Installation and Configuration Guide

Release 2.6 SP2
June, 2021

Mitel®

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: http://www.mitel.com/trademarks.

Contents

Chapter: 1 **Introduction 1**

InAttend system components 1

Chapter: 2 **Before You Begin 4**

InAttend Licenses 4
Software Requirements 4
Security Certificates 4
IIS Configuration to access TCA, WebAdmin, QM and other applications over HTTPS 5

Chapter: 3 **Call Manager Configuration 7**

Configuration for Skype for Business 7
SIP trunk Configuration on Skype for Business 7
TCP Configuration on Skype for Business 15
Closed Redirect and Queue Scheduling 16
TLS and SRTP Configuration on Skype for Business 16
Configuration for MX-ONE 17
Set ECF for extensions without right for ECF 17
PARAMETERS 17
SIP trunk Configuration on MX-ONE 18
Enabling the CSTA server in MX-ONE 18
Initiating the Route Access Code 19
Creating SIP routes toward the ACS server 20
TLS and SRTP Configuration on MX-ONE 25
Configuring TLS on MX-ONE SIP trunks 25
Configuring SRTP on MX-ONE 30
Configuring Day/Night Service Positions 30
Initiating the abbreviated number series 31
Initiating the abbreviated numbers 32
Initiating Day and Night Service Positions for a private route (internal call queue) 33
Initiating Day and Night Service Positions for a public route . . 33

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 94
InAttend Journal Configuration 98
Configuring the Authentication and Authorization (AnA) web service . .99
Configuring the AnA connection to the CMG server 99
Configuring the AnA connection to a Different Server 99
Enabling HTTPS for Image Fetching 100

Chapter: 7 Configuring the Presence Server 102

Viewing Presence Server Configuration 102
Adding a Microsoft Exchange Data Source 103
Adding a Microsoft Skype for Business Data Source 105
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 106
Creating a trusted application in Microsoft Skype for Business 107
Creating and importing certificates 108
Adding a Data Source 108
Adding a CISCO Data Source 109
Configuring the Cisco Unified Presence Server (CUPS) for InAttend 109
Configuring the Presence Server for CUPS 110
Adding a line state data source 112
Configuring a PBX link for line state (MX-ONE) 113
Configuring a PBX link for line state (MiVoice 5000) 116
Configuring a Line State Server (Cisco only) 119
Installing the Cisco Line State Server (LSS) component 119
Configuring the ACS Cisco Line State Server 122
Enabling a Secure Channel for AnA and TCA 123
Configuring the Presence Interface 124
Configure Directory Server (MiVoice 5000) 125
MiCollab and InAttend with MiV5000 129

Chapter: 8 Configuring Directory Server 131

Chapter: 9 Configuring MiCollab presence with InAttend 137

Micollab presence with InAttend in CMG 137
Micollab presence with InAttend in Standalone 138
Modifying Webadmin Configurations in InAttend for Standalone 139
Settings for Micollab with InAttend 141
Modifying CMG Web Service Configurations 142
Adding MiCollab Configuration File 143

Chapter: 10 Configuring InAttend profiles and users 145

Working with configuration profiles 145
Viewing InAttend configuration profiles 145

Modifying the Attendant Directories Profile 146
Change Directory View Automatically 148
Overlapping numbers 149
Modifying the Attendant Layout profile 149
Modifying the Attendant Messages profile 150
Modifying the Attendant PBX profile 152
Modifying the Attendant Search profile 155
Modifying the Server profile 159
Working with profile groups 160
Creating a new profile group 160
Modifying a profile group 161
Configuring InAttend users 161

Chapter: 11 Generate CSR in ACS 164

Chapter: 12 TLS Certificates Installation 166

Chapter: 13 Configuring the NeTS telephony system 169

Chapter: 14 Configuring the Media Server 176

Chapter: 15 Installing the InAttend Client 179

Configuring the InAttend Client 181

Chapter: 16 Configuring EFS 182

Chapter: 17 Setting up Quality Manager 183

Prerequisites 183
Installing the Quality Manger Server 183
Installing the Quality Manager Database 183
Installing the Quality Manager Service 184
Installing the Quality Manager Reports Web 184
Configuring the Quality Manager Server 185
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 188
Configuring the Journal Database 188
Configuring Working Hours in Quality Manager 189
Configuring customers in Quality Manager 190
Viewing queues in Quality Manager 191
Assigning customers to a domain in Quality Manager 192
Configuring interval sets in Quality Manager 193

Installing the Quality Manager Wallboard 196
Configuring the Quality Manager Wallboard application 196
Configuring the Quality Manager Database Connection 197
Configuring the InAttend Connection 198
Configuring the Queues to display 198
Configuring operators to display 199
Configuring the Wallboard layout 200
Configuring thresholds for alerts 201

Chapter: 18 Additional configuration tools 202

DAL configuration tool 202
CMG configuration tool 203
InAttend standalone deployment 203
InAttend with CMG 205

Chapter: 19 Verifying your installation 207

InAttend system verification 207
General 207
InAttend call handling 207
Line state and activities/forward 208
InAttend user interface 209
Quality Manager verification 209
Verifying the Quality Manager installation 210
Verifying the Quality Manager Wallboard 210

Chapter: 20 Logging 212

Log Levels 212
Log Directory for each Component 212
Default software 212
AnA Web Service 212
BluStar License Manager 213
BluStar Server and BluStar Presence Server 213
CMG Web Service 213
Enterprise License Manager (Server and Client) 213
Mitel LDAP Server 213
InAttend Client 213
Media Server 213
Network Telephony Services (NeTS) 213
Queue Manager 214
Telephony Configuration Manager 214
Optional Server Software 214
Optional Client Software 214

Chapter: 21 References 215

Chapter: 22 **Appendix A: Configuring telephony services in TCA 216**

Telephony services configuration sequence 216
Create a TCA configuration 218
Configure the call manager and ACS hosts 219
Add a site 220
Add a Line State Server 225
Add a Queue Manager 226
Configure the NeTS host 227
Create a media server and add it to the site 227
Create a queue for the site 228
Create an operator group and assign it to a queue 229
Configuring public recall queues 230
Private Queue Number for Individual Attendants 233
Configuring Voice systems 236
Deploy the configuration 236
Queue Overflow on No Answer 237
Play Different MoH for InAttend - for Different Queue 238

Chapter: 23 **Appendix B: CMG-specific configuration 240**

Configuring a CMG user as TCA admin 240
Adding the CMG Administrator to the InAttend Operator Group 240
Disabling default templates using Attendant special settings 241
Configuring Presence for the CMG Server 242
Optimizing Nicesrv 242
Configuring Presence Server when using more than one E-mail Message System 243

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.

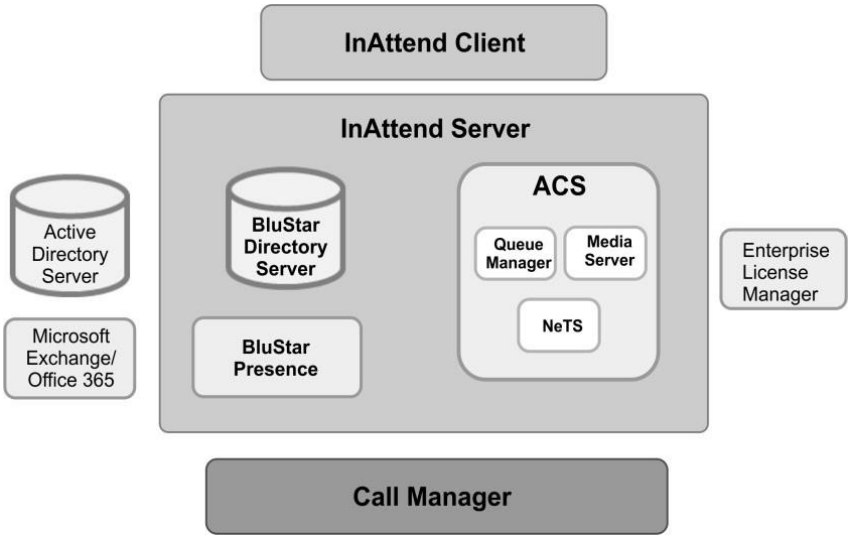
For advanced directory search and visitor management requirements, InAttend can be integrated with BluStar Collaboration Management (CMG). When InAttend is integrated with CMG, the attendant has the ability to set activities and forwarding for everyone registered in the CMG Server directory.

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:

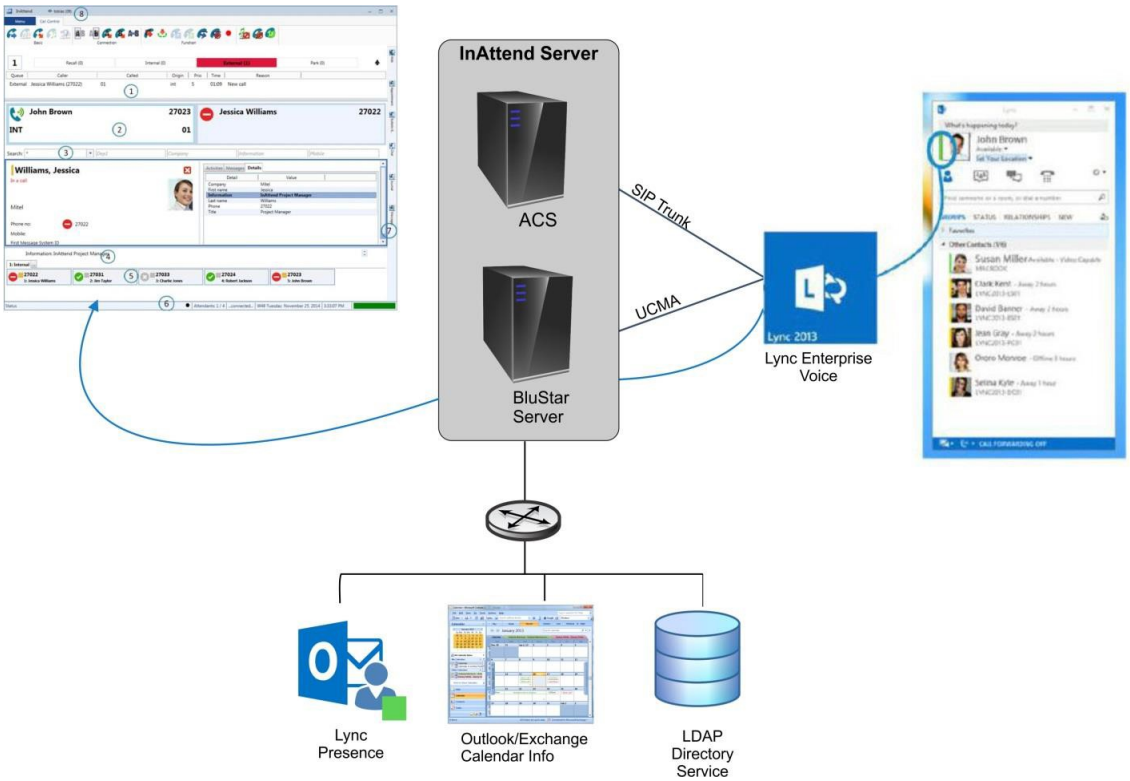
- **Enterprise License Manager**: handles licensing requirements for the InAttend application.
- **InAttend Server**: A telephony application that integrates with call managers, enabling call and media functionality. The components of the InAttend server include:
  - **BluStar Directory Server (or Active 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:

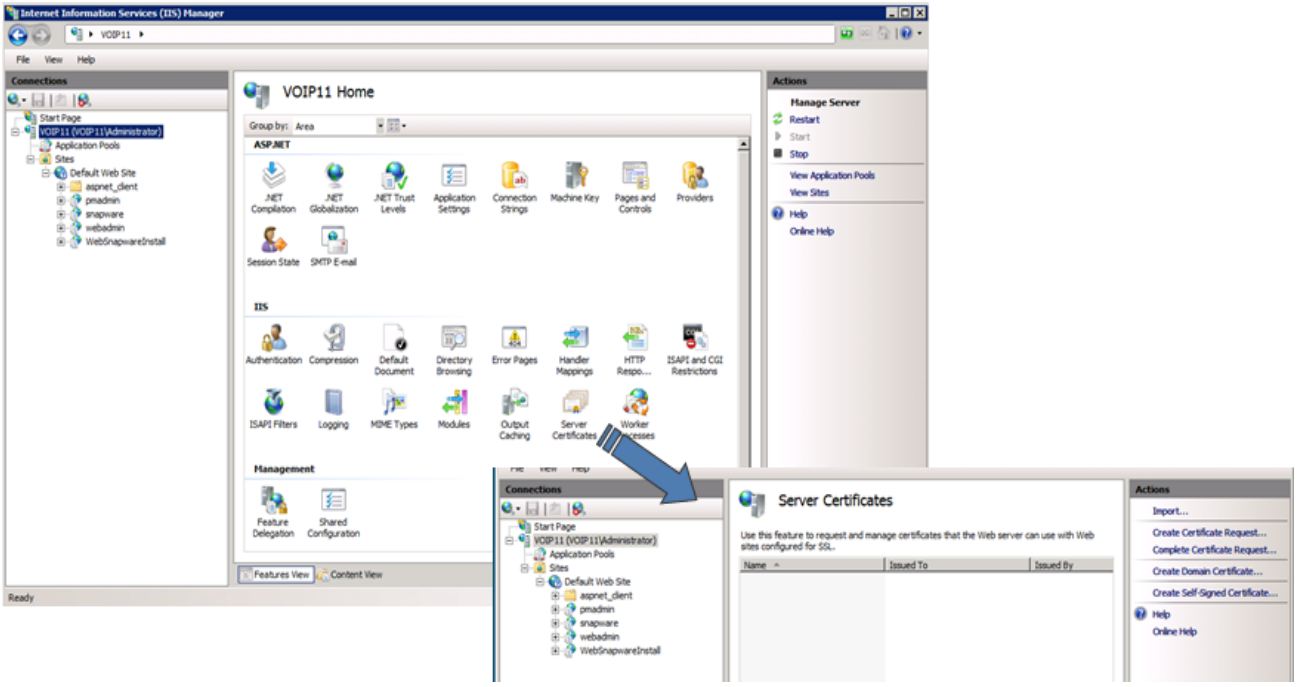
- Use IIS to create a certificate request.
- Submit the request to an online authority called a Certificate Authority (CA). Once approved, you will receive a certificate response which contains your digitally-signed public key.
- Install this certificate using IIS.

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

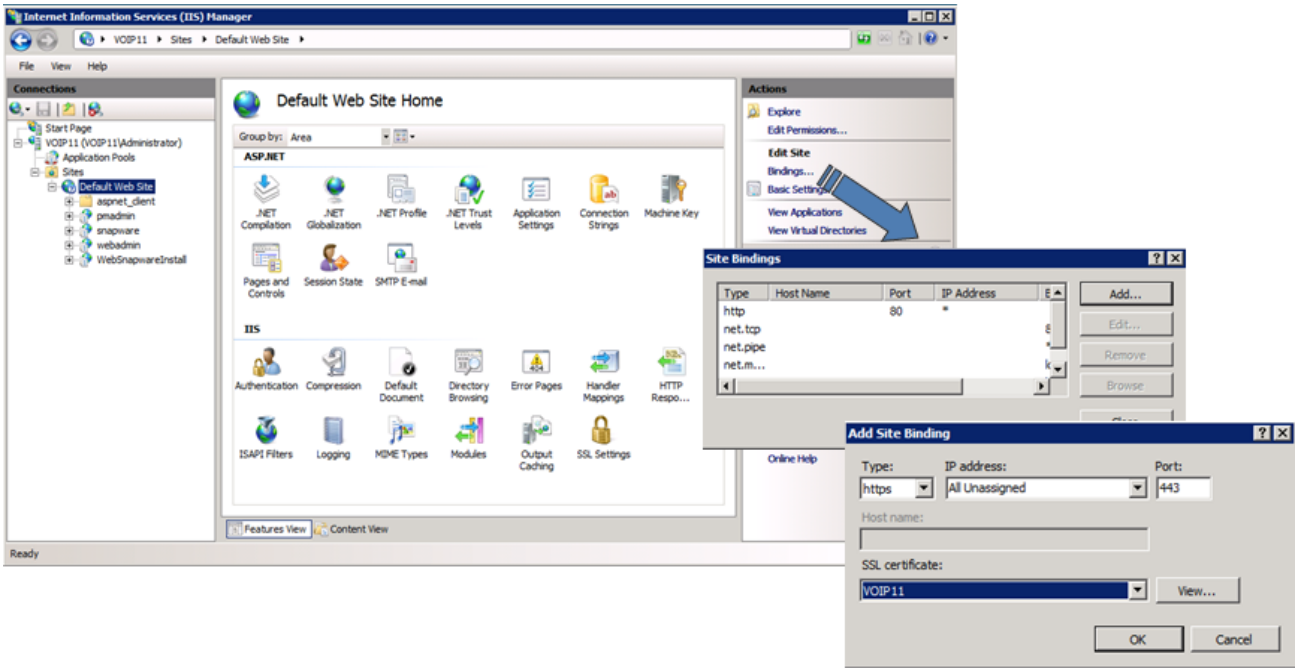
IIS Configuration to access TCA, WebAdmin, QM and other applications over HTTPS

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.

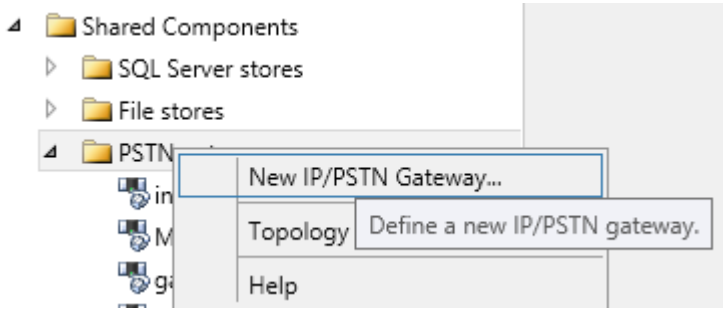
When you have CMG Web and Skype for Business, disable the Presence function in CMG Web.Update file Web config with below line: `<add key="SetBluStarPresenceStatus" value="false" />`

SIP trunk Configuration on Skype for Business

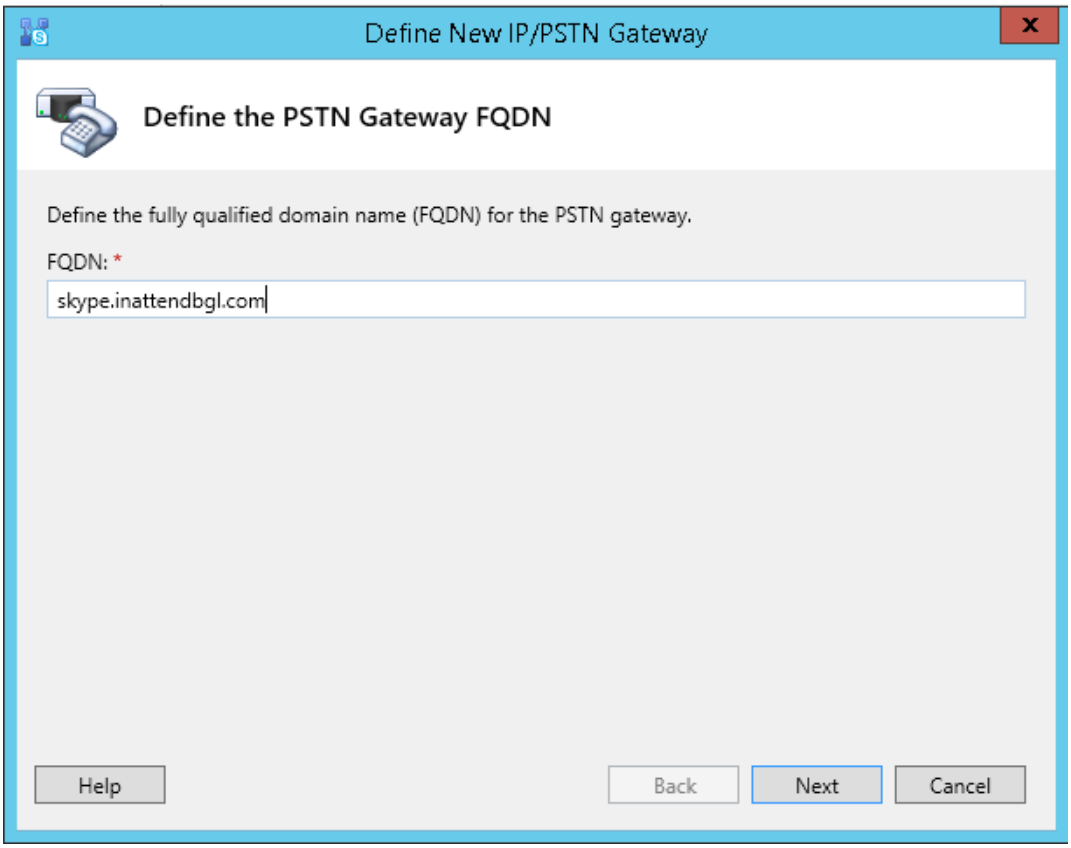
You must define a SIP trunk between the Microsoft Skype Mediation Server and the ACS component of the InAttend server.

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

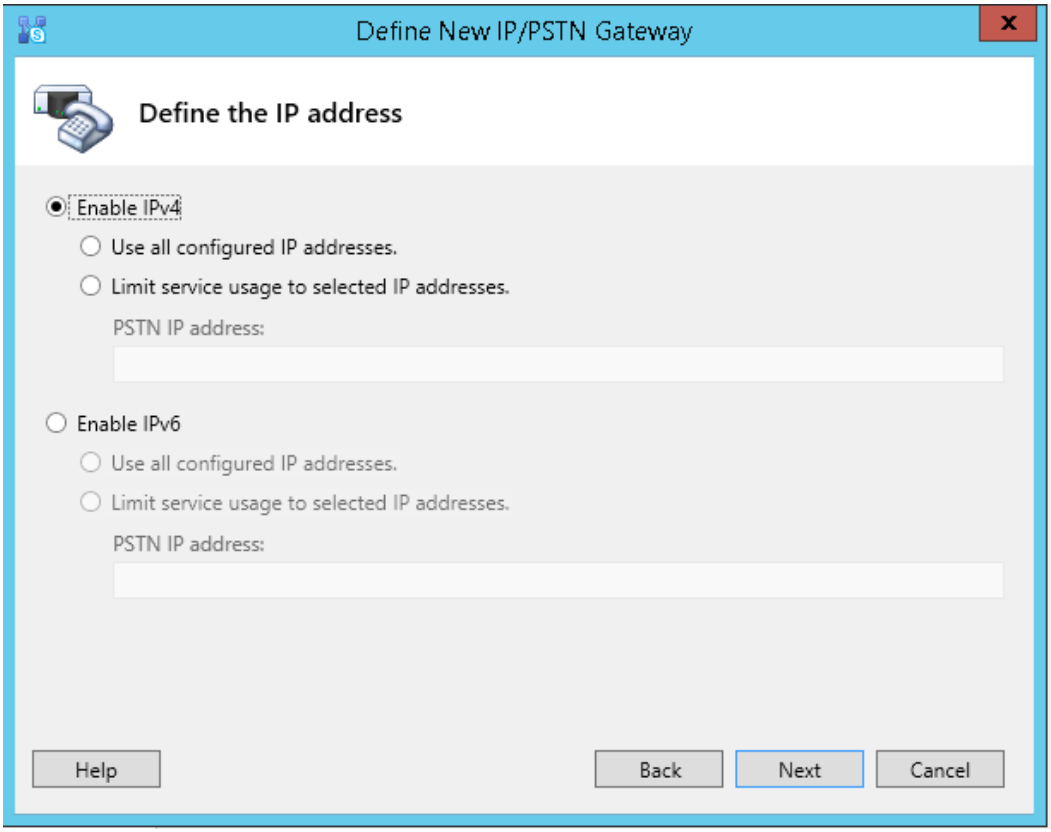
1. On the Skype Server, start the Topology Builder (**Start -> All Programs -> Skype for Business 2015 -> Topology Builder**).
2. In the Topology Builder, expand **Shared Components**.
3. Right-click on the **PSTN gateway** folder and select **New IP/PSTN Gateway** from the pop-up menu.



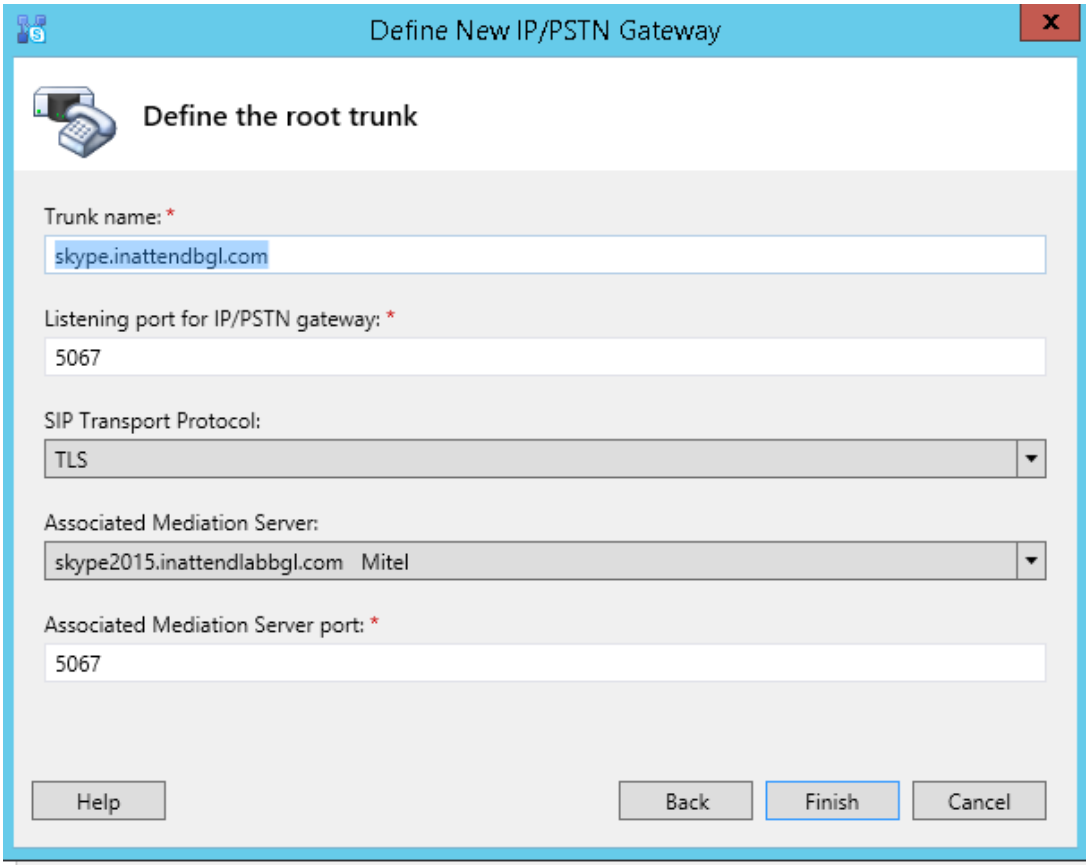
4. In the **Define the PSTN Gateway** window, enter the Fully Qualified Domain Name (FQDN) of the InAttend server and click **Next**.



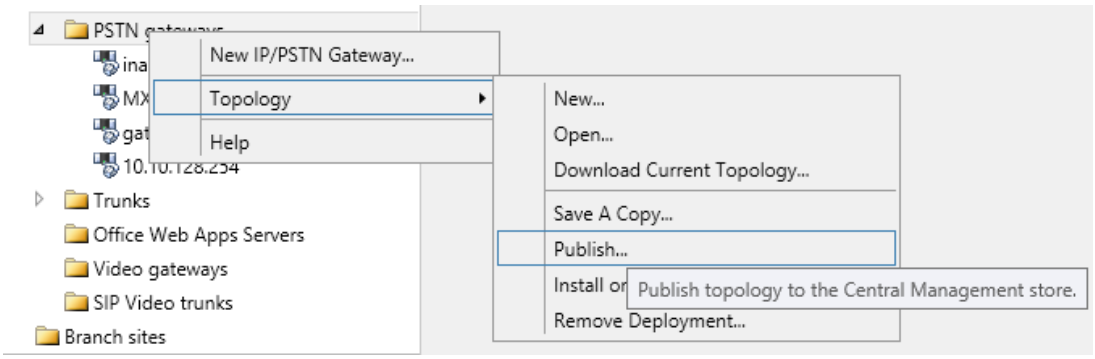
5. In the **Define the IP address** window, keep the default value ("Enable IPv4") and click Next.



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)



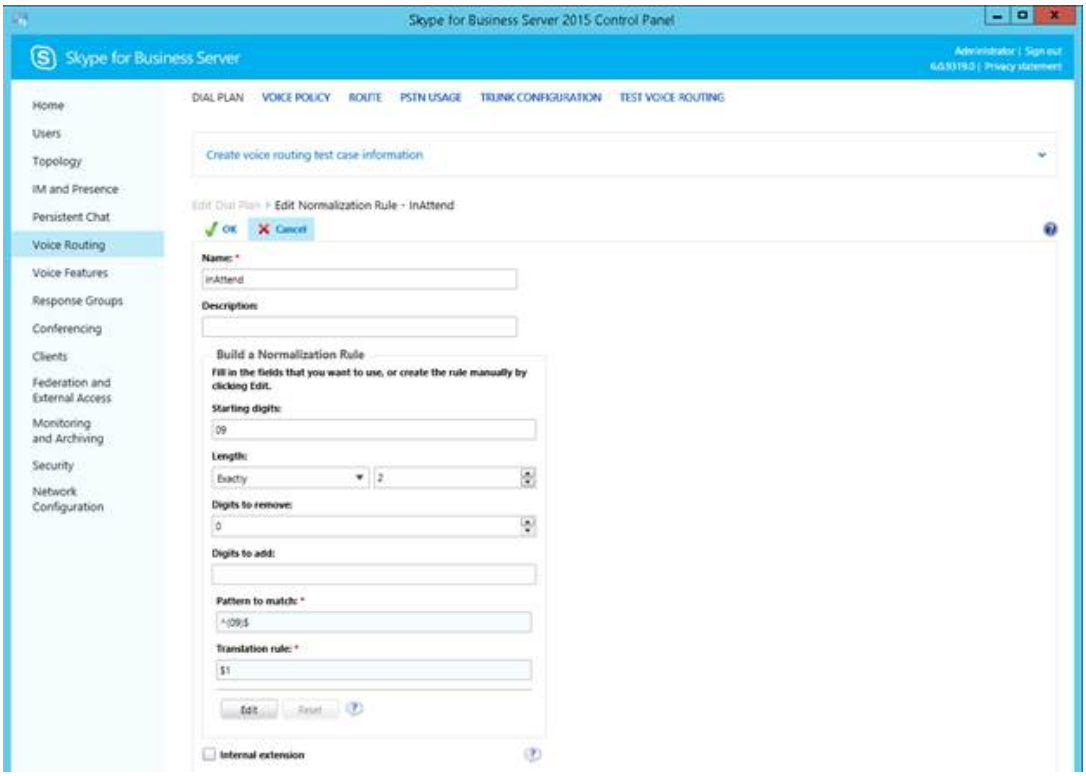
7. Publish the topology.
   a. In the Topology Builder, expand **Shared Components**.
   b. Right-click the **PSTN gateway folder** and select **Topology -> Publish** … from the pop-up menu.



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.

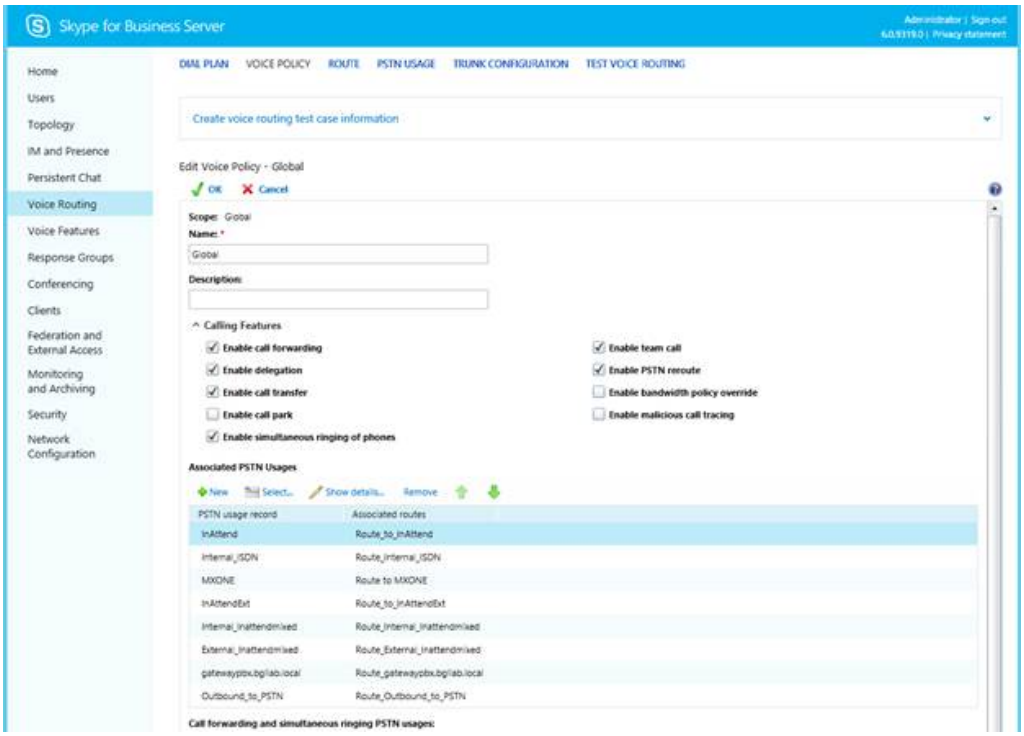
   a. On the **Dial Plan** tab, define a normalization rule appropriate for your organization, with at least a rule for Skype users to dial to InAttend. (Contact Microsoft for instructions on the appropriate setup for your company as required.)



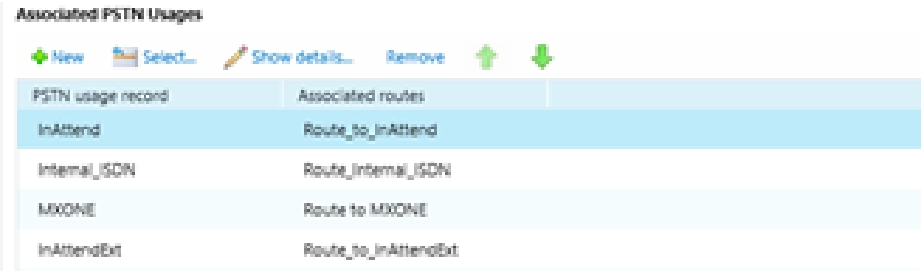
   b. Commit your changes.

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).

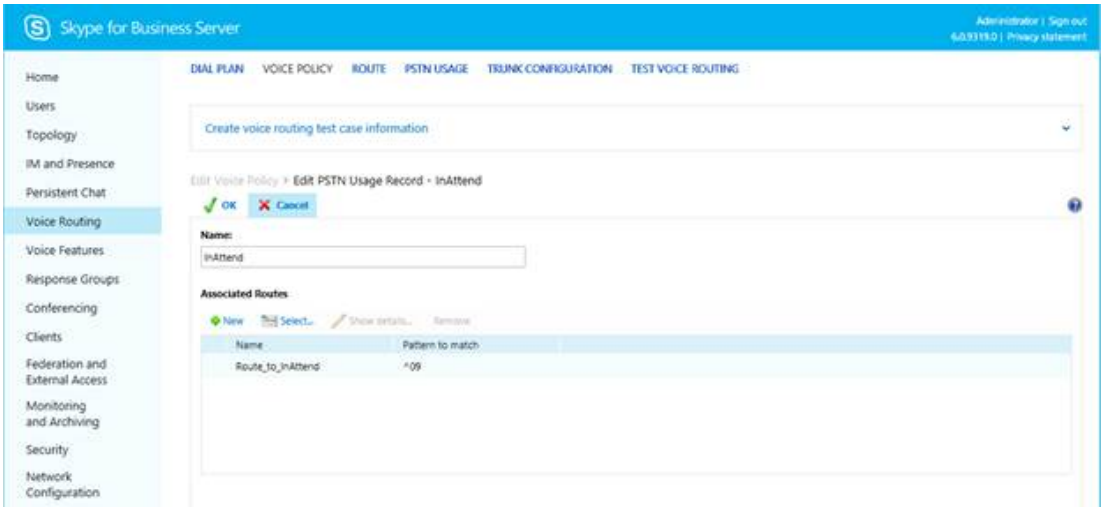
    a. On the Voice Policy tab, click **New** and select the type of policy applicable for your organization (**Site policy or User policy**).



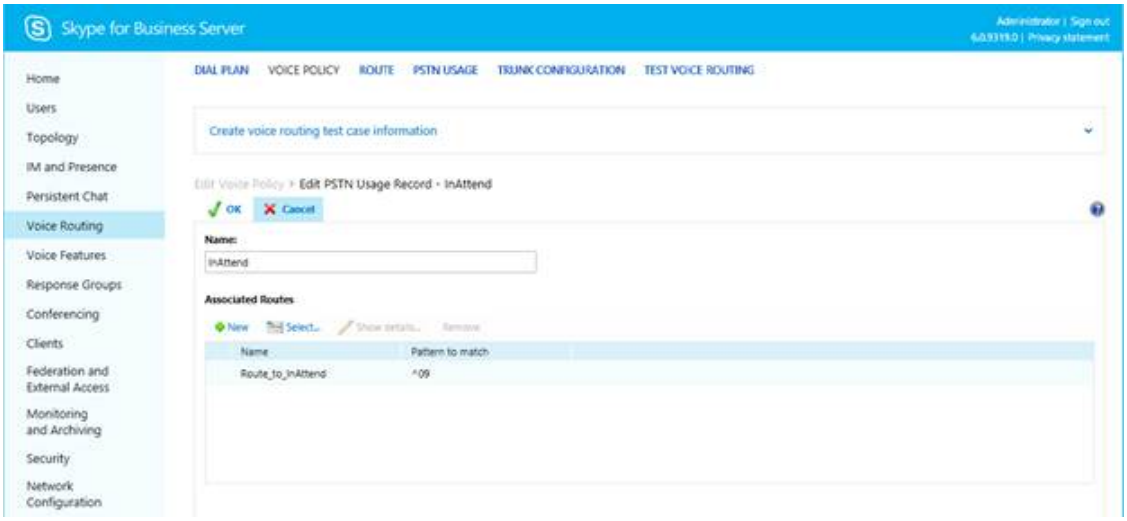
    b. Specify a **Name** and (optionally) a description for the voice policy.
    c. Click **OK** when finished.
    d. Under **Associated PSTN Usages**, click **New** to associate a new PSTN for this policy.



    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.

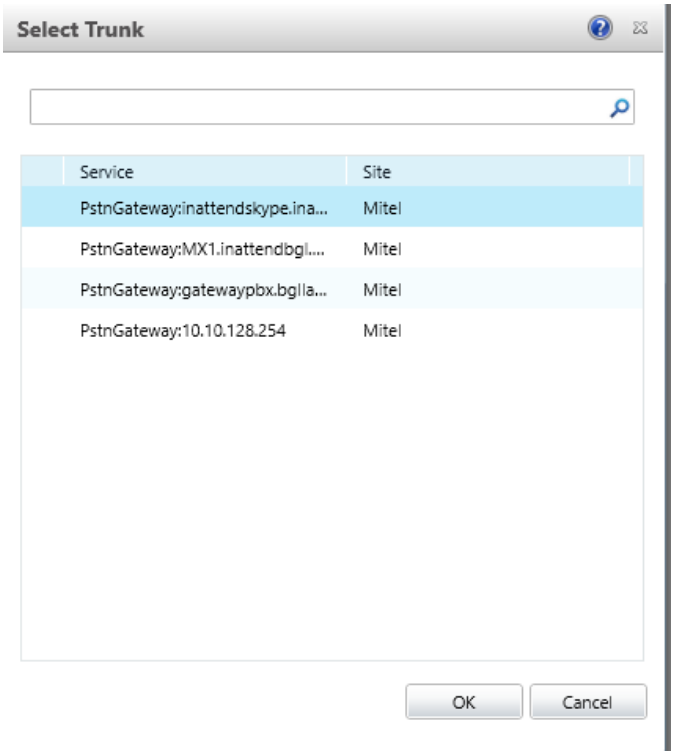


g. Specify a name and description for the new route.

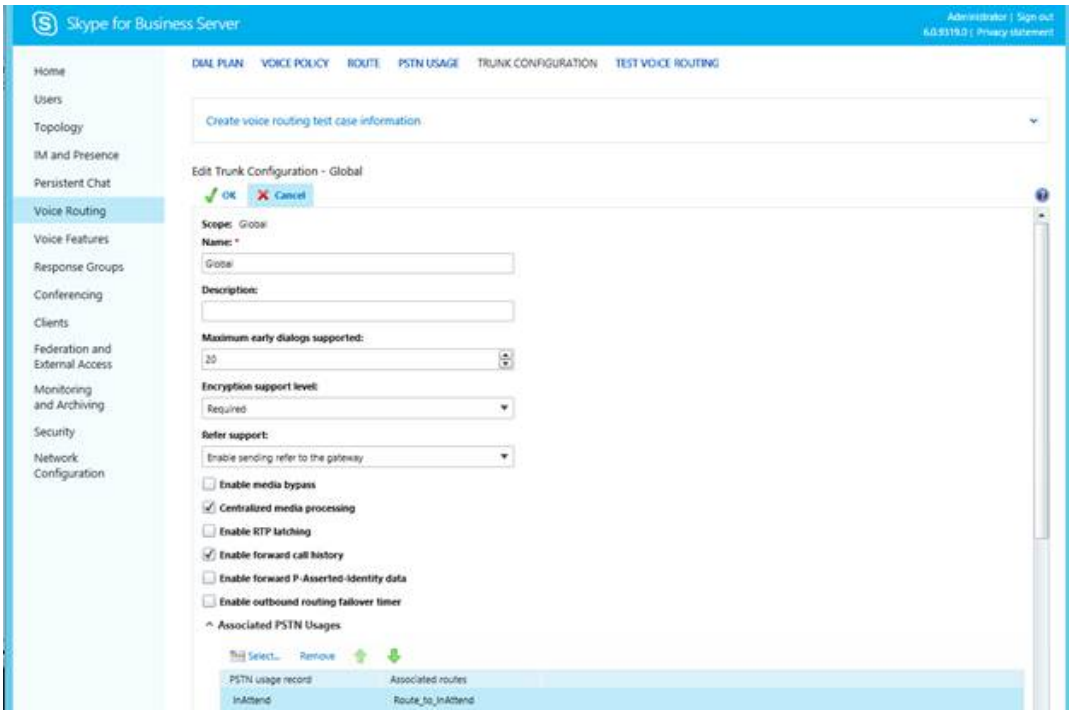


11. Associate the InAttend (ACS) PSTN gateway that you created in step 4 with the route.

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.



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.



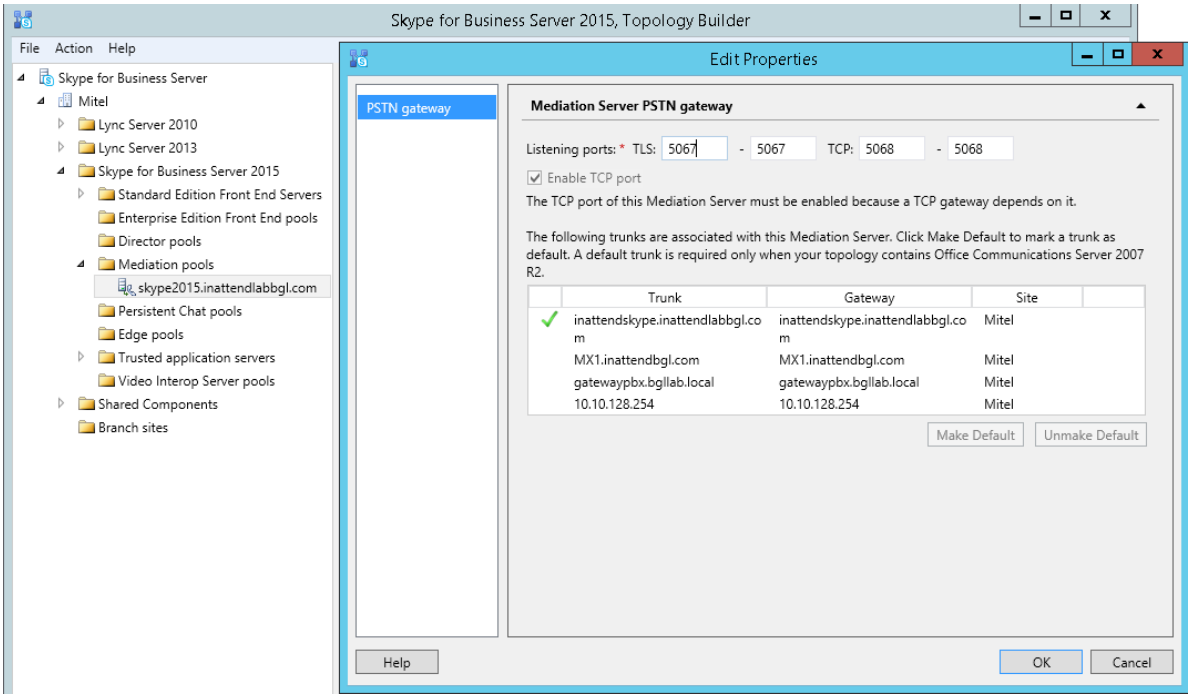
When setup is complete, assign Skype users to the Voice Policy you created in the above procedure.

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



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

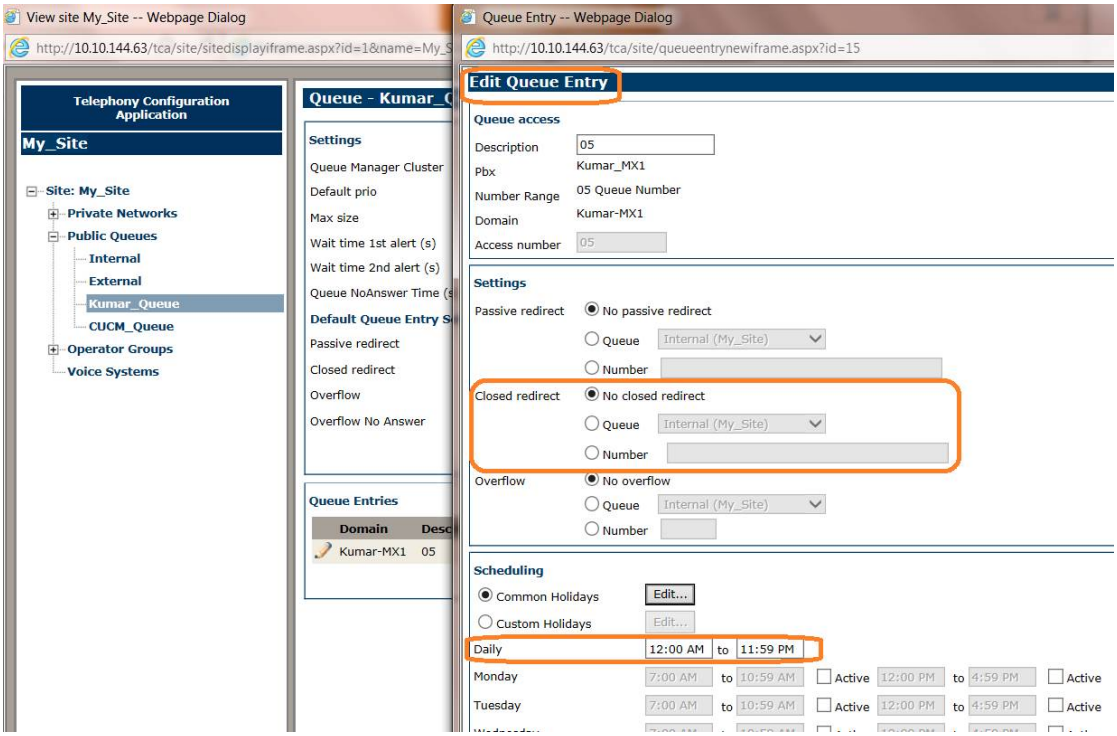
Public Queues under Telephony Configuration Application manages and can set the Call queue timings for a call queue entry.

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.



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).

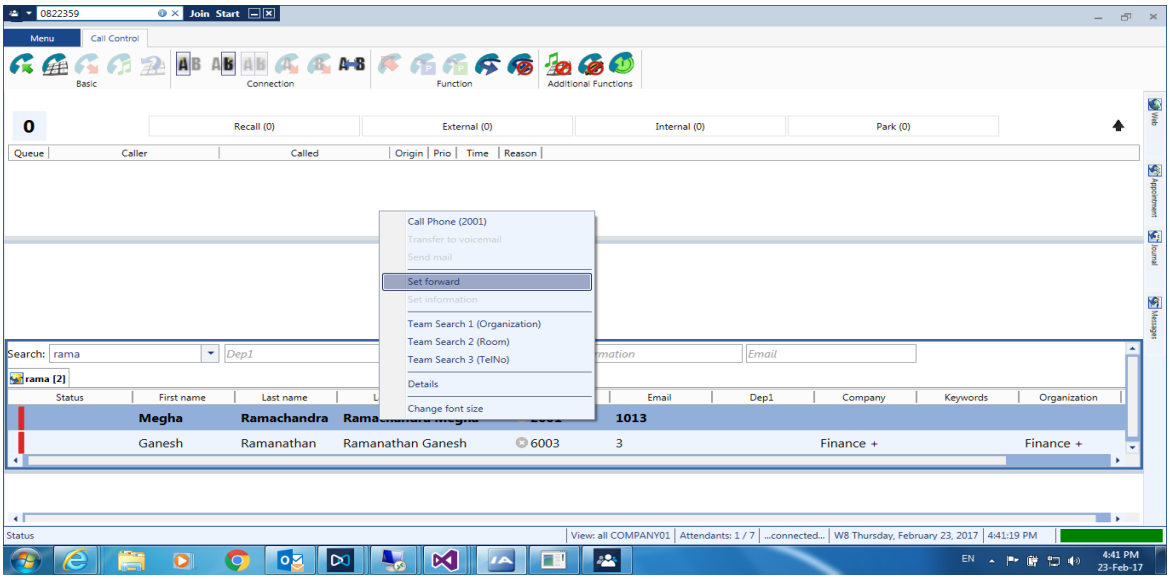
NOTE: If you restart Skype or the frontend server, you must also restart the InAttend server.

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.



PARAMETERS

--csta-serv

There is a new parameter exist in Mx-one that verifies –csta-serv xxxxxxxx1 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.

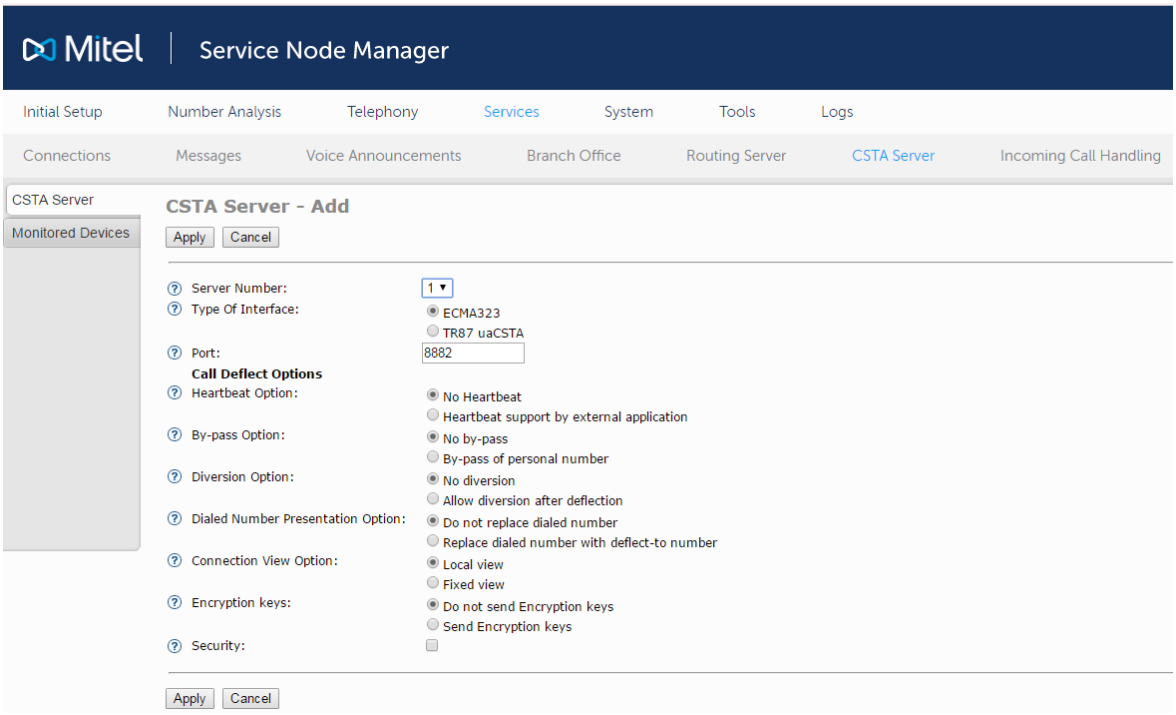
SIP trunk Configuration on MX-ONE

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.

