Installation and Configuration Guide

Release 2.6 SP2 June, 2021



Notice

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

> ®,™ Trademark of Mitel Networks Corporation
> © Copyright 2021, Mitel Networks Corporation All rights reserved

Contents

Chapter: 1	Introduction
Chapter: 2	Before You Begin4InAttend Licenses4Software Requirements4Security Certificates4IIS Configuration to access TCA, WebAdmin, QM and other applications overHTTPS5
Chapter: 3	Call Manager Configuration7Configuration for Skype for Business7SIP trunk Configuration on Skype for Business7TCP Configuration on Skype for Business15Closed Redirect and Queue Scheduling16TLS and SRTP Configuration on Skype for Business16Configuration for MX-ONE17Set ECF for extensions without right for ECF17PARAMETERS17SIP trunk Configuration on MX-ONE18Initiating the Route Access Code19Creating SIP routes toward the ACS server20TLS and SRTP Configuration on MX-ONE25Configuring TLS on MX-ONE30Configuring SRTP on MX-ONE30Configuring Day/Night Service Positions30Initiating the abbreviated number series31Initiating the abbreviated numbers32Initiating Day and Night Service Positions for a public route33Initiating Day and Night Service Positions for a public route33

	Configuring Direct Drop	34
	Simplified Configuration for MiV5000 since R7.2	35
	Direction Names	36
	Call Distribution Management	37
	Programming Call Distribution for InAttend Services	38
	DID Corporate Numbers	39
	SIP Trunk Configuration	39
	Add a SIP Trunk for InAttend	40
	Create SIP Routes	45
	What to do Next	45
	Transfer Authorization	45
	Configure Hardphone Subscriber	46
	Create an External Record	46
	Create Password	47
	Configuration for MiVoice 5000	48
	Direction Names	49
	Incoming Call Dialing Plan	50
	Access to Public Exchange	50
	Access to Directions	50
	Call Distribution Management	52
	Programming Call Distribution for InAttend Services	52
	DID Corporate Numbers	54
	SIP Trunk Configuration	54
	Add a SIP Trunk for InAttend	54
	Create SIP Routes	60
	Configure Aid/IID Handling	60
	Define the internal plans	60
	Composition of internal plans	61
	Convert internal plan	61
	Convert Network Plan - Internal Plan	62
	IID Handling	62
	What to do Next	67
	Configuration for Cisco Unified Communications Manager	69
	SIP Trunk security profile configuration	69
	SIP profile configuration	71
	SIP trunk configuration	72
	*23 service configuration	81
	*21 Service Configuration	82
Chapter: 4	Installing the InAttend license	83
	Installing Enterprise License Manager	83
Chapter: 5	Installing the InAttend Server	87
Chapter: 6	Configuring the InAttend system	94

		Running the Quick Configuration Wizard.94InAttend Journal Configuration.98Configuring the Authentication and Authorization (AnA) web service.99Configuring the AnA connection to the CMG server.99Configuring the AnA connection to a Different Server.99Enabling HTTPS for Image Fetching.00
Chapter:	7	Configuring the Presence Server
		Viewing Presence Server Configuration
		Adding a Microsoft Exchange Data Source
		Adding a Microsoft Skype for Business Data Source
		Installing the Unified Communications Managed API (UCMA) . 105
		Setting up the Microsoft Skype for Business environment 106
		Creating an application pool in Skype for Business
		Creating a trusted application in Microsoft Skype for Business 107
		Creating and importing certificates
		Adding a Data Source
		Adding a CISCO Data Source
		Configuring the Presence Server for CLIPS 110 matteria 109
		Adding a line state data source
		Configuring a PBX link for line state (MX-ONE)
		Configuring a PBX link for line state (MiVoice 5000)
		Configuring a Line State Server (Cisco only)
		Installing the Cisco Line State Server (LSS) component119
		Configuring the ACS Cisco Line State Server
		Enabling a Secure Channel for AnA and TCA
		Configuring the Presence Interface
		Configure Directory Server (MiVoice 5000)
		MiCollab and InAttend with MiV5000
Chapter:	8	Configuring Directory Server
Chapter:	9	Configuring MiCollab presence with InAttend
		Micollab presence with InAttend in CMG
		Micollab presence with InAttend in Standalone
		Modifying Webadmin Configurations in InAttend for Standalone 139
		Settings for Micollab with InAttend
		Modifying CMG Web Service Configurations
		Adding MiCollab Configuration File
Chapter:	10	Configuring InAttend profiles and users
		Working with configuration profiles
		Viewing InAttend configuration profiles

		Modifying the Attendant Directories Profile
		Change Directory View Automatically
		Overlapping numbers
		Modifying the Attendant Layout profile
		Modifying the Attendant Messages profile
		Modifying the Attendant PBX profile
		Modifying the Attenuant Search prome
		Working with profile groups
		Creating a new profile group 160
		Modifying a profile group 161
		Configuring In Attend users 161
Chapter:	11	Generate CSR in ACS
Chapter:	12	TLS Certificates Installation
Chapter:	13	Configuring the NeTS telephony system
Chapter:	14	Configuring the Media Server
Chapter:	15	Installing the InAttend Client
		Configuring the InAttend Client
Chapter:	16	Configuring EFS
Chapter:	17	Setting up Quality Manager
		Prereguisites
		Installing the Quality Manger Server
		Installing the Quality Manager Database
		Installing the Quality Manager Service
		Installing the Quality Manager Reports Web
		Configuring the Quality Manager Server
		Configuring the InAttend Server for Quality Manager 185
		Configuring multiple customers for Quality Manager 186
		Populating the Quality Manager Database with InAttend configuration 187
		Configuring the Quality Manager Database
		Configuring the Journal Database
		Configuring Working Hours in Quality Manager
		Configuring customers in Quality Manager
		Viewing queues in Quality Manager
		Assigning customers to a domain in Quality Manager 192
		Configuring interval sets in Quality Manager

	Installing the Quality Manager Wallboard196Configuring the Quality Manager Wallboard application196Configuring the Quality Manager Database Connection197Configuring the InAttend Connection198Configuring the Queues to display198Configuring operators to display199Configuring the Wallboard layout200Configuring thresholds for alerts201
Chapter: 18	Additional configuration tools
	CMG configuration tool
Chapter: 19	Verifying your installation
	InAttend system verification207General207InAttend call handling207Line state and activities/forward208InAttend user interface209Quality Manager verification209Verifying the Quality Manager installation210Verifying the Quality Manager Wallboard210
Chapter: 20	Logging
	Log Levels212Log Directory for each Component212Default software212AnA Web Service212BluStar License Manager213BluStar Server and BluStar Presence Server213CMG Web Service213Enterprise License Manager (Server and Client)213Mitel LDAP Server213InAttend Client213Media Server213Queue Manager214Telephony Configuration Manager214Optional Client Software214
Chapter: 21	References

Chapter: 22	Appendix A: Configuring telephony services in TCA
	Telephony services configuration sequence
	Create a TCA configuration
	Configure the call manager and ACS hosts
	Add a site
	Add a Line State Server
	Add a Queue Manager
	Configure the NeTS host
	Create a media server and add it to the site
	Create a queue for the site
	Create an operator group and assign it to a queue
	Configuring public recall queues
	Private Queue Number for Individual Attendants
	Configuring Voice systems 236
	Deploy the configuration 236
	$\begin{array}{c} \text{Output} \text{Output} $
	Dipy Different MoH for InAttend for Different Queue
	Play Different Mon for mattend - for Different Queue
Chapter: 23	Appendix B: CMG-specific configuration
	Configuring a CMG user as TCA admin
	Adding the CMG Administrator to the InAttend Operator Group 240
	Disabling default templates using Attendant special settings
	Configuring Presence for the CMG Server 242
	Ontimizing Nicesry 242
	Configuring Presence Server when using more than one E-mail Message Sys.
	tem

Introduction

Mitel InAttend is a user-friendly attendant application that handles high volumes of internal and external calls while providing advanced collaboration features.

InAttend integrates SIP-based call and queue handling, contact search options, calendar integration, line state and activity status information into a single application.

You can deploy InAttend with a number of SIP-enabled call managers, such as MiVoice MX-ONE, MiVoice 5000, Microsoft Skype for Business, or Cisco Unified Communications Manager, using SIP for call control and media streams.

For advanced directory search and visitor management requirements, InAttend can be integrated with BluStar Collaboration Management (CMG). When InAttend is integrated with CMG, the attendant has the ability to set activities and forwarding for everyone registered in the CMG Server directory.

This document describes the installation and configuration of InAttend using the InAttend installer. Other solution components such as the SQL Server, CMG server, MX-ONE server, CUCM can be installed on other machines, as long as they are network-accessible.

InAttend system components

The InAttend solution comprises the following components:

- Enterprise License Manager: handles licensing requirements for the InAttend application.
- **InAttend Server**: A telephony application that integrates with call managers, enabling call and media functionality. The components of the InAttend server include:
 - BluStar Directory Server (or Active Directory): provides directory services
 - BluStar Presence Server: provides calendar, presence, and line state information
 - Attendant Connectivity Server (ACS): provides queue management services (Queue Manager); handles media streams during calls (Media Server); and provides call handling and SIP communication to the call manager (NeTS)
- InAttend Client: A Windows-based attendant console application.



The Attendant Connectivity Server (ACS) component of InAttend is the SIP-based software that integrates with the platform to perform call control signalling and media sessions for queues, IVRs, and InAttend. An ACS-based SIP trunk has to be connected between the platform and the InAttend server.

Depending on the type of platform, a second link is needed from the BluStar server component of InAttend to the corresponding presence or platform interface.

In the example shown here, a UCMA interface is configured to the Skype for Business 2015 integration for presence and line state communication:



All inbound calls are routed via the SIP trunk connection and presented to the InAttend console. The UCMA connection is used by the attendants to retrieve presence and line state information about Skype users.

Additionally, the BluStar server component has connections to applications such as LDAP Directory Service and Microsoft Exchange so it can synchronize the Skype directory information with the attendant system and have access to real-time calendar information for Skype users.

InAttend installation types:

- InAttend stand-alone In this scenario, any LDAP directory can be used for directory information. BluStar Server (BSS) can consolidate multiple LDAP directories, such as Active Directory or CRM systems.
- **InAttend with CMG Server** With CMG Server, integration with communication servers makes it possible to divert CMG users' extensions according to the different activities that have been set for a user. The CMG Server also contains a database with directory information and other user data, public and private the latter can be viewed by the attendant.

Before You Begin

It is assumed that the person installing the InAttend system is an experienced system administrator or network administrator who knows how to install, configure, and manage Windows servers as well as the call manager (i.e., PBX) to be used in the InAttend system.

InAttend Licenses

Before you install InAttend, you have to obtain and install the InAttend license on the Enterprise License Manager (ELM) server.

Software Requirements

For software compatibility, refer to InAttend Compatibility Matrix and for hardware requirements, refer to InAttend Datasheet, available on InfoChannel.

Security Certificates

A server certificate is required for secure, encrypted communications (TLS) between InAttend and the call manager. TLS certificates are optional for MiVoice MX-ONE, MiVoice 5000 and mandatory for Microsoft Skype for Business.

You have to enter the certificate location when you run the Quick Configuration Wizard to configure the InAttend ACS component. To acquire a TLS certificate, you have to:

- Use IIS to create a certificate request.
- Submit the request to an online authority called a Certificate Authority (CA). Once approved, you will receive a certificate response which contains your digitally-signed public key.
- Install this certificate using IIS.

Refer to the Microsoft Support web site at https://support.microsoft.com for detailed instructions on requesting and installing certificates.

IIS Configuration to access TCA, WebAdmin, QM and other applications over HTTPS

To access TCA, WebAdmin, QM and other applications over https, do the following:

1. Create or import a server certification from the **IIS server** as shown in the below screen-shot.



- 2. Go to Sites> Default Web Site> Bindings
- 3. Click **Bindings** in the right-side of the pane and click **Add** to add a new https binding by choosing a certificate created in the first step as shown in the below screenshot.



NOTE: All the above settings are valid for TCA, WebAdmin, QM and other applications that you can access it over https.

Call Manager Configuration

You must set up SIP trunking on the call manager to enable SIP trunk configuration to the InAttend ACS. You must enable the appropriate transport protocols (TCP, TLS, SRTP) for communication between the call manager and InAttend.

Configuration for Skype for Business

Encryption is required for Microsoft Skype for Business deployments, so you must have a TLS security certificate installed before you start.

When you have CMG Web and Skype for Business, disable the Presence function in CMG Web.Update file Web config with below line: <add key="SetBluStarPresenceStatus" value="false" />

SIP trunk Configuration on Skype for Business

You must define a SIP trunk between the Microsoft Skype Mediation Server and the ACS component of the InAttend server.

To define a SIP trunk in Skype for Business 2015, do the following:

- On the Skype Server, start the Topology Builder (Start -> All Programs -> Skype for Business 2015 -> Topology Builder).
- 2. In the Topology Builder, expand Shared Components.
- 3. Right-click on the PSTN gateway folder and select New IP/PSTN Gateway from the pop-up menu.



4. In the **Define the PSTN Gateway** window, enter the Fully Qualified Domain Name (FQDN) of the InAttend server and click **Next**.

Define New IP/PSTN Gateway
Define the PSTN Gateway FQDN
Define the fully qualified domain name (FQDN) for the PSTN gateway.
skype.inattendbgl.com
Help Back Next Cancel

5. In the **Define the IP address** window, keep the default value ("Enable IPv4") and click Next.

CONFIGURATION FOR SKYPE FOR BUSINESS CALL MANAGER CONFIGURATION

CHAPTER 3

15	Define New IP/PSTN Gateway
5	Define the IP address
Enable U U Li	e IPv4 se all configured IP addresses. imit service usage to selected IP addresses. STN IP address:
○ Enabl ○ U ○ Li P:	e IPv6 se all configured IP addresses. imit service usage to selected IP addresses. STN IP address:
Help	Back Next Cancel

6. In the Define the root trunk window, enter values for the following parameters and click Finish:

- Trunk name: the FQDN of the InAttend server
- Listening port for IP/PSTN gateway: the InAttend TLS port (5061)
- SIP Transport Protocol: TLS (select from the drop-down menu)
- Associated Mediation Server: the FQDN of the Skype Mediation Server
- Associated Mediation Server Port: 5067 (default)

CHAPTER 3

Define New IP/PSTN Gateway
Define the root trunk
Trunk name: *
skype.inattendbgl.com
Listening port for IP/PSTN gateway: *
5067
SIP Transport Protocol:
TLS
Associated Mediation Server:
skype2015.inattendlabbgl.com Mitel
Associated Mediation Server port: *
5067
Help Back Finish Cancel

- 7. Publish the topology.
 - a. In the Topology Builder, expand Shared Components.
 - **b.** Right-click the **PSTN gateway folder** and select **Topology -> Publish** ... from the pop-up menu.

🔺 🚞 PSTN مصtحت	2105		
🌄 ina	New IP/PSTN Gateway		
1 мх	Topology	•	New
🌄 gat	Help		Open
ידי.דיד 10. 🖏	5.204		Download Current Topology
👂 🚞 Trunks			Save & Conv
🦲 Office Web /	Apps Servers		Sure A copy
			Publish
🛄 Video gatew	ays		Install of Publich tenelogy to the Central Management store
🚞 SIP Video tru	unks		Publish topology to the Central Management store.
🚞 Branch sites			Remove Deployment

8. Open the Microsoft Skype Control Panel and click Voice Routing in the left column.

- 9. Define the Dial Plan required to allow Skype users to dial to InAttend.
 - a. On the **Dial Plan** tab, define a normalization rule appropriate for your organization, with at least a rule for Skype users to dial to InAttend. (Contact Microsoft for instructions on the appropriate setup for your company as required.)

8	Skype for Business Server 2015 Control Panel	- 0 X
S Skype for Bu	usiness Server	Adwinistrator (Sign eut 6.03019.0 (Privacy statement
Skype for Bu Home Users Topology IM and Presence Persistent Chat Voice Routing Voice Features Response Groups Conferencing Clients Federation and Esternal Access Monitoring and Archiving Secutivy Network Configuration	DIAL PLAN VOICE POLICY BOUTE PSTN USAGE TRUNC CONFIGURATION TEST VOICE ROUTING Create voice routing test case information Create voice routing test cas	Advinidentic (Sign ext 6.0331930 (Prively statement
	51 fdt Sand (2)	
	laternal extension	

b. Commit your changes.

- **10.** Click on the **Voice Policy** tab to define a voice policy for the dial plan (Skype users have to be assigned to this policy later).
 - a. On the Voice Policy tab, click **New** and select the type of policy applicable for your organization (Site policy or User policy).

Skype for Bus	siness Server			Administrator Sq 6.0.5119.0 Privacy state
ome	DIAL PLAN VOICE POLICY	ROUTE PSTN USAGE TRUNK CONFIG	RATION TEST VOICE ROUTING	
sers				
opology	Create voice routing test ca	se information		
A and Presence				
ersistent Chat	Edit Voice Policy - Global			
oice Routing	√ OK X Cancel			
pice Features	Scope: Global			
elocose Groups	Global			
noferencing	Description			
omerencing				
lients	Calling Features			
ederation and demail Access	C Enable call forwarding		🐼 Enable team call	
tonitoring	C Enable delegation		C Enable PSTN resoute	
nd Archiving	C Enable call transfer		Enable bandwidth policy override	
ecurity	🛄 Enable call park		Enable malicious call tracing	
etwork	C Enable simultaneous ris	iging of phones		
enfiguration	Associated PSTN Usages			
	New Misced. /	Show details. Ramove 🍵 🐥		
	PSTN usage record	Associated routes		
	inAttend	Route_to_inAttend		
	internal JSON	Route_internal_ISDN		
	MXONE	Route to MXONE		
	InAttendExt	Route_to_inAttendExt		
	Internel_Inattendmixed	Route_internal_inattendmixed		
	External_inattendmixed	Route_External_Inettendmixed		
	gafewayptx.bgliab.local	Route_gatewayobx.bgliab.local		
	Outbound_to_PSTN	Route_Outbound_to_PSTN		

- b. Specify a Name and (optionally) a description for the voice policy.
- c. Click OK when finished.
- d. Under Associated PSTN Usages, click New to associate a new PSTN for this policy.

Associated	PSTN Usages				
New	Select	🖊 Show details	Remove	÷	÷
PSTN use	ge record	Associate	d routes		
InAttend	1	Route_to	InAttend		
Internal,	ISON .	Route_in	temai_ISDN		
MXONE		Route to	MXONE		
InAttend	16x1	Route_to	inAttendExt		

- e. Specify a name and (optionally) a description for the new PSTN usage record.
- f. Under Associated Routes, click New to associate a route with the PSTN usage record.

Skype for Bus	iness Server	Administrator i Signique 60.9311.0 Phase statisment
Home	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING	
Topology	Create voice routing test case information	· •
Persistent Chat	Citic Voice Policy > Edit PSTN Usage Record - InAttend	
Voice Routing	None	
Voice Features	PAttend	
Response Groups Conferencing	Associated Routes	
Clients	Name Pattern to match	
Federation and External Access	Route_to_inAttend *09	
Monitoring and Archiving		
Security		
Network Configuration		

g. Specify a name and description for the new route.

Skype for Bu	siness Server	Administrator i Sign out 6/03319.0 Privacy statement
Home Users	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING	
Topology IM and Presence	Create voice routing test case information	٠ •
Persistent Chat Voice Routing	√ OK ★ Cacet	θ
Voice Features Response Groups	li-Attend	
Conferencing Clients	Associated Routes • New Phil Select. / Show totals.	
Federation and External Access	Name Pattern to match Route to inAttern A09	
Monitoring and Archiving		
Network Configuration		

11. Associate the InAttend (ACS) PSTN gateway that you created in step 4 with the route.

- a. Under Associated Gateways, click Add.
- b. In the Select Trunk window, select the PSTN gateway you created for the InAttend (ACS).
- c. Click **OK** to save your changes.

Se	lec	t Trunk		23
_				
				٩
		Service	Site	
		PstnGateway:inattendskype.ina	Mitel	
		PstnGateway: MX1. in attend bgl	Mitel	
		PstnGateway:gatewaypbx.bglla	Mitel	
		PstnGateway:10.10.128.254	Mitel	
			ОК	ancel

- 12. To assign the InAttend gateway to the trunk, click the Trunk Configuration tab.
 - a. Click **New** and choose the type of trunk that is appropriate for your organization (**Site trunk** or **Pool trunk**).
 - b. Keep the default Encryption support level value ("Required").
 - c. Set Refer support to "None".
 - d. Click OK to save your changes.

S Skype for Bu	siness Server	Administrator Sign o 6.0.9319.0 Privacy Milterne
Home	DUAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING	
Users		
Topology	Create voice routing test case information	*
IM and Presence		
Persistent Chat	Edit Trunk Configuration - Global	
Males De dies	🚽 OK 💥 Cancel	
Voice Kouting	Scope: Global	
Voice Features	Name: *	
Response Groups	Gooel	
Conferencing	Description:	
Clients		
Enderation and	Maximum early dialogs supported:	
External Access	20	
Monitoring	Encryption support level:	
and Archiving	Required	
Security	Seter support:	
Network	Enable sending refer to the pateway	
Configuration	🗍 tnable media bypass	
	Centralized media processing	
	Enable RTP latching	
	C truble forward call history	
	Enable forward P-Asserted-Identity data	
	Enable outbound routing failover timer	
	Associated PSTN Usages	
	Per Select. Renove 🖀 🔶	
	PSTN usage record Associated routes	
	inacitrio noute, or, inacitrio	

When setup is complete, assign Skype users to the Voice Policy you created in the above procedure.

TCP Configuration on Skype for Business

If you are using a TCP SIP trunk for call handling between the InAttend server and Microsoft Skype call manager, you have to enable TCP on the Mediation Server component of the Skype Server.

Before you configure TCP on the Microsoft Skype server, you have to ensure that:

- the InAttend Server belongs to the same domain as the Skype call manager
- DNS is properly configured (i.e., FQDN has to be used in this setup)
- the port configuration towards InAttend is:
 - Skype TCP port = 5068
 - InAttend TCP port = 5060

19	Skype for Business S	erver 2015, Topology Builder		_ 🗆 X
File Action Help	10	Edit P	roperties	_ 🗆 X
File Action Help Skype for Business Server Mitel Lync Server 2010 Lync Server 2013 Skype for Business Server 2015 Skype for Business Server 2015 Standard Edition Front End Servers Enterprise Edition Front End pools Mediation pools Mediation pools Edge pools Trusted application servers Video Interop Server pools Shared Components Branch sites 	PSTN gateway	Edit P Addiation Server PSTN gateway stening ports: * TLS: 5067 2 Enable TCP port the TCP port of this Mediation Server r the following trunks are associated with efault. A default trunk is required only 2. Trunk m MX1.inattendbgl.com gatewaypbx.bgllab.local 10.10.128.254	5067 TCP: 5068 - 50 nust be enabled because a TCP gate h this Mediation Server. Click Make E r when your topology contains Office Gateway o inattendskype.inattendlabbgl.com gatewaypbx.bgllab.local 10.10.128.254	68 68 Way depends on it. Default to mark a trunk as communications Server 2007 Site Mitel Mitel Mitel Mitel Mitel Unmake Default
	Help			OK Cancel

NOTE: In the screen tick the "Enable TCP" check-box and the TCP window will open.

To enable TCP on the Skype Server, do the following:

- 1. On the Skype Server, start the Topology Builder (Start -> All Programs -> Skype for Business Server 2015 -> Topology Builder).
- 2. In the Topology Builder, expand **Mediation pools** and select the **Mediation Server** that is used between Skype and InAttend (ACS).
- 3. Right-click Edit Properties and select PSTN Gateway.
- 4. Under Mediation Server PSTN gateway, select Enable TCP port.

To get night mode (passive redirect / close mode / overflow) to work correct towards Skype, do the following:

• The redirect target for the queue answers the calls immediately (e.g. IVR welcome message) and not respond with other responses (e.g. sending busy or other error responses).

Closed Redirect and Queue Scheduling

Public Queues under Telephony Configuration Application manages and can set the Call queue timings for a call queue entry.

It can also redirect a call based on the scheduling for a call queue entry.

Queue entry consists of Passive Redirect, Closed Redirect, and Overflow.

1. Closed Redirect:

This function sets the calls to be moved / redirected to other options when the time for accepting a call is passed.

Closed redirect is based on 3 options under it:

- No Closed redirect Here a 'queue closed' prompt is displayed, which means the queue is currently closed to take any calls and the call drops.
- Queue Here the call is redirected to a different queue.
- Number Here the call is redirected to the number that is mentioned for the call to be forwarded to.

2. Scheduling:

When a call comes in a queue, it goes to the call manager first.

The call manager sets a time schedule for the call queue acceptance.

For example: If the time allotted for call acceptance is set as 10am to 6 pm, and a call comes in before 10 am or after 6 pm, this call is redirected as per the 'queue entry settings' or it is redirected as per the 'closed redirect' option selected.

View site My_Site Webpage Dialog		Queue Entry Webpage Dialog
Attp://10.10.144.63/tca/site/sitedisplayi	irame.aspx?id=1&name=My_S	Attp://10.10.144.63/tca/site/queueentrynewiframe.aspx?id=15
Telephony Configuration Application	Queue - Kumar_(Edit Queue Entry Queue access
My_Site ⊡-Site: My_Site	Settings Queue Manager Cluster Default prio	Description 05 Pbx Kumar_MX1 Number Ranne 05 Queue Number
Private Networks Public Queues Internal	Max size Wait time 1st alert (s)	Domain Kumar-MX1 Access number 05
- External - Kumar_Queue - CUCM_Queue - Operator Groups - Voice Systems	Queue NoAnswer Time (s Default Queue Entry S Passive redirect Closed redirect	Settings Passive redirect Queue Internal (My_Site) Number
	Overflow Overflow No Answer	Closed redirect Queue Internal (My_Site) Number
	Queue Entries Domain Desc	Overflow Internal (My_Site) Oqueue Internal (My_Site) Number Internal (My_Site)
		Scheduling Common Holidays Edit Custom Holidays Edit
		Daily 12:00 AM to 11:59 PM Monday 7:00 AM to 10:55 AM Artive 12:00 PM to 4:59 PM Artive
		Tuesday 7:00 AM to 10:59 AM Active 12:00 PM to 4:59 PM Active

TLS and SRTP Configuration on Skype for Business

TLS (for signalling encryption) is defined in the Microsoft Skype Topology Builder and SRTP (for media) is defined in the Microsoft Skype control panel.

Before you configure TLS and SRTP on the Microsoft Skype server, you have to ensure that:

- the InAttend Server belongs to the same domain as the Skype call manager
- DNS is properly configured (i.e., FQDN has to be used in this setup)
- the port configuration towards InAttend is:
 - Skype TCP port = 5068
 - Skype TLS port = 5067, uses FQDN
 - InAttend TCP port = 5060
 - InAttend TLS port = 5061
- a TLS certificate is available and installed on the InAttend server (see "TLS certificates installation" on page 128 for instructions).

NOTE: If you restart Skype or the frontend server, you must also restart the InAttend server.

Configuration for MX-ONE

The following information describes necessary configuration tasks on MX-ONE to integrate with InAttend. For detailed information about MiVoice MX-ONE configuration, refer to the MX-ONE product documentation.

Set ECF for extensions without right for ECF

During an incoming call, the operator can forward this call to a set external number. This external number can be set by the operator.

· 0822359	🛈 🗙 Join	Start 🖃 🗶				- 6	×
Menu Call Co	introl						
r f f	5 🕋 🗛 I		Function	i Functions			
0		Recall (0)	External (0)	Internal (0)	Park (0)	•	Web
Queue	Caller	Called	Origin Prio Time Reason				
			Call Phone (2001)	٦			Appointment
			Transfer to voicemail				1
			Send mail				ournal
			Set forward	j			
			Set information				1
			Team Search 1 (Organization)				Sessay
Search: rama	-	Dep1	Team Search 2 (Room)	mation Email		-	
🖼 rama [2]			Team search's (Teilvo)	-			
Status	First name	Last name	L Details	Email Dep1	Company Keywords	Organization	
	Megha	Ramachandra Rai	Change font size	1013			
1	Ganesh	Ramanathan Rar	nanathan Ganesh 🛛 💿 6003	3	Finance +	Finance +	
						- · ·	
Status			Vie	w: all COMPANY01 Attendants: 1 / 7 co	nnected W8 Thursday, February 23, 2017 4	:41:19 PM	
📀 🥝		💿 🔯 🔯			EN 2	+4:41 PN 23-Feb-	M 17

PARAMETERS

--csta-serv

There is a new parameter exist in Mx-one that verifies –csta-serv xxxxxxx1 is set with command csta -p -l x.

- D9: Diversion category override.
- Set feature request does not check the diversion category of the terminal when this is set to Yes.
- This allows activation of ECF, Follow-Me, Diversion on Busy and Diversion On No Reply, when the extension category is not allowing activation of the diversion from terminal.
 - 0 No.
 - 1 Yes.
- The switch requires an argument. The argument is single-valued.

The following sections describe how to configure SIP trunks and how configure the appropriate transport protocols on MX-ONE.

SIP trunk Configuration on MX-ONE

Use the MX-ONE Service Node Manager to configure MX-ONE for SIP trunking.

Enabling the CSTA server in MX-ONE

To enable the CSTA server in MX-ONE, do the following:

1. On the MX-ONE Service Node Manager main page, click Services > CSTA Server tab.

🕅 Mitel	Service N	ode Manager					
Initial Setup	Number Analysis	Telephony	Services	System	Tools	Logs	
Connections	Messages	Voice Announcements	Branch	Office	Routing Server	CSTA Server	Incoming Call Handling
CSTA Server Monitored Devices	CSTA Server - Apply Cancel	Add					
	? Server Number:? Type Of Interface:	1 ▼ ● ECI ● TRE	1A323 37 uaCSTA				
	Port:	8882					
	 (?) Heartbeat Option: 	∙ns ● No ● Hea	Heartbeat artbeat support by	external applicat	ion		
	⑦ By-pass Option:	● No ● By-	by-pass pass of personal n	umber			
	⑦ Diversion Option:	● No ● Allo	diversion w diversion after d	leflection			
	⑦ Dialed Number Pres	sentation Option:	not replace dialed lace dialed numbe	number r with deflect-to	number		
	⑦ Connection View Op	ption: Loc Fixe	al view ed view				
	② Encryption keys:	Do	not send Encryptio Id Encryption keys	on keys			
	⑦ Security:						
	Apply Cancel						

- 2. Select a server number and enter 8882 in the Port field.
- 3. Click Apply.

Initiating the Route Access Code

To initiate the Route Access Code, do the following:

- 1. On the MX-ONE Service Node Manager main page, click **Number Analysis** and then click on the **Number Plan** tab.
- 2. Click Number Series in the left panel.
- 3. On the Number Series page, select "External numbers" for the Number Series Type.



4. In the External Destination field, enter the Operator number (in this example, 08).

Initial Setup	Number Analysis	Telephony	Services	System	Tools	Logs
Number Plan	Call Diversion	Call Discriminatio	on Emerg	gency Number		
Number Series	Number	Series - Add -	Step 2/2			
Service Codes		aut > Annha On				
External Number Leng	gth	Appiy Ca	Incel			
Number Conversion	🕴 External N	umber Series				
Number Conversion U	pload 📀 External C	oordinated Destination:]
System Numbers	⑦ External D	estination :		08]
	? Least Cost	Routing Access Numbe	rs:]
	⑦ Common E)irect In-Dialing Operato	or Numbers:]
	Own Node	Number:				
	⑦ Common P	ublic Directory Number	5:]
	Access Nur	mbers for Mobile Extens	ion (without Author	ization):		
	Access Nur	mbers for Mobile Extens	ion (with Authorizat	ion):]
	Public Dest	ination Least Cost Rout	ing:			
	⑦ Direct Inwa	ard Service Access:]
	⑦ Fictitious D	estination Numbers:				

- 5. Click Apply to save your changes.
- 6. On the confirmation page, click **Done**.
- 7. Click on External Number Length in the left panel.
- 8. Enter the route access code in the **External Number** field, and specify the minimum and maximum length (set both to the same number).

Initial Setup	Number Analysis	Telephony	Services	System
Number Plan	Call Diversion	Call Discrimination	on Eme	rgency Number
Number Series	External	Number Leng	th - Add	
Service Codes	Apply Ca	ncel		
External Number Leng	th			
Number Conversion	② External f	Number: * 08		
Number Conversion U	pload ⑦ Minimum	Length: * 2		
System Numbers	Maximum	Lengun: Z		

- 9. Click Apply to save your changes.
- 10. Repeat steps 2 through 9 for the PBX main number (e.g. 5500).

Creating SIP routes toward the ACS server

To create the SIP routes towards the ACS server, do the following:

- 1. On the MX-ONE Service Node Manager main page, click **Telephony** and then click on the **External** Lines tab.
- 2. Click **Route** in the left panel.

🕅 Mitel	Service	Node Manag	jer				
Initial Setup	Number Analysis	Telephony	Services	System	Tools	Logs	
Extensions	Operator	Call Center	Groups	External Lines	System Data	IP Phone	DECT
Route Destination Corporate Name	Add	Using Template: <a>> <	ault template>	T	<u>Manage Templa</u>	tes	
Busy No Answer Rero	uting 💿 Select	a Route Name: All	 View 	Change			
Busy No Answer Rero	uting ⑦ Select	a Route Name: All	▼ View	/ Change			
Busy No Answer Rero Vacant Number Rerou Customer Rerouting Public Exchange Num	ting ⑦ Select	a Route Name: All	▼ View	Change			
Busy No Answer Rerou Vacant Number Rerou Customer Rerouting Public Exchange Num Charging	ting ber	a Route Name: All	▼ View	/ Change			

3. On the Route page, click Add and select "SIP" from the Type of Signalling list.

CHAPTER 3

Initial Setup	Number Analys	sis Te	elephony	Services	s System
Extensions	Operator	Call Cente	r Grou	ips	External Lines
Route	Route	e - Add - s	Step 1/9	9	
Destination	De De el	Next	A	-1	
Corporate Name	<- Back	Next ->	Apply Canc	el	
Busy No Answer Rero	uting (?) Type	of Signaling:	ISDN 30B+D PI	rivate ▼	
Vacant Number Rerou	iting		ISDN 30B+D PI	rivate ublic	
Customer Rerouting			ISDN 23B+D P	rivate	
Public Exchange Num	ber		ISDN 23B+D Pi IP Private, H.32	ublic 3	
Charging			SIP		
Mobile Direct Access I	Dest				

4. In the **Profile name** field, select **InAttend** from the drop-down list.

Initial Setup	Numbe	r Analysis	Те	lephony	Service	s System
Extensions	Operato	r	Call Center	r	Groups	External Lines
Route		Route	- Add - 9	Step 1	/ 9	
Destination					-	
Corporate Name		<- Back	Next ->	Apply	Cancel	
Busy No Answer Rer	outing	⑦ Type o	f Signaling:	SIP	•	
Vacant Number Rero	uting	Profile	Name:	InAttend		•
Customer Rerouting				AMCC Cisco		▲
Public Exchange Nun	nber			Default Exchangel	IM TCP	
Charging				Exchangel	JM_TLS_SRTP	
Mobile Direct Access	Dest			InAttend InAttendNo	оСВ	
				Lync_TCP	· · · · · · · · · · · · · · · · · · ·	
				Lync TLS	SRTP	
				MXONE-E	NUM-tieline	
				MXONE-e	mergency	
				MXONE-e	mergency_elin	
				MXONE-e	mergency_name	
				MXONE-ti	eline eline ECW	
				MiCollabA	M TCP	
				MiCollabA	M TLS SRTP	
				MiVoice50	00 00	
				MiVoiceBu	siness	•
		<- Back	Next ->	Apply	ancel	

- 5. Enter the Route settings using the information provided in the Help screen.
- 6. Click Apply. (For MX-ONE from 6.1 SP1):

Initial Setup	Number Analysis	Telephony	Services	System		
Extensions	Operator	Call Center	Groups	External Lines		
Route	Route -	- Add - Step	2 / 4			
Destination	General					
Corporate Name	<- Back	Next -> Apply	Cancel			
Busy No Answer Rerout	ing					
Vacant Number Rerouti	ng 🕜 Route N	⑦ Route Name: * InAttend				
Customer Rerouting	⑦ Route N	Number: 10 🔻				
Public Exchange Numbe	er					
Charging						
Mobile Direct Access De	est					

7. On the confirmation page, click **Done**.

Initial Setup	Numbe	er Analysis		Telephony	Servio	ces System
Extensions	Operato	or	Call Cer	nter	Groups	External Lines
Route		Route	- Add	- Step	3/4	
Destination		Individ	uals			
Corporate Name		<- Back	Next ->	Apply	Cancel	
Busy No Answer Rero	outing					
Vacant Number Reror	uting	Serv	/er	Trunk Inde	ex	
Customer Rerouting		? 1▼	*	1-10		
Public Exchange Num	nber					
Charging						
Mobile Direct Access	Dest					

8. To associate the external numbers with the InAttend route, click **Destination** in the left panel, and then click **Add** on the Destination page.

CHAPTER 3

Initial Setup	Number Analysis	Telephony	Services	System	Tools	Logs
Extensions	Operator	Call Center	Groups	External Lines	System Data	IP Phone
Route Destination	Destin	ation Using Template: <a>Defa	ault template>		 Manage Templat 	<u>es</u>
Busy No Answer Rero	outing ⑦ Select	Destination: All	View			
Customer Rerouting	Iting					
Public Exchange Num Charging	ber					
Mobile Direct Access	Dest					

- 9. On the Destination Add page, select "Destination" for the Type of Destination
- 10. Click Next.

Initial Setup	lumber Analysis	Telephony	Services	System
Extensions O	perator Cal	ll Center	Groups	External Lines
Route Destination Corporate Name	Destination Type of De <- Back No	on - Add - S estination ext -> Apply	tep 1/4	
Vacant Number Rerouting Customer Rerouting Public Exchange Number Charging	9 ⑦ Type of Des	stination: Dest Ficti	ination tious destination	
Mobile Direct Access Des	t			

11. On the Route Details page:

- a. Select the destination number from the list in the **Destination** field.
- **b.** Select InAttend from the list in the **Route Name** field.
- c. Click Next.

Initial Setup	Number Analy	/sis Te	lephony	Services	System
Extensions	Operator	Call Center	r Gro	oups	External Lines
Route	Dest	ination - A	dd - Ste	p 2/4	
Destination	Rout	e Details		-	
Corporate Name	<- Ba	k Next ->	Apply	ncel	
Busy No Answer Re	erouting				
Vacant Number Rer	outing 🕐 De	stination:	08-External	▼ Edit	
Customer Rerouting) ⑦ Ro	ute Name: stomer Choice:	InAttend	View	Edit
Public Exchange Nu	Imber	sconier choice.			
Charging					
Mobile Direct Acces	s Dest				

12. On the ADC Details page:

- a. Select "Seizure when minimum length attained" from the list in the **Type of Seizure of External** Line field.
- **b.** Select "Unknown private" from the list in the **Type of Called Number** field.
- c. Click Advanced.

Initial Setup	Number Analys	is Telephony	Serv	ices S	System	Tools		
Extensions	Operator	Call Center	Groups	External I	Lines S	ystem Data		
Route Destination	Desti	nation - Add - S	Step 3/	3				
Corporate Name Busy No Answer Rer	outing ADC L	Next -> Apply	Cancel					
Vacant Number Rero Customer Rerouting	(?) Dest (?) Rout (?) Alter	ination: te Name: mative Routing Choice:	08 InAtte 1▼	end				
Public Exchange Nu Charging Mobile Direct Access	nber ⑦ Star ⑦ Type ⑦ Forv	t Position for Digit Transm e of Seizure of External Lir vard Switching:	nission: 1 • ne: Seizu	1 ▼ Seizure when minimum length attained ▼				
	 ⑦ Type ⑦ Type ⑦ Type ⑦ Type ⑦ Use Advance 	e of Called Number: e of Calling Public Number e of Calling Private Numbe as Emergency Destination ed	Unkn r: Unkn n: O	own private ▼ own public ▼ own private ▼				

13. On the Advanced page, click Enable Enhanced Sent A-Number Conversion and then click Apply.

 Type of Protocol to use for Supplementary Service Call Offer: Type of Protocol for Call Back/Call Completion: 	 User to User Interface(UUI) Generic Function Protocol(GFP) User to User Interface(UUI) Generic Function Protocol(GFP)
③ Show Original A-Number:	I
⑦ Use Original A-Number's Type of Number:	
⑦ Enable Enhanced Sent A-Number Conversion:	
⑦ Use ETSI Diversion Supplementary Service:	
Basic	

14. Repeat steps 7 through 11 for the PBX main number.

15. On the confirmation page, click **Done**.

TLS and SRTP Configuration on MX-ONE

If TLS is required, the following conditions have to be met:

- The MX-ONE FQDN has to be properly defined on the Domain Name Server (DNS).
- The InAttend server has to trust the Certificate Authority (CA) that signed the certificate.

NOTE:

- Certificate handling for MX-ONE is not covered in this document. Please refer to the Certificate Management document in the MX-ONE product documentation.
- FQDN of InAttend Server should be added in etc/hosts file of MX-ONE server. This is required for FQDN resolving and TLS call to work from MX-ONE to InAttend.

To setup TLS/SRTP in MX-ONE, the proper encryptions licenses has to be loaded in the MX-ONE system.

Configuring TLS on MX-ONE SIP trunks

To configure TLS, do the following:

- 1. On the MX-ONE Service Node Manager main page, click **Telephony** and then click on the **External** Lines tab.
- 2. Click **Route** in the left panel.
- 3. On the Route page, click Add and select "SIP" from the Type of Signalling list.
- 4. On the Route settings, ensure that the following values are set in the Profile Settings:
 - Transport Protocol: TLS
 - Remote Proxy Port: 5061

Initial Setup	Number Analysis	Telephony	Services	System	Tools	Logs	
Extensions	Operator Call	Center Gro	ups Exte	ernal Lines	System Data	IP Phone	e DECT
Route	Route - Ac	ld - Step 4 /	4				
Destination	Profile spec	ific settings					
Corporate Name	<- Back Nex	t -> Apply Car	cel				
Busy No Answer Rerou	ting						
Vacant Number Rerouti	ng ? Profile spec	cific settings			InAttend		
Customer Rerouting	Remote Prox	y IP:		*	10.211.63.89		
Public Exchange Numb	er Transport Pro	otocol:		*	tls		
Charging	Remote Prox	y Port:		*	5061		
Mobile Direct Access D	est Telephony ->	> External Lines -> De:	r needs to initiate in stination.	n the Number Analysi	s -> Number Series	and it needs to t	be associated with the route in

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

Using TLS v1 instead of SSL v23

To use the TLS handshake method of TLS v1 instead of SSL v23, do the following:

- 1. On the MX-ONE CLI, run the command sudo -H /opt/mxone_install/bin/mxone_maintenance
- 2. From the menu option, select Certificate and click Ok.

lqqqq	qqqqqqdMiVoice MX-ONE	Maintenance Utility on server 'RCG-MXONE.inattendbgl.com'gggggggg	qqqqk
x Mai	in menu for MiVoice M	X-ONE maintenance	х
x lqq	Idadadadadadadadada	addaaaaddaadaaaaaaaaaaaaaaaaaaaaaaaaaaa	qqk x
хх	<pre>package_handling</pre>	Package handling in the system	X X
хх	upgrade	Upgrade MiVoice MX-ONE version	хх
хх	rollback	Rollback MiVoice MX-ONE version	x x
хх	repair	Repair server or ssh keys in system	x x
хх	uninstall	Uninstall complete system, all MiVoice MX-ONE versions	X X
хх	server	Server in system	X X
хх	lim	Lim in system	X X
хх	s by_server	Standby server in system	X X
хх	license	License handling	хх
хх	market	Market setting	X X
хх	diff_serv	Diff serv parameters	X X
хх	bonding	Bonding settings in system	X X
хх	cluster	Cluster handling	X X
хх	d ns_forwarding	DNS forwarding settings	хх
хх	seccheck	Seccheck settings	x x
хх	user	User management in server	хх
хх	webmanagment	Web server config	x x
хх	<pre>addon_software</pre>	Manage addon software	хх
хх	linux_software	Manage SLES software repositories (ServicePacks or Patchpackages)	X X
хх	certificate	Manage Certificates and TLS settings in MX-ONE	хх
хх	media_server	Manage settings for Media server	x x
хх	c assandra_database	Cassandra database handling	хх
хх	more_configuration	Manage settings in linux snmp, ntp, banner, iptables, ssh	хх
x mqq	laaaaaaaaaaaaaaaaaaaaaa		qqj x
х			х
х			x
tqqqq	<u>idadadadadadadadadada</u>	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	qqqq u
х		< <mark>O</mark> K > < Exit >	x
nqqqq	laaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	ddddj

3. In the choose option for certificate menu, select **mxone-tls** and click **Ok**.

MX-ONE Maintenance Utility					
If an enterprise CA or standalone root CA is to be used select 'certificate' to create the CSR and import later the signed certificate. Use also this option if TLS networking shall be used and a CSR shall be signed on another MX-ONE server.					
If neither an enterprise CA nor standalone root CA is to be used select 'auto' or 'root' plus 'server' to create needed certificates.					
The auto option will create and install a certificate with default settings and activate TLS in all servers in the MX-ONE system.					
Choose option for certificate.					
autoCreate and install default certificate and activate TLScertificateManage CertificaterootManage Root CertificateserverManage Server Certificatemxone-tlsManage TLS in MX-ONEmxone-seclevelManage Security level in MX-ONE					
< <mark>OK > < H</mark> elp > < Exit >					

4. In the TLS in MX-ONE menu, select configure-version and click Ok.

MX-ONE Maintenance Utility		
Choose option for TLS	in MX-ONE	
configure-version	Configure MX-ONE TLS version	
c onfigure	Configure MX-ONE to use TLS	
unset	Configure MX-ONE not to use TLS	
compare	Compare MX-ONE TLS files (can be used to check configuration)	
summary	View MX-ONE TLS Summary	
view	View, show if MX-ONE is configured for TLS	
<	OK > < Help > < Back >	

5. The MX-ONE maintenance utility dialog is displayed. From the menu, click Yes.



6. To select the server to configure TLS, select MX-ONE and click Ok.

M	X-ONE Maintenance Utility
Select	server(s) where to configure
MX-ONE	TLS.
[*]	RCG-MXONE.inattendbgl.com -
	< <mark>OK ></mark> < Back >

7. In the TLS version menu, select **TLSv1.1** and click **Ok**.



8. The TLS version successfully configured window is displayed. Click **Ok** to proceed further.



9. The next steps follow the configuration of MX-ONE TLS. To proceed select **MX-ONE to use TLS** option and click **Ok**.


10. In the MX-ONE maintenance utility window select Yes.



11. Select **MX-ONE** and click **Ok** to choose the server to configure MX-ONE TLS.



12. The MX-ONE TLS successfully configured window is displayed. Click **Ok** and execute the below command:

```
reload -u SIPLP, IPLP, TLP65, CSTServer, ConfigServer
```

MX-ONE Maintenance Utility
MX-ONE TLS successfully configured.
Check media encryption settings.
Complete the activation of MX-ONE TLS by reloading the following program units:
reload -u SIPLP, IPLP, TLP65, CSTServer, ConfigServer
<mark>< ○</mark> K >

NOTE: To generate CSR from InAttend Server, see section Generate CSR in ACS.

Configuring SRTP on MX-ONE

NOTE: This configuration requires a media encryption (SRTP) license in the MX-ONE (called VOIP-SECU-RITY).

