3] Trace     10	Log Level Delete older than (days) Max size (MB) [9] Debug+5 V 2 100 +	Address 10.70.128.73
Running Version: 1.9.25.0 Service Start Time: 8/7/2019 2:23:43 PM Service Status: Running Stop	Running Version: 9.4.108.0 Service Start Time: 8/8/2019 10:24:56 AM Service Status: Running Stop	

# **MULTI-TAS SETUP**

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 <u>Media</u> <u>Server</u> 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
  - o Configure multiple destination IP addresses in SIP trunk configuration
  - o Use a Trunk Group

Example: Configure Windows DNS with multiple HOST records

#### Sample environment

 Windows domain: seclab.com
 IP: 10.70.128.241

 MiCC-E server: mtas-micce
 IP: 10.70.128.241

 TAS 1:
 mtas-tas1
 IP: 10.70.128.242

 TAS 2:
 mtas-tas2
 IP: 10.70.128.243

 MX-ONE:
 ts1
 IP: 10.70.128.121

 DNS server
 seclab-dc
 IP: 10.70.128.101

DNS Manager				
	▶ 2	Ē		
<ul> <li>DNS</li> <li>SECLAB-DC</li> <li>Forward Lookup Zones</li> <li>Sectab.com</li> <li>sectab.com</li></ul>	Ame       Imn      Imn      Imn      Imn      Imnsys      micce-94    ECLAB-DE Properties      Debug Logging      Interfaces      Fo      Server version number:      6.0 6002 (0x1772)      Server options:      Disable recursion (al:      BIND secondaries      Fail on load if bad zoo      Enable notmask order      Secure cache again      Name checking:      Inade not date on potential	E vent Logging prwarders so disables forwar ne data st pollution	Type Host (A) Host (A) Host (A) Monitoring Advanced ders)	Data 10.70.1 10.70.1 7 × 1 Security 1 Root Hints 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	Load zone data on start	up: From A avenging of stale	Active Directory and records	I registry
	OK	Cancel	Rese Apply	t to Default

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

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

New Host 🛛 🗙	New Host 🗙
Name (uses parent domain name if blank):	Name (uses parent domain name if blank):
mtas-tas	mtas-tas
Fully qualified domain name (FQDN):	Fully qualified domain name (FQDN):
mtas-tas.seclab.com.	mtas-tas.seclab.com.
IP address:	IP address:
10.70.128.242	10.70.128.243
Create associated pointer (PTR) record	Create associated pointer (PTR) record
Allow any authenticated user to update DNS records with the same owner name	Allow any authenticated user to update DNS records with the same owner name
Add Host Cancel	Add Host Cancel

Create new zone (forward lookup) in seclab.com for mx1:

w Zone Wizard			2
Zone Name What is the name of the new zone	?		
The zone name specifies the portio authoritative. It might be your org- or a portion of the domain name (fi not the name of the DNS server.	n of the DNS names anization's domain n or example, newzor	pace for which this so ame (for example, m e.microsoft.com). Th	erver is icrosoft.com) e zone name is
Zone name:			
m×1			
	< Bac	< Next >	Cancel

Once mx-one is installed and configured to have host name ts1.mx1.seclab.com then the DNS will include the IP addresses for the LIMs in the system. In this example it is only 1 LIM:



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

🛔 DNS Manager					
File Action View Help	File Action View Help				
🗢 🔿 🙍 📅 🗔 🧕 🐟					
🚊 DNS	Name 🔺	Туре	Data	Timestamp	
🖃 📱 SECLAB-DC	mtas-micce	Host (A)	10.70.128.241	11/23/2019	
🖃 🧮 Forward Lookup Zones	🔲 mtas-tas	Host (A)	10.70.128.242	static	
	🔲 mtas-tas	Host (A)	10.70.128.243	static	
🖃 🛐 seclab.com	🔲 mtas-tas1	Host (A)	10.70.128.242	11/25/2019	
te t	mtas-tas2	Host (A)	10.70.128.243	11/19/2019	

Now the DNS server will alternate giving out address 10.70.128.242 and 10.70.128.243 when a DNS lookup is done for mtas-tas.