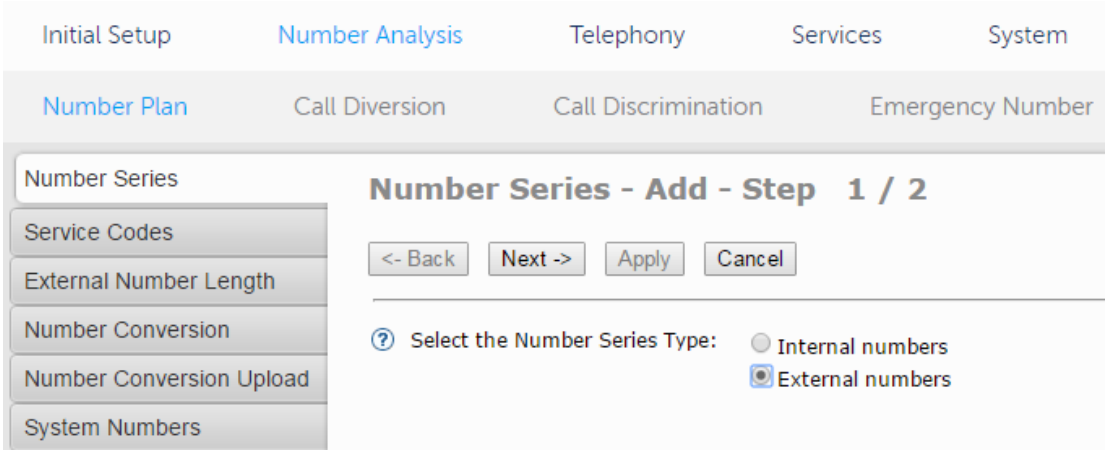


2. Select a server number and enter 8882 in the **Port** field.
3. Click **Apply**.

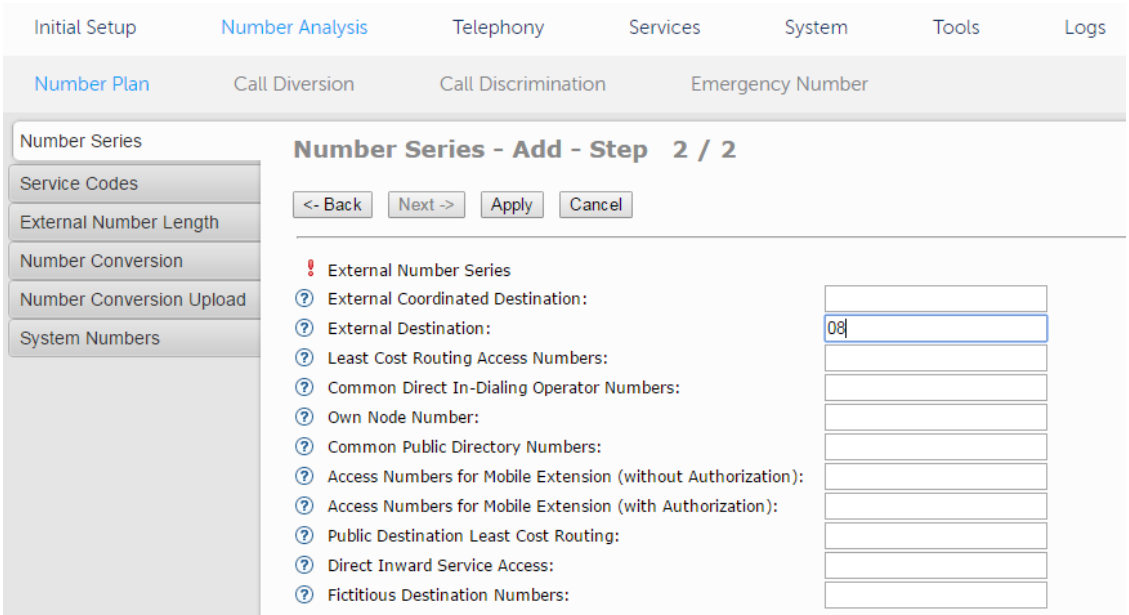
Initiating the Route Access Code

To initiate the Route Access Code, do the following:

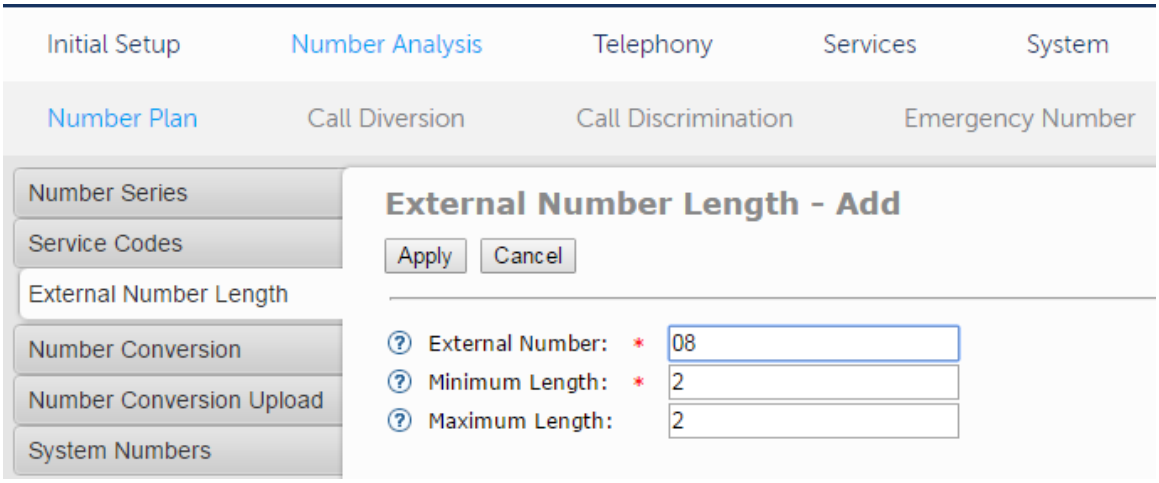
1. On the MX-ONE Service Node Manager main page, click **Number Analysis** and then click on the **Number Plan** tab.
2. Click **Number Series** in the left panel.
3. On the Number Series page, select “External numbers” for the **Number Series Type**.



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



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).

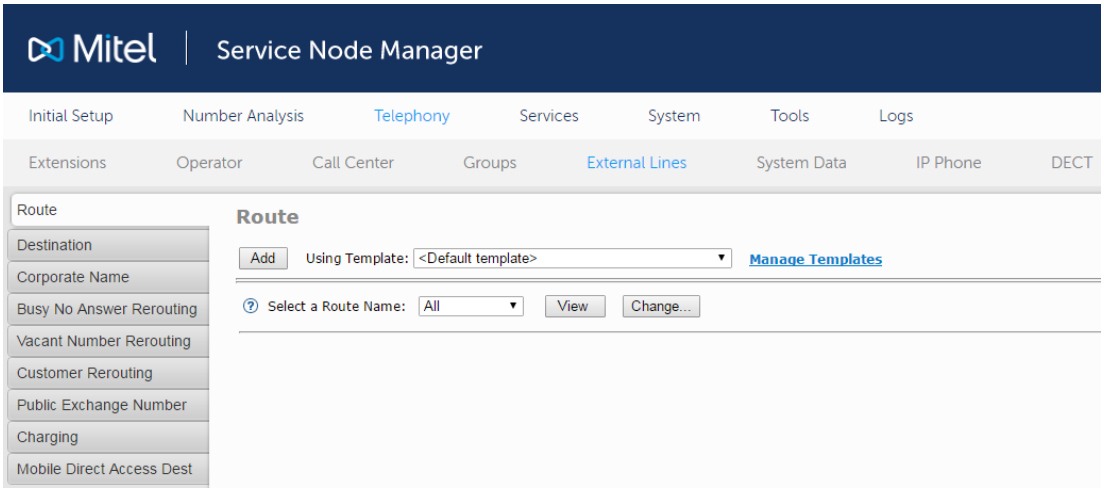


9. Click **Apply** to save your changes.
10. Repeat steps 2 through 9 for the PBX main number (e.g. 5500).

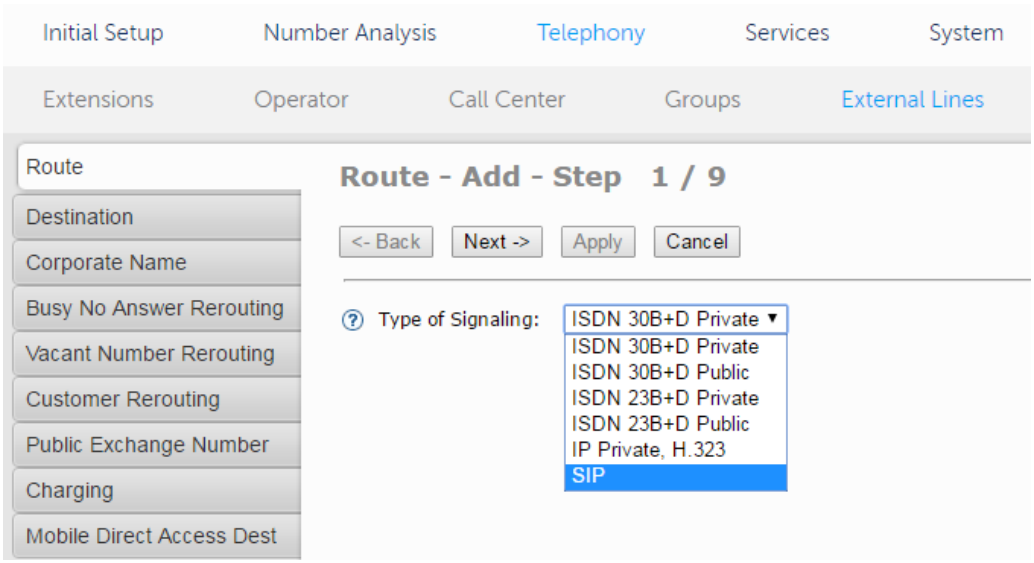
Creating SIP routes toward the ACS server

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

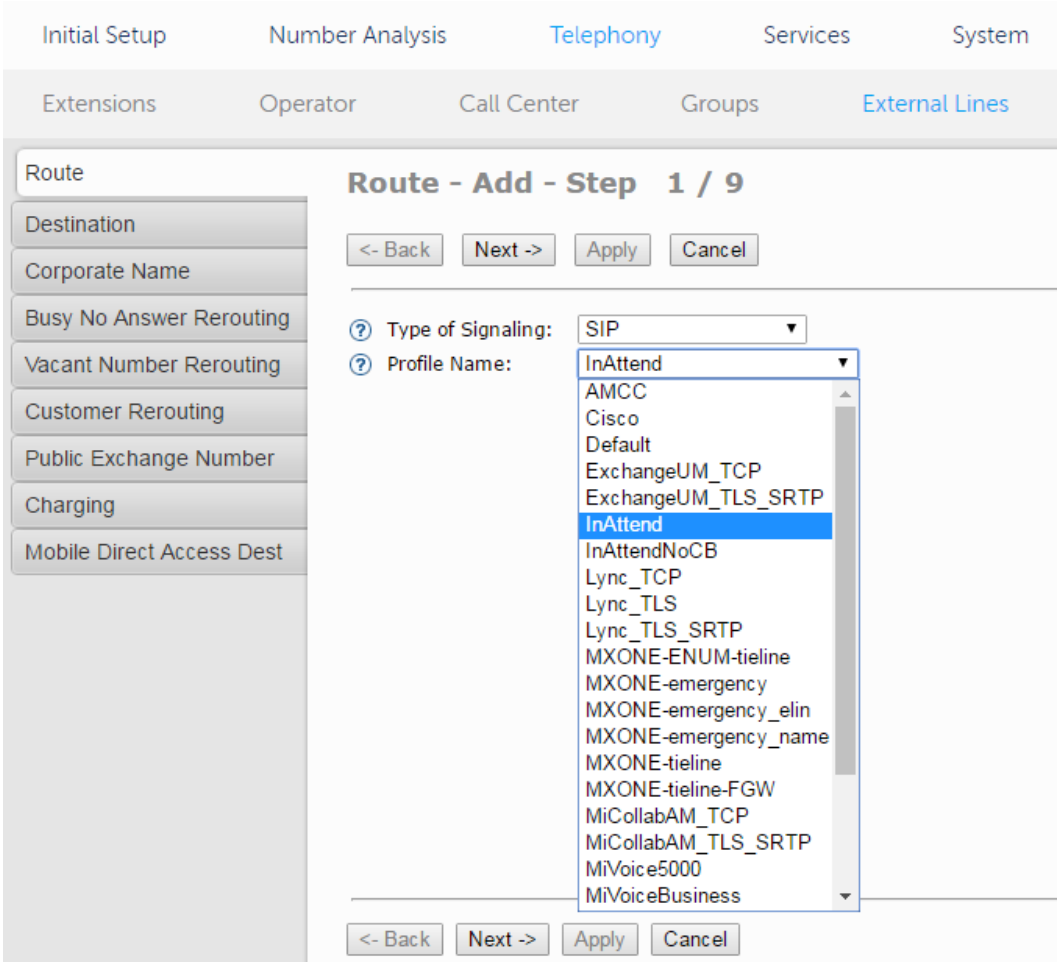
1. On the MX-ONE Service Node Manager main page, click **Telephony** and then click on the **External Lines** tab.
2. Click **Route** in the left panel.



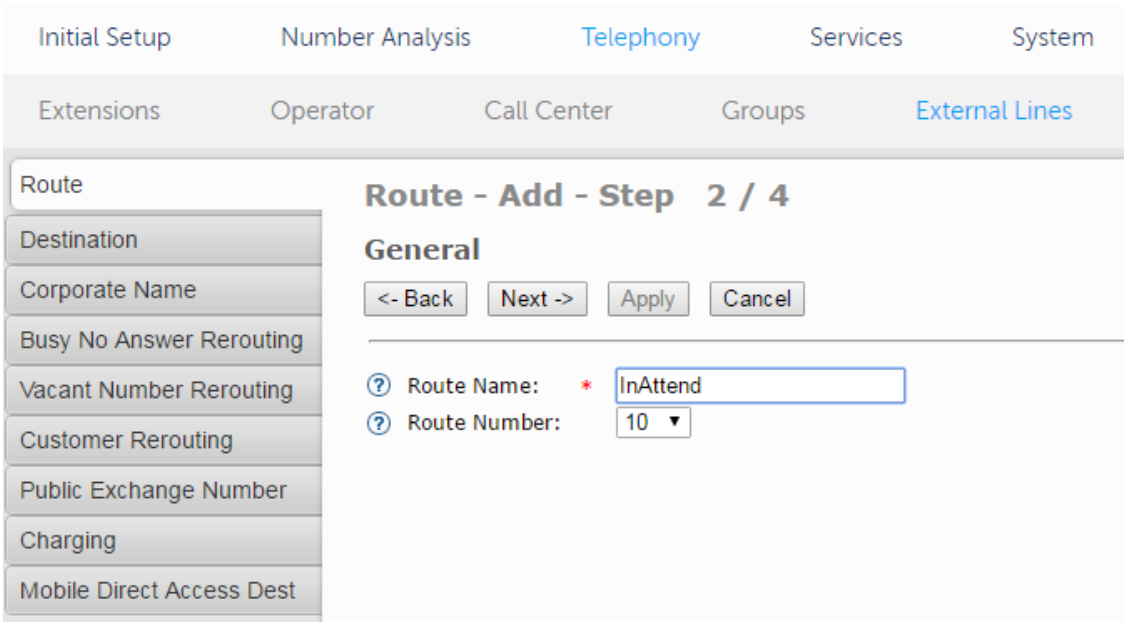
3. On the **Route** page, click **Add** and select “SIP” from the **Type of Signalling** list.



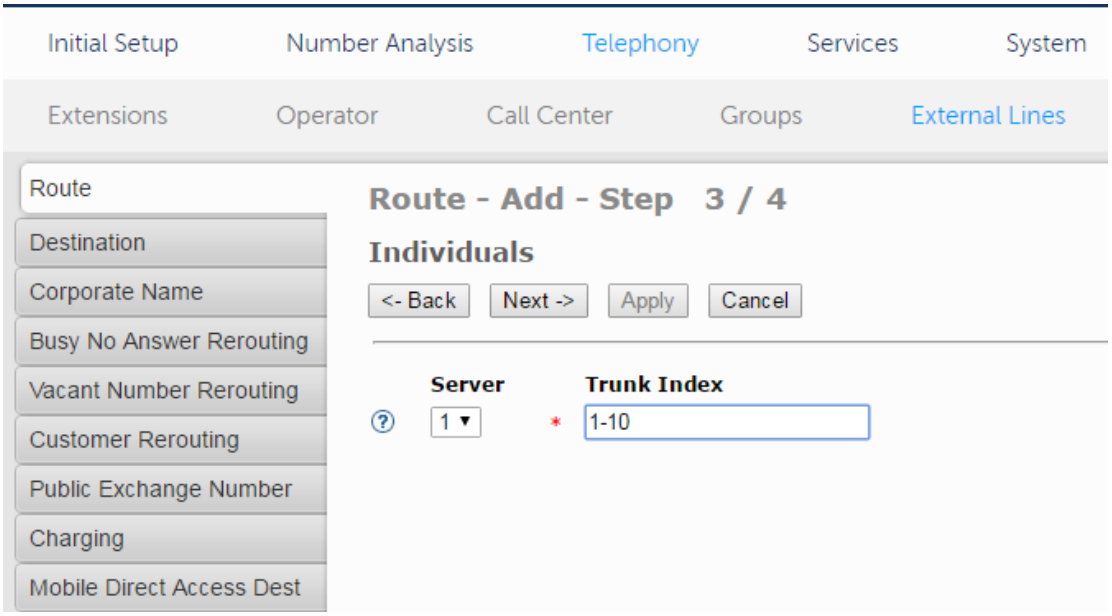
4. In the **Profile name** field, select **InAttend** from the drop-down list.



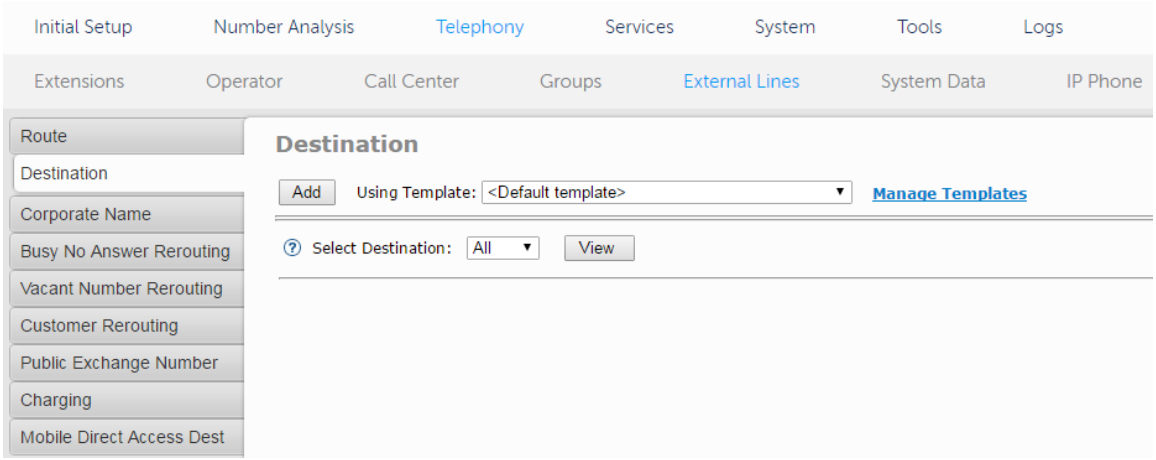
5. Enter the Route settings using the information provided in the Help screen.
6. Click **Apply**. (For MX-ONE from 6.1 SP1):



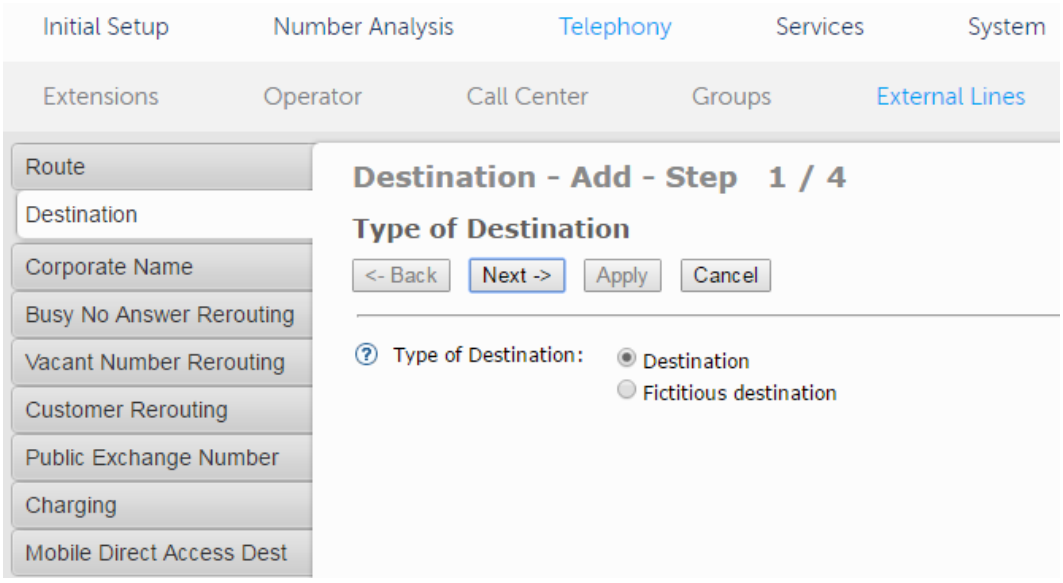
7. On the confirmation page, click **Done**.



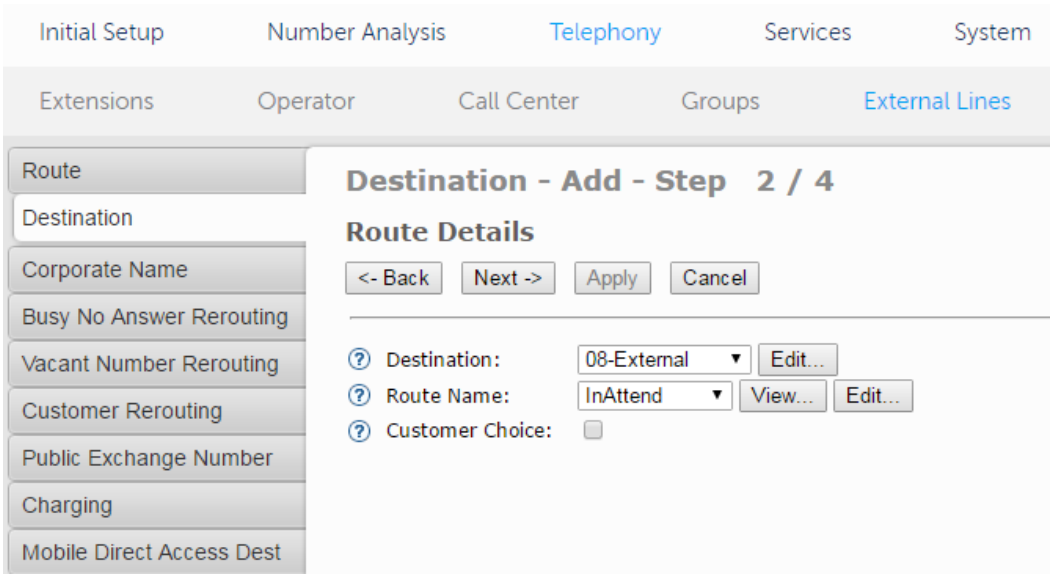
8. To associate the external numbers with the InAttend route, click **Destination** in the left panel, and then click **Add** on the Destination page.



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

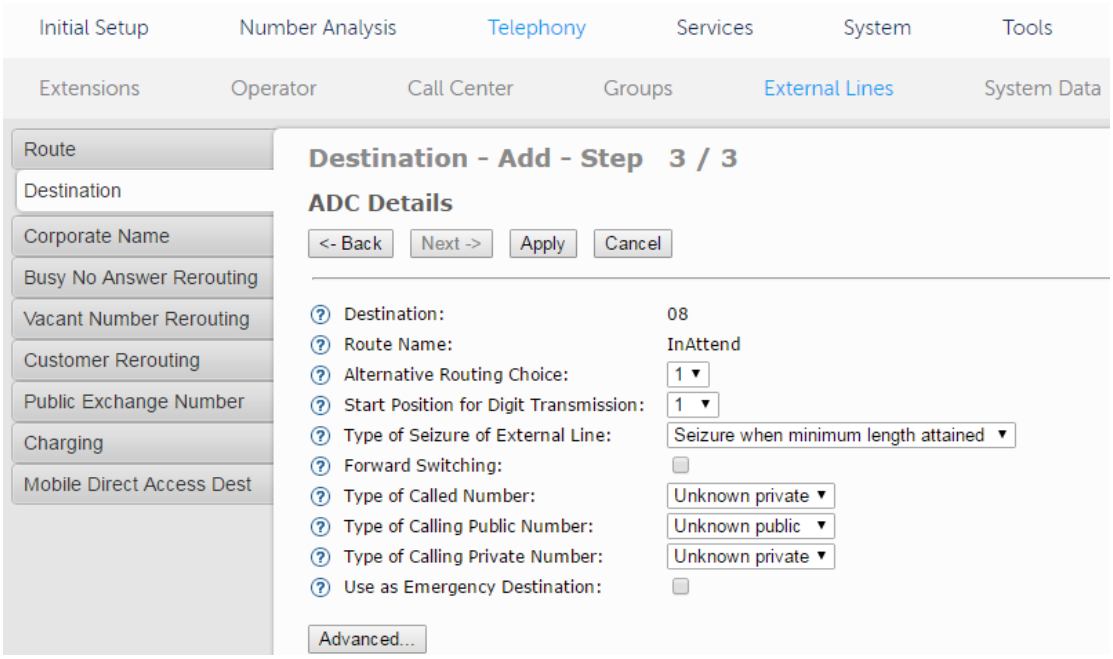


11. On the Route Details page:
    a. Select the destination number from the list in the **Destination** field.
    b. Select InAttend from the list in the **Route Name** field.
    c. Click **Next**.

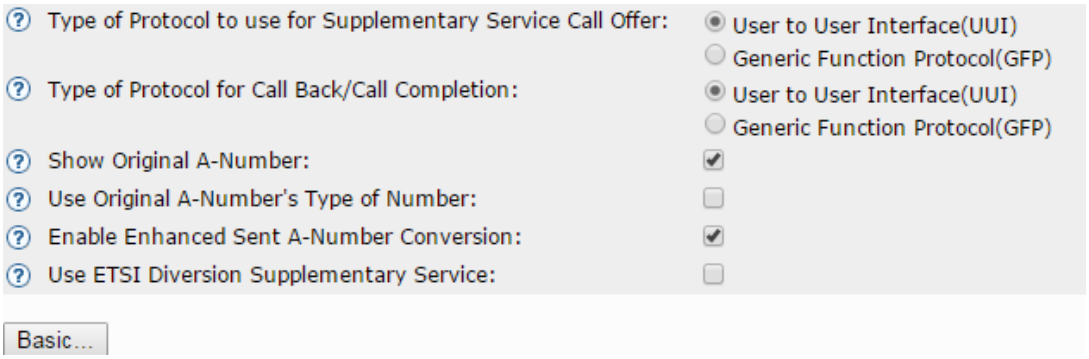


12. On the ADC Details page:

    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**.



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



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:

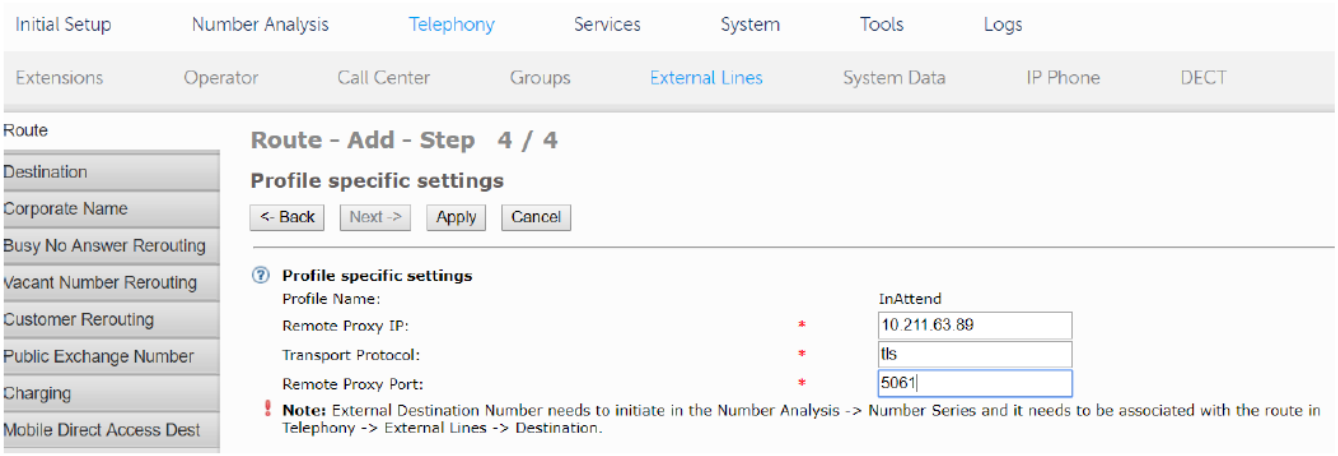
- Certificate handling for MX-ONE is not covered in this document. Please refer to the Certificate Management document in the MX-ONE product documentation.
- FQDN of InAttend Server should be added in etc/hosts file of MX-ONE server. This is required for FQDN resolving and TLS call to work from MX-ONE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

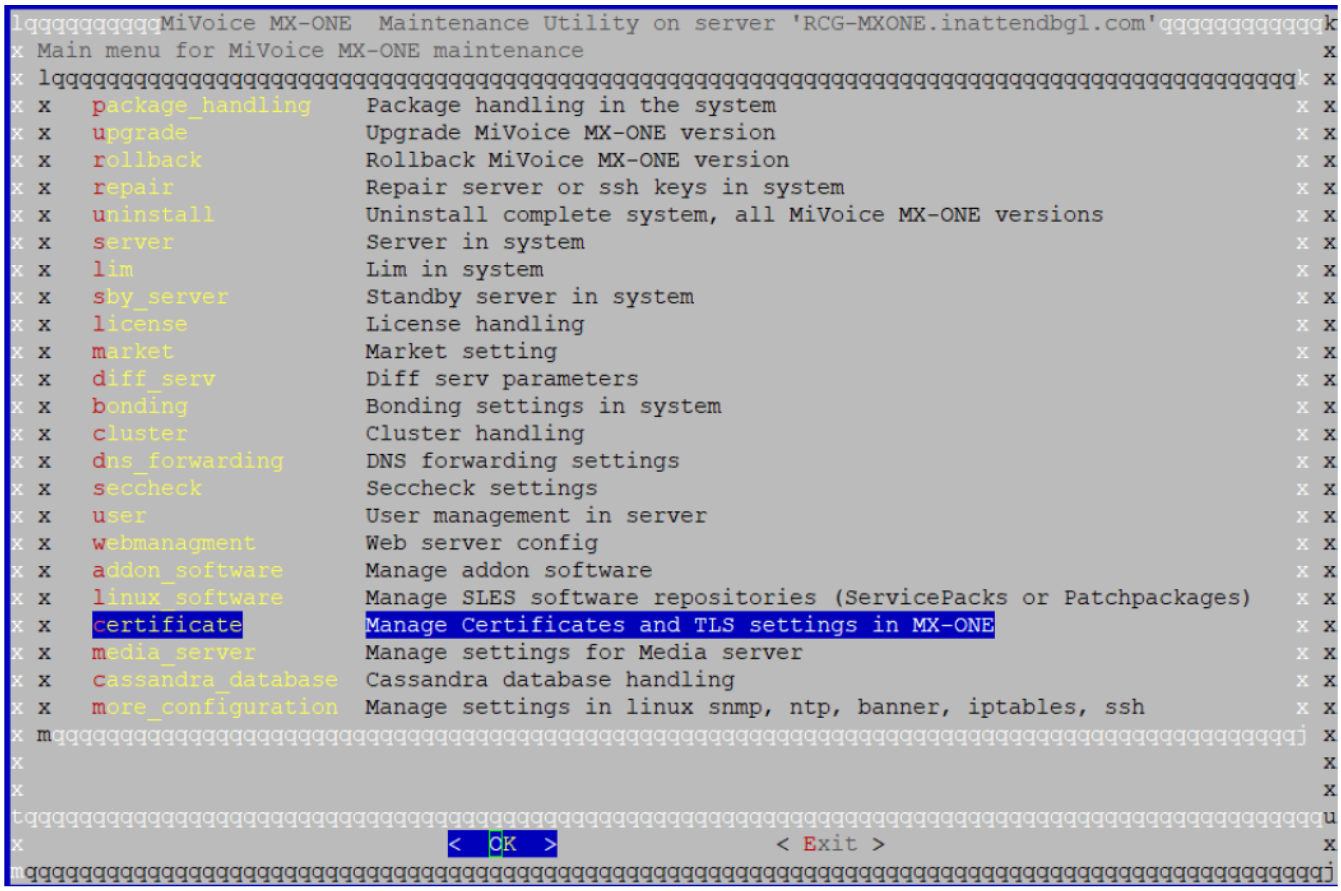


5. Click **Apply** to save your changes.

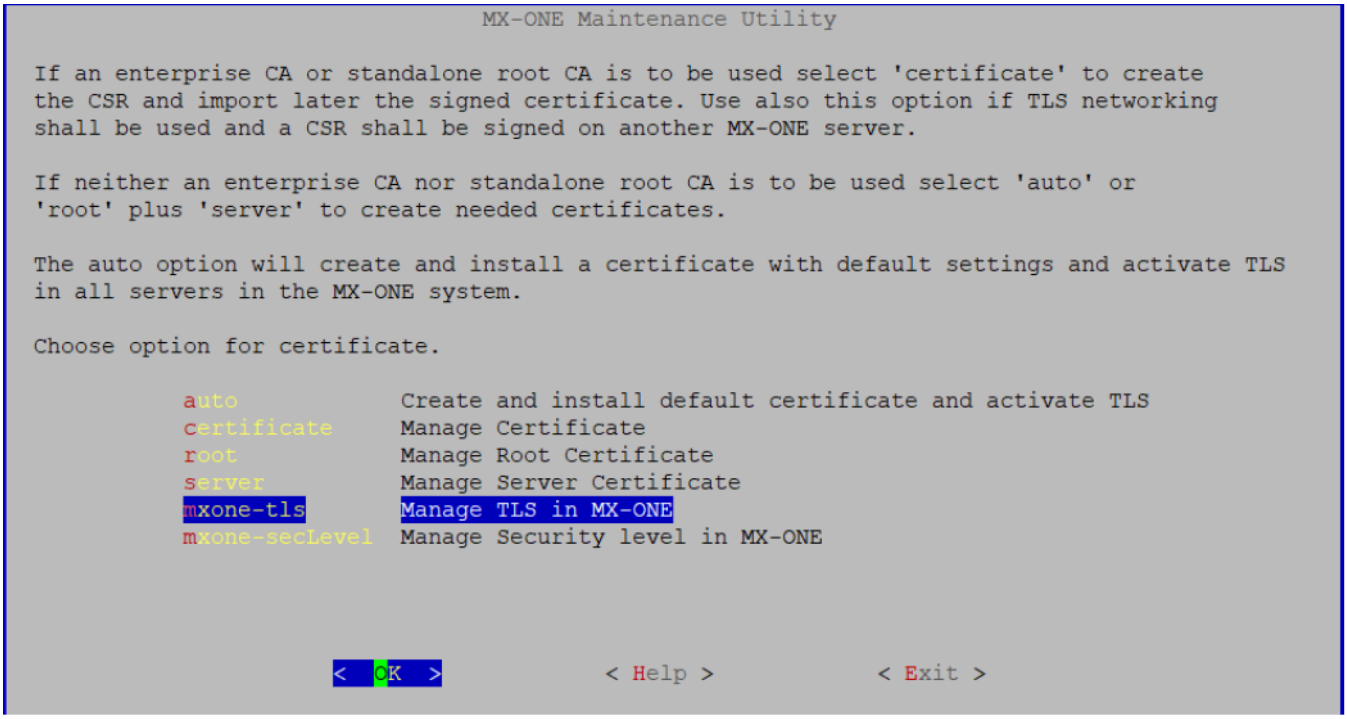
Using TLS v1 instead of SSL v23

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

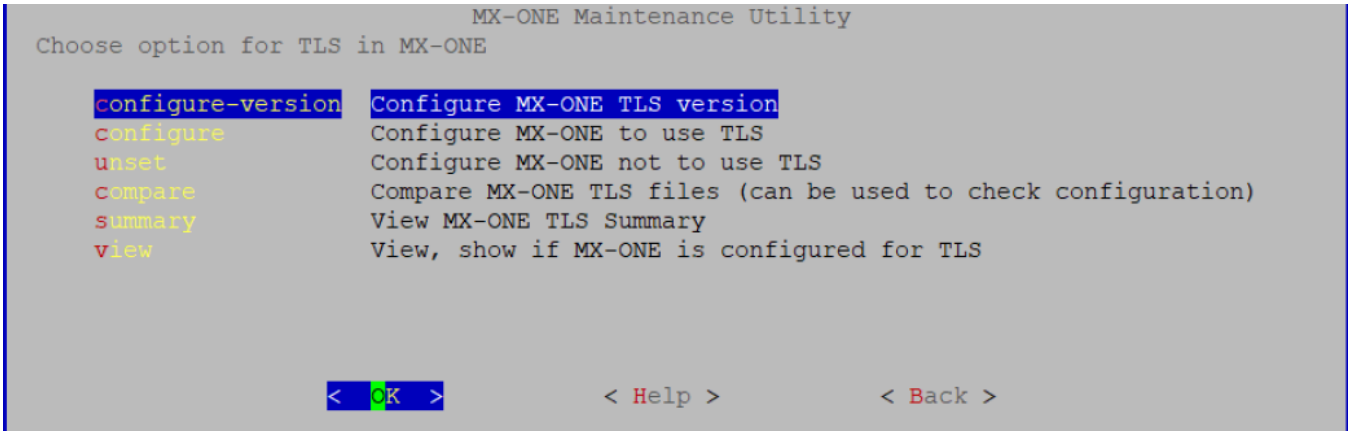
1. On the MX-ONE CLI, run the command `sudo -H /opt/mxone_install/bin/mxone_maintenance`
2. From the menu option, select **Certificate** and click **Ok**.



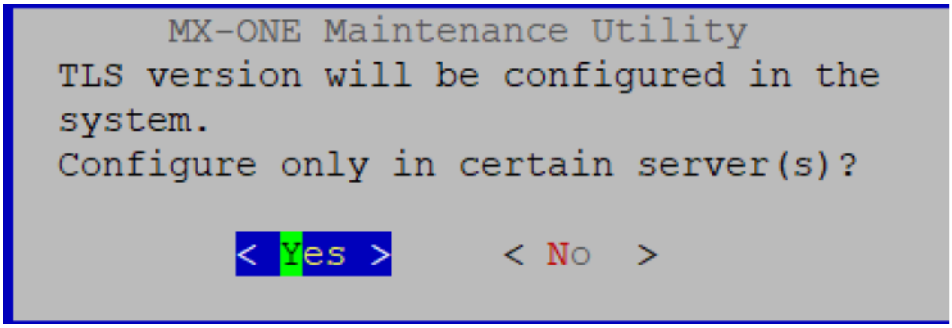
3. In the choose option for certificate menu, select **mxone-tls** and click **Ok**.



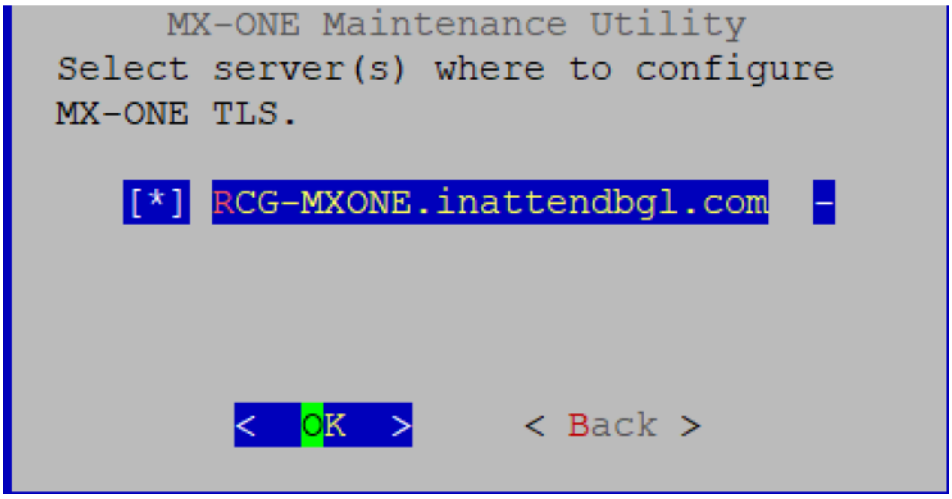
4. In the TLS in MX-ONE menu, select **configure-version** and click **Ok**.



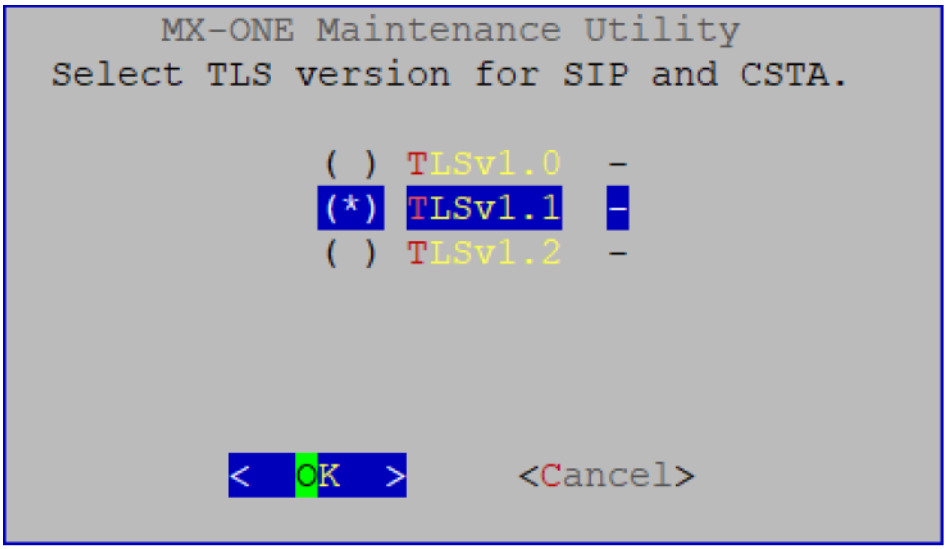
5. The MX-ONE maintenance utility dialog is displayed. From the menu, click **Yes**.



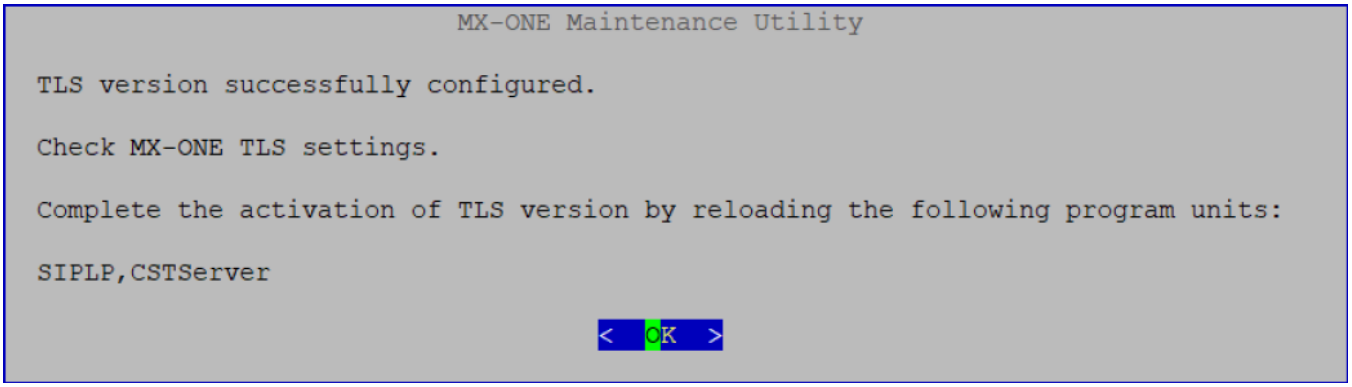
6. To select the server to configure TLS, select **MX-ONE** and click **Ok**.



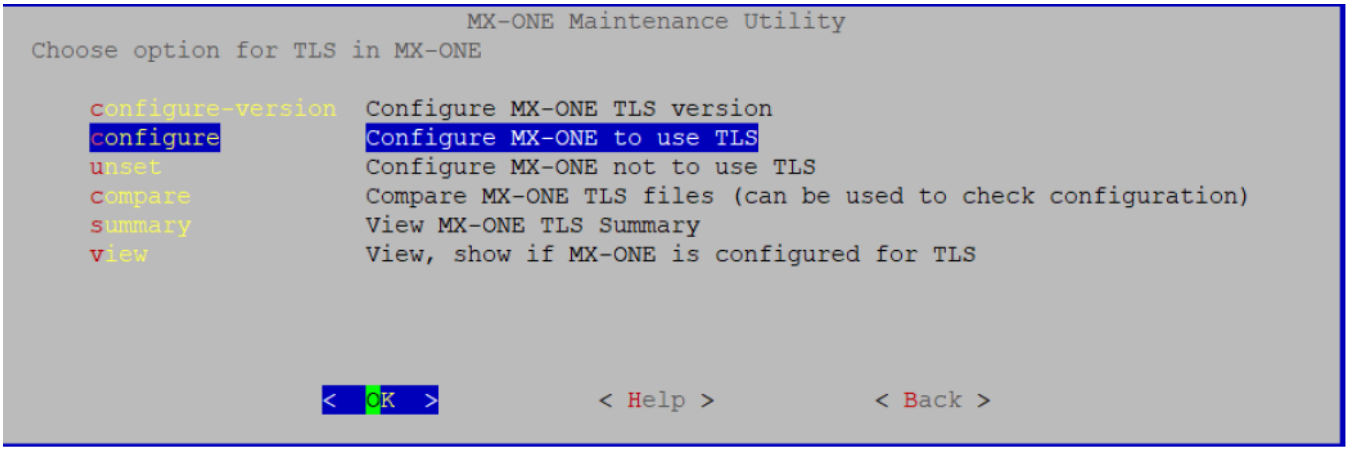
7. In the TLS version menu, select **TLSv1.1** and click **Ok**.



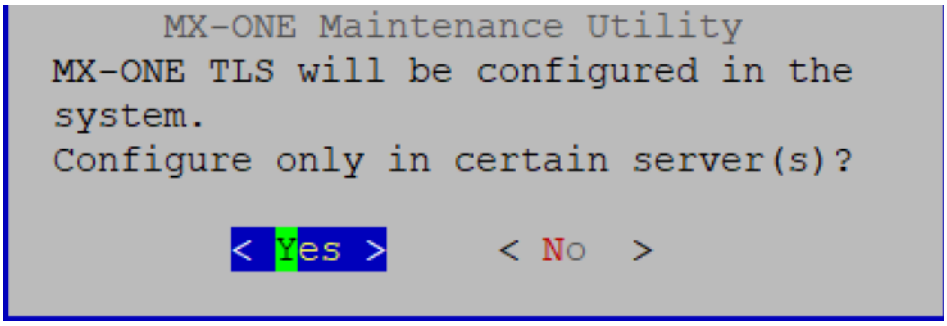
8. The TLS version successfully configured window is displayed. Click **Ok** to proceed further.



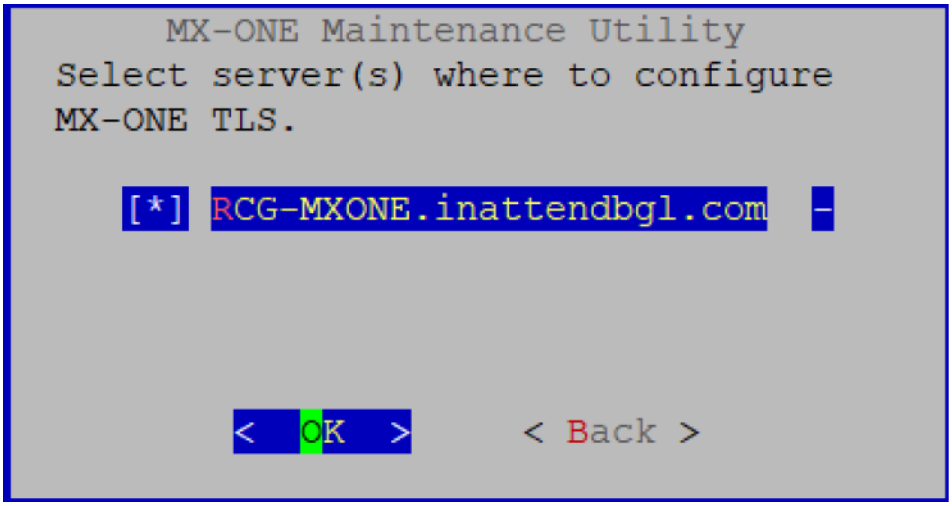
9. The next steps follow the configuration of MX-ONE TLS. To proceed select **MX-ONE to use TLS option** and click **Ok**.