To configure SRTP, do the following:

- 1. On the MX-ONE Service Node Manager main page, click Telephony and then click on the **IP Phone** tab.
- 2. Click Media Encryption in the left panel.
- 3. On the Media Encryption page, enable the following parameters:
 - Enable Media Encryption for IP Extensions
 - Enable Media Encryption for IP Trunks

Initial Setup	Number Analysis	Telephony	Services		System	Tools	Logs	
Extensions	Operator	Call Center	Groups	Externa	al Lines	System Data	IP Phone	DECT
Administrator	Media	Encryption						
Security Policy	Apply							
Telephony Domain								
SIP Domain	⑦ Enable	e Media Encryption for I	P Extensions:	4				
SW Server	⑦ Enable	e Media Encryption for I	P Trunks: ntor Modia Gatoway:	// I				
Connect Configuration	n File	e Hedia End ypdon for 1	inter media Gateway.					
Configuration File	Apply							
Unregistration								
Media Encryption								

4. Click Apply to save your changes.

Configuring Day/Night Service Positions

You can configure Day and Night service positions for the public or private trunk lines to InAtttend. You have to first initiate the abbreviated numbers series, then initiate the abbreviated numbers.

Initiating the abbreviated number series

To initiate the abbreviated number series, do the following:

- 1. On the MX-ONE Service Node Manager main page, click **Number Analysis** then click the **Number Plan** tab.
- 2. Click Number Series in the left panel.
- 3. Number Series page select "Internal numbers" in Number Series Type field, click Next.



4. On the Internal Number Series page, enter the Abbreviated numbers (in this example, 700 and 701) in the **Common Abbreviated Numbers** field, and then click **Apply**.

Initial Setup	Number Analysis		Telephony	Servio	ces Sys	tem Tools
Number Plan	Call Diversion		Call Discrimination		Emergency N	umber
Number Series	N	umber Se	eries - Add -	Step 2	2 / 2	
Service Codes						
External Number Length		Back	t -> Apply Ca	ncel		
Number Conversion		Internal Num	ber Series			
Number Conversion Uple	oad 🕐	Directory Nur	mbers:]
System Numbers	?	Common Ope	erator Numbers:			
	?	Individual Op	erator Numbers:			
	?	Common Abb	reviated Numbers:	700,701		

Click the External Number Length tab on the left side.

Initial Setup	Number Analysis	Telephony	Services	System
Number Plan	Call Diversion	Call Discrimination	on Emer	rgency Number
Number Series	External	Number Lena	th - Add	
Service Codes	Apply Ca	incel		
External Number Leng	gth			
Number Conversion	⑦ External	Number: * 08		
Number Conversion U	Ipload ⑦ Minimum	Length: * 2		
System Numbers	J Plaximum	z z		

Enter the minimum and maximum length details and click Apply.

Initiating the abbreviated numbers

To initiate the abbreviated numbers, do the following:

- 1. Click **Telephony** and then click on the **Extensions** tab.
- 2. Click Common Abbreviated Number in the left panel and click Add.
- 3. In the Common Abbreviated Number page, select the abbreviated number interval and click Next.

Initial Setup	Number Ana	ilysis Telep	hony	Services	System	То
Extensions	Operator	Call Center	Group	vs Exte	ernal Lines	Syste
Account Code	Co	mmon Abbre	viated N	umber - A	dd - Step	1/2
Common Category						
Common Service P	rofiles <-	Back Next ->	Apply	Cancel		
Common Abbreviat	ed Number	Customer Name:			None M	
Common Authoriza	tion Code 💿	Available Common At	breviated Nur	nber Intervals:	700-701 V	
Force Mobile Throu	gh PBX					

4. Enter the Operator number (09 in this example) in the **Translated number** field and select all **Traffic Classes**.

Initial Setup	Number	Analysis	Telephor	iy .	Servi	ces System	Tools
Extensions	Operator	Call	Center	Groups		External Lines	System
Account Code		Common	Abbrevia	ted Nu	mbe	er - Add - Step	2/2
Common Category							
Common Service Profile	es	<- Back	Next -> A	pply Ca	ncel		
Common Abbreviated N	lumber	() Common	Abbreviated Nu	mber	6	700 9	
Common Authorization	Code	 Common 	Abbreviated Na	me:	ľ	00 0	1
Force Mobile Through R	РВХ	Translated	d Number:		• [19]
Delay Seizure List		Common /	Abbreviated Nu	mber Class:	•	☑ Traffic Class 0 ☑ Traffic Class 1 ☑ Traffic Class 2 ☑ Traffic Class 3	
		⑦ Do Not Di	splay Translated	I Number:	[

- 5. Click **Apply** to save your changes.
- 6. Repeat steps 1 through 5 for the PBX main number

(for example, Abbreviated Number 701, Translated Number 55000).

Initiating Day and Night Service Positions for a private route (internal call queue)

Do the following:

- 1. Click **Telephony** and then click on the **External Lines** tab.
- 2. Click Busy No Answer Rerouting in the left panel and then click Add.
- 3. On the Busy No Answer Rerouting page, select a private route from the drop-down list in the **Route** field and click **Next**.

Initial Setup	Number Analys	is Telepho	ony Servi	ices Sy	vstem
Extensions	Operator	Call Center	Groups	External Lii	nes S
Route	Busy I	No Answer Re	erouting - A	dd - Step	1/2
Destination				-	-
Corporate Name	<- Back	Next -> App	oly Cancel		
Busy No Answer Rero	outing	Name: Private Per		Edit	
Vacant Number Rero	uting			Luit	
Quetemor Derouting					

4. Enter the Abbreviated number for the internal call queue in the **Common Day Number** and **Common Night Number** fields.

Initial Setup	ial Setup Number Analysis		hony S	ervices S	ystem
Extensions	Operator	Call Center	Groups	External L	ines
Route	Busy	No Answer I	Rerouting ·	- Add - Step	1/2
Destination				-	
Corporate Name	<- Back	Next -> A	opply Cancel		
Busy No Answer Ren	outing	Names Estargal	Pouto 1 M		
Vacant Number Rero	outing	e Name.	Vie Vie	w Edit	
Customer Rerouting					
Public Exchange Nur	mber				

5. Click Apply to save your changes.

Initiating Day and Night Service Positions for a public route

To initiate Day and Night Service Positions for a public route (external call queue), do the following:

- 1. Click **Telephony** and then click on the **External Lines** tab.
- 2. Click Busy No Answer Rerouting in the left panel and then click Add.
- 3. On the Busy No Answer Rerouting page, select a public route from the drop-down list in the **Route** field and click **Next**.

Initial Setup	Number Anal	ysis Teleph	nony Serv	ices	System	Tools
Extensions	Operator	Call Center	Groups	External	Lines	System Data
Route	Busy	No Answer F	Rerouting - A	dd - Ster	2/2	
Destination						
Corporate Name	<- Bac	ck Next -> A	pply Cancel			
Busy No Answer Re	erouting	the Manual	Colored Barder I			
Vacant Number Re	routing ⑦ Con	nmon Day Number:	701 G	Common Ni	ht Number:	701
Customer Rerouting	9					
Public Exchange N	umber	iced				

4. Enter the Abbreviated number for the external call queue in the **Common Day Number** and **Common Night Number** fields.



5. Click Apply to save your changes.

Configuring Direct Drop

To enable the MX-ONE to allow ACS to call/transfer to other ACS application numbers like Direct Drop, Private or Public Operator queues you must perform the following:

- 1. On the MX-ONE Service Node Manager main web page, click **Tools** and then click on the **Command** Line tab.
- 2. In the Command field, type ASPAC: PARNUM=118, PARVAL=0;

NOTE: If the PARVAL is set to 1, the call cannot be transferred from one operator to another operator individual queue.

🕅 Mitel	Service Node Manager	Logged in as: mxone	About User Guide
Command: 20 Latest Commands:	aspac:parnum=118,parval=0; Appl <select commands="" previous=""> V</select>	ly	<u>Help</u>
Input File:	Ignore error Execute Stop Pause Resur	se ne Clear Win	dow Close Window

3. Click Apply to save your changes.

Simplified Configuration for MiV5000 since R7.2

The following information describes necessary configuration tasks on MiVoice 5000 to integrate with InAttend. For detailed information about MiVoice 5000 configuration, refer to the MiVoice product documentation.

This flow illustrates the approach that you must follow to configure and integrate MiVoice 5000 and InAttend.



NOTE: Micollab is scheduled to be supported in the next Service Pack release of InAttend. The content in this section is pertinent post formal announcement of InAttend service pack 1 (2.5.1).

The configuration steps described in this section are examples based on the following constraints:

- Local Dialing on 4digits
- Dial plan for the country (France)
- Mono Call Distribution

- Three Queues
 - Internal 8100
 - External 8101
 - Return 8102
- Two InAttend clients
 - softphone 8103
 - hardphone 7311
- One IID number 0130964955 (one call distribution number)

Related Sections

Configure Directory Server (MiVoice 5000) Configuring a PBX link for line state (MiVoice 5000) MiCollab and InAttend with MiV5000 Appendix A: Configuring telephony services in TCA

Direction Names

You must modify the private direction LIA0 and set to free numbers 81* for InAttend. Go to **Dialing Plan** > **User dialing plan** > **Access to directions** > **Access to LIA0** and enter **80** in **Access code** field. **NOTE:** By default, 8 allows access to LIA0, changing access code to 80 will allow 81* numbers.

Web Admin home Subscribers	Access to LIAO Telephony service>Dialing plan>User dialing plan>Access to directions (3.2.4) 🚢 🖪 🗞 🏠 📮 📮 🖺 😫 🕑
System Dialing plan	Access restriction, belongs to AREA A
Access to directions Access to LIA0	Tone after access code NO Password request NO
Network and links Reception	Length of next number 4
Voice mail and tones Fast links	Specific numbers

Create a private direction for InAttend, for example **DINATT** as private direction for InAttend.

- 1. Go to Dialing Plan > Direction names.
- 2. Enter DINATT in **Private direction 2**.

In this screenshot example, LIA0 is already defined as Private direction

Web Admin home	Direction names		<u> </u>	~ =		n =	ī.	L.
Subscribers	Telephony service>Dialing plan>Direction names (3.1)	🌤 L§ N		n) 🛶	÷1		ц.	E
System	PSTN incoming	RESEAU	_					
Dialing plan	Local outgoing /81h	NATIONAL						
Direction names	Regional 1 outgoing /82h		٦.					
Network and links	Regional 2 outgoing /86h		٦.					
Reception	Regional 3 outgoing /87h		ī.,					
Voice mail and tones	Regional 4 outgoing /88h		٦.					
Fast links	Regional 5 outgoing /89h	DOM	ī.,					
	Regional 6 outgoing /84h		Ξ.					
	Regional 7 outgoing /85h		1					
	International outgoing /83h	INTER	1					
	Emergency calls /8bb	URGENCE	÷.					
	energency cars your	ondenide						
	Direct paging							
	Auto paging Internal calls							
	Auto paging External calls							
	Consultation call over trunk							
	Circuit packet coupler							
	Operators							
MV5000-R6.3 /AE00 FRA	Significant dial numbers		٦.					
Site: 002-SITE LOC	Voice mail							
CSTA SERVER 0: CONNECTED								
09/03/17 22:12:11	Private direction 1	LIA 0				_		
* CSTA SERVER 0: LINK IN FAULT	Private direction 2	DINATT						
· CSTA SERVER 0: CONNECTED	Private direction 3				-	_		

- 3. Go to Dialing Plan > User dialing plan > Access to directions > Access to DINATT.
- 4. Select AREA A from Access restriction belongs to drop-down list.
- 5. Enter 81(4) in the Specific numbers. This allows access to the private direction.

Here 81 is the prefix for InAttend calls, and 4 is the length of the number that can be configured. For example: 81-2000

Web Admin home	Access to DINATT 🖉 🔍 🖎 🖪 🖪 🖽 😫 🗔 (Ŧ
Subscribers	Telephony service>Dialing plan>User dialing plan>Access to directions (3.2.4)	_
System	Access restriction, belongs to AREA A	
Dialing plan User dialing plan	Access code	î
Access to directions Access to DINATT	Specific numbers	
Network and links		
Reception		
Voice mail and tones		
Fast links	5	

Call Distribution Management

This management domain is all about managing incoming calls according to :

- Timeslot (according to a calendar)
- Call origin (PSTN, TL or internal)
- Call number (special treatment for DISA number, for instance).

It also defines:

- The operator services on which incoming calls are distributed
- Interactive voice server (IVS) scripts
- DISA scripts
- DID corporate numbers.

The columns differ according to type of system: Mitel 5000 Gateways or MiVoice 5000 Server.

Programming Call Distribution for InAttend Services

You must define the call distribution for Inattend services, in the **Telephony Services > Web Admin > Reception > Call distribution management characteristics**. This menu is used to configure and display the different call distribution options available on the iPBX.

NOTE: All the given configurations are not multi-company. For a multi-company configuration, use **Display by company** option.

Three Queues are configured in InAttend Services

- For Internal Queue select Queue name INT INATTEND and select Day Routed to # as 8100
- For External Queue select Queue name EXT INATTEND and select Day Routed to # as 8101
- For Return Queue select Queue name RTRN INATTEND and select Day Routed to # as 8102

Web Admin home Subscribers	C.dist.ACC.0 Telephony service>Reception>Call distribution	on management>Characteristics (5.1.1)	🛎 🖪 🛇 🍙	■
System	<< <	1	2 3 4	>>>
Dialing plan Network and links	Names Definition Users	By its name ACC.0	0 •	
Call distribution management Characteristics Voice mail and tones Fast links		Call dist. 0 ACC.0 Call dist. 1 INT INJ Call dist. 2 EXT IN Call dist. 3 RTRN I	ATTEND IATTEND INATTEND	A III

To configure queue:

1. In canonic configuration, the prefix to reach the attendant service is 9. It is configured in the **User** dialing plan > Operator Call.

This prefix is used by all the subscribers irrespective of company or department.

Web Admin home	Company/department settings 🖉 🖪 🖪 🖎 🛆 🖻 🖪 🖪 🔄 😫 🖬 🖼
Subscribers	Telephony service>Subscribers>Hunt groups and companies>Multi-company management>Company/department settings (1.3.6.7)
Hunt groups and companies Multi-company management	Company name STE 0
Company/department settings	
System	Select the item
Dialing plan	
Network and links	
Reception	
Voice mail and tones	
Fast links	

2. The number that should be reached when InAttend is not available, should be configured in the MMI / Call Distribution Management.

NOTE: It can differ based on company and department.

- 3. Enter a number for **Night route to**. For defense cases (this number is reached when InAttend is not available)
- 4. Enable the call distribution by external, the InAttend service is reached through SIP trunk.
- 5. Set the Reference calendar to DAY mode.

NOTE: Calendars are handled by InAttend.

6. Set Day route value to 8100, this is the number for internal calls queue on InAttend.

Web Admin home Subscribers System Dialing plan Network and links	C.dist.INT INATTEND Telephony service>Reception>Call distribu Names Definition Users	ution management>Characteristics (5.1.) By its name States	I) 🚣 🖪 🛇	☆ ☞ ₽ ₽ ₽ 目 目 目 目
Reception Call distribution management Characteristics Voice mail and tones Fast links	Calendar associated should be always in DAY mode ; calendar are handled by InAttend	Day: routed to or to directory number Reduced:routed to or to directory number Night: routed to or to directory number Reference calendar	2100 CAL 1	For defense cases (this number is reached when InAttend is not available) The InAttend service is reached through SIP
	8100 = Number of « internal calls » queue on InAttend side	Call distr. authoriz. by exterior Day: routed to # Reduced:routed to # Night: routed to #	YES 8100	turnk, so can distribution by external should be enabled.

NOTE:

- a. For external returned queue, Direct DDI calls are presented to subscribers. If the user is not reachable (busy or does not answer), the call returns to the distribution management associated to the company of the user.
- **b.** For the internal and returned calls, the call distribution management depends on the company or the department of the subscriber.

DID Corporate Numbers

The number to reach attendant service from external network is declared as **Answering service**. Several answering services can be declared (one for Inattend service and others for specific call distribution services.)

For the internal and returned calls, the call distribution management depends on the company/department of the subscriber.

	Web Admin home Subscribers System Dialing plan Network and links	Answering services Telephony service>Reception Click here	Answering services (5.5) Number Co	😩 💽 🛇 🏠 🛸 💭 🕒 🗐 🖄 😫 🗹 🛛
()	Web Admin home	Answering services		
	Subscribers	Telephony service>Receptio	n>Answering services (5.5)	
	System		Received digits	4955
	Dialing plan		Cneck no overcharged	
	Network and links		Free announcements	
	Reception Answering services Answering services		Company Department	*****
	Voice mail and tones		Routing	CALL DIST
	Fast links		Call distribution Handled according to calle	
	Web Admin home	Appropriate convictor	-	
	Subscribers	Telephony service>Reception>Answering	a services (5.5)	🚢 💽 🛇 🎧 💐 🗅 🗎 🗐 🗳 🗹
	System		Number Compar	y Dept Handled by
~	Dialing plan		1 4955 *******	****** EXT INATTEND
	Network and links		2	
	Reception		3	

SIP Trunk Configuration

The ^{Solution} icon is used to change the configuration of a SIP trunk, you must use the **Advanced mode** for the SIP Trunk configuration.

Use the MiVoice 5000 Service Node Manager to configure Mi Voice 5000 for SIP trunking.

Add a SIP Trunk for InAttend

- 1. Navigate to Web Admin > Network and Links > Network > Trunk groups.
- 2. Enter the Trunk group names.

Web Admin home	Trunk group names 🐣 🖪 🕓 🛆 🖻
Subscribers	Telephony service>Network and links>Network>Trunk groups>Names (4.2.1.1)
System	Trunk group 1 FX.SIP
Dialing plan	Trunk group 2 FINATT
Network and links	Trunk group 5
Network	Trunk group 4
Names	Trunk group 5
Reception	Trunk group 6
Voice mail and tones	Trunk group 7
Fast links	Trunk group 8
	Trunk group 9

- 3. Set the signaling characteristics for the trunk group:
 - a. Select VOICE IP from the Physical Type drop-down list.
 - b. Select BOTHWAY from the Nature drop-down list.
 - c. Select SIP as the Signaling Type, from the drop-down list.
 - d. Select InAttend form the Subtype drop-down list.

Web Admin home Subscribers System Dialing plan	Characteristics of trunk grou Telephony service>Network and links>	up FINATT Network>Trunk groups>Characte Signaling characteristics:	ristics (4.2.12)
Network and links Network Trunk groups Characteristics Characteristics of trunk group FINATT		Physical type Nature Signalling type Subtype	VOICE IP
Reception Voice mail and tones Fast links		Char	acteristics

4. Click **Characteristics** and select the trunk protocol as TCP or TLS.

NOTE: UDP is not supported as trunk protocol between MiVoice 5000 and InAttend server.

SIP Trunk configuration in TLS/SRTP

NOTE: TLS/SRTP is available only since MiVoice 5000 7.1. It is used to secure the communication between MiVoice 5000 and InAttend.

NOTE: TLS is not supported on Mitel 5000 Gateways.

- a. Set TLS as the protocol from the Protocol drop-down list.
- b. Secure the SIP trunk with InAttend, a trusted certificate is mandatory for securing.
- Ilf the default SIP profile (used by the SIP terminal) uses a trusted certificate, it can be used for the InAttend trunk group. No specific TLS profile need be created for InAttend.
- If the default SIP profile uses a self-signed certificate, you must create a TLS profile for the InAttend trunk group.

To create a TLS profile for the InAttend trunk group:

i. Go to PBX MMI Telephony service > System > Security > Additional TLS profiles (2.4.2).Click the Names tab and create a TLS profile.

Additional TLS profiles : InAttend Telephony service>System>Security>Additional TLS profiles (2.4.2)	
Names Settings Users	By its name InAttend 🗸
	Profile 1 InAttend
	Profile 2
	Profile 3
	Profile 4
	Profile 5
	Profile 6
	Profile 7
	Profile 8
	Profile 9
	Profile 10

 ii. Click the Settings tab and configure either the Server port or Port/FQDN to be used for trunk connections. Configure the other parameters such as Security level, Type and Both way (MTLS).

Additional TLS profiles : InAttend Telephony service>System>Security>Additional TLS profiles (2.4.2) Names Settings Users	By its nar	ne InAttend 🗸
	Security level Type Both way (MTLS) Port/FQDN Server port	High v Client/server v v 5071 v

To assign the trusted certificate to the TLS profile:

Go to **Certificate management MMI 2.4.1.** Click the **Servers certificates assignment** tab and assign the trusted certificate to the TLS profile created in the preceding step b.

Certificates m Telephony services	nanagement »System»Security>Certificates management (2:	4.1)			
Certificates	Servers certificates assignment	Clients certificates as	ssignment C	ertification authorities	Revocation
			Available c	ertificates	
		Use	Name	Valid from	Valid until
		Inter-site Link	<u> </u>		
		WebAdmin	SelfSignedSH	HA2 22/06/20 19:46	5 20/06/30 19:46
		User Portal	SelfSignedSH	HA2 22/06/20 19:46	5 20/06/30 19:46
		Internet Gateway			
		SIP	SelfSignedSH	HA2 22/06/20 19:46	5 20/06/30 19:46
		LDAP server	SelfSignedSH	HA2 22/06/20 19:46	5 20/06/30 19:46
		InAttend	inattend_acs	_p12 26/06/20 19:25	26/06/21 19:25
		Profile Name	Trusted certi	ificate	

To assign the TLS profile to the SIP trunk configured with the InAttend server:

Go to PBX MMI **Telephony service > Network and links > Network > Trunk groups > Characteristics** (4.2.1.2) and select the TLS profile (configured in the preceding steps) in the trunk configuration.

FINATT VOICE IP BOTHWAY (advanced mode)			
Telephony service>Network and links>Network>Trunk groups>Characteristics (4.2.1.2)			
Signalling type	SIP		
Link state	CONNECT.		
Company	STE 0 🗸		
Department	SERV 0 V		
Protocol	TLS 🗸		
with TLS profile	InAttend 🗸		
Proxy n° 1	inattendserver.blrmivo5k.com		
- port	5061		
Proxy n° 2			
Domain / realm			
Local proxy	NO 🗸		
Proxy checking	····· ~		

c. Enter the proxy of InAttend server and port as 5061.

TRUNK71 VOICE IP BOTHWAY	
Telephony service>Network and links>Network>Tru	nk groups>Characteristics (4.2.1.2)
Signalling type	SIP
Link state	CONNECT.
Company	STE 0 🔻
Department	SERV 0 V
Protocol with TLS profile	TLS •
Proxy n° 1	10.211.210.77
- port	5061
Proxy n° 2	

d. Once the protocol is set to TLS, **SRTP support** option gets enabled. By default, the value is set to **SRTP preferred**.

elephony service/network and unks/network.	
REFER sending	
Support of video	
Support of T.38	
Support of other medias (IM, etc)	
SRTP support	SRTP preferred v
	SRTP preferred
Bearer type incoming	SRTP only
Calls from	SRTP disabled
Priority calls if transit	
Search DID numbers	

e. SRTP support can be disabled by either selecting SRTP disabled from the drop-down list or by disabling the voice ciphering check box from PBX MMI Telephony service >Network and links >Quality of service >Ciphering and IP settings.

Make sure that the generic parameter **Ciphering and IP settings** is general to enable/disable SRTP on all the endpoints. SRTP support can be disabled selecting SRTP disabled on the SIP Trunk

This parameter MUST also be set to enable SRTP between MiVoice 5000 and InAttend.

Ciphering QoS Advan	red Qo5	
	Signalling and voice ciphering	
	voice ciphering	
	Voice ciphering (i7xx)	
	function state	IN SERVICE
	updated on: 06/09/18 18:2 master site: 022-SITE22	5 ed: 4 node: 3
	working mode	SLAVE 🔻
	encryption	ALLOWED .
	Hash generation	NO Y
	- Files upload path	/5363a22ae6e214e933abfc86417a7756/ftp_67xxi

NOTE: SelfSigned certificate is not supported by InAttend.

SIP trunk configuration in TCP

- a. Set the protocol as TCP from the drop-down list.
- b. Enter the proxy of InAttend server and port as 5060.

Telephony service>Network and link	(s>Network>Trunk groups>Characteristics (4.2.1.2)
Signalling type	SIP
Link state	DISCONNECTED
Company	STE 0 V
Department	SERV 0 V
Protocol	TCP V
Proxy n° 1	10.211.210.77
- port	5060
Proxy n° 2	
Domain / realm	

NOTE: With TCP as trunk protocol, SRTP support option is unavailable in trunk configuration.

- 5. Configure the FINATT Voice IP:
 - a. Enable the Name Management check-box.
 - b. Select SEND ONLY from the On hold management drop-down list.
 - c. Enable the Re-invite without allowed SDP.
 - d. Select **DINATT** from the **Calls from** drop -down list.
 - e. Enable REFER SENDING check-box.
 - f. Select Disabled from Transfer to drop-down list.
 - g. Enter the IP for CAC IP Address.

Web Admin home	FINATT VOICE IP BOTHWAY (advar	nced mode)	
Subscribers	Telephony service>Network and links>Network	Trunk groups>Characteristics (4.2.1.2)	
System	Identity reception management:		
Dialing plan	- calling Id. in	PAI or PPI or RPID -	
Network and links Network Trunk groups Charactensitics Characteristics of trunk group EINATT VOICE IP BOTHWAY	Name management Forwarding management: - on busy / immediate forward forward on portugation		
Recention	- Torward on no answer		
Voice mail and tones	Voice mail		
Fast links	Local generation of tones On hold management - force IP address to 0 Support PRACK (100rel) Tones management before answer - support P-Eatly-Media Re-invite without allowed SDP Reject 1.38 REFER sending	SEND ONLY	
MV5000-R6.3 /AE00 FRA Site: 002-SITE LOC	Support of Video		
9/03/17 22:13:06 CSTA SERVER 0: CONNECTED	Support of other medias (IM, etc)		
CSTA SERVER 0: LINK IN FAULT 9/03/17 22:11:50 CSTA SERVER 0: CONNECTED	Bearer type incoming Calls from	CCBT+CCBNT	

Web Admin home	FINATT VOICE IP BOTHWAY (advanced mode)	
Subscribers	Telephony service>Network and links>Network>Trunk groups>Characteristics (4.2.1.2)	"■ [\$ ∨ 107 "+ +) [
ystem		
ialing plan	REFER sending	
etwork and links		
letwork	Support of video	
Trunk groups	Support of T 38	
Characteristics of trunk group	Support of other medias (IM_etc.)	
FINATT VOICE IP BOTHWAY	Support of other medias (m, etc)	
eception	Bearer type incoming CCBT+CCBNT -	
pice mail and tones	Calls from DINATT	
ist links	Priority calls if transit	
	Search DID numbers	
	- incoming digit translator number	
	- reject of numbers not assigned	
	Pro approving moreage caller charged	
	if called party free or hum 1	
	- Il called party free of busy 1	
	- If called party busy 2	
	- If number not assigned	
	Iransf. acc. to called ptv comp-dept	
	Transfer to Disabled	
	Truck group id (tel. record)	
	Irunk group monitoring	
MV5000-R6.3 /AE00 FRA Site: 002-SITE LCC	Max. nb of simultan, calls allowed	
03/17 22:13:06	CAC IP address 10.148.66.100	
STA SERVER 0: CONNECTED	Centre - CAC class	
STA SERVER 0: LINK IN FAULT	Centre - Cho class	
03/17 22:11:50	G711 Foread in made EAV/Medam	
STA SERVER 0: CONNECTED	G/11 Torcea in mode FAX/Modem	

Create SIP Routes

A route and a specific direction are associated to InAttend and an access code is defined in the user dialing plan.

- 1. Go to, Web Admin > Network and Links > Network > Routes.
- 2. Select **DINATT** from the **To direction** drop-down list.
- 3. Select FINATT from the On trunk group drop-down list.
- 4. In the Tx DINATT DIRECT 0 on FINATT set the required type.

What to do Next

Perform the following list of operations to successfully complete AID and IID configurations.

Transfer Authorization

To allow transit calls between Network calls and InAttend:

- 1. Go to the Subscribers > Rights > General settings.
- 2. Click the **Rights** tab and select **TK TK** and **TK TL** check-box.
- 3. Select LIST NOT USED from the Config trunk groups drop-down list.

Web Admin home Subscribers	Subscribers m	niscellaneo	ous setting	gs al settings (1.4.1)	100		🛎 🖪 🛇 🍙 🗣 🗛 🖳
Rights General settings	Subscriber	System	Rights	Application	Network	Security	
System Dialing plan			Fort	idding of gener	al call pick u		
Network and links			Fun	ction conferenc	e		
Reception			- 1k	nd tone			
Fast links			Forv	varding to TL su	bject to right	: 🗆	
			Trar	isfer authorizati	on		
			- TK	TK		 ✓ 	
			Co	nfig trunk group)S	LIST NOT	T USED 🔽
			- by - be	subsc. without	restriction s		
			- be	tween room set	s via op. con	s. 🗆	
			- via	op. cons. to pr	e-payment s	ets 🗌	
			- of - to	personal call set with PSTN a	ccess allowe	d 🗌	

Configure Hardphone Subscriber

1. Go to Subscriber > Subscription > Characteristics, select REFUSED from the Call waiting drop-down list.

Web Admin home Subscribers	Subscriptions 7311 Telephony service>Subscrit	pers>Subscription	s>Characteristics	(123)		🚢 🖪 🛇	6 R D D
Characteristics	Characteristics	Directory	Terminals	Keys	Forwards	Home automation	Phone book M
System Dialing plan Network and links Reception Voice mail and tones Fast links		Right to PC Logi Master of Pre-emp Use of E Call wai Return t External Assistan Announ	ciphering n only of conference ptive rerouting DISA function ting to console on a forwarding all t forwarding a cement list ca	spec. tim lowed llowed		JSED	S

Create an External Record

 Go to, Internal Records and click Add an external contact to create a new external record. An external record number must be added with the Internal Queue number Name STD_INATTEND IN ORDER to display STD_INATTEND when INATTEND CLIENT CALLS a LOCAL SUBSCRIBER

Web Admin home	Add an exte	mal contact						
nternal records	* A B C	DEFG	HIJKL	M N O P	QRS	Т	UVWX	X Y Z
External records	Name	Firstname	Localisation	N°abbrev	Number		Email	
Customization	EXT_3003			0	130963003			~
	INT_INATTEN	V		8	100			
	MITEL		Guyancourt	0	1309642000)		
	STD_INATTEI	N		9)			
	<							
	<							
	< Display v							
	Cisplay V Gender :			Nu	mber :	9	Confidentia	lity : Green list
	▼ Display ✓ Gender : Name :	STD_INATI	TEND	Nu Nº:	mber : abbrev :	9	Confidentia Hierarchy(s	lity : Green list
	€ Display ✓ Gender : Name : Firstname :	STD_INATT	TEND	Nu Nº: Loo	mber : abbrev : calisation :	9	Confidentia Hierarchy(s Email :	llity : Green list

Create Password

Create a password for InAttend account to access proxyldap

1. Go to Subscribers > Directory > Settings > Users accounts and set password for clients.

Web Admin home	Users accounts		
Subscribers	Telephony service>Subscribers>Directory>Settings	>Users accounts (1115)	
Directory	i2070 :		
Users accounts	- login	i2070	^
System	- password	*****	
Dialing plan	• 12 10 20 10 10 10		
Network and links	TWP :		
Reception	- login	twp	
Voice mail and tones	- password	**********	
Fast links			
	CC :		
	- login	acp	
	- password	*****	
	MICOLLAB ·		
	- login	MiCollab	
	login		
	- password		
	UC360 :		
	- login	UC360	
	- password	****	
	LIEESIZE -		
	- login	Lifesize	
	- nassword		
	- password		
	A340W :		
	- login	A340w	
MV5000-R6.4 RC /A501 FRA Site: 002-SITE LOC	- password		
30/05/17 17:55:29	INATTEND ·		
* CSTA SERVER 0: LINK IN FAULT	- login	InAttend	
* CSTA SERVER 0: CONNECTED	* password	****	
30/05/17 16:08:32	- password		V

Configuration for MiVoice 5000

The following information describes necessary configuration tasks on MiVoice 5000 to integrate with InAttend. For detailed information about MiVoice 5000 configuration, refer to the MiVoice product documentation.

This flow illustrates the approach that you must follow to configure and integrate MiVoice 5000 and InAttend.



NOTE: Micollab is scheduled to be supported in the next Service Pack release of InAttend. The content in this section is pertinent post formal announcement of InAttend service pack 1 (2.5.1).

The configuration steps described in this section are examples based on the following constraints:

- Local Dialing on 4digits
- Dial plan for the country (France)
- Mono Call Distribution
- Three Queues
 - Internal 8100
 - External 8101
 - Return 8102
- Two InAttend clients
 - softphone 8103
 - hardphone 7311
- One IID number 0130964955 (one call distribution number)

Related Sections

Configure Directory Server (MiVoice 5000) Configuring a PBX link for line state (MiVoice 5000) MiCollab and InAttend with MiV5000

Appendix A: Configuring telephony services in TCA

NOTE: This configuration is fully compatible with MiVoice 5000 release 7.2 and upper, and it will be kept in case of any upgrade from an older release.

NOTE: This configuration is also needed if a specific plan must be used to declare InAttend.

Direction Names

You must modify the private direction LIA0 and set to free numbers 81* for InAttend. Go to **Dialing Plan** > **User dialing plan** > **Access to directions** > **Access to LIA0** and enter **80** in **Access code** field. **NOTE:** By default, 8 allows access to LIA0, changing access code to 80 will allow 81* numbers.

Web Admin home	Access to LIAO
Subscribers	Telephony service>Dialing plan>User dialing plan>Access to directions (3.2.4) 🐃 🐚 💟 🖾 🖏 🎝 🖾 👘 🖓 🔛
System	Access restriction, belongs to AREA A 🖵
Dialing plan	Access code 80
Access to directions	Tone after access code NO 💌
Access to LIA0	Password request NO 💌
Network and links	Length of next number 4
Reception	Direction obtained on time-out NO
Voice mail and tones	Specific numbers
Fast links	1

Create a private direction for InAttend, for example **DINATT** as private direction for InAttend.

- 1. Go to Dialing Plan > Direction names.
- 2. Enter DINATT in **Private direction 2**.

In this screenshot example, LIA0 is already defined as Private direction

Web Admin home Subscribers System Dialing plan Direction names	Direction names Telephony service>Dialing plan>Direction names (3.1) PSTN incoming Local outgoing /81h During of the service /02b	RESEAU NATIONAL	> ·	ሬ	4	ום	C, I	
Network and links Reception	Regional 2 outgoing /82h Regional 2 outgoing /86h							
Voice mail and tones Fast links	Regional 5 outgoing /8/h Regional 4 outgoing /88h Regional 5 outgoing /89h	DOM						
	Regional 6 outgoing /84h Regional 7 outgoing /85h International outgoing /83h	INTER.						
	Emergency calls /8bh	URGENCE						
	Direct paging Auto paging Internal calls							
	Auto paging External calls Consultation call over trunk							
	Circuit packet coupler Operators							
MV5000-R6.3 /AE00 FRA Site: 002-SITE LOC	Significant dial numbers Voice mail							
09/03/17 22:13:06 • CSTA SERVER 0: CONNECTED 09/03/17 22:12:11 • CONNECTED	Private direction 1	LIA O					_	
CSIA SERVER 0: LINK IN FAULT 09/03/17 22:11:50 CSIA SERVER 0: CONNECTED	Private direction 2 Private direction 3	DINATT						

- 3. Go to Dialing Plan > User dialing plan > Access to directions > Access to DINATT.
- 4. Select AREA A from Access restriction belongs to drop-down list.
- 5. Enter 81(4) in the Specific numbers. This allows access to the private direction.

Here 81 is the prefix for InAttend calls, and 4 is the length of the number that can be configured. For example: 81-2000

Web Admin home	Access to DINATT 😤 🖪 😒 🛆 🗷 🖪 🖪 🔄 😫 🕢 🖻
Subscribers	Telephony service>Dialing plan>User dialing plan>Access to directions (3.2.4)
System	Access restriction, belongs to AREA A
Dialing plan User dialing plan	Access code
Access to directions Access to DINATT	Specific numbers
Network and links	
Reception	
Voice mail and tones	3
Fast links	4
	5

NOTE: The number of digits used by InAttend must be equal to the number of digits used by DID on the MiVoice 5000.

Incoming Call Dialing Plan

The incoming call dial plan is used to define the analysis made by the system for incoming calls from the network (DID and TL). This is used to modify and display the incoming call numbering plan.

Access to Public Exchange

This command is used to define access to the transit public network.

- 1. Go to, Dialing Plan > Incoming call dialing plan > Access to public exchange.
- 2. Enter the code to access the PSTN in transit. You should make this access code the same as the one used in the extension plan for simplicity purposes.
- 3. Select NATIONAL from Default direction drop-down list.
- 4. Enter **10** as default length for the extension plan.

Validating with the "Enter" key refreshes the screen and displays the access definition parameters.



Access to Directions

This command assigns to each direction defined for the incoming dial plan.

In InAttend you must configure incoming dialing plan to **International numbers**, **National Numbers**, **Emergency Numbers**, and **Domestic Numbers**.

To configure these dialing plans:

1. Go to, **Dialing Plan > Incoming call dialing plan > Access to direction** and select the direction from the **By its name** drop-down list.

This screen-shot shows an example of incoming dial plan configuration for National numbers.

Web Admin home Subscribers	Direction selection 🐣 🕵 📎 🏠 ጁ 📮 🗅
System Dialing plan	By its name NATIONAL
Incoming call dialing plan Access to directions	Select the item

- 2. Enter specific values for each parameters for the direction that you need to set as incoming dial plan.
 - A prefix
 - A dialing tone after the prefix
 - A dialing length
 - Specific numbers.

This screen-shot shows example of specific numbers for national numbers (for France – same as user dialing plan)

Web Admin home	Incoming plan: access to NATIONAL	4 B S		Ð		1 (ta	1±
Subscribers	Telephony service>Dialing plan>Incoming call dialing plan>Access to o	directions (3.3.3)	-÷	*			0
System	Direction defined downstream of	RESEAU V					
Dialing plan	Length of post number	10					
Incoming call dialing plan	Specific numbers	10					
Access to directions	1	07000-4(14)			٦.		
Network and links	1	07000-4(14)		-			
Pecention	2	0/1-2(")		_			
Neception Vicine and the sec	5	0885(*)					
voice mail and tones	4	10(4)					
Fast links	5	110-1(3)					
	6	113-4(3)					
	7	116(6)					
	8	117(3)		٦			
	9	118(6)		٦.			
	10	12-4(*)		ī			
	11	16(*)		7			
	12	19(*)		=			
	13	30-5(4)		-			
	15	360-4(4)		-			
	14	300-4(4)		4			
	15	3650(4)		-			
	16	3651(14)		_			
MV5000-R6.4 RC /A501 FRA	17	3652-*(4)					
Site: 002-SITE LOC	18	366-*(4)					
END PERIODIC BACKUP *	19	37-9(4)					
9/05/17 22:00:00	20						

The following screen-shot shows example of specific numbers for emergency numbers (for Francesame as user dialing plan)

		w.
Web Admin home	Incoming plan: access to URGENCE	
Subscribers	Telephony service>Dialing plan>Incoming call dialing plan>Acce	ess to directions (3.3.3)
System	Direction defined downstrea	am of RESEAU 🗸
Dialing plan Incoming call dialing plan	Access code	
Access to directions	Specific numbers	
Incoming plan: access to URGENCE	1	112(3)
Network and links	2	115(3)
Reception	3	119(3)
Voice mail and tones	4	15(2)
Fast links	5	17-8(2)
	6	

These characteristics are used by the iPBX to split incoming transit between two directions. You can do this by selecting the direction name.

If other directions require an access code, it can be created from **Dialing Plan > Direction names** and the direction will appear in the drop-down list.

The operator should program the tables for each direction to enable the iPBX to manage call transit.

You must also set incoming dialing plan to access the directions, that is the public network, calls the InAttend Server (Queue, Clients).

- 1. Go to, Dialing Plan > Incoming call dialing plan > Access to directions > Incoming plan: access to DINATT.
- 2. Enter 81(4)in Specific numbers.

Web Admin home	Incoming plan: access to DINATT	
Subscribers	Telephony service>Dialing plan>Incoming call dia	aling plan>Access to directions (3.3.3) 🐚 💙 🕼 🔫 🖓 📭
System	Acces	ss code
Dialing plan	Speci	fic numbers
Access to directions	1	81(4)
Incoming plan: access to DINATT	2	
Network and links	3	
Reception	4	
Voice mail and tones	5	
Fast links	6	
	7	

Call Distribution Management

This management domain is all about managing incoming calls according to :

- Timeslot (according to a calendar)
- Call origin (PSTN, TL or internal)
- Call number (special treatment for DISA number, for instance).

It also defines:

- The operator services on which incoming calls are distributed
- Interactive voice server (IVS) scripts
- DISA scripts
- DID corporate numbers.

The columns differ according to type of system: Mitel 5000 Gateways or MiVoice 5000 Server.

Programming Call Distribution for InAttend Services

You must define the call distribution for Inattend services, in the **Telephony Services > Web Admin > Reception > Call distribution management characteristics**. This menu is used to configure and display the different call distribution options available on the iPBX.

NOTE: All the given configurations are not multi-company. For a multi-company configuration, use **Display by company** option.

Three Queues are configured in InAttend Services

- For Internal Queue select Queue name INT INATTEND and select Day Routed to # as 8100
- For External Queue select Queue name EXT INATTEND and select Day Routed to # as 8101
- For Return Queue select Queue name RTRN INATTEND and select Day Routed to # as 8102

Web Admin home Subscribers	C.dist.ACC.0 Telephony service>Reception>Call distribution	n management>Characteristics (5.1.1)	▲ [] ◇ ☆ ♥ ₽ ⊑ 目 년 년 년
System	<< <	1234	>>>
Network and links	Names Definition Users	By its name ACC.0	•
Call distribution management Characteristics		Call dist. 0 ACC.0 Call dist. 1 INT INATTEND	<u>م</u>
Voice mail and tones Fast links		Call dist. 2 EXT INATTEND Call dist. 3 RTRN INATTEND	

To configure queue:

1. In canonic configuration, the prefix to reach the attendant service is 9. It is configured in the User dialing plan > Operator Call.

This prefix is used by all the subscribers irrespective of company or department.

Web Admin home Subscribers Hunt groups and companies Multi-company management Company/department settings	Company/department settings Telephony service>Subscribers>Hunt groups and companies>Multi-company management>Company/department settings (1.3.6.7) Company name STE 0
System	Select the item
Dialing plan	
Network and links	
Reception	
Voice mail and tones	
Fast links	

2. The number that should be reached when InAttend is not available, should be configured in the MMI / Call Distribution Management.

NOTE: It can differ based on company and department.

- 3. Enter a number for **Night route to**. For defense cases (this number is reached when InAttend is not available)
- 4. Enable the call distribution by external, the InAttend service is reached through SIP trunk.
- 5. Set the **Reference calendar** to **DAY** mode.

NOTE: Calendars are handled by InAttend.

6. Set Day route value to 8100, this is the number for internal calls queue on InAttend.

Web Admin home Subscribers System Dialing plan Natural and links	C.dist.INT INATTEND Telephony service>Reception>Call distribu Names Definition Users	ation management>Characteristics (51: By its name States	1) 😤 🕻 🗞	☆ ☞ ₽ Ե 目 티 티 티 티
Reception Call distribution management Characteristics Voice mail and tones Fast links	Calendar associated should be always in DAY mode ; <u>calendar</u> are handled by InAttend	Day: routed to or to directory number Reduced:routed to or to directory number Night: routed to or to directory number Reference calendar	v 2100 v 2100 CAL1 v	For defense cases (this number is reached when InAttend is not available) The InAttend service is reached through SIP
	8100 = <u>Number</u> of « internal calls » queue on InAttend side	Call distr. authoriz. by exterior Day: routed to # Reduced:routed to # Night: routed to #	YES	trunk, so call distribution by external should be enabled.

NOTE:

- a. For external returned queue, Direct DDI calls are presented to subscribers. If the user is not reachable (busy or does not answer), the call returns to the distribution management associated to the company of the user.
- **b.** For the internal and returned calls, the call distribution management depends on the company or the department of the subscriber.

DID Corporate Numbers

The number to reach attendant service from external network is declared as **Answering service**. Several answering services can be declared (one for Inattend service and others for specific call distribution services.)

For the internal and returned calls, the call distribution management depends on the company/department of the subscriber.

	Web Admin home Subscribers System Dialing plan Network and links	Answering services Telephony servicesReceptionsAnswering services (5.5) Click here
(Web Admin home	Answering services 🖀 🖪 🗞 🗞 🖧 🛤 🗅 🛤 🖄
	Subscribers System Dialing plan Network and links Reception Answering services Answering services Voice mail and tones Fast links	Telephory services ReceptionsAnswering services (5) Received digits 4955 Cneck nb overchargea Free announcements Company Department Routing Call distribution EXT INATTEND Handled according to caller NO
	Web Admin home Subscribers System Dialing plan Network and links Reception	Answering services Telephony services-Receptions-Answering services (5.5) Number Company Dept Handled by 1 4955 3

SIP Trunk Configuration

The **SIP** icon is used to change the configuration of a SIP trunk, you must use the **Advanced mode** for the SIP Trunk configuration.

Use the MiVoice 5000 Service Node Manager to configure Mi Voice 5000 for SIP trunking.

Add a SIP Trunk for InAttend

- 1. Navigate to Web Admin > Network and Links > Network > Trunk groups.
- 2. Enter the Trunk group names.

Web Admin home	Trunk group names 🧶 🖪 🖪 🔿
Subscribers	Telephony service>Network and links>Network>Trunk groups>Names (4.2.1.1) 🐃 🐚 💟 🖬 🖛
System	Trunk group 1 FX.SIP
Dialing plan	Trunk group 2 FINATT
Network and links	типк group 3
Network	Trunk group 4
Names	Trunk group 5
Reception	Trunk group 6
Voice mail and tones	Trunk group 7
Fast links	Trunk group 8
	Trunk group 9

- 3. Set the signaling characteristics for the trunk group:
 - a. Select VOICE IP from the Physical Type drop-down list.
 - b. Select BOTHWAY from the Nature drop-down list.
 - c. Select SIP as the Signaling Type, from the drop-down list.
 - d. Select **STANDARD** form the **Subtype** drop-down list.

Web Admin home	Characteristics of trunk grou	IP FINATT	
Subscribers	Telephony service>Network and links>N	Network>Trunk groups>Characte	ristics (4.2.1.2)
System		Signaling characteristics:	
Dialing plan	-		
Network and links		Physical type	VOICE IP
Network		Nature	BOTHWAY -
Characteristics		Signalling type	SIP
Characteristics of trunk group		Subture	STANDARD
FINATT		Subtype	I STANDARD
Reception	-		
Voice mail and tones		Char	acteristics
Fast links		- Containe	

4. Click Characteristics and select the trunk protocol as TCP or TLS.

NOTE: UDP is not supported as trunk protocol between MiVoice 5000 and InAttend server.

SIP Trunk configuration in TLS/SRTP

NOTE: TLS/SRTP is available only since MiVoice 5000 7.1. It is used to secure the communication between MiVoice 5000 and InAttend.

- a. Set TLS as the protocol from the Protocol drop-down list.
- b. Secure the SIP trunk with InAttend, a trusted certificate is mandatory for securing.
- Ilf the default SIP profile (used by the SIP terminal) uses a trusted certificate, it can be used for the InAttend trunk group. No specific TLS profile need be created for InAttend.
- If the default SIP profile uses a self-signed certificate, you must create a TLS profile for the InAttend trunk group.