### 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:

-		
🛃 10.70.128.121 - PuT		
mxone admin@ts1:	> sip route -print -route 1 -short	
Route data for S	P destination	
route : 1		
protocol	= tcp	
profile	= MiCC_Tas	
service	= PRIVATE SERVICES	
uristring0	= sip:?@mtas-tas.seclab.com	
fromuri0	= sip:?@mtas-tas.seclab.com	
remoteport	= 5060	
accept	= REMOTE IP	
match	= 10.70.128.242,10.70.128.243	
register	= SET_BY_PROFILE	
trusted	= TRUST_BY_PROFILE	
supervise	= ACTIVE SUPERVISION	
supervisetime	= 30	

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 used number 2100:

roddi:dest=21,route=1,adc= 050500000000250005001010000,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:

OnCallDelivered Properties		×
General Settings Branches		1
Monitored Device List: Delivered Device: ┌─ Time-outs ────	'TAS1:T1-BVD2100'',''TAS:	2:T2-BVD2
Initial (ms): Inter-digit (ms):	5000 2000	
Default Destination for Non-han Orphan Destination:	dled Calls:	
ОК	Cancel Apply	Help

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.

2

**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.
- 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:
	-		
		Type of Recording	
Beep Before F	Recording Starts	Encoding Type :	6
Min. (sec):	@M. Jourston	Max. Silence (se	c): @MaxSilence
Max. (sec):	@MaxDuration	Max. Retries:	2
Save Message	Interrupted Digit As	C Ap	pend
Media Object	ID: @Media	Object	
Recorded F	le		
Media Obi	act ID:	1	
Recorded	Length:	<b>S</b>	
Message		-	
Hecording Co	mpietea		

### 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	ТҮРЕ	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.

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
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
CPUAcceptLimit	When the machine CPU usage reaches the defined percent TAS will refuse to accept new sessions.	95
DisplayPrivateNumbersAs	Display string for numbers listed as private.	Anonymous
EarlyMediaForSoftphone	Indicates whether softphone should have early media played, when the call manager supports early media.	1 (True)
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.	950:333:- 17,0:30,1400:330:-

	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.	17,0:30,1800:330:- 17,0:1000
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)
IgnoreNumberChangePrefix	When the remote user is changed, indicates the number of ending digits that are significant when determining if the change is 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.	0 (compare entire number)
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)
Initial180Delay	When receiving an incoming INVITE, indicates how long TAS should wait before sending 180 Ringing.	0 (msec, indicates send immediately without delay)
MaxPendingCalls	Max number of simultaneous calls before incoming sessions are rejected	500
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
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)
PingInterval	How often to send OPTIONS message to call manager nodes/Media Servers as a keep-alive	60 (seconds)

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.	0 (False)
ProxyRewriteUnknownCstIdAsDi version	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)
ReferReplaceDiverted	When diverting a call from an external number to another external number, REFER + replaces occurs after call completion.	1 (True)
ReferReplacesTimeout	Max time allowed for a REFER + replaces to complete	3 (seconds)
RemoveSensitiveDataFromTrace	Indicates whether sensitive data such as DTMF digits is removed from the trace log file or traced normally.	0 (False)
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)
ShowRemoteUserInTransfer	When agent transfers caller A to party B, indicates whether B should view A's number	1 (True)
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)
SupportREFER	Indicates whether REFER + replaces is supported	1 (True)
TcpConnectTimeout	Max time to wait for the TCP connection to be established toward the call manager or Media Server	3200 (msec)
TIsFQDN	Value to use as the local FQDN for TLS	Hostname. <name of<br="">Windows domain&gt;</name>
X_Mxone_Endpoint_Disabled	Indicates whether the SIP header X-Mxone- Endpoint should be ignored when detecting the remote user name	0 (False)

#### TAS Integration – Installation Instructions



mitel.com

© Copyright 2020, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation, including itself and subsidiaries and authorized entities. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.