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

                                  <  OK  >
```

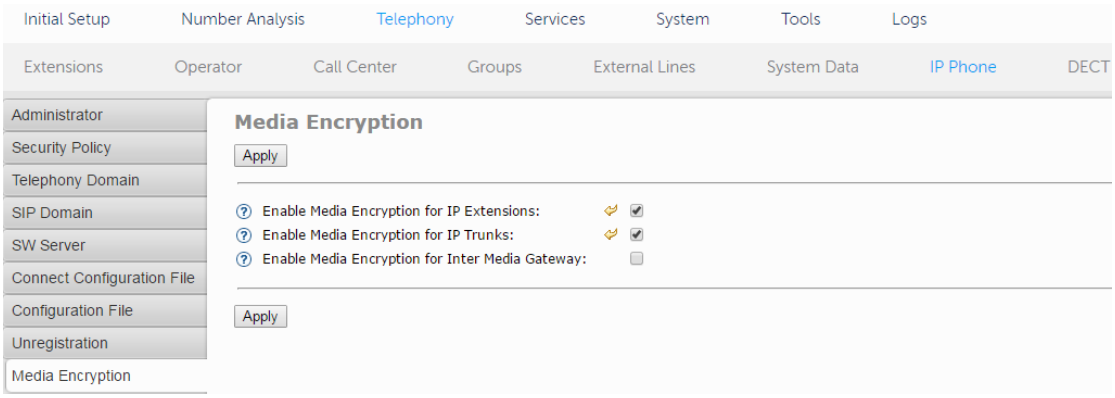
NOTE: To generate CSR from InAttend Server, see section Generate CSR in ACS.

Configuring SRTP on MX-ONE

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

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**



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

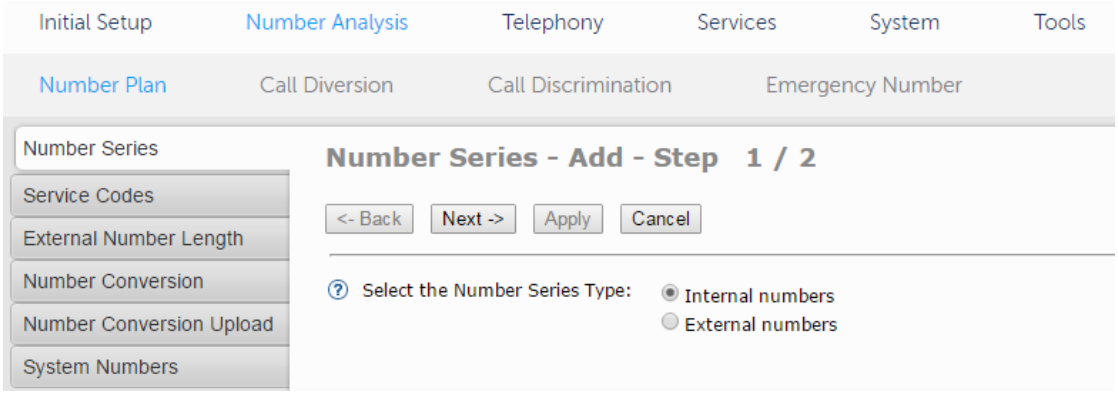
Configuring Day/Night Service Positions

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.

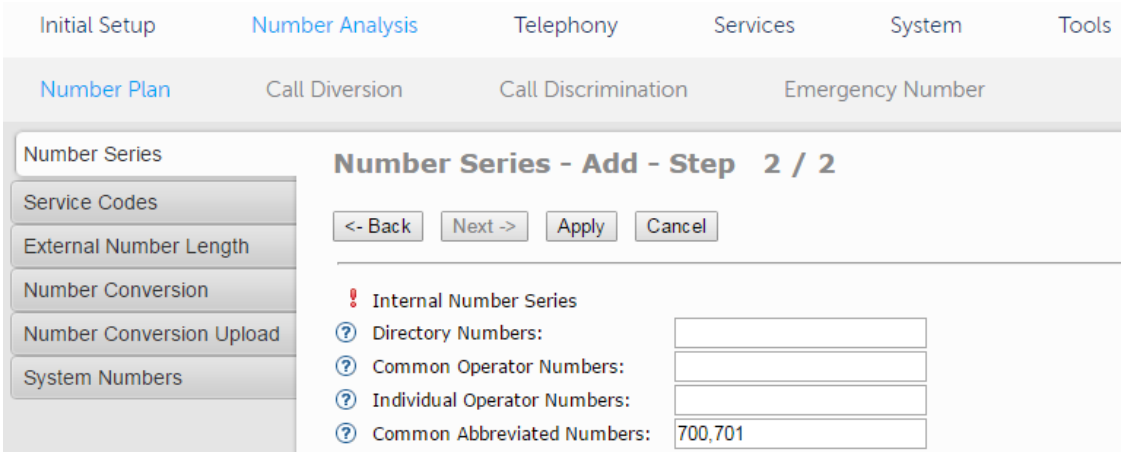
Initiating the abbreviated number series

To initiate the abbreviated number series, do the following:

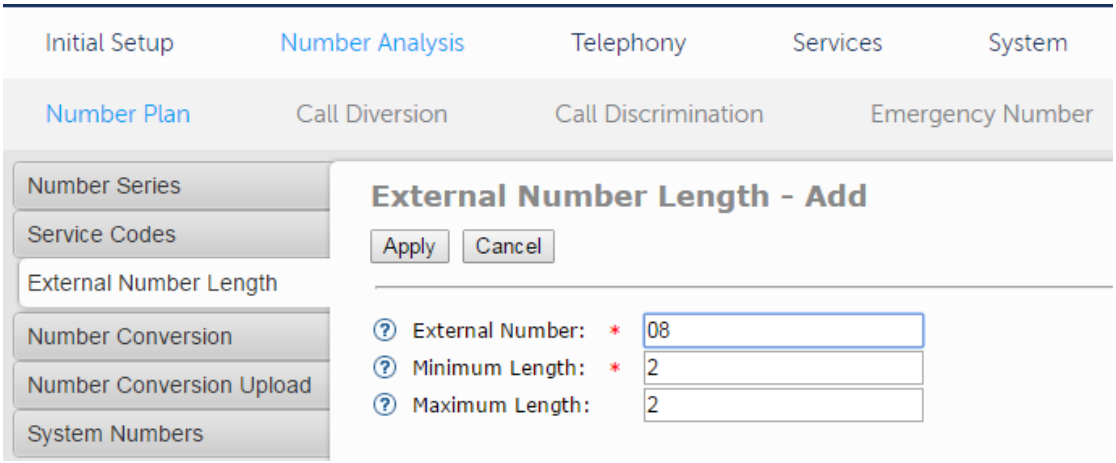
1. On the MX-ONE Service Node Manager main page, click **Number Analysis** then click the **Number Plan** tab.
2. Click **Number Series** in the left panel.
3. Number Series page select “Internal numbers” in **Number Series Type** field, click **Next**.



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**.



Click the **External Number Length** tab on the left side.

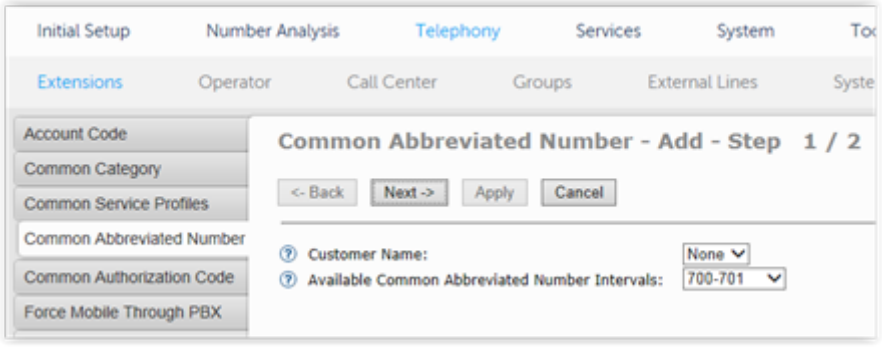


Enter the minimum and maximum length details and click **Apply.**

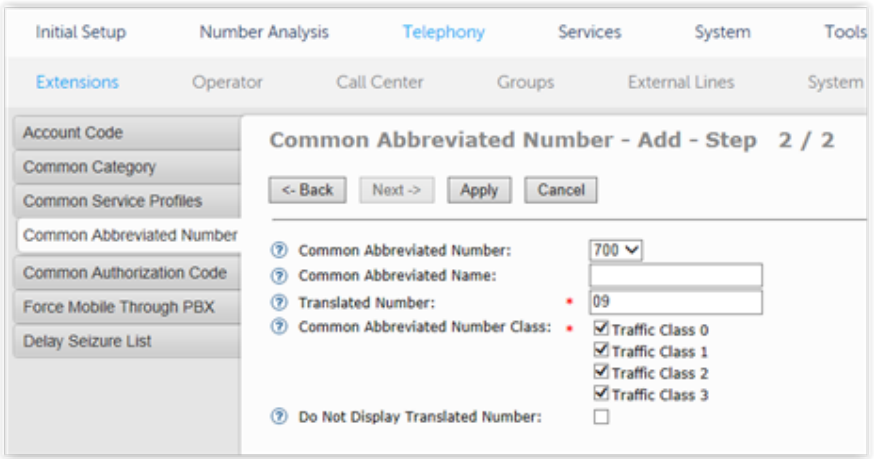
Initiating the abbreviated numbers

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**.



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



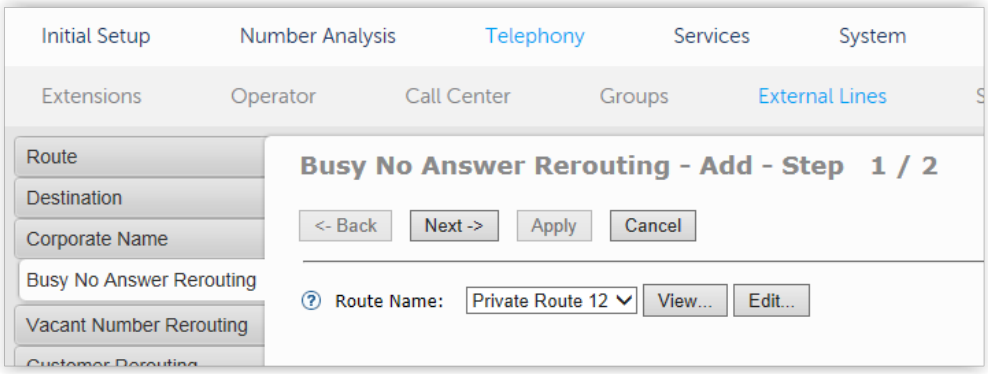
5. Click **Apply** to save your changes.
6. Repeat steps 1 through 5for the PBX main number

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

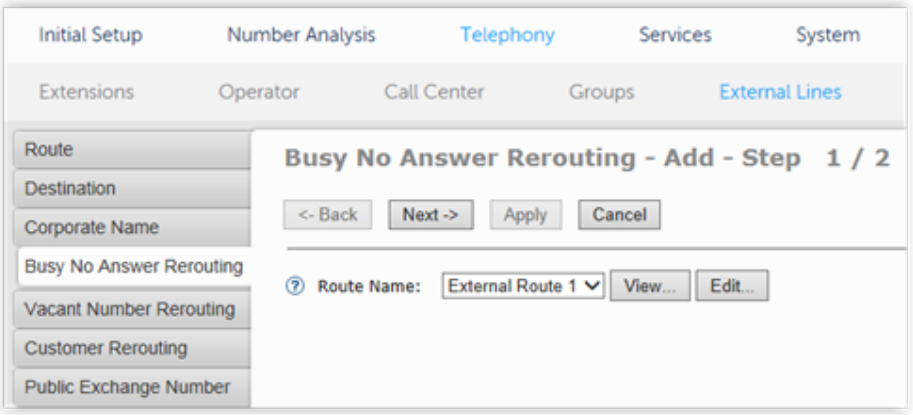
Initiating Day and Night Service Positions for a private route (internal call queue)

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**.



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

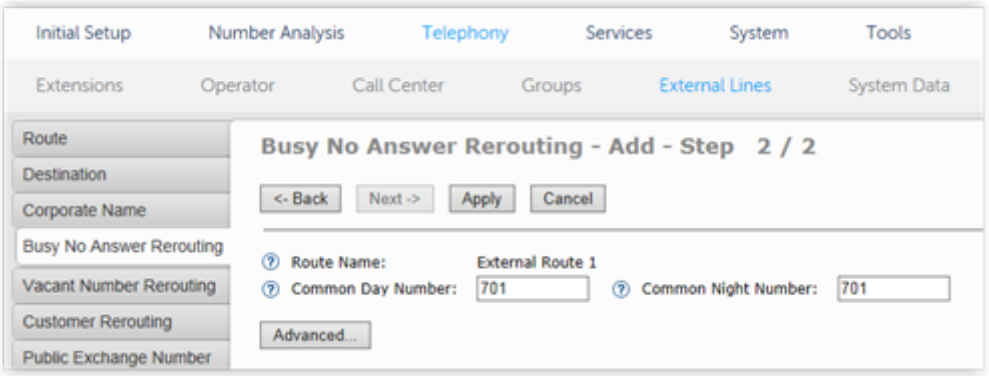


5. Click **Apply** to save your changes.

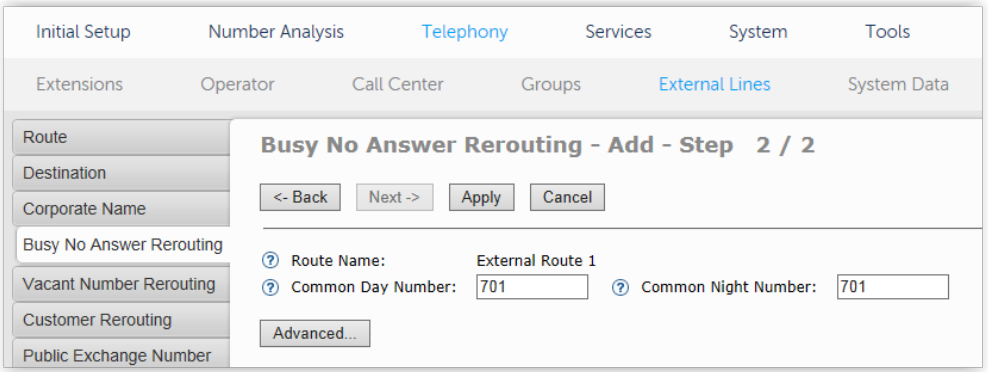
Initiating Day and Night Service Positions for a public route

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**.



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



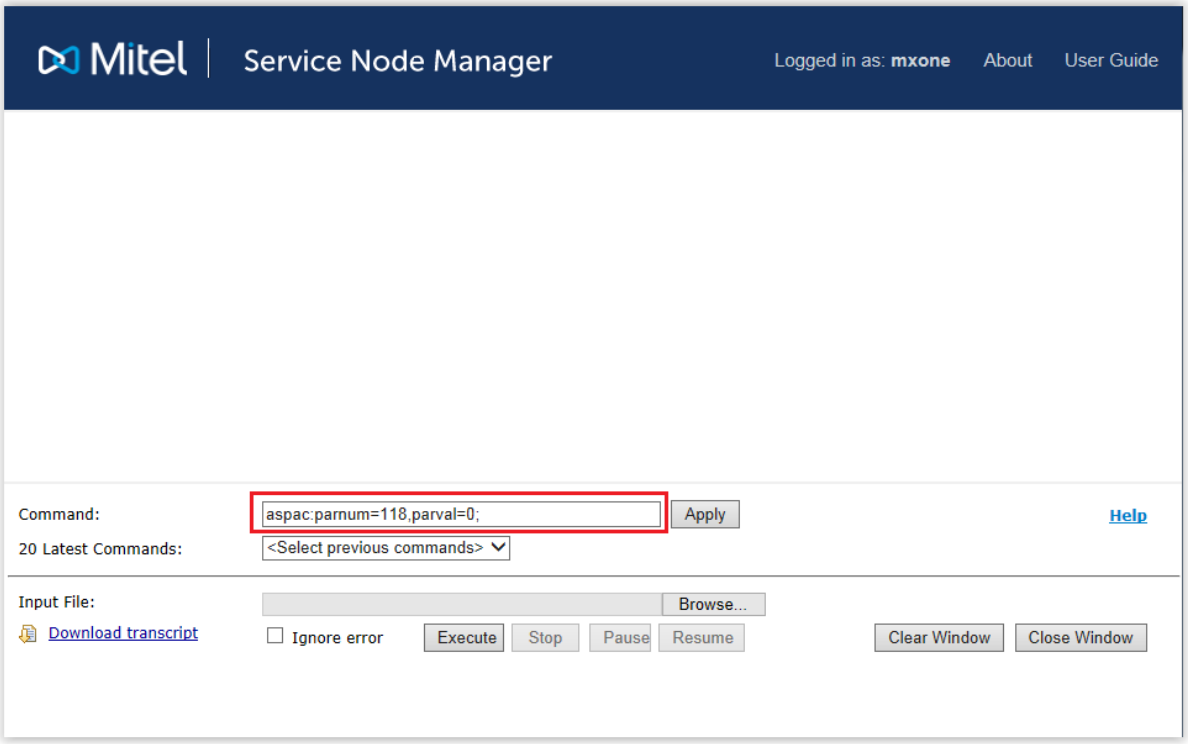
5. Click **Apply** to save your changes.

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.

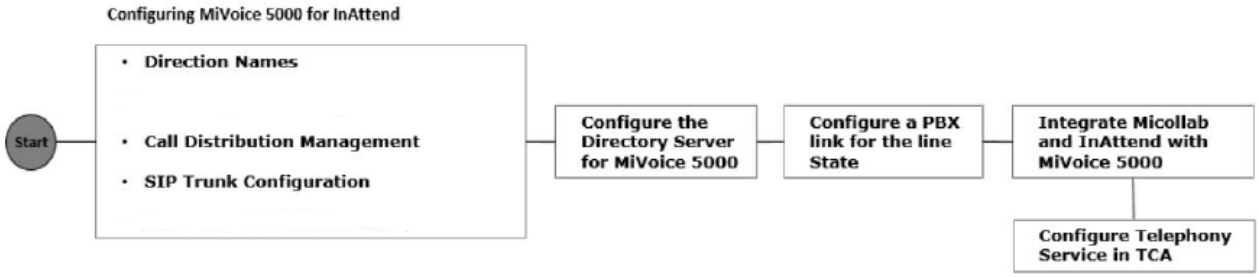


3. Click **Apply** to save your changes.

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)

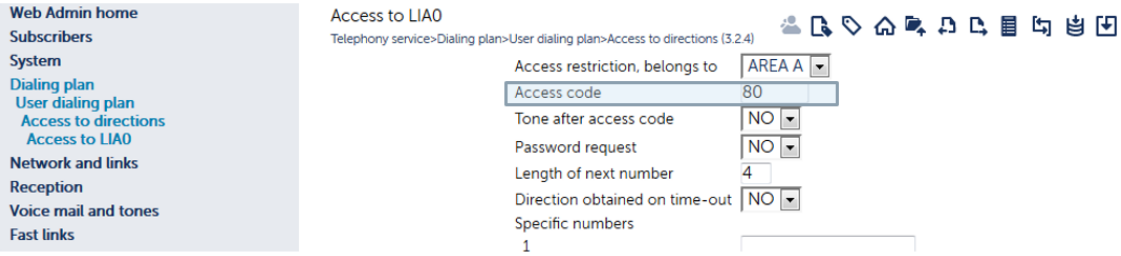
MiCollab and InAttend with MiV5000

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.



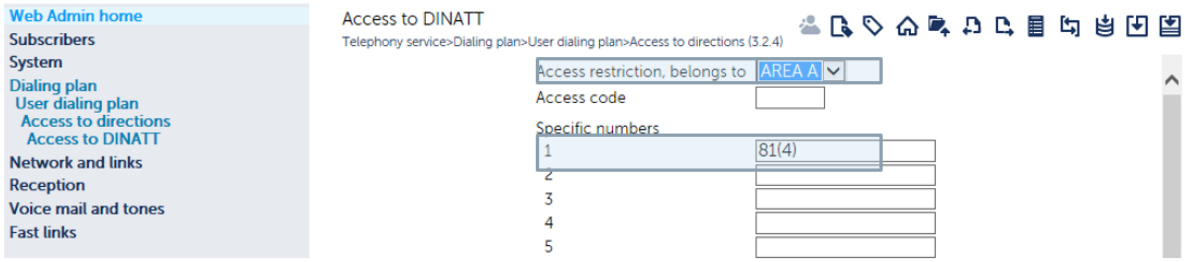
Create a private direction for InAttend, for example **DINATT** as private direction for InAttend.

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

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



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.

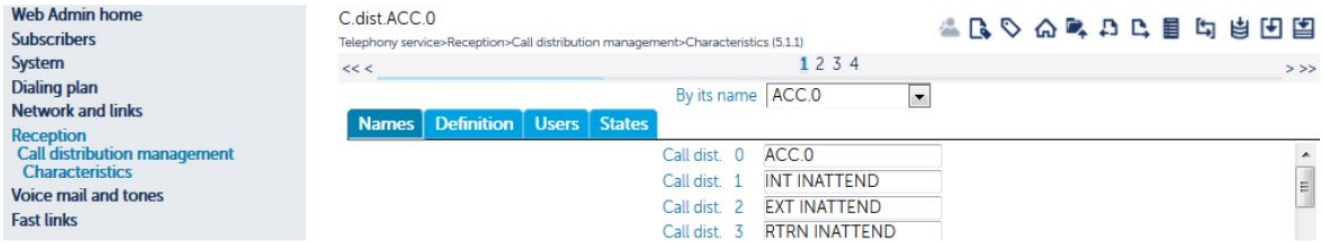
Programming Call Distribution for InAttend Services

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.

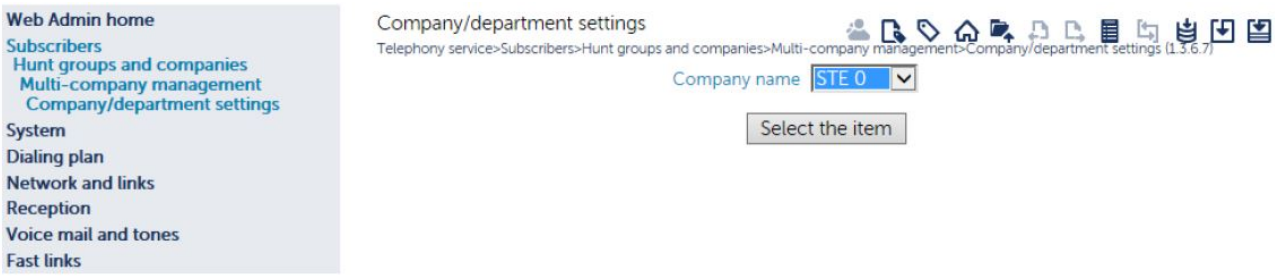
Three Queues are configured in InAttend Services

- 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**



To configure queue:

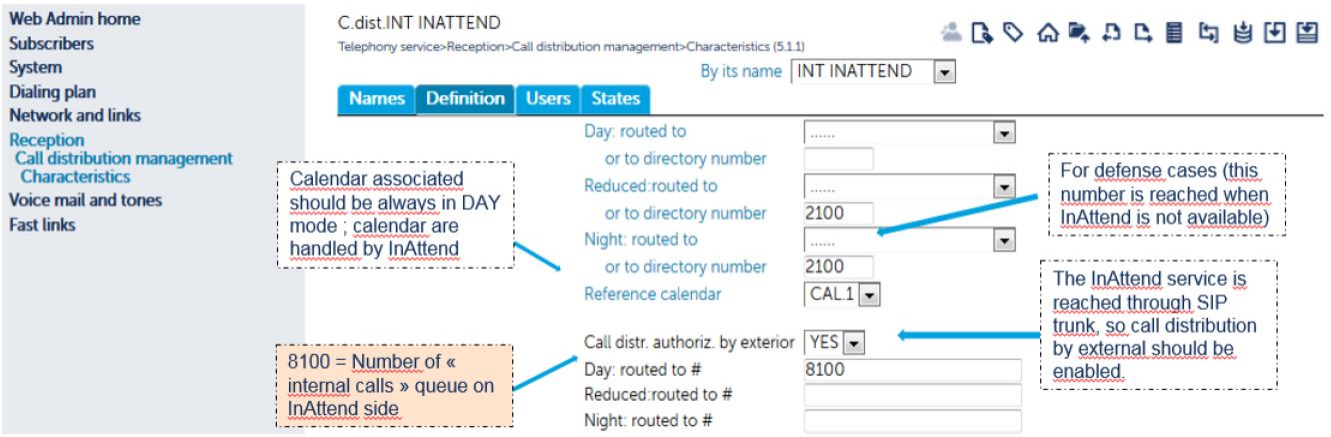
1. In canonic configuration, the prefix to reach the attendant service is 9. It is configured in the **User dialing plan > Operator Call**.
   This prefix is used by all the subscribers irrespective of company or department.



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.



NOTE:

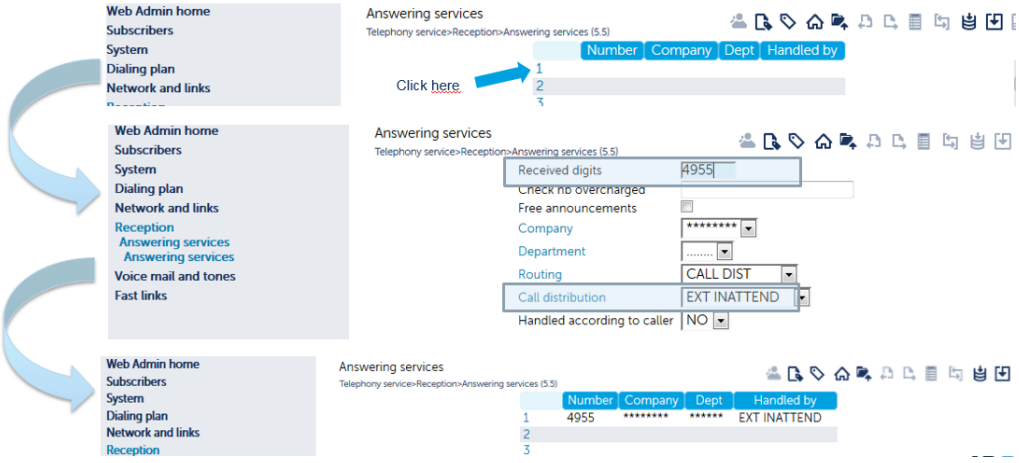
a. For external returned queue, Direct DDI calls are presented to subscribers. If the user is not reachable (busy or does not answer), the call returns to the distribution management associated to the company of the user.

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.



SIP Trunk Configuration

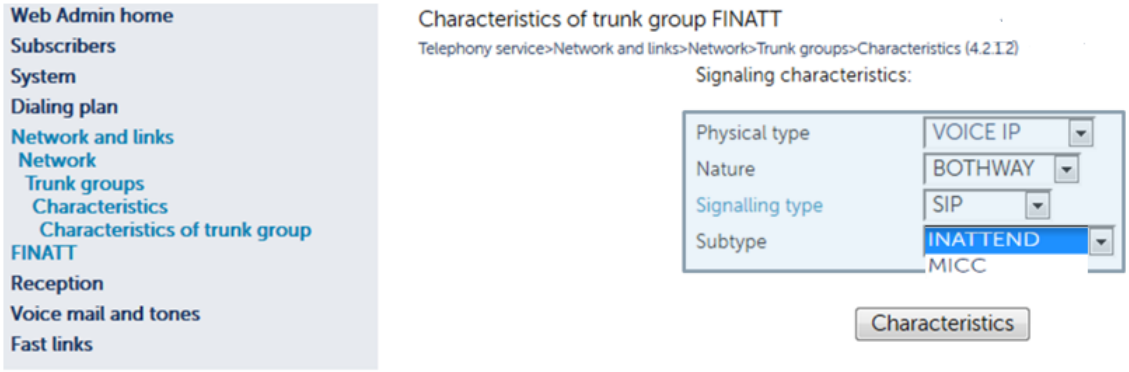
The  icon is used to change the configuration of a SIP trunk, you must use the **Advanced mode** for the SIP Trunk configuration.

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.

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.



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.

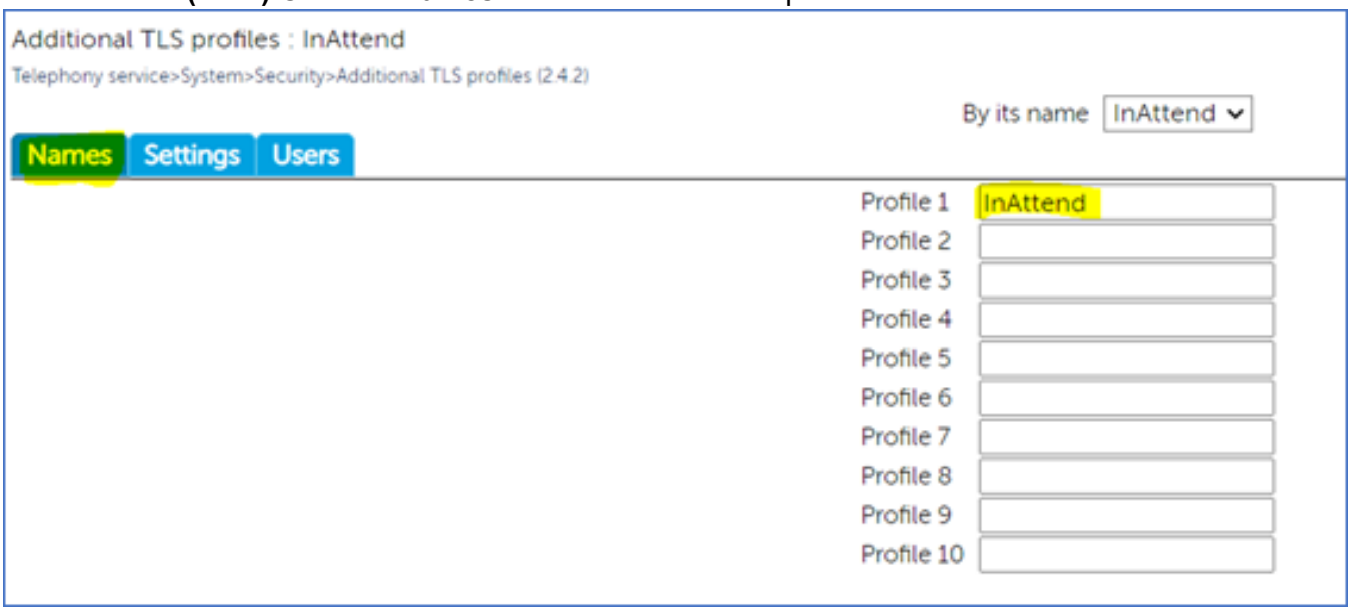
a. Set **TLS** as the protocol from the **Protocol** drop-down list.

b. Secure the SIP trunk with InAttend, a trusted certificate is mandatory for securing.

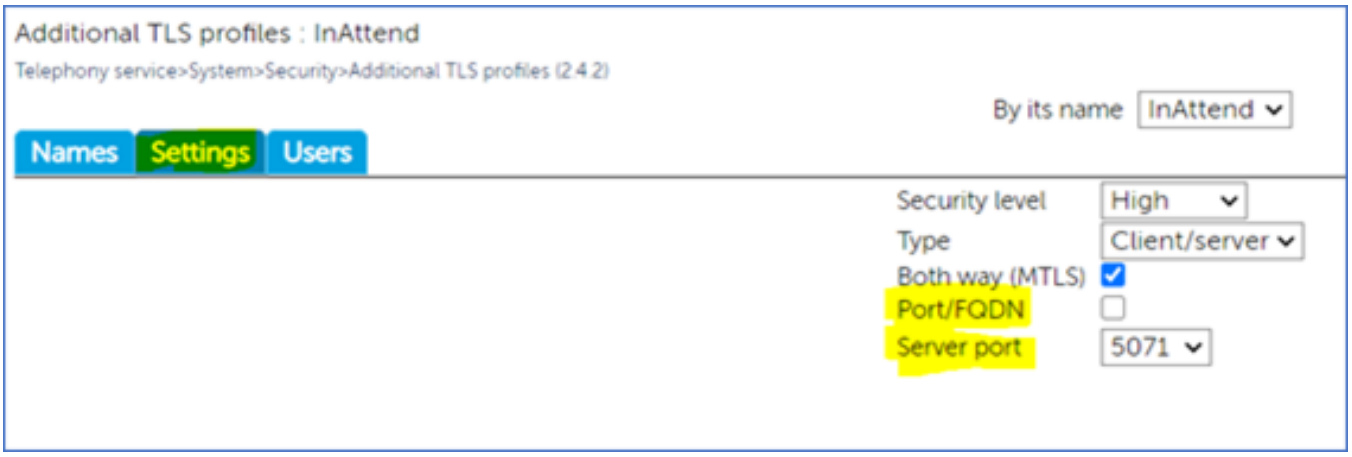
- IIf the default SIP profile (used by the SIP terminal) uses a trusted certificate, it can be used for the InAttend trunk group. No specific TLS profile need be created for InAttend.
- If the default SIP profile uses a self-signed certificate, you must create a TLS profile for the InAttend trunk group.

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.

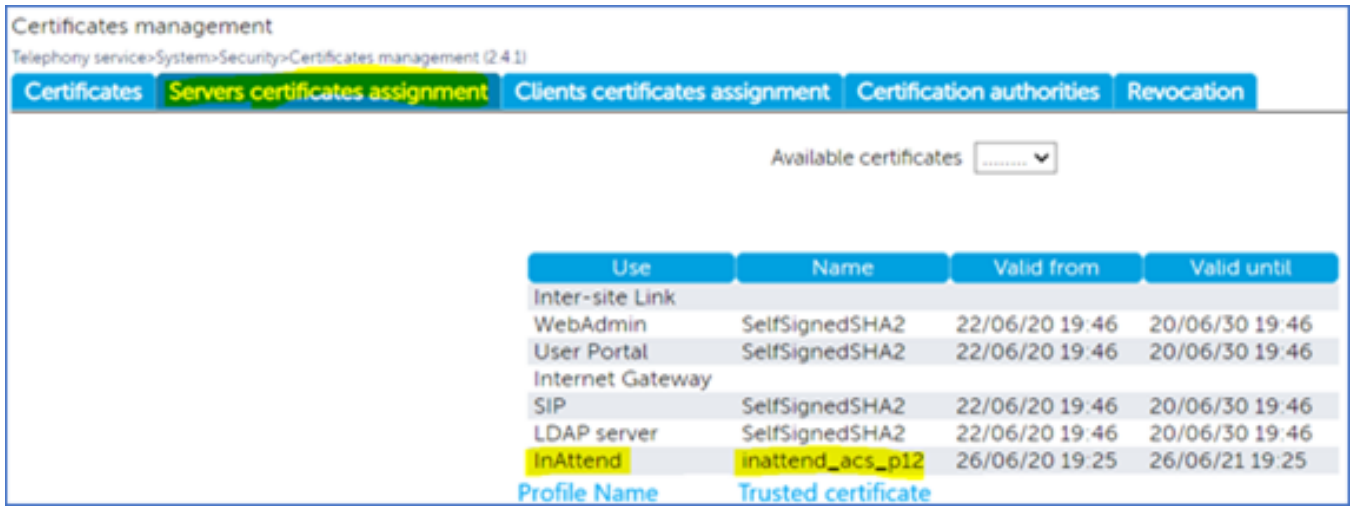


ii. Click the **Settings** tab and configure either the **Server port or Port/FQDN**to be used for trunk connections. Configure the other parameters such as **Security level, Type** and **Both way (MTLS).**



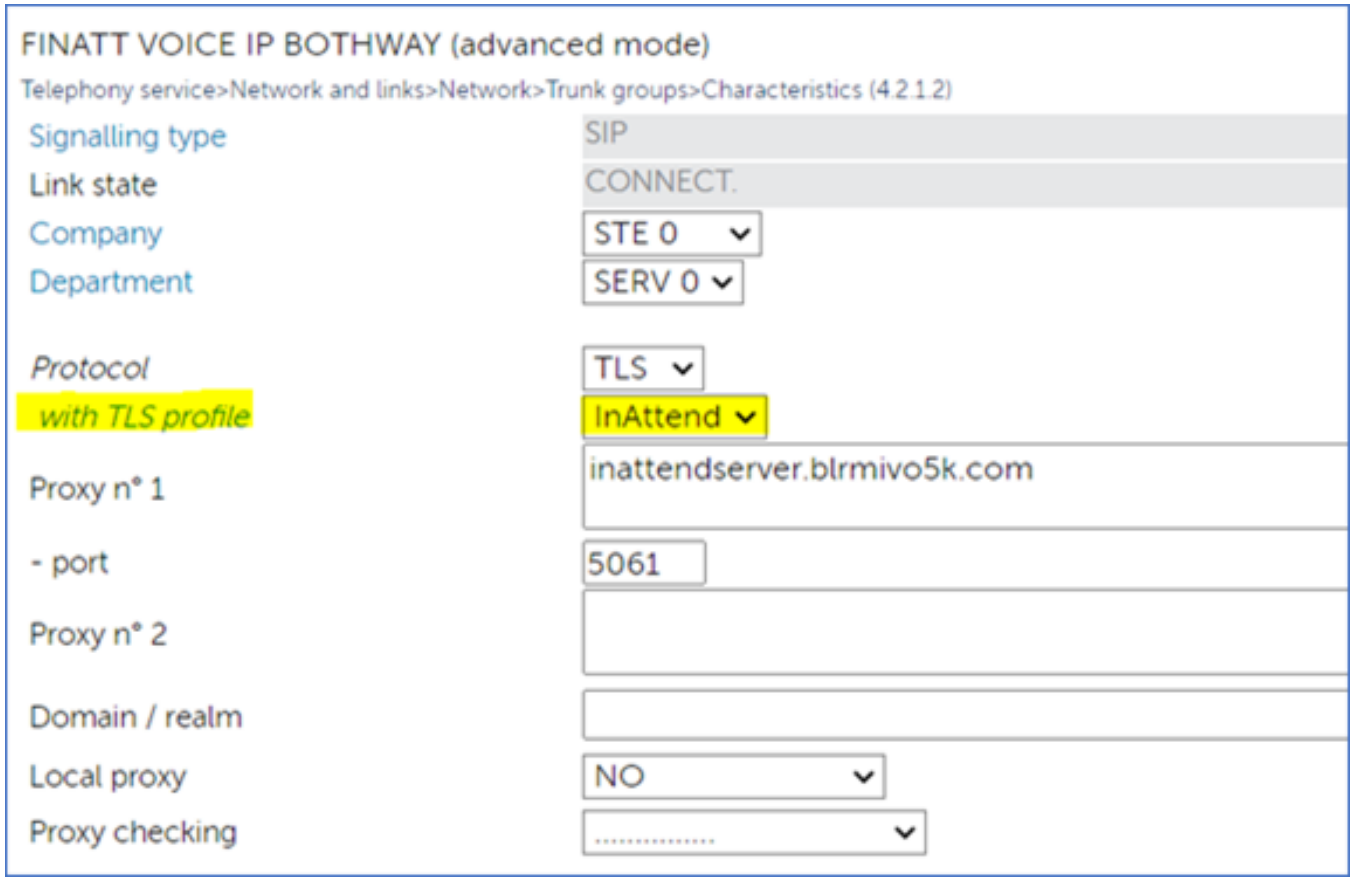
To assign the trusted certificate to the TLS profile:

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.

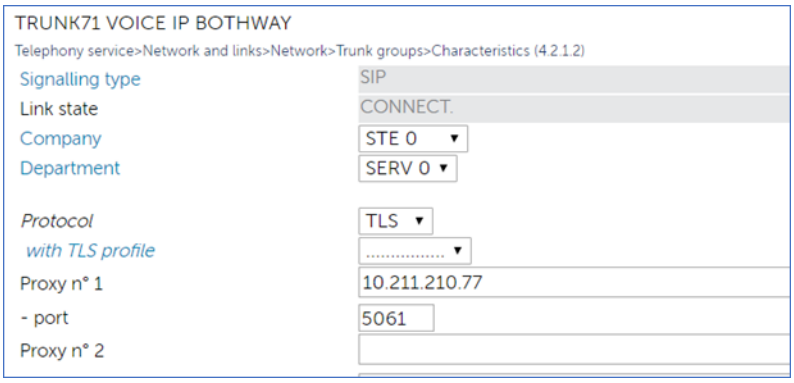


To assign the TLS profile to the SIP trunk configured with the InAttend server:

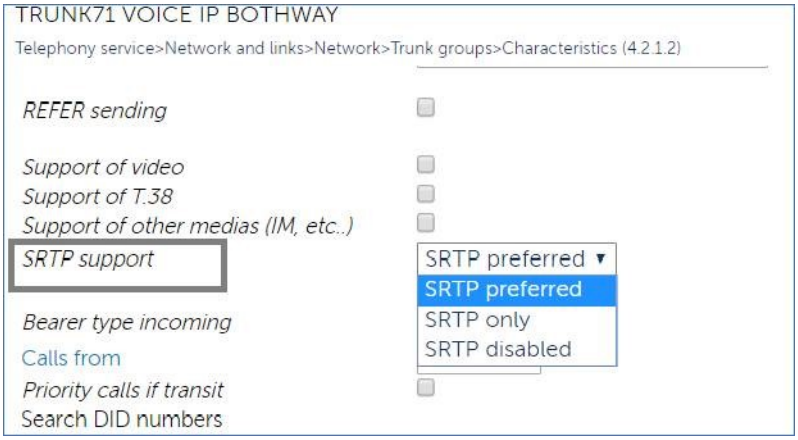
Go to PBX MMI **Telephony service > Network and links > Network > Trunk groups > Characteristics (4.2.1.2)** and select the TLS profile (configured in the preceding steps) in the trunk configuration.



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



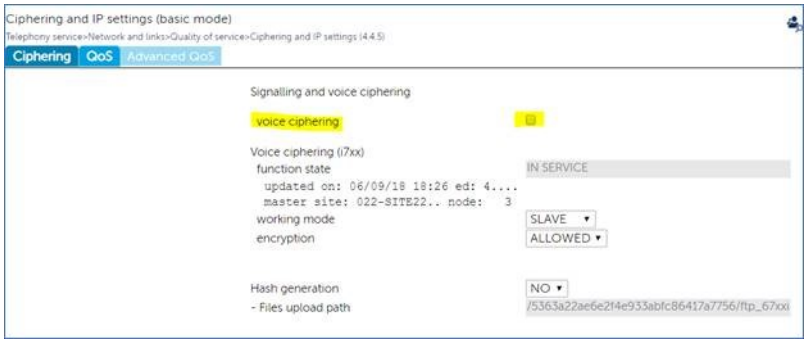
d. Once the protocol is set to TLS, **SRTP support** option gets enabled. By default, the value is set to **SRTP preferred**.



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

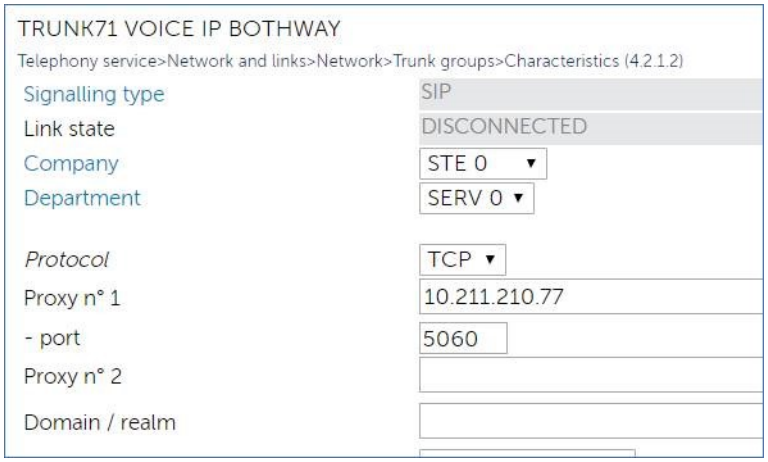
This parameter MUST also be set to enable SRTP between MiVoice 5000 and InAttend.



NOTE: SelfSigned certificate is not supported by InAttend.

SIP trunk configuration in TCP

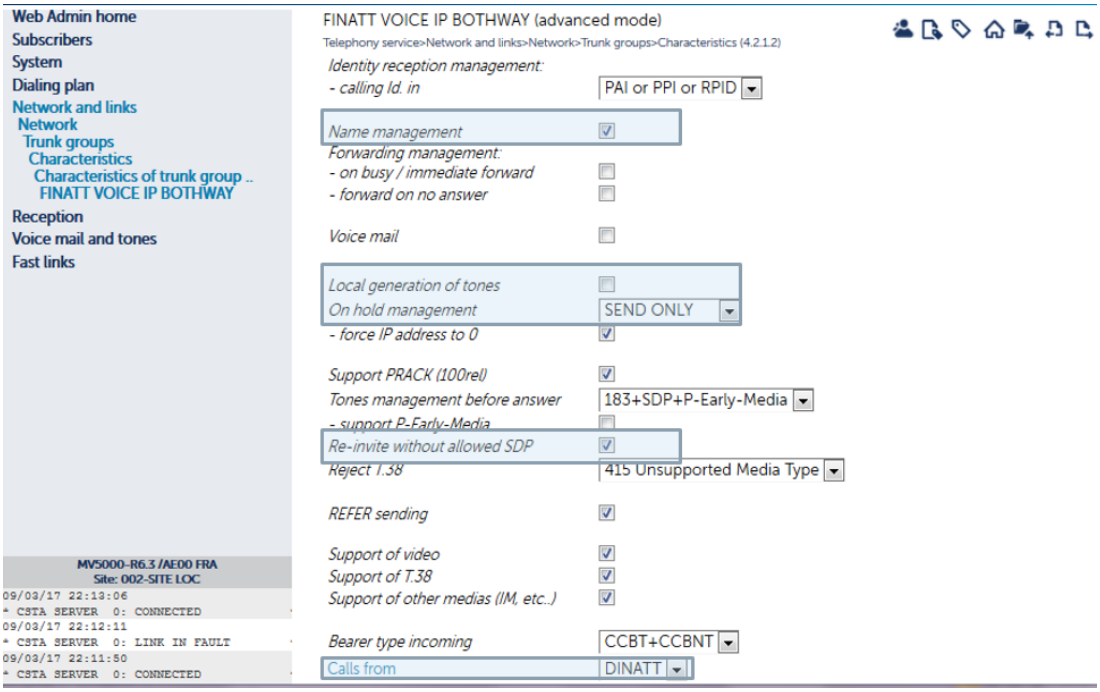
a. Set the protocol as **TCP** from the drop-down list.
b. Enter the proxy of InAttend server and port as 5060.

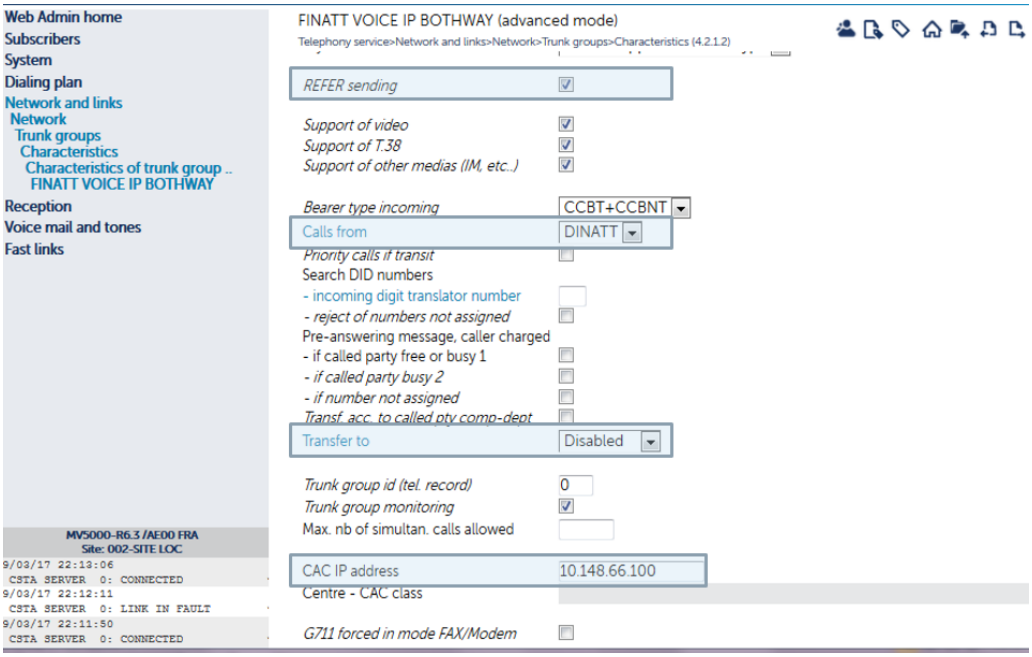


NOTE: With TCP as trunk protocol, SRTP support option is unavailable in trunk configuration.

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**.





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.

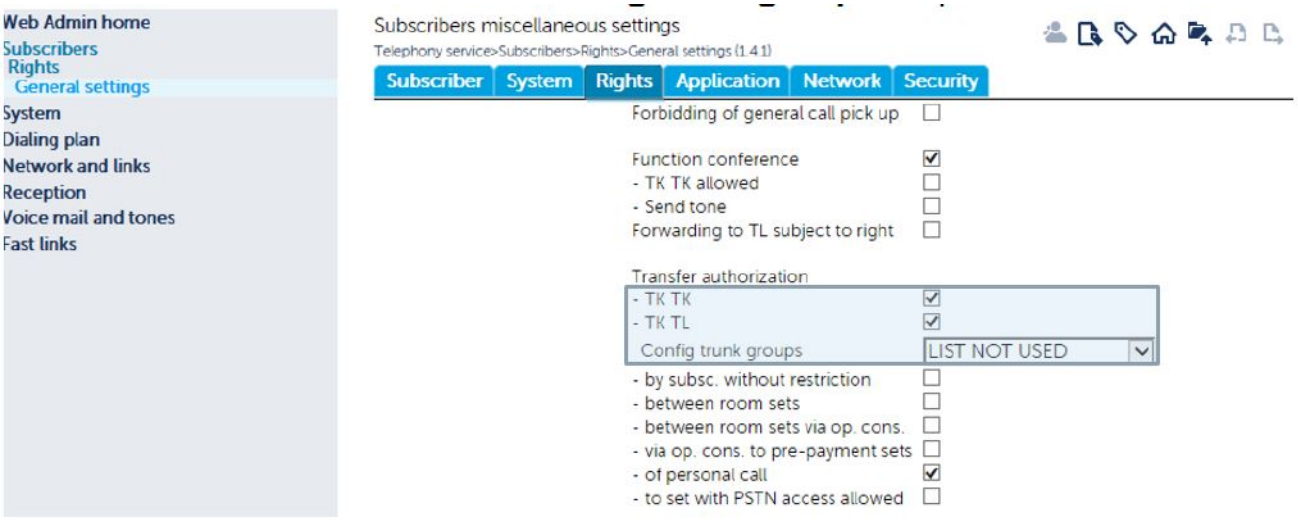
What to do Next

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.

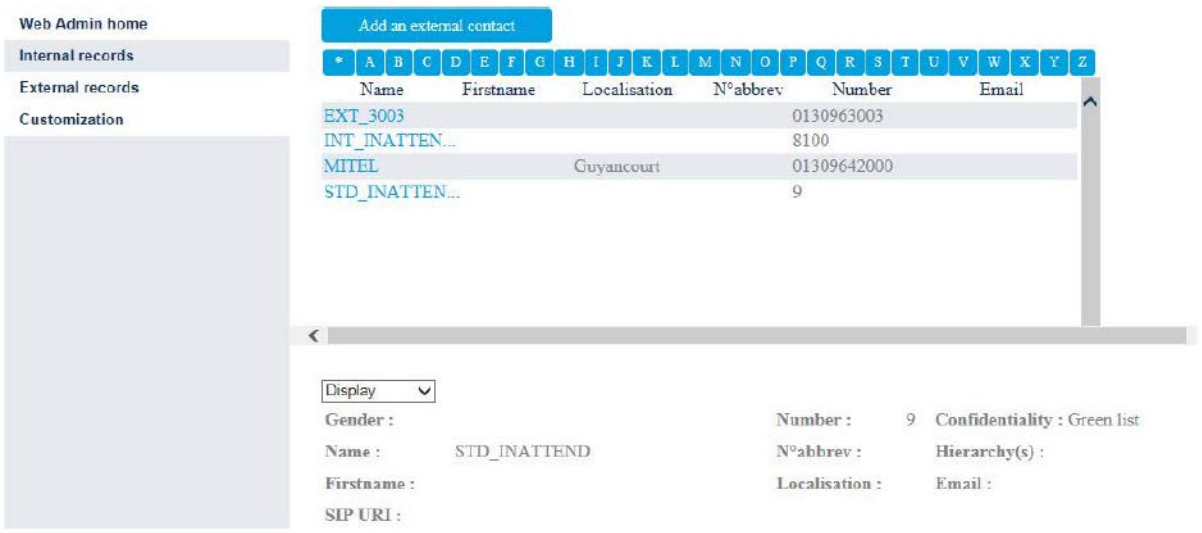


Configure Hardphone Subscriber

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

Create an External Record

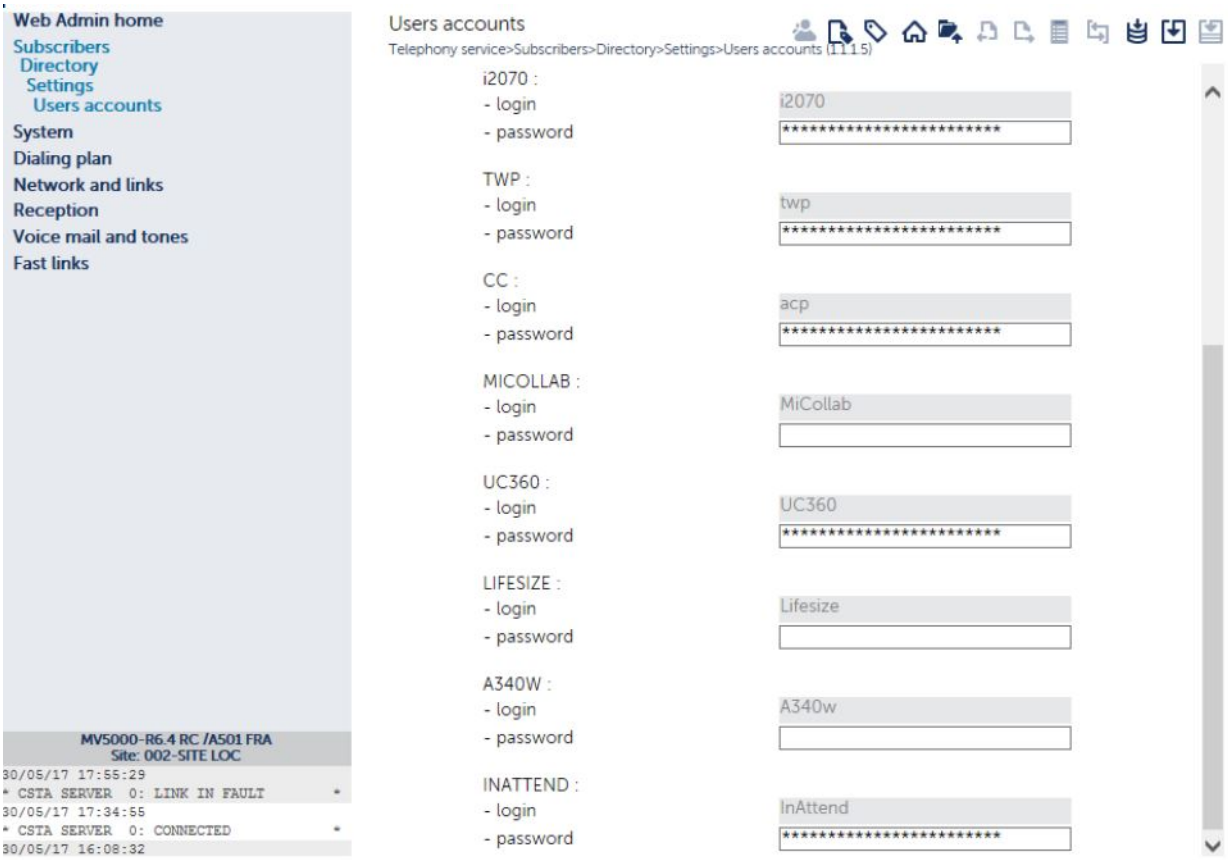
1. Go to, **Internal Records** and click **Add an external contact** to create a new external record. An external record number must be added with the **Internal Queue** number Name STD_INATTEND IN ORDER to display STD_INATTEND when INATTEND CLIENT CALLS a LOCAL SUBSCRIBER



Create Password

Create a password for InAttend account to access proxyldap

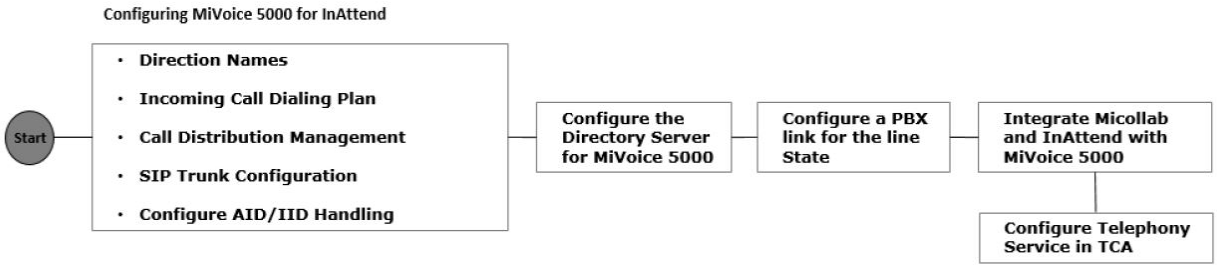
1. Go to **Subscribers > Directory > Settings > Users accounts** and set password for clients.



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

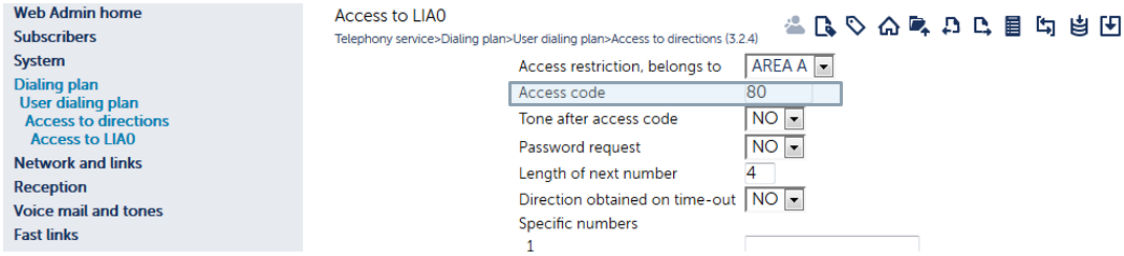
NOTE: This configuration is fully compatible with MiVoice 5000 release 7.2 and upper, and it will be kept in case of any upgrade from an older release.

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.

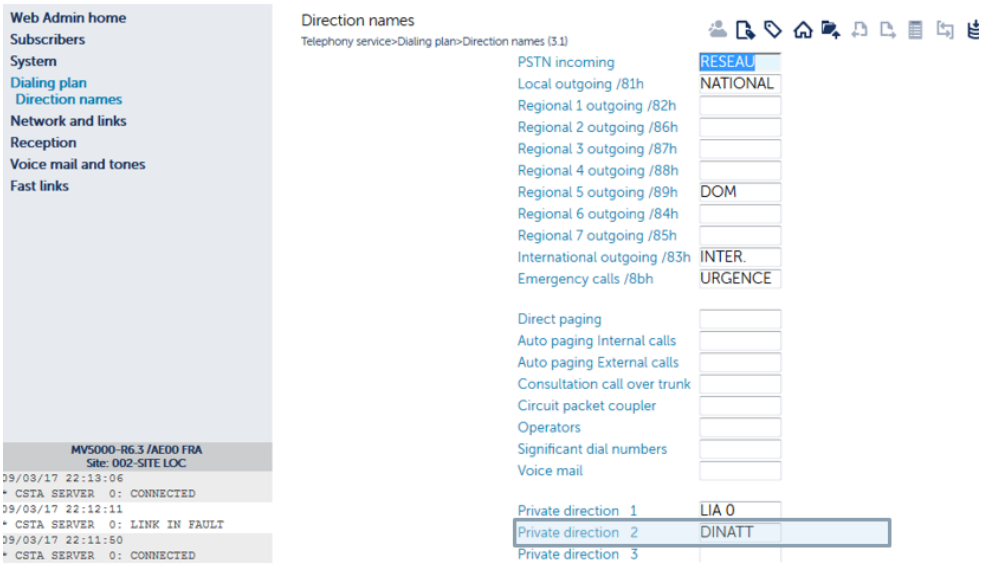
NOTE: By default, 8 allows access to LIA0, changing access code to 80 will allow 81* numbers.



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

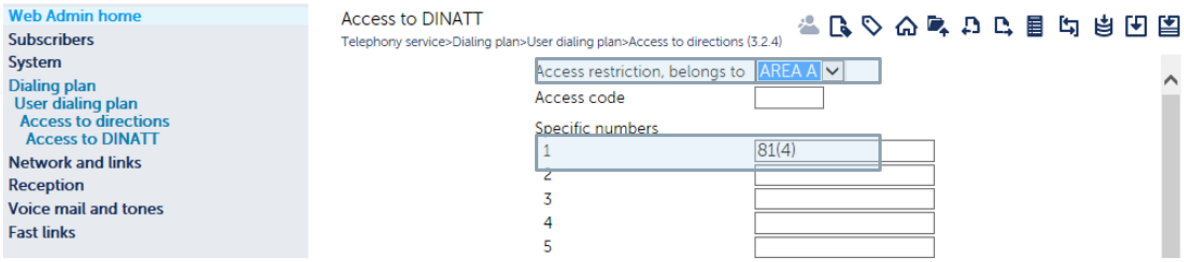
1. Go to **Dialing Plan > Direction names**.
2. Enter DINATT in **Private direction 2**.

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



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



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

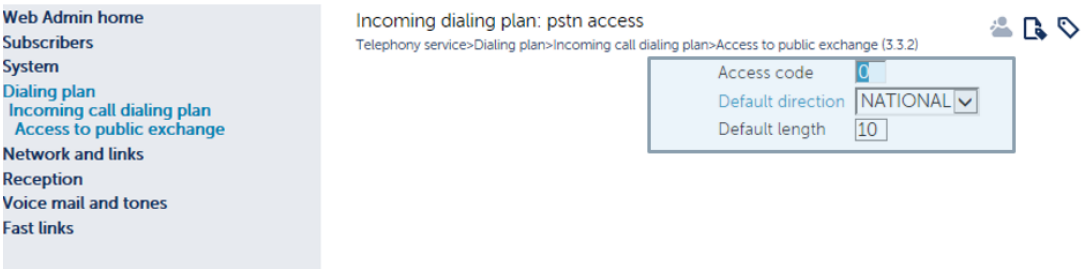
The incoming call dial plan is used to define the analysis made by the system for incoming calls from the network (DID and TL). This is used to modify and display the incoming call numbering plan.

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.



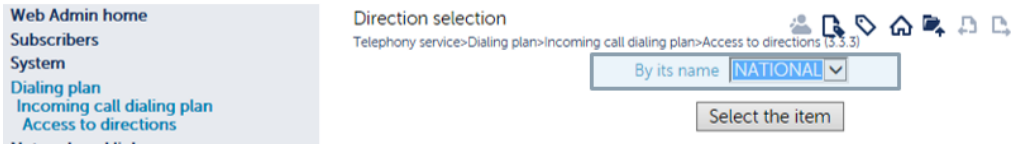
Access to Directions

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**.

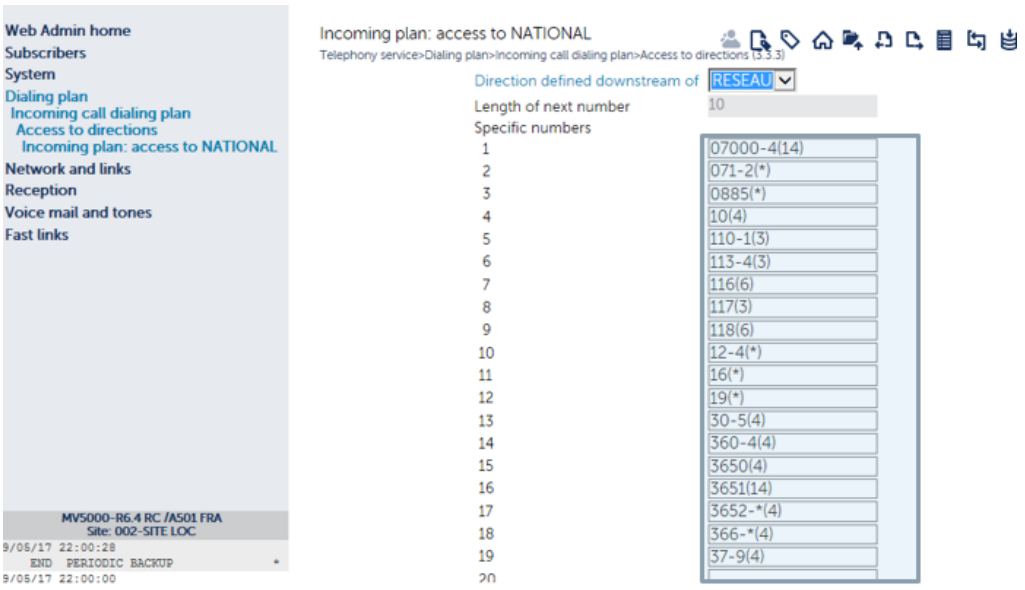
To configure these dialing plans:

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.

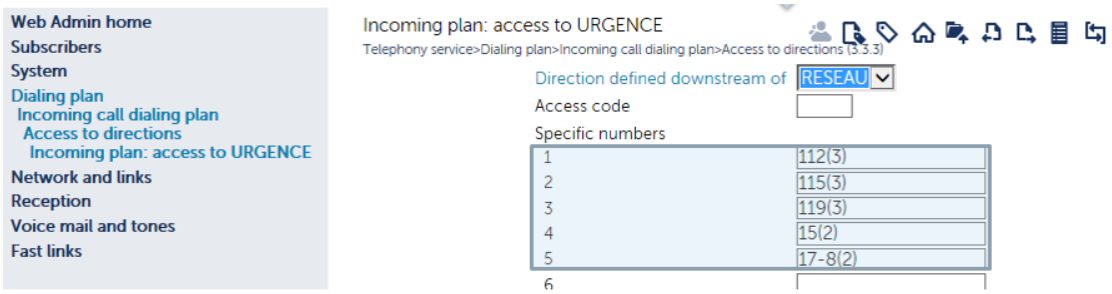


2. Enter specific values for each parameters for the direction that you need to set as incoming dial plan.
   - A prefix
   - A dialing tone after the prefix
   - A dialing length
   - Specific numbers.

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



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



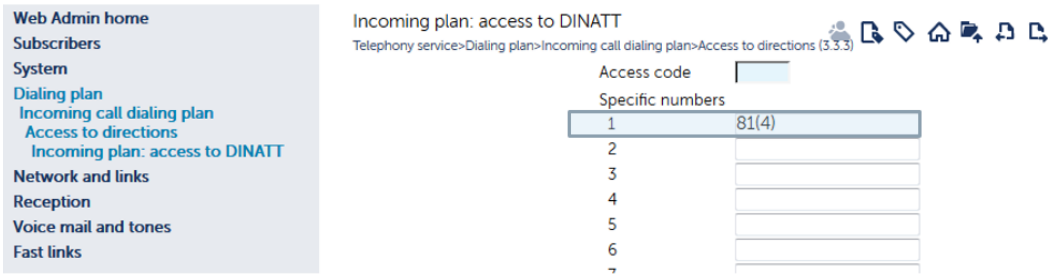
These characteristics are used by the iPBX to split incoming transit between two directions. You can do this by selecting the direction name.

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**.