To create a TLS profile for the InAttend trunk group:

i. Go to PBX MMI Telephony service > System > Security > Additional TLS profiles (2.4.2).Click the Names tab and create a TLS profile.

Additional TLS profiles : InAttend Telephony service>System>Security>Additional TLS profiles (2.4.2)		
	By its name InAttend 🗸	
Names Settings Users		
	Profile 1 InAttend	
	Profile 2	
	Profile 3	
	Profile 4	
	Profile 5	
	Profile 6	
	Profile 7	
	Profile 8	
	Profile 9	
	Profile 10	

ii. Click the Settings tab and configure either the Server port or Port/FQDN to be used for trunk connections. Configure the other parameters such as Security level, Type and Both way (MTLS).

Additional TLS profiles : InAttend Telephony service>System>Security>Additional TLS profiles (2.4.2) Names Settings Users	By its nan	ne InAttend 🗸
	Security level Type Both way (MTLS) Port/FQDN Server port	High v Client/server v v 5071 v

To assign the trusted certificate to the TLS profile:

Go to **Certificate management MMI 2.4.1.** Click the **Servers certificates assignment** tab and assign the trusted certificate to the TLS profile created in the preceding step b.

Certificates m	hanagement				
Certificates	Servers certificates assignment	Clients certificates a	ssignment C	ertification authorities	Revocation
			Available co	ertificates 🛄 🗸	
		Use	Name	Valid from	Valid until
		Inter-site Link	<u> </u>		
		WebAdmin	SelfSignedSH	A2 22/06/20 19:46	20/06/30 19:46
		User Portal	SelfSignedSH	A2 22/06/20 19:46	20/06/30 19:46
		Internet Gateway			
		SIP	SelfSignedSH	A2 22/06/20 19:46	20/06/30 19:46
		LDAP server	SelfSignedSH	A2 22/06/20 19:46	20/06/30 19:46
		InAttend	inattend_acs	p12 26/06/20 19:25	26/06/21 19:25
		Profile Name	Trusted certif	ficate	

To assign the TLS profile to the SIP trunk configured with the InAttend server: Go to PBX MMI Telephony service > Network and links > Network > Trunk groups > Characteristics (4.2.1.2) and select the TLS profile (configured in the preceding steps) in the trunk configuration.

FINATT VOICE IP BOTHWAY (advance	ed mode)
Telephony service>Network and links>Network>Tru	ink groups>Characteristics (4.2.1.2)
Signalling type	SIP
Link state	CONNECT.
Company	STE 0 🗸
Department	SERV 0 🗸
Protocol	TLS 🗸
with TLS profile	InAttend 🗸
Proxy n° 1	inattendserver.blrmivo5k.com
- port	5061
Proxy n° 2	
Domain / realm	
Local proxy	NO V
Proxy checking	······ v

c. Enter the proxy of InAttend server and port as 5061.

TRUNK71 VOICE IP BOTHWAY					
Telephony service>Network and links>Network>Trunk groups>Characteristics (4.2.1.2)					
Signalling type	SIP				
Link state	CONNECT.				
Company	STE 0 V				
Department	SERV 0 V				
Protocol with TLS profile	TLS •				
Proxy n° 1	10.211.210.77				
- port	5061				
Proxy n° 2					

d. Once the protocol is set to TLS, **SRTP support** option gets enabled. By default, the value is set to **SRTP preferred**.

elephony service>Network and links>Network:	> Irunk groups>Characteristics (4.2.1
REFER sending	
Support of video	
Support of T.38	
Support of other medias (IM, etc)	
SRTP support	SRTP preferred •
	SRTP preferred
Bearer type incoming	SRTP only
Calls from	SRTP disabled
Defenite conflor if the second	

e. SRTP support can be disabled by either selecting SRTP disabled from the drop-down list or by disabling the voice ciphering check box from PBX MMI Telephony service >Network and links >Quality of service >Ciphering and IP settings.

Make sure that the generic parameter **Ciphering and IP settings** is general to enable/disable SRTP on all the endpoints. SRTP support can be disabled selecting SRTP disabled on the SIP Trunk

This parameter MUST also be set to enable SRTP between MiVoice 5000 and InAttend.

Ciphering	QoS Advanced QoS		
		Signalling and voice ciphering	
		voice ciphering	<u>.</u>
		Voice ciphering (i7xx)	
		<pre>function state updated on: 06/09/18 18:26 ed: 4 master site: 022-SITE22 node: 3</pre>	IN SERVICE
		working mode	SLAVE •
		encryption	ALLOWED .
		Hash generation	NO Y
		- Files upload path	/5363a22ae6e214e933abfc86417a7756/ftp_67xx

NOTE: SelfSigned certificate is not supported by InAttend.

SIP trunk configuration in TCP

- a. Set the protocol as TCP from the drop-down list.
- b. Enter the proxy of InAttend server and port as 5060.

TRUNK71 VOICE IP BOTH	WAY
Telephony service>Network and lin	ks>Network>Trunk groups>Characteristics (4.2.1.2)
Signalling type	SIP
Link state	DISCONNECTED
Company	STE O 🔻
Department	SERV 0 V
Protocol	TCP V
Proxy n° 1	10.211.210.77
- port	5060
Proxy n° 2	
Domain / realm	

NOTE: With TCP as trunk protocol, SRTP support option is unavailable in trunk configuration.

- 5. Configure the FINATT Voice IP:
 - a. Enable the Name Management check-box.
 - b. Select SEND ONLY from the On hold management drop-down list.
 - c. Enable the Re-invite without allowed SDP.
 - d. Select **DINATT** from the **Calls from** drop -down list.
 - e. Enable REFER SENDING check-box.
 - f. Select **Disabled** from **Transfer** to drop-down list.
 - g. Enter the IP for CAC IP Address.

Web Admin home	FINATT VOICE IP BOTHWAY (advar	nced mode)	
Subscribers	Telephony service>Network and links>Network>Trunk groups>Characteristics (4.2.1.2)		● L\$ ◇ 63 = 41 L\$
System	Identity reception management:		
Dialing plan	- calling Id. in	PAI or PPI or RPID	
Network and links Network Trunk groups	Name management		
Characteristics Characteristics of trunk group	- on busy / immediate forward		
FINATT VOICE IP BOTHWAY	- forward on no answer		
Reception			
Voice mail and tones	Voice mail		
Fast links	Local generation of tones		
	On hold management	SEND ONLY	
	force IB address to 0		
	- Torce IP address to 0	V	
	Support PRACK (100rel)	V	
	Tones management before answer - support P-Farly-Media	183+SDP+P-Early-Media 💌	
	Re-invite without allowed SDP		
	Reject 1.38	415 Unsupported Media Type 💌	
	REFER sending		
	Support of video		
MV5000-R6.3 /AE00 FRA Site: 002-SITE LOC	Support of T.38		
09/03/17 22:13:06 - CSTA SERVER 0: CONNECTED	Support of other medias (IM, etc)		
* CSTA SERVER 0: LINK IN FAULT	Bearer type incoming	CCBT+CCBNT -	
09/03/17 22:11:50 * CSTA SERVER 0: CONNECTED	Calls from	DINATT	

Web Admin home	FINATT VOICE IP BOTHWAY (advar	nced mode)			
Subscribers	Telephony service>Network and links>Network	>Trunk groups>Characteristics (4.2	2.1.2)	● L\$ ∨ tri =+ +	,
System	-		· ·		
Dialing plan	REFER sending				
Network and links					
Network	Support of video				
Trunk groups	Support of T 38				
Characteristics	Support of other medias (IM_etc.)				
FINATT VOICE IP BOTHWAY	Support of other medias (im, etc)				
eception	Bearer type incoming	CCBT+CCBNT -			
oice mail and tones	Calls from	DINATT -			
ast links	Priority calls if transit				
	Search DID numbers				
	- incoming digit translator number				
	- reject of numbers not assigned				
	Pre-answering message, caller charge	ed			
	- if called party free or busy 1				
	- if called party busy 2				
	- if number not assigned				
	Transf acc to called ntv comp-dent				
	Transfer to	Disabled			
	Transfer to	Disabled			
	Trunk aroup id (tel. record)	0			
	Trunk group monitoring				
	Max ph of simultan, calls allowed				
MV5000-R6.3 /AE00 FRA Site: 002-SITE LOC	max. no or simultan, calls allowed				
03/17 22:13:06 CSTA SERVER 0: CONNECTED	CAC IP address	10.148.66.100			
03/17 22:12:11	Centre - CAC class				
STA SERVER 0: LINK IN FAULT					
/03/17 22:11:50 CSTA SERVER 0- CONNECTED	. G711 forced in mode FAX/Modem				
Construction of Construction					

Create SIP Routes

A route and a specific direction are associated to InAttend and an access code is defined in the user dialing plan.

- 1. Go to, Web Admin > Network and Links > Network > Routes.
- 2. Select **DINATT** from the **To direction** drop-down list.
- 3. Select FINATT from the On trunk group drop-down list.
- 4. In the Tx DINATT DIRECT 0 on FINATT set the required type.

Configure Aid/IID Handling

Define the internal plans

- 1. Go to, **Network and Links > Network > AID handling > Internal plans definition**. This screen is used to select the internal plans to be defined.
- 2. Select the required Use of Plan and select the PSTN or TL from the plan type.



Composition of internal plans

Assign directions to the plans declared in the system. On system reset, the carrier directions are configured for plan 1.

NOTE: Unless a direction is allocated to a plan, it will not appear in the list of available directions for all MMCs. If you want to change a specific direction which belongs to a plan, that direction must not be in use.

- 1. Go to Network and links > Network > AID handling > Internal plans composition.
- Select the plan from Direction drop-down that you have created. In this example it is Direction: DINATT.

Web Admin home	Composition of plans 🖉 🖪 🔊 🧄
Subscribers	Telephony service>Network and links>Network>AID handling>Internal plans composition (4.2.6.2)
System	Direction: RESEAU PLAN 1 👻
Dialing plan	Direction: NATIONAL PLAN 1
Network and links Network	Direction: INTER. PLAN 1
AID handling	Direction: DOM PLAN 1
Reception	Direction: URGENCE PLAN 1
Voice mail and tones	Direction: UA 0
Fast links	Direction: LIA U
	Direction. Dinat 1 PLAN 2

Convert internal plan

- 1. Go to, Network and links > Network > AID handling > Conversion internal plan network plan.
- Select an internal plan and to specify a trunk group from the On trunk group drop-down list and click Select the item to confirm your selection and move to the next screen.

NOTE: You cannot enter two exceptions for one direction. If you change the direction, this deletes the former exception and creates a new exception with the same parameters (there is no change of the network plan or network address nature).



- 3. Select YES from the Fallback present drop-down list.
- 4. Select PUBLIC TEL from corresponding to plan drop-down list.
- 5. Select UNDEFINED from address nature drop-down list.

Web Admin home	Conversion PLAN 2 on FINATT		P
Subscribers	Telephony service>Network and links>Network>AID handling>Conv	ersion internal plan - network plan (4.2	.6.3)
System	Fallback present	YES	
Dialing plan	- corresponding to plan		
Network and links	- corresponding to plan		
Network	- and to address nature	UNDEFINED 🗸	
AID handling	Event for the direction		
Conversion internal plan - network	Except for the direction	······ 💌	
plan			
Conversion PLAN 2 on FINATT			
Reception			
Voice mail and tones			
Fast links			

Convert Network Plan - Internal Plan

- 1. Go to Network and links > Network > AID handling > Conversion network plan internal plan.
- 2. Select an internal plan and to specify a trunk group from the **On trunk group** drop-down list and click **Select the item** to confirm your selection and move to the next screen.

Web Admin home	Select network dialing plan 🖉 🖪 🔊 🧄 🖻
Subscribers	Telephony service>Network and links>Network>AID handling>Conversion network plan - internal plan (4.2.6.4)
System	By its name PUBLIC TEL
Dialing plan	On trunk group FINATT
Network and links	
Network	Select the item
AID handling	Select the Kent
plan	
Reception	
Voice mail and tones	
Fast links	

- 3. Select YES from the Fallback present drop-down list.
- 4. Select plan from corresponding to plan drop-down list and select direction if defined.
- 5. Select UNDEFINED from the Except for address nature drop-down list.



IID Handling

NOTE: The IID is the corporate number of the attendant consoles, and it can differ from the IID (Installation Identification) defined when the subscription to the ISDN public network access was taken out.

1. Go to Network and links > Network > AID handling > IID.

Web Admin home	IID definition	2 B B A B B B
Subscribers	Telephony service>Network and links>Network>AID handling>IID (4.2	.6.5) 👝 🔽 🖓 🖓 🖓 🖓
System	IID 0: internal plan PLAN 1	$\mathbf{\mathbf{v}}$
Dialing plan	or direction	
Network and links Network	number 130964	955
AID handling	restricted presentation NO 🔽	
Reception	IID 1: internal plan 🗸	
Voice mail and tones	IID 2: internal plan	
Fast links		

The entry menu is composed of an area with three lines repeated 16 times.

- 2. Select the internal plan associated with the IID. For example, in the screenshot above, **Plan 1** is selected.
- 3. Select the direction associated with the IID.

If Plan is selected, you need not select the direction. That is you can either select plan or direction.

- 4. Enter the number for IID (maximum 28 digits), do not enter 0.
- 5. Select NO to restrict the presentation of IID numbers.

Outgoing handling

Handling AID/IID outgoing calls consists in indicating in the "Caller Identity" information the DID number of the calling set (known as the AID), or the corporate number of the attendant consoles, (known as the IID).

Go to, Network and Links > Network > AID handling > Outgoing handling and select the item.

Web Admin home	Selection of calling party	
Subscribers	Telephony service>Network and links>Network>AID handling>Outgoing handlings (4.2.6.7)	🐃 🐚 🗸 🖬 🖏 🖓
System	By plan	
Dialing plan	And by direction LOCAL	
Network and links Network AID handling Outgoing handlings	Select the item	
Reception		
Voice mail and tones		
Fast links		

For Local Calls InAttend

- 1. Select the LOCAL plan by direction and click select the item.
- 2. Select the request plan as PLAN2 from the drop-down list and select FINATT for the trunk group.
- 3. Select YES from the Fallback present drop-down list.
- 4. Select No for inhibit sending od IID and AID and select NEVER for send IID.
- 5. Select No for AID completed with IID.
- 6. Select No for AID set using DID number.

NOTE: User local number, so you need not configure number in plan 2 for each subscriber.

Web Admin home	Outgoing for LOCAL 🛛 🖉 🖪 🖪 🖪	비비
Subscribers	Telephony service>Network and links>Network>AID handling>Outgoing handlings (4.2.6.7)	90
System	And the requested plan PLAN 2	
Dialing plan		
Network and links Network	Fallback present YES	
AID handling Outgoing handlings Outgoing for LOCAL	- inhibit sending of IID and AID NO	
Reception	- Send IID NEVER V	
Voice mail and tones	- AID set using DID number	
rast unites	- digit translator number	
	Advanced characteristics	

For Inattend calls External

- 1. Select Plan 2 and click Select the item.
- 2. Select Plan 1 for the requested plan and select FX.SIP for trunk group.
- 3. Select YES for the Fallback present.
- 4. Select YES for AID Completed with IID and Select IID IMMEDIATE TRANSM from the processing drop-down list.

Web Admin home	Outgoing for PLAN 2	\sim		
Subscribers	Telephony service>Network and links>Network>AID handli	ng>Outgoing handlings (4.2.6.7)	= L\$ ∨ tu	
System	And the request	ed plan PLAN 1	1	
Dialing plan	On trunk group		-	
Network and links	Off dank group			
Network AlD bandling	Fallback present	YES 🗸		
Outgoing handlings	- AID completed	with IID YES		
Outgoing for PLAN 2	processing		MSM	
Reception	- processing			
Voice mail and tones	- digit translator	number		
Fast links	- IID number	0		
		Advanced characteristic	s	

5. Go to Network and links > Network > AID handling > IID and set the number.

NOTE: Set the index from 0 to 15, defined in the section "IID", on the line IID NUMBER

Web Admin home Subscribers	IID definition Telephony service>Network and links>Network>AID har	udling>IID (4.2.6.5)
System Dialing plan Network and links Network AID handling IID	IID 0: internal plan or direction number restricted presentatio	PLAN 1 V V 130964955 n NO V

For External transferred to External

- 1. Select Plan1 and click Select the item.
- 2. Select Plan1 for the requested plan and select YES for the Fallback present.
- 3. Select NO for AID Completed with IID and Select AID TRANSM from the processing drop-down list.
- 4. Select NO for inter-plan forwarding.

Web Admin home	Outgoing for PLAN 1 👛 🕓 🏠 🛼 📮	Р,
Subscribers System Dialing plan Network and links Network AID handling Outgoing handlings Outgoing for PLAN 1 Recention	Telephony service>Network and links>Network>AID handling>Outgoing handlings (4.2.6.7) And the requested plan PLAN 1 On trunk group Fallback present YES - AID completed with IID NO - processing AID TRANSM.	
Voice mail and tones Fast links	- digit translator number - inter-plan forwarding NO 💌 Advanced characteristics	

For External calls InAttend

- 1. Select **Plan1** for By Plan and click **Select the item**.
- 2. Select **Plan2** for the requested plan and select **FINATT** as trunk group and select **YES** for the **Fallback present**.
- 3. Select No for AID Completed with IID and Select AID TRANSM from the processing drop-down list.
| Web Admin home
Subscribers | Outgoing for PLAN 1
Telephony service-Network and links-Network-AID handlings-Outgoing handlings (4.2.6.7) |
|---|---|
| System | And the requested plan PLAN 2 |
| Dialing plan | |
| Network and links
Network | Fallback present YES |
| Outgoing handlings
Outgoing for PLAN 1 | |
| Reception | - processing AD TRAINSM. |
| Voice mail and tones | - digit translator number |
| Fast links | Advanced characteristics |

For InAttend calls InAttend

- 1. Select Plan2 and click Select the item.
- 2. Select Plan2 and select FINATT as trunk group and select YES for the Fallback present.
- 3. Select No for AID Completed with IID and Select AID TRANSM from the processing drop-down list.

Web Admin home Subscribers	Outgoing for PLAN 2 Telephony service>Network and links>Network>AID handling>Outgoing handlings (4.2.6.7)	i i i i i i i i i i i i i i i i i i i
System	And the requested plan PLAN 2	
Dialing plan		
Network and links Network	Fallback present YES	
AID handling Outgoing handlings Outgoing for PLAN 2	- AID completed with IID NO	
Reception	- processing AID TRANSM.	
Voice mail and tones	- digit translator number	
Fast links	Advanced characteristics	

For External Calls Local

1. Go to, Network and links > Network > AID handling > Incoming handlings, and select Plan1 and click Select the item.

Web Admin home	Select internal dialing plan	
Subscribers	Telephony service>Network and links>Network>AID handling>Incoming handlings (4.2.6.8)	🌥 🕒 🗸 1년 🖛 \cdots 🗆
System	By its name PLAN 1 👻	
Dialing plan	On trunk group	
Network and links Network AID handling Incoming handlings	Select the item	
Reception		
Voice mail and tones		

- 2. Select YES from the Fallback present, and select YES for add prefix to AID.
- 3. Select YES for same handling as AID.
- 4. Select INTER from the Except for the direction drop-down list.
- 5. Select YES for same handling as AID.

Web Admin home Subscribers	Incoming for PLAN 1 on Telephory service-Network and links-Network-AID handling-Incoming handlings (4.2.6.8)	4 G V A R A G
System	Fallback present YES -	
Dialing plan	- add prefix to AID	
Network and links Network	- digit translator number	
AID handling Incoming handlings	- ISDN IID auto. associated	
Incoming for PLAN 1 on	- same handling as AID YES	_
Reception	Except for the direction	
Voice mail and tones	- add prefix to AID YES 💌	
Fast links	- digit translator number	
	- ISDN IID auto. associated	
	- same handling as AID YES 💌	
	Except for the direction	
	Except for the direction	
	Except for the direction	

For Inattend calls Local

- Go to, Network and links > Network > AID handling > Incoming handlings, and select Plan2 from the plans name.
- 2. Select **FINATT** from the **On trunk group** drop-down list and click **Select the item**.

Web Admin home	Select internal dialing plan 🖉 🖪 🖪 🖪 🖪
Subscribers	Telephony service>Network and links>Network>AID handling>Incoming handlings (4.2.6.8)
System	By its name PLAN 2 V
Dialing plan	
Network and links	
Network	Coloct the item
AID handling Incoming handlings	Select the item

- 3. Select YES from Fallback present, and select No to add prefix to AID.
- 4. Enter 1 in the digit translator number.
- 5. Select YES from the same handling as AID.



6. Enter a Hardphone range and a softphone range.

NOTE: Hardphone number is configured in client InAttend. If hardphone is not needed, this translator is not required.

Web Admin home Incoming: calling number - translat. 1 Subscribers System Dialing plan Hardphone range Network and links Digit to translate 7ABC Translators to plan Incoming: calling party number or to direction Incoming: calling number - translat. Softphone range Digit to translate 81AB to plan Voice mail and tones Fast links	рс
---	----

What to do Next

Perform the following list of operations to successfully complete AID and IID configurations.

Transfer Authorization

To allow transit calls between Network calls and InAttend:

- 1. Go to the Subscribers > Rights > General settings.
- 2. Click the Rights tab and select TK TK and TK TL check-box.
- 3. Select LIST NOT USED from the Config trunk groups drop-down list.

Web Admin home Subscribers	Subscribers m Telephony services	niscellanec »Subscribers»	🛎 🖪 🛇 G	A D D				
General settings	Subscriber	System	Rights	Application	Network	Security		
System Dialing plan Network and links Reception Voice mail and tones Fast links		Fort Fun - TK - Se Forv Trar - TK	bidding of gener ction conferenc TK allowed nd tone varding to TL su isfer authorizati TK	al call pick u e bject to right on				
			- by - be - be - via - of - to	nfig trunk group subsc. without tween room set tween room set op. cons. to pr personal call set with PSTN a	restriction ts ts via op. con e-payment s ccess allowe	LIST NOT	USED	

Configure Hardphone Subscriber

1. Go to Subscriber > Subscription > Characteristics, select REFUSED from the Call waiting drop-down list.



Create an External Record

 Go to, Internal Records and click Add an external contact to create a new external record. An external record number 9 Name STD_INATTEND IN ORDER to display STD_INATTEND when INATTEND CLIENT CALLS a LOCAL SUBSCRIBER

Web Admin home	Add an exte	mal contact						
Internal records	* A B C	DEFG	HIJKL	MNO	PQRS	T	U V W X	YZ
External records	Name	Firstname	Localisation	N°abbrev	Number		Email	
Customization	EXT_3003				0130963003			~
	INT_INATTEN	L.			8100			
	MITEL		Guyancourt		01309642000)		
	STD_INATTEN	J			9			
	5							
	<							
	< Display V							
	Cisplay V Gender :			N	umber :	9	Confidentia	lity : Green list
	Clisplay ✓ Gender : Name :	STD_INATT	END	N	umber : °abbrev :	9	Confidentia Hierarchy(s	lity : Green list
	∑ Display ✓ Gender : Name : Firstname :	STD_INATT	END	N N L	umber : °abbrev : ocalisation :	9	Confidentia Hierarchy(s Email :	lity : Green list

Create Password

.

Create a password for InAttend account to access proxyldap

1. Go to Subscribers > Directory > Settings > Users accounts and set password for clients.

Web Admin home	Users accounts		
Subscribers	Telephony service>Subscribers>Directory>Setting	gs>Users accounts (1115)	
Directory	i2070 :		
Users accounts	- login	i2070	^
System	- password	******	
Dialing plan	• (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		
Network and links	TWP :		
Reception	- login	twp	
Voice mail and tones	- password	*****	
Fast links			
	CC :		
	- login	acp	
	- password	****	
	MICOLLAB :		
	- login	MiCollab	
	- password		
		·	
	UC360 :		
	- login	UC360	
	- password	****	
	LIFESIZE :		
	- login	Lifesize	
	- password		
	A340W :		
	- login	A340w	
MUSOOD-DE A DC JASOT EDA	- password		
Site: 002-SITE LOC	Passia		
30/05/17 17:55:29	. INATTEND :		
30/05/17 17:34:55	- login	InAttend	
* CSTA SERVER 0: CONNECTED	* - password	****	
30/05/17 16:08:32			~

Configuration for Cisco Unified Communications Manager

If you are using the Cisco Unified Communications Manager (CUCM) with you InAttend system, you must perform some configuration to integrate the call manager with InAttend.

SIP Trunk security profile configuration

The CUCM sometimes does not answer "Subscribe", if a trunk like the 'telephony part' is used.

So, a separate trunk for Cisco linestate is configured.

This trunk points back to the ACS (linestate) server on port 5070 (as shown in the image).

This trunk has a SIP security profile configured to the port 5070 to receive requests on the 5070 port.

Linestate is also configured to send across requests on the 5070 port.

To setup a SIP trunk security profile, do the following:

- 1. Login to the Cisco Unified CM Administration interface (http://<servername>/ ccmadmin).
- 2. Under SIP Trunk Security Profile Information, enable the following options:
 - Accept presence subscription
 - Accept unsolicited notification
 - Accept replaces header

CISCO Eor Cisco Unified Commu	Administration			
Svetem Call Douting Madia Desources	★ Advanced Features ★ Device ★ Application ★ User Management	ent 👻 Bulk Adminie		
System · Can Routing · Incula Resources	Auvanceu reatures · Device · Application · Oser manageme			
SIP Trunk Security Profile Configura	tion			
Save 🗙 Delete 🗋 Copy 🍨	Reset 🧷 Apply Config 🕂 Add New			
Status				
Status: Ready				
SIP Trunk Security Profile Informati	on			
Name*	ACS SIP SIMPLE Security profile			
Description	ACS SIP SIMPLE Security profile			
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*	5070			
Enable Application level authorization				
Accept presence subscription				
Accept out-of-dialog refer**				
Accept unsolicited notification				
C 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 configuration

To configure a SIP profile, do the following:

1. In Cisco Unified CM Administration, under SIP Profile Information, enable the Redirect by Application option.

- SIP Profile Information		
Name*	ACS-Profile	
Description	ACS system	
Default MTP Telephony Event Payload Type*	101	
Early Offer for G.Clear Calls*	Disabled	•
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites $\!\!\!\!\!*$	TIAS and AS	•
User-Agent and Server header information*	Send Unified CM Version Information as User-Ager	•
Accept Audio Codec Preferences in Received Offer*	Default	•
Dial String Interpretation*	Phone number consists of characters 0-9, *, #, and	•
Redirect by Application		
Disable Early Media on 180		
Outgoing T.38 INVITE include audio mline		
Enable ANAT		
Require SDP Inactive Exchange for Mid-Call Media Change		
Use Fully Qualified Domain Name in SIP Requests		
Assured Services SIP conformance		

2. Under Trunk Specific Configuration, select "Contact Header" from the pull-down list in the Reroute Incoming Request to new Trunk based on* field.

— Trunk Specific Configuration ————————————————————————————————————		
Reroute Incoming Request to new Trunk based o	on* Contact Header	•
RSVP Over SIP	Local RSVP	•
Resource Priority Namespace List	< None >	•
Fall back to local RSVP		
SIP Rel1XX Options*	Disabled	•
Video Call Traffic Class*	Mixed	•
Calling Line Identification Presentation st	Default	•
Deliver Conference Bridge Identifier		
Early Offer support for voice and video calls	(insert MTP if needed)	
Send send-receive SDP in mid-call INVITE		
Allow Presentation Sharing using BFCP		
Allow iX Application Media		
Allow Passthrough of Configured Line Device	Caller Information	
Reject Anonymous Incoming Calls		
Reject Anonymous Outgoing Calls		

SIP trunk configuration

To configure a SIP trunk, do the following:

1. In the Cisco Unified CM Administration interface, under **Trunk Configuration - Inbound Calls**, enable the **Redirecting Diversion Header Delivery – Inbound** option.

- Inbound Calls		
Significant Digits*	All	
Connected Line ID Presentation*	Default 🔻	
Connected Name Presentation*	Default 🔻	
Calling Search Space	< None >	
AAR Calling Search Space	< None >	
Prefix DN		
Redirecting Diversion Header Delivery - Inbound		

2. Under Trunk Configuration - Outbound Calls, enable the Check Redirecting Diversion Header Delivery – Outbound option.

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

Use Device Pool Redirecting Party Transformation CSS

NOTE: Make sure that the SUBSCRIBE Calling Search Space and the Rerouting Calling Search Space fit your number plan. In addition, Make sure that the inbound Calling Search Space on the SIP trunk fits your number plan.

The Acs Cisco LSS config component is used while configuring the sip trunk on ACS for Cisco.

When a call goes to the sip trunk, **udp** transport is used to define the Local port (here the local port is 5070).

It is also called as the 'termination port'. It terminates the sip trunk initiated from cucm.

When a linestate encounters a problem, it contacts the log level - For ex: Debug 3

(Debug 3 is the highest level of Debug used.)

This log path is mentioned in Folder. Other values are taken by default.

Click Save to update the values entered.

÷	
	ACS Cisco LSS config 🛛 💌
:	SIP/SIMPLE Transport udp V Local port 5070 Cverride Cisco port in NCLA 5070
	AXL Poll interval (s) 10 Max update/min 50 Retry after ms 1000 AXL port 8443 Bulk max size 100 Bulk workers 3
	Cisco "Forward to Voicemail" feature is enabled
	Log Level Debug+3 V Max size (MB) 10 🗘 Days to keep 14 🗘
•	Folder C:\ProgramData\Mitel\AcsCiscoLSS
	Save Cancel
	C:\Program Files (x86)\Mitel\AcsCiscoLSS\ServiceConfig.xml
Ļ	

To configure ACS Cisco linestate Server, the 'InAttend 2.4 (8.2016) – Installer' has to be installed (it is mandate).

D Ir	Attend 2.4 (8.2016) - Installer
Mitel InAttend InAttend Install Enterprise License Manager Install or Upgrade InAttend Server Install or Upgrade Schware	Introduction
Contact Mitel	Before installing, please read the Installation Preparation Guide and Release Notes for requirements and the necessary preparations. For more detailed information on all the steps, refer to the Installation and Configuration Guide. This document has the same structure as the package browser, so that you can easily navigate it for the information you need. Click here to browse the CPI Library (index.htm) View more information about Mitel Installer This product is protected by international copyright law. (c) 2016 Mitel Networks Corporation. All Rights Reserved. www.mitel.com Note: Install software from local hard drive, not from mapped drives or network.
	August 3, 2016

The host is configured here. For ex: a call manager in cucm.

	Host name	IP	Network name	Description
1	CUCM	10.10.144.18	CUCM	CISCO UC
Ì	INATTNDCMG	10.10.144.54	INATTNDCMG	Attendant Call Server

Creating a new host:

- 1. To create a new host, click the Pencil icon.
- 2. The Edit host webpage pop up is displayed.
- 3. Enter the host name, ip address, network name, and Description.
- 4. Click **Update** to save the changes.
- 5. New host is created.

LSS – Linestate Server

The 'Subsystems' section under 'Simple Config' defines different fields for ACS for cisco.

Linestate server defines the phone registry status, whether the phone is registered or not.

The Host, Port, In service timeout (ms), and Busy event timeout (ms) is defined to update the Linestate Server settings.

The port 3134 is same in Webadmin (presence server) as well.

Telephony Configuration Application	Line	estate Server -	MY-LSS	
	Setti	ngs		
SimpleConfig	Host		STANDALONE (Attendant Call S	Serve) 🗸
Hosts	Port		3134	
Public Networks Hosted Private Networks	In se	ervice timeout (ms)	1500	
	Busy	event timeout (ms)	150	
Linestate Servers				Update
MY-LSS ⊡Queue Managers	Dom	ains to monitor		
My_QueueManager		Domain	Service	
• NeTSs	1	Mitel (My_Site)	1000-1005 Office Phones	*
MY_ACS	1	MX1	7000-7006 My Phones 6000-6004 Phones 5004-5004 Phones	
- Media Servers				Add
My_MediaServer	Prov	iders		
	СТІ	manager		Username
	CUCI	м		NLSS_001

Domains to monitor

This field states the endpoint number of the domain defined.

The extension number of the phone is passed on here.

Queue manager

The host and the Domain can be added here. The values are default.

Telephony Configuration Application	Queue Manager Cluster - My_QueueManager
	Settings
⊡ SimpleConfig	Primary NeTS / NQM host INATTNDCMG (Attendant Call Serve) V
Hosts	Secondary NeTS / NQM host No secondary host V
Public Networks	Attendant client port 4812
Hosted Private Networks	QualityManager port 4813
Subsystems	Update
MY-LSS	Use LSS
e Queue Managers	Host
My_QueueManager	INATTNDCMG
NeTSs	V Add
•••• PBXSTDs	Serviced domains
Media Servers	Domain
My_MediaServer	Mitel (My_Site)
Sites	Add E

My ACS

My ACS takes default values set by the system.

The Host name and Sip Ports field is configured under My ACS.

The Sip Port value is configured to 5060.

Telephony Configuration Application	MY_ACS					
	Settings					
⊡ SimpleConfig	NeTS host STAND	ALONE (Attendant Call Serve)	\checkmark			
Hosts		Upda	ate			
Public Networks						
Hosted Private Networks	Sm Entries					
Subsystems	Domain	Description	Number/Range	State Machine		Queue Entries
- Linestate Servers	MX1	Internal Queue	09	Queue		
MY-LSS	MX1	Queues	2000	Queue		
Queue Managers	Mitel (My_Site)	CUCM_Queue	2300	Queue		
My_QueueManager						
- NeTSs	Tapi Service Provid	ers for STANDALONE				
MY_ACS	TSP name	CTI	manager	Username		
B-PBXSTDs	CiscoTSP001.tsp	CUCI	м	NETS_001		
Mitel	SIP Ports					
Mu MadiaCaman	Name	Description	Host name	SIP Port		
my_mediaserver	J SIP	NeTS SIP Port	STANDALONE	5060		
Sites					New	

PBXSTDs

Subsystems under Simple config are used to create new elements in the site.

Telephony Configuration Application	Subsystems
 SimpleConfig Hosts Public Networks Hosted Private Networks 	Subsystem Summary Linestate Servers Queue Managers
Subsystems	NeTSs
Linestate Servers MY-LSS Queue Managers NeTSs MY_ACS PBXSTDs Media Servers Media Servers My_MediaServer Sites	PBXSTDs Quality Manager Clusters Media Servers

e a new element in the site.

Subsystem Summary		
Linestate Servers	1	New
Queue Managers	1	New
NeTSs	1	New
PBXSTDs	1	New
Quality Manager Clusters	0	New
Media Servers	1	New

Click **New** to create a new PBXSTDs element.

The **PBXSTD – Mitel** window appears.

Select the appropriate Host, Port, and Domain.

Click Update.

Telephony Configuration Application	PBXSTD - Mitel
SimpleConfig Hosts Public Networks Hosted Private Networks Subsystems Linestate Servers MY-LSS Queue Managers My_QueueManager NeTSs MY_ACS PBXSTDs Mitel Media Servers My_MediaServer Siter	Settings Host INATTNDCMG ✓ Port 3129 Domain Mitel Update Use LSS Host INATTNDCMG ▲ ▲dd

Media Server

The host and Port values under Media Server settings page are default.

Telephony Configuration Application	Media Server - My_MediaServer
⊡-SimpleConfig	Settings Host INATTNDCMG V
	Update
Queue Managers My_QueueManager NeTSs	
-PBXSTDs	
→ Mitel → Media Servers	
Sites	

Add CUCM Cluster on a private network.



The CUCM version is same as the call manager.

Select the cucm version from the drop-down list.

Telephony Configuration Application	My_Network	- CUCM						
Application My_Site Site: My_Site Private Networks My_Network CuCM Domains Initel CuCM Users CuCM Users CuCM Users Initel Domains Initel Initel Domains Initel Initel Domains Initel Inite	Settings CUCM version BAT tool version AXL User NETS user prefix NLSS user prefix Hosts Hosts Host name CUCM	5.1 V cucm NETS_ NLSS_ L	Jpdate		Ρι	iblisher INATTN	CII manager primary V DCMG V Add	Pew
- Internal - External	Route Points Description	М	lumber					
- Operator Groups - InAttendCMG - Queues - Operator Group Users	SIP Ports Name	Description	Host name	SIP Port	Protocol	Use Trom	bone Transfer	
Voice Systems	J SIP_Trunk	SIP_Trunk	CUCM	5060	UDP	False	[New

Add sip port as 5060 and UDP under protocol field respectively.

The My_Network – CUCM – Domains is defined.

Telephony Configuration Application	My_Net	My_Network - CUCM - Domains					
My_Site	The list prese	nts the doma	ains in the CUCM o	uster.			
- Site: My_Site	Name	PBX Id	Domain Id 1	Internal prefix	SIP Domain	Phone Context	
- My_Network							New

The Port, Media Server, and Device ranges are defined.

Telephony Configuration Application	My_Networ	k- CUCM	- Domains - Mi	tel			
My_Site	Settings						
	PBX Id	1					
E Site: My_Site	Default internal p	refix 🖬					
Private Networks	ONM						
- My_Network	CMG View						
E CUCM	SIP Domain						
- Domains	SIP Domain Desc	ription					
Mitel	Phone context	· _					
CUCM Users	Create \$22 pumb						
cucm	Create 25-numb	ers		Undate			
NETS_001				opulate			
NLSS_001	Ports						
BAT	Name	Туре	Host name	Port	Protocol	Description	
Public Queues	SIP_Trunk	sip	CUCM	5060	UDP	SIP_Trunk	Ť
Internal	Add						
External							
- Operator Groups	Media servers						
- InAttendCMG	Name				Order		
Queues	My_MediaServer				1		
Operator Group Users	Add						
Voice Systems							
	Device ranges						
	Description	on	Number/Range	Т	уре	Usage	
	Office pho	nes	1000 - 2000	P	hone	Phone	
	🥒 InAttend		9000 - 9999	Δ	pplication number		
							New

The My_Network – CUCM – Users window displays the user properties.

Telephony Configuration Application	My_Network - CL	My_Network - CUCM - Users				
My_Site	Click on the edit icon to cha	nge a CUCM user's properties.				
	Username	Usage				
⊡ Site: My_Site	🥜 cucm	AXL				
Private Networks	NETS_001	NETS				
	NLSS_001	LSS				
Mitel						
CUCM Users						
cucm						
NETS_001						
NLSS_001						

Click the pencil icon to edit the cucm user properties.

Telephony Configuration Application	My_Network - CU	CM - Users	
My_Site	Click on the edit icon to chan	ge a CUCM user's properties.	
	Username	Usage	
⊟ Site: My_Site	🥖 cucm	AXL	
Private Networks	NETS 001	NETS	
- My_Network	2 NLSS 001	LSS	
E-CUCM	🖉 Edit CUCM User Web	ppage Dialog	×
Mitel	http://10.10.144.63/to	a/ctc/ccmclusterusereditiframe	e.asp
CUCM Users	Edit CUCM user		
—cucm			-
-NETS_001	Username cucm		
-NLSS_001	Password	nreviously set	
BAT	New paceword	,	Password has provided in the CUCM>AXL
Public Queues	New password		tab
-Operator Groups		Update Cano	el la
Voice Systems			

Edit CUCM User window appears.

Provide the AXL credentials here in the TCA. The list of device ranges associated to the user is displayed. (The device range value is taken automatically.)



Telephony Configuration Application	My_Network - CUCM - NLSS_001 The list presents the device ranges associated to the user.				
My_Site					
	Description	Number/Range	Туре		
	Office phones	1000 - 2000	Phone		
Private Networks					
- My_Network					
UCM					
- Domains					
Mitel					
cucm					
NETS 001					
NLSS_001					

Configuring webadmin

To configure the webadmin, create a Data source for cisco under the presence server.

Port 3027

Port 5077

STANDALONE

Data sources				
Name		- selec	t data source -	 Add data source
Cisco	Linestate	8		
MX-ONE	Linestate	8		
Authentication				
Check user credentials again	ist AD			
Trace Configuration				
Set trace				
rver				
STANDALONE Line	state		_	
Data	source name Cisco		Device	

Inside Data Source, click Advanced.

Backup server

Server name STANDALONE

Server					Save Back
	STANDALONE	Linestate Data source name Cisco Connection data Server name STANDALONE Backup server Range From To	Port 3027 Port 5077	Device Basic	Test connection
		Prefix Value Delete		Domain / Link	y: 2 This is the PBXSTD created i the TCA

The Domain / Link number is defined.

*23 service configuration

To configure *23 Service, do the following:

1. In Cisco Unified CM Administration interface, under Service Parameter Configuration, set the Strip # Sign from Called Party Number to "False" for the "Cisco CallManager" service:

Service*	Cisco CallManager (Active)	•	
Station KeepAlive	Interval.*	30	
Status Enquiry Pol	Flag *	False	-
Strip # Sign from	Called Party Number *	False	-
Session Handoff Al	erting limer	10	
T301 Timer *		180000	
T302 Timer. [*]		linear a	

- 2. Create the route pattern for the *23 service
 - a. Open the Call Routing menu and select Route/Hunt then Route Pattern.
 - **b.** In the Route Pattern Configuration dialog, create the following three Route Patterns for the *23 services:
 - #23#
 - *23*!#

- Dattom Definition -

- *23*!*!#
- c. For each pattern, click Add New and select the route to the ACS trunk in the Gateway/Route List.

Fattern Dennition		
Route Pattern*	*23*!#	
Route Partition	< None >	
Description		
Numbering Plan	Not Selected	*
Route Filter	< None >	*
MLPP Precedence*	Default	▼
Apply Call Blocking Percentage		
Resource Priority Namespace Network Domain	< None >	•
Route Class*	Default	•
Gateway/Route List*	ACS_84_SIP_trunk	•

d. Click Save when finished.

The new patterns are displayed in the Route Patterns list:

Route	Patterns (1 - 9) of 9)			Rows per Pag	e 50 🔻
Find Rou	ite Patterns where	Pattern 👻	begins with 🛛 🛨		Find Clear Filter	4
	Pattern *	Description	Partition	Route Filter	Associated Device	Сору
	<u>#23#</u>				ACS 84 SIP trunk	ß
	23!#				ACS 84 SIP trunk	ß
	<u>*23*1*1#</u>				ACS 84 SIP trunk	ß

*21 Service Configuration

 In Cisco Unified CM Administration interface, under Service Pararmeter Configuration, set the Strip # Sign from Called Party Number to False for the Cisco Call Manager service:

Service*	Cisco CallManager (Active)	V
Station KeepAlive Interval *		30
Status Enquiry Poll Flag.*		False
Strip # Sign from Called Party Number.*		False

- 2. Create the route pattern for the *21 service
 - a. Open the Call Routing menu and select Route/Hunt >Route Pattern.
 - **b.** In the **Route Pattern Configuration** dialog, create the following three Route patterns for the *21 services:
 - #21#
 - *21*!#
 - c. For each pattern, click Add New and select the route to the ACS trunk in the Gateway/Route list.

Pattern Definition		
Route Pattern*	*21*!#	
Route Partition	< None > •]
Description	Route to inttend	
Numbering Plan	Not Selected 🔻]
Route Filter	< None > v] .
MLPP Precedence*	Default 🔻	
Apply Call Blocking Percentage		
Resource Priority Namespace Network Domain	< None > v] .
Route Class*	Default 🔹]
Gateway/Route List*	InAttend v	(<u>Edit</u>)
Route Option	Route this pattern	
	Block this pattern No Error	

d. Click Save.

The new patterns are displayed in the Route patterns list:

Route Patterns	(1 - 3 of 3)				
Find Route Patterns where Pattern 🔻 begins with 🔻 Find Clear Filter					
	Pattern 🔦	Description	Partition	Route Filter	
	<u>#21#</u>	Route to inttend			InAttend
	<u>*21*!#</u>	Route to inttend			InAttend

Installing the InAttend license

Before you install InAttend, you have to obtain and install the InAttend license on the Enterprise License Manager (ELM) server. To complete the process, you must:

- Install the ELM Server (if not already present in your system).
- Generate a fingerprint file to uniquely identify the ELM host machine.
- Register the license voucher on the Mitel License Server.
- Install the InAttend license on the ELM server.

Installing Enterprise License Manager

Enterprise License Manager (ELM) is the client/server-based licensing server where InAttend product licenses are requested, stored, and managed. The Mitel Installer offers installation for both the server component (which maintains licenses and enforces limits) and the client component (which is used to make license requests). Web administration tools (used to administer licenses) are also installed.

You install either the ELM server or the ELM Client, but not both on the same host. If the InAttend server is being installed in a system that already has ELM installed for other products, then you only need to request new InAttend system and user licenses.

To install the ELM server software:

- 1. Double-click the **Install.exe** file in the top-level directory of your software package to launch the Mitel Installer.
- 2. In the Installer main window, click Install.
- 3. In the Install Wizard, select Install ELM Server/Client.

🔀 Mitel



Install Enterprise License Manager Wizard for installing ELM Server or Client.



Install InAttend Server (CMG) Wizard for installing InAttend on the same server as CMG Server.



Install InAttend Server Standalone Wizard for installing InAttend Server Standalone.



May 10, 2016

- 4. On the Install ELM Server/Client page, click Next to continue.
- 5. On the Welcome page of the Install Wizard, click Next to continue.
- 6. On the Feature Selection page, select Enterprise License Manager Server, and click Next.

Feature Selection	
Select the feature you want to ins	stall:
O Enterprise License Manag	er Client
Installs the license client n	needed to communicate with the license server.
Enterprise License Manage	er Server
Installs the license server, client needed to communi	web access, and other tools. Also installs the license icate with the license server.
nstallShield	
	< <u>B</u> ack <u>N</u> ext > Cancel

- 7. On the Choose Destination Location page, specify the installation path (either accept the default or browse to another location) and click **Next**.
- 8. On the License Server Options page, accept the default Port setting of 2580 and click Next.

9. On the Start Copying Files page, review your installation settings. Click **Back** to change a setting or click **Next** to start the installation.

Setup has enou change any sett copying files.	gh information to st ings, click Back. If	art copying the f you are satisf	e program files. ied with the sett	If you want to rev ings, click Next to	view or o begin
Current Settings					
Setup Type:					_
Enter	prise License Mana	ager Server			_
Target Directory C:\Pr	r: ogram Files (x86)\M	1itel\License N	/lanager\		
License server Host	located at: = 127.0.0.1				
Port =	= 2580				~
<					>

The Wizard installs the ELM Server software. When installation is complete, the Wizard displays an information page that describes the steps to install a license file.

10. Review the information and click **Continue**.

🕅 Mitel 🕴 InAtt	end
Enterprise License Manager (ELM)	Install license file
Install license file	Install a license file for InAttend. Read: InAttend Installation Preparation Guide ELM Technical Guide Mitel License Agreement
	When ordering an Mitel product from Mitel Plan, a voucher is generated in SLS and as soon as the voucher is registered (activated), a license file is created and delivered by e-mail. To generate the license file:
	1) On ELM Server, run Fingerprinter.exe to create file 'Fingerprint.blob'.
	2) Log on to Aastra Connect, and then click Licenses & Services.
	3) In the Register voucher field, enter voucher number and click Register.
	4) Upload the 'Fingerprint.blob' in Enter fingerprint.
	5) In System data and Ownership information details, you will see all the licenses from the Voucher you are registering, as well as the accumulated number of licenses. Click Confirm input.
	 Click Confirm & Generate License Key. The license is now generated and e-mailed to you.
	7) Install the license file in the ELM application.
Click 'Continue'.	Continue

11. On the Wizard Complete page, click Finish.

After you have installed the ELM server, you have to do the following to complete the licensing process:

- Generate the fingerprint file on the ELM server
- Register the license voucher on Mitel Connect
- Install the license file received from the Mitel License Server on the ELM server

For more information, refer Enterprise License Manager Technical Guide.