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.

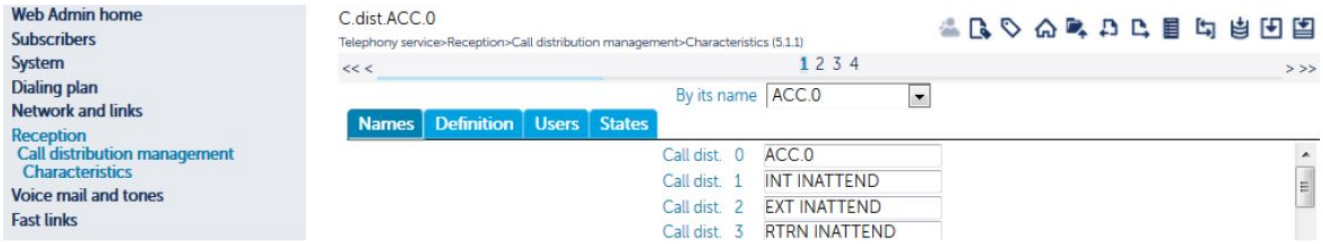
Programming Call Distribution for InAttend Services

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.

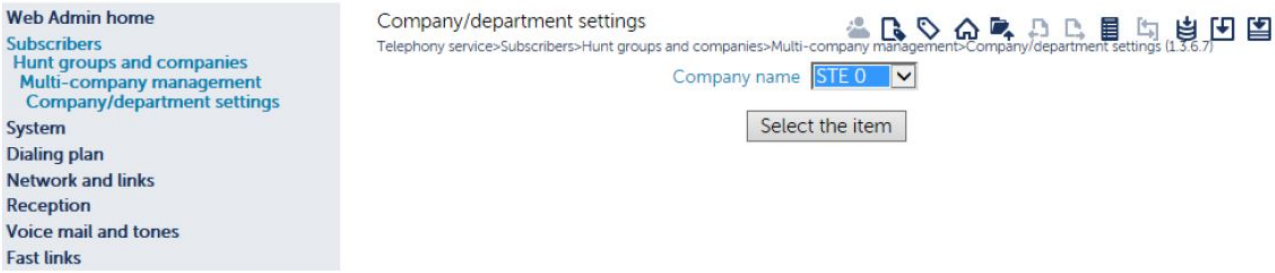
Three Queues are configured in InAttend Services

- 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**



To configure queue:

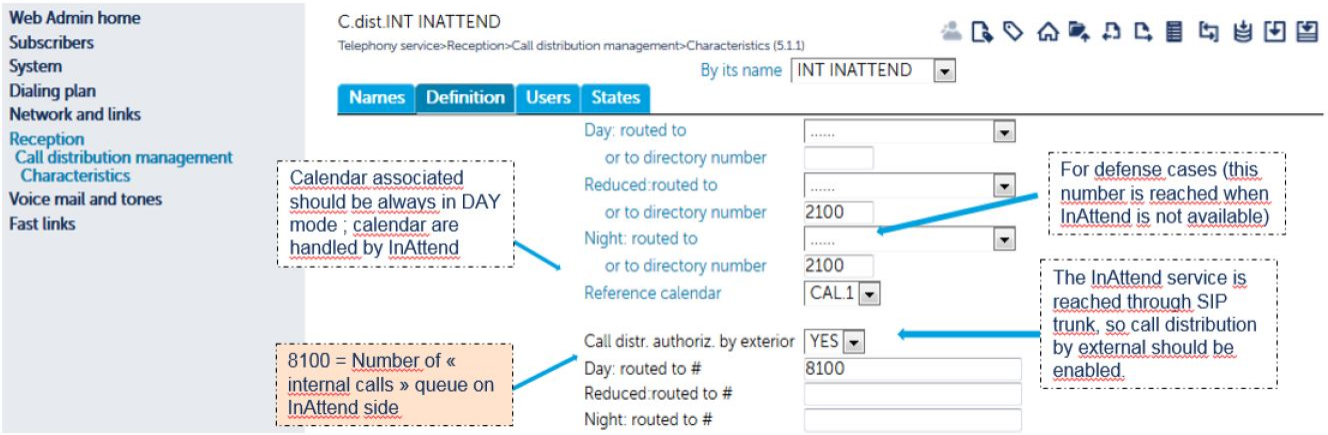
1. In canonic configuration, the prefix to reach the attendant service is 9. It is configured in the **User dialing plan > Operator Call**.
   This prefix is used by all the subscribers irrespective of company or department.



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.



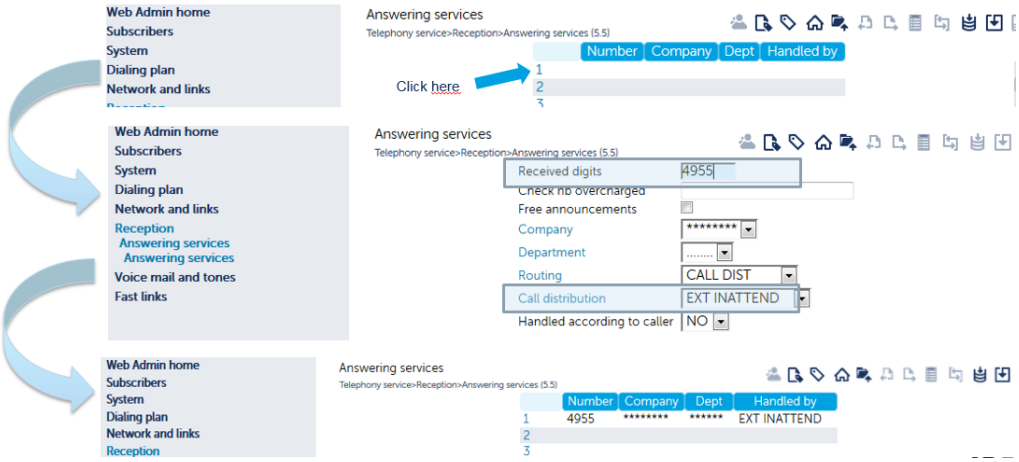
NOTE:

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.



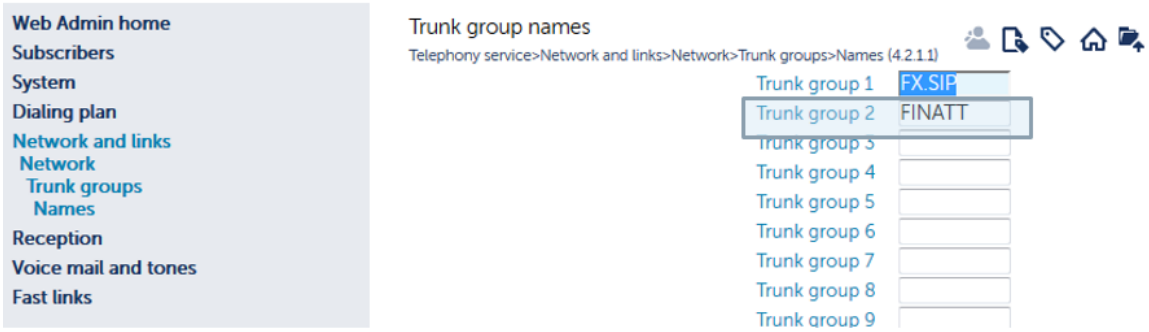
SIP Trunk Configuration

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

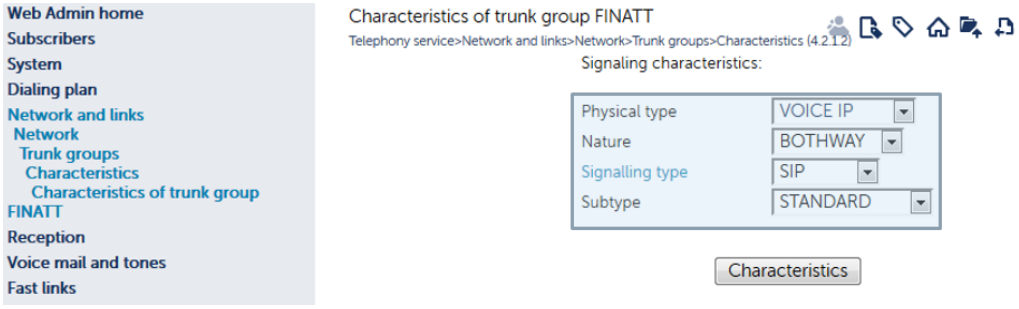
Use the **MiVoice 5000 Service Node Manager** to configure Mi Voice 5000 for SIP trunking.

Add a SIP Trunk for InAttend

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



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.



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

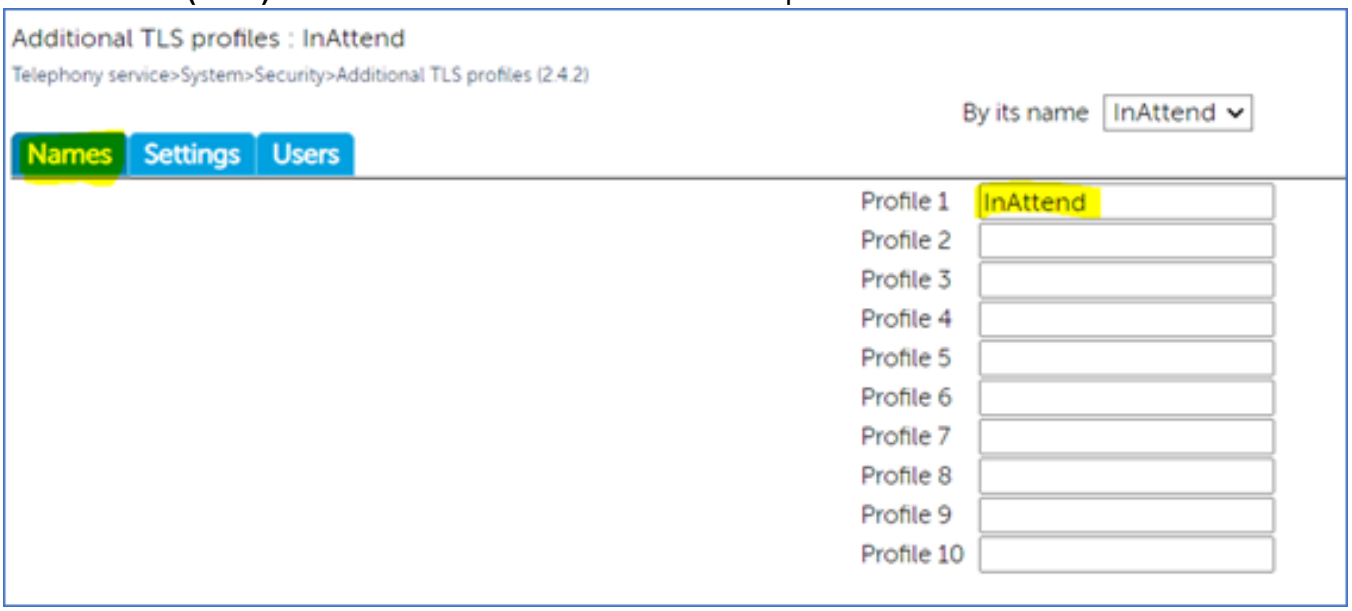
NOTE: TLS/SRTP is available only since MiVoice 5000 7.1. It is used to secure the communication between MiVoice 5000 and InAttend.

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.

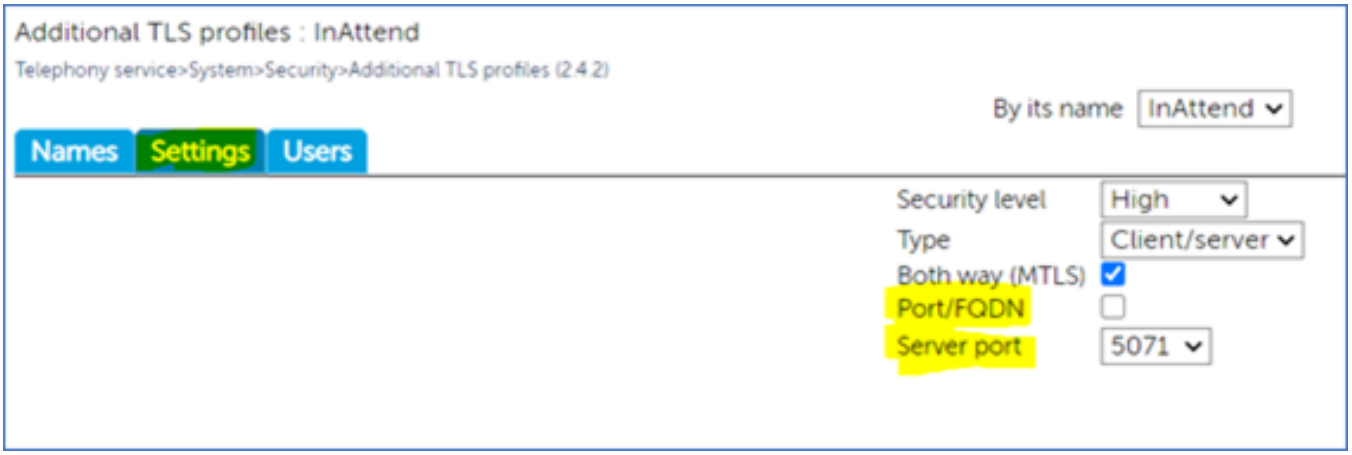
- IIf the default SIP profile (used by the SIP terminal) uses a trusted certificate, it can be used for the InAttend trunk group. No specific TLS profile need be created for InAttend.
- If the default SIP profile uses a self-signed certificate, you must create a TLS profile for the InAttend trunk group.

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.

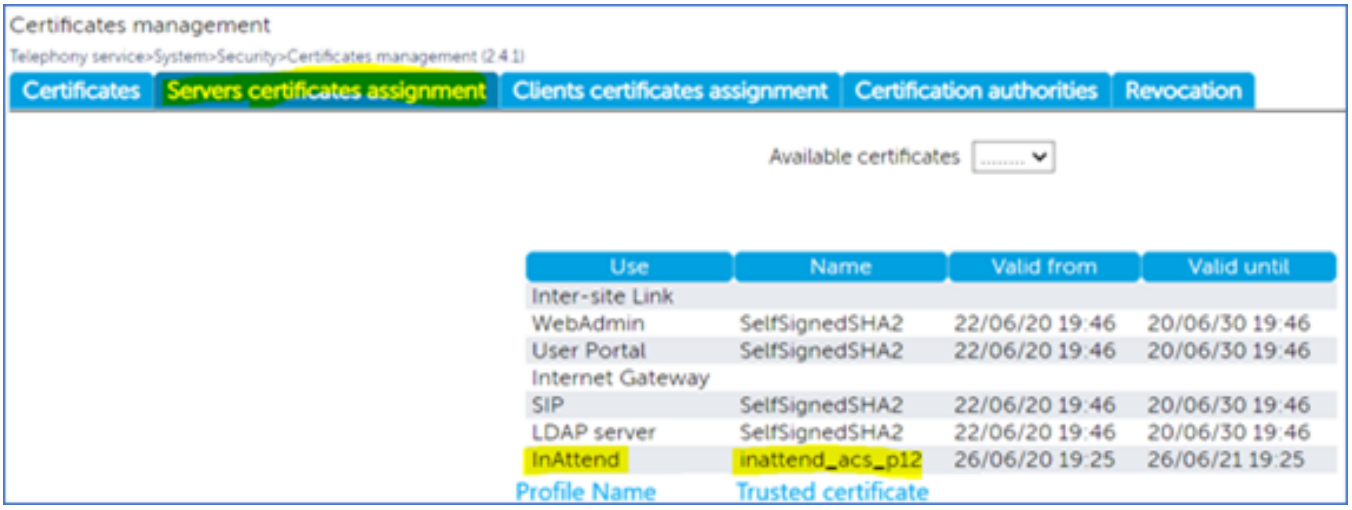


ii. Click the **Settings** tab and configure either the **Server port or Port/FQDN**to be used for trunk connections. Configure the other parameters such as **Security level, Type** and **Both way (MTLS).**



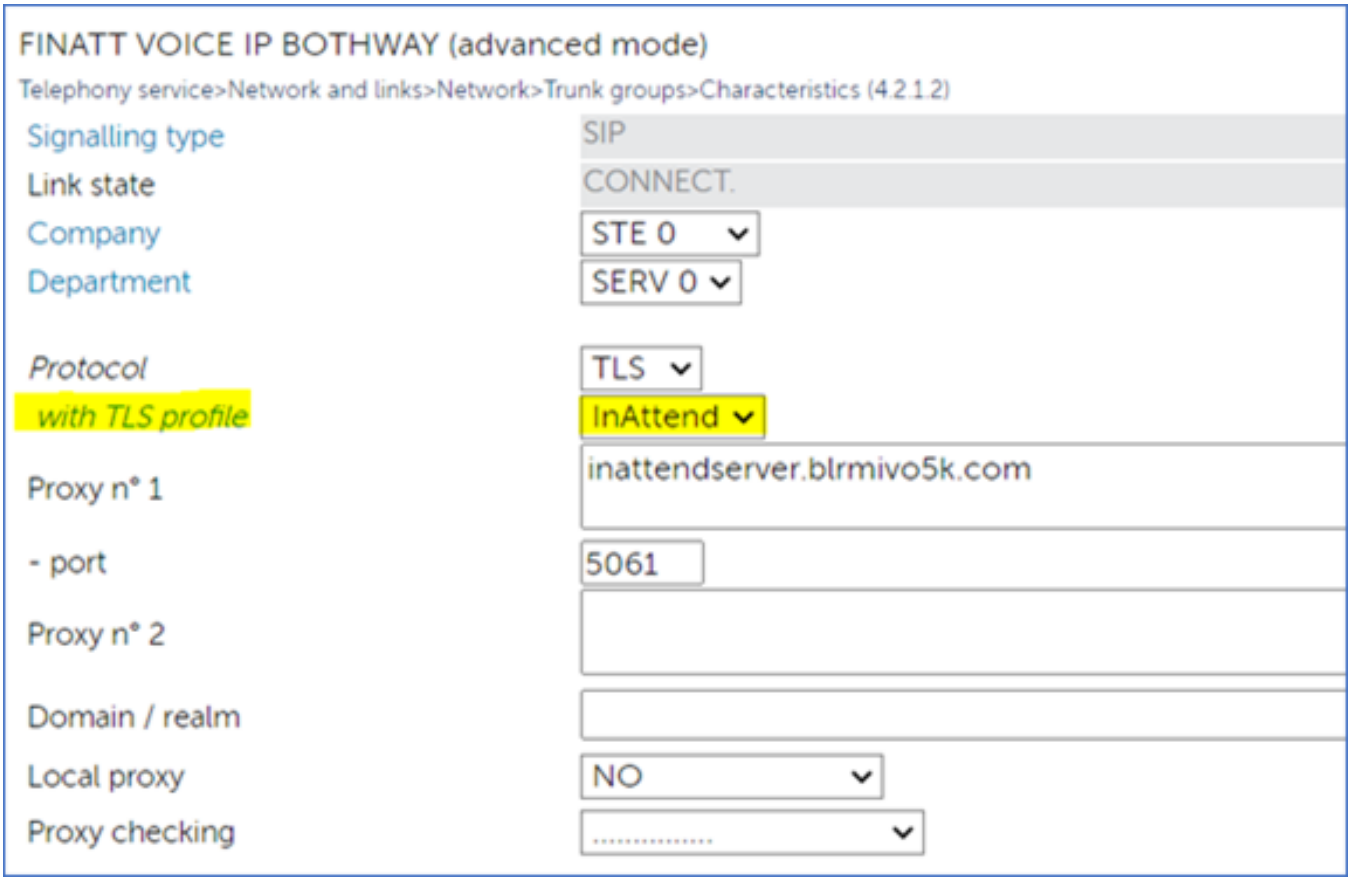
To assign the trusted certificate to the TLS profile:

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.

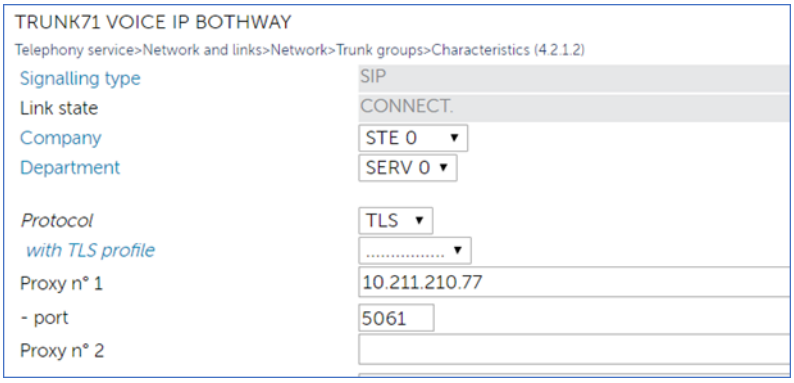


To assign the TLS profile to the SIP trunk configured with the InAttend server:

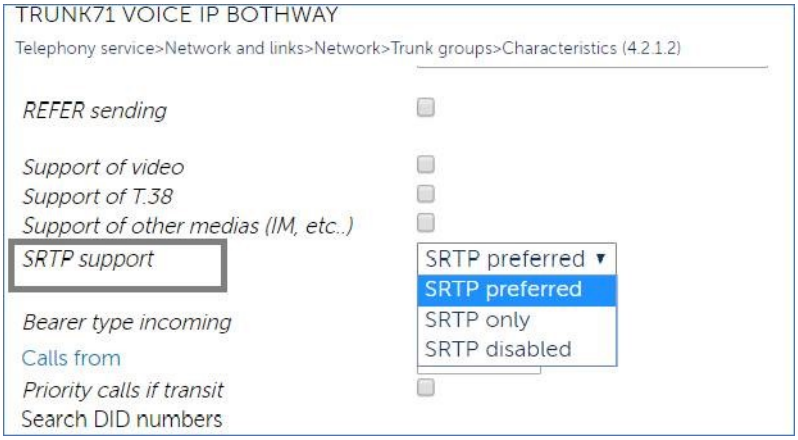
Go to PBX MMI **Telephony service > Network and links > Network > Trunk groups > Characteristics (4.2.1.2)** and select the TLS profile (configured in the preceding steps) in the trunk configuration.



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



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



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.

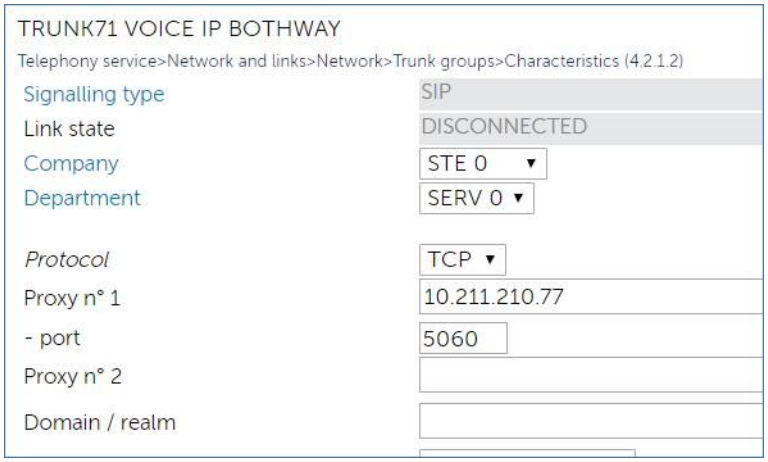
Make sure that the generic parameter **Ciphering and IP settings** is general to enable/disable SRTP on all the endpoints. SRTP support can be disabled selecting SRTP disabled on the SIP Trunk

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

NOTE: SelfSigned certificate is not supported by InAttend.

SIP trunk configuration in TCP

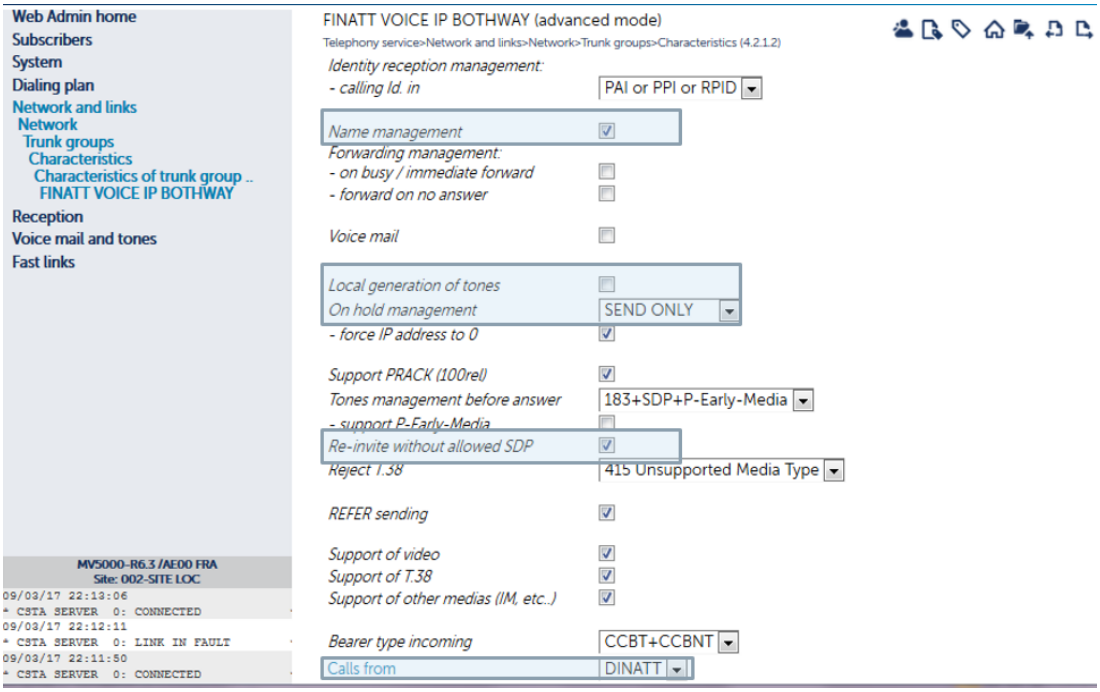
a. Set the protocol as **TCP** from the drop-down list.
b. Enter the proxy of InAttend server and port as 5060.

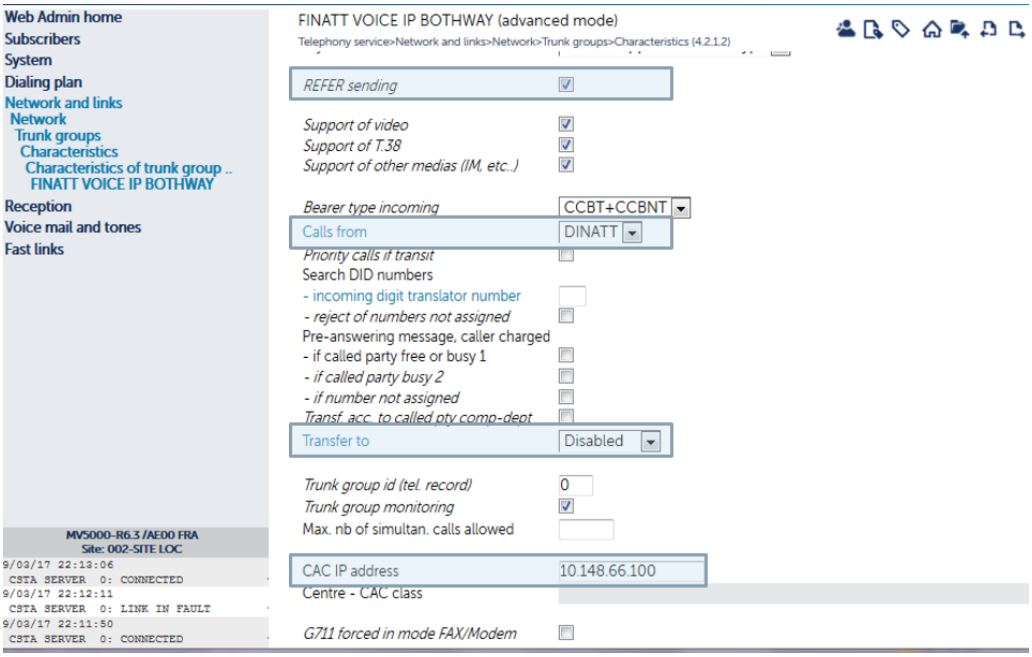


NOTE: With TCP as trunk protocol, SRTP support option is unavailable in trunk configuration.

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**.





Create SIP Routes

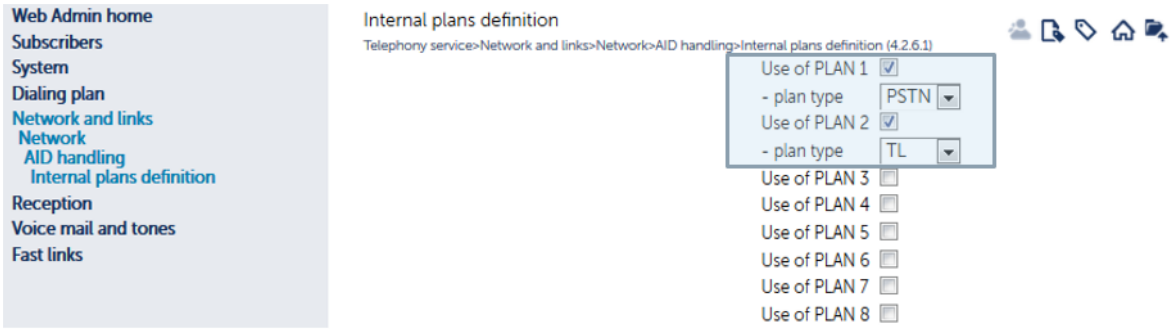
A route and a specific direction are associated to InAttend and an access code is defined in the user dialing plan.

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.

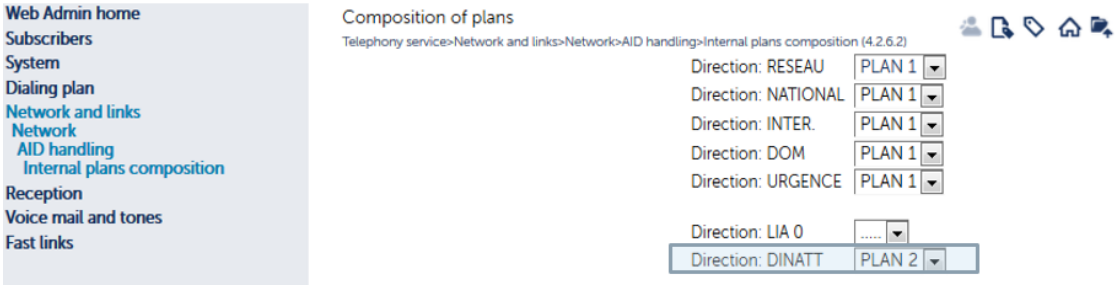


Composition of internal plans

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.

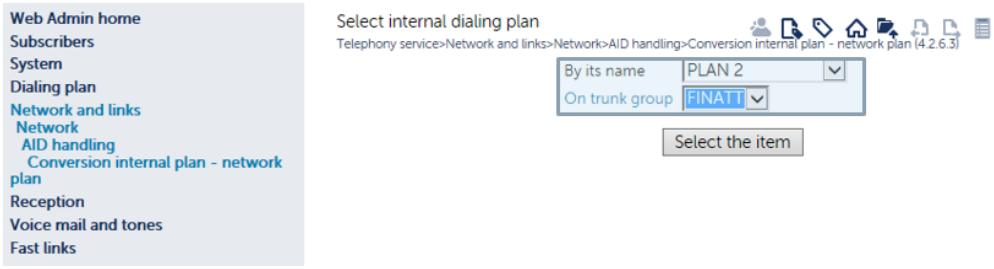
1. Go to **Network and links > Network > AID handling > Internal plans composition**.
2. Select the plan from **Direction** drop-down that you have created. In this example it is **Direction: DINATT**.



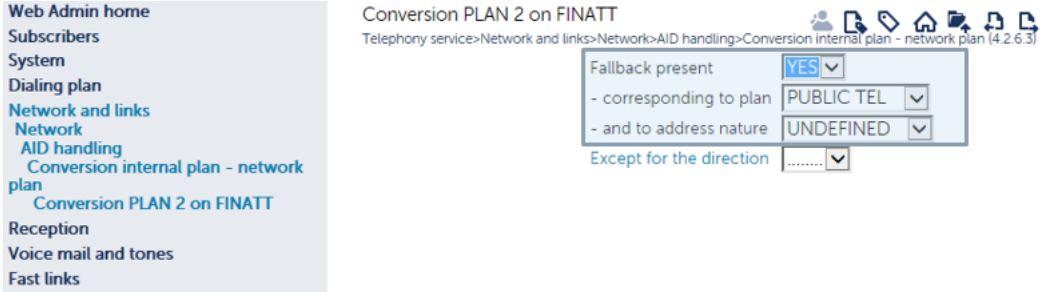
Convert internal plan

1. Go to, **Network and links > Network > AID handling > Conversion internal plan - network 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.

   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).

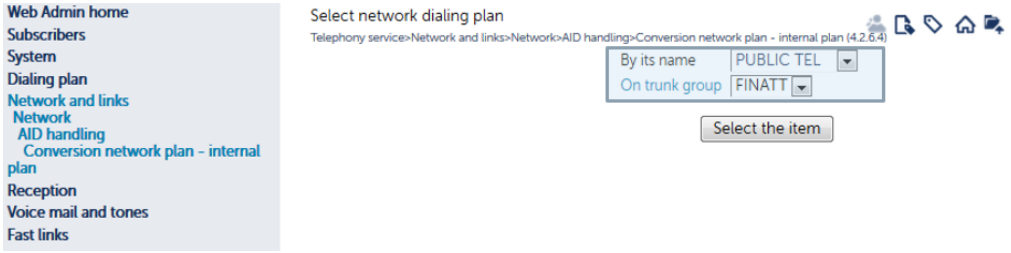


3. Select **YES** from the **Fallback present** drop-down list.
4. Select **PUBLIC TEL** from **corresponding to plan** drop-down list.
5. Select **UNDEFINED** from **address nature** drop-down list.

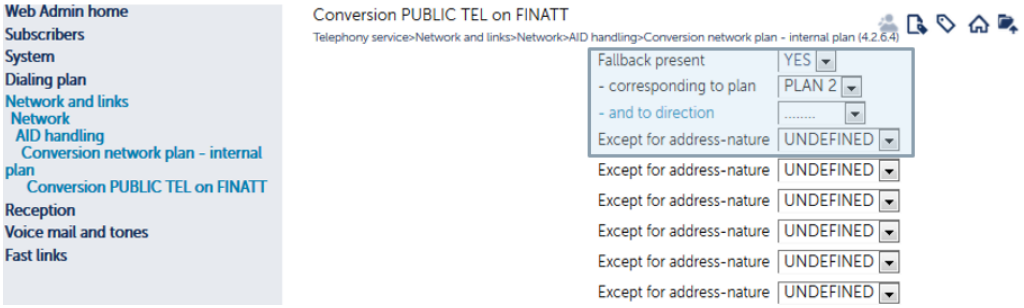


Convert Network Plan - Internal Plan

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.



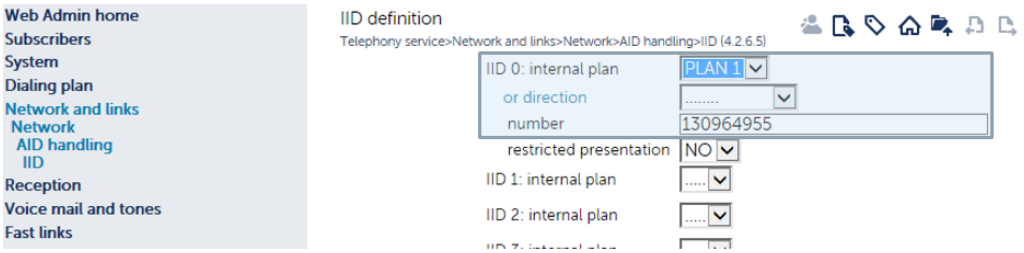
3. Select **YES** from the **Fallback present** drop-down list.
4. Select plan from **corresponding to plan** drop-down list and select direction if defined.
5. Select **UNDEFINED** from the **Except for address nature** drop-down list.



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**.



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

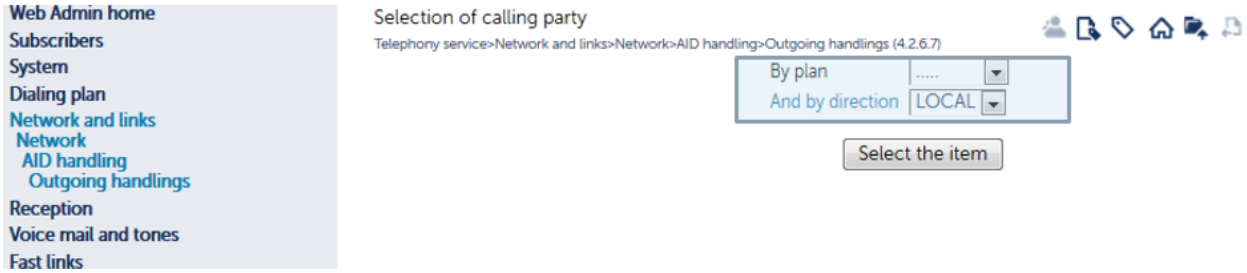
2. Select the internal plan associated with the IID. For example, in the screenshot above, **Plan 1** is selected.
3. Select the direction associated with the IID.

   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).

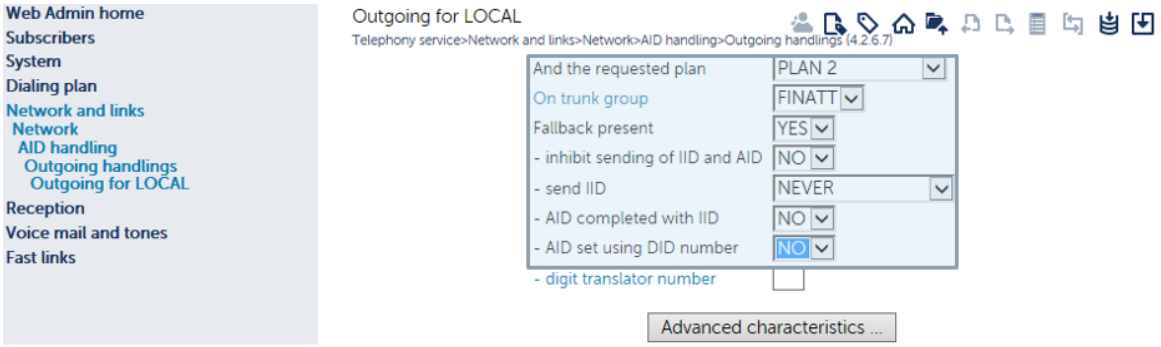
Go to, **Network and Links > Network > AID handling > Outgoing handling and select the item**.



For Local Calls InAttend

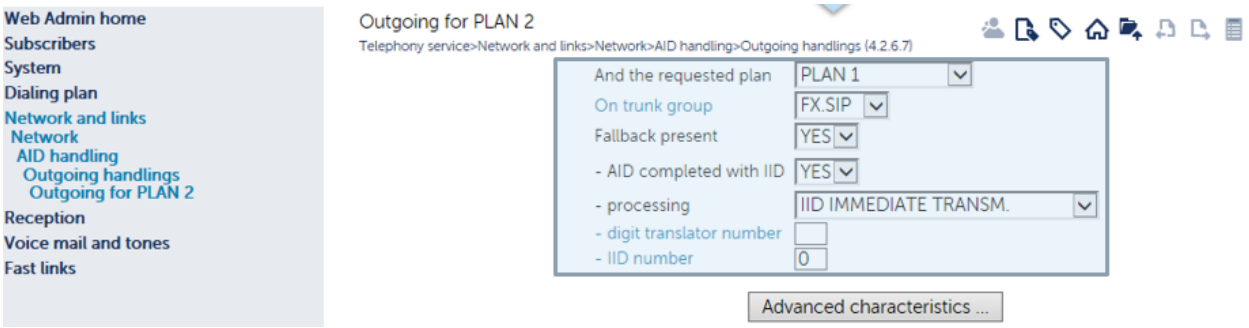
1. Select the **LOCAL** plan by direction and click **select the item**.
2. Select the request plan as **PLAN2** from the drop-down list and select **FINATT** for the trunk group.
3. Select **YES** from the **Fallback present** drop-down list.
4. Select **No** for **inhibit sending od IID and AID** and 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.



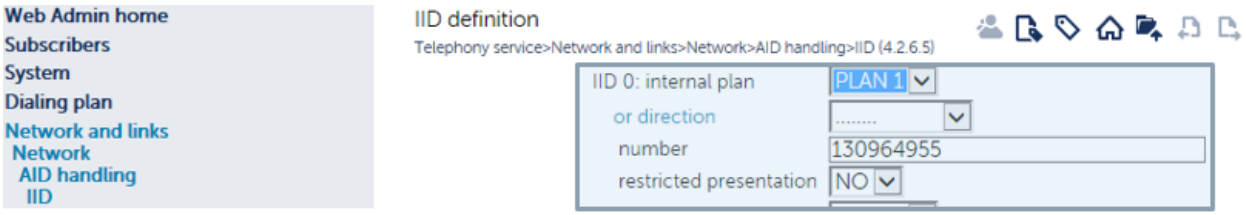
For Inattend calls External

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.



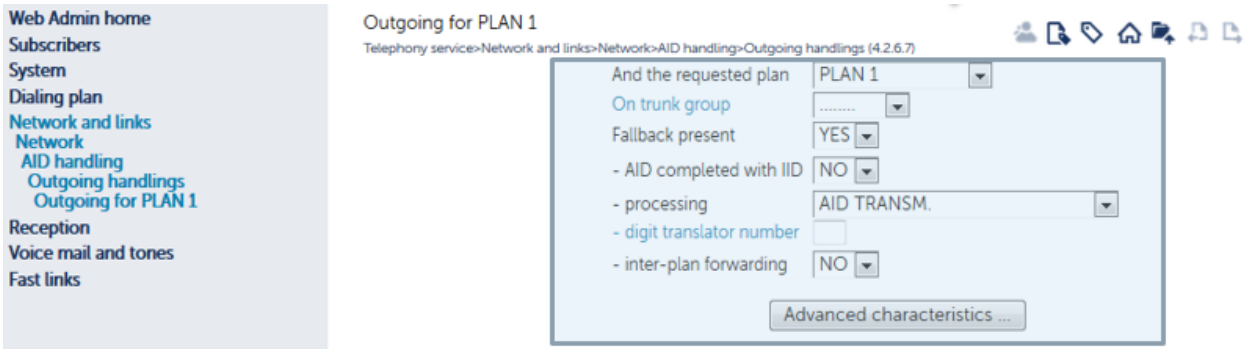
5. Go to **Network and links > Network > AID handling > IID** and set the number.

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



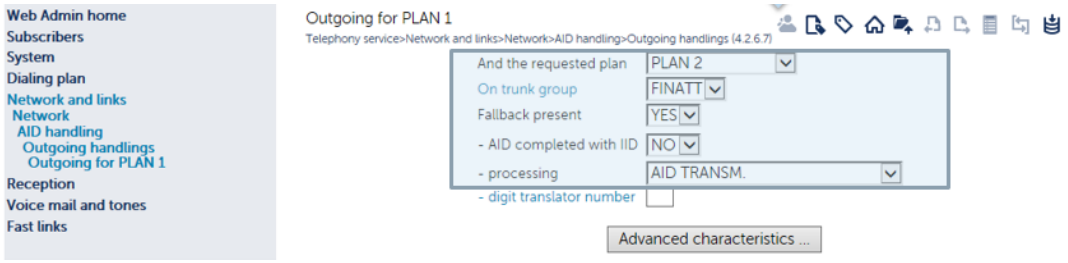
For External transferred to External

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**.



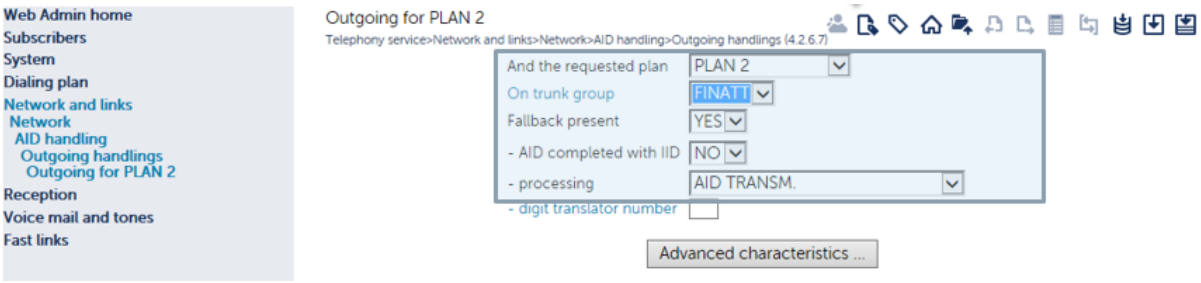
For External calls InAttend

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.



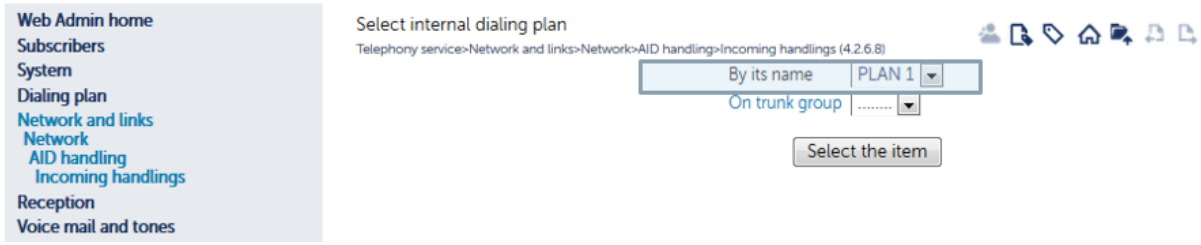
For InAttend calls InAttend

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.

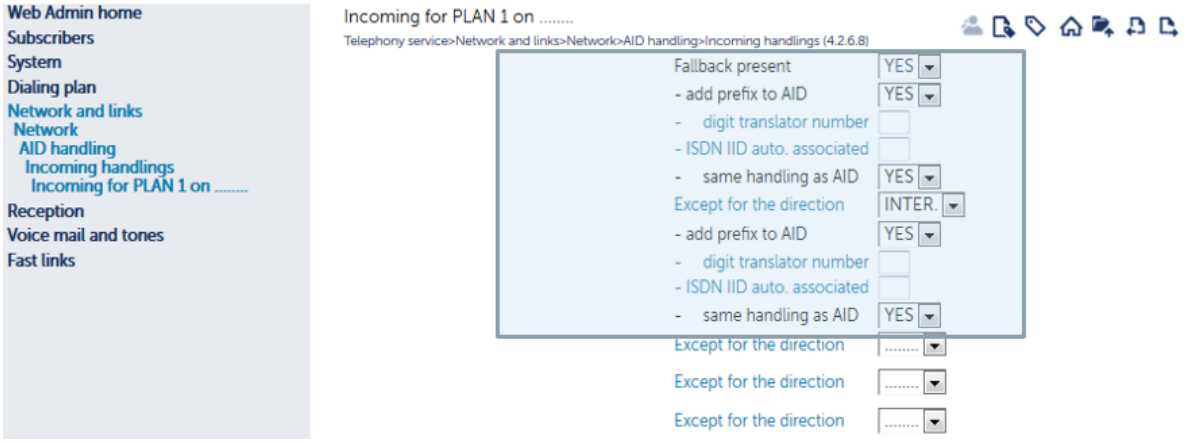


For External Calls Local

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

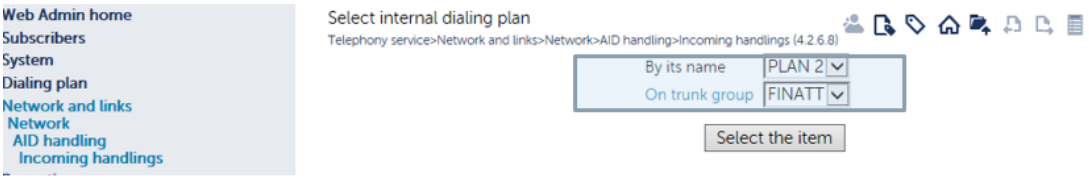


2. Select **YES** from the **Fallback present**, and select **YES** for **add prefix to AID**.
3. Select **YES** for **same handling as AID**.
4. Select **INTER** from the **Except for the direction** drop-down list.
5. Select **YES** for **same handling as AID**.

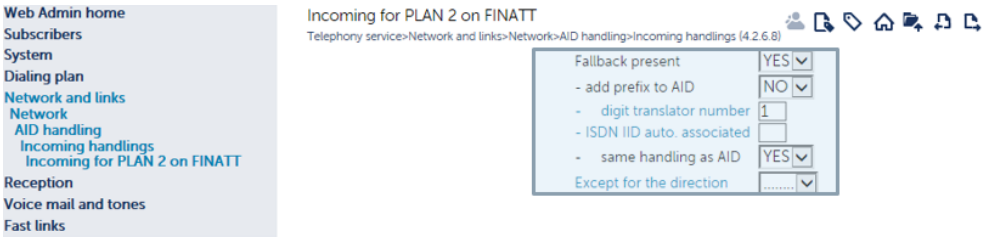


For Inattend calls Local

1. 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**.

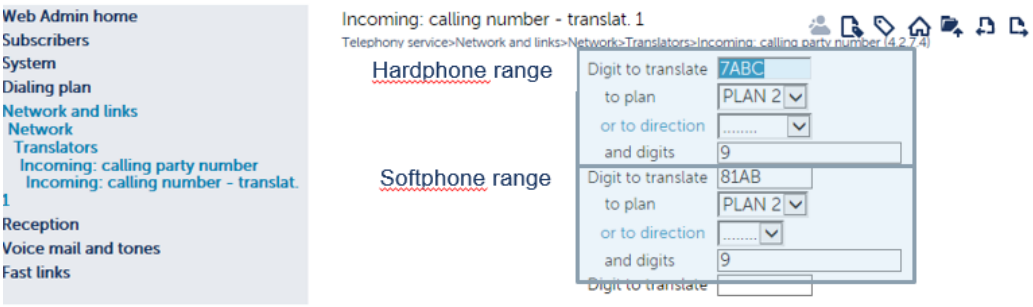


3. Select **YES** from **Fallback present**, and select **No** to **add prefix to AID**.
4. Enter **1** in the **digit translator number**.
5. Select **YES** from the **same handling as AID**.



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.



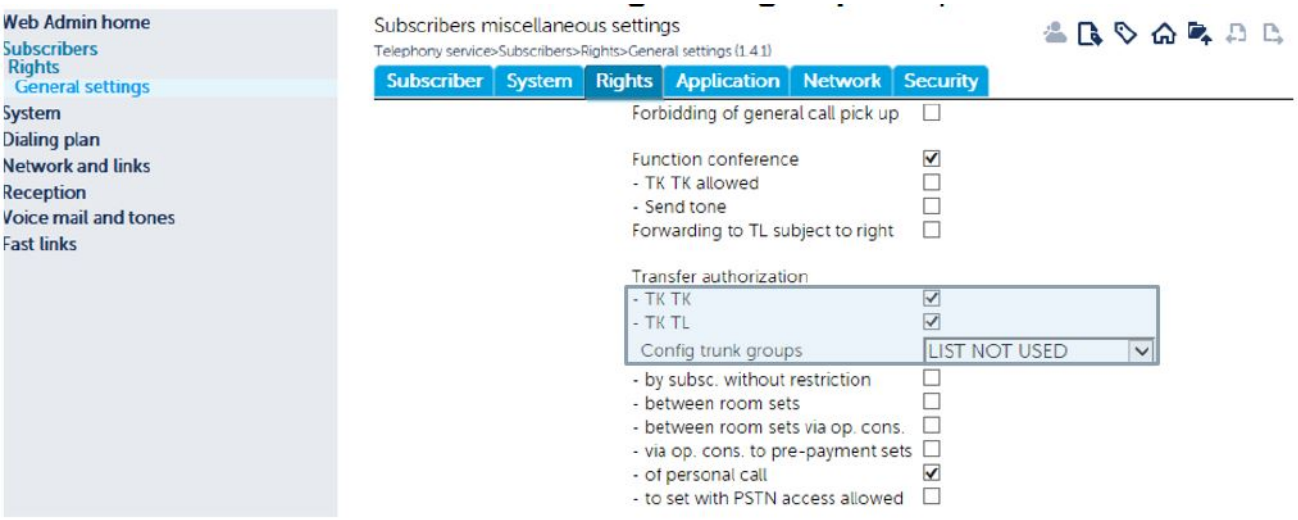
What to do Next

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

Transfer Authorization

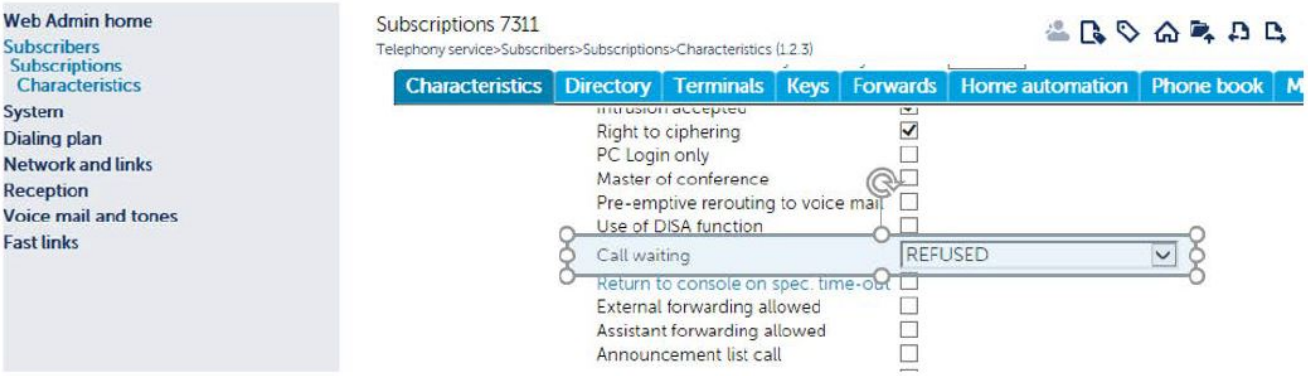
To allow transit calls between Network calls and InAttend:

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.



Configure Hardphone Subscriber

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



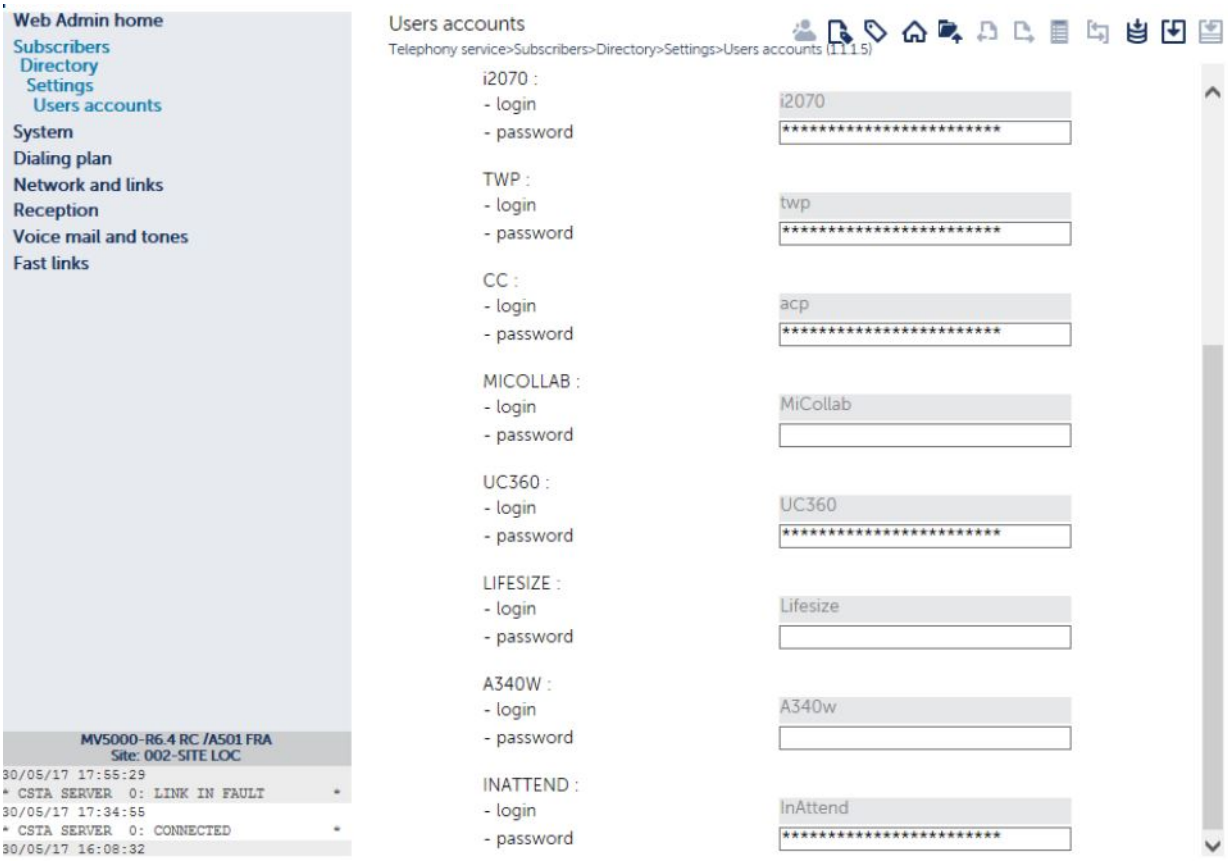
Create an External Record

1. 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

Create Password

Create a password for InAttend account to access proxyldap

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



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.

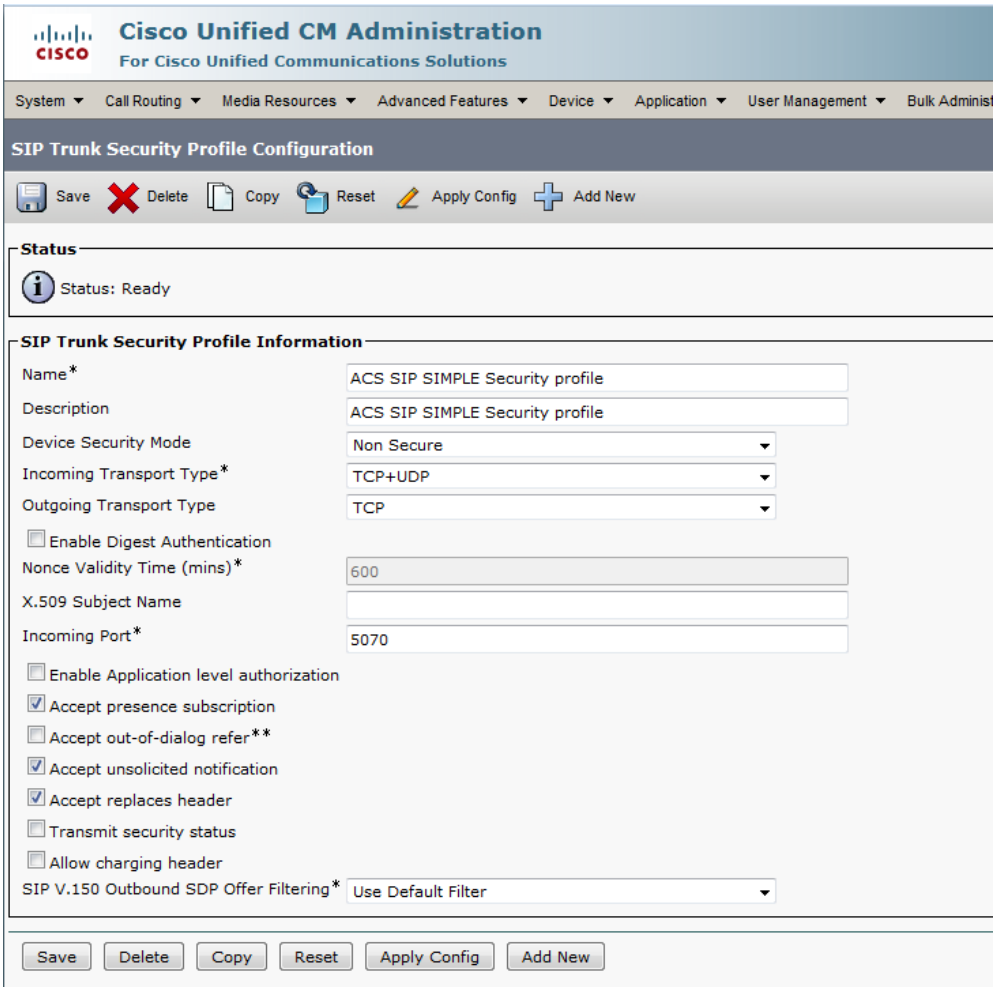
This trunk points back to the ACS (linestate) server on port 5070 (as shown in the image).

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:

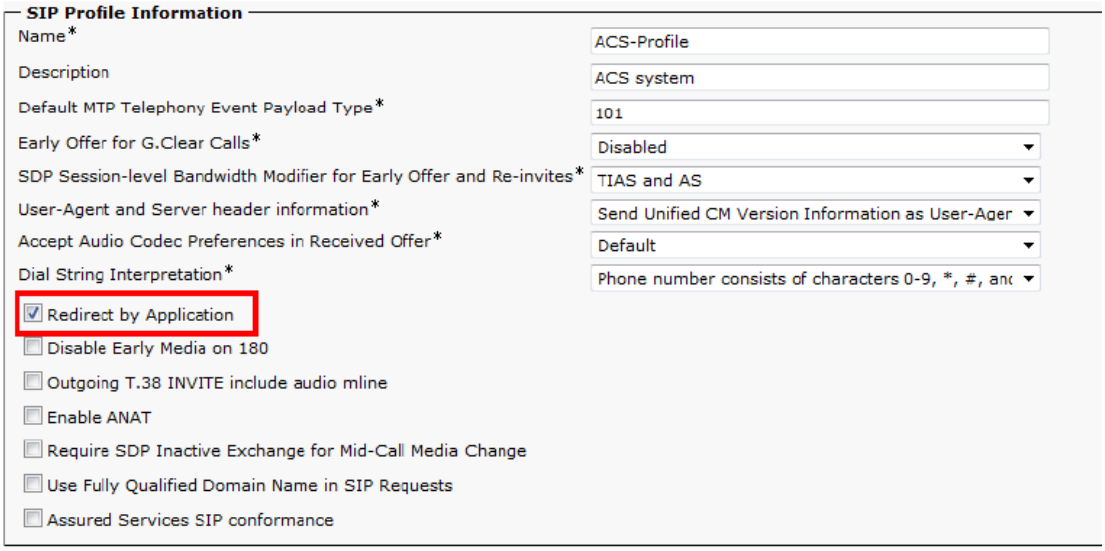
1. Login to the Cisco Unified CM Administration interface (http://<servername>/ ccmadmin).
2. Under SIP Trunk Security Profile Information, enable the following options:
   - **Accept presence subscription**
   - **Accept unsolicited notification**
   - **Accept replaces header**


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administ
SIP Trunk Security Profile Configuration
Save
Delete
Copy
Reset
Apply Config
Add New
Status
Status: Ready
SIP Trunk Security Profile Information
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
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

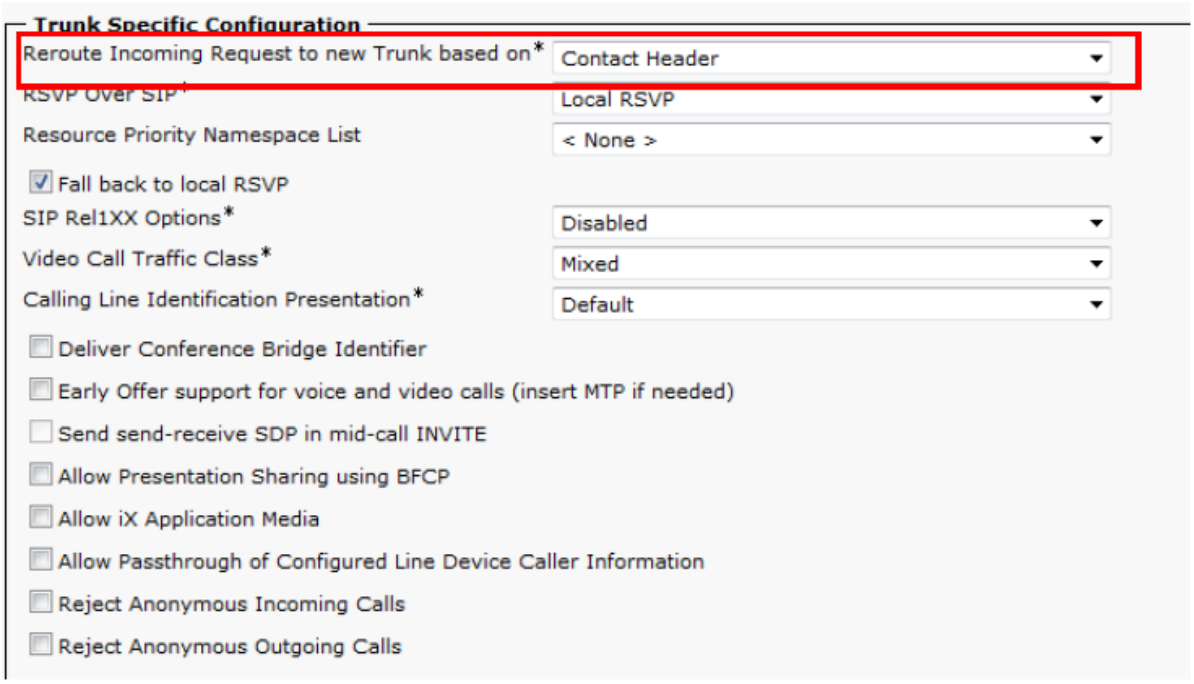
SIP profile configuration