Installing the InAttend Server

After you have installed the InAttend license, you can install the InAttend application software. You use the InAttend Software installation wizard to install all necessary components.

NOTE: InAttend can use CMG Server, BluStar Server (BSS) or any other LDAP-enabled directory for directory searches. If CMG Server is used, CMG - Web has to be installed prior to the InAttend installation.

You have to provide the following information during installation of the InAttend server:

- Type of call manager (e.g., MX-ONE, MiVoice5000)
- IP address of call manager
- IP address (or FQDN) of the SQL Server
- SQL login credentials (user name and password)
- IP address of the CMG server (for CMG installations)
- CMG database login credentials (for CMG installations)

To install the InAttend Server software, do the following:

- 1. Double-click the **Install.exe**file in the top-level directory of your software package to launch the Mitel Installer.
- 2. In the Installer main window, click Install.
- 3. In the Install Wizard, click on your installation option (Install InAttend Server Standalone or Install InAttend Server (CMG) if you are installing to an existing CMG deployment).
- 4. In the Installation window, review the components that are being installed.

Mitel InAttend

Install InAttend Server (CMG)

Component	Version	Installed	Information / Prerequisites	-
Before the Installation	-	-		
🐻 Microsoft XML Core Service 4.0	4.30.2100.0			
Microsoft VC 2008 SP1 Runtime	9.0.30729	9.0.30729		
Microsoft VC 2010 SP1 Runtime	10.0.40219	10.0.40219		
Microsoft VC 2012 Runtime	11.0.50727	11.0.50727		
Microsoft VC 2013 Runtime	12.0.21005	12.0.21005		
Microsoft .NET Framework 4.5 Full				
🐻 Oracle Java Development Kit (x64)	1.7			
🐻 Telephony Configuration Service (TCS)	2.0.53.0			
🐻 Telephony Configuration Application (TCA)	2.0.53.0			
🔀 Media Server	1.7.64.0			
🐻 Network Telephony Services (NeTS)	5.9.13.0			
🔀 Queue Manager	2.15.7.0			
🐻 Mitel LDAP Server	8.2.2			
🔀 BluStar Server	7.1.113			
🐻 InAttend History Service	2.3.14.0			
🐻 InAttend Quick Configuration Service	2.3.14.0			
🐻 InAttend Quick Configuration Web	2.3.14.0			
A la A Hand Oniale Cast annation				•
May 10, 2016			< Back Next >	Cancel

Components with a green check mark are already installed. Components with a red circle require a prerequisite that has not yet been installed. For example, the License Manager has to be installed before the InAttend installation can continue.

- 5. Correct any errors and click Next.
- 6. On the Installation Path page, specify an installation path (by accepting the default location or browsing to another location) and click **Apply**.
- 7. On the Before the Installation page, review the information and notes, and click **Continue** to start the installation.

Mitel InAttend	
➡ Before the Installation	Before the Installation
Microsoft XML Core Service 4.0 Oracle Java Development Kit (x64)	Before installing, please read the InAttend Installation and Configuration Guide and Release Notes for requirements. The following is required:
Telephony Configuration Service (TCS)	Administrator rights on each server being installed.
Telephony Configuration Application (TCA)	 Internet Information Services (IIS) 7.5, 8.0 or 8.5: Enable IIS 6 Management Compatibility, ASP and ASP.NET.
Network Telephony Services (NeTS)	CMG - BluStar Web 8.2 SP2 (if InAttend Server with CMG).
Queue Manager	Valid License (file) on the ELM Server.
Mitel LDAP Server BluStar Server	Note: - Only install Mitel LDAP Server for an InAttend standalone solution. - Do not configure Calendar Connection in WebAdmin if used together with
InAttend History Service	CMG (Calendar Connection located in the CMG BluStar Web package should be used instead).
InAttend Quick Configuration Service	For custom installations, use the classic package browser
InAttend Quick Configuration Web	For custom installations, use the classic package browser.
InAttend Quick Configuration	
Restart InAttend Server	*
Click 'Continue'.	Continue Cancel

The Wizard proceeds with software installation. The blue arrow in the left panel indicates installation progress.

- 8. For InAttend Server (CMG) installations only: The Wizard launches the LDAP server installation wizard. InAttend requires LDAP server information to retrieve information using LDAP from a data source such as Active Directory. You configure the LDAP Server to connect to the CMG database with administrator credentials.
 - a. Click Next to proceed with LDAP Server installation.
 - b. Specify the installation path for the LDAP Server and click Next.
 - c. Specify the server where the CMG database is installed and the login credentials to access the SQL server. Click **Next**.
 - d. Click Finish to complete the LDAP Server installation.
- For BluStar Server component installation, the Wizard system launches the BluStar Server Setup wizard. When you have reviewed the End User License Agreement, select "I accept the terms of the license agreement" and click Next.



10. Select the BluStar Server installation type and click Next.

	Mitel BluStar Server Setup		
🛤 Mitel	BluStar Server		
	Please select your BluStar Server installation type:		
	⑦ [Default (Single server installation]		
	C Custom (e.g. Multi server installation or special installation folder)		
Cancel	< <u>B</u> ack <u>N</u> ext>		

11. Select your call manager platform type and click Next.



12. Enter the IP address of the call manager and click Next.

	Mitel BluStar Server Setup	x
🕅 Mitel	BluStar Server	
	Please enter the IP address of the PBX	
	IP address 192	
Cancel	< <u>B</u> ack <u>N</u> ex	a>

13. Enter the IP address or FQDN of the SQL server or click **Browse** to search for it. Specify the SQL login credentials and click **Next**.

	InstallShield Wizard	×
🔀 Mitel 🛛	BluStar Server	
	Select the SQL Server to install to from the fit below or click <browse> to Servers. Please also specify a SQL Login ID and Password to authenticate be performed after pressing <nexb. SQL Server: SQL 2008SERVER Please enter the SQL-Server authentication: Login ID: sa Password:</nexb. </browse>	see a list of all SQL A connection test will Browse - Database Server × Browse - Database Server × From the list of servers below, select the database server you like to target. SOLEXONSEERVER VCENTERIVIM_SOLEXP
Cancel	< <u>B</u> ack	OK Cancel

The Wizard installs the BluStar Server components.

- **14. For InAttend Server (CMG) installations only**: There are additional configuration steps when you install InAttend in a CMG system.
 - a. Specify the credentials to access the Telephony Configuration Application (TCA) and Telephony Configuration Service (TCS) services and click **Next**.

Mitel BluStar Server Setup			
🕅 Mitel	BluStar Server		
	Please enter the necessary parameters to logon to TCA/TCS services		
	Server WIN2012R2		
	User niceadmin		
	Password aastra		
Cancel	< <u>B</u> ack <u>N</u> ext⇒		

b. Verify the URIs for the Authentication and Authorization (AnA) service and the NCLA service. Make the necessary changes and click **Next**.

Mitel BluStar Server Setup				
🕅 Mitel	BluStar Server			
	Please check the necessary URI parameters			
	AnA URI http://w/IN2012R2/nwana/anaservice asms			
	NCLA URI http://wIN2012R2/tcs/NclaProvider.asmx			
Cancel	< <u>B</u> ack <u>N</u> ex	6		

c. Verify the URIs for the User Manager Service and the Configuration Manager Service. Make the necessary changes and click **Next**.

	Mitel BluStar Server Setup	x
🛤 Mitel	BluStar Server	
	Please check the necessary URI parameters	
	User URI [http://WIN2012R2/tcs/usermanager.asmx	
	Conf URI http://WIN2012R2/tcs/configurationmanaget.asmx	
Cancel	< <u>B</u> ack <u>N</u> ext >	

d. Specify the server hosting the CMG database and the name of the database and click Next.

Mitel BluStar Server Setup		
🕅 Mitel	BluStar Server	
	Please enter the necessary parameters to access the CMG database	
	Server WIN2012B2	
	Database nice	
Cancel	< <u>B</u> ack	lext>

The Wizard creates the specified databases and starts the required services.

- **15.** When installation of the BluStar Server component is complete, click **Finish** to close the BluStar Server setup wizard.
- **16.** In the main InAttend Install Wizard, review the information about InAttend Quick Configuration and click **Continue** (you will access the Quick Configuration tool later).

D InAtt	end 2.2 (4.2015) - Alpha Installer
🛤 Mitel InAttend	
Sefore the Installation	InAttend Quick Configuration
Configure BluStar Web Service	For custom installations, use the classic Browse Packages.
InAttend Quick Configuration	Run this tool once, to deploy an initial configuration on your system.
Restart InAttend Server	Click here to change machine name.
	Launch InAttend Quick Configuration Web on 'MAIN' .
	\sim
Click 'Continue'.	Cgntinue Cancel

17. When the installation is complete, you are prompted to restart the InAttend server. Click **Continue** or **Click here to restart**... to restart.

Installation of the InAttend Server is complete. You are now ready to configure the system.

Configuring the InAttend system

After the server has restarted, you have to configure the InAttend system.

- You use the Quick Configuration Wizard to configure ACS parameters (only after initial installation). The required components are also created in the Telephony Configuration Application (TCA).
- You use the BluStar Server Administration tool (WebAdmin) to configure PBX links, Presence Server, and InAttend user configuration profiles.

Running the Quick Configuration Wizard

The InAttend Initial Configuration Wizard allows you to set system parameters quickly and easily.

- On the InAttend Server, launch the Quick Configuration wizard (click Start > Programs > Mitel > InAttend Quick Configuration).
- 2. Log in using the default credentials (Username: admin, Password: Mitel123).

-		- U ×
← → Ø http://localhost/AttendantCo	nfigWeb/Authentication/SignIn	.⇔+¢ fi ★ #
InAttend Quick Configurati ×		
	InAttend Quick Configuration	
	Username	
	admin	
	Password	
	Sign in	
	ugnin	

3. In the Initial Configuration box, click Launch Wizard.

🛤 Mitel 🛛	InAttend Quick Configuration	Sign Out
	Initial Configuration Wizard The InAttend Wizard will guide you during the process of setting up ACS, InAttend and BluStar server components on a single server. The wizard is only intended to run once on a new installation, to setup the initial configuration in order to get started. Launch Wizard	
	Advanced Configuration To get access to more configuration settings for ACS, InAttend and BluStar Server, the web configuration applications TCA for ACS and WebAdmin for InAttend and BluStar Server can be used. Open InAttend Configuration	

The Quick Configuration page launches. The following tables describes the parameters you can configure:

Call Manager	
Call Manager Type	Select the appropriate call manager (platform) from the drop-down list. Note! By default, the call manager type shown is Mitel-MiVoice MX-ONE . You can select the required call manager type from the drop-down list.
Call Manager IP or FQDN	Enter the IP address or FQDN of the platform.(Not visible when selecting Skype as Call Manager Type.)
Enable TLS and SRTP	Select this option to enable encryption. (This option is only available when certificates are installed on the server.)
Certificate	Select a certificate from the list of installed certificates.(This option is only available when TLS and SRTP are enabled.)
Device Range (start/end)	Enter the range of extension numbers for all phones on the platform.
Hybrid with Microsoft Skype for Business	Select this option to use Microsoft Skype as a presence server in conjunction with another Call Manager. (This option is available only when Skype is not selected in the Call Manager Type field.)
Use E.164 Number Format	Select this option to enable E.164 format in the system. (Example +46 8 568 67 xxx.)

Microsoft Skype for Business (only displayed when S4B is selected as Call Manager or Hybrid)		
Server Name	Enter the name of the Skype server.	
SIP domain	Enter the (Normally	SIP domain for which Skype will act as a phone manager. this is the string after the @ in the SIP address.
User URI	Enter the address.	system user name for InAttend in Skype, including full domain
Application Name	Enter the name of the trusted application in the Skype management pool.	
Application Port	Enter the port number the Skype application will use.Default port is 6000.	
Application User Agent URI	Enter the Globally Routable User-Agent URI of the Skype application. This is the SIP URI which identifies a specific user agent.	
Certificate Name	Enter the certificate name created by Skype for the BluStar server.It is required for TLS and SRTP encrypted communication.	
Federate Presence	Activate this option to enable telephone line state changes (busy, out, etc.) from the presence server to be published and used by Skype and Skype Users.	
LDAP filter	This value acts as a key that the presence server uses to look up relevant user info. It then pushes that info towards Skype.Default value is "(mail=*)".	
Cisco Unified Communication Manager (only displayed when Cisco is selected as Call Manager)		
Cisco CUCM AXL User		Enter the user name of the AXL User.Needed to set forwarding from the InAttend Client.
Cisco CUCM AXL Password		Enter the password of the AXL User

Application Services	
ACS Server Hostname	Enter the hostname of the Attendant Communication Server.
ACS Server IP	Enter the IP address of the Attendant Communication Server.
Use CMG	Select this box for CMG installations of InAttend.

CMG (only displayed when Use CMG is selected)		
CMG Server	Enter the hostname of the CMG Server.	
Email Field	Select the field that contains email addresses in CMG.Default is "FirstMessageSystemId".	

LDAP Server (only displayed when CMG is NOT selected)		
LDAP Server	Enter the IP address of the LDAP server used for directory look-ups.	
Port	Enter the TCP/IP port number to use for LDAP communications Default is 389.	
Search Base	Configure the LDAP connection to where you have installed the LDAP server (BluStar Server or Active Directory).Default is "c=com".	
SIP Address Field Name	Enter the SIP Address field name from the LDAP database (used to look up presence subscription information). The default value is "sipAddress".	
Authentication	Select the type of credentials used to access the LDAP server. Anonymous (default), Username, or Username and Domain.	
User Name	Enter the user name of the authorized credentials for LDAP server access. (Not displayed when "Anonymous" is selected for Authentication.)	
Password	Enter the password of the authorized credentials for LDAP server access. (Not displayed when "Anonymous" is selected for Authentication.)	
Domain	Enter the domain used for LDAP server access. (Not displayed when "Anonymous" or "Username" is selected for Authentication.)	

Queues	
External Access Number	Enter the number that external users dial to contact the Attendant.
External Queue Time setting	Select Basic to apply the same time interval for all days.Select Per Day to configure up to two time intervals per day.
External Queue Time (from/to)	Set the time interval for when the queue is active.
Internal Access Number	Enter the number that internal users dial to contact the Attendant. Default is 09.
Internal Queue Time Setting	Select Basic to apply the same time interval for all days.Select Per Day to configure up to two time intervals per day.
Internal Queue Time (from/to)	Set the time interval for when the queue is active (same as External Queue).

Microsoft Exchange Calendar (if CMG Calendar Connection is used – Skip this section)	
Configure Exchange	Select this check box to use Microsoft Exchange Calendar integration. When selected, the settings below become available.
Server	Enter the host name of the Exchange server.

Mail domain	Enter the mail domain (the string after "@" in Exchange email addresses).		
Use HTTPS	Select this check box to use secure HTTP.		
Username	Enter the user name to access the Exchange server.		
Password	Enter the password to access the Exchange server.		
Domain	Enter the domain used to connect to the Exchange server.		

Add Users		
Add new user	Select this check-box to add an InAttend user.	
User name	Enter the user's name.	
Email	Enter the user's email address.	
Password	Assign a password to the user.	
Add new user	Select this check-box to additional InAttend users.	

- 4. When you have made the required configuration entries, click **Apply Configuration**.
- 5. When the configuration process is complete, reboot the InAttend server.

NOTE: At this point all the required components are configured in the Telephony Configuration Application (TCA). If you want to make changes to the existing configuration of your telephony services in TCA, see "Appendix A: Configuring telephony services in TCA".

InAttend Journal Configuration

The InAttend client has a journal feature displaying the call history for the attendants.

This information is stored in the database by InAttend History Service. InAttend History Service has to be installed on the same server as the InAttend Server (DAL Service).

- If a single ACS Queue Manager is used and is installed on the same server, no configuration is required. Also, if a single ACS Queue Manager is used and the system has been configured with the InAttend Quick Configuration wizard, to manual configuration is required.
- If ACS Queue Manager is installed on another server, InAttend History Service has to be configured to point to the location of all ACS Queue Manager Services.

The configuration can be made in AttendantHistoryServiceConfig.xml located in the folder where InAttend History Service is installed, typically:

C:\Program Files (x86) \Mitel\InAttendHistoryService\

The configuration file has a section QueueManagerList where multiple QM entries can be added, each pointing to a Queue Manager server. The default configuration looks like below, and is modified if Queue Manager is located on another server:

<QueueManagerList> <QueueManager>localhost</QueueManager>

CONFIGURING THE INATTEND SYSTEM

</QueueManagerList>

After making configuration changes to the configuration file, the Windows service InAttend History Service has to be restarted.

Configuring the Authentication and Authorization (AnA) web service

The Authentication and Authorization Service (AnA) Web Service is used to verify that the administrator users and InAttend attendants are authorized to use certain services when logging in to InAttend. The AnA web service can connect to the CMG Server (for CMG installations) or the BluStar Server (for standalone installations).

- If you are using InAttend with CMG, the AnA web service is already installed. •
- If you are using InAttend in a standalone deployment, you have to install the AnA web service from the Installation wizard.

Configuring the AnA connection to the CMG server

By default, the AnA connects to the CMG database as "localhost", using the same credentials that Configuration Manager uses. If you do not want to use the default setting, you have to configure the web.config file for AnA so that the AnA web service can connect to the CMG database server.

- 1. Open the web.config file for AnA.
- 2. Change the value of the following parameter by replacing "localhost" with the new CMG database server:

<add key="DefaultDatabaseServer" value="localhost"/>

3. Change the value of the following parameter to from "true" to "false":

<add key="FetchDbUsernamePassword" value="false"/>.

4. Save your changes to the file.

Configuring the AnA connection to a Different Server

By default, TCS and TCA connect to the AnA web service as "localhost". If you do not want to use the default setting, you have to configure the web.config file for TCS and TCA in order to connect to AnA when located on a different server.

- 1. Open the web.config file for TCS and TCA.
- 2. Change the value of the following parameter by replacing "localhost" with the server hosting the AnA web service:

<add key="anaUrl" value="http://localhost/nwAna"/>

3. Save your changes to the file

Enabling HTTPS for Image Fetching

The InAttend Client fetches the image from the logical image directory (**LogicImageDir**) configured in the CMG CM. This can be secured by configuring both CMG CM and CMG DM to use HTTPS.

User image parameters		
ShowImages	ENABLED	Defines whether or not the users photo should be shown
PictureField	TELNO - Phone	Defines the field containing the reference to the image
PhysImageDir	c:\inetpub\www.root\CMG Office\subscriberimages\	Defines the physical image directory (Format: E.g. C:\inetpub\www.root\CMGOffice\subscriberimages\)
LogicImageDir	/CMGOffice/subscriberima ges	Defines the logical image directory (Format E.g. /CMGOffice/subscriberimages)
PictureFileExt	JPG 🗸	Defines the image file extension. NOTE! png is not valid for NOW
ImageHeight	106	Defines the height of the image (Default value: 106)
ImageWidth	79	Defines the width of the image (Default value: 79)

The steps to be followed for CMG deployment are as below:

- 1. Open CMG Configuration Manager and expand CMG Web Components.
- 2. Click Parameters and do the following:
 - a. Verify/Change the physical image directory in: PhyscImageDir
 - b. Verify/Change image directory path in: LogicImageDir
 - c. Verify/Change image file extension in: **PictureFileExt**
 - d. Add the extension number to provide a reference to the image in: PictureField
 - e. Change the status to enabled in: ShowImages

In the scenario, where the InAttend client is a standalone deployment or the LogicImageDir is not specified in the CMG Deployment, the images are fetched from the Webadmin directory and the InAttend client falls back to look at http://serverlp>/webadmin/subscriberimages/

To allow secure transmission of the image, the **Special settings** must be enabled in the Webadmin to securely fetch the image using HTTPS.


To enable HTTPs in the InAttend Client, do the following:

- 1. Go to Attendant Special Settings
- 2. Enter the name as Image Over Https to the Profile name field
- 3. Enter a description in the **Description** field
- 4. Enter the value as Image Server HTTPS in the Parameter field
- 5. Enter the value as 1 in the Parameter value field
- 6. Click the button and the settings gets reflected in the right-side window pane
- 7. Click **Save**to save your changes

After adding the parameter for enabling the HTTPs, restart the iisreset command.



Configuring the Presence Server

The BluStar Presence Server can aggregate presence information from Microsoft Exchange and Microsoft Skype for Business, as well as line state information from the call manager, and provide the information to InAttend clients.

You have to configure the data sources from which the Presence Server receives presence information. InAttend supports the following types of data sources for presence information:

- Microsoft Exchange
- Microsoft Skype for Business
- Line status (from a PBX)

NOTE: If you configured Exchange or Skype for Business settings during configuration of the InAttend Server (see "Running the Quick Configuration Wizard"), a data source for the Presence Server is already present.

Viewing Presence Server Configuration

To view Presence Server configuration, do the following:

- 1. Access the BluStar Server Administration web interface by typing the URL: http://<hostname>/webadmin in a supported web browser, where <hostname> is the InAttend server address.
- 2. Log in with the administrator credentials (default username: admin, default password: Mitel123).
- 3. Select Presence Server and then Configuration.

The system displays current Presence Server configuration, including any data sources created during initial configuration of the InAttend server.

🔀 Mitel	User Configuration	CTI Server	Presence Server	Tools Help		
Presence Server	r configuration	1	Presence Interface	20		
WIN2008R2	-	1	3	- 15	Avera and	-
Server					Save	
WIN2008R2	WIN2008R2					
	Data sources					
	Name WIN2008R2	Uni	state O	select data source -	Add data source	
	Authentication					
	Check user credentials again	nst AD				
	Trace Configuration Set trace					

4. In the **Authentication** section, you can enable or disable the option to check user credentials against Active Directory (enabled by default).

When subscribing to presence information about other users, and to publish presence status, InAttend users have to provide their Active Directory credentials. The BluStar Server verifies that the credentials match the information for the user in Active Directory.

- 5. In the **Trace Configuration** section, click **Set trace** if you want to enable trace functionality
- 6. On the Trace configuration page, enter values for the following parameters:
 - Number of log files: number of log files generated by the system (default is 10).
 - Max. size of file: maximum size of the file before existing data is overwritten with new data (default is 5MB).
 - File name: the path and file name for the log file.
 - Error | Info | Debug: select one option to specify the level of detail in the log file. Error level contains the least amount of information, and Debug contains the most detail.
- 7. Click Save to save your changes.

Adding a Microsoft Exchange Data Source

You can configure a Microsoft Exchange Server as a calendar source for presence information on the Presence Server. InAttend clients can subscribe to the calendars of specific users from Microsoft Exchange, to receive events when appointments are modified or start and finish.

You have to configure an Exchange user account on the Exchange Server that can access multiple Microsoft Exchange calendars.

To add a Microsoft Exchange data source, do the following:

1. On the Presence Server configuration page, select the **Exchange (Calendar)** option from the data source type drop-down list and click **Add data source**.



- 2. On the new Exchange data source page, specify a name for the data source in the **Data source name** field (has to be unique in the Presence Server configuration).
- 3. Optionally, enter a valid email address (has to be configured on the Exchange data source) and click **Test connection** to verify that the Exchange Server is reachable.

Server				Save Back More
3	win200882	Exchange Data source name	Email address	Test connection

- 4. In the Connection data section, specify the Exchange Server address and the user credentials for the account created to access the Exchange Server:
 - Server name: the hostname or IP address of the Exchange Server.
 - Mail domain: postfix (i.e., string after @) of the email addresses on the Exchange Server.
 - Username: the username for the account created to access the Exchange calendars.
 - **Password**: the password for the account created to access the Exchange calendars.
 - Domain: the Windows domain of the Exchange Server.

Connection data	
Server name	Usemame
Mail Domain mitel.com	Password .
hans.test@mitel.com	Domain

- 5. In the Access type section, select the method used to access the Exchange Server. For Microsoft Exchange 2007, 2010, or 2013, select WebService(2007, 2010, 2013) and enter values for the following fields:
 - Access protocol: select the protocol used to communicate with the Exchange Server (http or https).
 - Authentication: the method of mailbox access configured on the Exchange Server (impersonation or delegation).
 - Use notification service: enable to use the Mitel Presence Notification service for Exchange calendar updates (recommended).

When enabled, the Presence Server polls the Notification Service for Exchange calendar updates and fetches changed calendar information from the Exchange Server directly (based on notifications received by the Notification Service).

- Use autodiscover service: enable to retrieve the Exchange Server assigned for the user (for Microsoft Exchange Online / 365 only).
- Request URL: If you enabled the Use notification service option, specify a URL for the Notification Service that can be accessed from the Exchange Server.
- Event URL: Specify a URL to be used by the Exchange Server when changes occur on subscribed mail boxes.
- 6. Click **Save** to save your changes.
- 7. Click **More** in the upper right corner of the page to configure the visibility of Exchange calendar events in the InAttend client.
- 8. On the advanced configuration page, enter values for the following fields:
 - Update interval: the refresh interval between calendar event updates from the Exchange Server.
 - Time Offset: the offset to apply to calendar event times, if the InAttend Server and the Exchange Server are in different time zones.
 - Categories of calendar entries to be published: select the type of calendar entries to be published to InAttend clients.
 - Override calendar entries' properties by static text before publishing: enable if you want to substitute the public calendar entry's Subject and Location information with a specific text string.
 - Replace "Subject" by: the text to replace the Subject property of the public calendar entry.
 - **Replace** "Location" by: the text to replace the Location property of the public calendar entry.
 - Show private appointments: enable to publish calendar entries marked "private".

- Replace "Subject" by: the text to replace the Subject property of the private calendar entry.
- Replace "Location" by: the text to replace the Location property of the private calendar entry.
- 9. Click **Save** to save your changes.
- 10. Click **Back** to return to the Exchange data source page.
- 11. Click **Back** to return to the main Presence Server configuration page.

The new Exchange data source appears in the list of Presence Server data sources on the main Presence Server configuration page.

Adding a Microsoft Skype for Business Data Source

You can configure a Skype for Business Server as a source for presence information on the Presence Server. Microsoft Skype provides presence information about its users, but also publishes presence information about InAttend users on the Microsoft presence server.

Note the following requirements:

- The InAttend Server belongs to the same domain as the Microsoft Skype Server.
- InAttend supports only Microsoft Skype for Business 2015 or later for presence.

Installing the Unified Communications Managed API (UCMA)

You have to install the Unified Communications Managed API (UCMA) component on the InAttend Server before configuring the system for Microsoft Skype presence. The system uses the UCMA to communicate with the Microsoft Skype Presence and Instant Messaging (IM) system.

NOTE: The Desktop Experience feature has to be activated prior to the UCMA installation. You activate this feature using the Windows Server Manager.

To install Unified Communications Managed API (UCMA), do the following:

- 1. Double-click the **Install.exe**file in the top-level directory of your software package to launch the Mitel Installer.
- 2. In the Installer main window, click Browse Packages.
- 3. In the left panel of the Installation Wizard, expand the **Optional Server Components** folder and then expand the **Microsoft Skype for Business 2015 Presence Information** folder.
- 4. Select the **Unified Communications Managed API** component and in the main Installer window, click the **Install Unified Communications Managed API** ... link.
- 5. In the Runtime Setup window, click Next.
- 6. On the End User License Agreement page, review the terms of the license agreement, then check I accept the terms in the License Agreement and click Next.
- 7. When the wizard completes the UCMA installation, click Finish to exit.

Setting up the Microsoft Skype for Business environment

Before you can configure the Presence Server to exchange presence information with the Skype for Business server, you have to complete the following tasks on the Skype for Business server:

- create a single application pool for the InAttend Server
- · create a trusted application for the application pool

You have to be logged in as a user with domain administrator rights.

NOTE: The following instructions are intended for experienced and certified Microsoft professionals. Failure to run commands properly may have significant consequences on the Microsoft Skype for Business environment.

Creating an application pool in Skype for Business

To create the application pool and trusted application, do the following:

- Launch the Skype for Business 2015 Topology Builder (Start > All Programs > Microsoft Skype for Business 2015 > Skype Server Topology Builder).
- 2. On the Welcome page, select the **Download Topology from existing deployment** option and click **OK**.



The system downloads the topology for you deployment.

- 3. In the Save Topology As window, specify a name for the XML backup and click Save.
- In the left navigation panel, browse to the Skype for Business 2015 > Trusted application servers folder.
- 5. Right-click on the Trusted application servers folder and select New Trusted Application Pool.

CHAPTER 7

- 6. In the Define New Trusted Application Pool window:
 - a. Enter the Fully Qualified Domain Name (FQDN) of the InAttend server in the FQDN field.
 - **b.** Select the **Single computer pool** option.
 - c. Click Next.
- 7. On the **Select next hop server** page, you can optionally specify a pool to be used as the next hop server for the Trusted Application pool.
- 8. Click Finish when you have completed your changes.

Creating a trusted application in Microsoft Skype for Business

The trusted application for InAttend requires a unique ID. The FQDN is the fully qualified domain name of the InAttend server, and the port corresponds to the listening port on the InAttend server.

You create the trusted application with the Skype for Business Server Management Shell tool.

- Launch the Skype for Business Server Management Shell as an administrator (Start > All Programs > Microsoft Skype for Business Server 2015 > Skype for Business Server Management Shell).
- 2. Enter the following command to create the trusted application:

```
New-CsTrustedApplication
-ApplicationId <app_ID>
-TrustedApplicationPoolFqdn <InAttend_FQDN >
-Port <port on InAttend>
```

3. Enter following command to enable the topology:

Enable-CsTopology

4. Restart the Skype server.

Creating and importing certificates

If you have not already done so as part of Microsoft Skype for Business call manager configuration, you have to create and import the required certificates.

See "TLS certificates installation" for instructions.

Adding a Data Source

When you have completed configuration of the Skype for Business environment, you can configure the Presence Server with a Skype for Business data source.

NOTE: You can use the Get-CsTrustedApplication command in the Lync Server Management Shell tool to obtain the Skype information necessary for data source configuration.

To add a Skype for Business data source, do the following:

1. On the Presence Server configuration page, select the **Skype** option from the data source type drop-down list and click **Add data source**.



- 2. On the new Lync data source page, specify a name for the data source in the **Data source name** field (has to be unique in the Presence Server configuration).
- 3. Optionally, enter a valid SIP address and click **Test connection** to verify that the Lync Server is reachable.
- 4. In the Connection data section, enter values for the following parameters:
 - Server name: hostname or IP address of the Lync Server.
 - SIP domain: postfix (i.e., string after @) of the SIP addresses for Lync users.
 - User URI: a valid SIP URI for a Lync user (required to identify the endpoint on the Lync Server).
 - Application name: the name of the trusted application created for the InAttend Server on the Lync Server.
 - Application port: the port of the trusted application created for the InAttend Server on the Lync Server.
 - Application user agent URI (GRUU): the Globally Routable User-Agent URI (GRUU) of the trusted application.
 - Certificate name: the name of the certificate created for the InAttend Server.
 - Federate Presence: enable to have the Presence Server publish line state changes or InAttend client presence changes to Lync users.

 Activate permanent subscriptions: enable to keep subscriptions independent from the InAttend clients subscribing to them (e.g., to federate the line state of phones without an active InAttend client).

Server	Save Back
WIN2008R2	Lyne
	Data source name SIP address Test connection
	Connection data
	Server name
	SIP domain
	User URI
	Application name
	Application port
	Application user agent uri (Gruu)
	Certificate name
	Federate Presence
	Activate permanent subscriptions
	LDAP filter (telephoneNumber=")

5. Click **Save** to save your changes.

The new Lync data source appears in the list of Presence Server data sources on the main Presence Server configuration page.

Adding a CISCO Data Source

In an InAttend system with a Cisco Unified Communication Manager (CUCM), the InAttend Presence Server obtains presence information from the Cisco Unified Presence Server (CUPS).

You have to configure the Cisco Unified Presence Server (CUPS) to connect to the InAttend Presence Server, and perform additional configuration on the InAttend Presence Server before adding the Cisco data source.

Configuring the Cisco Unified Presence Server (CUPS) for InAttend

To configure the CUPS for a connection with the InAttend (BluStar) Presence Server, do the following:

- 1. Log on to the web-based Cisco Unified CM IM and Presence Administration tool.
- 2. Ensure that the SIP Listener port is on:
 - a. Select System > Application Listeners.
 - b. Check that there is a Listener Type of "SIP", with the port set to 5060.
 - c. Click Save to apply your changes.
- 3. Add the InAttend Presence Server IP address to the CUPS' incoming access control list (ACL).
 - a. Select System > Security > Incoming ACL.
 - b. Click Add New.
 - c. Enter the incoming ACL configuration settings (description and IP address for the InAttend Presence Server).
 - d. Click Save to apply your changes.
- 4. Check the SIP domain of the CUPS by selecting **Presence > Domains**.

Configuring the Presence Server for CUPS

To configure the Presence Server to obtain presence from the Cisco Unified Presence Server CUPS), you have to first create a data source type for the CUPS, then add a data source for the CUPS.

To configure the Presence Server for CUPS, do the following:

- 1. In the WebAdmin tool, select **Tools** and then **Administration settings**.
- 2. Create a new parameter for the CUPS:



- a. In the Section field, enter "PresenceServerDatasources"
- b. In the Parameter name, enter "CUPS".
- c. Click Add.

The new parameter appears in the parameter table.

3. For the new CUPS parameter, set the Parameter value to "true".

BluStar Server Administration »	admin		(DAL: IN/	ATTEND22 / DB: INATTEND22)	
🕅 Mitel	User Configuration CTI Server	Directory Server Pres	sence Server Tools	Help	
Administration set	tings	1	2	4	-
InAttend22 Session timeout (min) [60 Refresh interval (sec) [5 Section	Parameter name	Add Defa	uit Reset	Seve	
Parameter name	Parameter value	Default			
DBMaintenance			^		
Active	1				
PbxLinkList					
3Com NBX 100	false	1			
PresenceServerDatasources					
CUPS	true		~		
Quicklinks (PBX links) (Direc	ctory Server Configuration Presence Server	Configuration Presence Inter	face Service manager		

- 4. Click Save to apply your changes.
- 5. Select Presence Server and then Configuration.
- 6. On the Presence Server configuration page, select the CUPS (Presence) option from the data source type drop-down list and click Add data source.
- 7. On the new CUPS data source page, specify a name for the data source in the **Data source name** field (has to be unique in the Presence Server configuration).
- 8. Optionally, enter a valid SIP address and click **Test connection** to verify that the Cisco Unified Presence Server is reachable.
- 9. In the Connection data section, enter values for the following parameters:
 - Server: hostname or IP address of the CUPS.
 - TCP port: TCP port for the CUPS.
 - UDP port: UDP port for the CUPS.
 - SIP domain: postfix (i.e., string after @) of the SIP addresses for Cisco users.

Presence Serv	er configuration	2 20	- 1
Server	CUPS Data source name CUPS Connection data Server 10.105.87.9 TCP Port 5066 UDP Port 5066 Sip domain Svc.se.aastra.com	SIP address	Save Back Test connection

- 10. Click Save to apply your changes.
- 11. Click **Back** to return to the Presence Server configuration page.

Adding a line state data source

The Presence Server uses line state information to calculate user availability. You have to configure a line state data source for the PBX as a source for the Presence Server in addition to other data sources (e.g., calendar).

- For MX-ONE and MiVoice 5000 call managers, the Presence Server requests line state information through the CTI Server component of the BluStar Server (which handles PBX links).
- For Cisco call managers, the Presence Server requests line state information through the ACS Cisco Line State Server component (an optional InAttend software component that has to be installed separately from the InAttend Installation Wizard. See "component "for detailed instructions.

By default, the Presence Server retrieves line state information for all extensions configured on the PBX's. If you want to restrict the extensions for which line state information is requested, you can specify one or more ranges, patterns, or prefixes to identify the extensions.

To add a Line state data source, do the following:

1. On the Presence Server configuration page, select the **Linestate** option from the data source type drop-down list and click **Add data source**.

Prese WIN20:	nce Serve	er configuration	
Server			Save
	WIN2012R2	WIN2012R2	
		Data sources	
		Name	Exchange (Calendar)
		Authentication	NetCom (Linestate)
		Check user credentials against	AD
		Trace Configuration	
		Activate trace	error
		Number of log files 10	info
		Max. file size (MB) 5	ø debug
		File name C:\Progra	m Files (x86)\Aastra\BluStar Server\Trace\PresenceServer\PresenceServer.log

- 2. On the new Linestate data source page, specify a name for the data source in the **Data source name** field (has to be unique in the Presence Server configuration).
- Optionally, enter a valid extension number in the Device field and click Test connection to verify that the PBX is reachable via the CTI Server.
- 4. In the Connection data section, enter values for the following parameters:
 - Server name: hostname or IP address of the machine hosting the CTI Server (for MX-ONE), or the machine hosting the ACS Cisco Line State Server (for Cisco Unified Communications Manager).
 - Port: the port of the CTI Server or ACS Cisco Line State Server (default is 5077, but has to be the same as the value configured on the CTI Server).

- Backup server: hostname or IP address of the backup CTI Server, if available.
- Port: the port of the backup CTI Server (default is 5077).
- 5. If you want to restrict the extensions for which line state information is retrieved, click the **Advanced** button beside the Connection data box.

Server				Save Back
3	WIN2008R2	Linestate Data source name	Device	Test connection
		Connection data	Advanced	
		Server name WIN2006R2	Port 5077	
		Backup server	Port 5077	

NOTE: You can configure a combination of restrictions by range, prefix or pattern

- a. Range section: To specify one or more ranges of extensions to be monitored, enter values in the **From** and **To** fields and click the arrow button to add them to the list.
- **b. Pattern** section: To specify one or more patterns to identify monitored extensions, enter a value in the Pattern field and click the arrow to add the pattern to the list.

For example, if you specify a pattern of "8xxx", all extension numbers that start with "8" and that have a length of 4 tokens are monitored.

c. **Prefix** section: To specify a prefix for identifying monitored extensions, enter a number in the **Value** field (to a maximum of 3).

NOTE: If you configure a **Prefix** without **Delete** option, it is just a restriction.

For example, the extensions for DN 8002 and DN 8502 are monitored with the pattern "8xxx" specified, if the prefix is not configured.

- If you specify a prefix of 800, you get the line state for DN 8002 and not for DN 8502.
- If you specify a prefix of 850, you get the line sate for DN 8502 and not for DN 8002.
- d. **Domain/Link**: If multiple PBX links are used to connect to multiple communication servers, the PBX link to be used for this specific data source can be identified by the number / index of the PBX link, as shown in the PBX links list on the **CTI Server -> PBX links** page.

Enable the **use specific domain/link** option and specify the PBX link number.

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

The new Line state data source appears in the list of Presence Server data sources on the main Presence Server configuration page.

Configuring a PBX link for line state (MX-ONE)

A PBX link is a connection from the CTI Server (a component of the BluStar Server) to an MX-ONE call manager. The InAttend system can support multiple PBX links simultaneously (for example, for installations with multiple offices that have separate communication servers).

You create a PBX link so that the CTI Server uses the PBX link to retrieve line state information about specified devices.

To create a PBX link, do the following:

- 1. Access the BluStar Server Administration web interface by typing http://<hostname>/webadminin a supported web browser, where <hostname> is the InAttend server address.
- 2. Log in with the administrator credentials (default username: admin, default password: Mitel123).

3. Select CTI Server and then PBX links.



The system displays the PBX links page and lists all configured PBX links.

4. On the PBX links page, click Add PBX link.

PBX I	links				1		8	_
	0	-			JAN AND AND AND AND AND AND AND AND AND A	0		
Server							Refresh Add	I PBX Link
3	WIN2012R2	All	Servers					
-1	All Servers							
			75	PBX link	PBX link No.	Server	1	

5. On the PBX link configuration page, enter values for the following parameters:

PBX link name: the name for the connection. **Server**: select the InAttend Server from the drop-down list.

6. In the Telephone system section, enter values for the following parameters:

PBX link confid	uration			
PDA IIIK comi	Juración	Rea -		
Properties	PBX link name MX-ONE Server WIN2000R2	PBX link number 1		Back to the link list
Telephone system	Telephone system			
Telephony	Talanhona sustam	MILLER MY ONE		
Direct connection	response system	MINDLE NO-UNC	-	
Server settings	PBX connection	Direct Connection	v	
Number alignment	Recognition of external /	Prefa	~	
	internal phone numbers.	1.1108	-	
	Value	0		
	Handling of outgoing numbers	None	v	
	Handling of incoming numbers	None	~	

Telephone system: the PBX type (e.g., MiVoice MX-ONE); select a value from the drop-down list. **PBX connection**: the type of PBX connection (value is pre-populated based on the type of telephone system selected).

Recognition of external/internal phone numbers: select the method that the PBX uses to differentiate internal and external device numbers (by prefix, by length of device ID, or by an explicit or implicit flag for external numbers).

Value: (dependent on the value for Recognition of external/internal phone numbers).

- If you selected **DeviceID length**, enter the maximum internal device number length + 1.

- If you selected **Prefix**, enter the value prepended to numbers to identify them as external numbers.

Handling of outgoing numbers: select the method used by the CTI server to handle outbound calls from the drop-down list (dependent on how the PBX is configured; default value recommended). **Handling of incoming numbers**: select the method used by the BluStar server to handle incoming calls from the drop-down list (dependent on how the PBX is configured; default value recommended).

7. Click on **Telephony** in the left panel to configure telephony options for the PBX.

PBX link configu	Iration	2.4	2.1	-
Properties	PBX link name MX-ONE Server WIN2000R2	PBX link number 1	80	(A to the link list
Telephone system	Telephony			
Telephony	External line prefix			
Direct connection Server settings	Area code prefix			
Number alignment	Area code			
	Use phone number block from	10		
	Extended device checking			
	Host prefix			

External line prefix: the prefix used for external extension numbers.

Area code prefix: the prefix to be used with the area code (e.g., "0" if the area code is "0711"). **Area code**: the area code of the server location.

Use phone number block from/to: the sequence of numbers from devices running on this link, if the devices have no link number.

Extended device checking: Enable to recognize hanging calls on the server. After a call is cleared, the CTI Server can synchronize the state with the PBX to remove any stale calls.

Host prefix: Enable if you have multiple call managers with the same device number ranges and need to specify a unique prefix.

If the PBX connection type is a direct connection, click **Direct Connection** to configure TCP/IP parameters for the PBX:

IP address: IP address of the PBX. **Port**: port for connecting to the PBX.

Path of Csta32.dll: path to the internal library used for the PBX connection; keep default value.

9. Click **Number alignment** on the left panel to configure translation of an incoming number to a different outgoing number, in cases where a call to a given device number has to be routed to a different number.

Specify an incoming and outgoing number pair, then click the arrow button to add them to the list.

PBX link config	guration	-	5		1	-	
Properties	PBX link name MX-ONE Server WIN200IR2	PBX I	nk number 1		Bei	A to the link list	
Telephone system Telephony Direct connection Server settings Number alignment	Number alignment (for even Node number incoming outgoing	ts)	Node	e number outgoing			

NOTE: This feature is only used when absolutely necessary. If there are any errors in the list, it may be difficult to determine why certain users are not reachable.

10. Click **Save** to save your changes.

The new PBX link appears on the main PBX links page.

Configuring a PBX link for line state (MiVoice 5000)

You must create a PBX link so that the CTI Server uses the PBX link to retrieve line state information about specified devices.

- 1. Log in to the **BluStar Server Administration** web interface, using administrator credentials.
- 2. Select CTI Server and then select the PBX links.



The system displays the PBX links page, and lists all configured PBX links.

3. On the PBX links page, click Add PBX link.



- 4. On the **PBX link configuration** page, enter values for the following parameters:
 - **PBX link name**: the name for the connection.
 - Server: select the InAttend Server from the drop-down list.

5. In the **Telephone system** section, enter values for the following parameters:

BluStar Server Administration »	admin		(DA	L: WIN-II	NATTEND / DB: WIN-INATTEND)
🕅 Mitel	User Configuration CTI	Server Directory Server	Presence Server	Tools	Help
PBX link configura	tion		1		12
Properties PB Set	X link name MiVoice5000 rver WIN-INATTEND	PBX link number			Save Back to the link list
Telephone system	elephone system				
Telephony	elephone system	MiVoice 5000			
Direct connection		Direct Connection			
Server settings	DA connection	Direct Connection	v		
Number alignment R	ecognition of external / ternal phone numbers	Prefix	~		
V	alue	0			
н	andling of outgoing numbers	None			
н	andling of incoming numbers	None	~		

- a. Telephone system: the PBX type (MiVoice5000); select a value from the drop-down list.
- **b. PBX connection**: the type of PBX connection (value is pre-populated based on the type of telephone system selected).
- **c.** Recognition of external/internal phone numbers: select the method that the PBX uses to differentiate internal and external device numbers (by prefix, by length of device ID, or by an explicit or implicit flag for external numbers).
- d. Value: (dependent on the value for Recognition of external/internal phone numbers).
 - i. If you selected **DeviceID length**, enter the maximum internal device number length + 1.
 - ii. If you selected **Prefix**, enter the value prepended to numbers to identify them as external numbers.
- e. Handling of outgoing numbers: select the method used by the CTI server to handle outbound calls from the drop-down list (dependent on how the PBX is configured; default value recommended).
- f. **Handling of incoming numbers**: select the method used by the BluStar server to handle incoming calls from the drop-down list (dependent on how the PBX is configured; default value recommended).
- 6. In the **Telephony** section, enter values for the following parameters:

🕅 Mitel	User Configuration	CTI Server	Directory Server	Presence Server	Tools	Help
PBX link configi	uration			1		Zn,
Properties	PBX link name MIVoice5000 Server WIN-INATTE		PBX link number			Save Back to the link lit
Telephone system	Telephony					
Telephony	Esternal line and for	0	-			
Direct connection	External line pretix	U				
Server settings	Area code prefix	0				
Number alignment	Area code	33	1			
	Use phone number block fr	rom	to			
	Extended device checki	ing				
	Host prefix					

- a. External line prefix: the prefix used for external extension numbers.
- b. Area code prefix: the prefix to be used with the area code (e.g., "0" if the area code is "0711").
- c. Area code: the area code of the server location.
- d. Use phone number block from/to: the sequence of numbers from devices running on this link, if the devices have no link number.
- e. Extended device checking: Enable to recognize hanging calls on the server. After a call is cleared, the CTI Server can synchronize the state with the PBX to remove any stale calls.
- f. Host prefix: Enable if you have multiple call managers with the same device number ranges and need to specify a unique prefix.
- If the PBX connection type is a direct connection, click **Direct Connection** to configure TCP/IP parameters for the PBX:
 - IP address: IP address of the PBX.
 - Port: port for connecting to the PBX.
 - Service ID: service ID to the PBX.



8. In the **Number alignment** section, enter an incoming and outgoing number pair, then click the arrow button to add them to the list.



NOTE: This feature is only used when absolutely necessary. If there are any errors in the list, it may be difficult to determine why certain users are not reachable.

9. Click **Save** to create the PBX.

The new PBX link appears on the main PBX links page.

Configuring a Line State Server (Cisco only)

InAttend does not use the CTI Server to obtain line state information from a Cisco call manager. To obtain line state from a Cisco Unified Communication Manager (CUCM), you have to install the Cisco Line State Server (LSS) component, using the Installation Wizard.

Installing the Cisco Line State Server (LSS) component

The Cisco Line State Server is an optional software component that you can install from InAttend Installation Wizard.

You have to have Microsoft .NET Framework 4.5 Full installed (available through the InAttend Install Wizard). If the InAttend server is running on Windows Server 2012/R2, .NET Framework 4.5 is already included.

NOTE: ACS Cisco LSS has to be installed by a user with Administrator rights.ACS Cisco LSS has to be uninstalled by the Administrator

If present, you have to uninstall the old SIP Line State Server (JLSS), before installing the Cisco Line State Server.

To install the Cisco Line State Server, do the following:

- 1. Double-click the **Install.exe** file in the top-level directory of your software package to launch the Mitel Installer.
- 2. In the Installer main window, click Browse Packages.
- 3. In the left panel of the Installation Wizard, expand the **Optional Server Software** folder and select **Cisco Line State Server**.



4. In the main window of the Install Wizard, click Install ACS Cisco Line State Server.

The Installation Wizard launches the Mitel ACS Cisco LSS Setup wizard.

5. On the Welcome page of the ACS Cisco Line State Server setup wizard, click Next.



6. On the End User License Agreement page, review the terms of the license agreement, then check I accept the terms in the License Agreement and click Next.

谩	Mitel ACS Cisco LSS Setup	, <u> </u>				
End-User Licen Please read the	ise Agreement	🕫 Mitel				
MITEL SOFTV	WARE LICENSE AGREEMENT	<u>^</u>				
Last Revised:	November 9, 2014					
This is a licen Sweden AB, ((herein the "L terms and con "Agreement") Programs un	This is a license agreement between you, the customer, and Mitel Sweden AB, (herein "Mitel"). By commencing using the software (herein the "Licensed Programs"), you agree to be bound by these terms and conditions of this software license agreement (herein the "Agreement"). Therefore, do not commence using any of the Licensed Programs until you have carefully read and understood the following v					
	Print Back	Next Cancel				

7. On the **Destination Folder** page, specify the installation path for the ACS Cisco LSS (or keep the default path) and click **Next**.

虔	Mitel ACS Cisco LSS Setup
1	Destination Folder Click Next to install to the default folder or click Change to choose another. Differ
	Install Mitel ACS Cisco LSS to:
	C:\Program Files (x86)\Mitel\AcsCiscoLSS\ Change
	Back Cancel Cancel

8. On the Ready to install Mitel ACS Cisco LSS page, click Install.

The wizard installs the ACS Cisco LSS component, and displays a progress bar.

ц.	Mitel ACS Cisco LSS Setup	_ 🗆 🗙
Installin	g Mitel ACS Cisco LSS	🕅 Mitel
Please wai	t while the Setup Wizard installs Mitel ACS Cisco LSS.	
Status:	Installing new services	
	Back	ext Cancel

- 9. When the wizard completes the Mitel ACS Cisco LSS setup, click **Finish** to exit.
- 10. Restart the server. Click the Click here to restart link in the Install wizard.

Configuring the ACS Cisco Line State Server

When the installation process is finished, the ACS Cisco Line State Server is configured with default values. If required, you can change configured values using the ACS LSS Config tool.

To modify default ACS Cisco Line State Server settings, do the following:

- 1. Launch the ACS LSS Config tool (**Start -> Programs -> Mitel -> ACS LSS Config**). The system launches the ACS LSS Config tool.
- 2. In the configuration tool interface, change the default values as necessary.

CHAPTER 7

ACS Cisco LSS config ×
SIP/SIMPLE Transport tcp V Local port 5070 🗘
AXL Poll interval (s) 10 Max update/min 50 Retry after ms 1000 100 AXL port 8443 Bulk max size 100 Bulk workers 3 100 Cisco "Forward to Voicemail" feature is enabled Image: State of the state of th
Log Level Debug+3 V Max size (MB) 10 2 Days to keep 14 2 Folder C:\ProgramData\Mitel\AcsCiscoLSS
<u>Save</u> D:\Program Files (x86)\Mitel\AcsCiscoLSS\ServiceConfig.xml

3. Click Save to save your changes.

Enabling a Secure Channel for AnA and TCA

To enable a secure communication channel for AnA and TCA do the following:

- 1. In the Webadmin, go to the User Configuration > Configuration Profiles.
- 2. Click on the listed PBX and select Properties.
- 3. In the **Properties > Interface**, enter the AnA Server and TCS Server path, as shown in the screenshot.

edit profile: InAttend		
Properties		Save Back
Interface	Profile name	InAttend
Settings	Description	Default Attendant PBX profile via ACS.
	External line prefix Maximum device length Company prefix Number format Display domain n Webservice AnA Server Inttp TCS Server Inttp	0 n 4 Classic ▼ ame DS://WIN-1A7HEK9NLVT DS://WIN-1A7HEK9NLVT

Configuring the Presence Interface

The Presence Server must be able to access an LDAP source to process line state. You configure the LDAP connection to the Mitel LDAP server or to an external LDAP source on the Presence Interface page.

By default, the internal BluStar directory server is defined as the LDAP database. It provides features to import content from multiple source servers. You can merge different data sources and grant access to both internal and external contacts without any additional load on the source systems.

If you are not using the BluStar LDAP database, you can configure the Presence Server to connect directly to one external directory (e.g., Microsoft Active Directory) via LDAP. Note that with this configuration, every directory lookup on the Presence Server (e.g. each subscription) represents a direct access to the external source.

NOTE: The Presence Interface configuration page is populated with the LDAP Server information you specified when running the Quick Configuration Wizard. Use this procedure to change those settings.

To configure the Presence Server interface, do the following:

1. In the WebAdmin tool, select Presence Server and then Presence Interface.



The system displays the Presence Interface configuration page.

Presence Inte	erface configuration	6		
WIN2008R2	-	Min -		
Server				Seve
WIN2008R2	WIN2008R2			
	SIP Configuration SIP TCP Port 5062	SIP UDP Port 5062		
	Directory Configuration	Email		Test connection
	O Default Advanced	() inactive		
	Server			
	LDAP Server	WIN2006R2	LDAP Port 389	
	Search base	c=com		
	Login			
	Anonymous	User or DN		
	O With user information	Password		
	O User and domain (ADS)	Domain		
	Attributes			
	Mail address	mail	SIP address sipAddress	
	Business phone	telephoneNumber	Private phone nomePhone	
	Mobile phone	mobileTelephoneNumber	Account name accountName	
	Search			
	dia a land	Taba belechonette	antur .	

2. In the SIP Configuration section, enter values for the following parameters:

SIP TCP Port: TCP port used for SIP (default is 5062) **SIP UDP Port**: UDP port used for SIP (default is 5062) 3. In the Directory Configuration section, select the mode of directory configuration:

Default: use the internal BluStar LDAP database (all configuration parameters are read-only) **Advanced**: specify an external LDAP database(remaining parameters are configurable)

4. If you selected the Advanced configuration mode, enter values for the following parameters:

In the Server section, identify the LDAP server:

LDAP server: the host name or IP address of the LDAP server.

LDAP port: the TCP/IP port for the LDAP server.

Search base: the base DN(i.e., the location in the directory from which the LDAP search begins). In the **Login** section, specify the method of authentication on the LDAP server:

Authentication method on the LDAP server (**Anonymous, With user information**, or **User and domain (ADS)**)

User or DN: the user name of the authorized credentials for LDAP server access (disabled when "Anonymous" is selected).

Password: the password of the authorized credentials for LDAP server access (disabled when "Anonymous" is selected).

Domain: the domain used for LDAP server access (only enabled if "User and domain (ADS)" is selected).

In the **Attributes** section, specify the attribute definitions on the LDAP server (the Presence Server uses these attributes to fetch presence information):

Mail address: LDAP database attribute for email (e.g., mail).

Business phone: LDAP database attribute for business phone number(e.g., telephoneNumber).

Mobile phone: LDAP database attribute for mobile phone (e.g., mobileTelephoneNumber).

SIP address: LDAP database attribute for SIP address (e.g., sipAddress).

Private phone: external LDAP database attribute for private phone(e.g., privatePhone).

Account name: external LDAP database attribute for mail(e.g., accountName).

In the Search section, specify the attribute definitions for search in the LDAP server:

<Sip>: LDAP attribute for a SIP address (e.g., mail)

<Tel>: LDAP attribute for a phone number (e.g., telephoneNumber)

- 5. Optionally, specify a valid email address in the **Email** field, and click **Test connection** to verify that the LDAP server is reachable.
- 6. Click Save to save your changes.

Configure Directory Server (MiVoice 5000)

To configure the directory server for MiVoice 5000 with InAttend, perform the following instructions.

- 1. In the **Directory server configuration** page of BluStar WebAdmin, enter the following values for the parameters.
 - a. In the fields under Settings, identify the LDAP server:
 - i. Current suffix: enter dc=mitel dc=com
 - ii. Port: enter the TCP/IP port number
 - iii. Size limit of search: Enter a value for the number of entries (for example, 50000)
 - b. In the fields under Logging:
 - i. Select the Logging is active check box.
 - ii. Enter a size for Logfile size (Kbyte), (for example: 4000)

- iii. Enter the number of log files to store (for example: 100)
- iv. Select the mode.
- c. In the Delete/Write access section
 - i. Enter the username.
 - ii. Enter the password.

BluStar Server Administration	» admin			(DA	L: WIN-IN	ATTEND / DB: WIN-INATTEND)
🕅 Mitel	User Configuration (CTI Server	Directory Server	Presence Server	Tools	Help
Directory server o	configuration			1		1.2
Server						Delete server Save
LDAP Server	IN-INATTEND					
A SCII Import	Settings					
LDAP Import	Current suffix dc=mit	el.dc=com				
SOAP Import	Port 389	_				
Attributes	Size limit of search 50000	entries				
Index						
Import Status	Logging					
	Logging is active					
	Logfile size (KByte) 4	000 (○ Status mode			
	Number of logfiles 1	00 (Debug mode			
	Delete/Write access					
	User	Manager				
	Distinguished name (DN)	cn=Manager	, dc=mitel,dc=com			
	Password	•••••				

- d. In the LDAP Import settings section,
 - i. Check the Delete Old entries and Full database reset check box.
 - ii. Choose Every day option for the Auto Import.
 - iii. Choose No import verification for Import rollback

CHAPTER 7



e. Enter the InAttend login credentials in the User accounts page.

Web Admin home	Users accounts	
Subscribers	Telephony service>Subscribers>Directory>Settings>Users	
Directory	i2070 :	
Users accounts	- login	i2070
System	- password	*****
Dialing plan		
Network and links	TWP :	
Reception	- login	twp
Voice mail and tones	- password	******
Fast links		
	CC :	
	- login	acp
	- password	*******
	MICOLLAB :	
	- login	MiCollab
	- password	
	UC360 :	110700
	- login	00360
	- password	**********
	11550175	
	LIFESIZE :	Liferize
	- login	Lifesize
	- password	
	4340W -	
	- login	A340w
	- togin	
MV5000-R6.4 RC /A501 FRA Site: 002-SITE LOC	- password	
30/05/17 17:55:29 * CSTA SERVER 0: LINK IN FAULT *	INATTEND :	
30/05/17 17:34:55	- login	InAttend
* CSTA SERVER 0: CONNECTED *	- password	*****
30/05/17 16:08:32		✓

i. Use the same credentials in the LDAP Import server settings.

BluStar Server Administration »	admin (DAL: WIN-INATTEND / DB: WIN-INATTEND
🕅 Mitel	User Configuration CTI Server Directory Server Presence Server Tools Help
Directory server of	tings
Server configuration	Import now Activate Save
LDAP Server W	IN-INATTEND LDAP Import settings LDAP Import settin
L DAR Import	
SOAP Import	Default 🗸
Export	Server settings
Attributes	Server 10.148.79.171 Port 5389
Index	New search base Search bases
Import Status	ou=people,ou=local,o=AASTRA,dc=DOMAIN,dc=com
	Alternative import filter object:lass=person E Enabled 'Paged Import' Page Size 500 OLDAP SCOPE ONELEVEL
	Login
	O Anonymous User or users DN cn=InAttend,ou=Users,dc=DOM
	With user information Password
	O User and domain (ADS) Domain
Quicklinks (PBX links) (Dir	ectory Server Configuration Presence Server Configuration Presence Interface Service manager

ii. Map the attributes of the user, example is shown in the following screenshot.

BluStar Server Administrat	tion » admin			(DAL: WIN-INATTEND	/ DB: WIN-INATTEND)
🔀 Miteľ	User Configuration C1	TI Server Director	y Server Presence Ser	ver Tools Help	
Directory serve	er configuration		1	2	2
Server configuration LDAP Server ASCII Import	WIN-INATTEND		LDAP Import settings	Import now	Activate Save
LDAP Import	Corresponding attributes		Custom attributes		
SOAP Import	Enter <xyz> for fixed values</xyz>		Check the attributes your	want to import and insert	the position
Export	displayName	Name	Source attribute	Target attribute	
Attributes	displayGN	First name	Drivate	misc29	1
Index		Street		mise30	
Import Statue		ZIP			
	localisationDesc	City			
	telephoneNumber	Business phone			
		Private phone			
	attr1	Mobile phone			
		Facsimile			
	mail	Mail address			
	recordType	Organization			
	hierarchySV	Department	Add		
		SIP address			

iii. After you set the required attributes, click Import now to display the Import Status.

BluStar Server Administratio	n » admin			(DA	AL: WIN-II	NATTEND / DB: WIN-	INATTEND)
🕅 Mitel	User Configuration	CTI Server	Directory Server	Presence Server	Tools	Help	
Directory server	· configuration			1		2	2
Server configuration							Refresh
LDAP Server	WIN-INATTEND						
A SCII Import	Import/Export				Auto	matically refresh view	
LDAP Import	mporecepore	400				,	
SOAP Import	Data imported:	108		Manual LDAP Import			
Export				Manual ASCII Import			
Attributes				Cancel Import			
Index							
Import Status	Data exported:	0		Cancel export			
	Messages						
	01/06/2017 14:03:50 Manu	al import is activa	ted. (108/108) data reco	rds			

MiCollab and InAttend with MiV5000

CSTA ports configured for MiCollab and InAttend towards MV5000 have to be different,

- 1. Check the CSTA Ports assigned with MiCollab and InAttend, go to **Applications > MiCollab Client Service**.
- 2. Micollab port is set to 3211, retain the same value.

Audio, Web and Video PBX Node Details Conferencing PBX Node Details MiVoice Border Gateway « Settings MiCollab Client Service Bescription: MiCollab Client Deployment IP address / hostname: Licensing Information Extension length: ServiceLink SIB Conference SAC:	
MiVoice Border Gateway PEX Node Details NuPoint Web Console « Settings MiCollab Client Deployment Licensing Information Description: MiCollab Client Deployment Licensing Information IP address / hostname: ServiceLink Sile Conformer EAC:	
NuPoint Web Console « Settings MicColab Client Service Description: MicColab Client Deployment IP address / hostname: Licensing Information Extension length: ServiceLink SIR Conference SAC:	
MCClab Client Service Description: MV5000 MiCollab Client Deployment IP address / hostname: 10.10.203.10 Licensing Information Extension length: 10 ▼ ServiceLink SIR Conference EAC: #40	
MiCollab Client Deployment Licensing Information IP address / hostname: 10.10.203.10 ServiceLink Extension length: 10 ▼ ServiceLink SIP Conference ECC 100	
Licensing Information Extension length: 10.10.200.10 ServiceLink SIR Conference EAC #40.	
ServiceLink Calenson rengun. 10	
SIN Contercordo FOC	
Install Applications Sin Contentione rAC. 40	
Status Dialing prefix:	
Administration Voice mail server:	
Web services Voice mail number:	
Backup View (an files Voice mail public number:	
Event vig mod	
System information	
System monitoring Username: User	
System users Password:	
Shutdown or reconfigure Language: [Default] V	
Virtualization	
Configuration » Plus Dialing Settings Integrated Directory Service	
MiCollab Client Integration Wizard « CSTA Settings	
MiCollab Settings	
Miclosab Language 3211	
Networks Extended checking of the phone device	
E-mail settings Print PDU	
Google Apps Number of Iog files: 10	
DHCP May file size (MB): 2	
Date and Time Size (wD).	
nostnames and addresses Protocol file: pdullace	
DVGFin-TDV4 Tunnel Use phone number block: from to	
SNMP	
Ethernet Cards » CLID Translation	
Review configuration	

3. Enter **3215** in Port for InAttend.

🕅 Mitel	User Configuration CTI Serv	er Directory Server Presence S	Server Tools Help
PBX link config	juration	. 1.	
	RRY link name Mill/ojco5000	PBY link number 1	Save Back to the link list
Properties	Server INATTENDMV5000		
Telephone system	Direct connection		
Telephony	IP - address 10.10.144.21	Activate PDU trace	
Direct connection		Number of log files	10
Server settings	Port 3211	Number of log lifes	
Number alignment	Service ID 1	Max. file size (MB)	3
		Protocol file	c:\pdu.txt

4. Enter **3215** for MiV5000 to be configured with CSTA port.

Mitel Telep	hony service			admin InattendMV5k
Web Admin home Subscribers System Dialing plan Network and links Data links TCP/IP - X25 gateway TCP - X25 addres port transl. TCP - X25 addres port transl.	Top - X25 adds: port transl.: 030 Telephony service-Network and Inico-Data Inico-TCPIP - X25 generation TCP - X25 address port transl. (43.6.1)	Port X25 number Mode Call data (values) - ascii - hexa(00/07) - hexa(08/0F)	3215 9011601 NOT DEFINED •	
		Action		

Configuring Directory Server

This chapter describes the configuration of the Directory Server component of theBluStar Server. **NOTE:** The BluStar Server does not contain its own directory (aside from CSV-filesstored locally for enhancing **higher authority directories** with entries which are e.g.typically not in an AD such as phones on floors, in server rooms, etc.). The BluStar Server reads the content of higher authorities' LDAP server and / or ADand presents the results to the BluStar clients offloading mentioned **source servers**.The import from such **source servers**can be automated and scheduled for times withlow traffic / low load conditions.

You must not install the BluStar Directory Server instance on the same server togetherwith another LDAP Server like MS Active Directory – otherwise you have to specify adifferent port because the LDAP default port 389 may already be in use.

1. LDAP Server Details:

Menu: Directory Server ->Configuration ->LDAP Server

In the navigation section on the left the respective **source server** can be selected and the appropriate configuration for the BluStar Server to access the **source servers** must be provided.

Settings:

Parameter	Explanation
Current suffix	Base DN (default: "dc=mitel, dc=com").Once "Save" is clicked the BluStar Server will ask for confirmation since the (cached) database will be reset and all existing data will be deleted from the cache of the BluStar Server.
Port number	TCP/IP port for the LDAP server of the BluStar Server (default: 389)
Size limit of search	Maximal number of search results returned

Logging:

Parameter	Explanation
Active	Enables / disables logging of the LDAP server component of the BluStar Server
Status Mode	Only status messages should be logged
Debug Mode	Status and debug messages should be logged
Log file size (Kbyte)	Maximum file size used for log files (default: 4000 kB)
Number of log files	Number of log files used (will be overridden / re-used once the maximum is exceeded).

Important:

Logging in Debug Mode should only be activated temporarily to create detailed logs for a specific issue.

Logging in Debug Mode can influence the performance of the LDAP Server and should therefore be deactivated after the logs were created.

Delete/Write Access:

User / DN/Password - Credentials for delete/write access to the Directory Server component of the

Link-Button (available for multi-server installations only, for single server installations mentioned options can be accessed from the navigation bar on the left directly). This button opens more option in the navigator menu to the left for

- ASCII Import (note, there are 2 tabs)
- LDAP Import (note, there are 3 tabs)
- Attributes
- Index
- Import Status

2. ASCII/CSV Import details

Menu: Directory Server ->Configuration ->ASCII Import

ASCII files with delimiters also known as CSV files can be imported to the BluStar Server database for being able to find i.e. extensions which do not exist in higher authorities' databases like AD, i.e. phones on floors, in server rooms, etc. The ASCII / CSV file may contain a first line containing column descriptions for the file but the BluStar Server just refers to the number of the column, thus the first line may have to be ignored when importing the file. (use the configuration option "Row(s) containing no data")

Example for a file structure (1st line to be ignored, is just descriptive): cn;sn;givenName;streetAddress;postalCode;postalAddress;telephoneNumber;homePhone;mobileTeleph oneNumber;mail;facsimile;company;department;sipAddress

Anabelle Duck;Duck;Anabelle;;;;4711;;;anabelle.duck@noreply.com;;;; Berta Duck;Duck;Berta;;;;4712;;;berta.duck@noreply.com;;;; Willi Duck;Duck;Willi;;;;4223;;;willi.duck@noreply.com;;;;

When importing an ASCII / CSV file the BluStar Server ignores blanks between delimiters and it is also agnostic to CR or CF/LF delimiters at the end of each line. Thus, the second example file (below) will lead to the same result when imported as the first example above:

cn; sn; givenName; streetAddress; postalCode; postalAddress; telephoneNumber; homePhone; mobile-TelephoneNumber; mail; facsimile; company; department; sipAddress

Anabelle Duck; Duck; Anabelle; ; ; ; 4711; ; ; anabelle.duck@noreply.com; ; ; ; Berta Duck; Duck; Berta; ; ; ; 4712; ; ; berta.duck@noreply.com; ; ; ;

Willi Duck; Duck; Willi; ; ; ; 4223; ; ; willi.duck@noreply.com; ; ; ;

Menu: Directory Server ->Configuration ->ASCII Import ->ASCII import settings (1st tab)

Parameter	Explanation
Profile is active	Enables / disables the ASCII Auto import
Multi file support	Enables "multi file support" for up to 5 different import files

Parameter	Explanation
File path and name	Enter the file path and file name for the file containing data to be imported.
Limiting character	The character delimiter used for separating the columns
Row(s) containing no data	Enter the number of row(s) at the beginning of the file which shall be skipped during import
Overwrite / Delete old entries, Full database reset	Defines how to handle old entries when importing from a file
Allow duplicate entries	Allow duplicate entries where the first name, last name, company and department are the same.

Auto Import

Configures scheduled import. Specify time of day, the day(s) of the week for automated import.

Import rollback

Parameter	Explanation
No import verification	Disable checking the minimum number of entries imported
Minimum numbers of entries to import	Check the minimum number of entries imported. If the minimum number is not exceeded, the import will be invalid and no change to the database will be committed

Menu: Directory Server ->Configuration ->ASCII Import ->ASCII importattributes(2ndtab):

Parameter	Explanation
Position in the life	Allows strong the imported data into favored fields, the position of the corresponding column within a row has to be mapped to the LDAP attributes.
Custom attributes	Assign imported columns to custom LDAP attributes. Enter the position in the file and mark the checkbox of the custom LDAP attribute.

3. LDAP Import details

Menu: Directory Server ->Configuration ->LDAP Import

LDAP sources can be i.e. OpenLDAP servers, the LDAP server of MiVoice Office 400 or others.

Menu: Directory Server ->Configuration ->LDAP Import ->LDAP import settings (1st tab)

The Activate button activates the LDAP Auto import feature.

LDAP Import Settings

Parameter	Explanation
Profile is active	Shows the status of the Auto Import
Overwrite entries, Delete old entries and Full database reset:	Define how to handle old entries when importing from LDAP sources
Allow duplicate entries	Allow duplicate entries where the first name, last name, company and department are the same.

Auto Import

Configures scheduled import. Specify time of day, the day(s) of the week for automated import. It is also possible to import the ASCII import at the same time.

Import rollback

Parameter	Explanation
No import verification	Do not check the minimum number of entries imported
Minimum numbers of entries to import	Check the minimum number of entries imported. If the minimum number is not exceeded, the import will be invalid and no change to the database will be committed

Menu: Directory Server ->Configuration ->LDAP Import ->LDAP import server settings (2nd tab) Server Settings

Parameter	Explanation
Server	Name or IP address of the LDAP server the data shall be imported from.
Port	TCP port for doing LDAP connection.
Search bases	Position in the directory structure where LDAP bind is done.
Alternative import filter	LDAP import filter
Enable 'Paged import'	Activate for executing a paged import (e.g. used for Active Directory imports, LDAP v3 is needed on the LDAP Server).
LDAP scope	Subtree or Onelevel

Login

Parameter	Explanation
Select the type of the LDAP login	Anonymous, With user information, User and domain (ADS).
Username	LDAP DN with access rights
Password	Password required for access the remote LDAP source
Domain	Enter an ADS domain.

Menu: Directory Server > Configuration > LDAP Import > LDAP Import Attributes (3rd tab)

Parameter	Explanation
Corresponding attributes	For importing data from another LDAP data base, the attributes of the remote LDAP servers have to be assigned to the attributes of the Mitel LDAP server. Using " <xyz>" fixed values can be used.</xyz>
Custom attributes	Maps custom LDAP attributes for the import.Example: Source attribute: businessCategory, target attribute: monitorGroup where monitorGroup is a custom attribute.

Export options details:

Menu: Directory Server->Configuration ->Export

As the BluStar Server collects directory information from various sources it may be desirable to let the BluStar Server dump its cached directory information gathered from mentioned sources; this is the purpose of the Export function.

Export Settings

Parameter	Explanation
Profile is active	Enables /disables the export
File path and name	Enter the file name and file path to export the data to
Create header in export file	Enable first line in the file to contain the column names
Export all entries	Export all entries from the LDAP server (complete export)
Export only entries of the following organization	Limit the export to a specific organization. Example: Mitel Deutschland GmbH.

Auto Export

Configures scheduled export. Specify time of day, the day(s) of the week for automated export.

Custom Attributes

Parameter	Explanation
Target attribute	Enables custom attributes from the LDAP server to be exported

5. Attributes

Menu: Directory Server->Configuration ->Attributes

Specifies custom LDAP attributes for the import/export.

Example: monitorGroup is a custom LDAP attribute which is a target attribute for LDAP import to which a source LDAP attribute businessCategory is mapped.

6. Index:

Menu: Directory Server->Configuration ->Index

More LDAP attributes to be indexed in order to accelerate the search within the LDAP server must be specified here. Changing this option is not recommended for administrators inexperienced with BluStar Server performance tuning.

7. Import Status:

Menu: Directory Server->Configuration ->Import Status

Manual import of ASCII files or LDAP data to the LDAP component of the BluStar Server and manual exporting data to an ASCII file. The current configuration of LDAP or ASCII (see above) is used.

A message window will show the status of the current automatic / manual import / export.

To update the messages displayed press the "refresh button" of the web browser to reload the page or enable the automatic refresh view option.
Configuring MiCollab presence with InAttend

InAttend is integrated with MiCollab based on email subscription. The InAttend client uses MiCollab as a source of reference to the presence. MiCollab provides both IM presence and telephony presence for the InAttend Client.

Micollab presence with InAttend in CMG

In this deployment, InAttend consolidates presence using CMG Directory Manager and MiCollab. Therefore, you must ensure that the email ID of the user that you create in CMG Directory Manager is same as the email ID mentioned in the MiCollab Client.

Figure 1 and Figure 2 respectively show examples of the user details as in MiCollab Client and in CMG Directory Manager.



Figure 9.1: User details as in MiCollab Client

		Shetty Vibh	an (4001)			÷
Main Form Phonetic Org	anization Keywords	Recurr.Act. Settings				
				Save	Reset	<< >>
Message systems	Secret	Address				^
E-Mail V		vibnan.snetty@inattendbgi	.com			
None 🗸						
None 🗸						
None 🗸]
CMG Web	v					
CMG Speech Office						
Message waiting	\checkmark					
Workgroup administrator						
Name directory	v					
Organization directory	V					
Enable name search	v					
Enable CMG Web search	✓					
Delete password in CMG Office Web	, ×					
Calendar synchronization	_					
enabled						
blocked						~
I						

Details entered in CMG Directory Manager.

Micollab presence with InAttend in Standalone

In this deployment, InAttend consolidates presence using Active Directory Manager and MiCollab. Therefore, ensure that the email ID of a user mentioned in MiCollab Client is same as the email ID mentioned in the Active Directory.

Figure 1 and Figure 2 respectively show examples of the user details as in MiCollab Client and in Active Directory.



Figure 9.2: User details as in MiCollab Client

CHAPTER 9

Account	Account						
Organization	First name:	Vibhan				Account expires:	Never
Member Of	Middle initials:						O End of
Password Settings	Last name:	Shetty					
Profile	Full name: *	Vibhan Shetty	0	for the state of t		Password options: O User must change pass	word at next log on
Policy	User UPN logon: User SamAccountName Io	inattendbgl	0	vibhan.shetty	•	Other password option Smart card is required	is ed for interactive log on
Silo	Protect from accidental	deletion				Password never expi	ires
Extensions						User cannot chan	ge password
						Encryption options:	
						Other options:	
	Log on hours	Log on to					
	Organization						
	Display name:	Vibhan Shetty				Job title:	Senior developer
	Office:		_			Department:	Enterprise
	E-mail:	vibhan.shetty@inattendbgl.com				Company:	Mitel India
	Web page:		_			Manager:	

User details as in the active directory

Modifying Webadmin Configurations in InAttend for Standalone

1. Log-in to the WebAdmin.

BluStar Server Administration »	admin			(DAL: IN	ATTENDI	/IV5000 / DB: INA	TTENDMV5000)
🕅 Miteľ	User Configuration	CTI Server	Directory Server	Presence Server	Tools	Help	
Welcome admin				6	1	•	
Quicklinks							
PBX links Directory Server Configuration							
Presence Server Configuration							
Presence Interface							
Service manager							

2. Select User Configurations > Configuration profiles, select the InAttend Search Profiles.

BluStar Server Administration	» admin	(DAL: INATTEND	MV5000 / DB: INATTENDMV5000)
🕅 Miteľ	User Configuration CTI Server D	Directory Server Presence Server Tools	Help
Configuration pro	files	40	• 4
Profile name Pr	ny	• Search	Add configuration profile
Profile type Pr Attendant Directories InA Attendant Layout InA Attendant Messages InA Attendant PBX InA Attendant Search InA Attendant Search InA	ofile name Attend LDAP Attend Attend Attend Attend Attend	Description LDAP Attendant Directories Default Attendant Layout pr Default Attendant Messages Default Attendant PBX profi Default Attendant Search pr Default Server profile (wit	Assignments Copy Delete Image: Copy Copy Copy Copy Copy Copy Copy Copy

3. Select Attendant Search(Profile type) or InAttend(Profile name).

BluStar Server Administration	» admin		(DAL: INATTENDMV5000 / DB:	INATTENDMV5000)
🕅 Miteľ	User Configuration CTI Se	erver Directory Server	Presence Server Tools Help	
Attendant Search				
edit profile: InAttend				
Properties			(Save Back
Settings				
Result layouts	Profile name InAttend			
Search	Default Attendant S	Search profile.		
Details view			li li	
	Automatic search		Search cache	
	Search delay (in milliseconds)	500 🔻	Number of entries off •	
	Minimum number of characters	3 🔻	Timeout (in seconds) 60 •	
	Team search		Extended search fields	
	Team search 1 Team search	2 Team search 3	Search attribute Result layout	
	T	•	Field 1 Department Default	•
	Company, Departm Room	TelNo	Field 2 Company	•
	Result layout Default	*	Field 3 Information	•
			Field 4 Email Default	•
			Field 5 Keyword	*

4. Go to, Attendant PBX > Settings > Linestate, select the Use MiCollab for presence check box and configure the other parameters as shown in the below screen-shot.

Attendant PBX edit profile: InAttend Properties Save Back Interface Settings SMS messages from BSW Queues Call control Show queue list Use numpad only for dialing Show SMS text Show queue counters A/B fields Linestate **Context menu functions** Acquire focus for incoming call Email attribute Email . Send mail SIP address attribute SIPAddress Show company ۳ Set forward Show hidden numbers Show presence status as linestate Set information Automatic flash for details view Support overlapping numbers Transfer to voicemail Flash on B-field when available Use MiCollab for presence Change view based on domain Minimum number length 3 BLF Allow BLF dragging

Settings for Micollab with InAttend

The configuration steps in this section is applicable for integration of Micollab with InAttend for both CMG and standalone.

Activate Presence from MiCollab in InAttend

 Log-in to the Webadmin and select User Configuration > Configuration Profiles > Attendant PBX InAttend/InAttend CMG > Setting

perties			Save Back
Interface	Settings		
Settings	Queues	Call control	SMS messages from BSW
	Show queue list	Use numpad only for dialing	Show SMS text
	A/B fields	Linestate	Context menu functions
	□ Acquire focus for incoming call ☑ Show company ☑ Show hidden numbers ☑ Automatic flash for details view □ Flash on B-field when available ☑ Change view based on domain Minimum number length 3	Email attribute FirstMessageSystemId SIP address attribute FirstMessageSystemId SIP address attribute FirstMessageSystemId SIP overlapping numbers Use MiCollab for presence	Send mail Set forward Set information Transfer to voicemail

• Select 'Use MiCollab for presence'

From InAttend 2.6 SP1 onwards the support for MiCollab will be with MiCollab 9.1.

The InAttend server **IP/FQNDN (Fully Qualified Domain Name)** should be configured as a trusted presence source. This will be done by adding the InAttend server **IP/FQDN** in the **MiCollab Client Service Configuration**.

Applications Users and Services	MiCollal	o Client Ser	vice Confi	guratio	n			,	?)		
Audio, Web and Video	Enterprise	Synchronization	PBX Nodes	Accounts	Corporate Directory	ACD Settings	Collaboration	Features Peering Federation			
MiVoice Border Gateway	This page cor	tains enterprise-wide	e configuration se	ttings, includi	ng the ability to creat	e and delete enter	prises.				
NuPoint Web Console											
MiCollab Client Service MiCollab Client Deployment	Settings										
Licensing Information	oottingo								÷.,		
ServiceLink	< Settings										
Install Applications	Enterprise II	k:	mimv5k	Read Consider	an anima Els in etter						
Administration	Entermine d		micolab C	Hendhal mite	on minvok inatten						
Web services	Vaiss mail a			vox.inatenoogl.mrei.com							
Restore	Voice mail o	siver type.	NuPoint	Embedder	d U EMEM						
View log files	Administrato	ra mai	minvok.m	attenubyi.inite	A.COM						
System information	Switch type:		Million 5000								
System monitoring	Collaboratio	n server type:	MiCollab Aud	io, Web and Vide	eo Conferencing						
System users Shutdown or reboot	Avatar URL:		http://mimv5k	inattendbgl.mite	al.com/ucs/avatar/dn/min	tv5k/					
Virtualization	Language:		English (U	S)		Ŧ					
Configuration	Time zone:		ASIA/KOL	KATA			٣				
MiCollab Client Integration Wizard	» Calendar	Integration									
MiCollab Settings MiCollab Language											
Vidyo Settings Networks	« Trusted S	ervers				(Add S	erver) (Delete Sen	<u>ret]</u>			
E-mail settings Geogle Apos	Descr	iption	Server			Тур	be .				
DHCP	MIV50	00	10.211.63.8	15		Pre	sence. IM				
Date and Time Hostnames and addresses	In Atte	nd	inattendmy	5000 inattendbol	Loom	Pre	sence				
Domains ID-d-in-ID-d-Turnel		nd-Ganesh	10 211 50 4	12		Pre	sence				
SNMP		ad Mt/5000	10 211 63 3	-		Dre					
Ethernet Cards Review configuration			10.211.00.7	•		ric.					
Applications Users and Services	Trusted	Server Det	ails						?		
Audio, Web and Video Conferencing	Add New True	teri Server							-		
MiVoice Border Gateway	Add Hell Hus								-		
MiCollab Client Service	Description				1						
MiCollab Client Deployment	Description.										
Coensing Information	Hostname:										
Install Applications			The fields below id	entify the suppor	ted types of Trusted Ser	vers. You must select	at least one type fro	m the list.			
Status			Presence - Int IM Tousted In	isted Presence V	rvatcher Entity						
Administration Web services			IN - HUSLOU II	istaint message v	Senang Chery						
Backup											
Restore	Create	Cancel									
Event viewer	Create										
System information											
System monitoring											
system users Shutdown or reboot											
Virtualization											

Modifying CMG Web Service Configurations

NOTE: Administrator must stop the Mitel CMG Web Service before making any changes to the file "Mitel-BluStarWebServiceConfig.xml".

The CMG Web Service configuration file is available in the install directory C:\Program Files (x86)\Mitel(Aastra)\BluStarWebService.

Administrator must change **UseMiCollab** value to "true". By default, it will be "false". All other parameters in the file will remain same as default, save and close the file and start the BSW service.

xml version="1.0" encoding="utf-8"?
<pre>B<sbustarwebserviceconfig xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"></sbustarwebserviceconfig></pre>
Database connection string example: server*localhost;database*nice;User ID*nice;Password*Tomat2007
<cmgdatabaseconnectionstring>server=10.10.144.193;database=nice;User ID=nice;Password=Tomat2007</cmgdatabaseconnectionstring>
<cmguserinformationserviceurl>http://10.10.144.193/CMGUserInformationService/CMGUserService.asmx</cmguserinformationserviceurl>
<cmgactivityserviceurl>http://10.10.144.193/CMGActivityService/CMGActivityService.asmx</cmgactivityserviceurl>
<anaserviceurl>http://10.10.144.193/nwAna/AnAService.asmx</anaserviceurl>
<anausername>BluStarWeb</anausername>
<anapassword>AastraBSW80</anapassword>
<validateservicecalls>true</validateservicecalls>
<listenport>8002</listenport>
<sipport>5060</sipport>
<loglevel>3</loglevel>
<bypasslicensecheck>true</bypasslicensecheck>
<logpath></logpath>
<daystokeeplogs>10</daystokeeplogs>
<maxlogsizemb>100</maxlogsizemb>
<presenceserverconnectionudp>false</presenceserverconnectionudp>
<duplicates>1</duplicates>
<pre><phonecontextisuserparameter>false</phonecontextisuserparameter></pre> /PhoneContextIsUserParameter>
<pre><usemicollab>true</usemicollab></pre>

Adding MiCollab Configuration File

NOTE: Administrator must stop the Mitel CMG Web Service to make any changes to the file "MiCollab-Config.xml".

Administrator must manually create a new file "MiCollabConfig.xml" in the path

<Drive C/Drive D :\Program Files (x86)\Mitel\BluStarWebService>

You can copy and paste the following content to the file you create and edit the required parameters.

```
<?xml version="1.0" encoding="utf-8" ?>
```

<MiCollabConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">

<MiCollabMasterUser>4001</MiCollabMasterUser>

<MiCollabDomain>mimv5k.inattendbgl.mitel.com</MiCollabDomain>

<MiCollabPort>8008</MiCollabPort>

<UserLimit>4</UserLimit>

<UseCache>true</UseCache>

<NotifyTime>0</NotifyTime>

<SpikeBuster>false</SpikeBuster>

</MiCollabConfig>

- 1. MiCollabMasterUser: This is the username used by the CMG Web service to communicate with MiCollab.
- MiCollabDomain: This defines the MiCollab enterprise domain where MiCollab is deployed. MiCollabDomain must have the same string as in the MiCollab Client Server Manager > MiCollab Enterprise > Enterprise domain field. Select the FQDN(Fully Qualified Domain Name) string, which is resolvable on the CMG Web Services.

NOTE: Only the FQDN is allowed, the IP address does not work.

- MiCollabPort: This defines the port used by CMG Web service to communicate with MiCollab. The default port used by CMG Web Service is 8006.
- 4. UserLimit: This defines the maximum number of users that are sent as part of subscribe request to MiCollab.
- 5. UseCache This specifies the options, whether to use the cache for storing presence information or not. The default and recommended value is "true".

- 6. NotifyTime This specifies the timer wait time, that is the time that the service will wait before another subscribe is sent. The default value is 500 ms, you can configure the time based on your requirement.
- 7. SpikeBuster This ensures optimal usage of the CPU resource, this parameter must be enabled only during the high-performance conditions.

After the required parameters are entered, you must start the CMG Web Service,

NOTE: Administrator can use any authentic MiCollab user credential as the master user name. The user name is case sensitive.

NOTE: The supported upgrade version for InAttend 2.6 SP1 is MiCollab 9.1.

Configuring InAttend profiles and users

You use the BluStar Server Administration tool to modify configuration profiles that control InAttend client functionality and to add users to the InAttend system.

Configuration profiles control different aspects of InAttend client functionality. Profile groups contain one or more configuration profiles. InAttend users are assigned to profile groups, and inherit the configuration profiles contained in that group.

Working with configuration profiles

Configuration profiles control important settings for the InAttend client that cannot be configured by the attendants themselves. The configuration profiles are assigned to users through profile groups.

The system provides the pre-defined configuration profiles for InAttend.

Viewing InAttend configuration profiles

- 1. Access the BluStar Server Administration web interface by typing the URL: http://<hostname>/webadmin in a supported web browser, where <hostname> is the InAttend server address.
- 2. Log in with the administrator credentials

(default username: admin, default password: Mitel123).

3. Select User Configuration and then Configuration profiles.



The system displays the Configuration profiles page and lists all predefined profiles.

Configuration	profiles				
				Add c	onfiguration prof
Profile name	Profile type				
	any	✓ begins with ✓ Search			
Number of found profiles	s 7				
Profile type	Profile name	Description	Assignmen	ts Copy	Delete
Attendant Directories	InAttend CMG	LDAP Attendant Directories	۱		•
Attendant Layout	InAttend CMG	Default Attendant Layout pr			•
Attendant Messages	InAttend CMG	CMG Attendant Messages prof			•
Attendant PBX	InAttend CMG	CMG Attendant PBX profile v		- L	•
Attendant Search	InAttend CMG	CMG Attendant Search profile.	١		•
Attendant Special settings	InAttend		<u></u>		•••
Server	InAttend	Default Server profile (wit			8

Modifying the Attendant Directories Profile

The Attendant Directories profile defines LDAP search data sources for the InAttend client. To modify the Attendant Directories profile, do the following:

- 1. On the Configuration profiles page, click on Attendant Directories in the list of profiles.
- 2. On the Edit profile page, click the name of the data source.

Attendant Dire	ectories nd CMG	2	4	9		8
Properties						Save Back
Datasources	Datasources					
New LDAP Datasource	Profile name	InAttend CMG				
New CMG Datasource	Description	LDAP Attendant Directories pr	rofile.	~		
Set caption	Description			\sim		
	Name	Туре	Server			
	Mitel	CMG	InAttend22		3	

The system displays the Data source page for the profile.

- 3. If you want to define a new LDP data source:
 - a. Click on New LDAP Datasource in the left panel.
 - b. On the LDAP Datasource page, enter values for the following parameters:
 - Name: the name of the LDAP Datasource
 - Server: the hostname or IP address of the LDAP server
 - Backup server: the hostname or IP address of the backup LDAP server(if present)
 - Port: the port for connections to the LDAP server
 - Search base: the base DN

(i.e., the location in the directory from which LDAP searches begin)

- Additional filter: the criteria through which search requests are filtered (by default), all entries from the LDAP Datasource are used for queries
- LDAP version: version of LDAP used (v2 or v3)
- · LDAP login settings: select the method of authentication on the LDAP server
- Anonymous: no user credentials required
- User information: authorized user name and password required
- User and Domain (ADS): authorized user name and password, and domain required
- c. Click Save to save your changes.
- 4. If you want to define a new CMG data source (for CMG installations):
 - a. Click on or New CMG Datasource.
 - b. On the CMG Datasource page, enter values for the following parameters:
 - Name: the name of the CMG Datasource.
 - Server: the hostname or IP address of the CMG server
 - Backup server: the hostname or IP address of the backup CMG server (if present)
 - · Server side sorting: enable to have the search results sorted by CMG

(if available)

CMG Server login data: select the method of authentication on the CMG server
 Attendant user credentials: use the InAttend client user credentials
 Username: the user account authorized to access the CMG server
 Password: the password for authorized to access the CMG server

Attendant Dire	ctories		Z		8
edit profile: InAtten	nd CMG	1000			6 M
Properties					Save Back
Datasources	CMG				
New LDAP Datasource	Name	Mitel			
New CMG Datasource	Server	InAttend22			
Set caption	Backup server				
	Port	5199			
		Server side sorting			
	CMG server log	in data			
	Attendant u	user credentials			
	OUsername				
	Password	•••••			

- c. Click Save to save your changes.
- 5. If you want to change the default field names displayed in the InAttend client:
 - a. Click on Set caption.

Attendant Direc	ctories d CMG	2	4	n		
Properties						Save Back
Datasources	Datasources					
New LDAP Datasource	Profile name	InAttend CMG				
New CMG Datasource Set caption	Description	LDAP Attendant Directories pr	rofile.	$\langle \rangle$		
	Name	Туре	Server			
	Mitel	CMG	InAttend22		•	

b. On the Caption page, specify the field name you want displayed in InAttend to replace the default field name. For example, if you want the default field of "Company" to be displayed as "Division", type "Division" in the "Company=" entry.

Caption	
AbsenceReason=	
AccessControlFlag=	
ActivationDate=	
CardKev=	
Child=	
Company=Division	
Cordless=	
CustomerGroup=	
DeactivationDate=	
Department=	
DepartmentAlt=	
Departmenteriu=	
Empil-	
Employee=	
Eacsimile=	
FirstMessageSystem=	
FirstMessadeSvstemId=	
FirstMessageSystemType=	
FirstName=	
Flags=	
Flags2=	
[<u>110432</u> -	

- c. For CMG installations, click Use CMG descriptions to use the default captions defined by CMG>
- d. Click Save to save your changes.
- 6. Click **Back** to return to the main Configuration profiles page.

Change Directory View Automatically

InAttend can be configured to "automatically change view" based on the incoming call. The feature can be enabled in WebAdmin, PBX-Profile, Settings section, where Change view based on domain can be checked. Please note that this feature is only available for CMG, not when InAttend is used with LDAP only.

For the configuration to work, each ACS domain configured in TCA has to have a CMG View name and PBX Id specified. The attendant user has to also have permissions to access this view, which can be configured in CMG Configuration Manager.

InAttend will automatically change the view when a call is answered. This will ensure that directory search is performed in a specific view. It is still possible to change the status manually to another view to make searches for other users.

The table describes how InAttend automatically can change view for incoming calls.

Call SCENARIO	VIEW SELECTION
User call attendant queue	Use domain for queue to select view
User A call user B, where B is forwarded to attendant	Use domain for B's extension to select view

When making outgoing calls, InAttend will ensure that the correct ACS domain is used. The table below describes this process.

Call SCENARIO	DOMAIN SELECTION
Call directory entry from the search result list	Use PBX Id of directory entry to select domain

Call a number not available in the directory from the search result list	Use current view to select domain 1
Call using dial dialog, unique number defined in ACS	Use number defined in ACS to select domain
Call using dial dialog, overlapping number defined in ACS	Use current view to select domain 1
Call using dial dialog, number not defined in ACS	Use current view to select domain 1

If no unique domain can be found based on the current view, the PBX Id of the attendant is used to select domain.

Overlapping numbers

Overlapping numbers are supported if they are defined in different ACS domains and different PBX Ids used in CMG.

To support presence and line state with overlapping numbers, the setting "Support overlapping numbers" must be enabled in WebAdmin, PBX-Profile, and Settings section. For presence and line state subscriptions, the domain Id (derived from the PBX Id) of the user or extension is used for presence requests. The domain Id must match the PBX link number configured for the CTI Server in WebAdmin.

ACS domains must be configured with one domain per PBX for one to one mapping between ACS domains and CMG PBX Ids. An ACS domain is only configured with one CMG PBX Id.

NOTE: To have the complete functionality of overlapping numbers, you must enable the Change view based on domain in WebAdmin.

Modifying the Attendant Layout profile

The Attendant Layout defines the functions available in the InAttend client and the layout of the interface.

To modify the Attendant Layout profile, do the following:

- 1. On the Configuration profiles page, click on Attendant Layout in the list of profiles.
- 2. On the Edit profile page, you can select the following layout options:
 - a. Layout list: select a layout with or without the Busy Lamp Field section.
 - **b. Panel list**: select the functions that appear in the panel on the right side of the InAttend client (e.g., chat, send a message)
 - c. Settings: enable or disable "Blind support" (for visually impaired attendants); when enabled, line state and presence state icons change to text.