To configure a SIP profile, do the following:

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



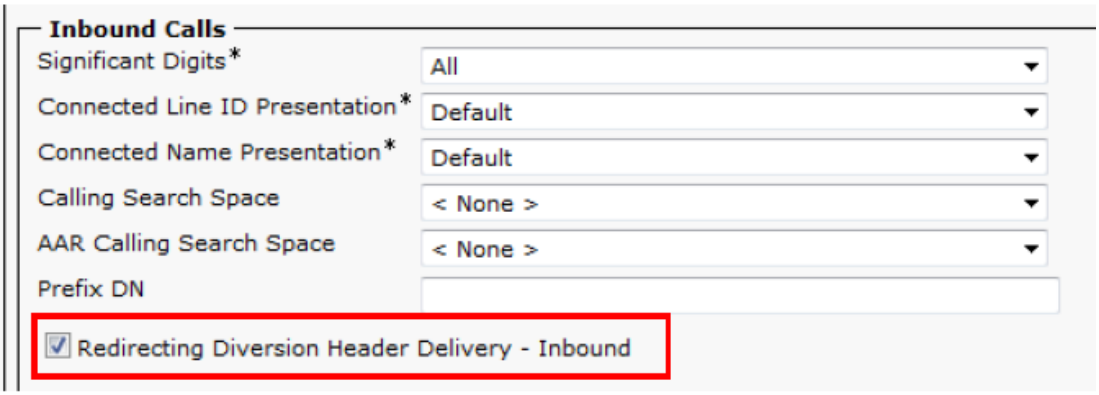
2. Under **Trunk Specific Configuration**, select “Contact Header” from the pull-down list in the **Reroute Incoming Request to new Trunk based on*** field.



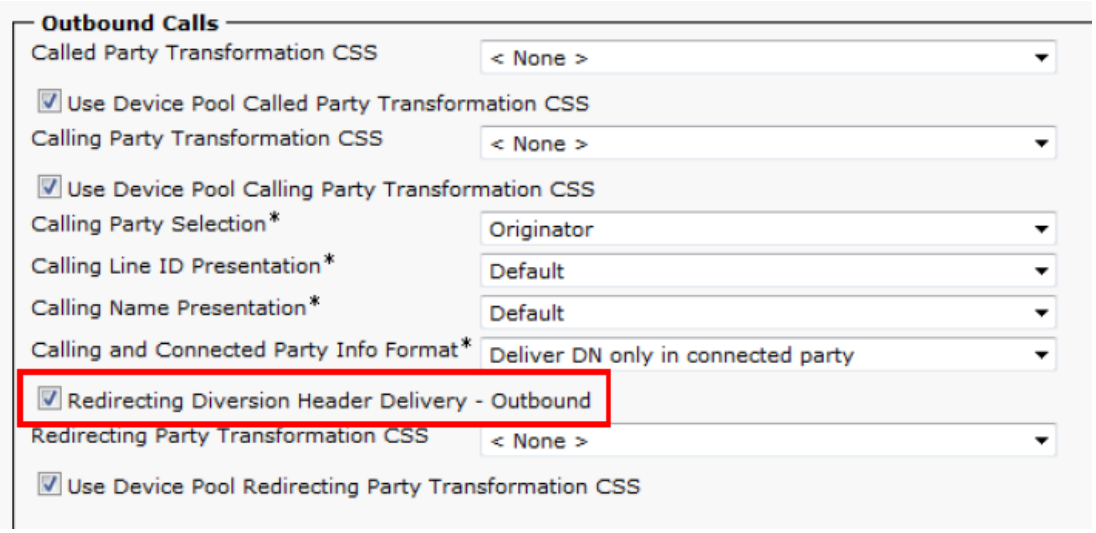
SIP trunk configuration

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.



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



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).

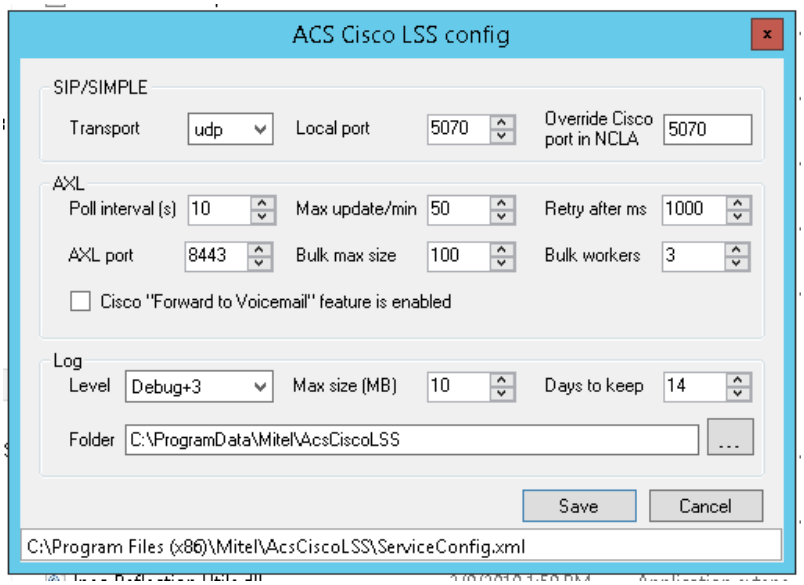
It is also called as the ‘termination port’. It terminates the sip trunk initiated from cucm.

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

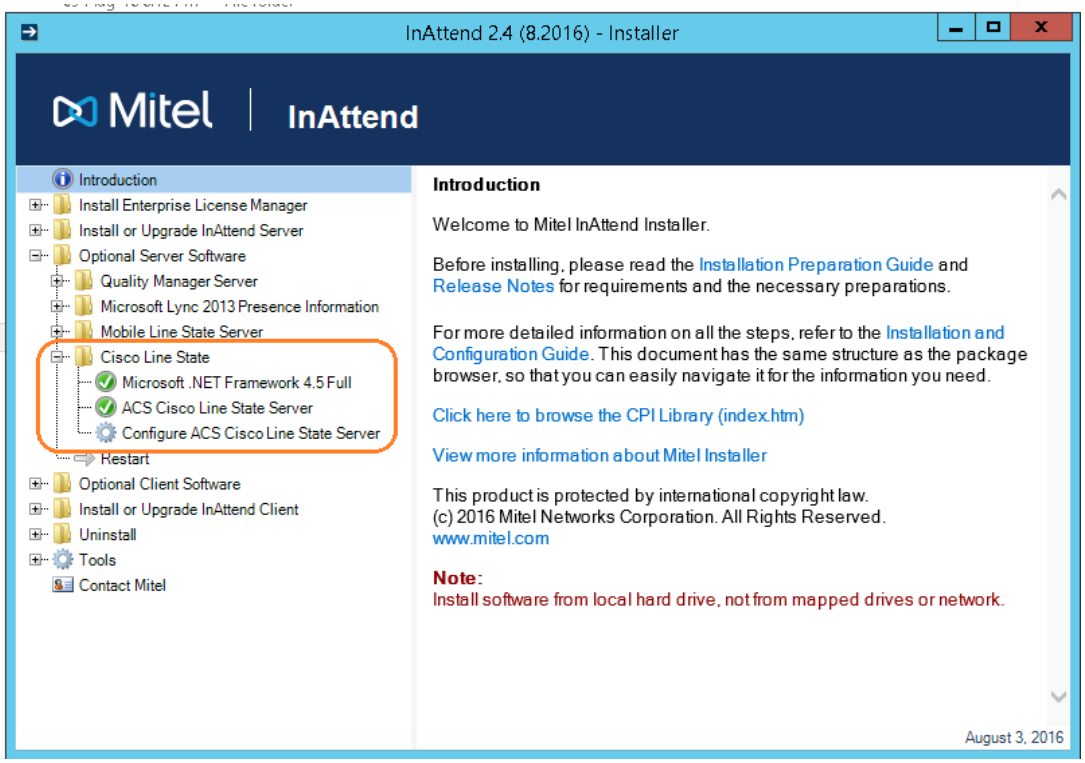
(Debug 3 is the highest level of Debug used.)

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

Click **Save** to update the values entered.



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



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

	Host name	IP	Network name	Description
	CUCM	10.10.144.18	CUCM	CISCO UC
	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.

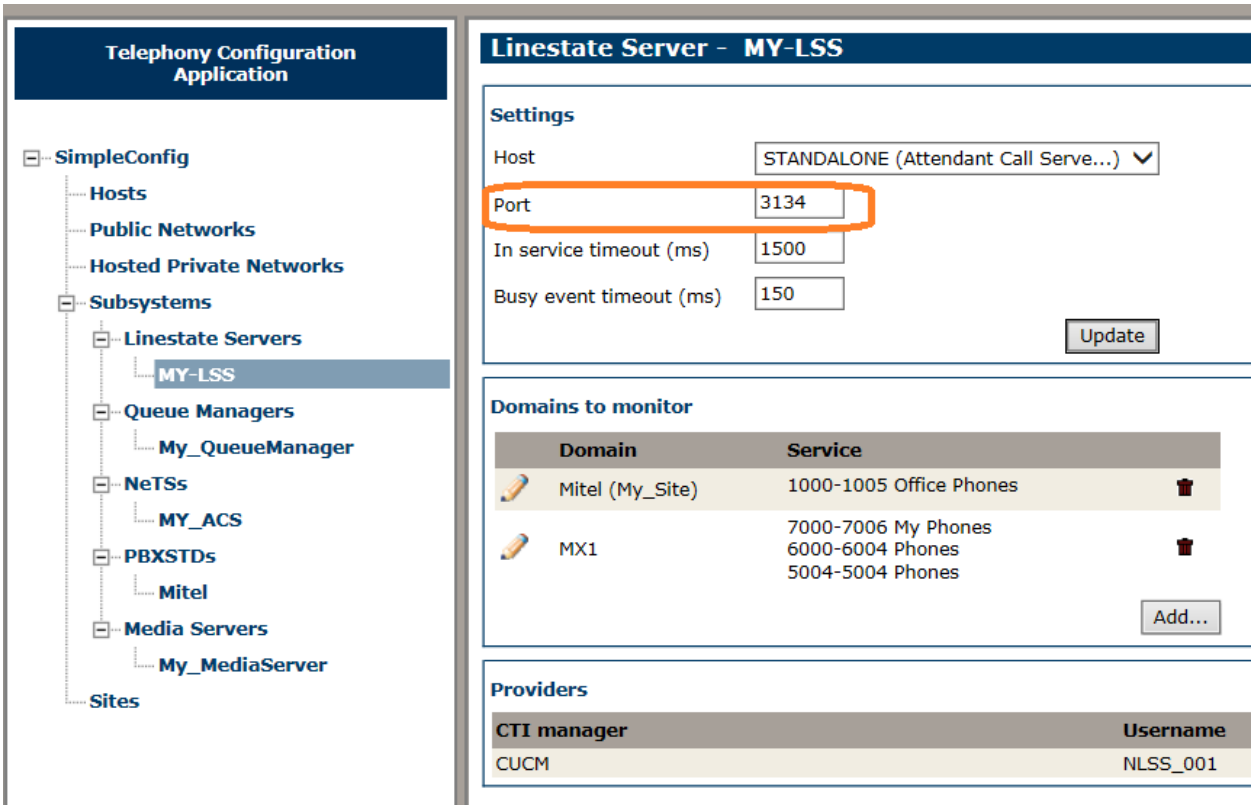
LSS – Linestate Server

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.



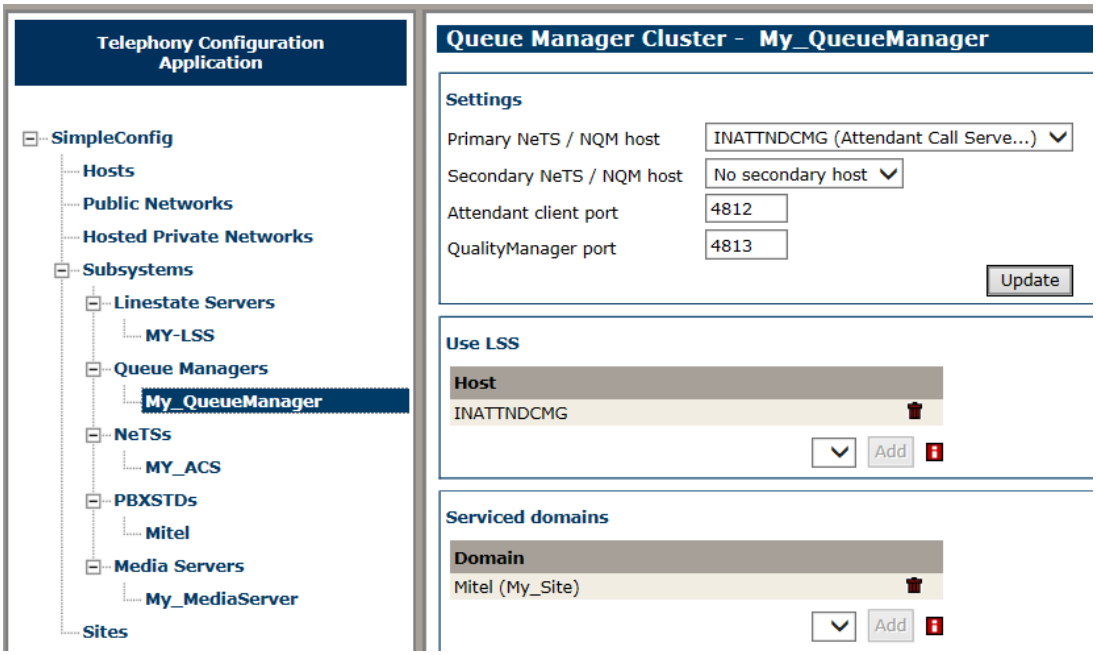
Domains to monitor

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.

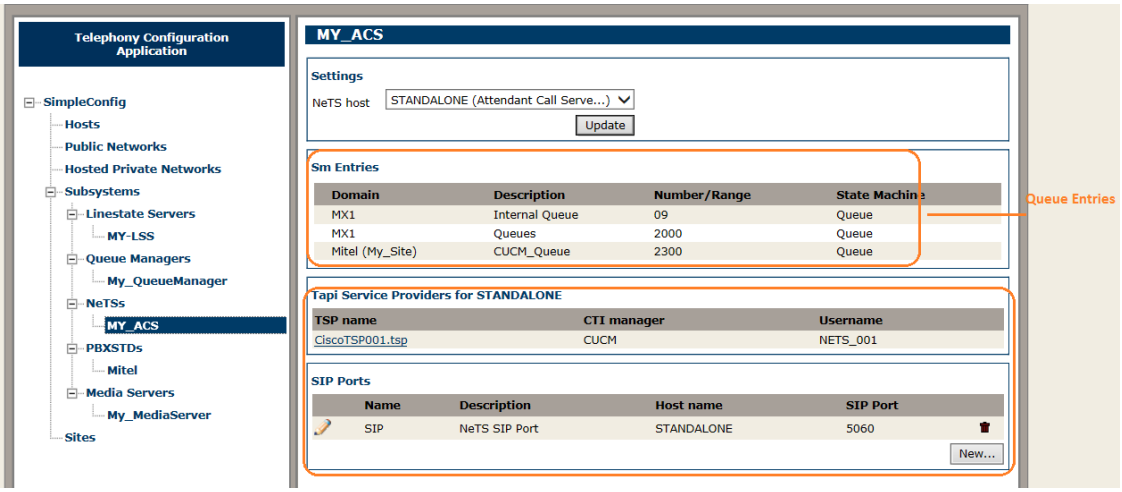


My ACS

My ACS takes default values set by the system.

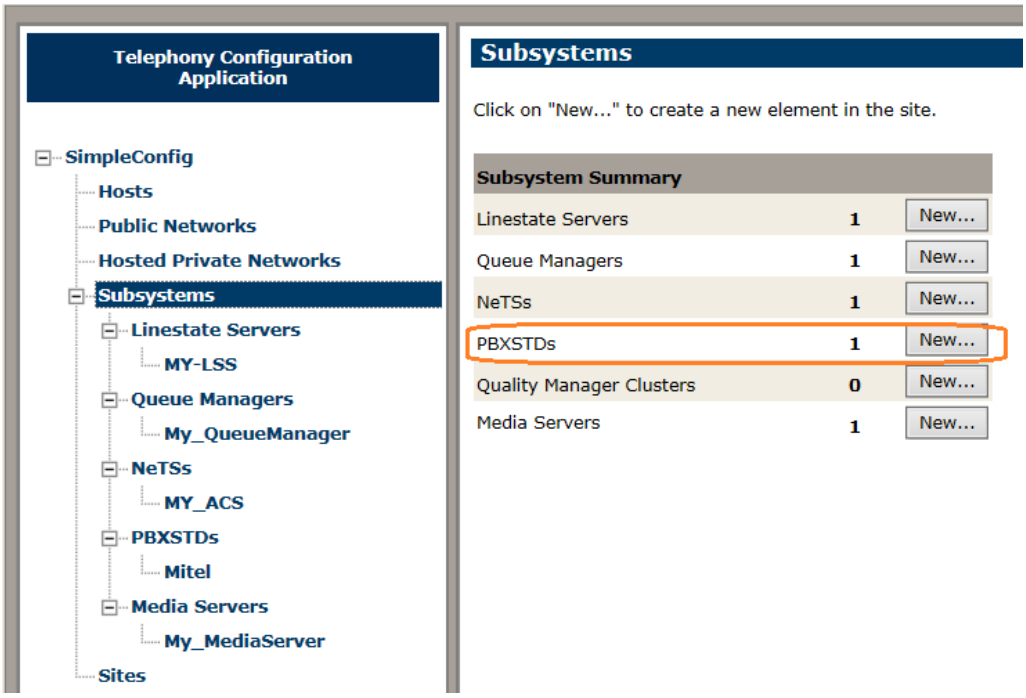
The Host name and Sip Ports field is configured under My ACS.

The Sip Port value is configured to 5060.



PBXSTDs

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

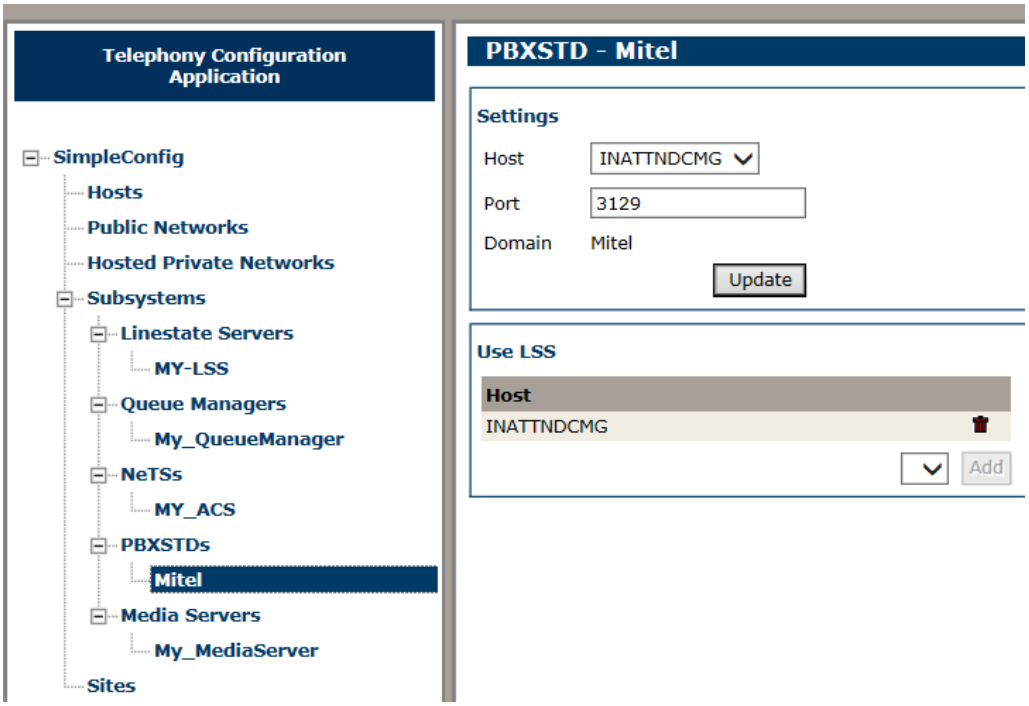


Click **New** to create a new PBXSTDs element.

The **PBXSTD – Mitel** window appears.

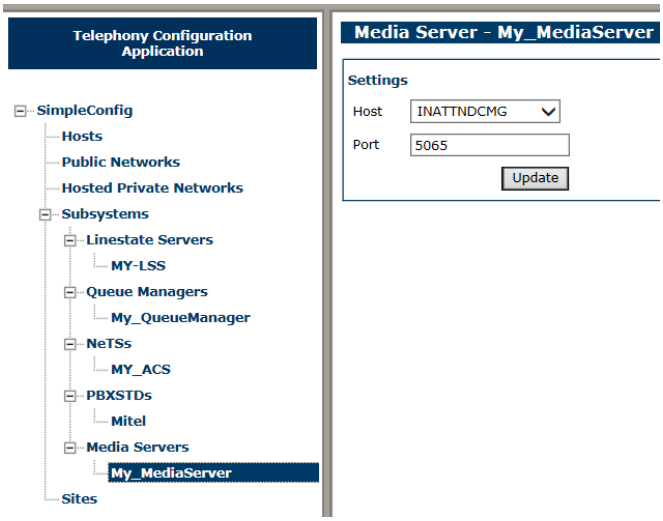
Select the appropriate Host, Port, and Domain.

Click **Update**.

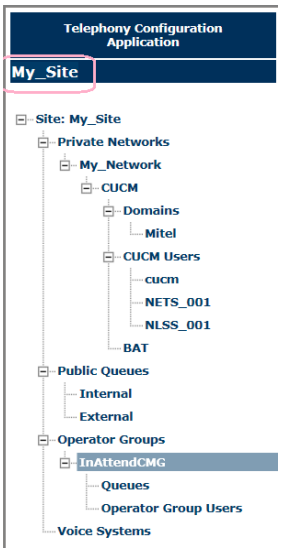


Media Server

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

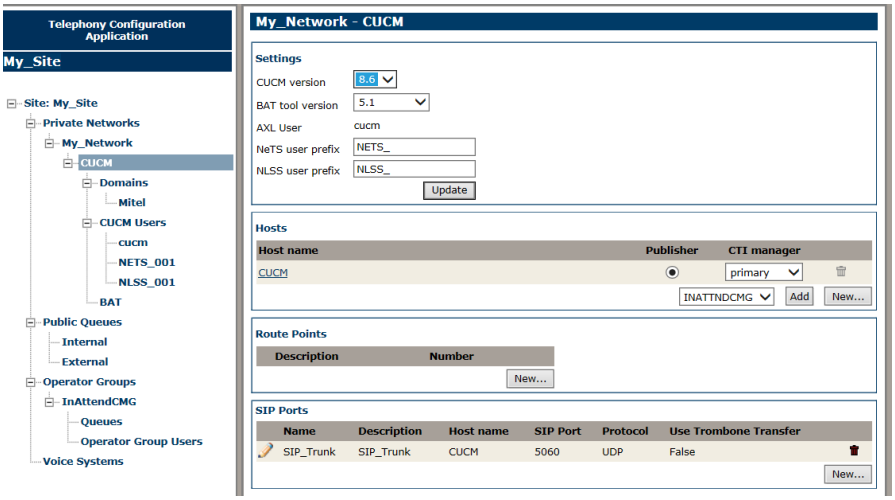


Add CUCM Cluster on a private network.



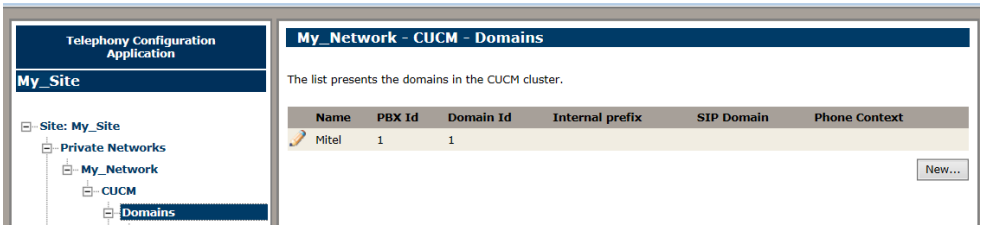
The CUCM version is same as the call manager.

Select the cucm version from the drop-down list.

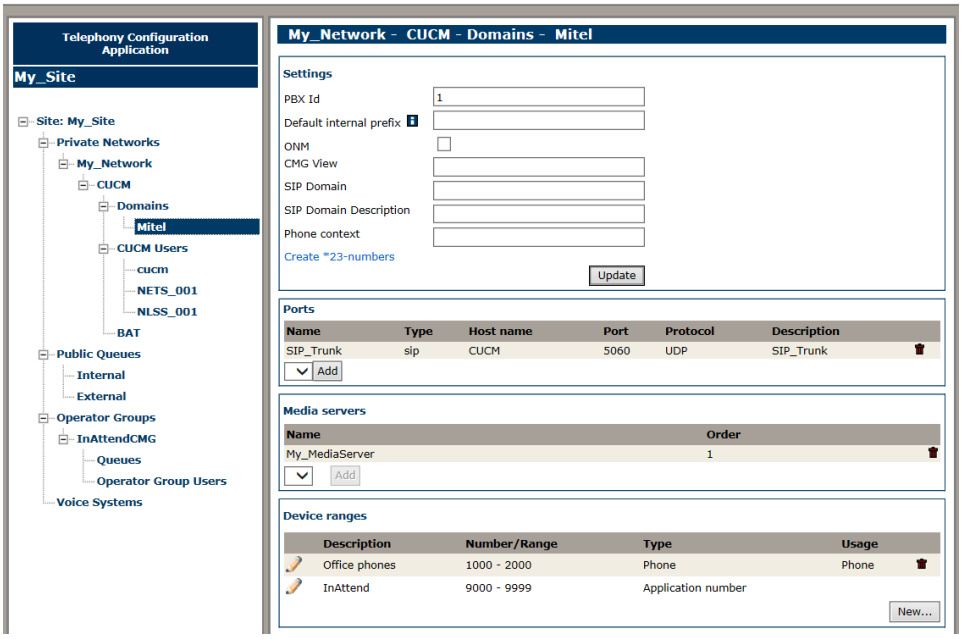


Add sip port as 5060 and UDP under protocol field respectively.

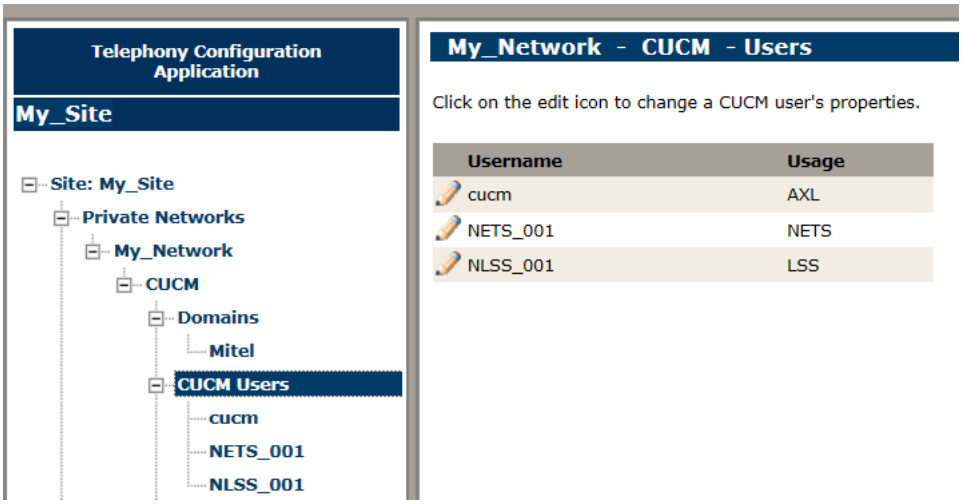
The My_Network – CUCM – Domains is defined.



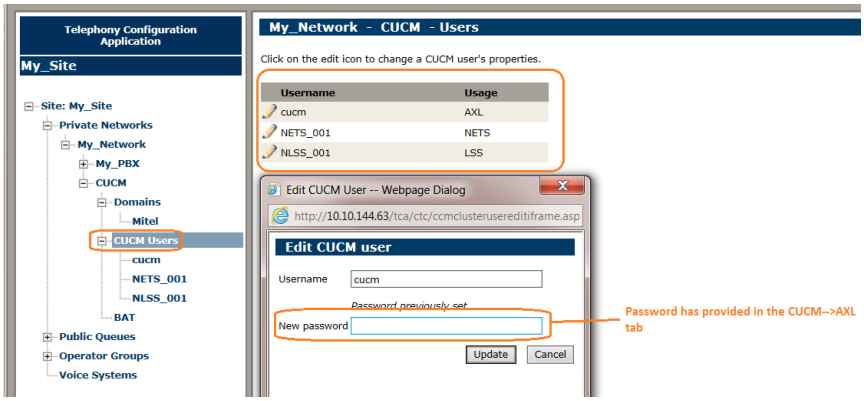
The Port, Media Server, and Device ranges are defined.



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

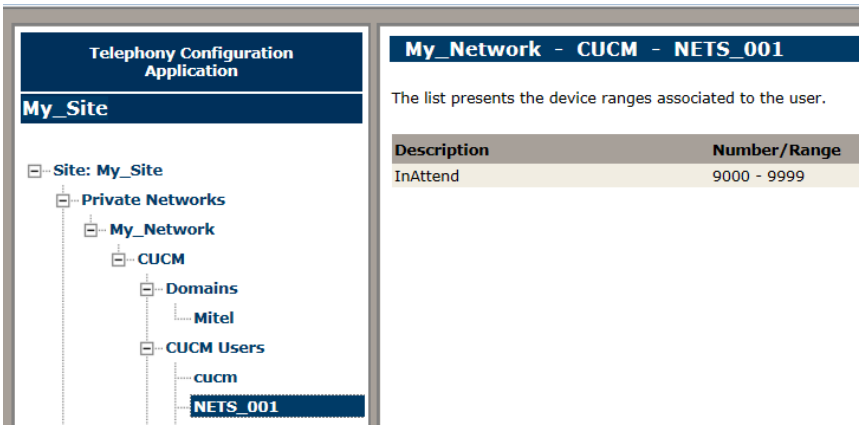


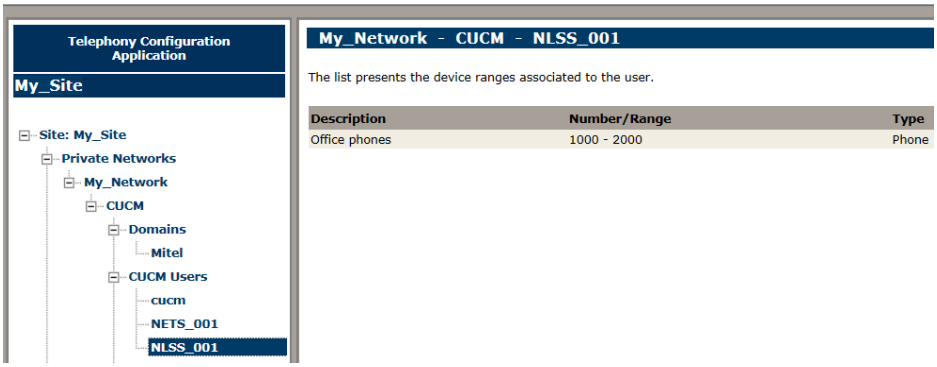
Click the pencil icon to edit the cucm user properties.



Edit CUCM User window appears.

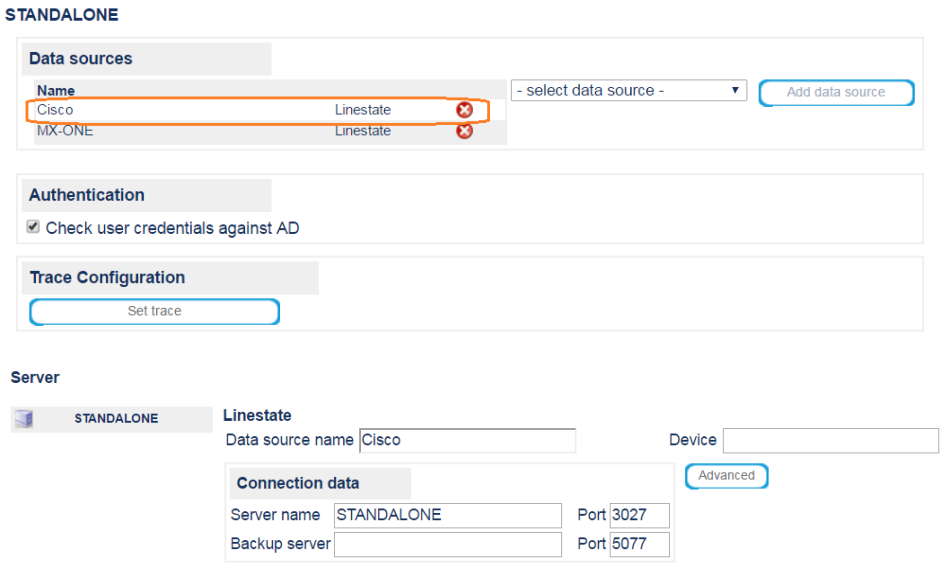
Provide the AXL credentials here in the TCA. The list of device ranges associated to the user is displayed. (The device range value is taken automatically.)



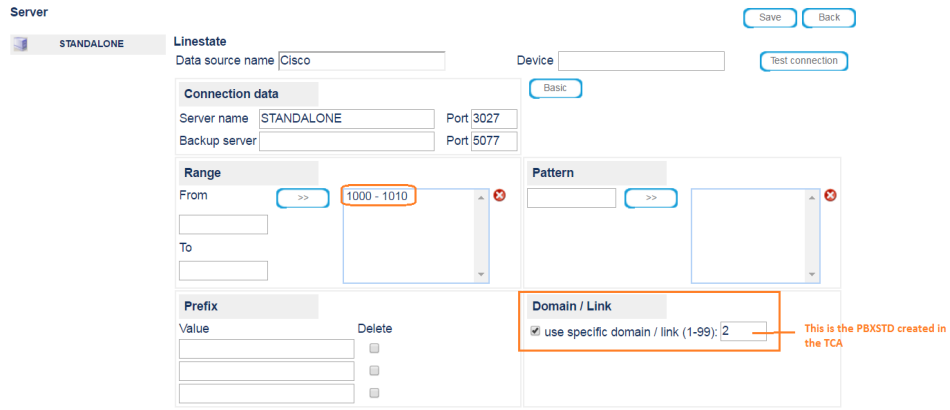


Configuring webadmin

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



Inside Data Source, click **Advanced**.

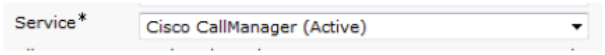


The Domain / Link number is defined.

*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:

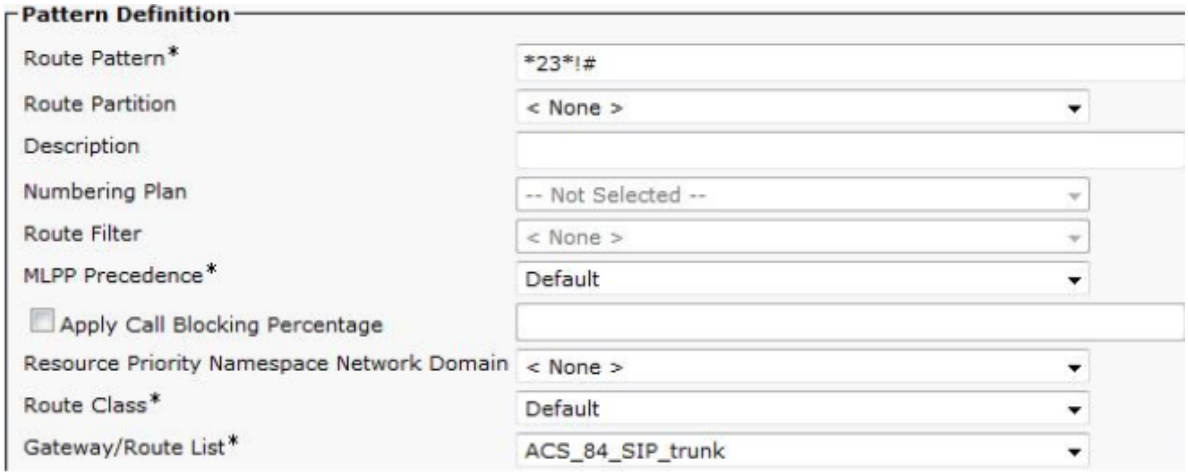


2. Create the route pattern for the *23 service

   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:

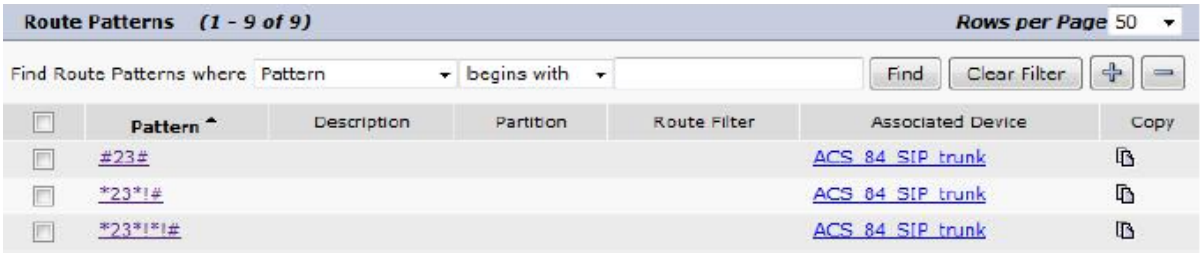
- #23#
- *23*!#
- *23*!*!#

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



   d. Click **Save** when finished.

The new patterns are displayed in the Route Patterns list:



*21 Service Configuration

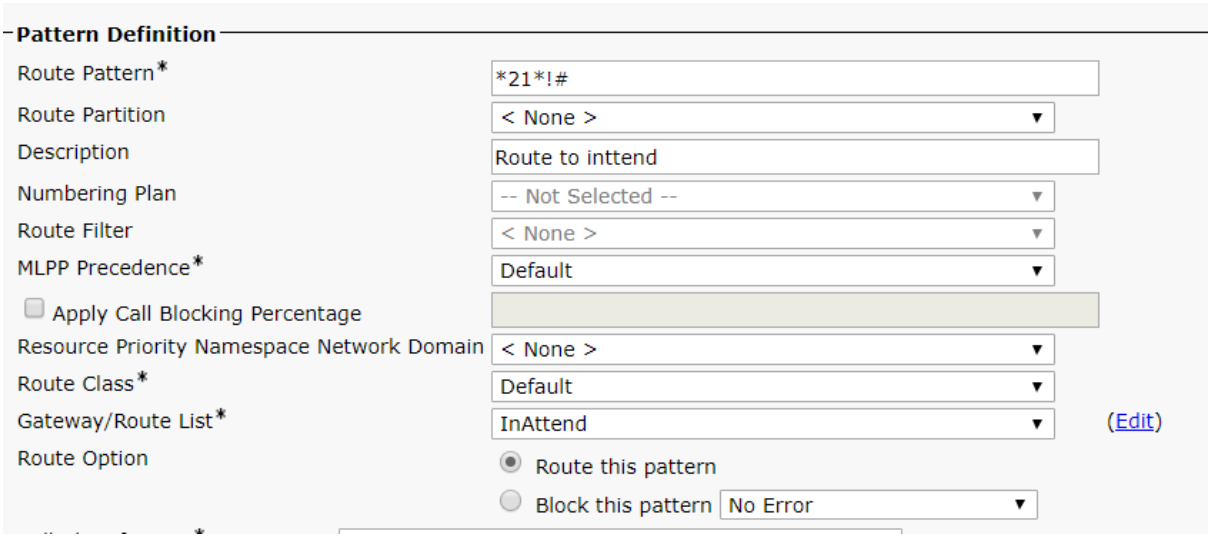
1. In Cisco Unified CM Administration interface, under **Service Pararmeter Configuration**, set the **Strip # Sign from Called Party Number** to **False** for the Cisco Call Manager service:

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**.



   d. Click **Save**.

The new patterns are displayed in the Route patterns list:

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

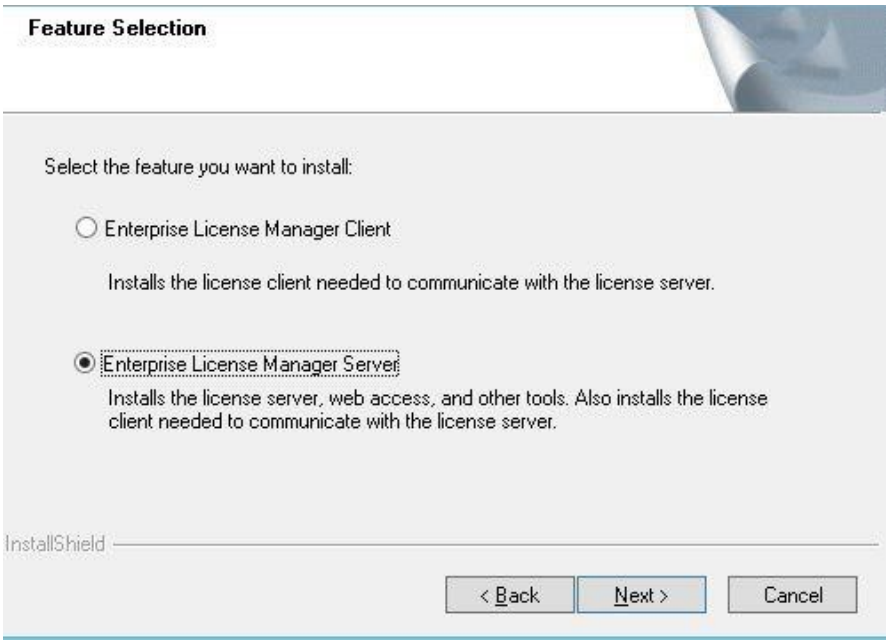
Enterprise License Manager (ELM) is the client/server-based licensing server where InAttend product licenses are requested, stored, and managed. The Mitel Installer offers installation for both the server component (which maintains licenses and enforces limits) and the client component (which is used 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:

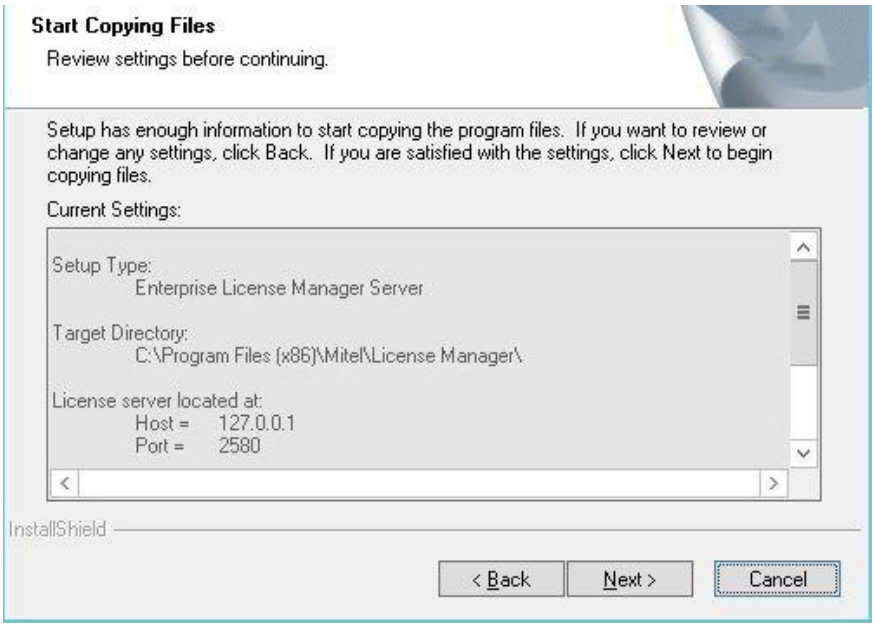
1. Double-click the **Install.exe** file in the top-level directory of your software package to launch the Mitel Installer.
2. In the Installer main window, click **Install**.
3. In the Install Wizard, select **Install ELM Server/Client**.

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**.



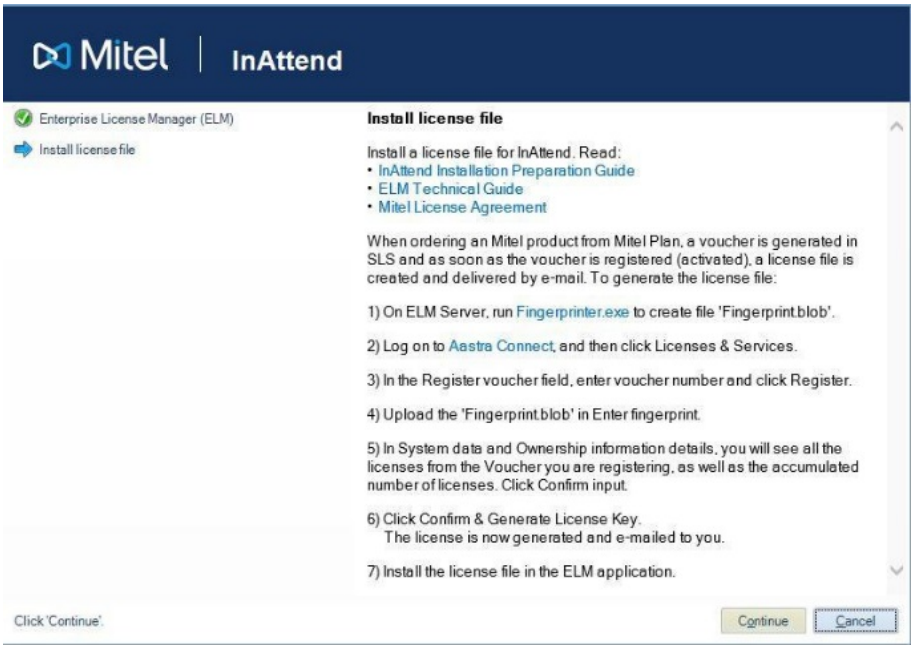
7. On the Choose Destination Location page, specify the installation path (either accept the default or browse to another location) and click **Next**.
8. On the License Server Options page, accept the default **Port** setting of 2580 and click **Next**.

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



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**.



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.

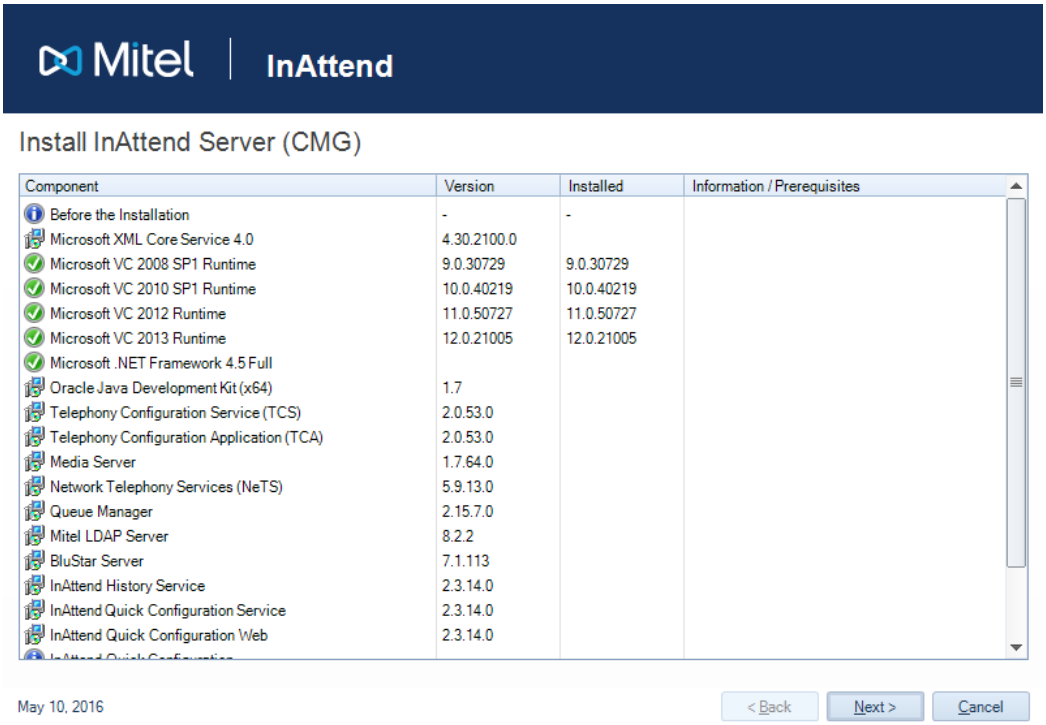
NOTE: InAttend can use CMG Server, BluStar Server (BSS) or any other LDAP-enabled directory for directory searches. If CMG Server is used, CMG - Web has to be installed prior to the InAttend installation.

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)

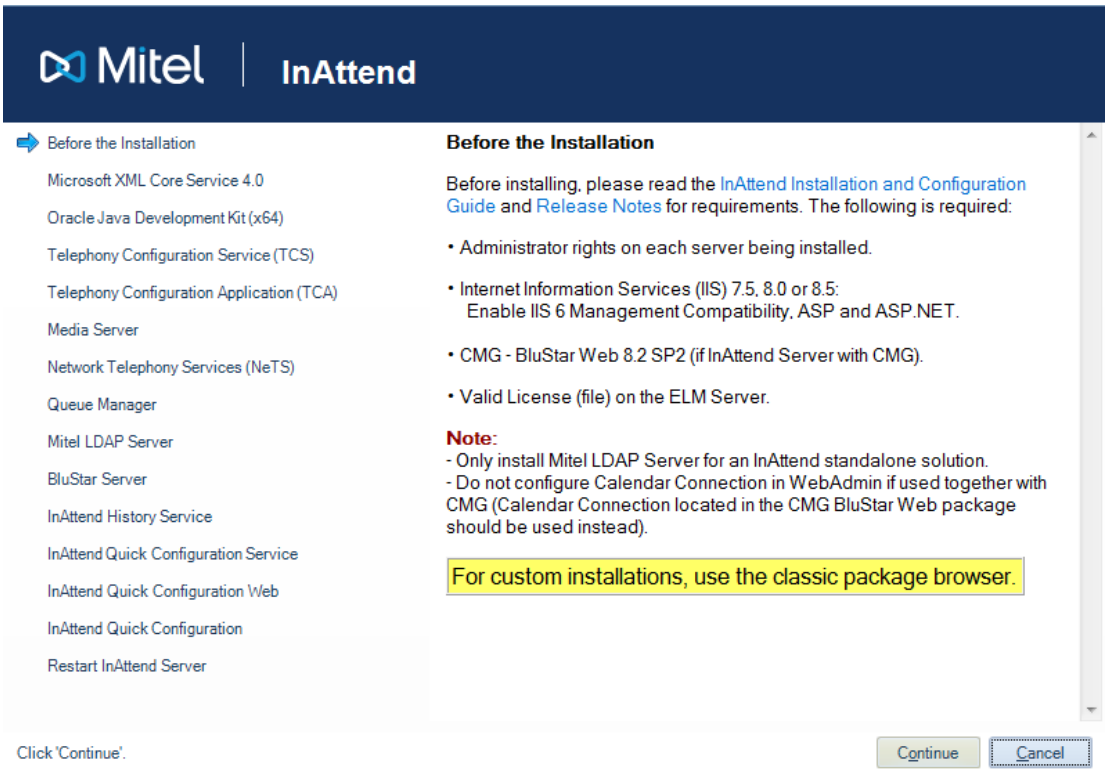
To install the InAttend Server software, do the following:

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.



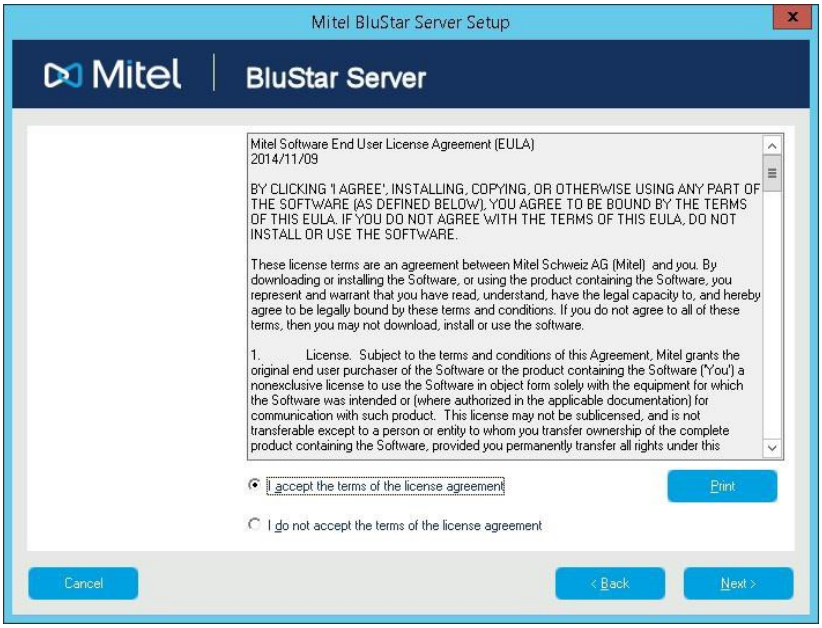
Components with a green check mark are already installed. Components with a red circle require a prerequisite that has not yet been installed. For example, the License Manager has to be installed before the InAttend installation can continue.

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.

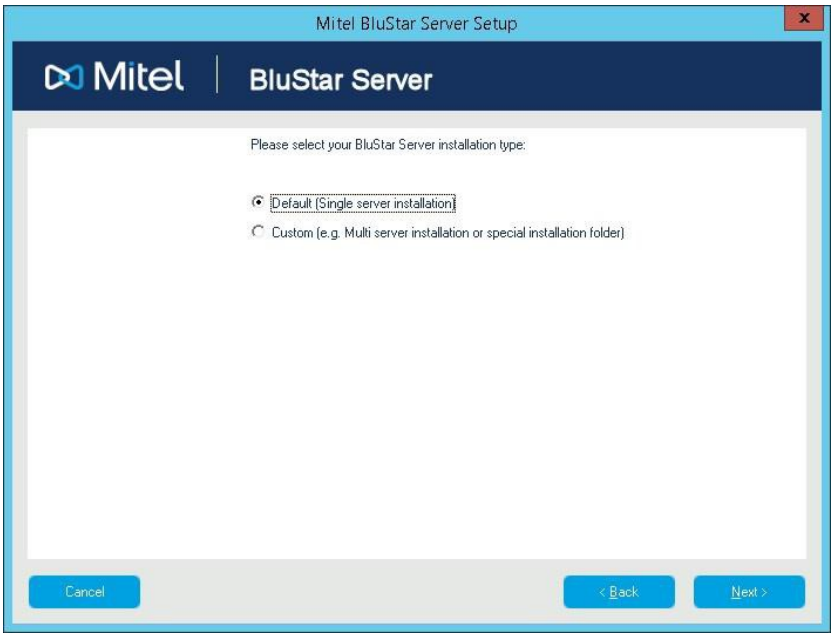


The Wizard proceeds with software installation. The blue arrow in the left panel indicates installation progress.

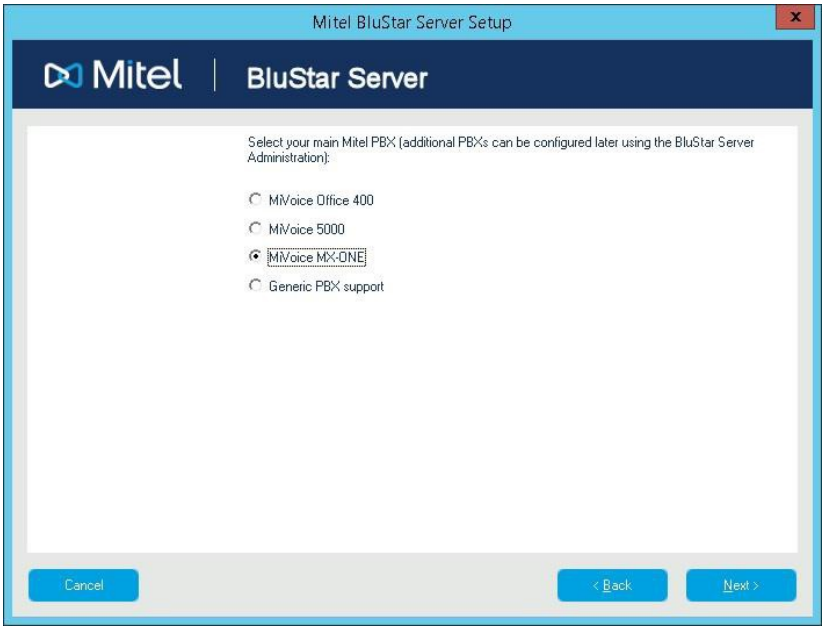
8. **For InAttend Server (CMG) installations only**: The Wizard launches the LDAP server installation wizard. InAttend requires LDAP server information to retrieve information using LDAP from a data source such as Active Directory. You configure the LDAP Server to connect to the CMG database with administrator 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.
9. 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**.



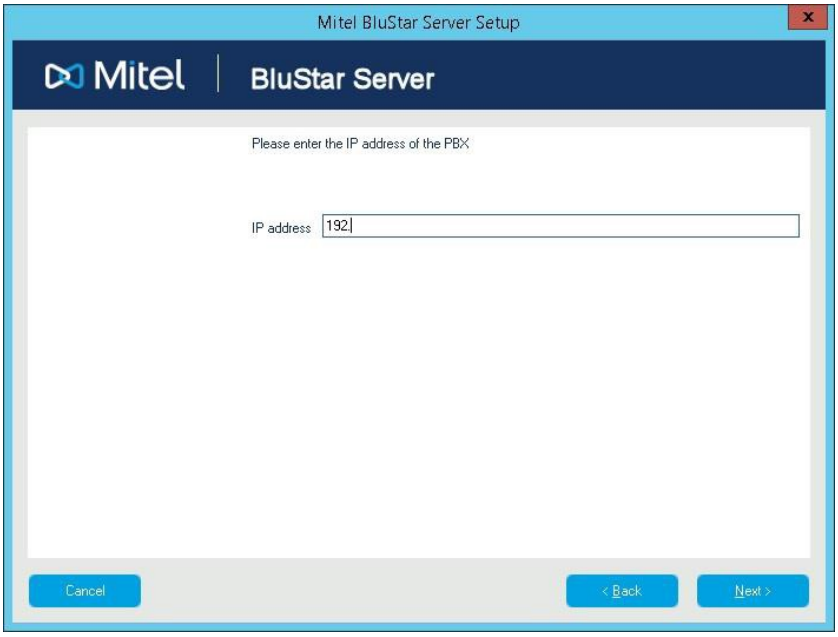
10. Select the BluStar Server installation type and click **Next**.



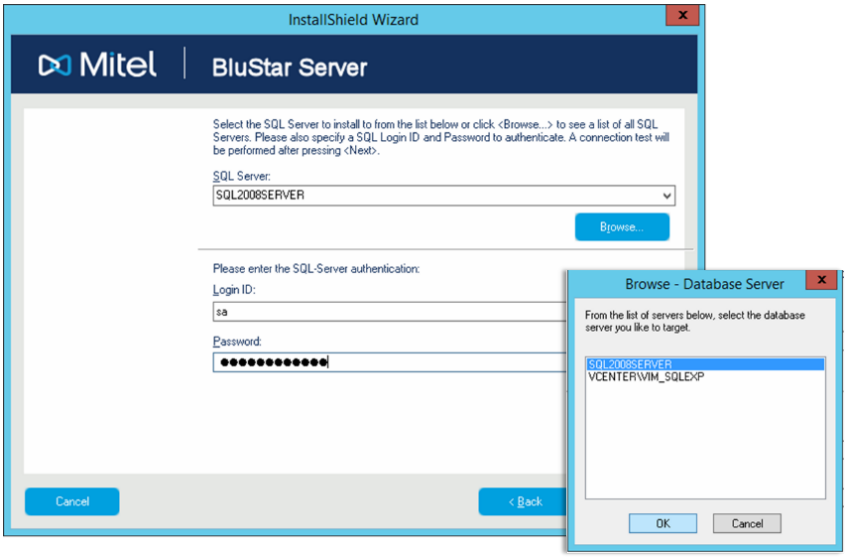
11. Select your call manager platform type and click **Next**.



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



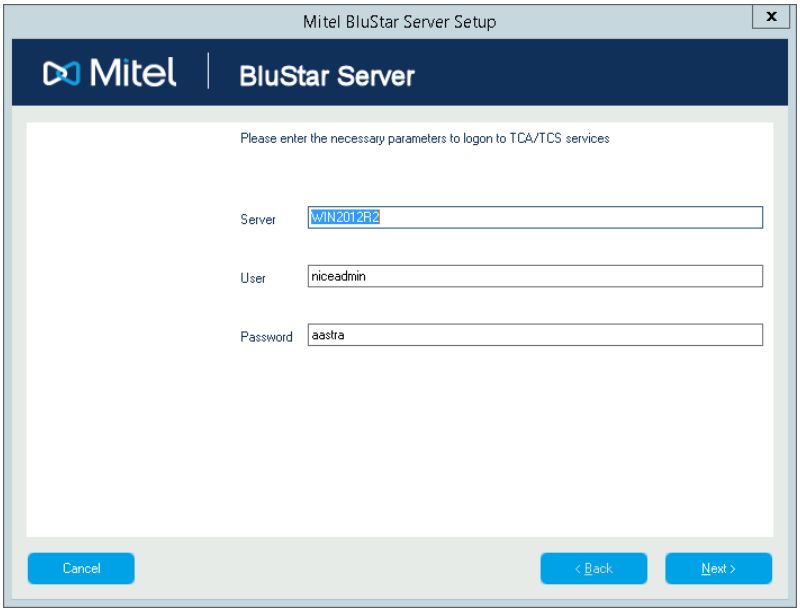
13. Enter the IP address or FQDN of the SQL server or click **Browse** to search for it. Specify the SQL login credentials and click **Next**.



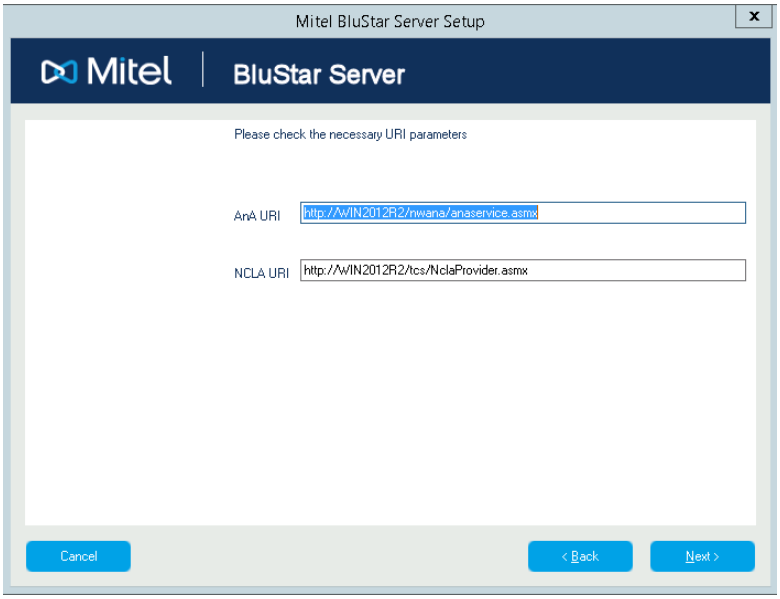
The Wizard installs the BluStar Server components.

14. **For InAttend Server (CMG) installations only**: There are additional configuration steps when you install InAttend in a CMG system.

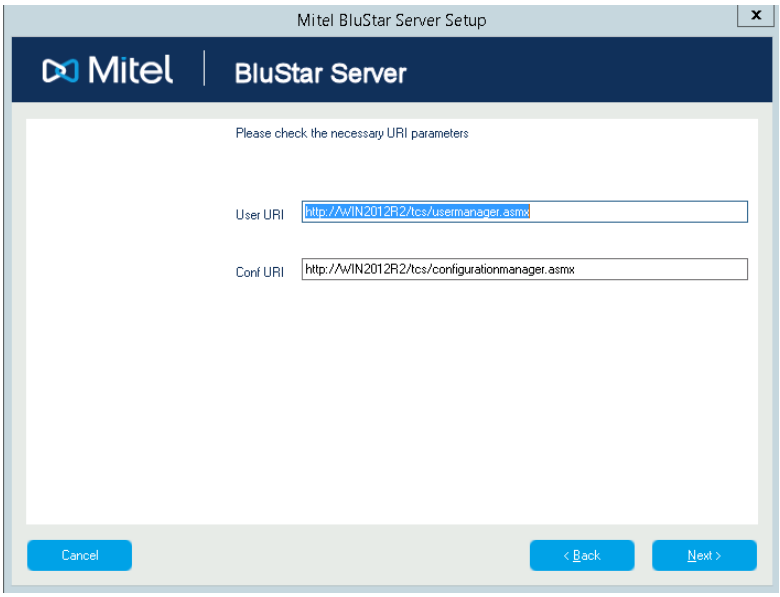
    a. Specify the credentials to access the Telephony Configuration Application (TCA) and Telephony Configuration Service (TCS) services and click **Next**.



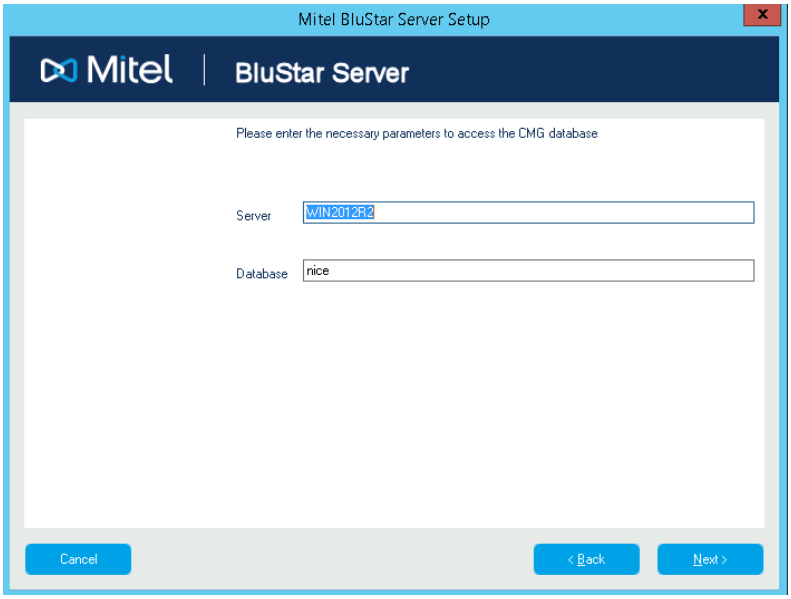
    b. Verify the URIs for the Authentication and Authorization (AnA) service and the NCLA service. Make the necessary changes and click **Next**.



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



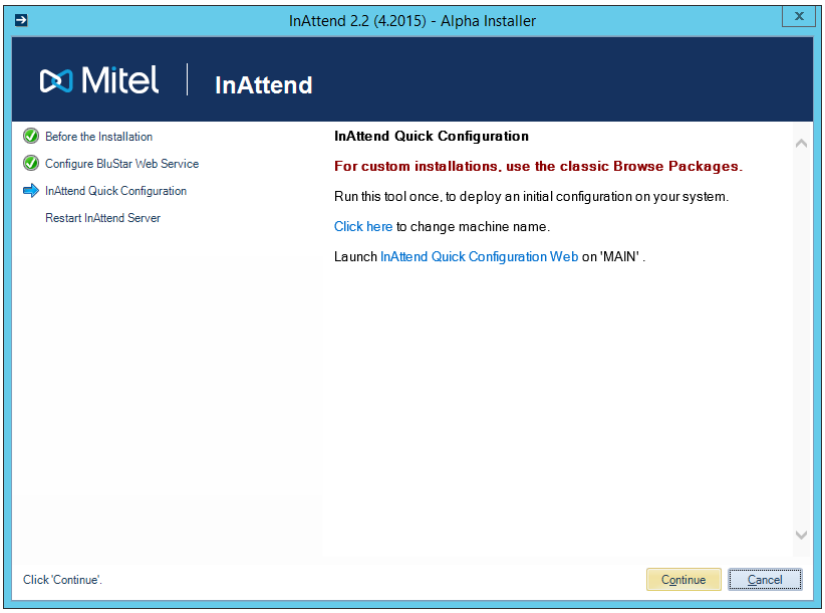
d. Specify the server hosting the CMG database and the name of the database and click **Next**.



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).



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

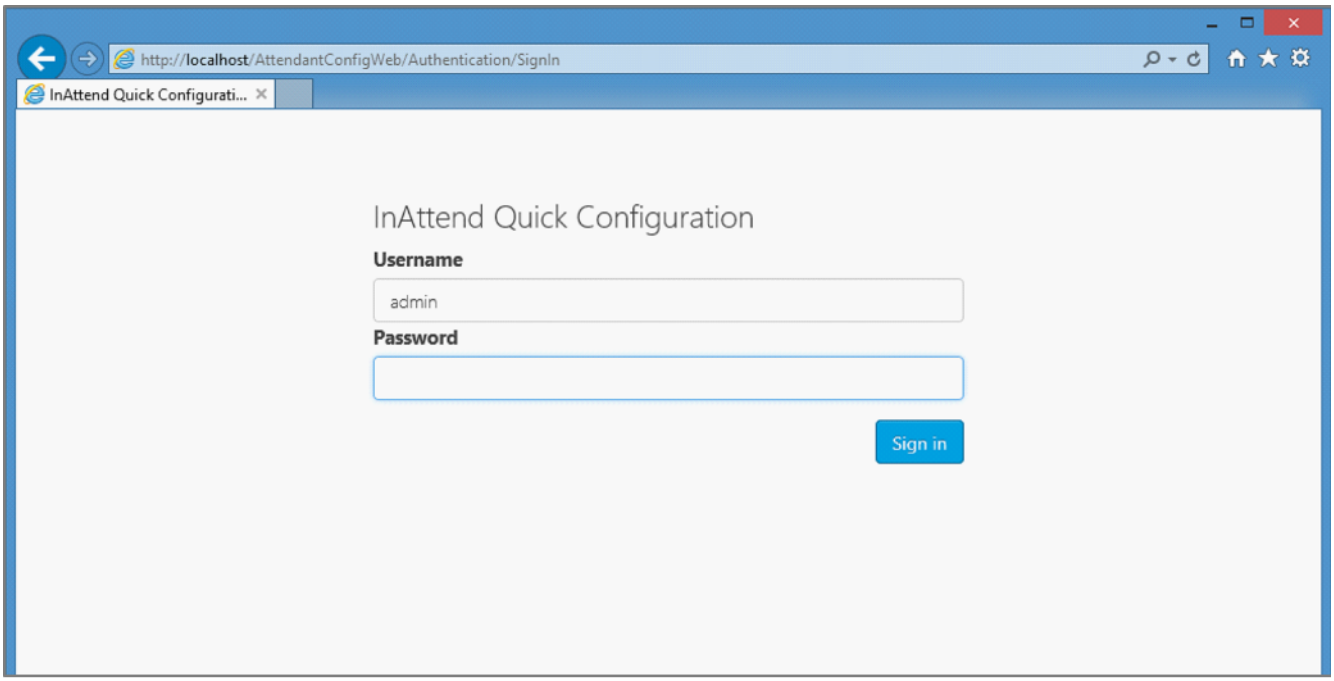
After the server has restarted, you have to configure the InAttend system.

- 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.

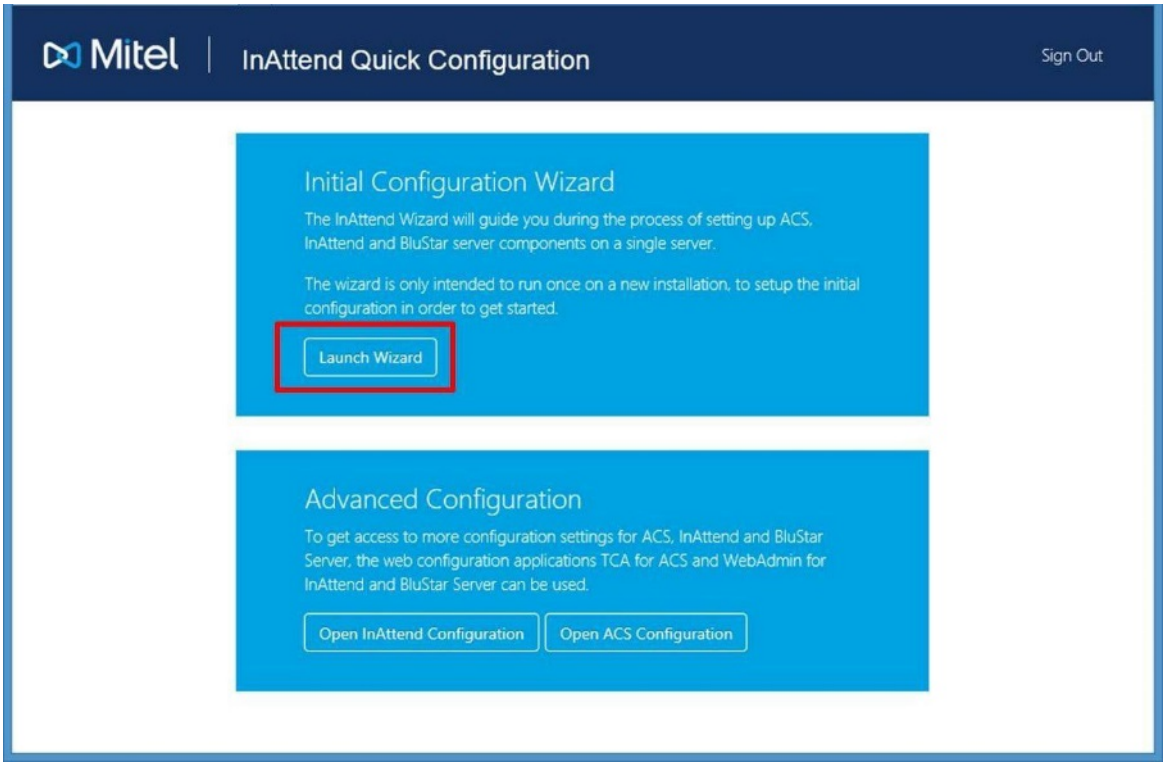
Running the Quick Configuration Wizard

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

1. 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**).



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



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 SIP domain for which Skype will act as a phone manager. (Normally this is the string after the @ in the SIP address.
User URI	Enter the system user name for InAttend in Skype, including full domain address.
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>
```

```
    </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 stand-alone 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.

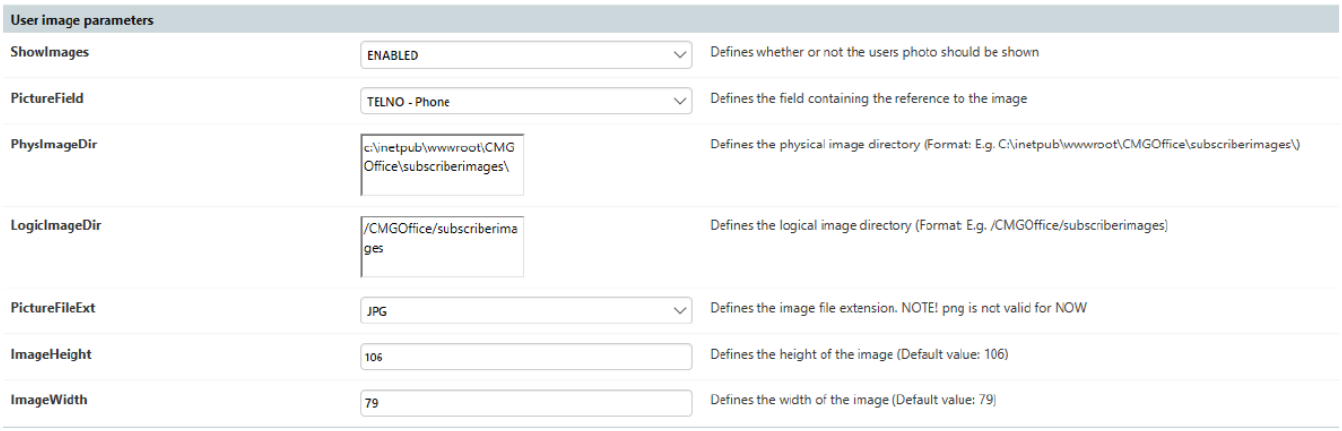
1. Open the `web.config` file for TCS and TCA.
2. Change the value of the following parameter by replacing "localhost" with the server hosting the AnA web service:

```
    <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.

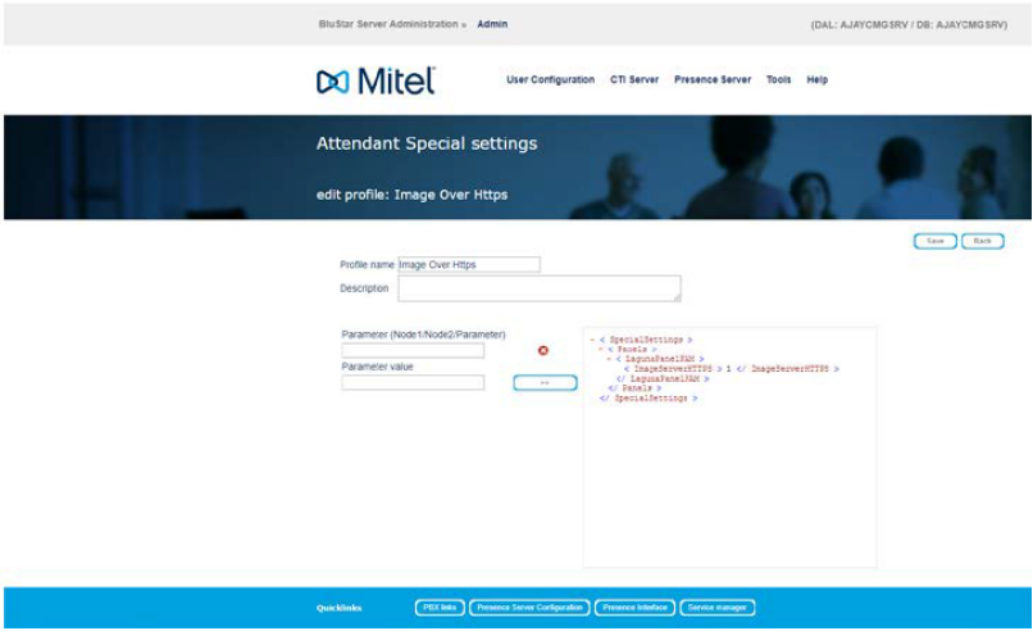


The steps to be followed for CMG deployment are as below:

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://serverIp>/webadmin/subscriberimages/**

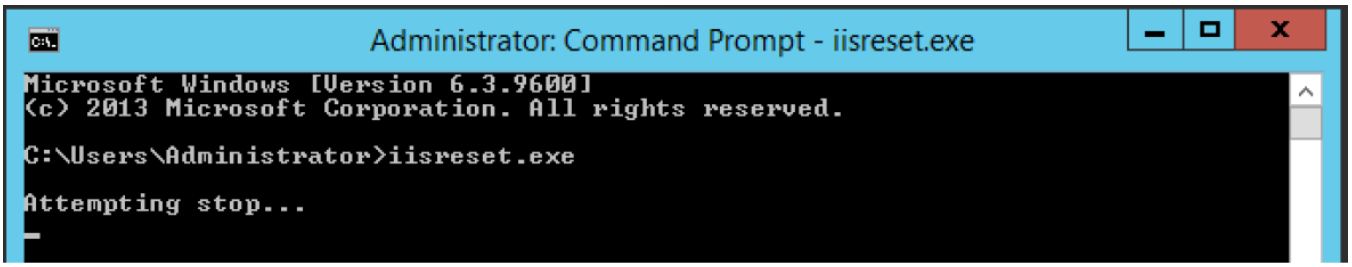
To allow secure transmission of the image, the **Special settings** must be enabled in the Webadmin to securely fetch the image using HTTPS.



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)

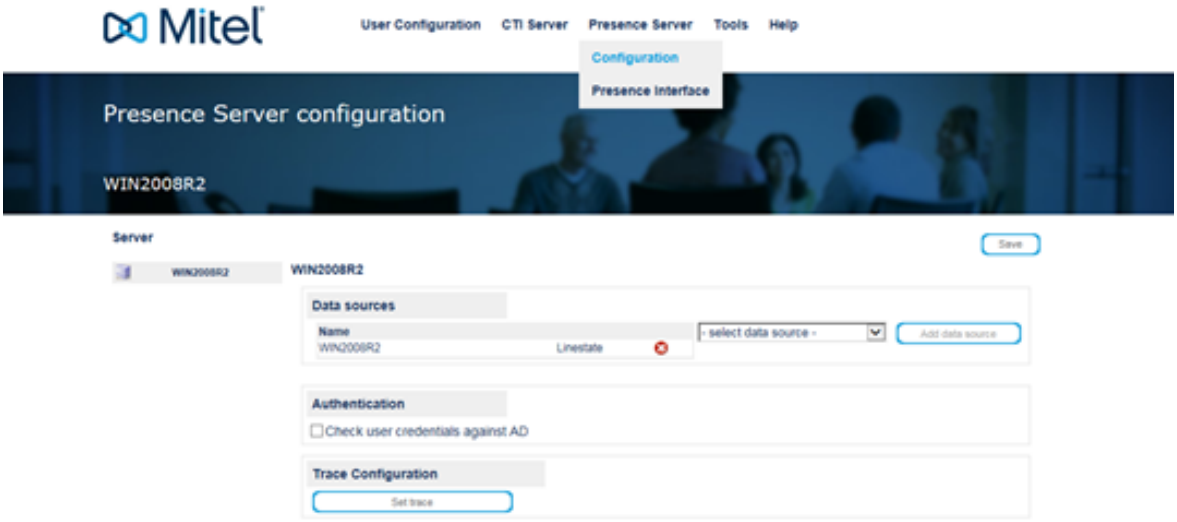
NOTE: If you configured Exchange or Skype for Business settings during configuration of the InAttend Server (see “Running the Quick Configuration Wizard”), a data source for the Presence Server is already present.

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.



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.

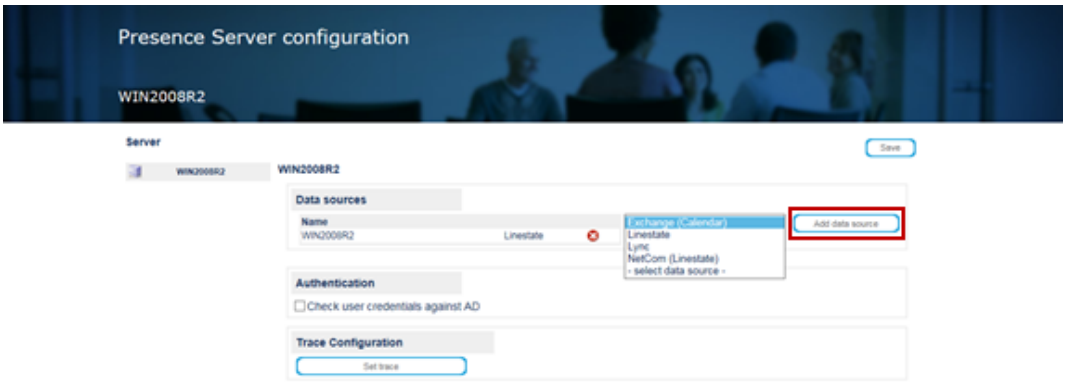
Adding a Microsoft Exchange Data Source

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.

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.

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

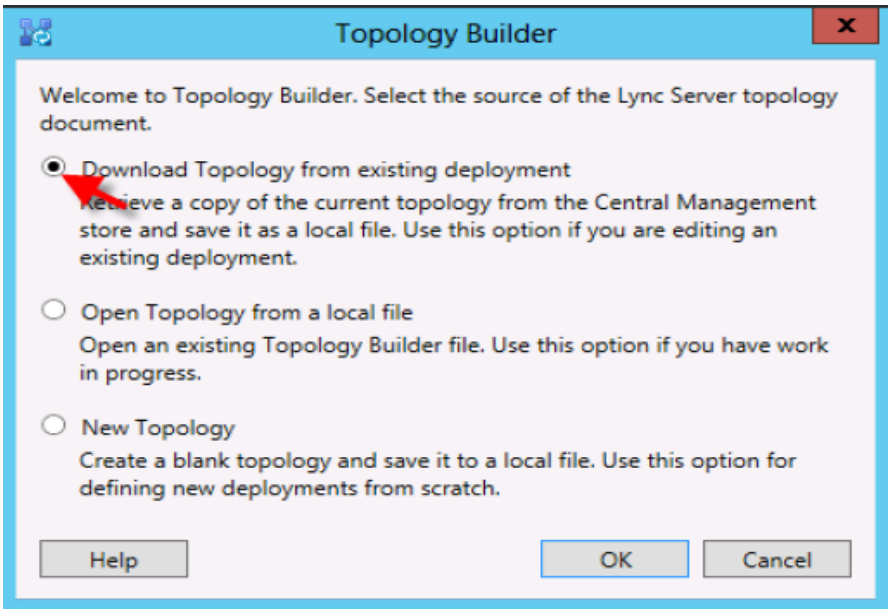
You have to be logged in as a user with domain administrator rights.

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

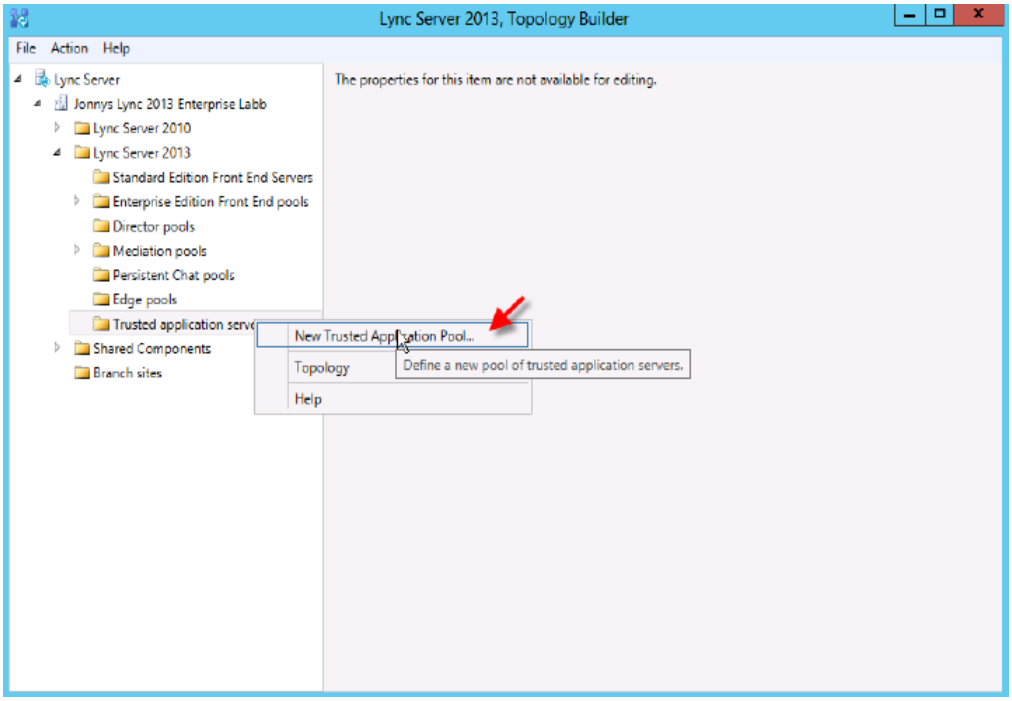
To create the application pool and trusted application, do the following:

1. 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**.
4. 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**.



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.

1. 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.

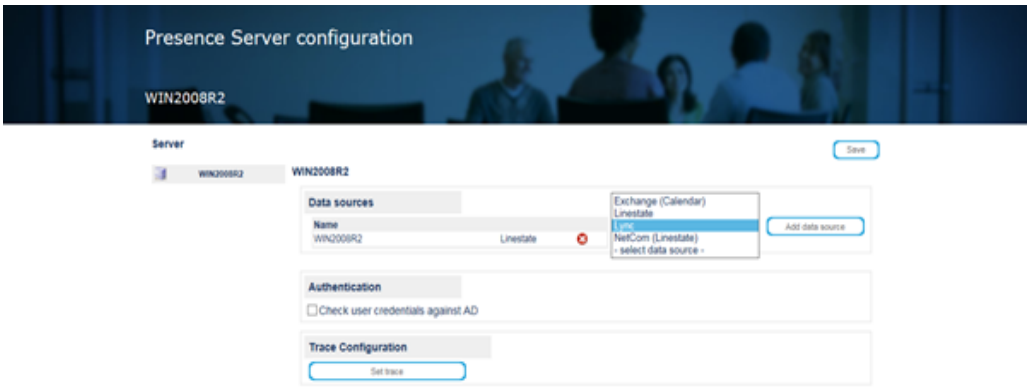
Adding a Data Source

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).

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:

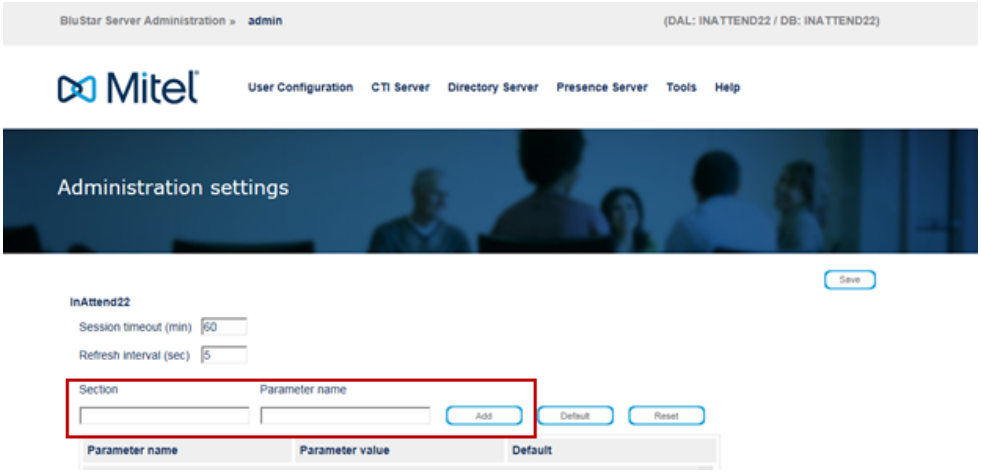
1. Log on to the web-based Cisco Unified CM IM and Presence Administration tool.
2. Ensure that the SIP Listener port is on:
   a. Select **System > Application Listeners**.
   b. Check that there is a **Listener Type** of “SIP”, with the port set to 5060.
   c. Click **Save** to apply your changes.
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:

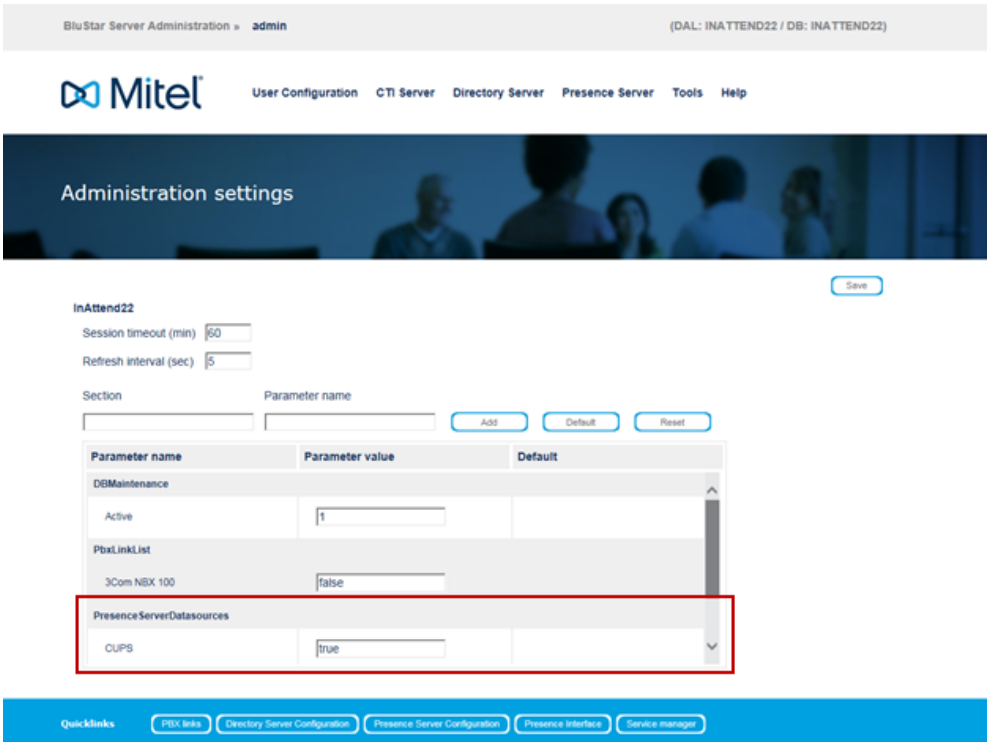
1. In the WebAdmin tool, select **Tools** and then **Administration settings**.
2. Create a new parameter for the CUPS:



   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”.



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.

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

Adding a line state data source

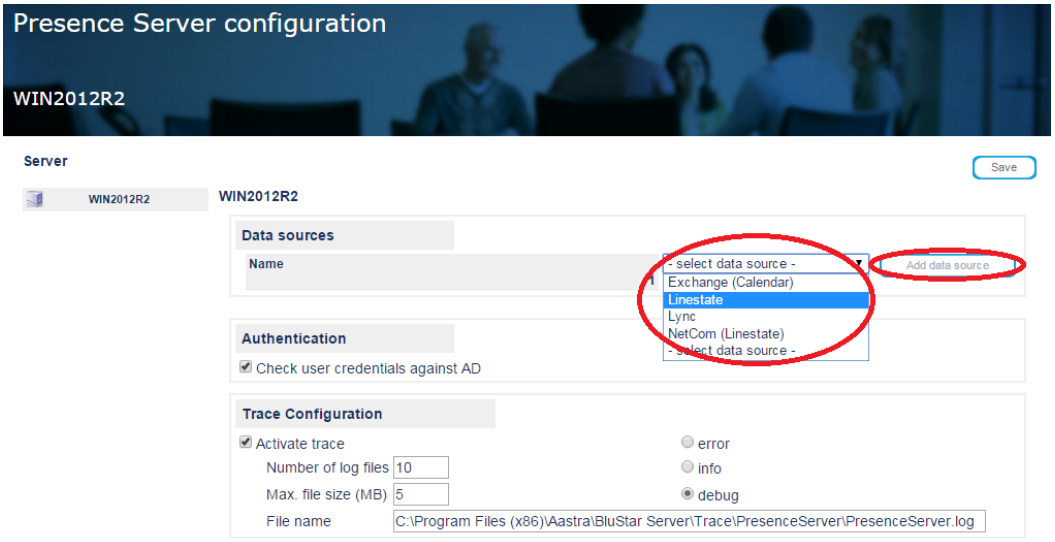
The Presence Server uses line state information to calculate user availability. You have to configure a line state data source for the PBX as a source for the Presence Server in addition to other data sources (e.g., calendar).

- 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:

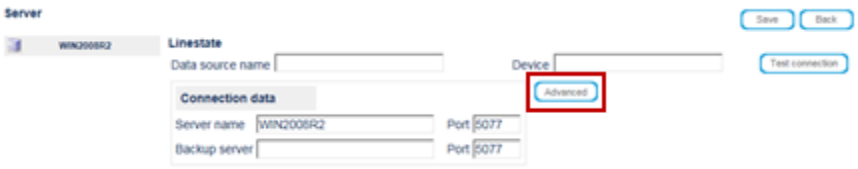
1. On the Presence Server configuration page, select the **Linestate** option from the data source type drop-down list and click **Add data source**.



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).
3. 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.



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)

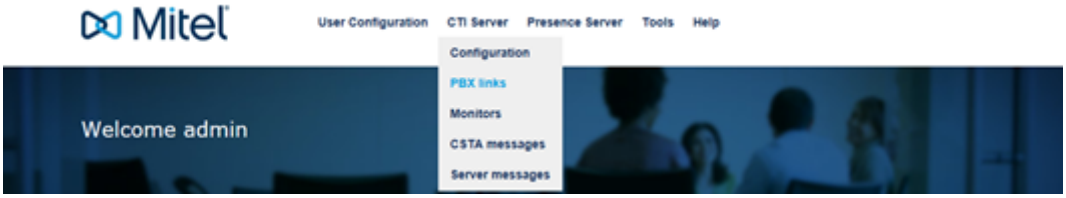
A PBX link is a connection from the CTI Server (a component of the BluStar Server) to an MX-ONE call manager. The InAttend system can support multiple PBX links simultaneously (for example, for installations with multiple offices that have separate communication servers).

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:

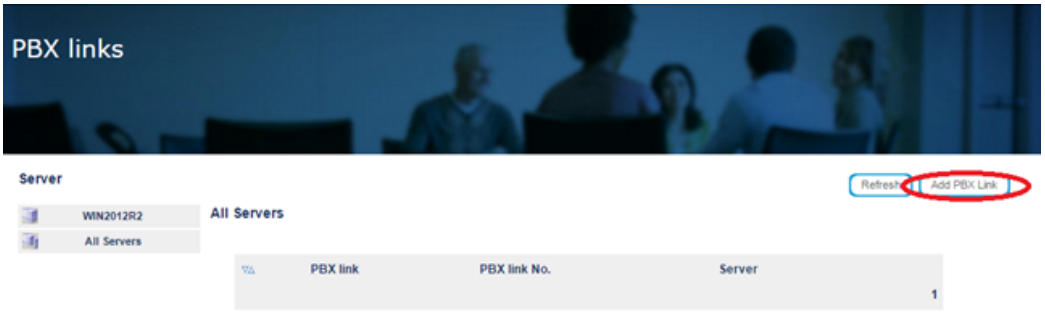
1. Access the BluStar Server Administration web interface by typing `http://<hostname>/webadmin` in a supported web browser, where <hostname> is the InAttend server address.
2. Log in with the administrator credentials (default username: admin, default password: Mitel123).

3. Select **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**.



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:

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.