Attendant edit profile: In	Layout hAttend CMG	2.2	2 4
Profile name InAt Description Defa	tend CMG ault Attendant Layout profile.	0	Save Back
Layout list	Panel list	Settings	
QUE A an O SEARCI	UES I AB	Blind support Microsoft Lync presence color sche	me
QUE A an SEARCI BL	UES ☐ Chat d B ☐ Information H / PAM ☑ Journal F ☑ Messages ☑ PAM ☑ Queues ☑ Search		

- 3. Click Save to save your changes.
- 4. Click Back to return to the main Configuration profiles page

Modifying the Attendant Messages profile

InAttend supports different modes for sending messages from the attendant: email (via SMTP), CMG messaging (for CMG installations), email via local email client ("mailTo") or via XML push to phones.

The Attendant Messages profile defines the message template and the channel used when an attendant sends an email message from the InAttend client.

To modify the Attendant Layout profile, do the following:

 On the Configuration profiles page, click Attendant Messages in the list of profiles. On the Edit profile page, you can create one or more customized message templates for messages sent from an attendant (the attendant selects a template when sending a message).

Attendant Messa	ges			
edit profile: InAttend C	MG	A.		
Profile name InAttend (CMG		Description CMG Attendant Messages pro	Save Back
Subject/Template		<u> </u>	Subject Message from attendant at %time Message from %caller Message from %attendantuser	
Channel list				
Channel name		>>	Channel name Type Recipient address field CMG CMG Email	0
Recipient address field SMTP	Email	~		
Server name				
Sender email address				
Password (optional)	•••••			
OCMG				
O Local email client (mailTo:)				
O XML Push	INATTEND22	~		

- In the Subject/Template field, enter the text you want to appear in the subject line of new messages. Click the blue arrow to add the template to the list.
 - **a.** Valid placeholders are:
 - i. Message from attendant at %time (current time).
 - ii. Message from %caller (current caller).
 - iii. Message from %attendantuser (attendant signature).
 - b. Create additional templates as required.

You can reorder them in the list by selecting the up/down arrows.

- 3. In the Channel list section, you can configure one or more channels for sending messages (the attendant selects the channel when sending a message). For each channel, enter values for the following parameters:
 - a. Channel name: identify of the channel (displayed in the InAttend Message panel).
 - b. Recipient address field: the attribute that contains the mail address.
 - c. SMTP: select this channel to send messages via SMTP.
 - i. Server name: name of the SMTP server.
 - ii. Sender email address: email address.
 - iii. Password (optional): password for the email address if required.
 - d. CMG: select this channel to use integrated CMG messaging.
 - e. Local email client (mailTo): select this channel to use a local e-mail client.
 - f. **XML Push**: select this channel to send text messages to phones (for use with Cisco Call Manager).
- 4. Click **Save** to save your changes.

5. Click **Back** to return to the main Configuration profiles page.

Modifying the Attendant PBX profile

The Attendant PBX profile defines PBX-specific settings for InAttend, such as external line prefix and maximum extension length.

To modify the Attendant PBX profile, do the following:

- 1. On the Configuration profiles page, click on Attendant PBX in the list of profiles.
- 2. On the Edit profile page, you can enter values for the following parameters:
 - a. External line prefix: A code to access an external line
 - b. Maximum device length: Maximum length of extensions on the PBX
 - c. Company prefix: A prefix specific to the organization
 - d. Number format: Select a number format from the pull-down list.

Attendant PB>	(nd CMG	2	A -	8
Properties				Save Back
Interface	Profile name	InAttend CMG		
Settings	Description	CMG Attendant PBX profile via ACS.	\sim	
	External line prefix Maximum device ler Company prefix Number format	0 ngth 6 E.164		
	Connectivity Ser Display domain Webservice AnA Server	ver (ACS) n name NATTEND22 NATTEND22		

- 3. In the Connectivity Server (ACS) section, enter values for the following parameters:
 - a. **Display domain name**: Enable to additional domain information provided by the ACS server in the A/B panel.
 - b. Ana Server: The hostname or IP address of the server hosting the Authentication and Authorization (AnA) web service. If the configuration is being made to support HTTPS then https:// should be added, for example http://GTSCMGAND10.

c. TCS server: The hostname or IP address of the server hosting the Telephony Connection Service (TCS) web service. If the configuration is being made to support HTTPS then https:// should be added, for example http://GTSCMGAND10.

🕅 Mitel	User Configuratio	n CTI Server	Directory Server	Presence Server	Tools	Help	
Attendant PBX			1	. 1			
edit profile: InAttend	СМG	6		100		4	
Properties						S	ave Back
Interface	Profile name	InAttend CMG					
Settings	Description	CMG Attendant	PBX profile via ACS		$\langle \rangle$		
	External line prefix Maximum device length Company prefix Number format	5 Classic	v				
	NOW Display domain na Webservice AnA Server https TCS Server https	me ://GTSCMGAND ://GTSCMGAND	010				

- 4. If you want to change additional settings related to how the InAttend client interacts with the PBX, click on **Settings** in the left panel.
- 5. On the Settings page, select the options you want to make available to InAttend clients:

🕅 Miteľ	User Configuratio	n CTI Server	Directory Server	Presence Server	Tools	Help	
Attendant PBX							
edit profile: InAttend	CMG	CO.		T.A.			1
Properties						Sav	e Back
Interface	Profile name	InAttend CMG					
Settings	Description	CMG Attendant PE	3X profile via ACS.		$\hat{}$		
	External line prefix						
	Maximum device length	5					
	Company prefix						
	Number format	Classic	V				
	NOW						
	Display domain na	me					
	Webservice						
	AnA Server https	://GTSCMGAND10	<u>)</u>				
	TCS Server https	://GTSCMGAND10					

a. In the Queues section:

Show queue list: Enable to display all calls in the queue list.

Show queue counters: Enable to display the number of calls in the queue.

b. In the A/B fields section:

Acquire focus for incoming call: Enable to bring the InAttend application to the foreground when a call comes in.

Show Company: Enable to show the company of the incoming caller.

Show hidden numbers: Enable to display the hidden numbers of the incoming call.

Automatic flash for details view: Enable or disable automatic flash of caller's details (if available in the directory) on an incoming call or a callback call.

Flash on B-field when available: Enable or disable flash on B-field when the caller details are available.

Change view based on domain: Enable or disable to change the view based on domain. For more details on change view behaviour, see section 9.1.3 CHANGE DIRECTORY VIEW AUTOMATICALLY.

Minimum number length: the minimum length of a number for a directory lookup by the A/B Panel. c. In the **Call control** section:

Use numpad only for dialling: Enable to allow dialling from the number pad only.

d. In the Context menu functions section, select the functions available for a given contact in the Search panel (when right-clicking on a contact):

Send mail

Set forward

Set information

Transfer to voicemail

e. In the Linestate section:

Email attribute: The attribute used for Presence subscriptions (select from the drop-down list).

SIP address attribute: The attribute used for Presence subscriptions if the Email attribute is empty.

Show presence status as linestate: This attribute when enabled shows the linestate status same as the presence status.

Support overlapping numbers: Enable to support overlapping numbers.

f. In the SMS messages from BSW section:

Show SMS text: Enable to show the sms text; that is, configured in the Messages tab of InAttend client.

g. In the Journal section:

Lock-Show only my calls- Enable the check box for the InAttend client to display only the operators own calls.

NOTE: If this parameter is enabled, then the Show only my calls check box is selected and disabled.

h. In the IM section: Select the Use SFB Chat check box to enable the IM functionality.



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

Modifying the Attendant Search profile

The Attendant Search profile defines search behaviour for the InAttend client and the layout for search results.

To modify the Attendant Search profile, do the following:

- 1. On the Configuration profiles page, click on Attendant Search in the list of profiles.
- 2. Settings page: select the search options you want to make available to InAttend clients:

Attendant Sea	nrch	
edit profile: InAtte	nd CMG	
Properties		Save Back
Settings Result layouts	Profile name InAttend CMG	
Search	Description CMG Attendant Search profile.	0
	Automatic search Search delay (in milliseconds) 250 V Minimum number of characters 3 V	Search cache Number of entries off v Timeout (in seconds) 60 v
	Team search Team search 2 Team search 3 Team search 1 Team search 2 Team search 3 OrgName Room TeiNo Result layout Default TeiNo	Extended search fields Search attribute Field 1 Department V Field 2 Company V Default V Field 3 Information V Default V Field 4 V Default V Field 5

a. In the Automatic search section, enter values for the following parameters:

Search delay (in milliseconds): the amount of time before automatic progressive search begins.

Minimum number of characters: the minimum number of characters required to trigger an automatic progressive search.

b. In the Team search section, enter values for the following parameters:

- Team search 1
- **c.** In the **Search cache** section, set parameters InAttend's integrated search cache. If a search result is found in the cache, no directory lookup is initiated:

Number of entries: the size of the search cache.

Timeout (in seconds): length of time before entries are removed from the search cache.

d. In the **Extended search** fields section, define up to five additional search fields for attendant search queries (in addition to the default criteria of name and number). These extended search fields appear beside the **Search box** in the InAttend client.

For each field, select a search attribute from the drop-down list.

Select a layout for the results from the drop-down list.

- **NOTE:** In the Search Result list in InAttend, keywords can be displayed in two different ways depending on which of these fields have been selected:
- **Keyword**: Only display the keyword for the directory entry that matched the keyword search criteria
- Keywords: Display all keywords for the directory entry.

NOTE: If the **Information field** is configured for the **Extended search fields** in the InAttend Client, then the search is restricted up to 245 characters.

- 3. If you want to modify the default layouts for Search Results, click on Result layouts.
 - a. Select one of the layout templates (Default, Telno, or LastName) to view the layout details.

Attendant Se edit profile: InAtt	arch end CMG	LAS M
Properties Settings	Result layouts	Save Back
Search Details view	Result layout Default LastName TelNo	La Result layout La Layout name Default New Layout Columns
		Search attribute

b. You can make the following changes to the layout:

To add a search attribute to the layout, select it from the drop-down list in the **Search attribute** field and click the arrow button to the right of the field.

To re-order the columns in the results, click on the arrows to move the search attribute up or down in the list (the top of the list corresponds to the first column in the search results).

Click Save Layout to save your changes.

Attendant Ser	arch end CMG	2 20 - 1
Properties Settings	Result layouts	Save Back
Result layouts Search Details view	Result layout Default LastName TelNo	Result layout Layout name Default New Layout Save Layout Columns
		Search attribute

- 4. If you want to modify the search mode, click on Search.
 - a. Enable **Reset search when call has ended** to clear search results when the attendant finishes a call.
 - **b.** Enable **Phonetic search** to include similar-sounding results in the search (e.g., searching for "Muller" will also find "Müller"). There is a XML file containing the phonetic search rules for each language.
 - c. n the Search mode section, select the preferred search mode from the list.

Attendant Se	arch end CMG
Properties	Save Bock
Settings	Search
Result layouts	Reset search when call has ended
Search	Phonetic search
	Search mode
	Automatic search attributes AbsenceReason Image: Company
	Additional search options + AbsenceReason >> +Company S

d. In the Automatic search attributes section, you can specify attributes used for an automatic search (only available for LDAP directories); the search uses the logical OR operator if there are multiple attributes:

Select an attribute from the drop-down menu and click the arrow key to add the attribute to the list.

e. In the Additional search options section, you can specify additional attributes for search (only for LDAP directories). For example, a search for "test +Mitel" will filter on users with company containing "Mitel".

Select an attribute from the drop-down menu and click the arrow key to add the attribute to the list.

- 5. If you want to modify the Details view for an incoming call, click **Details view**.
 - a. Select what you want to be displayed in the Detail view of the InAttend client.

Attendant Sea	arch	8
edit profile: InAtte	nd CMG	
Properties		Save Back
Settings	Details view	
Result layouts	First additional attribute Cordless	
Search	Second additional attribute Information	
Details view	Picture attribute Telno V Obetails	
	Hide comment column	
	Attributes for the details list	
	O Show all attributes	
	Show attributes	
	Search attribute 💉 >	
	Search attribute	
	Company O O O O O	
	Decartment	
	Email O O O O	
	FirstMessageSystemId 💿 😳 🔕	
	FirstName 🕢 🛇 🛇 🖏	
	FourthMessageSystemic O O O O	
	LastName O O O O O O 123>>>	

First additional attribute: the first of two attributes displayed on the left side of the PAM Panel in the Details view (select an attribute from the drop-down list).

Second additional attribute: the second of two attributes displayed on the left side of the PAM Panel in the Details view (select an attribute from the drop-down list)

Picture attribute: the attribute that contains information about the attendant's subscriber image (depends on the Picture Server, is normally a DN).

Hide comment column: disables the comment / information field in the left side of the PAM Panel in the Details view.

b. Specify which attributes you want displayed in the Details view:

Show all attributes: display all attributes in the contact's Details view.

Show attributes: specify the attributes you want displayed in the Details View by selecting an attribute from the drop-down list and clicking the arrow key.

You can change the order of the attributes by clicking on the arrows beside an entry to move it up or down in the list.

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

Modifying the Server profile

The Server profile specifies the location of the Presence Server, License Manager Server, and the Presence server.

To modify the Server profile, do the following:

- 1. On the Configuration profiles page, click on **Server** in the list of profiles.
- 2. On the Edit profile page, ensure that the following parameters are set correctly:

Presence Server: the server where InAttend is installed **License Manager**: the server where the License Manager is installed **CMG Web service**: the server where CMG Web is installed

Server edit profile: InAttend CMC			
Profile name InAttend CMG Description Default Server profile	x (with Presence Server).	_	Save Back to the overview
Presence Server		Ç	
INATTEND22	Global calendar settings		
Backup server	O No access		
	 Reading access Writing access 		
BluStar License Manager			
Server INATTEND22			
Backup server			
BluStar Web Service Server INATTEND22			

Working with profile groups

A profile group contains one or more configuration profiles that control InAttend client functionality. You can add or remove configuration profiles from an existing profile group, or create a new profile group. InAttend users assigned to a profile group inherit the functionality defined by the configuration profiles in that group.

By default, the system creates one profile group (the InAttend group). Please note that InAttend users have to be assigned to a profile group that contains the following configuration profiles:

- Attendant Directories
- Attendant Layout
- Attendant Messages
- Attendant PBX
- Attendant Search
- Server

Creating a new profile group

To create a new profile group, do the following:

- 1. Access the BluStar Server Administration web interface by typing the URL: http://<hostname>/webadmin in a supported web browser, where <hostname> is the InAttend server address.
- 2. Log in with the administrator credentials

(default username: admin, default password: Mitel123).

3. Select User Configuration and then Profile groups.



- 4. On the Profile group's page, click Add profile group.
- 5. On the Add Profile Group page, enter values for the following parameters:

Group name: a name to identify the profile group. **Description**: a brief description of the profile group.

6. Select the configuration profiles that you want to include in the profile group by checking the box beside the entry for the profile in the list.

Group Name	InAttendCMG		CMG Operator Group My_Operators
Description	CMG Profile Gr InAttend.	oup for	
Profile name		Profile type	
		any	begins with 💌 Search
Attendant I	e Directories Layout	InAttend Ch InAttend	ne MG
M Attendant	Messages PBX	InAttend Ch	MG
Attendant	Search	InAttend CM	MG
Attendant I Attendant I Attendant I Server Attendant I Attendant I	Search Directories	InAttend CM InAttend InAttend LD	MG DAP

7. Click **Save** to save your changes.

Modifying a profile group

To modify an existing profile group, do the following:

- 1. On the Profile groups page, click on the profile group you want to edit.
- 2. On the Edit profile group page, you can:
 - a. change the name of the profile group
 - b. change the description for the profile group
 - c. select or remove configuration profiles from the profile group
- 3. Click Save to save your changes.

Configuring InAttend users

When you create a new user, you assign the user to a profile group. The information is automatically propagated to the TCA.

- 1. Access the BluStar Server Administration web interface by typing the URL: http://<hostname>/webadmin in a supported web browser, where <hostname> is the InAttend server address.
- 2. Log in with the administrator credentials

(default username: admin, default password: Mitel123).

3. Select User Configuration and then Users.



4. On the Users page, click Add user.

Users		2.4	2		
Search field	Search type Username V begins with Number of found users A Mark all in search	Search	Add user Edit selected users	Delete selecte	d users
	Username	Mail address		Copy Delete	
	a400			D 🖸	
	admin				
	blustar_web			D 🖸	
	comdasys_amcc			C)	

5. On New User page, click User general (under Properties) and enter values for the following fields:

Username: the name of the new InAttend user **Email**: Enter the email address for the new InAttend user.

User general	2.4.0	
Properties		Save Back to the administration
User general	Username UserName	
Password/security	EMail username@company.com	
Profile groups		

6. Click Password/security and enter values for the following fields:

Password: the password for the new InAttend user. **Confirm password**: repeat the password for the new InAttend user.

User password/s	security	
New User		6 T.
Properties		Save Back to the administration
User general	Password ••••	
Profile groups	Confirm password	

7. Click **Profile groups** and select the profile group to which the user will belong (for example, InAttend CMG).



8. Click **Save** to save your changes.

Generate CSR in ACS

To generate CSR in ACS, do the following:

- 1. Start MMC on the ACS server. Go to **Files**, and select **Add/Remove Snap-in**. Click Certificate and expand Certificate with the computer account.
- 2. Click Personal > Certificate and go to All Task > Advance Operations > Create Customer Request.

GentFicates (Local Computer) CMGYMWARE28-CA 04.05.2019 <all></all>	cm
CMGYMWAREZ8-CA CMGYMWAREZ8-CA Z8.05.2028 <aii></aii>	<∿
Centificates 🖡 🖓 Wilsyc-CMGVNWARE20 WILsyc-CMGVNWARE20 17.09.2023 Server Authenticetic	n ⊲∿
🕀 🛅 Trusted Root Certification Authorities	
🕀 🗀 Enterprise Trust	
표 💼 Intermediate Certification Authorities	
🕆 🎦 Trusted Publishers	
E Untrusted Certificates	
Third-Party Root Certification Authorities	
🗉 🛅 Trusted People	
Other People	
Remote Desktop	
Cortricate Enrolment Requests	
Instruction Carol Trusted Roots	
Insted Devices	
All Tasks Request New Certificate	
Befret Import	
Ref. (20)	
Export List Avverticed operations of Create Vaccon Reducestor.	
View View	
Arranae Icons 🕨	
Line up Loops	
Help	

- 3. Click Next repeatedly for three times to get the Certificate Enrollment window.
- 4. The Certificate Enrollment window is displayed. Click Details > Properties.
- 5. The Certificate Properties window is displayed. Click the General tab and add a friendly name.



- 6. Click Subject tab, add a common name and IP address in the IP address (v4) field.
- 7. Click **Apply** to save the changes.
- 8. Click Private Key tab, go to Hash Algorithm and enter the algorithm as sha1. Click Ok.

Certificate Properties	×
General Subject Extensions Private Key	
Cryptographic Service Provider	۲
Key options	۲
Select <u>H</u> ash Algorithm Select Hash Algorithm to be used for this request	8
Hash Algorithm: sha1	
Select Signature Eormat	۲
Key permissions	۲
Learn more about private key	
OK Cancel	Apply

9. Click next and select a file name. Click Finish to generate the request.

Open a browser and access the CA server for requesting and downloading the certificate for the ACS server.

NOTE: After downloading the certificate, the file must be imported to the Personal/Trusted certificate folder. Please see *TLS Certificates Installation* for more information on Install TLS in ACS server.

TLS Certificates Installation

A certificate is required for the TLS-encrypted communication to the Microsoft Skype for Business server. You have to install a certificate before you setup communication with the Skype for Business Server.

The Certificate snap-in allows you to browse the contents of the certificate stores.

To add a snap-in and import the MX-ONE, or MiVoice 5000, or Skpye certificate for TLS into ACS, do the following:

- 1. Open the Windows MMC application.
- 2. In the Console 1 window, open the File menu and select ADD/Remove Snap-in.
- 3. Select Certificates from the Available snap-ins list and click Add.
- 4. Select Computer account and click Next.
- 5. Select Local computer (Computer account) and click Finish. Certificates are now available in the Selected snap-ins list under Console root.
- 6. In the Add or Remove Snap-ins window, click Ok.
- 7. In the Console 1 [Console Root] window, click File and then Save.
- 8. Select a file name and click Save.
- 9. Expand Certificates and then expand Personal.
- Click on the Certificates folder. Select Action > All tasks > Import. The system launches the Certificate Import Wizard.
- 11. In the Certificate Import Wizard, click Next.
- 12. Select a certificate file to import, then click Next.
- 13. When the certificate import is complete, click Ok.

CHAPTER 12

Ele Action Vew Favgetes Window Help								_18 X
Console Root Certificates (Local Computer) Prisonal	Issued To * C_icmgvmware20	Issued By CMGVMWARE20-CA CMGVMWARE20-CA	Expiration Date 04.06.2019 20.05.2020	Intended Purposes <al> <al></al></al>	Friendly Name cmgvmware20 <none></none>	Status Certi	Actions Certificates	
Emtification Trusted Root Certification Authorities Entermediate Certification Authorities Trusted Publishes Unitrusted Certification Certification Trusted Publishes Certification Enterple Certification Enterple Certification Environment Requests Second Certification Environment Certification Environment Requests Second Certification Environment Trusted Devices Trusted Devices	WHEVE-CHOMMARE20	WHSVDISIONARE20	17.09.2023	Server Authentication	dunes		More Actions	•
Personal store contains 3 certificates.	121.							

On the ACS server activate TLS with the imported certificate using NETS config.

Network Telephony	y Services configuration		×
NeTS SIP Queue	Manager		
Use SIP			
Local settings	TLS support Required	•	
SIP nodes	Allow untrusted certificates		
TLS			
	Name 20	Issued by	Expiration c
			20.05.2019
	O WMSvc-CMGVMWABE20	WMSvc-CMGVMWABE20	17 09 2023
		mmore-emarmmanezo	11.00.2020
1	•		Þ
KCan	cel <u>Apply</u>		

In TCA the port and the protocol for MX-ONE must be changed to 5061 and TLS respectively and then should be deployed. The **Mitel Network Telephony Services** must be restarted.

Configuring the NeTS telephony system

You can use the NeTS configuration tool to configure the NeTS telephony system for SIP. Configuration parameters are grouped on different tabs:

- NeTS tab: contains parameters that are specific to NeTS operation itself.
- SIP tab: contains parameters that control SIP settings in NeTS.
- Queue Manager Tab: contains parameters that control call recordings and logging.

To configure the NeTS telephony system, do the following:

- 1. Open the NeTS configuration tool (Start -> Programs -> Mitel -> NeTS).
- 2. Select the NeTS tab.

Network Telephony Services configuration X
NeTS SIP Queue Manager
Enable NCLA
Statemachine folder C:\Program Files (x86)\Mitel\TelephonyServices\Statemachines\
Statemachine unload poll interval (s) Max acceptable service startup duration (s) 60 20
Logging
Folder C:\Program Files (x86)\Mitel\TelephonyServices\Log\
Level Debug+5 V Delete older than (days) 7 🗘 Max size (MB) 10 🔪
NeTS Tester on all inbound calls Enable NeTS Remoting API
Trace statemachine loading
OK Cancel Apply

- 3. Enter values for the following parameters:
 - **a. Enable NCLA**: determines whether NeTS reads the NCLA file deployed by TCS to the machine. This is always checked when ACS is used to run InAttend or CMG speech.
 - b. Statemachine folder: the location of the state-machine files (use the default).
 - c. Statemachine unload poll interval (h): the period (in hours) at which NeTS checks the state machine to determine whether the state-machine is loaded but not used (and therefore has to be unloaded).
 - d. Max acceptable service startup duration (s): not applicable (parameter not used).
 - e. Logging Folder: location for storing log files.
 - f. Logging Level: the level of detail in the log (select a value from the pull-down list).
 - g. Logging Delete logs older than (days): maximum age of the log files before they are deleted.
 - h. Logging Max Size (MB): the maximum size for the log files. After the log file reaches the system creates a new log file.
 - i. NeTS Tester on all inbound calls: leave unchecked (parameter not supported).
 - j. **Trace statemachine loading**: enable to debug loading of statemachines. When turned on, the system provides detailed information on what succeeds and what does not when loading a statemachine. If checked during service start, NeTS attempts to load all statemachines in the statemachine folder.
 - k. Enable NeTS Remoting API: Enables WCF service "NeTS remoting".
- 4. Select the SIP tab.

	Network Telephony Services configuration
NeTS SIP	Queue Manager
Use SIP Local settings Redirects SIP nodes TLS	NeTS local SIP port for media control IINATTEND-SUNIL:5067 Outbound proxy I Use local IP in "From" header Juse local IP in "Contact" header Follow redirects Use OPTIONS as to check if calls are valid Allow REGISTER requests Media-SDP in 180 Ringing Transfer Ato B Hold before transfer Allow numbers with leading + (E.164) Load balance Media Servers PRACK support Not_Supported Option to check if SIP trunks are up. (p) Served-by-Ne TS Header Max wait for 100 Trying on Outbound calls. (ms) 1200
OK	Cancel Apply

- 5. Enable the Use SIP option (mandatory).
- 6. Click Local settings in the left panel and enter values for the following parameters:
 - a. NeTS local SIP port for media control: NeTS has a dedicated server-port for communication with the Media server. (This generally cannot be 5060, 5061, or 5065 since these are already used by NeTS, NeTS for TLS and Media server respectively.) The default is ":5067" which will open the server's default gateway IP address. If a different IP address is used, enter the full IP address and port (e.g., 192.168.123.45:5067).
 - **b. Outbound proxy**: SIP address of the proxy (if used) for all outbound transactions (e.g., 192.168.123.45:5080; transport=tcp).
 - c. Use local IP in "From" header: Some PBX's consider NeTS to be a SIP extension rather than a trunk. In such cases, the PBX may require the From-header to be <accessnumber@PBX-IP>. However, most PBX's handle the trunk; this option is enabled.
 - d. Use local IP in "Contact" header: Some PBX's consider NeTS to be a SIP extension rather than a trunk. In such cases, the PBX may require the Contact-header to be <accessnumber@PBX-IP>. However, most PBX's handle the trunk; this option is enabled.
 - e. Follow redirects: Instead of routing outbound calls, the PBX may answer with a 302 Moved Temporarily message. When this option is enabled, NeTS automatically makes a new call to the destination. If disabled, NeTS informs the application layer (QueueManager or Speech) that the call attempt failed with cause forwarded.

It is up to the application to decide if another call to the new destination is made or not.

- f. Use OPTIONS as keep-alive: Used to detect calls not cleared correctly. When there is an active call, NeTS can send out OPTIONS within the SIP-dialog to the PBX to verify that the PBX is still aware of the call.
- g. Media-SDP in 180 Ringing: if enabled, NeTS creates a conference session with the Media Server before sending a 180 Ringing message back to the PBX on inbound calls. Otherwise the 180 ringing is without SDP. Some PBX's (i.e., Skype) prefer this behaviour. NeTS does not send any early media regardless of setting.
- h. Transfer A to B: When an attendant has two calls and has to connect them, this option determines whether A is connected to B (enabled) or B is connected to A (disabled). The default (A to B) works well on most PBX's. On the Avaya call manager, the recommendation is B to A (i.e., option is disabled).
- i. Allow numbers with leading + (E.164): if disabled, NeTS removes the plus-sign on inbound and outbound calls.
- j. Load balance Media Servers: Enables or disables load balancing across multiple Media Servers. Normally NeTS communicates with the first Media server in its list that answers. This means in practice that the first Media Server that is available handles all calls. If load balancing is enabled, NeTS selects a Media Server at random from the list, to ensure load balancing across multiple Media Servers. If using this option, consider whether there are any WANs between NeTS and the Media Servers.
- k. PRACK support: specifies whether NeTS handles PRACK or not. Recommendation is "Required" if supported by the PBX. Mandatory if using a Cisco call manager. (Without PRACK enabled, some scenarios with early transfers might fail.)
- Option to check alive interval: If greater than zero, NeTS sends out-of-dialog OPTIONS to all known SIP proxies/call managers to see if they are alive. When selecting a proxy for an outbound call, NeTS prefers proxies that have answered the OPTIONS requests (and which are therefore known to be up).
- m. Served-by-NeTS Header: The header that NeTS adds to SIP messages indicates that the PBX numbers must be considered for an outbound call. The number is the number that was used to call NeTS originally.

NOTE:

- P-Served-User parameters must not be changed when integrating with the official supported PBX's, unless specifically instructed by Mitel. The requirement for what header to use is solely dictated by the call manager.
- X-Mitel-ACS-operator-id is a custom SIP header that carries the operator information. This information is carried from NeTS to the call manager in the format: operatorId@extension; for example: xyz@1234.

The custom header sends a response in the following scenarios:

- a. During Inbound call when an operator picks up the call, custom header will be sent in 200 OK.
- b. During Outbound call when an operator initiates the call, custom header will be sent in INVITE.
- c. During a Recall or when a call is parked, if the call is picked up by multiple operators, a separate **UPDATE** request is sent for each pick up, with the custom header carrying the new operator information.
- d. When **MOH** is set for queue, **200 OK** is sent before operator picks up the call. In this scenario, custom header is sent in **UPDATE** after operator picks up the call.

Max Wait for 100 Trying on Outbound calls (ms): maximum time NeTS waits for the 100 TRYING message for outbound calls.

NOTE: When an Operator/attendant calls an MX-ONE extension, the extension displays associated attendant name together with the ACS number. In the logs, from Header of **SIP INVITE** contains name along with ACS number as below:

From: "<OperatorName>" <sip:12345@10.211.xx.xx:5060;user=phone>;

7. Click **Redirects** in the left panel and enter values for the following parameters:

On media server failure / On unassigned number: Specifies how NeTS handles failures. When contact with a Media Server fails or when a call has been made to a non-handled number (i.e., a number without an assigned statemachine) NeTS sends an error-response. You can set the Response code for these events and specify a SIP address in the Contact of the response, indicating an alternate location to try and contact to the server.

- 8. Click **SIP** nodes in the left panel and enter any additional information for Media Servers and SIP proxies (apart from what is already in NCLA). Generally recommended to leave empty.
 - a. Media servers: the list of Media Servers to use. If any Media Servers are listed here, information in NCLA is ignored.
 - b. Default SIP proxies: the list of SIP proxies to use. When making outbound calls (in A or B field) NeTS sends the SIP-messages to one of these proxies. If any SIP proxies are listed here, information in NCLA is ignored.
 - **c. ACS local SIP proxy**: the SIP proxy through which to send all traffic. If a SIP proxy is specified, information in NCLA is ignored.
 - d. **Proxy timeout**: The amount of time (in milliseconds) that NeTS has to wait for a proxy to respond. Red time if it is known to not work well (previous timeout) or Green if it worked last attempt.
- 9. Click **TLS** in the left panel and enter values for the following parameters:

TLS support: specifies whether TLS is supported. Select a value from the list:

- Not supported: The TLS port is not opened. If a call manager attempts to connect, Windows indicates that the port is closed (socket error 10054).
- Supported: The TLS port is open but requests on non-TLS ports are also served.
Required: Both TLS and non-TLS ports are open. If a non-TLS request is received, NeTS responds
with a 301 Moved Permanently message, with the new Contact the same as the request URI, but
with the port and transport changed to TLS.

Allow untrusted certificates: Enables or disables verification of certificates. Normally NeTS verifies that the certificate of the remote endpoint of TLS connections are valid. Enabling this option disables that check. This option may be useful for testing an installation but cannot be used in production environments, as the system would be vulnerable to man-in-the-middle attacks.

Allow SSLS: By default NeTS only supports TLS 1 or higher.

Select NeTS certificate: A list of the certificates available in the computers certificate store. NOTE:

- When verifying that TLS is properly configured, follow these steps to test: access NeTS from a regular web browser and see if the connection succeeds. Start by going to http://NETS.computer:5060 to see that access to non-TLS works.
- Then change to https://NETS.computer:5061 to see that your web browser trusts the certificate that NeTS uses. (Note that you web browser might trust different certificates and use different client certificates than the call manager.)
- 10. Select the Queue Manager tab.

CHAPTER 13

N.TC.	CID	Cueue Managar		
TV015	SiP			
Voice	Prompts F	Path (C:\Program Hies (x35)\Mitel\QueueManager\VoicePrompts		
Reco	rding	¥	_	_
Reco	rding pati	h C:\Program Files (x86)\Mtel\QueueManager\AttendantRecord	ings	
Tmp	path	C:\Program Files (x86)\Mtel\QueueManager\AttendantRecord	lings\Tm;	***
Flena	itte	%ATT_ID\%y-%m-%d\%H%M%S.wav		
Filena	me forma	st: Ny Year		۷
Perso	nal Greet	ing		
Promp	t path			
Loggi Folde	ng r C:\P	rogram Files (x86)\Mitel\QueueManager\Logs		
Leve	Debu	g+3 ✓ Delete older than (days) 7 🔆 Max size (MB)	0 🔅	
Outbo	suna Pron			
Hards	shone Ca	fler Number 9		
		Court Note		

Enter values for the following parameters:

- Voice Prompts Path: If a prompt in TCA is entered without a path, this path is added as prefix. This
 is the path as Media server finds it. You can use environment variables on the computer in this path
 (e.g., [PROMPTS ROOT]\QueueManager).
- Recording path: the location where saved recordings are stored.
- Tmp path: the temporary location where the .wav file of a recorded call is stored. When the call ends, if it is marked to be saved, it is moved to the location specified in the Recording path field. It is recommended that the Tmp path be local on the Media Server. If recording is set to on-demand, all calls are first recorded and stored to the Tmp path and then moved (if saving is configured); otherwise the .wav files are deleted.
- Filename and Filename format: the name of the stored files, which contains instructions for the format. If you add a backslash (\), you can sort recordings into directories.
 - For example, %ATT_ID%y-%m-%d%H%M%S.wav would make one folder for each attendant/day
 of the year and name the files by the time of the call.

- For the attendant recordings to be saved with Called number and Calling number details, Filename field in Queue Manager tab of NETS config must be updated as below: %ATT_ID\%y-%m-%d\%H%M%S_%A_NUM_%B_NUM.wav
- Doing this the administrator can delete recordings based on Called/Calling number.
- Personal Greeting Prompt Path: to eliminate the repetition of the welcome message, a personal
 greeting is recorded that is played for each incoming call when operator answers the call.
 - The Administrator keeps the <OperatorLoginName@QueueEntryNumber@domainID>.wav file in the system where media server is present. This file name contains operator login name, queue entry number, and the domain id.
 - When <OperatorLoginName@QueueEntryNumber@domainID>.wav file is present in the system, this file is played after the operator picks the call. It is same for all the queues including recall queue.
 - When <OperatorLoginName@QueueEntryNumber@domainID>.wav file is not present in the system, the system falls back to <OperatorLoginName>.wav file for all the queues except recall queue.
 - The <OperatorLoginName>.wav file is never played for recall queues and the call is directly connected to receptionist in this scenario.
 - If both the files are not present, the call is directly connected to operator. The wav file is heard by receptionist as well.
 - No Configuration is required for this feature as this behavior is observed only for queue entry and not for queue.

Once the greeting is played, no other person greeting is played again to the called party.

Set the path to empty to disable the function.

- Logging Folder: location for storing log files.
- Logging Level: the level of detail in the log (select a value from the pull-down list).
- Logging Max Size (MB): the maximum size for the log files. After the log file reaches the system creates a new log file.
- Outbound From Number: Sets the number to be displayed on the called phone; that is, when the
 operator places an outgoing call, this number is displayed on the called phone. If this parameter is
 not set, the number configured in the InAttend System Configuration is displayed on the called
 phone.
- Hardphone Caller Number: Sets the number for the operator's device; that is, when NeTS calls the
 operator's device, this number is displayed on the operator device. If this parameter is not set, the
 NeTS/ QueueManager uses 0 as calling number.

Configuring the Media Server

You use the MediaServer Configuration tool to configure the Media Server.

To configure the Media Server, do the following:

1. Open the MediaServer config tool (Start -> Programs -> Mitel -> MediaServer Config).

MediaServer Configuration v1.7.64.0
MediaServer Properties
SIP port Dialog TTL
:5065 10 min
RTPport range
40000-50000 L RTCP
MOH File C:\Program Files (x86)\Mitel\MediaServer\ringing way
I rim recordings Codec Preference
pcma,pcmu,g722,g729,fc2833 all
Audia Eilas Dafu
C:\Program Files (x86)\Mitel\MediaServer\Prompts\
Default Recording Rate
SRTP SDP Offer O 8 kHz
SRTP Best Effort C 16 kHz
MediaServer Logs
Log Path
C:\Program Files (x86)\Mitel\MediaServer\Logs
Trace V 0 MB 10 days
OK Apply Cancel

- 2. Enter or change the values for the following parameters as required:
 - SIP port: The port number where the Media Server listens for SIP sessions, and optionally Ethernet interface.

:port for the default Ethernet interface

<interface>:port for a specific Ethernet interface

NOTE: If more than one network adapter is present in the server, make sure that both NeTS and the Media Server are using the same network adapter, by specifying the IP address in the SIP Port configuration. The same IPaddress as in the TCA host configuration for the NeTS is used.

- Dialog TTL: Number of minutes a SIP dialog may exist without receiving any RTP data.
- RTP port range: the ports reserved for RTP traffic.
- RTCP: enables Real Time Transport Control Protocol (RTCP), the control protocol for RTP.
- MOH File: This is the path to the Music file configured in the MediaServer configuration. The file
 must be an A-law/U-Law wav file. The music is played when the call is placed in the following situations:
 - On Hold
 - Camp on Queue
 - Park Queue
 - In the Queue

MediaServer Properties	
SIP port	Dialog TTL
5065	10 min
RTPport range	
40000-50000	RTCP
MOH File	
C:\Program Files (x86)\Mite	el\MediaServer\ringing.wav
Trim recordings	
Codec Preference	
ncma ncmu g722 g729 fc2	2833 all
Porward DTMF to conte	erence
Audio Files Prefix	
C:\Program Files (x86)\Mite	MediaServer/vinging.wav
	Default Recording Rate
SRTP SDP Offer	O 8 kHz
SRTP Best Effort	16 kHz
Media Server Loos	
Ci) Program Files (x96)) Mite	Madia Secure Lace
C. (Flogiani Files (coo) (Mile	n Wedid Server Logs
Trace Max	0 MP 2 dave
nace v	2 udys

- Trim recordings: enables the removal of silent parts from recorded messages.
- Codec Preference: Defines the preferred codecs in prioritized order (e.g., alaw, ulaw, rfc2833).
- Audio Files Prefix: Not used by InAttend.

- SRTP SDP Offer: enables encryption of outgoing calls. (NOTE: this setting is not recommended for MX-ONE).
- SRTP Best Effort: Allows an answer without SRTP. If not enabled, "SRTP Strict" is applicable (i.e. RTP/SAVP is the SDP profile used in the SDP offer and SRTP is not allowed to be disabled if it has been enabled before).
- Default Recording Rate: The recording rate for media. Possible values are:

8 kHz (PCMA/8000 – 64 kbps)

16 kHz (L16/16000 – 256 kbps)

This default setting is used if there is no other value specified by NeTS.

- If you select the recording rate as 8.000 samples per second, Media Server saves the data in PCMA (also known as A-law).
- If you select the recording rate as 16.000 samples per second, Media Server saves the data in L16 (also known as 16 bit PCM).
- Log Path: Path to the directory where the log files are saved.
- Log Level: Level of details in log files.
- Max Size: The maximum size of the log file, in MB.
- Discard After: Clears the log file after a specified number of days.

Installing the InAttend Client

After you have completed configuration of the InAttend server, you can install and configure the InAttend Client for your users. The InAttend Client provides the user interface for the InAttend application.

To install the InAttend client software on each client machine:

- 1. Double-click the **Install.exe** file in the top-level directory of your software package to launch the Mitel Installer.
- 2. In the Installer main window, click Install.
- 3. In the Install Wizard, select Install InAttend Client.
- 4. In the Installation window, review the components that are being installed. Components with a green check mark are already installed. Click **Next**.

🕅 Mitel InAttend				
Install InAttend Client				
Component	Version	Installed	Information / Prerequisites	
 Microsoft VC 2010 SP1 Runtime Microsoft VC 2012 Runtime Microsoft VC 2013 Runtime Microsoft .NET Framework 3.5 Microsoft .NET Framework 4.7.2 Restart 	10.0.40219 11.0.50727 12.0.21005 3.5 4.7 -	10.0.40219 11.0.61030 12.0.21005 3.5.30729.4926 4.7.03062 -		
Jan 15, 2019			< <u>B</u> ack <u>N</u> ext >	<u>C</u> ancel

5. On the Welcome page for InAttend Client Setup, click Next.



- 6. On the Configuration page, enter the server address for the Data Access Service in the Hostname field. (In single-server deployments, this is the hostname or IP of the InAttend server.) If a backup server is used, enter the address for the Data Access Server backup server in the Backup field. Click Next to continue.
- 7. On the Configuration page, enter the **Extension** number for the attendant and click Next.

Mitel InAtte	nd Setup 🛛 🗙
Configuration	🕅 Mitel
Please enter the answer extension you want to us	se for your Attendant:
Extension 12345	
Installshield -	< <u>B</u> ack <u>N</u> ext > Cancel

8. On the Choose Destination Location page, specify the **Destination Folder** (by accepting the default or browsing to a different location). Click **Next** to continue.

Mitel InAttend Setup	X
Choose Destination Location Select folder where setup will install files.	🕅 Mitel
Setup will install InAttend in the following folder. To install to this folder, click Next. To install to a different folder, click Brows another folder.	se and select
Destination Folder C:\Program Files (x86)\Mitel\InAttend\	Browse
InstallShield	Cancel

9. Click Install to start the InAttend Client installation.

Mitel InAttend Setup	x
Ready to Install the Program The wizard is ready to begin installation.	🕅 Mitel
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back the wizard.	. Click Cancel to exit
InstallShield	Cancel

10. On the Wizard Complete page, click Finish to close the wizard.

The InAttend Client software is installed.

Configuring the InAttend Client

Refer to InAttend User Guide, for more information on how to configure the InAttend Client.

Configuring EFS

Encrypting File System (EFS) is a feature that provides filesystem-level encryption.

It is recommended to enable EFS on the folders where the application log, trace files and database backups are stored. This will ensure that prevention of unauthorized access

You must start InAttend services components using admin credentials or the user account which has administrator privileges.

If you start these services components using local system credentials, some of the services will not start and the log will not be generated.

Reference to log files that needs to be encrypted – Section 18.2 Log Directory for each Component **NOTE:** EFS is only possible on NTFS

Services (Local)					
elect an item to view its description.	Name	Description	Status	Startup Type	Log On As
	Message Queuing	Provides a	Running	Automatic	Network Service
	Microsoft (R) Diagnostics Hub Sta	Diagnostics	-	Manual	Local System
	Alicrosoft Account Sign-in Assistant	Enables use		Manual (Trig	Local System
	🖾 Microsoft App-V Client	Manages A		Disabled	Local System
	Microsoft iSCSI Initiator Service	Manages In		Manual	Local System
	Microsoft Passport	Provides pr		Manual (Trig	Local System
	Microsoft Passport Container	Manages Io	Running	Manual (Trig	Local Service
	🔍 Microsoft Software Shadow Copy	Manages so		Manual	Local System
	🖏 Microsoft Storage Spaces SMP	Host service		Manual	Network Service
	Mitel BluStar License Service	Mitel BluSta	Running	Automatic	.\Administrator
	🍓 Mitel BluStar Web Service	Backend ser	Running	Automatic (D	.\Administrator
	🍓 Mitel Calendar Connection Default	Mitel Calen	Running	Automatic	Local System
	🍓 Mitel Configuration Agent	Receives co	Running	Automatic	.\Administrator
	🍓 Mitel CTI Server	CTI Server f	Running	Automatic	.\Administrator
	🍓 Mitel DAL Server	Data Access	Running	Automatic	.\Administrator
	🍓 Mitel Directory Server	Directory Se	Running	Automatic	Local System
	🎑 Mitel Enterprise License Manager	Administers	Running	Automatic	.\Administrator
	🍓 Mitel InAttend Configuration Service	Backend ser	Running	Automatic (D	Local System
	🍓 Mitel InAttend History Service	Service resp	Running	Automatic (D	.\Administrator
	🍓 Mitel MediaServer	Mitel SIP Ba	Running	Automatic	.\Administrator
	🍓 Mitel Network Telephony Services	Mitel Netw	Running	Automatic	.\Administrator
	🍓 Mitel Presence Notification	Mitel Calen	Running	Manual	.\Administrator
	🍓 Mitel Presence Server	Presence Se	Running	Automatic	.\Administrator
	🍓 Mitel Queue Manager	Mitel Queu	Running	Automatic	.\Administrator
	🏩 Mitel Service Manager	Service Man	Running	Automatic	Local System

Setting up Quality Manager

You can extend InAttend functionality with the installation of optional components. The **Browse Pack-ages** view (the classic package browser) contains the software required for the installation of optional components.

To open the package browser, click the **Browse Packages** link in the Mitel Installer main window. The package browser window displays the InAttend software components.

The Quality Manager enables measurement and reporting of real-time and historical InAttend traffic and evaluates call flow. The Quality Manager Wallboard (typically installed on a client PC) provides real-time traffic views.

Prerequisites

Note the following before you install the Quality Manager Server components:

- Microsoft XML Core Services has to be installed before the Quality Manager Service.
- MSXML Core Services is an application for processing Extensible Style Sheet Language Transformation (XSLT) in XML files. This component is typically installed during InAttend Server installation, but you can also install it from the Quality Manager Server folder in the Classic Browse Packages installer.
- The Quality Manager Service must be installed before the Quality Manager Wallboard application.
- After upgrading Quality Manager Reports Web, the qmadmin password is reset. The new qmadmin password is 'mitel', valid for both upgrade and new installation.

NOTE: After the first login to Quality Manager Reports Web, user must change the password for qmadmin.

Installing the Quality Manger Server

The Quality Manager Server has three components:

- Quality Manager Database
- Quality Manager Service
- Quality Manager Reports Web

Installing the Quality Manager Database

If a database already exists, the system saves all existing data and upgrades the database. However, it is strongly recommended that you back-up the database before installation.

NOTE: Connection information is only used during installation and provides the installation with system administrative rights on the selected Microsoft SQL Server.

To install the Quality Manager database, do the following:

- 1. Double-click the **Install.exe** file in the top-level directory of your software package to launch the Mitel Installer.
- 2. In the Installer main window, click Browse Packages.

- 3. In the left panel of the Installation Wizard, expand the **Optional Server Components** folder and then expand the **Quality Manager Server** folder.
- 4. Under the Quality Manager Server folder in the left panel, click on Quality Manager Database.
- 5. In the main Installer window click Install or upgrade CMG Quality Manager Database.
 - The Installation Wizard launches the Quality Manager Database Setup wizard.
- 6. On the Welcome page, click Next.
- 7. On the End User License Agreement page, review the terms of the license agreement, then check I accept the terms in the License Agreement and click Next.
- 8. On the Quality Manager Database configuration page:
 - a. In the **Database host** field, specify the name of the Microsoft SQL Server where the main Quality Manager Database resides.

Select **SQL Login** and enter the **Username** and **Password** of the SQL administrator. Click Next.

- 9. On the Ready to Install page, click Install to install the Quality Manager Database.
- 10. When the wizard completes the Quality Manager Database installation, click Finish to exit.

Installing the Quality Manager Service

To install Quality Manager Service, do the following:

- 1. In the left panel of the Installation Wizard, expand the **Optional Server Components** folder and then expand the **Quality Manager Server** folder.
- 2. Under the Quality Manager Server folder in the left panel, click on Quality Manager Service.
- 3. In the main Installer window click Install or upgrade CMG Quality Manager Service.

The Installation Wizard launches the Quality Manager Service Setup wizard.

- 4. On the Welcome page, click Next.
- 5. On the End User License Agreement page, review the terms of the license agreement, then check I accept the terms in the License Agreement and click Next.
- 6. On the **Destination Folder** page, specify the installation path for the Quality Manager Service (or keep the default path) and click **Next**.
- 7. On the Ready to install Quality Manager Service page, click Install.

The system installs the Quality Manager Service. The system also installs the Configuration Agent if not already installed.

8. When the wizard completes the Quality Manager Service installation, click Finish to exit.

Installing the Quality Manager Reports Web

You can install Quality Manager Reports Web on any computer that has access to the Quality Manager server through the network. It is recommended that you install Quality Manager Reports Web on the main Quality Manager server.

Before you start the installation, make sure Internet Information Services (IIS) is installed.

To install Quality Manager Reports Web, do the following:

- 1. In the left panel of the Installation Wizard, expand the **Optional Server Components** folder and then expand the **Quality Manager Server** folder.
- 2. Under the Quality Manager Server folder in the left panel, click on Quality Manager Reports Web.
- 3. Click the link Install or upgrade CMG Quality Manager Reports Web.
- 4. On the Welcome page, click Next.
- 5. Read and accept the license agreement.
- 6. On the **Select Web Site** page, select a web site and enter the name of the web application, and click **Next**.
- 7. On the **Destination Folder** page, specify the installation path or keep the default path. Click **Next**.
- 8. On the Quality Manager Database configuration page:
 - a. In the **Database host** field, specify the name of the Microsoft SQL Server where the main Quality Manager Database resides.

Select **SQL Login** and enter the **Username** and **Password** of the SQL administrator. Click **Next**.

9. On the Ready to install Quality Manager Reports Web page, click Install.

The system installs the Quality Manager Reports Web component.

10. When the wizard completes the Quality Manager Reports Web installation, click Finish to exit.

Configuring the Quality Manager Server

To complete the set up the Quality Manager Server, you have to:

- configure the InAttend Server to recognize the Quality Manager service
- populate the Quality Manager database with the InAttend configuration information
- configure the Quality Manager service using the QM Configuration Manager tool

Configuring the InAttend Server for Quality Manager

The InAttend Server has to be aware of Quality Manager for call information to be delivered to Quality Manager. To configure the InAttend Server for Quality Manager, you have to create a new Quality Manager cluster in the Telephony Configuration Application (TCA).

To create a Quality Manager cluster, do the following:

- 1. Open a browser and log in to the TCA tool (http://<InAttend-Server-address>/tca).
- 2. Click on the configuration profile for your InAttend system in the left panel.
- 3. Click on **Subsystems** in the left panel to display the Subsystems page in the main window.
- 4. Click on the New button in the Quality Manager Clusters entry.

Telephony Configuration Application	Subsystems Click on "New" to create a new	element in th	ne site.
Jaco-Lab	Subsystem Summary		
	Linestate Servers	1	New
	Queue Managers	1	New
Subsystems	NeTSs	1	New
Linestate Servers	PBXSTDs	0	New
⊕ Queue Managers	Quality Manager Clusters	0	New
• NeTSs	Media Servers	1	New

- 5. In the New Quality Manager cluster window:
 - a. In the Name field, specify a name for the Quality Manager cluster.
 - **b.** In the Host field, select the server on which the Quality Manager resides from the pull-down menu.
 - c. Select the Queue Manager cluster to use for Quality Manager.
 - d. Click Add.

Setting	S
Name	Quality Mgr cluster 🛛 🗙
Host	AKKRUM (InAttend server) V New
Use Qu	eue Manager Cluster
Queue	Manager Cluster
	Queue Manager 🗸 Add

- 6. Click Create to create the Quality Manager cluster.
- 7. In the main window, click **Deploy** to deploy your configuration changes. Note that the new system configuration has to be deployed before Quality Manager can collect any statistics.

Configuring multiple customers for Quality Manager

You can generate reports for multiple customers using Quality Manager. To enable this functionality, you have to define a domain for each customer in TCA. If more than one customer belongs to the same call manager, the number (device) ranges has to be unique for each customer. It is also very important that the customer's queue access number is configured in the correct domain.

- 1. In TCA, click Sites in the left panel to display the Sites page in the main window.
- 2. On the Sites page, click **My_Site** and expand the private network component in the left panel to display the new network and the new call manager.
- 3. Click **Domains** to display domain information for the call manager in the main window.

- 4. Create a new domain for the customer. For detailed instructions, see "Add a domain to the PBX" on page 186.
- 5. Repeat step 4 for each additional customer.
- 6. Click **Deploy** in the main window to deploy the new configuration.

Populating the Quality Manager Database with InAttend configuration

The InAttend configuration architecture has to be stored in the Quality Manager database for Quality Manager system configuration. You have to configure the connection to the InAttend database before configuring the remainder of the Quality Manager Service.

You use the QM Configuration Manager tool to configure the Quality Manager Service.

- Launch the QM Configuration Manager tool from the Windows Start menu (Start > Programs > Mitel -> Quality Manager Config).
- 2. On the QM service settings tab, set the following parameters:
 - a. In the General section, specify values for the following:
 - Queue Manager Degrade Timeout: The interval the Quality Manager waits for events and data from Queue Manager before considering the Queue Manager to be unavailable. The Queue Manager could be unavailable due to a network failure or an error in the Queue Manager.
 - **Operator Login Degrade Timeout**: The interval used to set the time of an operator log out event that occurs when the Quality Manager is shut down. If the Quality Manager Service is shut down, operator events are no longer registered. If an operator logs out during this time, Quality Manager does not know the exact time of this logout event but records a time for the event when started again. The time is set to the current time or the previous login event's time plus the Operator Login Degrade Timeout, whichever occurs first.
 - b. In the Log settings section, specify values for the following:
 - Log path: The location where Quality Manager Log files are stored.
 - · Log filter level: The level of detail recorded in the log file.
 - c. In the DB connection section, specify values for the following:
 - **Integrated Security**: enables or disables Windows integrated security as the authentication mode (if enabled, the User and Password fields are disabled).
 - Server: the IP address of host where the InAttend database resides.
 - Database: the name of the InAttend database.
 - User: the name of the account used to access the InAttend database.
 - Password: the password for the account used to access the InAttend database.
 - d. In the Journal DB connection section, specify the values for the following:
 - Server: Enter the IP Address of the database server.
 - Database: Enter the name of the database. By default, the value of Database is Milog.
 - Username: Enter the username with access to the same database. By default, the username is sa.
 - **Password**: Enter the password of the user.
 - e. Click Test connection to verify that the Quality Manager can access the InAttend database.
- 3. Click Save settings.

- 4. Click Close to close the QM Configuration Manager tool.
- 5. Re-start the Quality Manager Service.

When the Quality Manager Service starts, it detects that a new InAttend configuration is available on the server and populates the Quality Manager database with the information.

6. Stop the Quality Manager Service to complete the remainder of the configuration.

Configuring the Quality Manager Database

You can specify how long the Quality Manager database retains data, using the QM Configuration Manager tool.

To configure the Quality Manager database, do the following:

- Launch the QM Configuration Manager tool from the Windows Start menu (Start > Programs > Mitel -> Quality Manager Config).
- 2. Select the DB settings tab.
- 3. Select values for the following settings:
 - Archive data: indicates that old data (statistics) is archived in another database.
 - Delete data: indicates that old data (statistics) is deleted.

Note that deleted data is permanently lost.

- Clear data after <x> days: days before data being cleared (default is 730 days).
- 4. Click Save DB settings to apply your changes.

Use the remaining tabs in Quality Manager Configuration Manager Application to configure data that Quality Manager uses (e.g., customers and queues). This data is stored in the main Quality Manager database.

Configuring the Journal Database

After installing the QM service, perform the following to configure Journal Database

- 1. Go to the QM Configuration Manager and enter the following parameters for the primary server in the **Journal DB connection**.
 - Server: Enter the IP Address of the database server.
 - Database: Enter the name of the database. By default, the value of database is Milog.
 - Username: Enter the username with access to the same database. By default, the username is sa.
 - Password: Enter the password of the user.
- 2. In case of redundancy servers, optional back-up server can be configured, enter the parameters for the backup server in the **Journal Backup DB connection**.
- 3. Click Save Settings and execute IISRESET. This will refresh new values in the QM web.

CHAPTER 17

QM Configuration Manager			-	
M service settings DB settings Work	ing hours Custome	rs Queues Domains Interval sets		
General				
Queue Manager Degrade Timeout	minutes			
Operator Login Degrade Timeout 480	minutes			
Log settings				
Log path C:\Program File	s (x86)\Mitel\Quality	Manager\Logs		Browse
Log filter level Debug3	•			
DB connection				
Integrated security				
Server localhort	User	amuser		
Database am	Password			
Ja				
		Test connection		
Journal DB connection				
Server 10.211.63.95	User	sa		1
Database milog	Password		Test connection	
Journal Backup DB connection				
Server	User			1
Database	Password		Test connection	

Configuring Working Hours in Quality Manager

The Quality Manager is aware of switchboard working hours to show operator working hour statistics correctly. You set working hour parameters in the QM Configuration Manager.

After the new working hours have been configured, it takes up to ten minutes before the changes take effect.

In the QM Configuration Manager application, do the following:

- 1. Select the Working hours tab.
- 2. Select the days of the week that the switchboard is open.
- 3. For each working day, specify the hours for open and close of business, or select **24-hour open** if the switchboard is open 24 hours a day.
- 4. Click Save working days to apply your changes.

🔡 QM Configuration	Manager					
QM service settings	DB settings Working h	iours Customers Q	ueues Domains Interval	sets		
Working days			-	7		
Monday	Open 8:00 💌	Close 18:00 -	24-hour open			
🔽 Tuesday	Open 8:00 💌	Close 18:00 💌	🔲 24-hour open			
🔽 Wednesday	Open 8:00 💌	Close 18:00 💌	🔲 24-hour open			
🔽 Thursday	Open 8:00 💌	Close 18:00 💌	🔲 24-hour open			
🔽 Friday	Open 8:00 💌	Close 18:00 💌	🔲 24-hour open			
🗖 Saturday	Open 0:00 💌	Close 0:00 💌	🔲 24-hour open			
🗖 Sunday	Open 0:00 💌	Close 0:00 💌	🗖 24-hour open			
			Save working days	_		
Exceptions						
Description		Date	Every year			
				DeleteEdit	New	
W. Europe Stand	W. Europe Standard Time (automatic daylight saving time configured) Reassign working hours					
					Close	

5. Optionally, define one or more exceptions to the configured working days. For example, the switchboard might be closed on a statutory holiday, even though it might occur on a weekday.

In the Exceptions section, click New.

- 6. In the New exception dialog, do the following:
 - a. In the **Description** field, enter a name for the exception.
 - b. In the **Date** field, enter a date for the exception.
 - c. Check the Occurs yearly option if the exception occurs every year on the same date.
 - d. Click Create to apply your changes.

The new exception appears in the list of exceptions on the Working hours tab.

- 7. Repeat steps 5 to 6 for each additional exception.
- 8. Click Reassign working hours to save your changes.

NOTE: If you do not reassign the working hours, the statistics shown may be misleading. Working hours are reassigned even if you select to keep the default working hour's settings.

Configuring customers in Quality Manager

You can create and edit customers on the Customer tab of the QM Configuration Manager application. You have to define at least one customer for Quality Manager to collect statistics. **NOTE:** Quality Manager identifies a customer by the domain of the customer's access numbers (route points) to the queues. The domain for each customer is defined on the Domains tab. A domain cannot be shared between two customers.

In the QM Configuration Manager application, do the following:

1. Select the **Customers** tab.

🔜 QM Configuration Manager		
QM service settings DB settings Working ho	urs Customers Que	ues Domains Interval sets
New customer Name J V Active Create Cano	el	
Name	Active	
Aastra Mitel	Yes Yes	
Delete Edit domains	dit	

- 2. To add a new customer, do the following in the **New customer** section:
 - a. In the Name field, specify a name for the customer.
 - **b.** Select the **Active** option if the customer is an active customer in the system. (Customers not marked as active can, for example, be previous customers or prospective customers.)
 - c. Click Create to add the customer.

The new customer appears in the list of existing customers.

- 3. If you want to edit the name of an existing customer, double-click on the customer entry in the list and specify a new name in the **Edit customer** dialog.
- 4. If you want to edit the customer's ranges, select the customer from the list and click on Edit.
- 5. If you want to delete an existing customer, select the customer from the select and click **Delete**. Note that you cannot delete a customer if there are already statistics stored for that customer.

Viewing queues in Quality Manager

Queues are defined in the ACS (using the TCA tool), and are stored in the Quality Manager database with the collected queue statistics. Queues are stored in the Quality Manager when the Quality Manager Service receives configuration information from the ACS.

In the QM Configuration Manager application, do the following:

1. Select the Queues tab.

The Queues tab displays a list of all queues configured for InAttend, with the following information for each queue:

- Name: the name of the queue in Quality Manager. You can rename a queue to make the queue reports more customized.
- Queue ID: The unique identifier for the queue in the ACS.

- Queue Name: the name of the queue in the ACS.
- Queue Type: the queue type configured in the ACS (public or private).

🔡 QM Configuration	Manager				
QM service settings	DB settings Vorking hours	Customers Que	eues Domains In	terval sets	
Name	Queue ID Q	ueue Name	Queue Type		
External	281050f0-ab3 E:	xternal	public		
Internal	edf63117-5e6 In	ternal	public		
Park	d/df28e2-6c5 P	ark	private		
Park Danall	325fdcfd-b575 P	ark "	private		
Recall Recall SA	23640036-160 H	ecall cooll CA	private		
SA NECAROA	d951ad07.077 Si	есанод А	public		
J. J.	0001000r0rr 0/	-	public		
1					
					E dit
L					
					Close

- 2. If you want to edit the name of a queue in Quality Manager, double-click on the queue entry in the list.
- 3. In the Edit queue dialog, specify a new name in the Name field.

Note that all other queue information is read-only. Any other changes to queue configuration is done in the ACS (using the TCA tool).

4. Click **Update** to save your changes.

Assigning customers to a domain in Quality Manager

The customers you create in the QM Configuration Manager tool (see above) are assigned to a domain. Domains are configured in InAttend using the TCA tool and are stored in the Quality Manager database when the Quality Manager Service receives configuration information from the ACS (at service start-up). **NOTE:** Domains cannot be shared. A customer might have several domains, but a domain can only belong to one customer.

In the QM Configuration Manager application, do the following:

1. Select the Domains tab.

The **Domains** tab displays a list of the domains configured for InAttend.

🔡 QM Conl	iguration Manager							
QM service	settings DB settings \	Working hours 🛛 (Customers Qu	leues Dor	mains	Interval sets		
NCLA ID	Name	Domain type	Customer					
1: Domai	Domain 1	PBX	Aastra					
2: Domain2	Domain2	PBX	Mitel					
1								
								Save

- 2. Select a domain entry in the list, and click on the **Customer** field.
- 3. Select a customer from the drop-down list to assign the customer to that domain.
- 4. Click Save to apply your changes.

Configuring interval sets in Quality Manager

An interval set is a collection of intervals used to measure certain types of statistics, such as queue time, handling time, camp-on time, and total call time, average queue time and average handling time. An interval is measured in seconds.

When you create intervals, you specify values that Quality Manager uses to determine the boundaries for each interval. For example, an interval set with intervals of 0-5s, 5-10s, 10-15s, 15-30s, 30-60s and >60s has boundary values of 5, 10, 15, 30 and 60.

Intervals are defined as "closed-open". Each interval includes all numbers between the start and end boundaries, including the start value but not the end value. For example, the interval 5-10s includes 5 but not 10 (since 10 is included in the next interval).

NOTE: Once intervals have been added to an interval set, you cannot change them, as this could compromise statistics that have already been collected.

When you configure the interval sets, consider which interval sets you need for each statistic type (Stat-Type). Statistic types can share interval sets (for example, queue time and camp-on time could use the same interval set).

In the QM Configuration Manager application, do the following:

- 1. Select the Interval sets tab.
- 2. In the Interval sets section, click New.

In the **New interval set** dialog, specify a name for the new interval set and click Create to save your changes. The new interval set appears in the list.

	Intervals					
		New into	erval set intervalseti Create	× Close		
tatType intervals	ets			Delete	<u>E</u> dt	New
atType Jueue time Fanding time Camp on time	Valid from	ID	SetName			
wa car ume wa queue time wa handling time						

- 3. Select the interval set you created from the list and click Edit.
- 4. In the Edit interval set window, click Create intervals to add intervals to the interval set. (The Create intervals option is only available for empty interval sets.)

NOTE: Once intervals have been added to an interval set, you cannot change them.

- 5. In the Edit intervals window, do the following:
 - **a.** Specify a value for the first interval value.
 - b. Click Insert to add the interval boundary to the set.
 - c. Repeat for each boundary you want to define for the interval set.
 - d. When you have added all interval boundaries, click Save to apply your changes.

Edit intervals	×
Boundary (sec) 5 10 15 30 60	insert
	<u>S</u> ave
	<u>C</u> lose

e. Click Close to exit the dialog.

The new interval set and intervals are displayed in the Interval sets area of the main tab.

Г	Inter	val sets	
	ID	Name	Intervals
	6 7 8 9		0<11, 11<31, 31<60, 60 0<5, 5<15, 15<30, 30 0<10, 10<20, 20<30, 30<40, 40 0<60, 60<120, 120<240, 240<480, 480<960, 960
	,		Delete Edit New

- 6. If you want to change the name of an existing interval set:
 - a. Select the interval entry in the list and click Edit.
 - b. Specify a new for the interval set.
 - c. Click Update name.
- 7. If you want to delete an existing interval set, select the entry in the list and click Delete.

An interval set can be deleted only if it has not been used to collect statistics. If the interval set that has already been used for statistics, a warning message is displayed and the set is not deleted.

8. To assign an interval set to a StatType, do the following:

a. In the StatType interval sets section, select a StatType from the list in the left panel.

- b. Click New.
- 9. In the NewStatType interval set dialog, do the following:

StatType interval sets				
StatType Queue time Handling time Camp-on time Total call time Avg queue time Avg handling time	Valid from	ID	SetName	New StatType interval set StatType Handling time Valid from Interval set ID Intervalset1 (1) Create Close
				Delete Edit <u>N</u> ew

a. In the Valid from field, select the date from which to activate the interval set.

The valid-from date has to be equal to or greater than the current date. If there are no previous Stat-Type interval sets connections, you can use the current date. Otherwise the valid-from date has to be greater than the current date. All valid-from dates start at midnight, local time.

- **b.** In the **Interval set ID** field, select the interval set for the StatType from the pre-populated drop-down list.
- c. Click Create to apply your changes.

10. Repeat steps 9 and 10 for additional StatTypes, as required.

NOTE: A StatType can have several interval sets but only one can be active at a time. This means that you can add an interval set to a StatType in advance and it takes effect on the specified valid-from date. The interval sets for each StatType includes intervals with an adequate level of detail for the collected statistics to be meaningful.

For example, if all calls are answered within 30 seconds, an interval set with intervals of 0-45s, 45s-1min is not useful, since all calls fall into the first interval.

However, an interval set with intervals of 0-5s, 5-10s, 10-15s, 15-20s, 20-25s, 25-30s and >30s is more appropriate.

If you are uncertain of the queue time distribution, you can start with one interval set; if it does not meet your needs, you can change to another set at a later time.

Installing the Quality Manager Wallboard

The Quality Manager Wallboard is a PC client application that provides a real time view of traffic in the InAttend system. This application is usually installed on a different machine, but can reside on the same machine as the Quality Manager Server.

Before installing Quality Manager Wallboard, follow the steps given below:

- Create an attendant user (see User Configuration, on page 126).
- Add the attendant user to an operator group in TCA. Make sure the operator group is configured with at least all of the queues that the Wallboard application will monitor.

To install the Quality Manager Wallboard, do the following on the client machine:

- 1. Double-click the **Install.exe**file in the top-level directory of your software package to launch the Mitel Installer.
- 2. In the Installer main window, click Browse Packages.
- 3. In the left panel of the Installation Wizard, expand the **Optional Server Components** folder and then expand the **Quality Manager Server** folder.
- 4. Click on the Quality Manager Wallboard (optional) component.
- 5. In the main Installation Wizard window, click the Install or upgrade CMG Quality Manager Wallboard (optional) link.

The Installation Wizard launches the Quality Manager Wallboard Setup wizard.

- 1. On the Welcome page, click Next.
- 2. On the End User License Agreement page, review the terms of the license agreement, then check I accept the terms in the License Agreement and click Next.
- **3.** On the **Destination Folder** page, specify the installation path for the Quality Manager Wallboard application (or keep the default path) and click Next.
- On the Language page, select the language you want to use in the Quality Manager Wallboard interface.
- 5. On the Ready to install Quality Manager Wallboard page, click Install.

The system installs the Quality Manager Wallboard application.

6. When the wizard completes the Quality Manager Wallbaord installation, click **Finish** to exit.

Configuring the Quality Manager Wallboard application

You configure the Quality Manager Wallboard application from the Settings menu in the application itself.

To access the Wallboard Settings tool, do the following:

- Launch the Quality Manager Wallboard application from the Start menu (Start > Programs > Mitel > Quality Manager Wallboard).
- 2. Open the File menu and select Settings, or press F9.

The application displays the Wallboard Settings page.

Configuring the Quality Manager Database Connection

You have to configure a connection between the Quality Manager Wallboard application and the Quality Manager database to receive information on InAttend traffic.

To configure the connection to the Quality Manager database, do the following:

1. Select the **QM database** tab.

🥙 Wallboard settings	
QM database ACS Queues Operators Layout Thresholds	
Server: 192.168.162.20	
Database: qm	
User: qmuser	
Password:	
Refresh interval (s): 5	
Connect	
	OK Cancel

- 2. Specify values for the following parameters:
 - Server: the IP address of the server hosting the Quality Manager database.
 - Database: the name of the Quality Manager database (i.e., qm).
 - User: the name of the account configured for Quality Manager Database access. The user account "qmuser" is created during Quality Manager Installation and is configured with access to the QM database.
 - Password: the password of the account configured for Quality Manager Database access. Default value is "Tomat2007".
 - **Refresh intervals**: The number of seconds between data updates from the Quality Manager database. Shorter refresh intervals result in a heavier processing load on the database.
- 3. Click **Connect** to test the connection to the Quality Manager database.
- 4. Click **OK** to apply your changes.

Configuring the InAttend Connection

To configure the connection to the InAttend server, do the following:

1. Select the **ACS** tab.

y Wallboard s	ettings	-	
QM database	ACS Queues Operators Layout Thresholds		
QueueMana	ger		
Server:	192.168.162.20		
Port:	4813		
AnA URL:	http://192.168.162.20/nwAnA		
TCS URL:	http://192.168.162.20/TCS		
CMG opera	lor		
Username:	niceadmin		
Password:	••••••		
Company:			
	Connect		
		ОК	Cancel

- 2. In the Queue Manager section, specify values for the following parameters:
 - Server: IP address of the InAttend server.
 - Port: TCP port number of the ACS Queue Manager component, configured in the Telephony Configuration Application (TCA). Default value is 4812.
 - AnA URL: URL to the Authentication and Authorization service (e.g., http://<hostname>/nwAnA).
 - TCS URL: URL to the Telephony Configuration Service (e.e., http://<hostname>/TCS).
- 3. In the CMG operator section (for installations including CMG BluStar Server), specify values for the following parameters:
 - **Username**: user name of an operator created for the Quality Manager Wallboard application (created in the CMG Configuration Manager).
 - **Password**: password of the operator created for the Quality Manager Wallboard application.
 - Company: company of the operator as configured in CM Configuration Manager
- 4. Click Connect to connect to the InAttend system.

Configuring the Queues to display

Queues are stored in the database by the Quality Manager, which receives information on all queues in InAttend. You can rename queues using the QM Configuration Manager.

Only public queues are displayed in the Wallboard.

To configure the queues to display in the Wallboard application, do the following:

1. Select the Queues tab.

Mallboard settings		- - X
QM database ACS Queues Operators Layout Thresholds Available queues Displayed queues External Internal Recall-SA SA Image: SA SA SA		
	ок	Cancel

- 2. Select a queue from the **Available queues** list and click the right arrow to move it to the **Displayed queues** list.
- 3. Repeat step 2 for each additional queue you want to display.
- 4. To remove a queue from the Wallboard display, select the entry in the Displayed queues list and click the left arrow to move it back to the **Available queues** list.
- 5. Optionally, change the order of the displayed queues by selecting a queue in the **Displayed queues** list, and clicking on the up or down arrows to move the queue higher or lower in the list.
- 6. Click OK to apply your changes.

Configuring operators to display

To configure the operators to display in the Wallboard application, do the following:

1. Select the **Operators** tab.

Wallboard settings		
QM database ACS Queues Operators Layout Thresholds Available operators Displayed operators Eka-1 Ekanbar Speech Jessica Bka-2 Eka-2		▲ ▼
	ок	Cancel

2. Select an operator from the **Available operators** list and click the right arrow to move it to the **Displayed operators** list.

- 3. Repeat step 2 for each additional operator you want to display.
- 4. To remove an operator from the Wallboard display, select the entry in the **Displayed operators** list and click the left arrow to move it back to the **Available operators** list.
- 5. Optionally, change the order of the displayed operators by selecting an operator in the **Displayed operators** list, and clicking on the up or down arrows to move the operator higher or lower in the list.
- 6. Click OK to apply your changes.

Configuring the Wallboard layout

You can customize the Wallboard display to accommodate the size and resolution of the screen. You can also specify whether the Wallboard shows a summary of call traffic or statistics by operator. Do the following:

1. Select the Layout tab.

Startup in full screen Show table Startup in full screen Image: Sum / Op Window mode Queues Sum / Op Titles font size: 10 ÷ 10 ÷ Cell font size: 14 ÷ 14 ÷ Column titles height: 30 ÷ Row titles width: 130 ÷ Cell min width: 65 ÷ Cell max width: 0 ÷ O ÷ 70 ÷ Cell min height: 0 ÷ O ÷ 0 ÷ Cell min height: 0 ÷ O ÷ 0 ÷ Cell max height: 0 ÷ O ÷ 0 ÷ Cell max height: 0 ÷	M database ACS Queues O	Operators Layout Thresholds		
Startup in full screen Summary table Operators table Window mode Queues Sum / Op Titles font size: 10 ÷ 10 ÷ Cell font size: 14 ÷ 14 ÷ Column titles height: 30 ÷ 30 ÷ Row titles width: 130 ÷ 135 ÷ Cell min width: 65 ÷ 65 ÷ Cell min height: 0 ÷ 70 ÷ Cell min height: 0 ÷ 0 ÷ Cell min height: 0 ÷ 0 ÷ Cell min height: 0 ÷ 0 ÷			Show table	
Window modeQueuesSum / OpTitles font size: $10 \div 10 \div$ Cell font size: $14 \div 14 \div$ Column titles height: $30 \div 30 \div$ Column titles height: $10 \div 10 \div$ Cell min width: $65 \div 65 \div$ Cell min height: $0 \div 70 \div$ Cell min height: $0 \div 0 \div$	Startup in full screen		Summary table	Operators table
QueuesSum / OpQueuesQueuesSum / OpTitles font size: $10 \div 10 \div 10$ Titles font size: $12 \div 12$ Cell font size: $14 \div 14$ $14 \div 20$ Cell font size: $20 \div 20$ Column titles height: $30 \div 30$ 30 Column titles height: 40 Row titles width: $130 \div 135$ Row titles width: $160 \div 160$ Cell min width: $65 \div 65$ Cell min width: $75 \div 75$ Cell max width: 0 70 Cell min height: 0 Cell min height: 0 0 0 0 Cell max height: 0 0 0 0	Window mode		Full screen mode	
Index on size:I0Index on size:I2I2Cell font size:I4I4Cell font size:I2I2Column titles height:I14I4Cell font size:I2I2Column titles height:I10I14I4Cell font size:I12I2Column titles height:I14I14I4I4I4I4Row titles width:I130I135Column titles height:I40I40Cell min width:I130I135Cell min width:I60I160Cell max width:I0I70Cell max width:I0I100Cell max height:I10I100Cell min height:I10I100Cell max height:I10I100I100I100I100Cell max height:I10I100I100I100I100Cell max height:I10I100I100I100I100Cell max height:I10I100I100I100I100Cell max height:I10I100I100I100I100Cell max height:I10I100I100I100I100Cell max height:I10I100I100I100II00Cell max height:I10I100II00II00II00Cell max height:I10II00II00II00II00Cell max height:I100II00II00II00II00IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Titles font size	Queues Sum / Op	Titles font size:	Queues Sum / Op
Cell non size:141414Cell non size:202020Column titles height:30 30 30 135 Column titles height: 40 40 40 Row titles width:130 135 135 Column titles width: 160 160 160 Cell min width:65 65 65 Cell min width: 0 75 75 75 Cell max width:0 70 10 Cell min height: 0 100 100 Cell max height:0 0 0 10 100 100	Coll fast size:		Cell fest size:	12 ÷ 12 ÷
Column titles height: 30 ÷ 30 ÷ Column titles height: 40 ÷ 40 ÷ Row titles width: 130 ÷ 135 ÷ Row titles width: 160 ÷ 160 ÷ Cell min width: 65 ÷ 65 ÷ Cell min width: 75 ÷ 75 ÷ Cell max width: 0 ÷ 70 ÷ Cell min height: 0 ÷ 0 ÷ Cell min height: 0 ÷ 0 ÷ Cell min height: 0 ÷ 0 ÷ Cell max height: 0 ÷ 0 ÷ Cell max height: 0 ÷ 0 ÷	Cell Ioni Size.	14 🕂 14 🕂	Centionit size:	20 🛨 20 🛨
Row titles width: 130 ÷ 135 ÷ Row titles width: 160 ÷ 160 ÷ Cell min width: 65 ÷ 65 ÷ Cell min width: 75 ÷ 75 ÷ Cell max width: 0 ÷ 70 ÷ Cell max width: 0 ÷ 100 ÷ Cell min height: 0 ÷ 0 ÷ Cell min height: 0 ÷ 0 ÷ Cell max height: 0 ÷ 0 ÷ Cell max height: 0 ÷ 0 ÷	Column titles height:	30 🕂 30 🕂	Column titles height:	40 🛨 40 🛨
Cell min width: 65 65 Cell min width: 75 75 75 Cell max width: 0 70 Cell max width: 0 100	Row titles width:	130 🕂 135 🕂	Row titles width:	160 🛨 160 🛨
Cell max width: 0 70 Cell max width: 0 100 100 Cell min height: 0 0 0 Cell min height: 0 </td <td>Cell min width:</td> <td>65 🛨 65 🛨</td> <td>Cell min width:</td> <td>75 🛟 75 🛟</td>	Cell min width:	65 🛨 65 🛨	Cell min width:	75 🛟 75 🛟
Cell min height: 0 - Cell min height: 0 - 0 <t< td=""><td>Cell max width:</td><td>0 + 70 +</td><td>Cell max width:</td><td>0 ÷ 100 ÷</td></t<>	Cell max width:	0 + 70 +	Cell max width:	0 ÷ 100 ÷
Cell max height: 0 ÷ 0 ÷ Cell max height: 0 ÷ 0 ÷	Cell min height:		Cell min height:	
	Cell max height:		Cell max height:	

- 2. Enable the **Startup in full screen** option if you want the Wallboard application to start up in full screen mode. By default, the application starts in window mode.
- 3. In the Show table section, select one of the following options:
 - Summary table: the application displays a summary of all call traffic
 - Operators table: the application displays calls statistics by operator
- 4. Optionally, customize the display parameters for font size and cell width in the Window mode section (if the application runs in window mode) or the Full screen mode section (if the application runs in full screen mode):
 - Titles font size: font size of column headers and row headers.
 - Cell font size: font size of values in table cells.
 - Column titles height: fixed height (in pixels) of the top row containing all column headers.
 - Row titles width: fixed width (in pixels) of the left most column containing all row headers.
 - Cell min width: minimum dynamic width (in pixels) of cells. If set to 0, no restriction applies.

- Cell max width: maximum dynamic height (in pixels) of cells. If set to 0, no restriction applies.
- Cell min height: minimum dynamic height (in pixels) of cells. If set to 0, no restriction applies.
- Cell max height: maximum dynamic height (in pixels) of cells. If set to 0, no restriction applies.
- Titles font bold: enables or disables display of bold font style for column and row headers.
- 5. Click **OK** to apply your changes.

Configuring thresholds for alerts

You can configure the Wallboard application to alert the user when the values for waiting calls, average time in queue, or average handling time exceed defined thresholds.

There are two warning levels. If the first threshold is reached, the text flashes red. If the second level is reached the data for that parameter turns red and remains red until the value drops below the specified threshold.

To configure thresholds for Wallboard alerts, do the following:

1. Select the **Thresholds** tab.

Wallboard settings		
QM database ACS Queues Operators Lavout Thresholds		
Flashing Alert		
Calls waiting: 0		
Avg Q time (s): 20 50		
Avg handling time (s): 20 50		
	ок	Cancel

- 2. In the **Calls waiting** field, specify the threshold to trigger a flashing alert and the threshold to trigger a red text alert for the number of calls waiting to be answered.
- 3. In the **Avg Q time (s)** field, specify the threshold to trigger a flashing alert and the threshold to trigger a red data alert for the average time (in seconds) spent in a queue.
- 4. In the **Avg handling time (s)** field, specify the threshold to trigger a flashing alert and the threshold to trigger a red data alert for the average handling time (in seconds) for calls.
- 5. Click **OK** to apply your changes.

Additional configuration tools

The following configuration tools are also available if you want to make changes to your system configuration after initial installation and configuration:

- DAL configuration tool: used to verify/change parameters used by the Data Access Layer in BluStar • server.
- CMG configuration tool: used to verify/change InAttend parameters after initial setup.

DAL configuration tool

To review or change any of the Data Access Layer parameters in BluStar server, do the following:

1. Navigate to the BluStar Server folder (Start > Program Files > Mitel > BluStar Server) and double-click on the DALConfigurationTool.exe file.

The system opens the DAL Configuration tool.

2		[DAL Configuration		-)	¢
Fil	File ?							
	- Connection to DAL IP / Host Address Port	Service (necessary for Snapware Serve [INATTEND22 5071	er, PM Server, IPTSAPI Server, WebAdm Backup IP / Host Address Backup Port	iin (IIS))	Save	3		^
	Connection to Wet IP / Host Address Connection to SQL	Admin (necessary for Attendant client a	nd Attendant update service)		Save	•		=
	 Connection to SQL IP / Host Address User Password Database 	DB's (necessary for DAL Service, Webv . sa sa according Instance <\SQLEXPRESS> Test	Admin (IIS)) Backup IP / Host Address Backup User Backup Password Backup Database	xxxxxxxxx AastraConfig Instance <\SQLEXPRE Test	Save			=
	Version	8.0.0.0						~

- In the Connection to DAL Service section:
 - a. Update values for the following parameters:
 - IP / Host Address: address of the server where the Data Access Layer (DAL) service is installed.
 - Port: port number for the DAL server (default is 5071).

- **Backup IP / Host Address**: Address of the backup server where the Data Access Layer (DAL) service is installed (if available).
- Port: port number for the backup DAL server (default is 5071).
- b. Click Save to apply your changes.
 NOTE: The parameters in the Connection to WebAdmin section are not applicable for the InAttend installation.
- 3. In the Connection to SQL DB's section:
 - a. Update values for the following parameters:
 - IP / Host Address: address of the SQL server where the BluStar server database is installed.
 - User: name of the SQL user account with access to the BluStar server database.
 - Password: password for the SQL user account with access to the BluStar server database.
 - Database: name of the BluStar server database.
 - Instance <\SQLEXPRESS>: enable if you are using SQL Express.
 - **b.** Click **Test** to verify the connection to the SQL database.
 - **c.** Repeat steps (a) and (b) for the SQL server with the backup BluStar server database, if applicable.
 - d. Click Save to apply your changes.
- 4. Close the DAL Configuration tool.

CMG configuration tool

When you install InAttend, the information that you provide in the Quick Configuration Wizard is stored in the system. You can use the CMG configuration tool to verify or change your settings.

InAttend standalone deployment

To review or change any of the initial setup information provided during InAttend standalone setup, do the following:

 Navigate to the BluStar Server folder (Start > Program Files > Mitel > BluStar Server) and double-click on the CMGConfigTool.exe file.

The system opens the CMG configuration for WebAdmin tool.

X	CMG config	uration for WebAd	lmin 🔄	□ X
File ? Authentication mod BluStar / InAtte	e			<u> </u>
Connection to SQL IP / Host address User Password Database Test	DB INATTEND22 sa nice Instance <\SQLEXPRESS>	Connection to Web IP / Host address User Password	Admin INATTEND22 admin xxxxxx	
Web services Ana Service TCS User Manage TCS Configuration TCS Ncla Provider	r Manager		Save	

InAttend with CMG

To review or change any of the initial setup information provided during InAttend setup with CMG server, do the following:

1. Navigate to the BluStar Server folder (Start > Program Files > Mitel > BluStar Server) and double-click on the CMGConfigTool.exe file.

X		CMG configura	ation for WebAd	lmin	_ [×
File ?							
	Authentication mode	CMG database					^
Г	Connection to SQL DB		Connection to CMG	TCA			
	IP / Host address INATTEND22		IP / Host address	INATTEND22			
	User sa		User	niceadmin			
	Password XXXXXXX		Password	*****			
	Database nice						
	Test	EXPRESS>					=
Г	Web services						
	Ana Service					-	
	TCS User Manager						
	TCS Configuration Manager						
	TCS Nola Provider						
					Save		~

- 2. In the Authentication mode section, ensure that the BluStar / InAttend database option is selected.
- 3. In the **Connection to Connection to WebAdmin** section, update values to the following parameters to provide WebAdmin access to ACS configuration:
 - IP / Host Address: address of the server where TCA is installed (default is the server where ACS is installed).
 - User: name of the user account with permissions to log on to TCA (default is admin).
 - Password: password for the user account with permissions to log on to TCA (default is Mitel123).
- 4. Click Save to apply your changes.
- 5. In the Authentication mode section, ensure that the CMG database option is selected.
- 6. In the **Connection to SQL DB** section, update values to the following parameters to provide WebAdmin access to the CMG configuration:
 - IP / Host Address: address of the server where CMG is installed.
 - User: name of the SQL user account with access to the CMG server database.
 - Password: password for the SQL user account with access to the CMG server database.
 - Database: name of the CMG server database.

- Instance <\SQLEXPRESS>: enable if CMG is installed on a server with SQL Express
- 7. Click **Test** to verify the connection to the CMG database.
- 8. In the Connection to CMG TCA section, update values to the following parameters to provide WebAdmin access to ACS configuration:
 - IP / Host Address: address of the server where TCA is installed (default is the server where ACS is installed).
 - User: name of the user account with permissions to log on to TCA (default is niceadmin).
 - Password: password for the user account with permissions to log on to TCA (default is mitel).

NOTE: If WebAdmin cannot connect to TCA, the "CMG Operator Group" option will not be available in the WebAdmin Profile Group page

- **9.** In the **Web services** section, you can specify URLs to provide WebAdmin with access to InAttend web services:
 - AnA Service: http://<server>/nwana/anaservice.asmx
 - TCS User Manager: http://<server>/tcs/configurationmanager.asmx
 - TCS Configuration Manager: http://<server>/tcs/usermanager.asmx
 - TCS Ncla Provider: http://<server>/tcs/NclaProvider.asmx
- 10. Click Save to apply your changes.

Verifying your installation

You can validate the InAttend installation via the BluStar Server WebAdmin tool.

- 1. Access the BluStar Server Administration web interface by typing the URL: http://<hostname>/webadmin in a supported web browser, where <hostname> is the InAttend server address.
- 2. Log in with the administrator credentials.
- 3. Select Tools and then Service manager.
- 4. Verify that all of the relevant services to your InAttend installation are running properly.

InAttend system verification

The following verification steps are provided to assist you in ensuring that all required InAttend features are functioning properly.

General

Verify the following aspects of the InAttend system:

TASK	PASSE D	COMMENT
Verify that ELM license values are appropriate for your installation (e.g., languages for Speech, SA ports, InAttend users, etc.)		
If your solution supports visually impaired operators, ensure that the "Blind Support" option is enabled in the Attendant Layouts configuration profile (BluStar WebAdmin).		
Verify that all configured prompts are played (welcome, personal greeting, queue, Music on Hold, camp on busy, queue with message, etc.)		
Verify that there is enough memory for log files and attendant recordings.		

InAttend call handling

Verify speech path for all of the following call scenarios:

TASK	PASSED	COMMENT
Place an outgoing call		

TASK	PASSED	COMMENT
Answer an incoming call		
Blind transfer call (camp on)		
Call in A and consult call from B		
Call in A and consult call from B, toggle A and B		
Consult call from B with early transfer		
Consult call from B with transfer after answer		
Recall busy		
Recall no answer		
Blind transfer call to new queue		
Consult transfer call to new queue		
Transfer outgoing A and outgoing B		
Transfer to hunt group		
Direct drop from InAttend		
Park/retrieve call		
DTMF		
Mute call		
Call queue when all operators logged out		
Call recording		
Dialling settings (preview dialling, one-click dialling, or one-click and transfer)		
Intrusion (with forced release for MX-ONE)		
Automatic Call Distribution (ACD) or to all attendants		
Black listed – do not answer		
Select different calls from queues (not just first available)		
Perform a search in Quick Info via BSW and click-to-dial number		

Line state and activities/forward

Verify line state and forwarding information for each of the following use cases:
TASK	PASSED	COMMENT
Verify the line state on the extension		
Set an activity from InAttend		
Remove an activity from InAttend		
Repeat above for PN and IVR		
Set forward from InAttend		
Remove forward from InAttend		
Perform a large search and verify line state		
Perform an F10-key search and verify line state		
Verify CMG Web activities		

InAttend user interface

Verify the following functions on the InAttend user interface:

TASK	PASSED	COMMENT
Perform an F10-key search from InAttend, clear by pressing the Esc key		
Perform an F10-key search from InAttend, clear by pressing "x"		
Perform an F10-key search from InAttend, and scroll the results		
Perform a large search and scroll the search list		
Verify history information		
Verify InAttend activity information		
Verify queue timeout updates		
Verify language and time zone		
Send message and chat		

Quality Manager verification

Use the following procedures to verify proper installation and configuration of the Quality Manager component and the Quality Manager Wallboard application.

Verifying the Quality Manager installation

To verify the Quality Manager installation, do the following:

- 1. Open a browser and enter the URL for the Quality Manager Reports application (http://localhost/qm if you are navigating from the server where QM Reports is installed).
- 2. Log in with the user name "qmadmin" and password "mitel".
- 3. Generate a report (for example, **Traffic > Call Traffic**).
 - a. Select today as the time interval.
 - **b.** Select half-hour as the granularity.

The generated report contains a graph and a table with no data.

- 4. Make a call to an operator.
 - a. Make a call that is routed to the switchboard.
 - **b.** Answer the call in the InAttend client.
 - c. End the call.
- **5.** Regenerate the Quality Manager report with the same time interval and granularity. The generated report contains a graph and a table showing the answered call at the appropriate interval.

Verifying the Quality Manager Wallboard

To verify the Quality Manager Wallboard, do the following:

- Start the Quality Manager Wallboard application (Start > Programs > Mitel > Quality Manager Wallboard).
- 2. On an operator workstation, make a call to one of the queues monitored by the Wallboard.

The call appears in the "Calls waiting" cell of the queue. The operator log on.

Queues	Exter	nal .		Internal		Forward	Overflow
Calls waiting	0		1		1		0
Incoming calls	s 0			0		0	0
Answered call	s 0		0			0	0
Abandoned cal	ilis Q		0			Q	Q
Avg Q time	0:0	0	0:00		0:00 0:0		0:00
wa handling time 0:00		0	0:00			0.00	0.00
	-		_	0.00	_	0.00	0.00
	Summary	Direct	Forward	Recall	Total	Op. summary	
	Summary Incoming calls	Direct	Forward	Recall	Total Q	Op. summary	1
	Summary Incoming calls Answered calls	Direct 0 0	Forward O O	Recall 0	Total O O	Op. summary Logged on Calls waiking	1 1
	Summary Incoming calls Answered calls Abandoned calls	Direct O O O	Forward O O O	Recall O O	Total O O O	Op. summary Logged on Calls weiking	1
	Summary Incoming calls Answered calls Abandoned calls Avg Q time	Direct 0 0 0 0:00	Forward 0 0 0 0	Recall 0 0 0 0:00	Total 0 0 0 0:00	Op. summary Logged on Calls waiting	1 1

3. Answer the call and then hang up.

After a few seconds the data in the Summary view is displayed along with the following fields:

- Incoming calls
- Answered calls
- Avg Q time
- Avg handling time

	External		1	nternal		Forward	Overflow
Calls waiting	0			0		0	0
Incoming calls	g calls O			1		0	0
Answered calls	calls 0		1			0	0
Abandoned calls	0			0		0	0
Avg Q time	0:0	0		0:09		0:00	0:00
Avg handling tim	ne 0:0	0	0:05			0:00	0:00
	-				_		
Si	ummary coming calls	Direct	Forward	Recall 0	Total	Op. summary	1
51 10 An	ummary coming calls iswered calls	Direct 1 1	Forwerd O O	Recall O O	Total 1 1	Op. summary Logged on Calls waiting	1
St In An	ummary coming calls swered calls	Direct 1 1 0	Forward O O	Recall O O	Total 1 1 0	Op. summary Logged on Calls waiting	1 0
St In- An Ab	ummary coming calls swered calls andoned calls rg Q time	Direct 1 1 0 0:09	Forward 0 0 0 0:00	Recall 0 0 0 0 0:00	Total 1 1 0 0:09	Op. summary Logged on Calls waiting	1 0

NOTE: The **Op. summary table** includes the logged on operators as configured in the Wallboard settings dialog. If no operators have been configured to be displayed, the **Op. summary table** includes all logged on operators.

Logging

All components in CMG have log files for troubleshooting.

Make sure that enough hard drive space is available, as there is no size limiter (except for number of days) for the logging. This could, in extreme cases on servers with a small C: drive, fill up the hard drive. For example, the individual log files for CMG Web Service can reach 900 MB in size each.

It is recommended to have at least 50 GB available for log files.

Log Levels

The log levels are set in the Registry. The levels are from lowest level (Error) to highest (Debug). The higher log level the more information is written to the log file.

Log Level	REGISTRY Value	Description
Error	0	Error logs are written when errors occur.
Warnings	1	Warning logs are written when the system diverges from normal behaviour.
Info	2	Info logs are written for normal events in the system. This is the default log level for customer site installations.
Trace	3	Detailed logs but without extra data output needed for debugging.
Debug	4,5,6 or 7	The most detailed log level. Logs debug data.

Log Directory for each Component

This section describes where find the log files for each component.