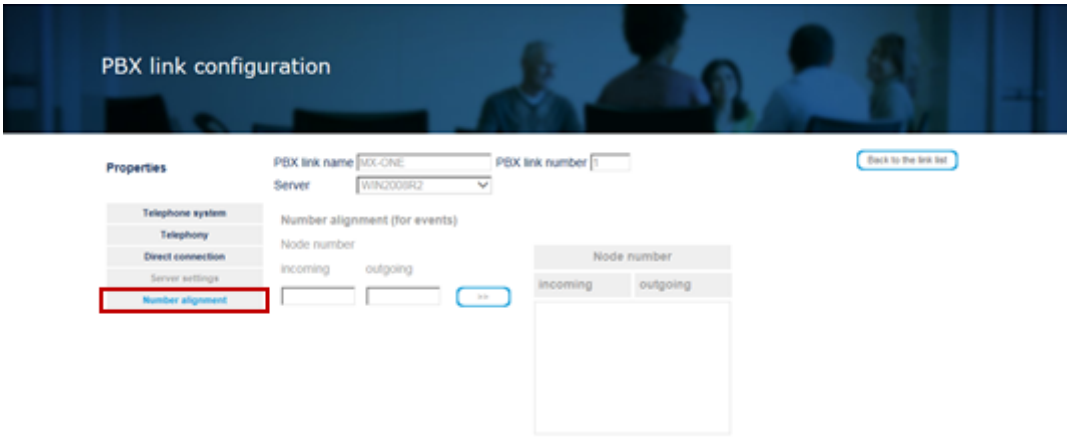
External line prefix: the prefix used for external extension numbers.
Area code prefix: the prefix to be used with the area code (e.g., “0” if the area code is “0711”).
Area code: the area code of the server location.
Use phone number block from/to: the sequence of numbers from devices running on this 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.

8. 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.



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.

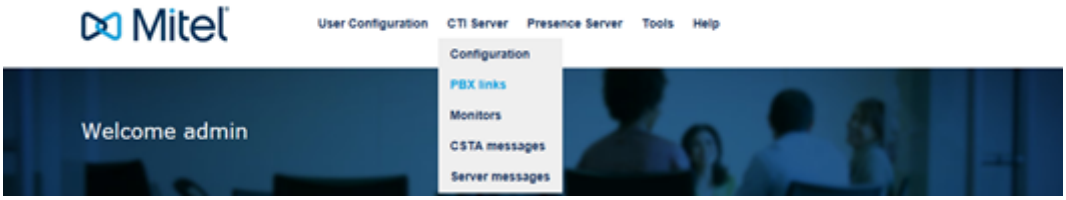
10. Click **Save** to save your changes.

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

Configuring a PBX link for line state (MiVoice 5000)

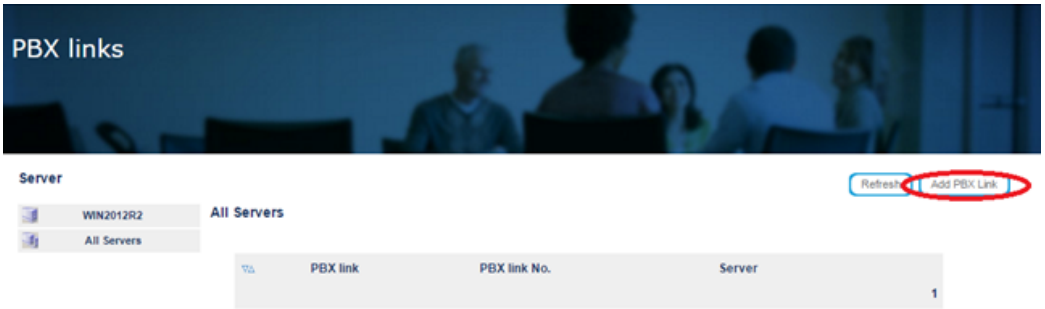
You must create a PBX link so that the CTI Server uses the PBX link to retrieve line state information about specified devices.

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



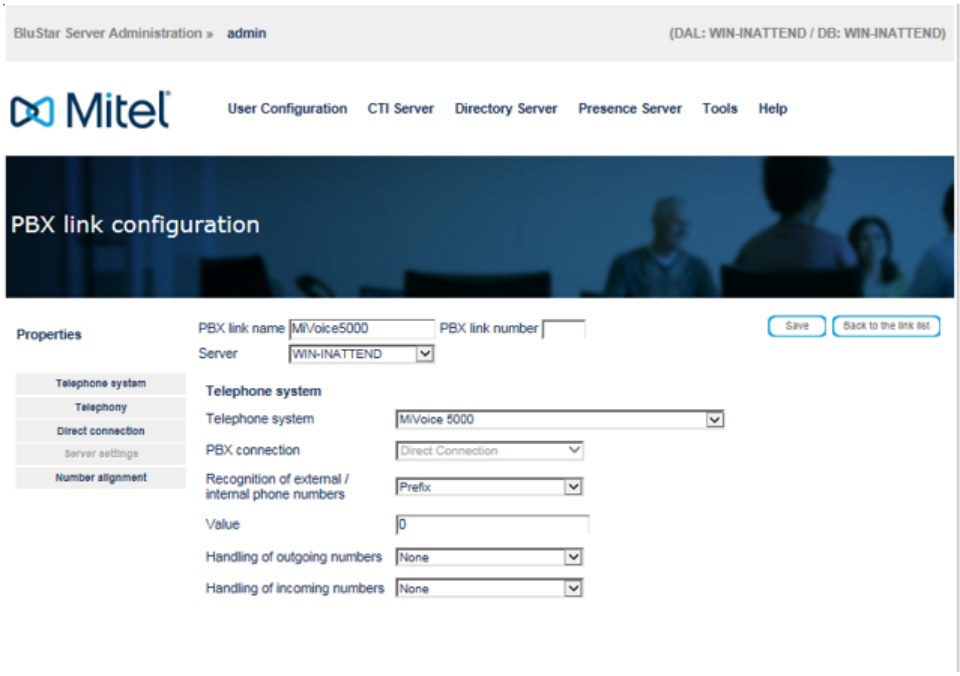
The system displays the PBX links page, and lists all configured PBX links.

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



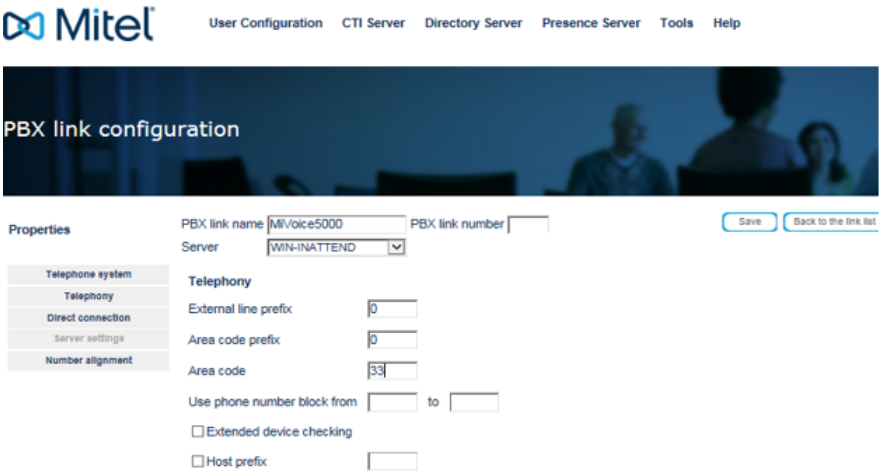
4. On the **PBX link configuration** page, enter values for the following parameters:
   - **PBX link name**: the name for the connection.
   - **Server**: select the InAttend Server from the drop-down list.

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



   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).

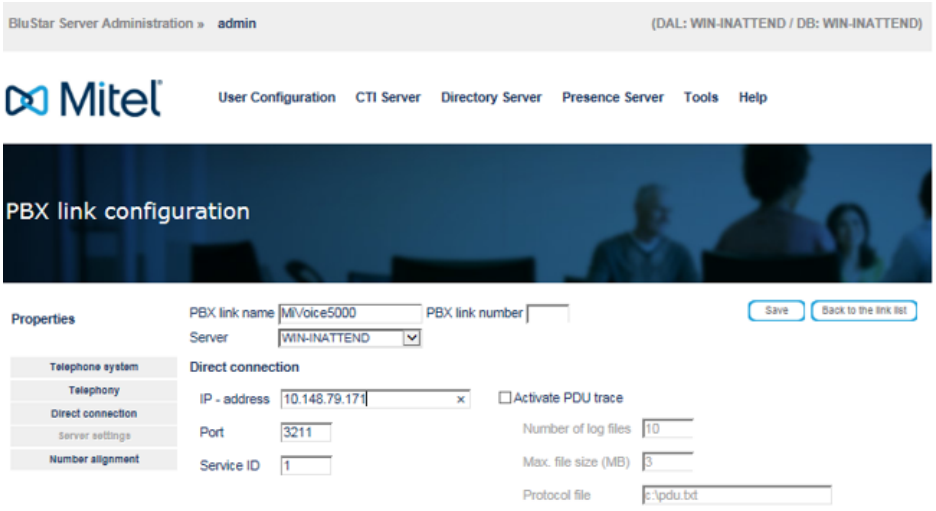
6. In the **Telephony** section, enter values for the following parameters:



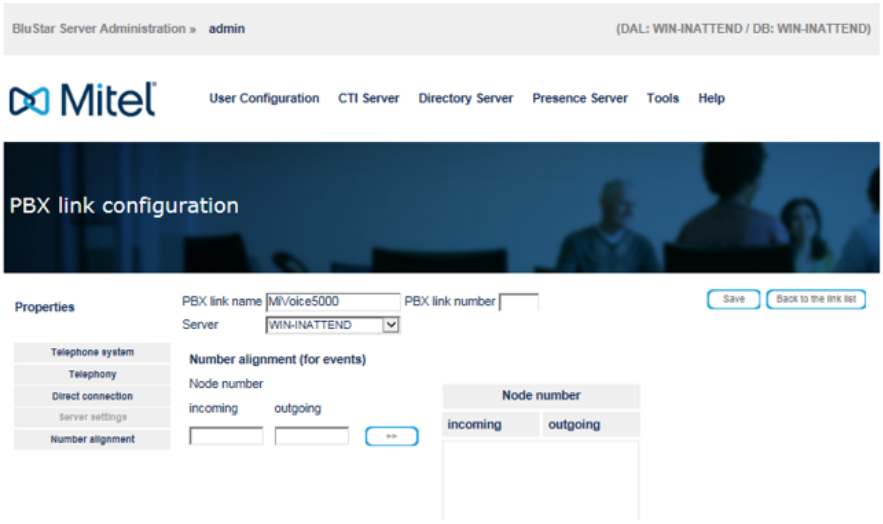
a. **External line prefix**: the prefix used for external extension numbers.
b. **Area code prefix**: the prefix to be used with the area code (e.g., “0” if the area code is “0711”).
c. **Area code**: the area code of the server location.
d. **Use phone number block from/to**: the sequence of numbers 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.

7. 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.

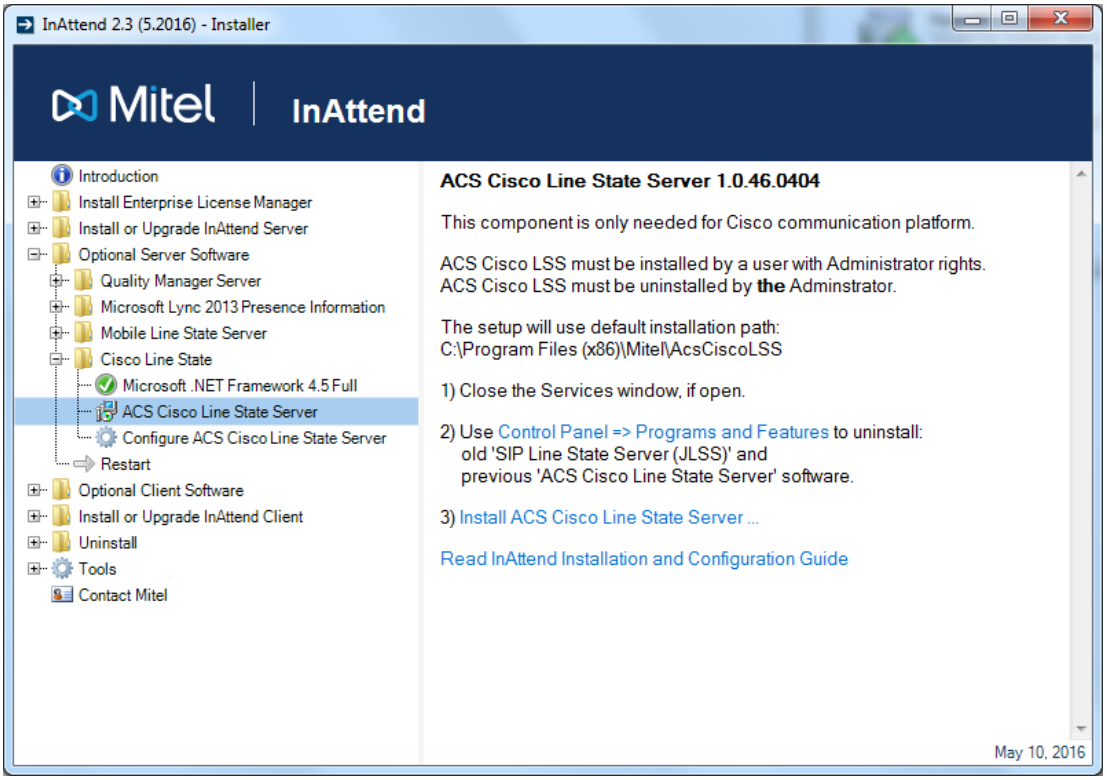
You have to have Microsoft .NET Framework 4.5 Full installed (available through the InAttend Install Wizard). If the InAttend server is running on Windows Server 2012/R2, .NET Framework 4.5 is already included.

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.

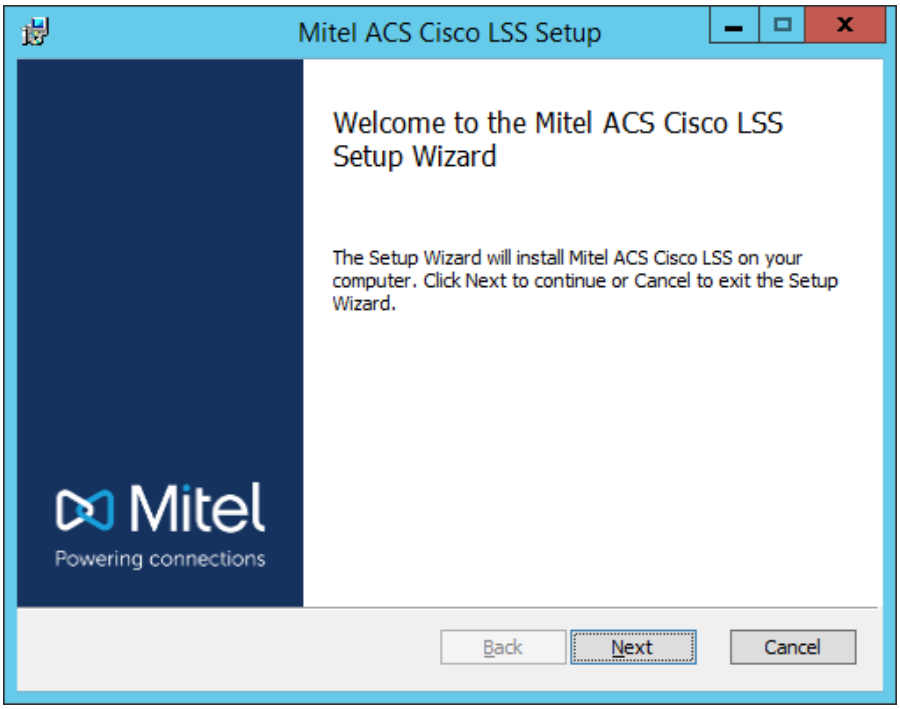
To install the Cisco Line State Server, do the following:

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**.



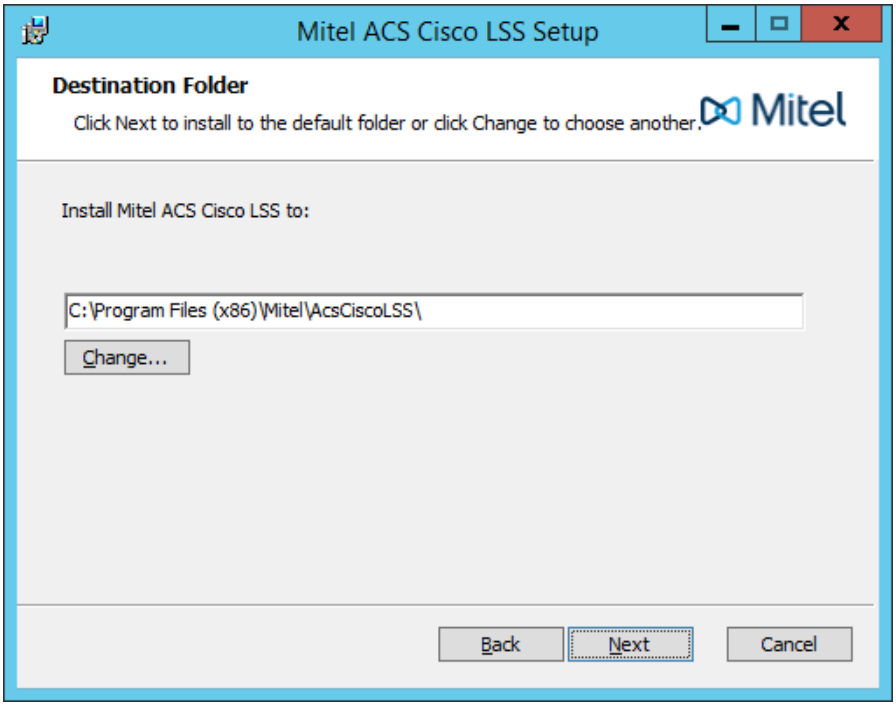
4. In the main window of the Install Wizard, click **Install ACS Cisco Line State Server**.

   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.



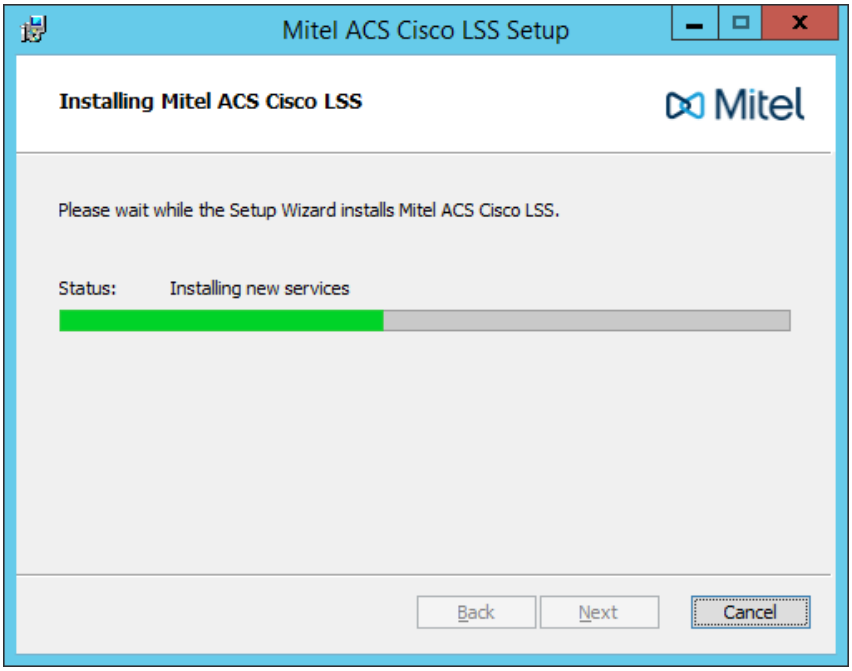
6. On the **End User License Agreement** page, review the terms of the license agreement, then check **I accept the terms in the License Agreement** and click **Next**.

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



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.



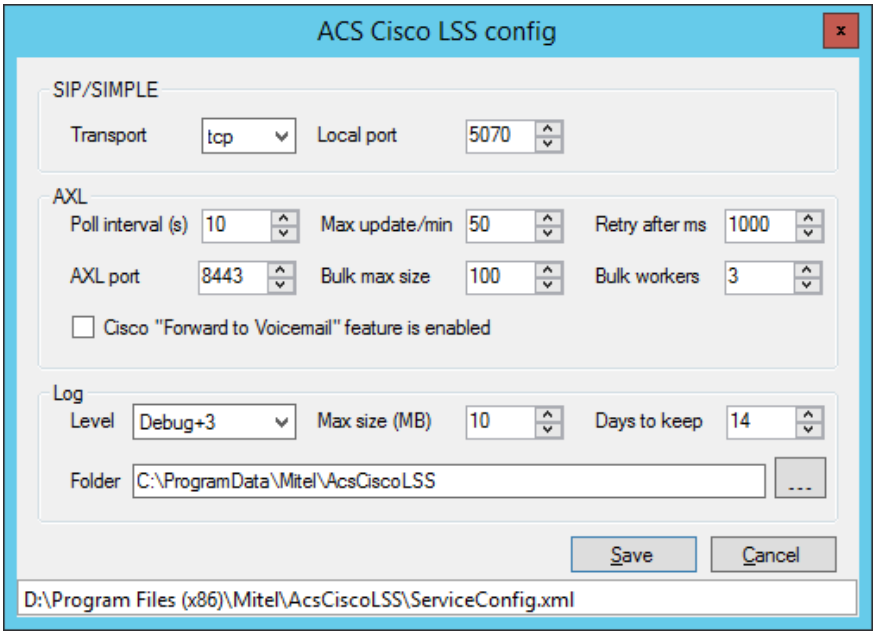
9. When the wizard completes the Mitel ACS Cisco LSS setup, click **Finish** to exit.
10. Restart the server. Click the **Click here to restart** link in the Install wizard.

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.

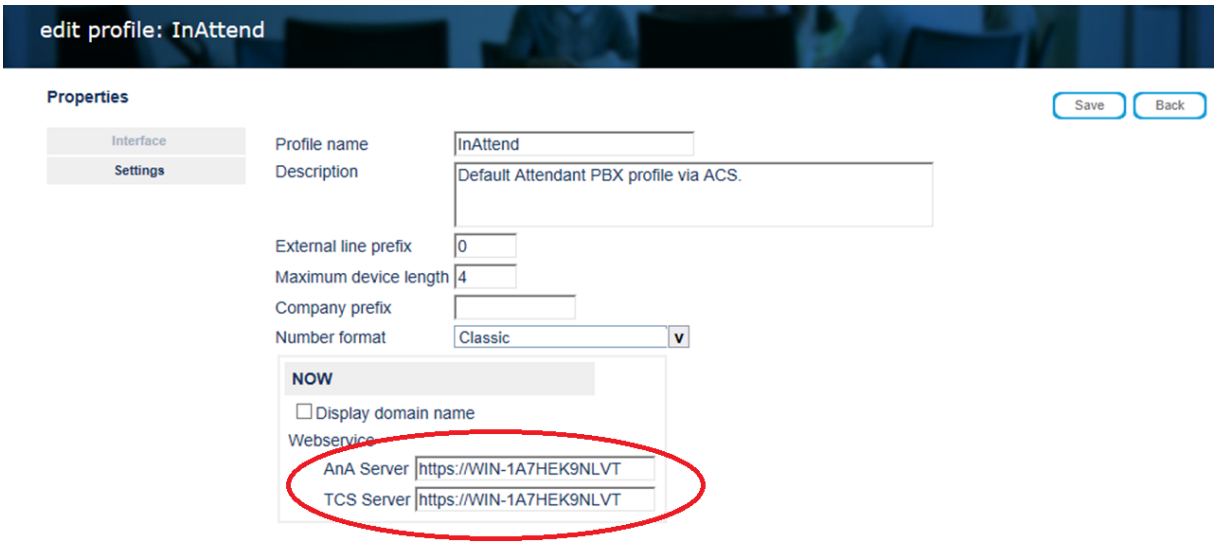


3. Click **Save** to save your changes.

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.



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.

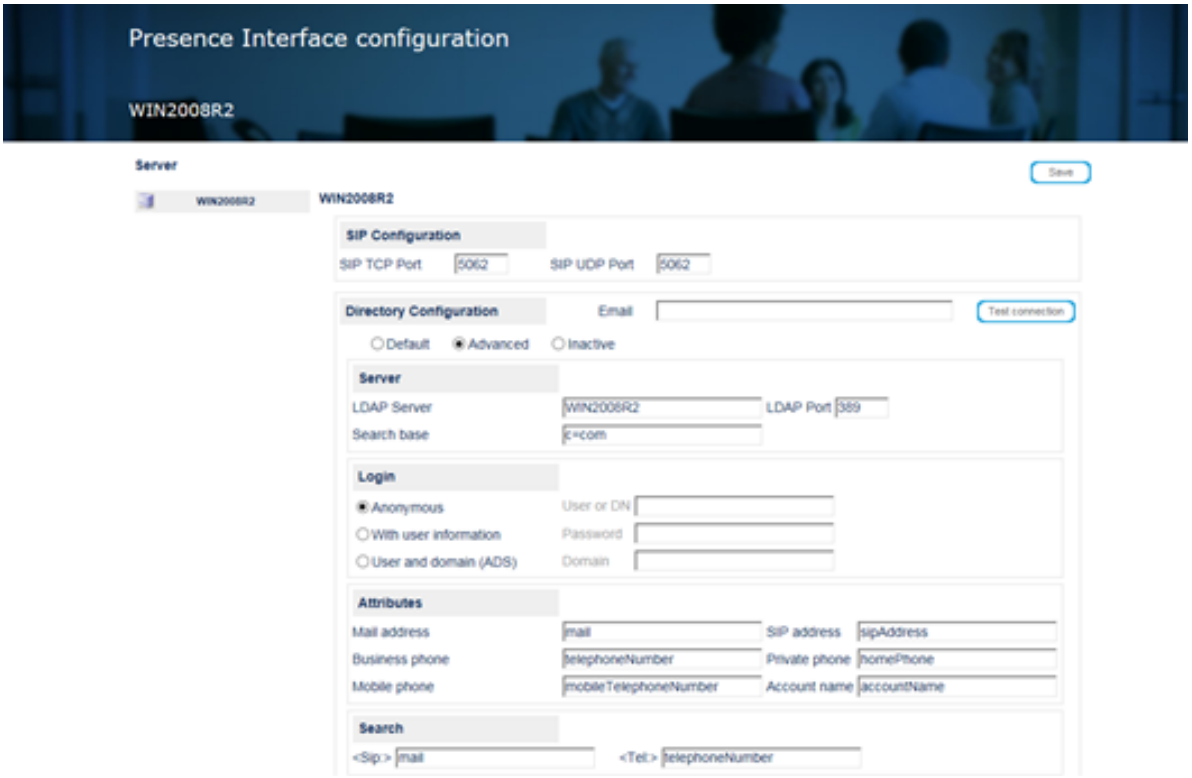
If you are not using the BluStar LDAP database, you can configure the Presence Server to connect directly to one external directory (e.g., Microsoft Active Directory) via LDAP. Note that with this configuration, every directory lookup on the Presence Server (e.g. each subscription) represents a direct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



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.

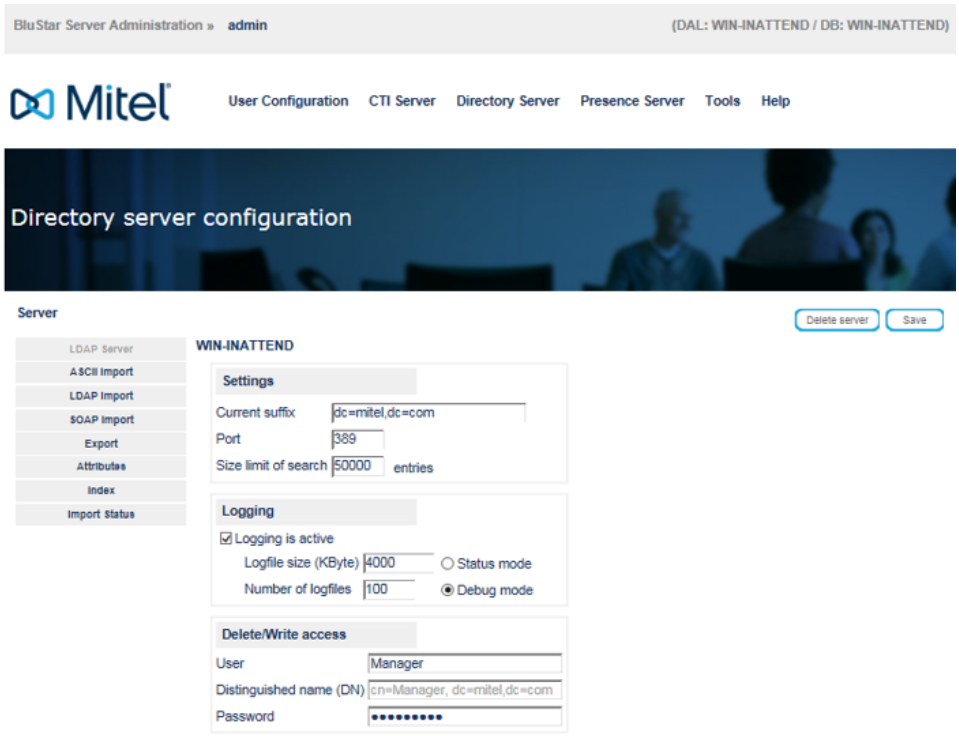
Configure Directory Server (MiVoice 5000)

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

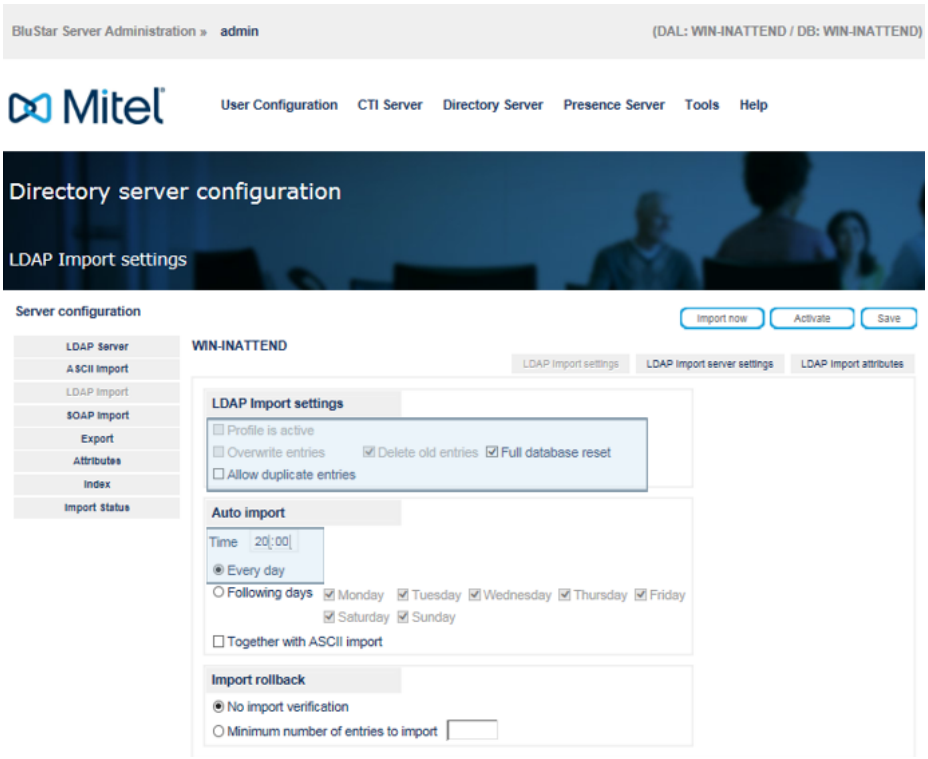
1. In the **Directory server configuration** page of BluStar WebAdmin, enter the following values for the parameters.
   a. In the fields under **Settings**, identify the LDAP server:
      i. **Current suffix**: enter dc=mitel dc=com
      ii. **Port**: enter the TCP/IP port number
      iii. **Size 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.

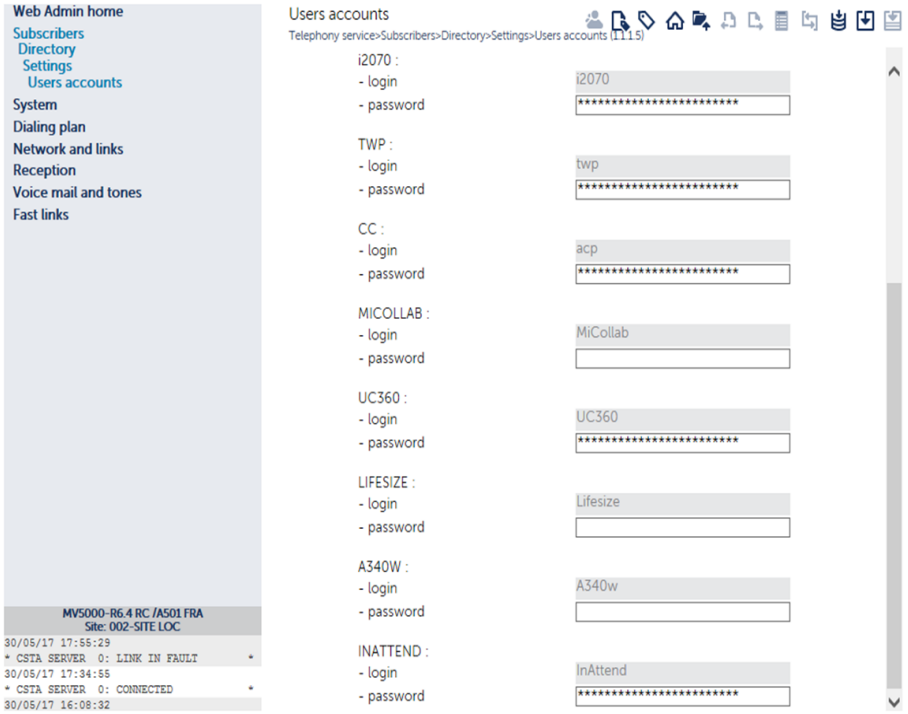
c. In the **Delete/Write access** section
   i. Enter the username.
   ii. Enter the password.



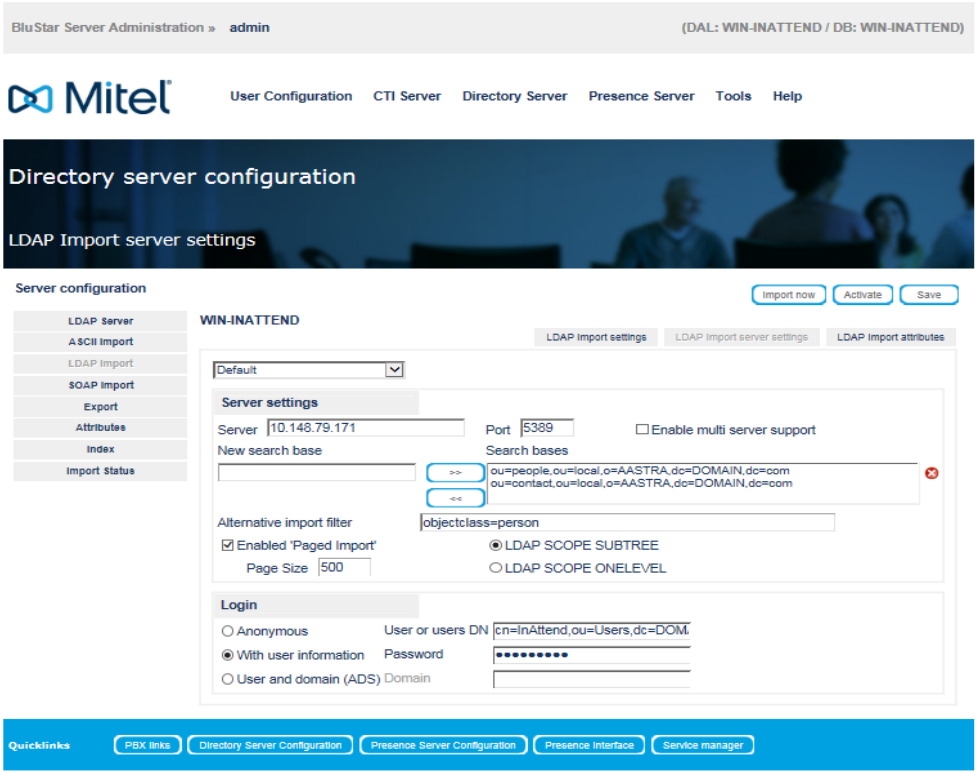
d. In the **LDAP Import settings** section,
   i. Check the **Delete Old entries** and **Full database reset** check box.
   ii. Choose **Every day** option for the Auto Import.
   iii. Choose **No import verification** for Import rollback



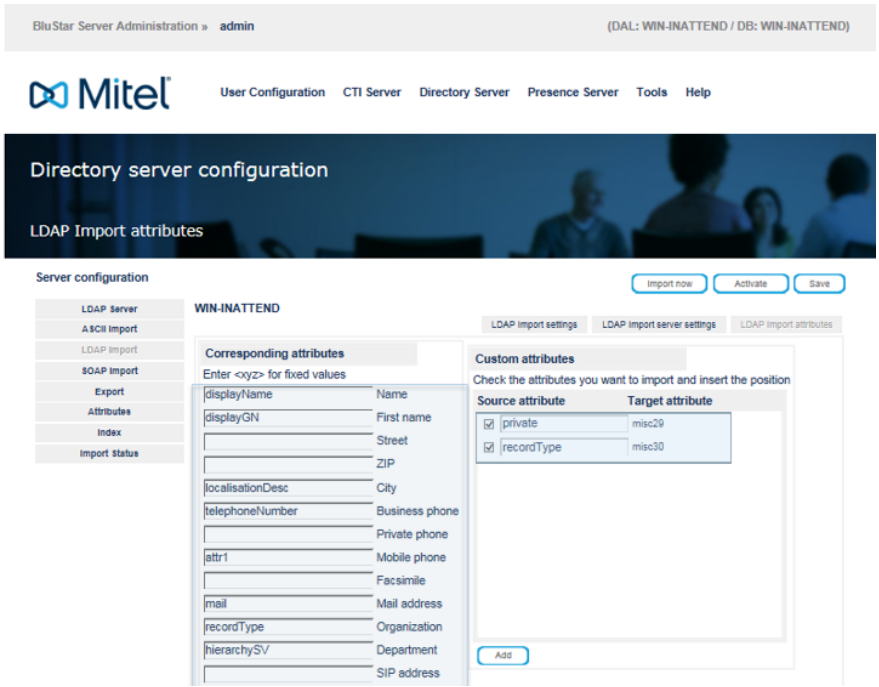
e. Enter the InAttend login credentials in the **User accounts** page.



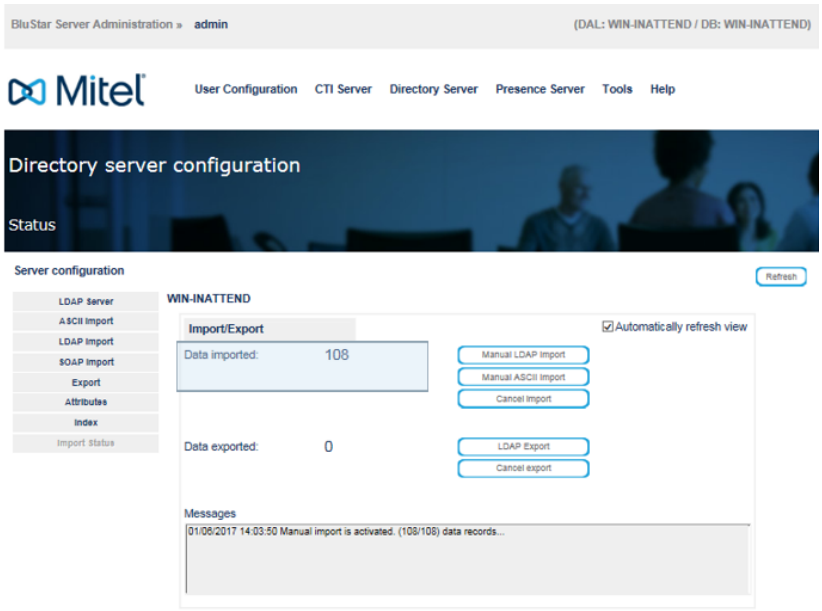
i. Use the same credentials in the **LDAP Import server** settings.



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



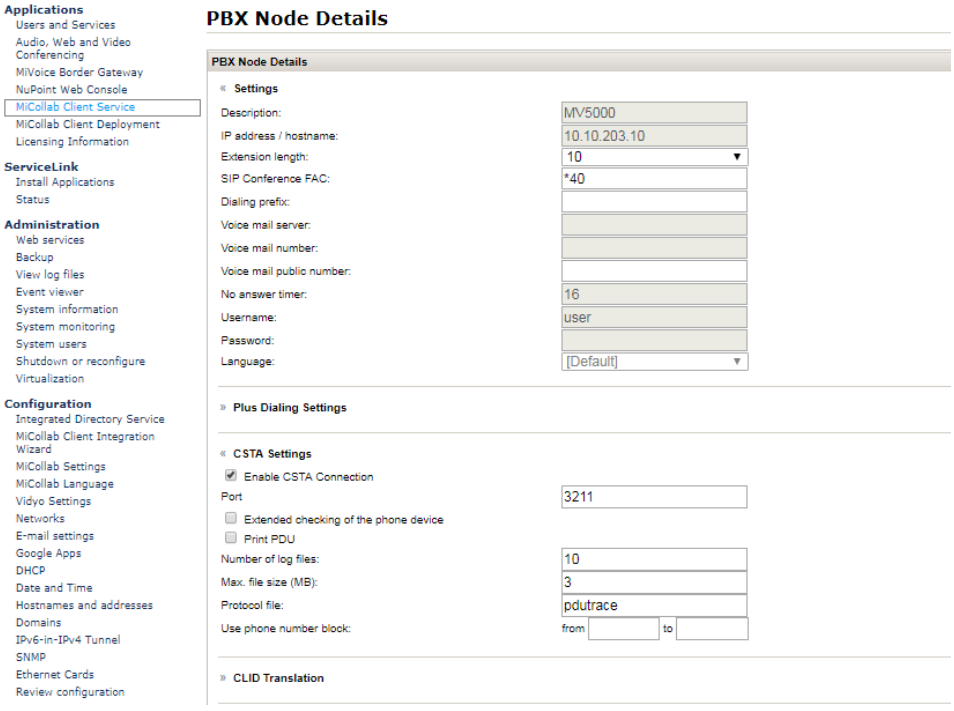
iii. After you set the required attributes, click **Import now** to display the **Import Status**.



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.



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

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

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; mobileTelephoneNumber; 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.
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.

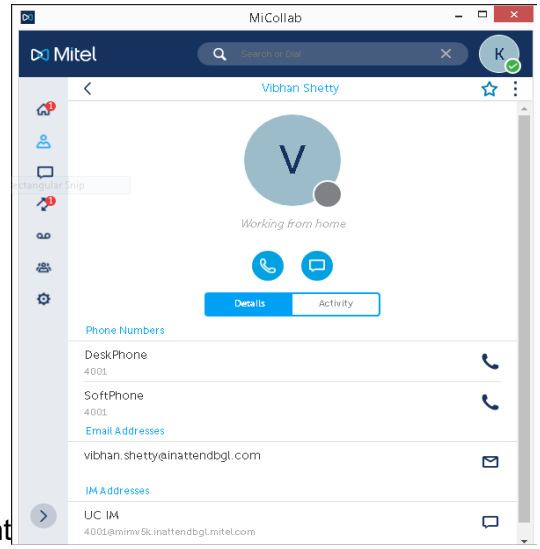
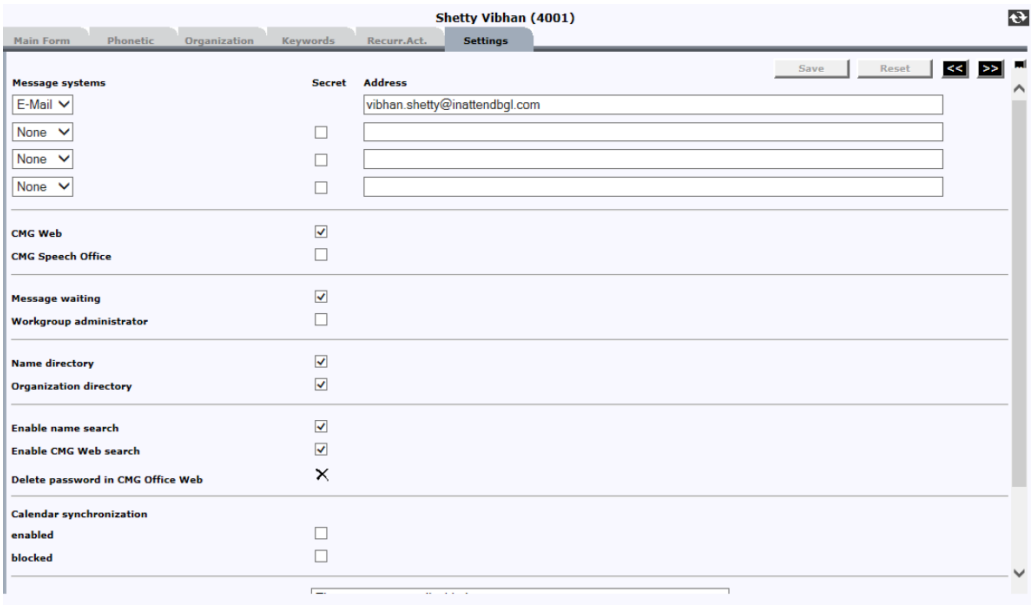


Figure 9.1: User details as in MiCollab Client



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.

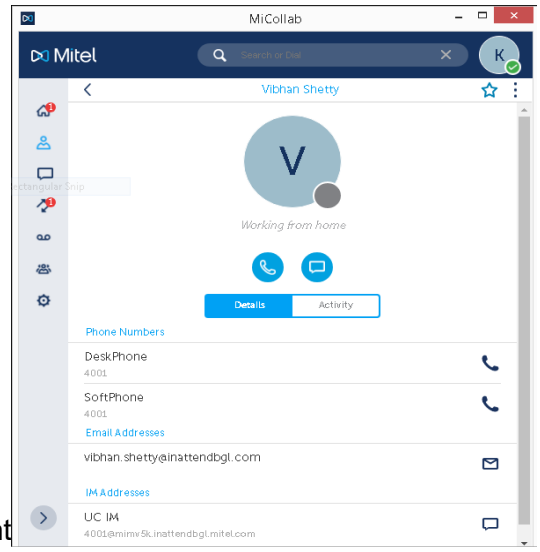
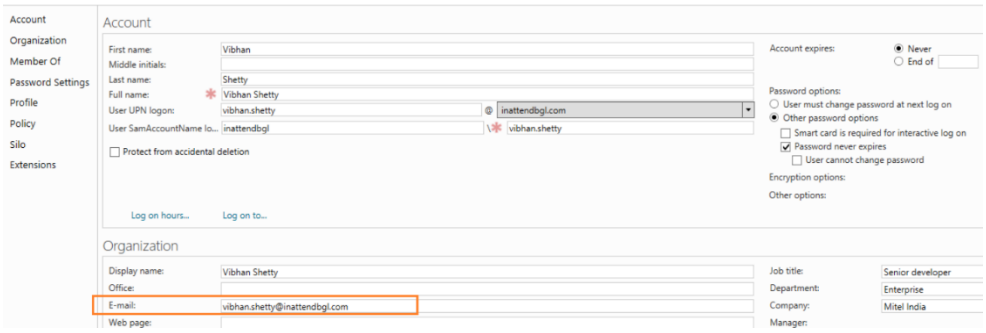


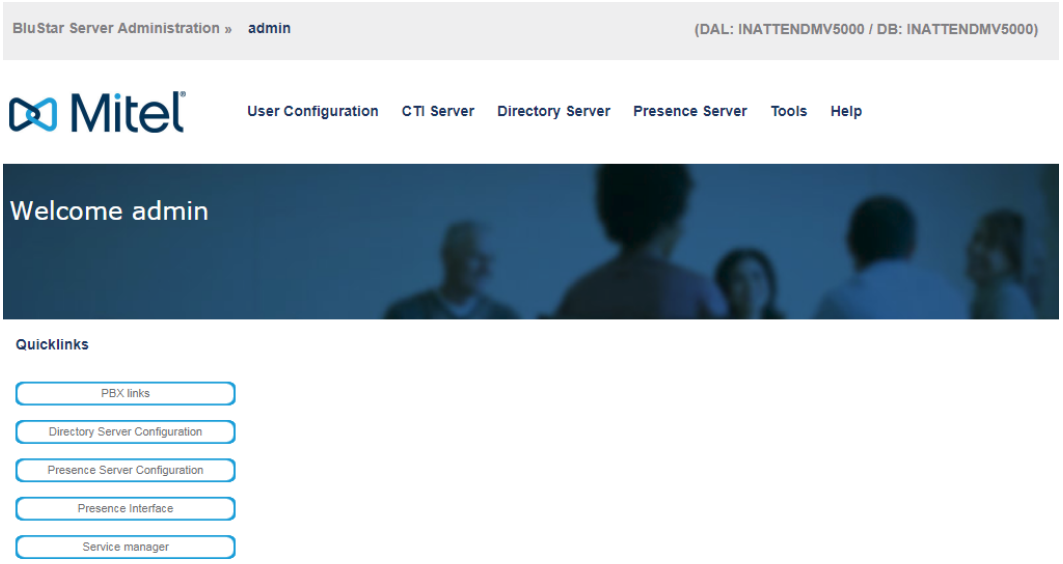
Figure 9.2: User details as in MiCollab Client



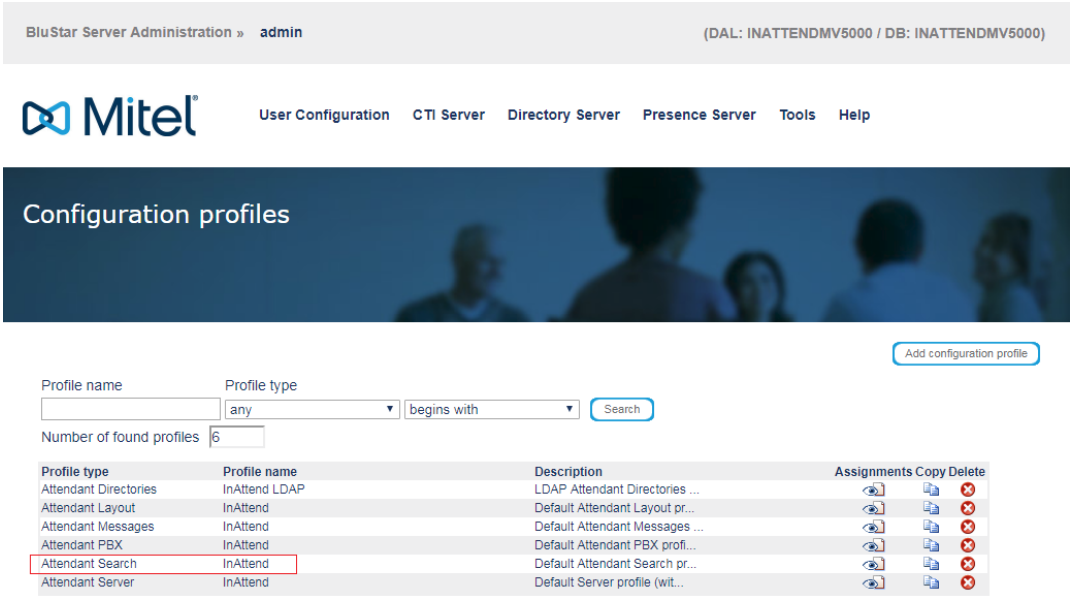
User details as in the active directory

Modifying Webadmin Configurations in InAttend for Standalone

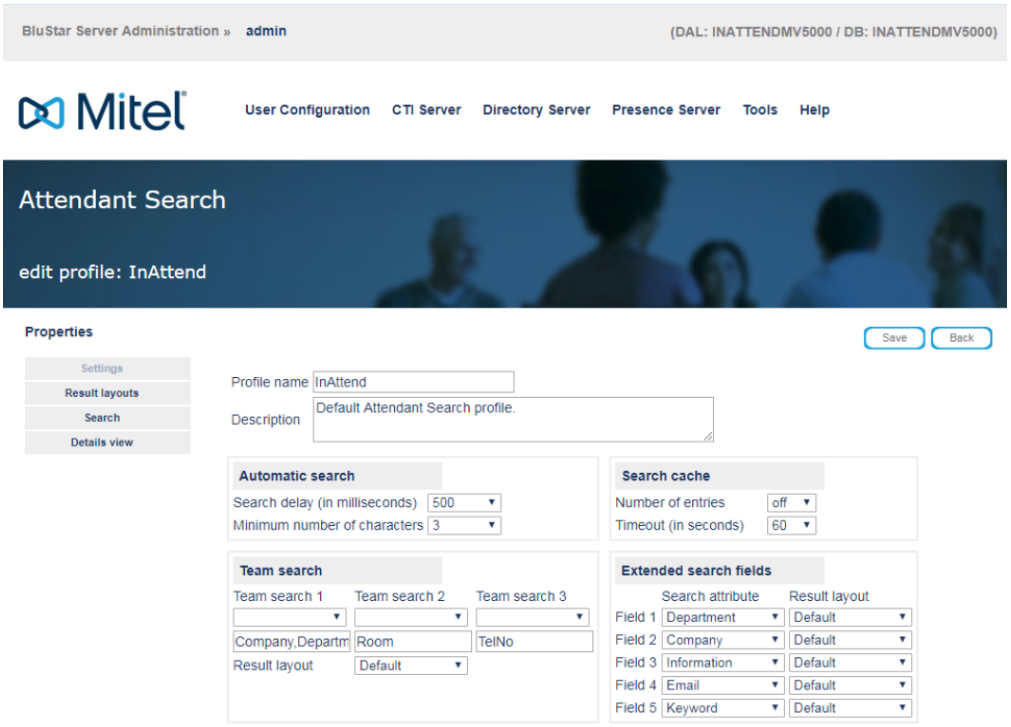
1. Log-in to the WebAdmin.