On new installations, the default log directory starts with:

```
C:\ProgramData\Mitel\...C:\Program Files (x86)\Mitel\...
```

On upgraded system, the default log directory starts with:

```
C:\ProgramData\Aastra\...
```

```
C:\ProgramData\Netwise\...
```

```
C:\Program Files (x86)\Aastra\...
```

Default software

AnA Web Service

The default log directory for Ana Web:

```
Service:C:\nicesrv\log
```

BluStar License Manager

The default log directory for BluStar License Manager is:

C:\Program Files (x86)\Mitel\BluStarLicensemanager\

BluStar Server and BluStar Presence Server

The default log directory for BluStar Server is:

C:\Program Files (x86)\Mitel\BluStar Server\Trace

The default log directories for BluStar Presence Server are:

C:\Program Files (x86)\Mitel\BluStar Server\Trace\PresenceServer

CMG Web Service

The default log directory for CMG Web Service is:

C:\ProgramData\Mitel\CMGWeb.Service

Change of log level (1-7, default 3) for CMG Web Service:C:

\Program Files (x86)\Mitel\CMGWebService\CMGWebServiceConfig.xml

Enterprise License Manager (Server and Client)

The default log directory for ELM server and client is:C:

\Program Files (x86) \Mitel\License Manager\log

Mitel LDAP Server

The default log directory for Mitel LDAP Server:

C:\Program Files (x86)\Mitel\TSLDAP\log

InAttend Client

The default log directory for InAttend Client is:

C:\Program Files (x86)\Mitel\Attendant

InAttend History Service

InAttend Quick Configuration Service

InAttend Quick Configuration Web

Media Server

The default log directory for Media Server is:

C:\Program Files (x86)\Mitel\MediaServer\Logs

Network Telephony Services (NeTS)

The default log directory for Network Telephony Services (NeTS) is:

C:\Program Files (x86)\Mitel\TelephonyServices\Logs\NeTS

Queue Manager

The default log directory for Queue Manager is:C:

\Program Files (x86)\Mitel\QueueManager\Logs\QueueManager

Telephony Configuration Manager

The default log directory for Telephony Configuration Application is:

C:\ProgramData\Mitel\Logs

Optional Server Software

Quality Manager Database - C:\Program Files (x86)\Mitel\QualityManager\Logs Quality Manager Service- C:\Program Files (x86)\Mitel\QualityManager\Logs Quality Manager Reports Web - C:\temp\logs Mobile Status Connection - C:\temp\MSCLogs ACS Cisco Line State Server- C:\ProgramData\Mitel\AcsCiscoLSS

Optional Client Software

Quality Manager Wallboard

References

[1]Mitel Installer Overview
[2]InAttend User Guide (installed with InAttend Client software)
[3]InAttend System Overview
[4]InAttend Installation Preparation Guide
[5]InAttend Compatibility Matrix (Note: available on InfoChannel)
[6]InAttend Datasheet (Note: available on InfoChannel)
[7]Enterprise License Manager Technical Guide
[8]BluStar Server Installation and Configuration Guide
[9]Mobile Status Connection Installation and Maintenance Guide
[10]CMG Configuration Guide (Note: available in BSW CPI)
[11]Certificate Management Operational Directions (available in MX-ONE CPI)
[12]VoIP Security Operational Directions (Note: available in MX-ONE CPI)

Appendix A: Configuring telephony services in TCA

The Telephony Configuration Application (TCA) is a web-based application used to configure the Telephony Server system. TCA provides template configurations that you can use to simplify configuration.

TCA configuration has two levels:

- · Main level: contains common and shared resources like hosts and subsystems.
- Site level: contains customer-specific information such as call manager environment, device ranges (number plan), queues and operator groups.

This section provides an example of how to create one site including two hosts: a call manager (MX-ONE) and the InAttend server (ACS).

NOTE: The host and network names have to be true DNS names, and the IP address has to exist in the network.

Telephony services configuration sequence

The main tasks for configuration of the InAttend telephony server in TCA are as follows:

- **1.** Create the main TCA configuration file.
- 2. Create hosts for the call manager and for the ACS.
- 3. Add a site to contain customer-specific configuration (e.g., queues, operator groups, etc).
 - a. Create a network
 - b. Add a PBX.
 - c. Add a domain and configure the domain with the PBX.
- 4. Configure subsystems (Line State Server, Queue Manager, Media server).
- 5. Configure queues.
- 6. Create an operator group and associate the group to a queue.
- 7. Deploy the configuration.

You can access the TCA tool from a supported browser (for example, Internet Explorer or Edge Chromium), using the following address: http://<TCA web server>/TCA (where <TCA web server> is the InAttend server address).

A TCA configuration file is a database using an XML document that defines the system configuration. This file contains configurations for all call manager components. TCA supports multiple configurations, but since one configuration file contains information for the entire InAttend system, only one configuration file is typically used.

When creating a configuration, it is recommended that you use one of the predefined configuration templates. When you use a predefined template, the system automatically creates the required components for your configuration. You only need to customize the components with your specific configuration.

For example, when you use the pre-defined InAttend MX-ONE SIP Template, the following components are automatically created in TCA:

TCA Main Configuration: MX-ONE SIP Template

Telephony Configuration Application	Sites	
 InAttend Sample Hosts Public Networks Hosted Private Networks Subsystems Linestate Servers LSS1 LSS2 Queue Managers QueueManager 1 NeTSs ACSSERVER1 ACSSERVER2 Media Server1 Media Server2 Sites 	The list presents all sites in the configuration. Click on New to create a new site. To endivise the site, click on the site name To rename a site click on the pen icon. A site can only be deleted if it does not contain any items. To delete a site click on the trash bin to the right. Name Site1 1 New	
	Working with: InAttend Sample Last deployed (UTC): Never deployed Deploy Lo	gout

TCA Site Configuration: MX-ONE SIP Template

Telephony Configuration Application	Site1 Click on any item in the treeview on left hand
Site 1	Click on any item in the treeview on left hand side to create a new element in the site.
	Working with: InAttend Sample Last deployed (UTC): Never deployed Deploy

Create a TCA configuration

The configuration example described in the following sections uses the Empty Template, to describe creation and configuration of all required components.

To create a new TCA configuration, do the following:

- 1. Open a browser and log in to the TCA tool ().
- 2. On the Configurations page, click on the icon beside the Empty Template.

Telephony Configuration Application	Configurations			
No configuration loaded	Configurations Click on the configuration name symbol to the right. The chose configuration, dick on the track source link and choosing 'Save	e to work with the con n configuration will be bin to the right of th Target As" in the p	figuration. To create a new configuration click on t the template for the new configuration. To delete e configuration. Dewnload a file by right clicking e popup menu.	he "new" a n the
	Configuration name		Last deployed	
	Ben template	(source)	1/21/2015 9:03:01 AM	🔳 🔬
	InAttend Sample	(source)		i 🌛
	To create a new configuration f Template name	rom the template clic	k on the "new" symbol to the right. Description CMGVala Without CTC - Tamplate	
	CMBVoice without CTC - Temp	ale	Chovoice without Circ - remplate	
	CUCM SIR Template		CUCM SIR Template	5
	CUCM SIP Template Empty Template		CUCM SIP Template Empty Template	<u> </u>
	CUCM SIP Template Empty Template InAttend CUCM SIP Template		CUCM SIP Template Empty Template InAttend CUCM SIP Template	Q Q
	CUCM SIP Template Empty Template InAttend CUCM SIP Template InAttend MX-ONE SIP Template	2	CUCM SIP Template Empty Template InAttend CUCM SIP Template InAttend MX-ONE SIP Template	* * 2
	CUCM SIP Template Empty Template InAttend CUCM SIP Template InAttend MX-ONE SIP Template Single ACS Template	ē	CUCM SIP Template Empty Template InAttend CUCM SIP Template InAttend MX-ONE SIP Template Single ACS Template	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	CUCM SIP Template Empty Template InAttend CUCM SIP Template InAttend MX-ONE SIP Template Single ACS Template Single CTC Template	2	CUCM SIP Template Empty Template InAttend CUCM SIP Template InAttend MX-ONE SIP Template Single ACS Template Single CTC Template	
	CUCM SIP Template Empty Template InAttend CUCM SIP Template InAttend MX-ONE SIP Template Single ACS Template Single CTC Template Single CTC With Queue Messa	e ges - Template	CUCM SIP Template Empty Template INAttend CUCM SIP Template INAttend MX-ONE SIP Template Single ACS Template Single CTC Template Single CTC Template	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	CUCM SIP Template Empty Template InAttend CUCM SIP Template InAttend MX-ONE SIP Template Single ACS Template Single CTC Template Single CTC With Queue Messa	e ges - Template	CUCM SIP Template Empty Template InAttend CUCM SIP Template InAttend MX-ONE SIP Template Single ACS Template Single CTC Template Single CTC With Queue Messages - Template	6 6 6 6 6 7 6 7 6 7 7 0

3. Enter a name for the configuration and click Create.

TCA displays the Configuration overview page.

Telephony Configuration	Configuration overview:
Application	
	Information about current configuration:
<mark>-</mark> • New Sample Config	Configuration: New Sample Config
Hosts	Last deployed: Never deployed
Public Networks	Last deployed info:
Hosted Private Networks	
Subsystems	Show deployment info
Sites	
	Documentation:
	Show System overview
	Show TSP configuration
	Show CUCM configuration
	Other tasks:
	Load another configuration
	Working with: New Sample Config Last deployed (UTC): Never deployed Deploy Logout

Configure the call manager and ACS hosts

You need two hosts defined in your telephony server configuration: one host for the call manager and one host for ACS.

- 1. First, create the ACS host. In the left panel of the TCA interface, click on Hosts. TCA displays the Hosts page in the main window.
- 2. Click on the New button to create a new host.

Telephony Configuration Application	Hosts	-			
⊡- New Sample Config Hosts Public Networks	The list presents all host Click on New to create Click on the edit icon to To delete a host click on	s. a new host. change a host the trash bin	t's properties. to the right.		
- Hosted Private Networks - Subsystems - Sites	Host name	IP	Network name	Description	Ne v

- 3. In the New Host window, specify values for the following fields:
 - Host name: the hostname (known in the network) of the server. The host name is used by software to identify the machine on which it is running.
 - **IP address**: the IP address of the server. This field is optional when network name is specified and DNS-SRV lookup is used.

Network name: The network name is used by software connecting to the specified machine (i.e., have to be routable from the network). Use the IP address if the name is not routable. The network name has to be a host FQDN. This field is mandatory when DNS-SRV lookup is used.

If only when no IP address is specified, then NeTS does DNS SRV lookup on the specified "networkName".

If IP address is specified for HOST, then that shall be used.

- Description: some descriptive information for the host.

NOTE: IP address, Host name and Network name are the fields that are used when contacting a specified host (through IP address or DNS lookup).

10.211.63	3.76/tca/host/host	editpopup.asp	x?id=1	
Edit host				
Host name	MX171	×	1	
IP address	10.211.63.140			
Network name	mx171.inattendbgl.co	m		
Description	PBX			
Note! Host name	, Ip address and Netw the configuration to wo	ork name must e	xist on the	

- 4. Click Create to save your changes.
- 5. Repeat steps 2 to 4 to create the call manager host (with the appropriate parameter values for the call manager). The system displays the new hosts on the Hosts page

Telephony Configuration Application	Но	sts				
B - SimpleConfig Hosts	The I Click Click To de	ist presents all ho on New to creat on the edit icon t lete a host click o	osts. Ite a new host. Ito change a host's prop on the trash bin to the	erties. right.		
Public networks		Host name	IP	Network name	Description	
Hosted Private Networks	1	IA26M	10.211.63.76	IA26M	Attendant Call Server	
Subsystems Sites	1	MX171	10.211.63.140	mx171.inattendbgl.com	PBX [New

Add a site

The site configuration contains customer-specific information such as call manager environment, device ranges (number plan), queues and operator groups. There has to be at least one site in the configuration.

- 1. In the left panel of the TCA interface, click on Sites.TCA displays the Sites page in the main window.
- 2. Click on the New button to create a new site.



3. In the New site dialog, enter a name for the site and click Create.



TCA creates the new site and displays the new site on the Sites page.

Telephony Configuration Application	Sites
 □-InAttend Sample … Hosts … Public Networks … Hosted Private Networks ④-Subsystems … Sites 	The list presents all sites in the configuration. Click on New to create a new site. To edit/view the site, click on the site name To rename a site click on the pen icon. A site can only be deleted if it does not contain any items. To delete a site click on the trash bin to the right. Name Site 1 1 New

Configure a network for the site

You create a network for your site and add a PBX. A network can continue one or more call managers. In this example, there is one call manager.

- 1. Click on the site entry to open the site configuration. TCA opens the Site page in a new window.
- 2. On the Site page, click on **Private Networks** in the left panel to display the Private Networks page in the main window.
- 3. Click the **New** button to create a network.

Telephony Configuration Application	Private Networks
Site 1	The list presents all private networks in the site. Click on the trash bin to the right to delete a network or New to create a new network.
 □- Site: Site 1 □ Private Networks □ Public Queues □ Operator Groups □ Voice Systems 	Click on the network name to rename a network. Name

4. In the **New network** dialog, enter a name for the network and click **Create**.

CHAPTER 22



TCA creates the network component and displays the network on the Private Networks page.

Telephony Configuration	Private Networks
Site 1	The list presents all private networks in the site. Click on the trash bin to the right to delete a network or New to create a new network.
⊡-Site: Site 1	Click on the network name to rename a network.
Private Networks Public Queues Operator Groups	Name
Voice Systems	Ne w

Add a PBX to the network and configure a SIP port

Do the following:

1. Expand the Private Networks component in the left panel and click on the entry for the display the network you just created.

TCA displays the new network in the main window.

2. Click the **New** button to add a PBX (call manager) to the network.

Telephony Configuration Application	My Network		
Site 1	The list presents all PBXs in Click on the trash bin to the or <i>New</i> to create a new PB Click on the PBX name to re	n the selected private network. a right to delete a PBX IX. ename it.	
Private Networks	Name	Туре	
			New

- 3. In the Create new PBX window, specify values for the following fields:
 - Select PBX type: select Generic PBX or CUCM (for Cisco call managers only).
 - Name: the name of the call manager.
 - Type: the type of call manager (e.g., MX-ONE).
- 4. In the SIP Port section, click New to add a SIP port.
 - a. In the New SIP port window, specify values for the following fields:
 - Name: name of the SIP port.

- **Description**: optional additional information.
- Host: select the host you created for the call manager from the list.
- **Port**: keep the default value of 5060. SIP normally uses default port 5060 for UDP/TCP and 5061 for TLS. For Skype, however, port 5068 is used for UDP/TCP and 5067 for TLS.
- **Protocol**: select the appropriate protocol from the list.
- Use Trombone transfer: enable or disable this option.

Trombone transfer is enabled for certain call managers (e.g., Skype and CUCM) but is disabled for MX-ONE. If trombone transfer is enabled (True), the NeTS process will act as a B2BUA (Back To Back User Agent) and keep control of all legs of the complete call session.

b. Click Create to add the SIP Port.

The new port appears in the SIP port list.

5. Click Create to create the PBX.

NOTE: If you configure NeTS to use TLS in the NeTS configuration tool, NeTS opens port 'n+1' for communication although 'n' is the port configured in TCA as the PBX SIP port

Add a domain to the PBX

Do the following:

- 1. Expand the Private Networks component in the left panel to display the new network and the new call manager.
- 2. Click **Domains** to display domain information for the call manager in the main window.
- 3. Click the **New** button to create a new domain for the call manager.



- 4. In the **New** domain window, specify values for the following fields:
 - Name: name of the domain.
 - PBX ID: ID of the call manager you created earlier (TCA uses this ID to map between the call
 manager and the domains in TCA).
 - Internal prefix: internal prefix to be used (if configured for the call manager)
 - CMG View: name of the CMG view that is used if using several customer groups in CMG (the CMG view defines what the operator sees in the Search view.)
 - **SIP domain**: DNS domain in To/From-headers if required by the call manager. Otherwise the hostname or IP address of NeTS computer is used.
 - SIP domain description: optional information for SIP domain.

- **Phone context**: phone-context=xxx in the sip URI if required or used by the call manager. Also used to map incoming calls to a TCA domain.
- Autogenerate *23: Enable or disable option to generate an absent code for CUCM call manager. Enable for Cisco call managers only.
- 5. Click **Create** to create the domain.

Configure the new domain

After you have created the domain, you can add device ranges and assign a SIP port.

- 1. Expand the **Private Networks** component in the left panel to display the new domain you created under the call manager.
- 2. Click on the entry for the new domain to display the Domain page in the main window.

The device ranges associated to the domain are listed on the Domain page. There are two types of device ranges: application number (used for queues) and phone (configured for routing issues).

3. In the Device Ranges section, click on the **New** button to add a device range.

Telephony Configuration Application	My Network	- MX-()NE - Domain	s-Doma	ain 1		
ite1	Settings						
	PBX Id		1				
Site: Site1	Default internal	prefix 🖪					
- Private Networks	CMG View						
• My Network	SIP Domain						
MX-ONE	SIP Domain Des	cription					
- Domains	Phone context						
Domain 1	Create *23-num	bers	,				
Public Queues					Update		
+Operator Groups							
Voice Systems	Ports						
	Name	Туре	Host name	Port	Protocol	Description	
	Media servers	5.6					
	Name					Order	
	MediaServer1					1	
	MediaServer2					2	
	- Add						
	Device ranges						
	Descriptio	n		Ra	ange	Туре	
	🥜 Office pho	nes		20	00 - 9999	Phone	
	🥒 Operators	and CMG	Speech	10	000 - 1999	Application number	

- 4. In the New device range window, specify values for the following fields:
 - **Type**: the device range type; select Phone.
 - Description: optional information to describe the device type (e.g., "Office phones").
 - Internal prefix: leave blank.
 - Range: specify the number range for all devices configured on the PBX (e.g., 12000 to 15999).
- 5. Click **Create** to add the device range.
- 6. Click **New** in the Device Ranges section again to configure the attendant number.

- 7. In the **New device range** window, specify values for the following fields:
 - Type: the device range type; select Application Number.
 - Description: optional information to describe the device type (e.g., "Attendant").
 - Internal prefix: leave blank.

NOTE: This is the internal prefix of the domain if a partitioned CUCM is used. While creating any device range for E.164 number, you must enter the prefix in Internal Prefix area and provide the number range without any prefix.

- Range: specify the number range (e.g., 09 to 09).
- 8. Click Create to add the device range.

The new device ranges are now displayed in the domain Device ranges list.

Devi	ice ranges			
	Description	Range	Туре	
1	Office Phones	12000 - 15999	Phone	Ť.
2	Attendant	09	Application number	Ť
				New

9. In the Ports section, assign the SIP port you created on the PBX to the new domain. Select it from the pull-down menu and click Add.

Ports					
Name	Туре	Host name	Port	Protocol	Description
SIP port 1 (si	p) on MX-ON	IE port: 5060 protoco	I: TCP 🗸 Add		

10. Click **Close** to complete the site configuration.

Add a Line State Server

Add a LineState Server to monitor the line state of the devices configured in the site.

- 1. Click on **Subsystems** in the left panel of the TCA interface to display the Subsystems page in the main window.
- 2. Click the New button beside the Linestate Servers entry to add a line state server.

Telephony Configuration	Subsystems	
Аррисации	Click on "Nev" to create a ne	welement in the site.
New Sample Config	Subsystem Summary	
Public Networks	Linestate Servers Queue Managers	0 New
Subsystems	NeTSs	0 Ne vr
Sites	PBXSTDs	
	Media Servers	0 Nev

- 3. In the New Linestate Server window, specify values for the following fields:
 - Name: name of the Linestate Server (e.g., LSS1).
 - Host: select the call manager host you configured earlier from the list.

- Port: for MX-ONE, enter 5077. This is the socket TCP port used by the Linestate Server to listen for incoming connection requests from the call manager.
- Domains to service: specify the domains to monitor. Click the Add button and in the LSS domain to monitor window, select the PBX and the device ranges you configured earlier. These are the domains and phone ranges that the LineState Server monitors for line sate requests.
- 4. Click **Create** to add the Linestate Server.

Add a Queue Manager

Do the following:

- 1. Click on **Subsystems** in the left panel of the TCA interface to display the Subsystems page in the main window.
- 2. Click the New button beside the Queue Managers entry to add a queue manager.
- 3. In the New Queue Manager Cluster window, specify values for the following fields:
 - Name: name of the Queue Manager.
 - NeTS / NQM host: select the ACS host you configured earlier from the list.
 - Secondary NeTS / NQM host: specify only if you configured a secondary ACS host.
 - Attendant client port: keep the default value of 4812. This is the socket TCP port used by Queue Manager to listen for incoming InAttend client connections.
 - Quality Manager Port: keep the default value of 4813. This is the port used by Quality Manager (optional InAttend application).
- 4. Click Create to add the Queue Manager.

The system displays the new Queue Manager subsystem in the left panel.

- 5. Click on the new Queue Manager entry in the left panel to display the Queue Manager Cluster page in the main window.
- 6. In the Use LSS section, specify the Linestate Server that the Queue Manager uses to obtain line state information from the call manager. Select the Linestate Server you created earlier from the pull-down list and click **Add**.

Queue Manager Clus	ter - Queue Manager 1
Settings	
Primary NeTS / NQM host	ACS (ACS host)
Secondary NeTS / NQM host	No secondary host
Attendant client port	4812
QualityManager port	4813
	Update
Use LSS Host	
Serviced domains	
Domain	
	Domain 1 🗸 Add 📔

7. In the Service domains section, specify the domain you created earlier from the pull-down list and click **Add**. (This is the domain that the cluster supports in terms of, for example, *23 services).

CHAPTER 22

Queue Manager Clus	ter - Queue Manager 1
Settings	
Primary NeTS / NQM host	ACS (ACS host)
Secondary NeTS / NQM host	No secondary host
Attendant client port	4812
QualityManager port	4813
	Update
Use LSS	
Host	
	LSS 1 Add
Serviced domains	
Domain	
	Domain 1 🔽 Add 🖪

8. Click Update to save your changes to the Queue Manager.

Configure the NeTS host

When you create the Queue Manager component, the system automatically creates a NeTS component for the ACS host you specify in the Queue Manager Config.You have to perform additional configuration to enable the NeTS component.

- Expand the NeTS component in the left panel to display the NeTS host created for the Queue Manager.
- 2. Click on the entry for the new NeTS host to display the NeTS host page in the main window.
- 3. In the SIP Ports section, click on the New button to add a SIP port.
- 4. In the New SIP port window, specify values for the following fields:
 - Name: specify a name for the SIP port.
 - Description: optional additional information for the SIP port.
 - Port: keep the default of 5060.

(This is the SIP port on the NeTS side, not the call manager).

5. Click **Create** to save your changes.

Create a media server and add it to the site

You have to define a media server for your InAttend configuration.

- 1. Click on **Subsystems** in the left panel of the TCA interface to display the Subsystems page in the main window.
- 2. Click the New button beside the Media Servers entry to add a line media server.
- 3. In the New Media Server window, specify values for the following fields:
 - Name: specify a name for the media server.
 - Host: select the ACS host where the media server resides from the pull-down list.
 - Port: keep the default of 5065.
- 4. Click Create to save your changes.
- 5. You have to add the new Media Server to your site.

Click on **Sites** in the left panel of the TCA interface and in the main window, select the site you created earlier.

- 6. On the Site page, expand the Site component to display the network and domain sub-components.
- 7. Click on the domain that you created earlier to display the Domain page in the main window.
- 8. In the Media servers section, select the media server you created earlier and click **Add** to add the server to your domain.

Media servers		
Name	Order	
MS1	1	
Add		

Create a queue for the site

You configure queues for incoming calls and add them to operator groups. A queue can be configured for handling by any operator group. Each queue can have one or more queue entries.

There has to be at least one external queue. Normally, internal queues are pre-defined.

- 1. On the Site page, click **Public Queues** in the left panel to display the Public Queues page in the main window.
- 2. On the Public Queues page, click **New** to create a new queue.
- 3. In the New Queue window, enter values for the following fields:
 - a. Settings section:
 - Name: name for the queue (displayed in the InAttend client).
 - Queue Manager Cluster: select the Queue Manager cluster that you created earlier.
 - Default prio: default priority. Queues are prioritized in the InAttend client from left to right. A higher number indicates higher priority.

NOTE: If the created queue should be used as a Public Parking Queue then you must set the prio to 0, if the prio is not set to 0 the queue will not work as a parking queue.

- **Max size**: length of the queue (i.e., the maximum number of callers that the queue can handle at a given time). When the maximum queue size is reached the overflow behaviour configured on the queue entry is triggered.
- Wait time 1st alert (s): the interval (in seconds) after which the first alert is sent to the attendants to alert them that a call has not been answered. The queue display turns orange and an orange dot appears beside the call entry in the InAttend client.
- Wait time 2nd alert (s): the interval (in seconds) after which the second alert is sent to the attendants to alert them that a call has not been answered. The queue display turns red and a red dot appears beside the call entry in the InAttend client.

b. Default Queue Entry Settings section:

- Active: the time interval for when the queue is active. When the queue is not active, all calls are redirected to the passive redirect queue/address.
- **Passive redirect**: the queue or number that calls are redirected to if no attendant is handling this queue (that is, no attendant on duty has this queue in their InAttend client configuration).

NOTE: The passive redirect destination must have a good capacity in accepting and handling calls. It should not respond busy. In the case of Mx-One, the destination can be a hunt-group.

- Overflow: the queue or number that calls are redirected to if the queue is full.
- 4. Click **Create** to save your changes.

Create an operator group and assign it to a queue

You should create an operator group for InAttend users and assign the operator group to the site's queue.

- 1. Click on **Operator Groups** in the left panel of the TCA interface to display the Operator Groups page in the main window.
- 2. Click the **New** button to add an operator group.
- 3. In the New Operator Group window, enter values for the following fields:
 - a. Settings section:
 - **Name**: name for the operator group.
 - Queue Manager Cluster: select the Queue Manager cluster that the InAttend client connects to.
 - ACD: enable or disable Automatic Call Distribution. If enabled, enter a value for answer timeout (s) (i.e., the number of seconds until an attendant in the group is black-listed due to inactivity. A blacklisted attendant has to manually log in again in order to receive calls)
 - Solidus eCare: enable if the operator group is dedicated to the Attendant Agent solution.
 - **None**: when selected, call to this operator group are presented to all operators in the group.
 - Intrusion allowed: enable to use the MX-ONE intrusion feature.
 - **Initialize timeout (s)**: the interval (in seconds) that the InAttend client waits for the Queue Manager to initialize; otherwise the client assumes an error.
 - **Connect timeout (s)**: the interval (in seconds) that the TCP socket connection waits before assuming an error.
 - Enable Conference Tone: enable this to play a conference tone on entry or exit of a caller in 3-party conference (caller A, B, and attendant) for the following scenarios.

Attendant enters a 3-way call (talking to A and B at the same time)

Operator dropping call on B-panel

User A leaving the conference

User B leaving the conference

• **Recording Prompt**: plays a prompt to the caller or called (external party) indicating that the call is being recorded. If it is not configured, that is, if the option is left blank, no prompt is played but the call may be recorded.

The call can be recorded on demand or by default all calls are recorded. This prompt is configured based on operator group from TCA.

NOTE: This feature is not for creating ad hoc conferences for people.

For upgraded clients the shortcut key must be configured manually in the InAttend Options dialog. For new installations, the shortcut key is pre-defined.

Conference tone will play only if it configured in TCA.

• Clerical time (s): Specify the time (in seconds) for an operator group to perform clerical work.

b. Use LSS section:

Select a linestate server from the pull-down list and click Add.

- **c.** Camp on section:
 - i. **Recall no answer timeout (s)**: the interval (in seconds) before calls transferred to internal or external extensions are sent back to the attendant after no answer. Default for internal is 30.

Default for external is 30.

NOTE: The timeout value is selected on whether the target is internal/external.

- **ii. Recall busy timeout (s)**: the interval (in seconds) before a transferred call is sent back to the attendant when the user is busy (default is 20).
- iii. **Recalls from Consult Calls**: enable or disable. Determines whether calls are sent back to the attendant in case of no answer on a consult call.
- iv. **Behaviour**: Select the application to run when a call enters a "camp on queue" (e.g., Music on Hold, to play music while the caller waits for the target extension or attendant to answer).
- d. Click Create to save your changes.

NOTE: The system creates two private queues when the Operator Group is created: a queue for Recall and a queue for Park. You can change these on the Queue Settings page.

- 4. Expand the **Operator Groups** component in the left panel to display the new operator group.
- 5. Click on **Queues** (under the new operator group) to display the Queues page for the operator group in the main window.
- 6. In the Displayed queues section, select the queue you create earlier from the pull-down list and click **Add**.

Displayed queues			
Name	Prio	Туре	
Park	<u>0</u>	private	
Recall	20	private	
Queue MX-ONE	<u>5</u>	public	*
			Add 1

NOTE: If you make any change in Operator Groups, restart the InAttend Client.

Configuring public recall queues

To assign a public recall queue, a Public Queue is added under "Public Queues" first.

NOTE: It is not allowed to use a "public operator queue" i.e. reached by an access number as a public recall and/or park queue.

For example: If we want to create a new queue – Uma_Bhat, follow the below steps:

- 1. Go to Public Queues.
- 2. Select New Queue.
- 3. Enter a desired **Name** for the new queue.
- 4. The values for Queue manager cluster, Default prio, Max size, Wait time 1st alert, Wait time 2nd alert, and Queue NoAnswer Time is taken by default.
- 5. Click Create.

CONFIGURING PUBLIC RECALL QUEUES APPENDIX A: CONFIGURING TELEPHONY SERVICES IN TCA

Tolophony Configuration	Public Queues	New Oueue Web	page Dialog	×
Application		Attp://10.10.144.4	8/tca/site/queuenewiframe.htm	
My_Site	The list presents all public q Click on the trash bin to the	New Queue		
Site: My_Site Private Networks InternalExternalISDNShankar_QOperator GroupsVoice Systems	or New to create a new qu Click on the queue name to Name External Internal ISDN Shankar_Q	New Quere Settings Name Queue Manager Clust Default prio Max size Wait time 1st alert (s Wait time 2nd alert (s Queue NoAnswer Tim	er Uma_Bhat × My_QueueManager × 5 100) 10 s) 30 le (s) 60	
		Default Queue Entr Only used when creat Passive redirect Closed redirect	y Settings ing new queue entries. No passive redirect Queue Internal V Number Number No closed redirect Queue Internal V	
		Overflow Overflow No Answer	Number No overflow Queue Internal Number No overflow Queue Internal V	
			O Number Create C	ancel

A New Queue – Uma_Bhat is created. This queue does not have an access number.

Site	Settings				
	Queue Manager Cluster	My_QueueManager 🗸			
Site: My_Site	Default prio	5			
Private Networks	Max size	100			
- Public Queues	Wait time 1st alert (s)	10			
Internal	Wait time 2nd alert (s)	30			
External	Queue NoAnswer Time (s)	60			
Kumar_Queue	Default Queue Entry Sett	ings			
Uma Bhat	Passive redirect	No passive redirect	O Queue	Internal (My_Site)	✓ ○ Number
Operator Groups	Closed redirect	• No closed redirect	O Queue	Internal (My_Site)	✓ ○ Number
- MX1_Operators	Overflow	No overflow	O Queue	Internal (My_Site)	V O Number
Queues	Overflow No Answer	No overflow Answer	🔿 Queue	Internal (My_Site)	V O Number
E CUCM_Operators					Upda
Queues	Queue Entries				
Voice Systems	Domain Description	Access number	Active	Overflow Passive	e Closed Behavior
	•				

Queue entry without an access number

The Call queues are Private by default under the Recall and Park.

Function	Used queue
Recall - Busy For Internal Calls	Recall (private)
Recall - Busy For External Calls	Recall (private)
Recall - No Answer For Internal Calls	Recall (private)
Recall - No Answer For External Calls	Recall (private)

Park		
Function	Used queue	
🍠 Park Queue	Park (private)	

To change a private queue to a public queue, follow the steps.

- a. Go to Operator Groups.
- b. Select CUCM Operators.
- **c.** In the **Recall** section, click the pencil icon to access the Queue Settings > Private queue (to be changed to public).
- d. Go to Queue Settings.

Queue settings Webpage Dialog	
http://10.10.144.63/tca/site/operatorgrouprecallsettingsiframe.asp	px?i=busyInt&functionNam
 http://10.10.144.63/tca/site/operatorgrouprecallsettingsiframe.asp Queue settings: Recall - Busy For Internal Calls Choosing private queue will return calls to the same attendant that precedence settings to public queues are possible. Choosing public queue will allow all attendands in the same operator gr calls. Other attendants may also answer the call if the same queue is ad groups. Private Public Choose from existing Public Queue Internal (My_Site) Kumar_Queue (My_Site) CuCM_Queue (My_Site) Uma_Bhat (My_Site) 	ox?i=busyInt&functionNam viously handled the call. oup to answer returned ded to other operator
Kumar_Queue (My_Site) CUCM_Queue (My_Site) Uma_Bhat (My_Site)	Ok Cancel

- e. The Queue Settings Recall Busy for Internal Callswindow is displayed.
- f. 2 radio buttons for Public and Private are displayed.
- g. Choose the queue (Uma_Bhat) to be changed to public.
- h. Select Public.
- i. Click Ok.

The private queue Uma_Bhat is changed to public queue.

Private Queue Number for Individual Attendants

The administrator can define a private queue for an operator group. The administrator can also define the queue access number or the number range for the private queue similar to public queues.

The attendant is responsible to maintain unique number for each attendant. **NOTE:** The route for private queue access number is created by the call manager to ACS.

Ð	View site My_Site Webpage Dialog	×
	Type of Season 0 Toole Type of Season Toole Toolse that applicable while configuring with our Softwater thread (s) Chinals thread (s) China	
	Use LSS	ь
	Head Visiosistop V	I
	Camp an Rectal no Answer filmsbut Internal 20 external 20 (2) Rectal bury timesul (2) Rectal from Cansult Call	
	Behavior Music on hold Settings	U
	Table Contraction of the Contrac	
	Function Used assess	
	Facult - Barry for Internal Calls Anall Introduct Anall - Barry for Internal Calls Anall - Barry for Internal Calls Anall - Barry for Internal Calls Anall Introduct Anall - Barry for Internal Calls Anall Introduct	
	Purch Function: Vocal queues I Park Queue : Rath_Instants)	
	Princeto Queene	
	Pro-Asing Sample-Config Last displayed (Server Ince) 2017-02-22 Display Config Last displayed (Server Ince) 01:02:53 Display Config].

Private Queue before creation

Entropies Allowed Internet Sector Sec	
L	Update
Use USS	
vsoeskrop	
Camp an Recall for answer timeson Recall for answer timeson Recall form Corevel Recalls from Corevel Construction	
Bahavor Null not	Update
Recal	
Function Used guess	
Facult - Barry For Internal Cafe Facult Jonata Facult - Barry For Internal Cafe Facult - Internal Cafe	
Park Function Used genese Park Queue Each Laterates	
Princete Queues Balana Princete Queues Balana Princeteon Princete Queues Big	Updata

Private Queue after creation

CHAPTER 22

	View site My_Site Webpage Dialog	
New Private Queue		
Settings		
Name		
Queue Manager Cluster	My_QueueManager V	
Default prio	5	
Max size	5	
Wait time 1st alert (s)	10	
Well New Test slott (s)	30	

New Private Queue

NOTE: If you check the Private Queue Status checkbox, the Private Queue feature is enabled. Click edit option icon next to Private Queue to edit the Private Queue configuration.

Use LSS	
Host	
VSDESKTOP	
	► Add
Camp on	
Recall no answer timeout internal	0 external 20
(s)	
Recall busy timeout (s) 20	
Recalls from Consult Calls	
Behavior Music on h	old
Descrill	
Recall	
Function	Used queue
Recall - Busy For Internal Calls	Public_Recall
Recall - Busy For External Calls	Recall (private)
Recall - No Answer For Internal Calls	Public_Recall
Recall - No Answer For External Calls	Recall (private)
Park	
Eunction Used queue	
Park Queue Public Park	
- and good - abite_rank	
Private Queue	
Private Queue Status	
Function Queue	
🥜 Private Queue 🛛 MyQ 👕	

Private Queue Access page

Configuring Voice systems

To configure a new voice system to the site, perform the following steps:

- 1. Click the site entry to open the site configuration. TCA opens the **Site** page in a new window.
- 2. On the **Site** page, click **Voice Systems** in the left panel to display the **New Voice entry** page in the main window.

Voice entry Webpage Dialog				
http://10.10.144.48/tca/site/voiceentrynewiframe.aspx				
New Voice er	itry	^		
Туре	CMG Speech			
Number Range	81000 - Internal Queue			
Queue Manager	My_QueueManager 🗸			
Access number	81000 - 81000			
	Create Cancel			
		~		
<	>			

- **3.** Select the required type of speech from the **Type** drop-down list. The following types of speech are available:
 - a. CMG Speech: This speech type uses the same method that an attendant client uses to drop a call into a mailbox.
 - **b.** Direct drop CMG Speech: This speech type is configured to enable direct drop from the InAttend client (or Speech Attendant) to the CMG speech voicemail of a user.
 - **c. Direct drop to external system**: This speech type is used for a standalone system. With this type of speech the operator can route a call to a third party voicemail server or system.
- 4. Select the number range for the queue.
- 5. Select a queue manager cluster from the Queue Manager drop-down list.
- 6. Enter the required access numbers for the SIP Trunk.
- 7. Click **Create** to create the Voice System.

Deploy the configuration

When you have completed configuration changes in TCA, you have to deploy the configuration to make it active.

- In the Site page or the main TCA configuration page, click **Deploy** in the bottom right-hand of the page. To deploy the configuration in TCA, click the Deploy button at the right bottom of the Site page. The Deploy configuration dialog is displayed:
- 2. In the Deploy configuration window, click Deploy to confirm.

The system deploys the selected configuration.

3. Click **Close** to exit the TCA.

NOTE: You must restart Queue Manager and NeTS, when you switch between two different configurations in TCA. (For example, to switch between config1 to config2, deploy config2 in TCA, and then restart NeTS and Queue Manager services).

Queue Overflow on No Answer

When calls go to different queues for attendants sitting in different geographical locations, the customer needs to configure overflow in TCA, so calls are forwarded when they are not answered. The customer can achieve their goals in response time using:

- 1. Overflow No Answer time Edit box:
 - "Overflow No Answer time" edit box is added in the queue below wait time 2nd alert.
 - There is no dependency on "Wait time first alert" and "Wait time second alert" timers.
 - This is a must (*) field, but the value has to be positive integer.
 - The entered time is applicable to all the queue entries.

<i>(i</i>)	View site My Site Webpage Dialog	X
		Queue Entry Webpage Dialog
Telephony Configuration Application	Queue - Internal	Edit Queue Entry
My_Site	Settings	Queue access
	Queue Manager Cluster My_QueueManager V	Description Internal
⊡Site: My_Site	Default prio 5	Pbx My_PBX
Private Networks	Max size 100	Number Range 08 Internal
	Wait time 1st alert (s) 10	Domain My_Domain
External	Wait time 2nd alert (s) 30	Access number 08
+ Operator Groups	Queue NoAnswer Time (s) 60	Settings
Voice Systems	Default Queue Entry Settings	Passive redirect No passive redirect
	Passive redirect	O Queue External (My. Site)
	Closed redirect No closed redirect Queue	
	Overflow Overflow Oqueue	
	Overflow No Answer No overflow Answer Queue	
		Queue External (My_Site) V
	Queue Entries	Overflow No overflow
	Domain Description Access number Active	Queue External (My_Site) V
	J My_Domain Internal 08	
		Scheduling
		Common Holidays Edit
		O Custom Holidays
		Daily 12:00 AM to 11:59 PM
		Monday 12:00 AM to 11:59 PM Active 12:00 AM to 11:59 PM Active
		Tuesday 12:00 AM to 11:59 PM Active 12:00 AM to 11:59 PM Active
		Wednesday 12:00 AM to 11:59 PM Active 12:00 AM to 11:59 PM Active
		Thursday 12:00 AM to 11:59 PM Active 12:00 AM to 11:59 PM Active
		Friday 12:00 AM to 11:59 PM Active 12:00 AM to 11:59 PM Active
		Saturday 12:00 AM to 11:59 PM Active 12:00 AM to 11:59 PM Active
		Sunday 12:00 AM to 11:59 PM Active 12:00 AM to 11:59 PM Active
-		

2. Overflow on no answer queue setting:

A new "overflow on no answer" field is added in the settings of Queue similar to "Overflow".

- The available options are:
 - No Overflow
 - Queue
 - Number.

By default, "No Overflow" is selected.

- When No Overflow on no answer is selected :

The call is not diverted irrespective of the value in the "Overflow No Answer time" spin control.

- When Queue is selected:

A combo box is enabled with configured queues and user can select the queue to move the call after the "Overflow No Answer time".

- When Number is selected

An edit box is enabled and user can write the number to divert the call on "Overflow No Answer time" timeout.

The behavior is same as that of "Overflow" but not for recall queues.

Default Queue Entry Settings				
Passive redirect	◉ No passive redirect ○ Queue	External (My_Site) V O Number		
Closed redirect	● No closed redirect ○ Queue	External (My_Site) V O Number		
Overflow	No overflow	External (My_Site) V O Number		
Overflow No Answer	◉ No overflow Answer ○ Queue	External (My_Site) V O Number		
		Update		

Play Different MoH for InAttend - for Different Queue

The administrator can configure a custom MoH in TCA by specifying the path of a .wav file in the **MoH File** field and update this setting for each queue. The custom **MoH file** can be confiured for Public and Private queues. The MoH file will be played when a call is on hold, parked, or on recall queue. To play the default MoH file configured in Media Server for a particular queue, the **MoH file** field can be kept empty for that queue.

Site	Settings					
Site Site: My_Site Private Networks Public Queues Internal External SA Recall-SA test Operator Groups My_Operators Oueues	Queue Manager Cluster Default prio Max size Wait time 1st alert (s) Wait time 2nd alert (s) Queue NoAnswer Time (s) MOH File Default Queue Entry Sett Passive redirect Closed redirect Overflow	My_QueueManager >> 5 30 20 40 10 C:\Program Files (x8# ings O No passive redirect No closed redirect No closed redirect		ediaServer\Chillingt External (My_Site) External (My_Site)	Ausic.way	
Operator Group Users SA Voice Systems	Overflow No Answer	No overflow Answer	O Queue	External (My_Site)	V O Number	Update

ueue Entry - Mic	rosoft Edge	-		×
D 211.63.76/to	a/site/PersonalQueue.aspx?i=15&functionNa	me=Persona	l&queu	eld=1
Private Queue	•			
Name	pq			1
Max size	5			
Wait time 1st aler (s)	10			
Wait time 2nd ale (s)	t 30			
MOH File	C:\Program Files (x86)\Mitel\MediaServer	r\ChillingMus	ic.wav	
	Add			
Update				
Private Queue a	ccess			
Description				
Pbx	My_PBX V			
Number Range	62 - Internal Queue			

Appendix B: CMG-specific configuration

If you are using InAttend with CMG Server, you have to perform some additional configuration:

- Configure a CMG user as TCA admin
- Add the CMG administrator to the operator group
- · Configure presence for the CMG server
- Optimize Nicesrv

For more information, refer to the online help for Configuration Manager.

Configuring a CMG user as TCA admin

If you are using InAttend with CMG Server, you have to configure a CMG user with TCA administrator privileges in order to login to TCA. You configure the user in the Configuration Manager tool.

To configure the CMG user with TCA Admin privileges, do the following:

- 1. Log in to the Configuration Manager tool.
- 2. Select All users, then select the user account that has TCA admin privileges, and click Add Service.
- 3. In the **Telephony Configuration Application** field, select **ADMIN** and click **Ok**.
- 4. Click Save on the All Users page to save your changes.

Adding the CMG Administrator to the InAttend Operator Group

You have to add the CMG Administrator to the InAttend operator group in the Telephony Configuration Application (TCA).

To add the CMG administrator to the operator group, do the following:

- 1. Log in to the TCA.
- 2. Open your TCA configuration and click on Sites in the left panel.

On the Sites page in the main window, click on the entry for your site to open the site configuration. TCA opens the Site page in a new window.

- 3. On the Site page, expand **Operator groups** in the left panel to display the configured operator groups.
- 4. Click **CMG Users** to display the CMG Users page in the main window.
- On the CMG Users page, select the company from the drop-down list in the first field and select CMG user from the drop-down list in the second field. Click Add. Second column and c page in the main window.

Disabling default templates using Attendant special settings

1. Remove the default message template from InAttend client via Attendant Special settings in webadmin.

Attendant Special settings	
add profile: MessageTemplate	
Profile name MessageTemplate Description Remove the default message template from	m client
Parameter (Node1/Node2/Parameter) MessageTemplate\DisableDefau Parameter value 1 >>	< SpecialSettings />

- 2. Add Attendant Special setting Profile name as MessageTemplate.
- 3. Add the Parameter:

MessageTemplate/DisableDefaultTemplate

4. Add the Parameter value to 1.

5. Add **Profile name** and **Description** then click **Save**.

Profile name	MessageTemplate			
Description	Remove the default message template from client			
Parameter (Parameter v	Node1/Node2/Parameter) - < SpecialSettings > - < MessageTemplate > < DisableDefaultTemplate > 1 DisableDefaultTemplate </ MessageTemplate			

6. Add the new Profile type Attendant Special settings to the Profile Group.

Configuring Presence for the CMG Server

To integrate with BluStar Presence Server when using InAttend with CMG Server, you have to configure the following settings in CMG Configuration Manager:

- BluStar Presence Server
- BluStar Presence Username

To configure presence for the CMG server, do the following:

- 1. Log in to the Configuration Manager tool.
- 2. Select CMG Web and then select Parameters.
- 3. Select BluStar/LDAP Directory Server and enter the information for BluStar Presence Server and BluStar Presence Username.
- 4. Click Save to apply your changes.

For more information, refer to the online help for Configuration Manager.

Optimizing Nicesrv

Nicesrv is the process used by InAttend clients to access the CMG Server database. Optimization of nicesrv is achieved using the following formula:

```
MaxThreads = NumberOfAttendants * 8
MinThreads = 0.75 * MaxThreads
Connections = MaxThreads
```

To optimize the Nicesrv process, do the following:

1. Open the Spman tool and set the NICESRV parameters:

Program	NICESRV		
Program path	nicesrv.exe		<u>S</u> ave
Parameters	-15		
Wait	0		<u></u>
Max restarts	4		Delete
Start order	0		
Enabled	V		
Desktop			Previous
State	Running		Next
Start time	15-05-22 15:01		
Errors	0		
Additional par	ameters		
Group	Name	Value	
Tune	 LongTimeout 	7	
	LongTimeou	at 7	_

2. Click Save to apply your changes.

Configuring Presence Server when using more than one E-mail Message System

The InAttend client is in some situations using the wrong result when trying to select an email address. To avoid the problem, we recommend that a misc field in the CMG database is used instead when searching and fetching the results for email addresses that is used for Linestate.

Prerequisite

An email address has to be unique in the CMG database for presence to work (duplicates are not allowed). If a person/extension is inserted multiple times - email address cannot be the same, use an alias or leave it blank. When duplicates are found for a record they will not be used.

Populate **misc29** (Field29) in the db with correct email addresses (CMG DM or import) - the field is synced with the ldap table in the nice db as well.

Do the following:

 In the config tool webadmin - Presence Server - Presence Interface - section Attributes and Search. This example uses misc29 but any misc field can be used. Change the value (default mail) Mail address and SIP address in Attributes to misc29 and <Sip:> in Search to misc29 and save:

Attributes		
Mail address	misc29	SIP address misc29
Business phone	telephoneNumber	Private phone homePhone
Mobile phone	mobileTelephoneNumber	Account name accountName
Search		
<sip:> misc29</sip:>	<tel:> telephoneNu</tel:>	mber

 Change the search criteria for the InAttend client in webadmin - User Configuration - Configuration profiles - Attendant PBX for the correct profile, click on the box Settings. In the lower right corner settings for Linestate 2 attributes are displayed Email attribute and SIP address attribute. Change to Field29 (Misc29) on both rows (default is FirstMessageSystemId) and save:

Linestate				
Email attribute	Field29 (Misc29)	•		
SIP address attribute	Field29 (Misc29)	•		
Show presence status as linestate				

3. Restart these services: CMG web, Presence server and DAL server.

Restart InAttend clients.

NOTE: E-mail message system can also be used to send text messages to mobile phones or using different SMTP servers for outgoing emails.
User details as in MiCollab Client 137 User details as in MiCollab Client 138



mitel.com

© Copyright 2021, 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.