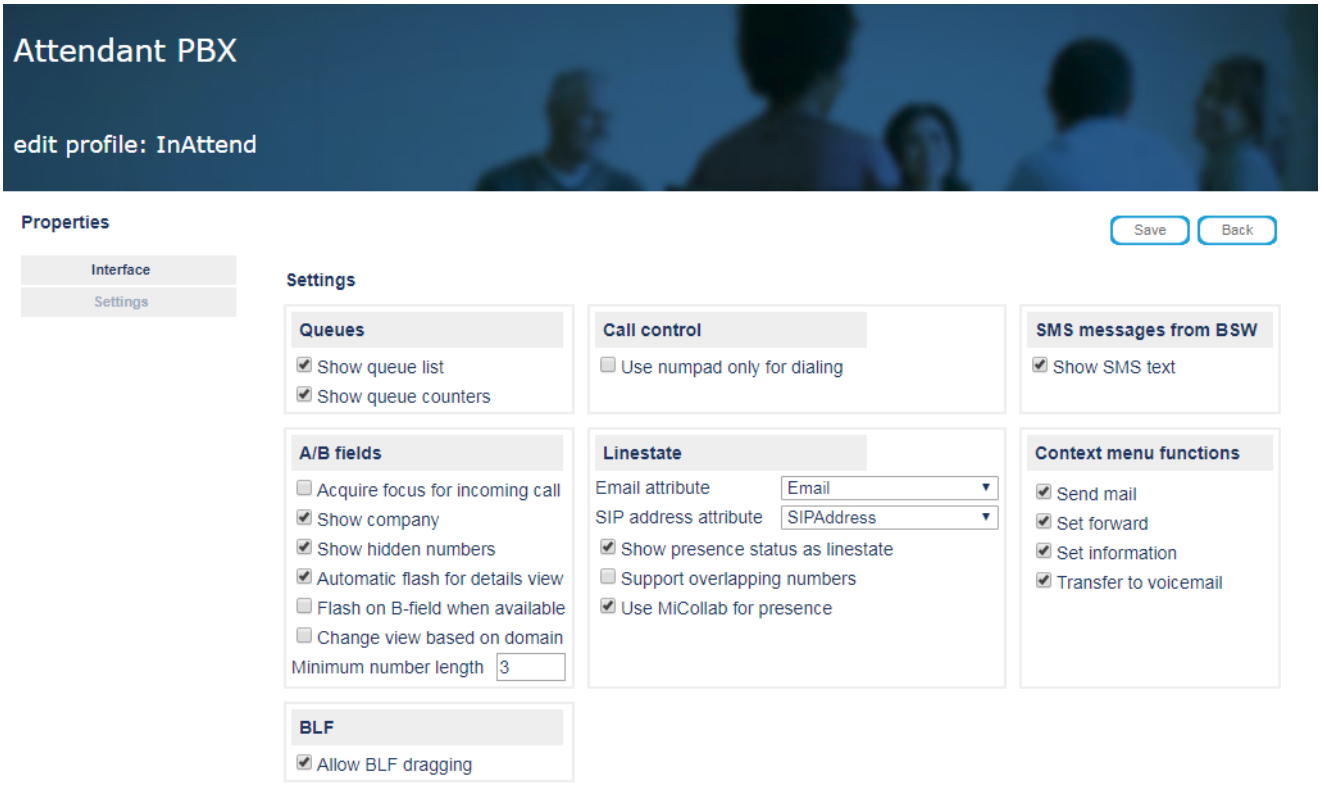
2. Select **User Configurations > Configuration profiles**, select the InAttend Search Profiles.



3. Select **Attendant Search**(Profile type) or **InAttend**(Profile name).



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.

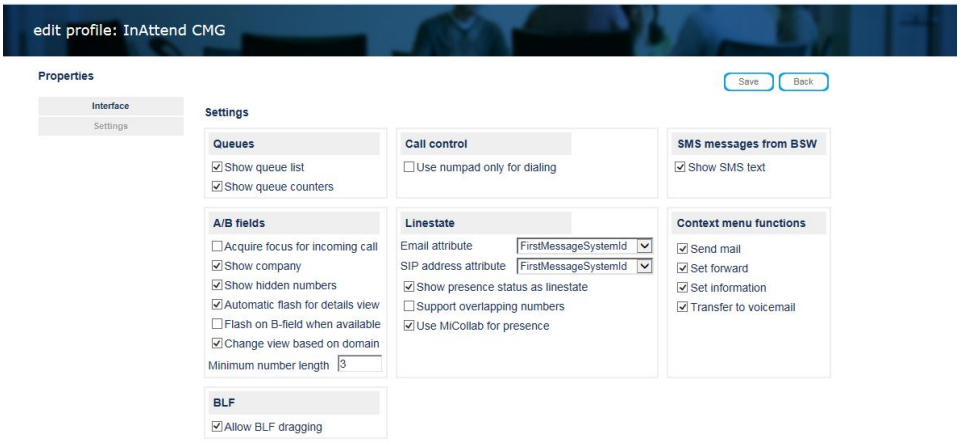


Settings for Micollab with InAttend

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

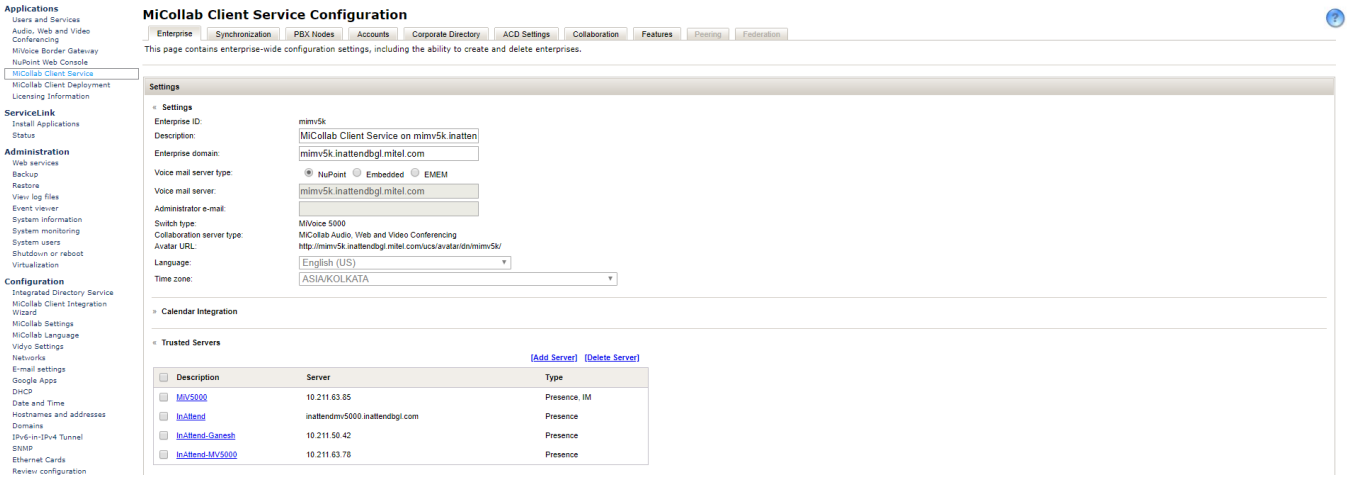
- Log-in to the Webadmin and select **User Configuration** > **Configuration Profiles** > **Attendant PBX InAttend/InAttend CMG** > **Setting**

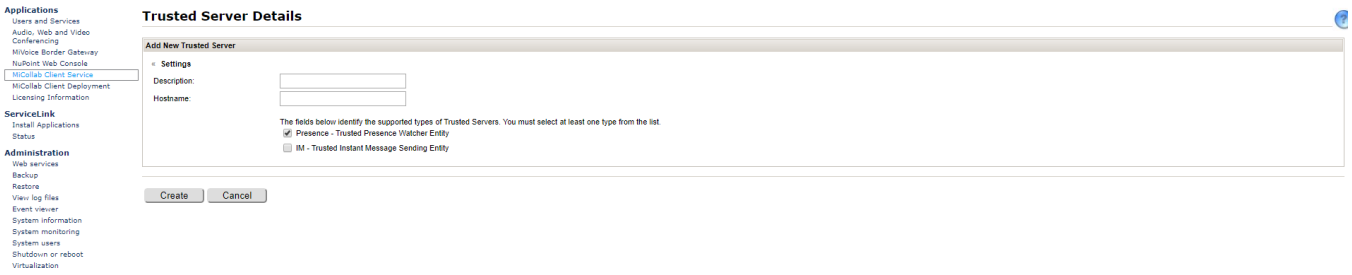


- Select ‘Use MiCollab for presence’

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**.





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.

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.
2. MiCollabDomain: This defines the MiCollab enterprise domain where MiCollab is deployed. MiCollab-Domain 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.
3. 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

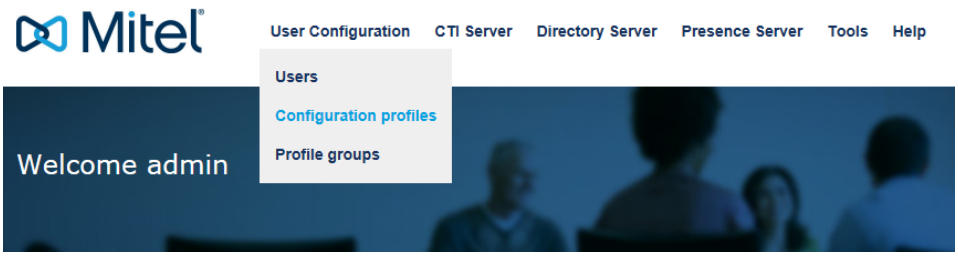
Configuration profiles control important settings for the InAttend client that cannot be configured by the attendants themselves. The configuration profiles are assigned to users through profile groups.

The system provides the pre-defined configuration profiles for InAttend.

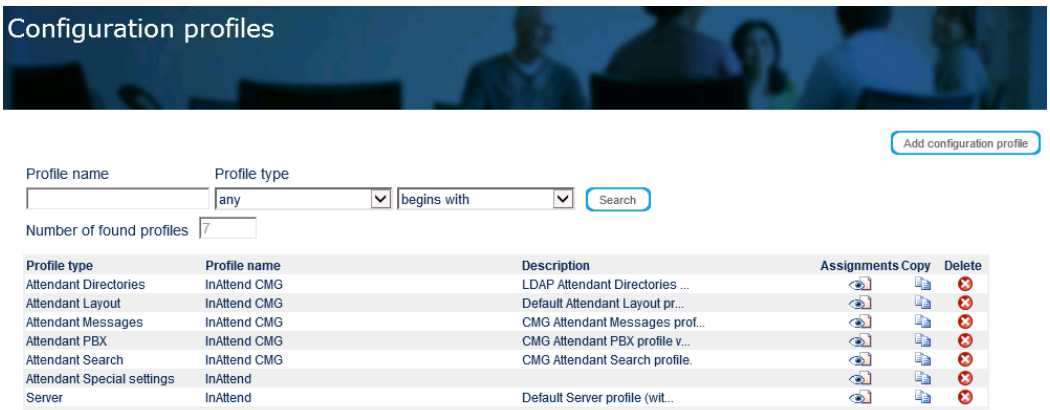
Viewing InAttend configuration profiles

1. Access the BluStar Server Administration web interface by typing the URL: http://<host-name>/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**.



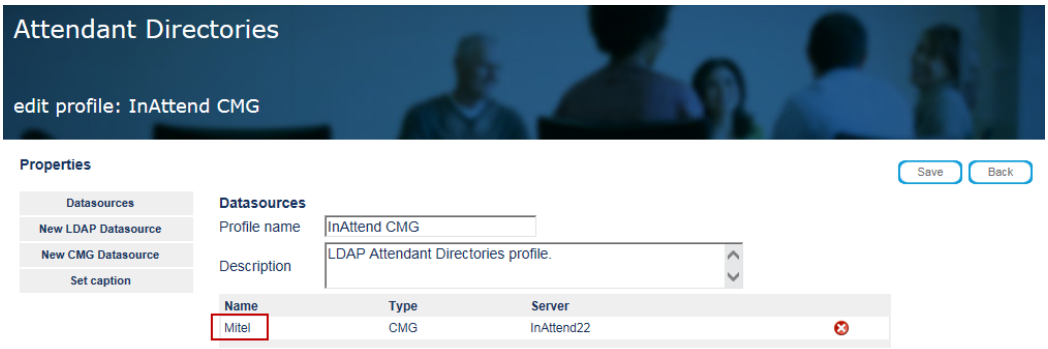
The system displays the Configuration profiles page and lists all predefined profiles.



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.



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

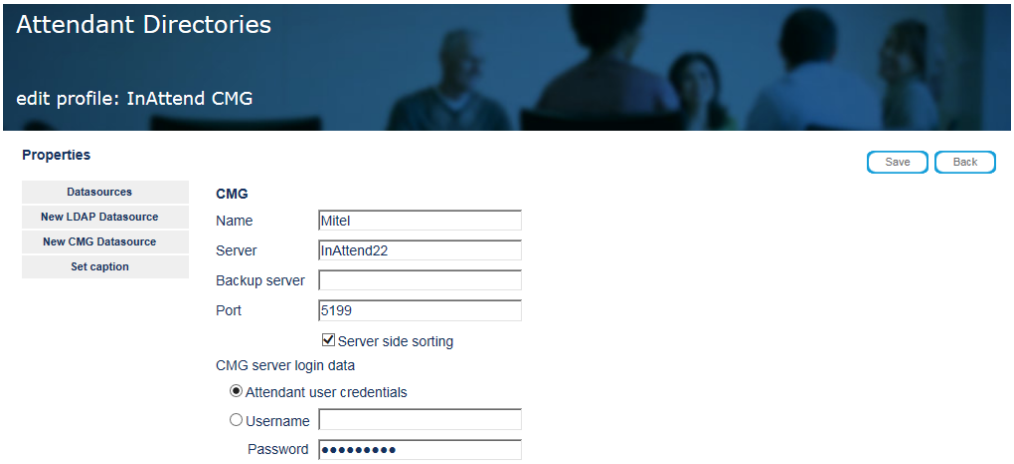
(if available)

- 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

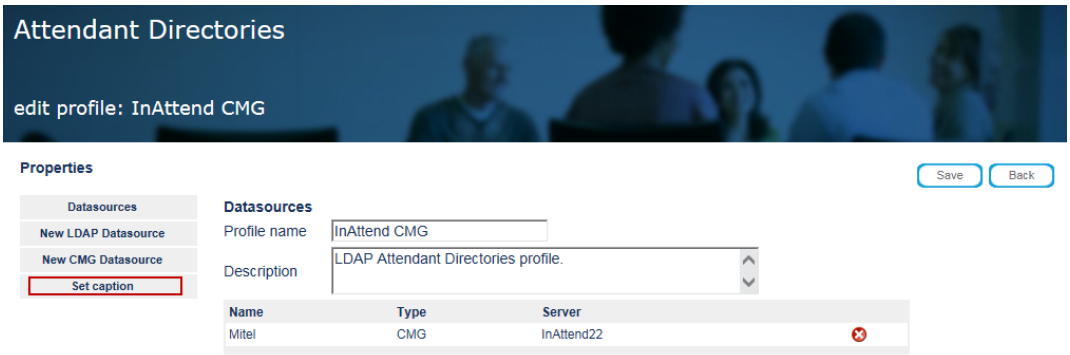
  Password: the password for authorized to access the CMG server



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**.



   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.

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.

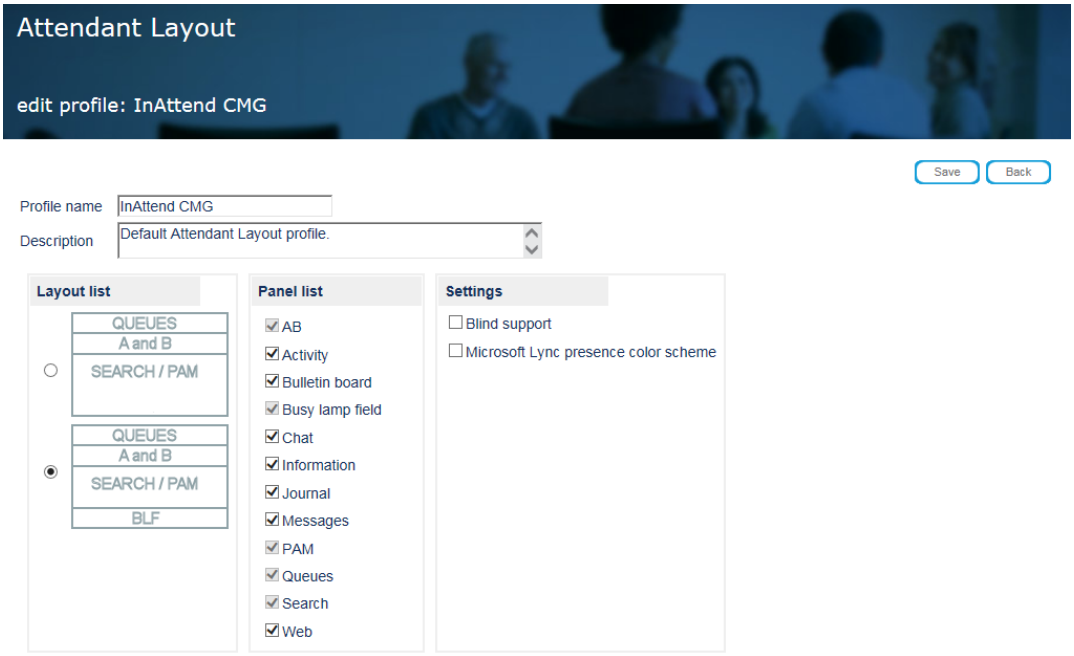
NOTE: To have the complete functionality of overlapping numbers, you must enable the Change view based on domain in WebAdmin.

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.



3. Click **Save** to save your changes.
4. Click **Back** to return to the main Configuration profiles page

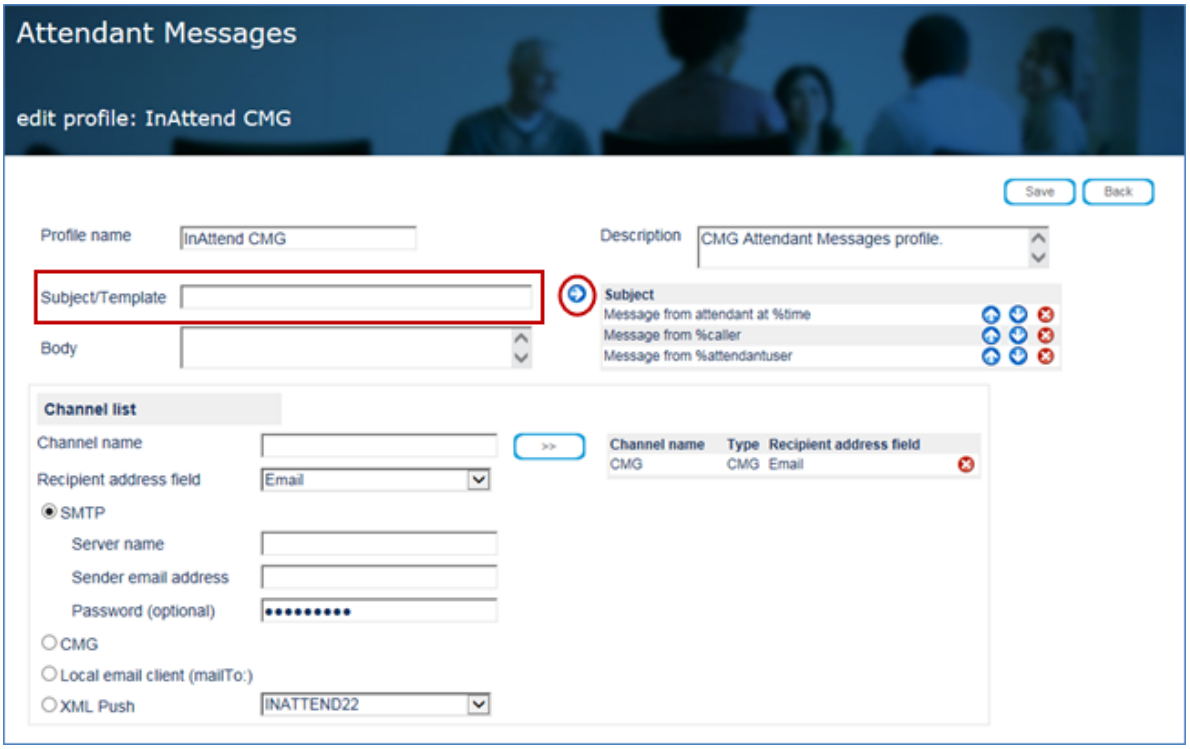
Modifying the Attendant Messages profile

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:

1. 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).



2. 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.

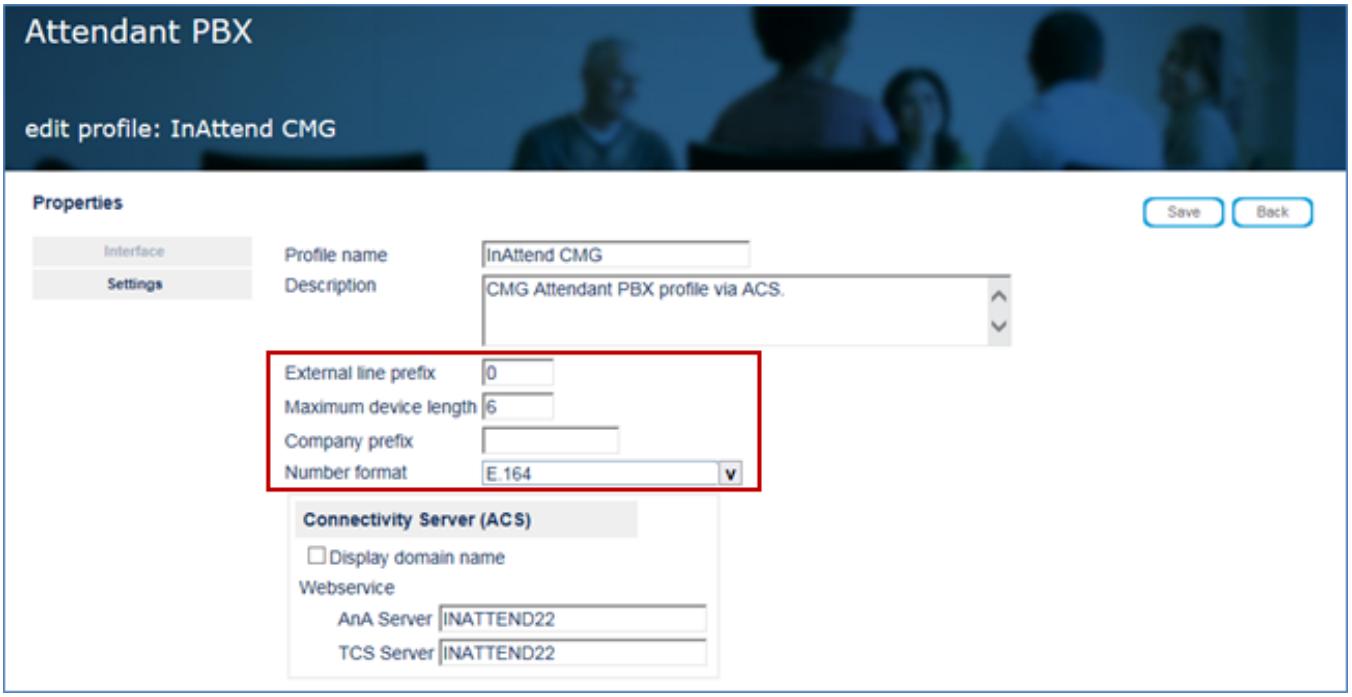
5. Click **Back** to return to the main Configuration profiles page.

Modifying the Attendant PBX profile

The Attendant PBX profile defines PBX-specific settings for InAttend, such as external line prefix and maximum extension length.

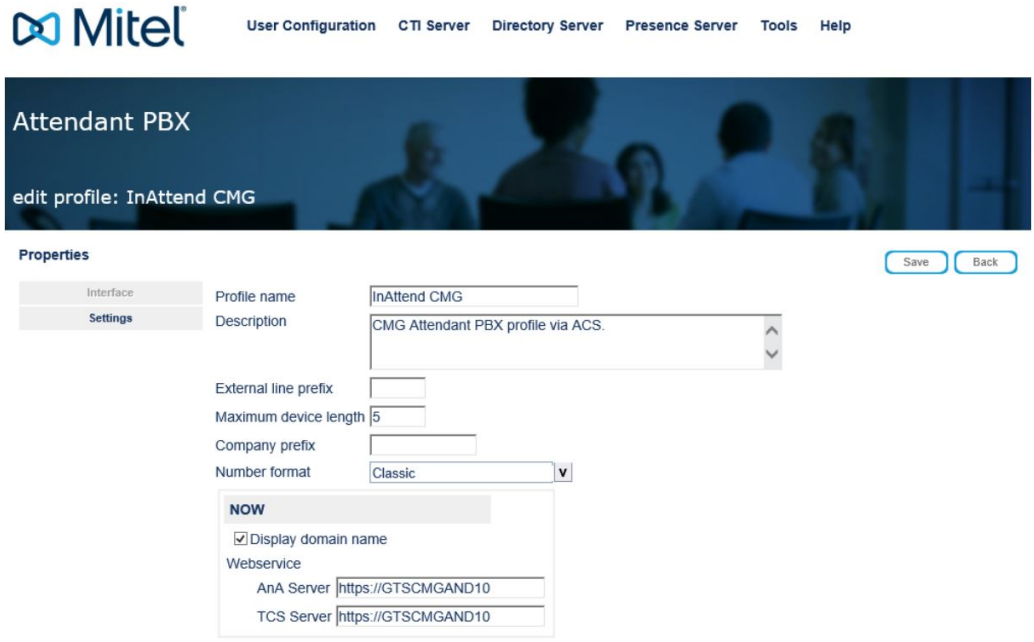
To modify the Attendant PBX profile, do the following:

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.

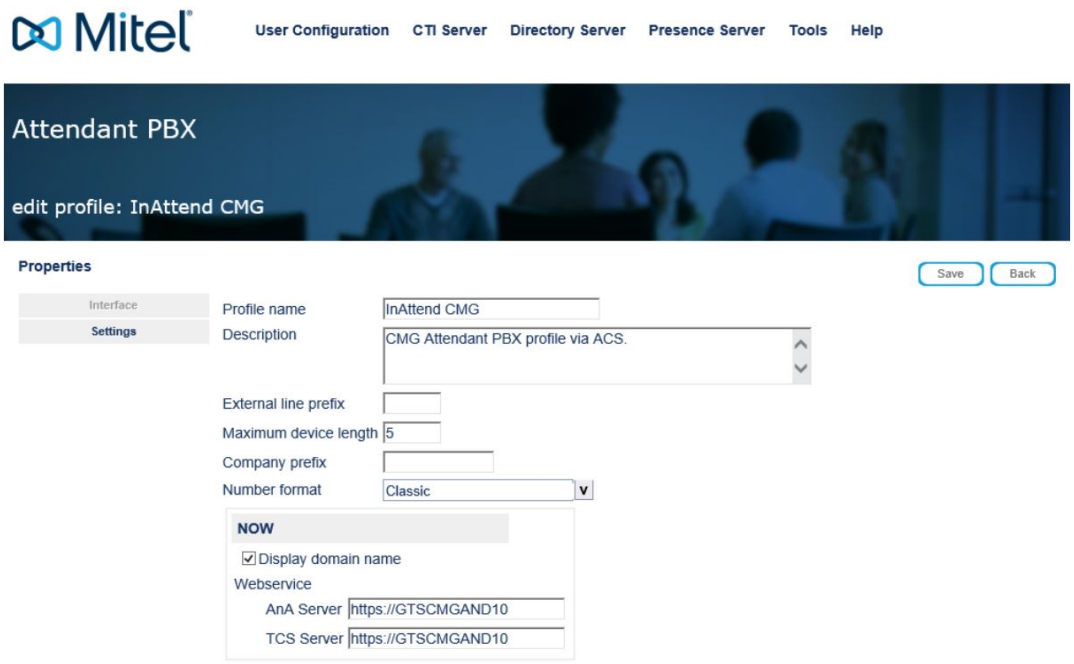


3. In the Connectivity Server (ACS) section, enter values for the following parameters:
    a. **Display domain name**: Enable to additional domain information provided by the ACS server in the A/B panel.
    b. **Ana Server**: The hostname or IP address of the server hosting the Authentication and Authorization (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.



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:



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**:

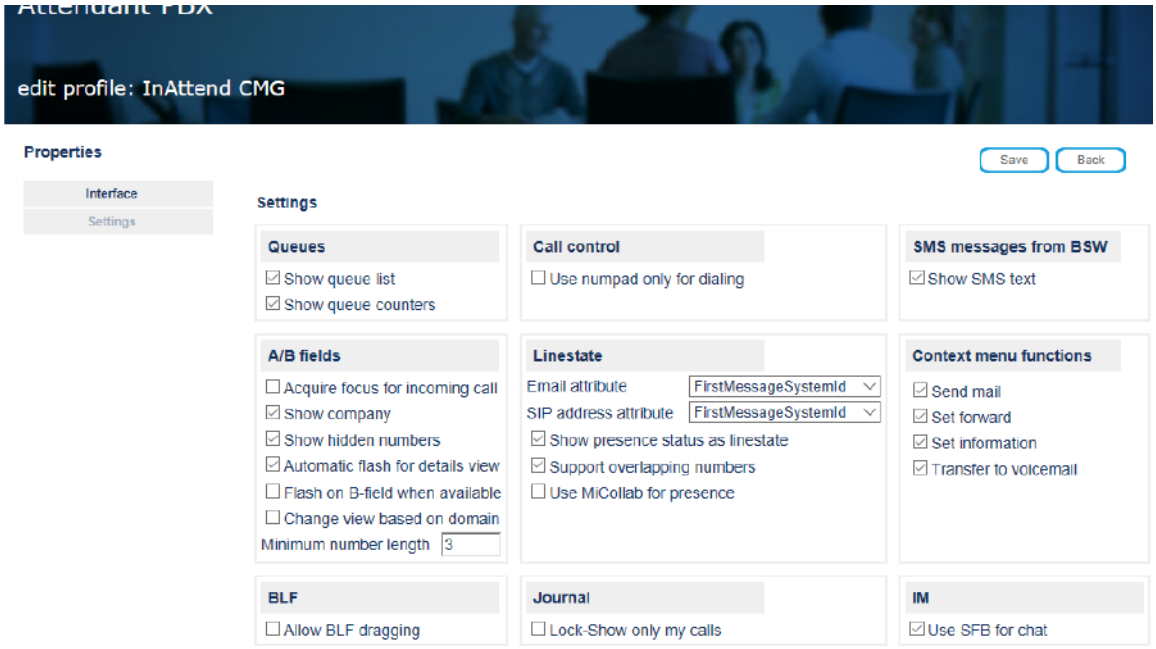
Show SMS text: Enable to show the sms text; that is, configured in the Messages tab of InAttend client.

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.



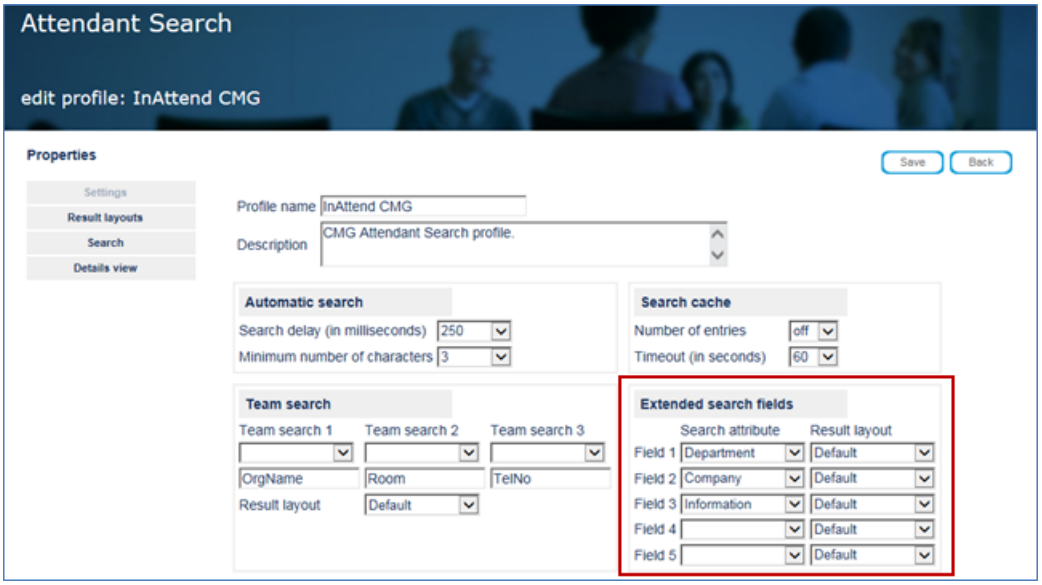
6. Click **Save** to save your changes.

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:



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.

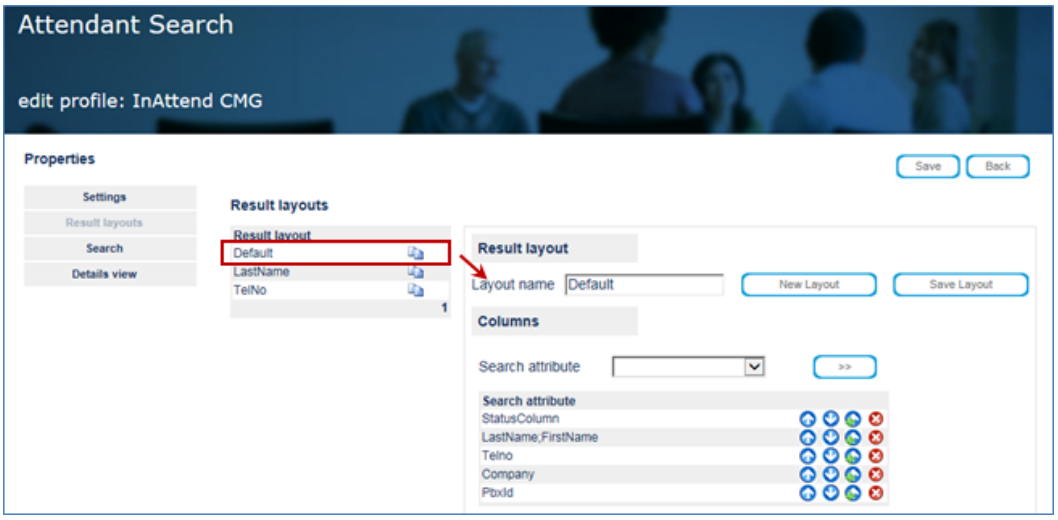
NOTE: In the Search Result list in InAttend, keywords can be displayed in two different ways depending on which of these fields have been selected:

- **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.

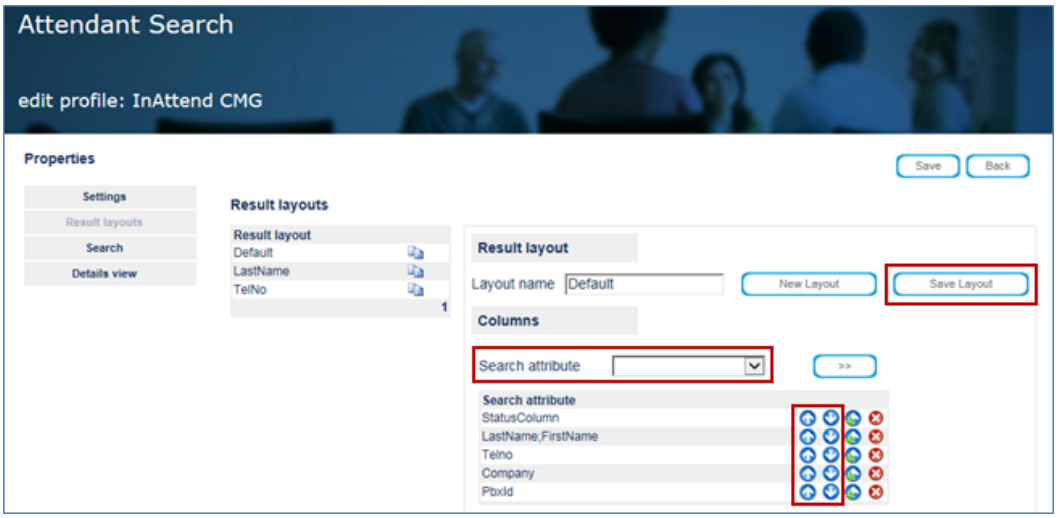


   b. You can make the following changes to the layout:

   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.

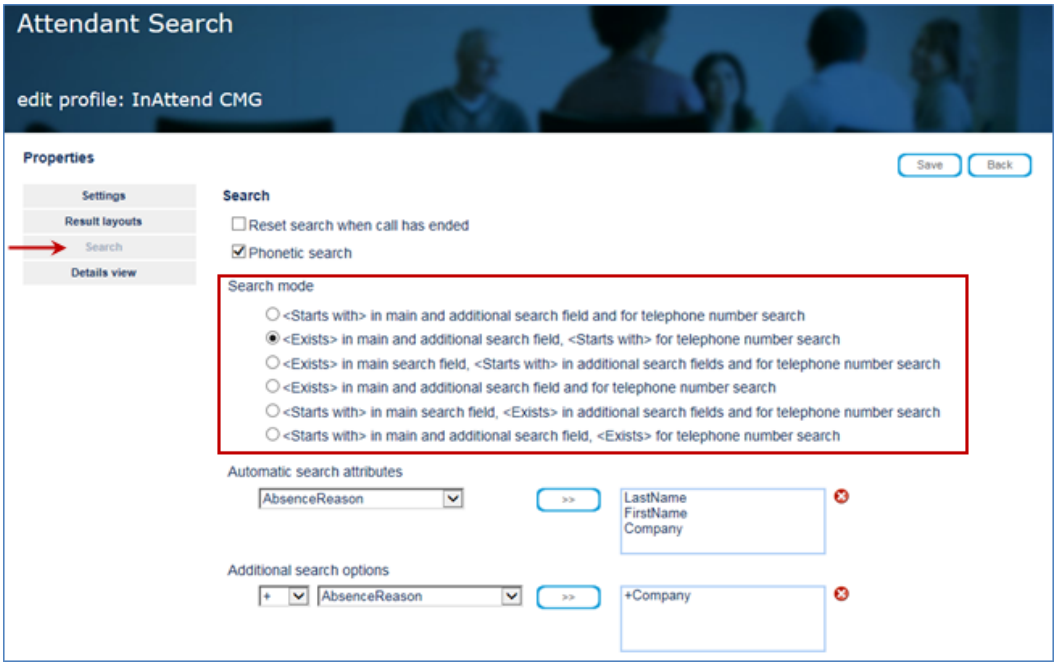
   To re-order the columns in the results, click on the arrows to move the search attribute up or down in the list (the top of the list corresponds to the first column in the search results).

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



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.



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:

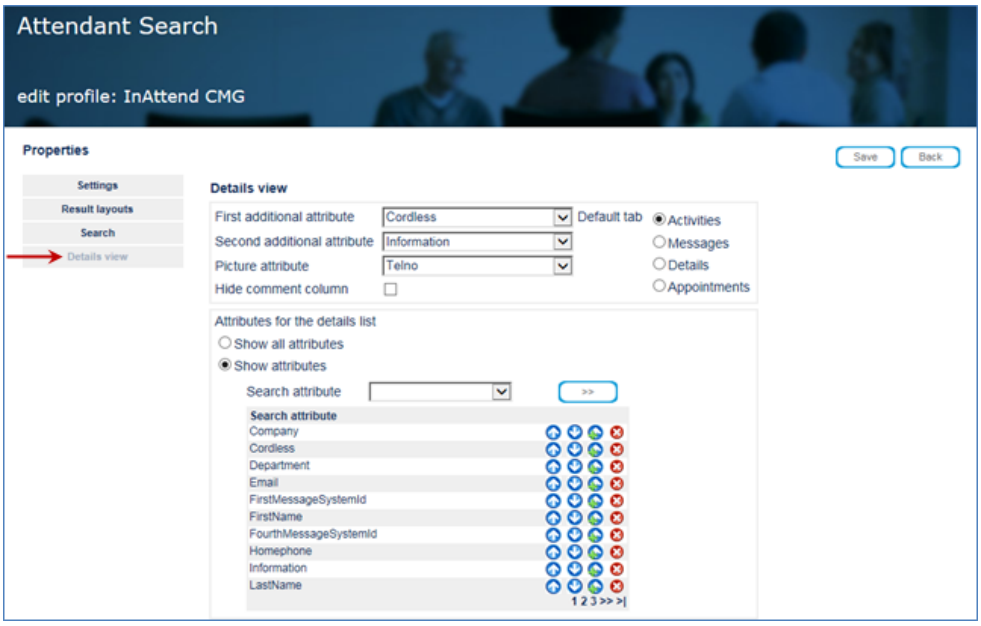
Select an attribute from the drop-down menu and click the arrow key to add the attribute to the list.

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.



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.

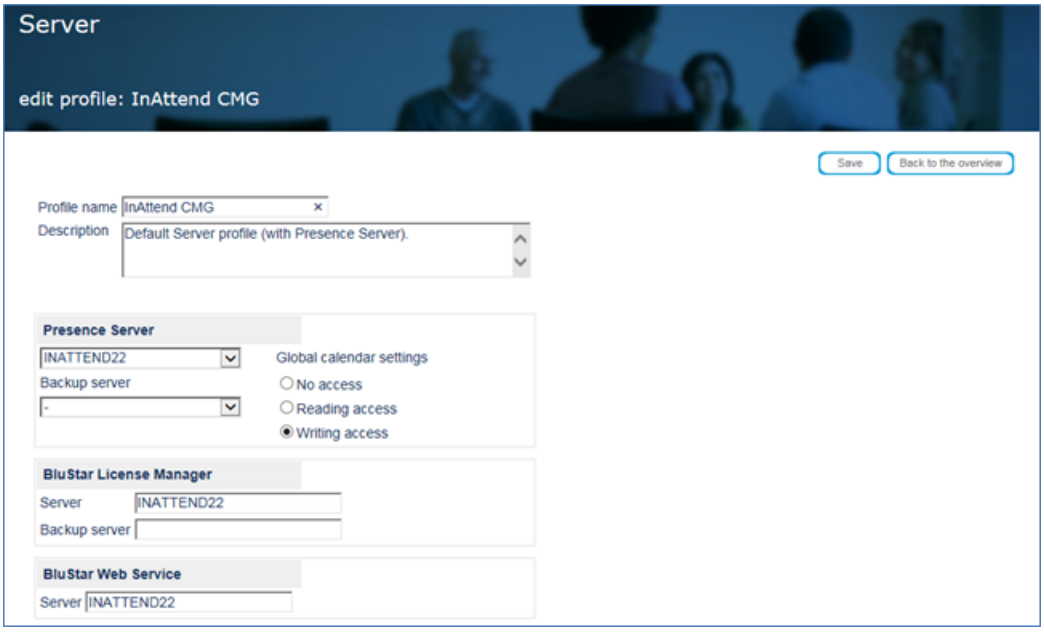
Modifying the Server profile

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



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:

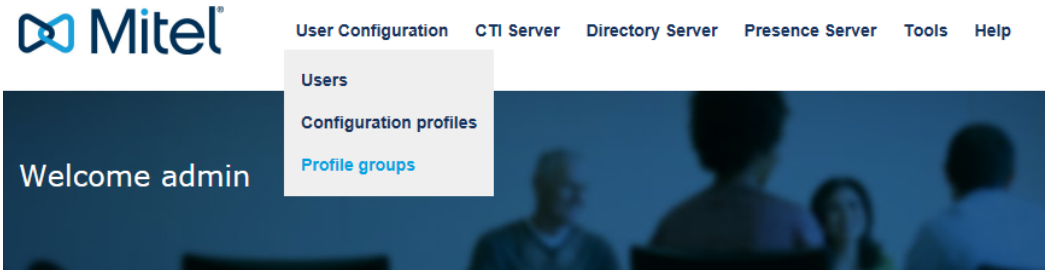
- Attendant Directories
- Attendant Layout
- Attendant Messages
- Attendant PBX
- Attendant Search
- Server

Creating a new profile group

To create a new profile group, do the following:

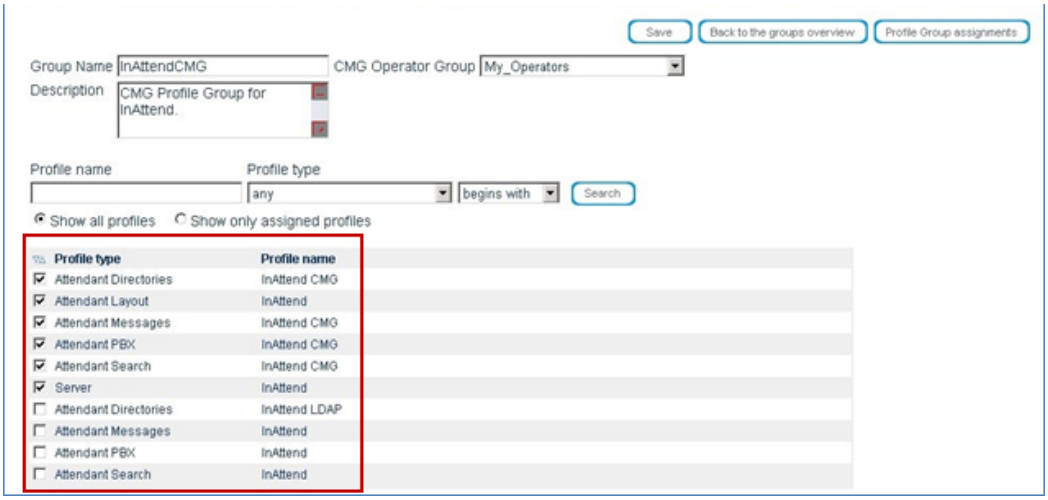
1. Access the BluStar Server Administration web interface by typing the URL: `http://<host-name>/webadmin` in a supported web browser, where <hostname> is the InAttend server address.
2. Log in with the administrator credentials

   (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.



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

Modifying a profile group

To modify an existing profile group, do the following:

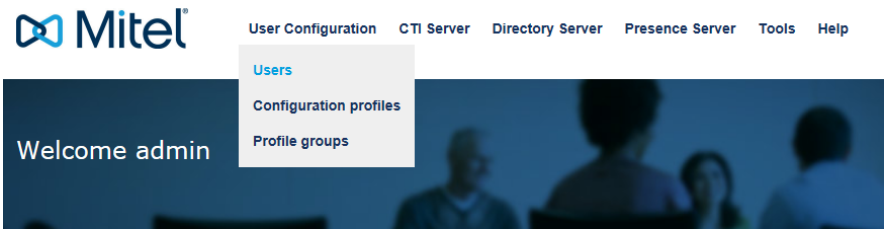
1. On the Profile groups page, click on the profile group you want to edit.
2. On the Edit profile group page, you can:
   a. change the name of the profile group
   b. change the description for the profile group
   c. select or remove configuration profiles from the profile group
3. Click **Save** to save your changes.

Configuring InAttend users

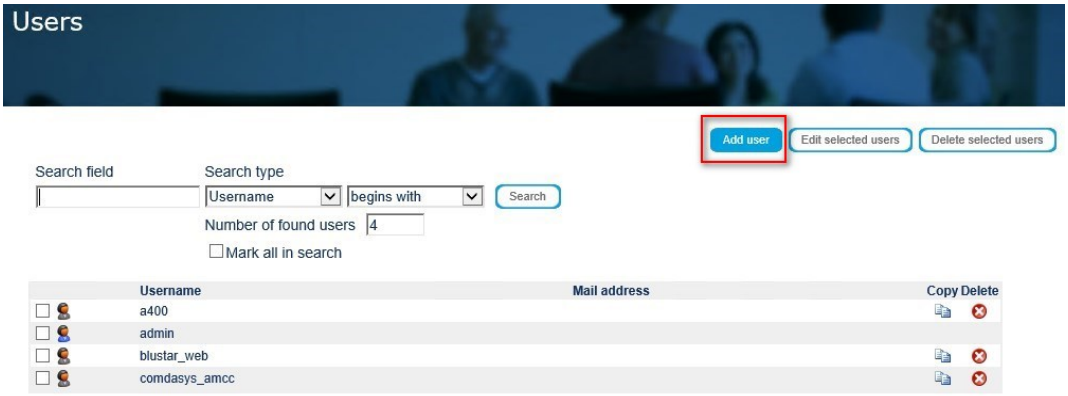
When you create a new user, you assign the user to a profile group. The information is automatically propagated to the TCA.

1. Access the BluStar Server Administration web interface by typing the URL: `http://<host-name>/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**.

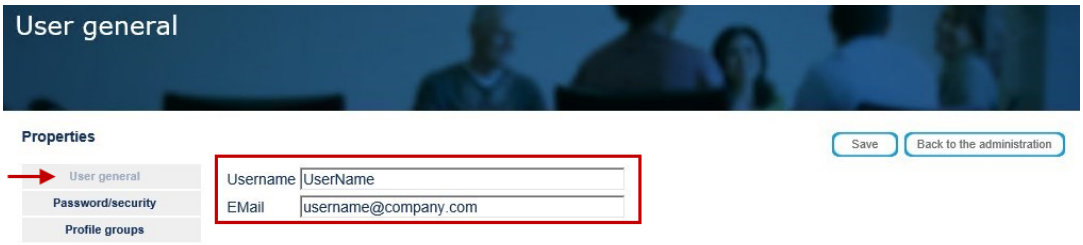


4. On the Users page, click **Add user.**



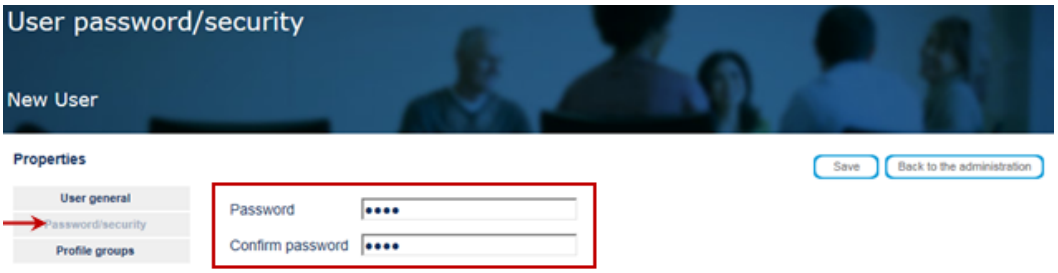
5. On New User page, click **User general** (under Properties) and enter values for the following fields:

   Username: the name of the new InAttend user
   Email: Enter the email address for the new InAttend user.

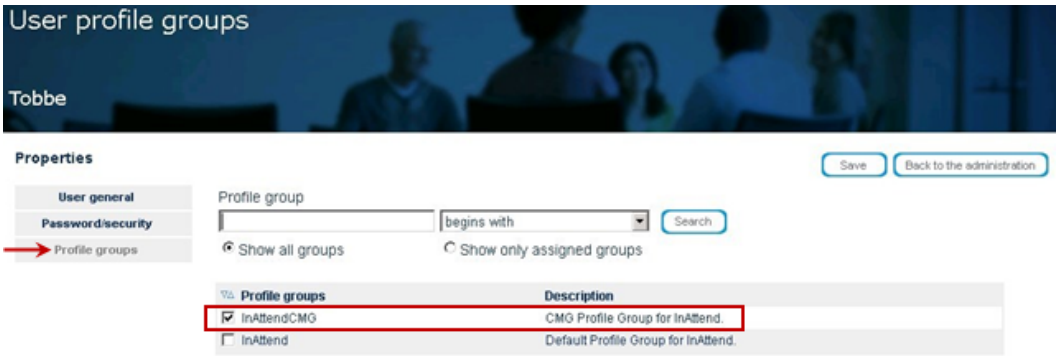


6. Click **Password/security** and enter values for the following fields:

   Password: the password for the new InAttend user.
   Confirm password: repeat the password for the new InAttend user.



7. Click **Profile groups** and select the profile group to which the user will belong (for example, InAttend CMG).

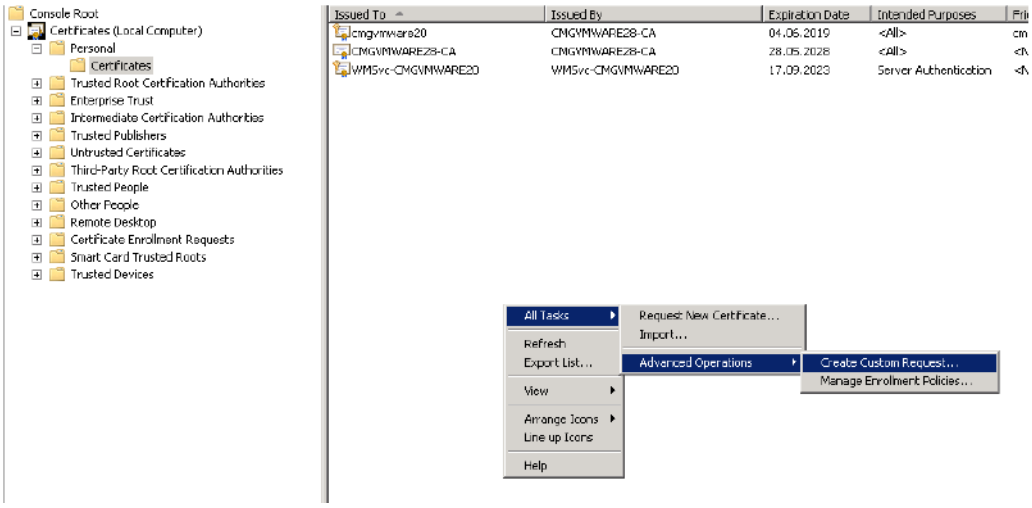


8. Click **Save** to save your changes.

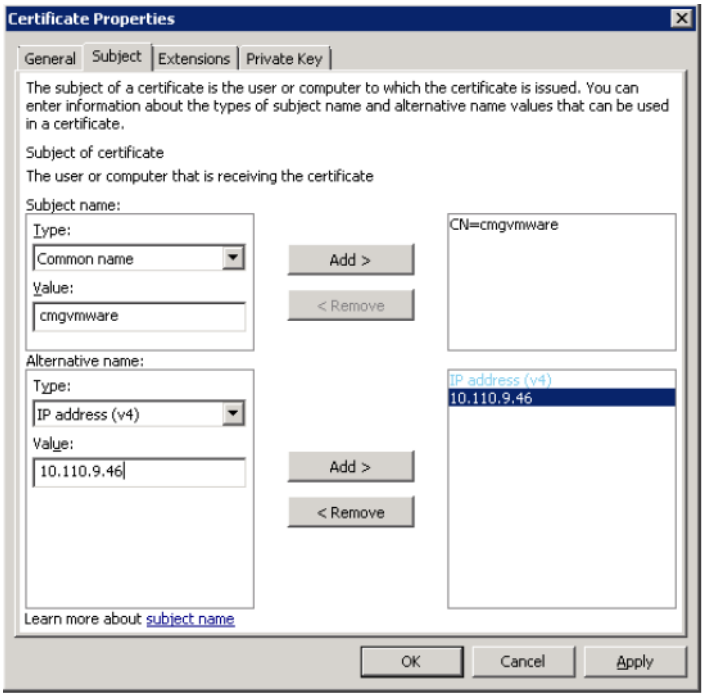
Generate CSR in ACS

To generate CSR in ACS, do the following:

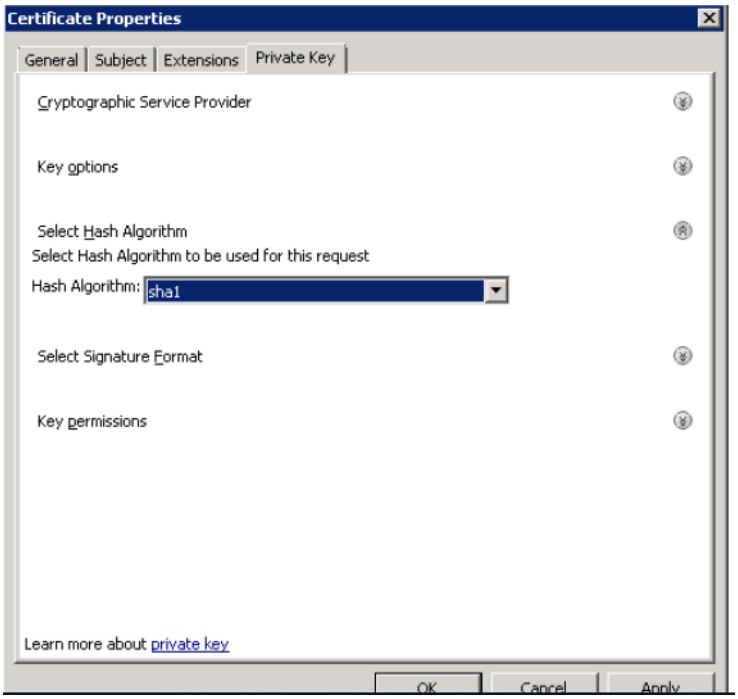
1. Start MMC on the ACS server. Go to **Files**, and select **Add/Remove Snap-in**. Click Certificate and expand Certificate with the computer account.
2. Click **Personal > Certificate** and go to **All Task > Advance Operations > Create Customer Request**.



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**.



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.

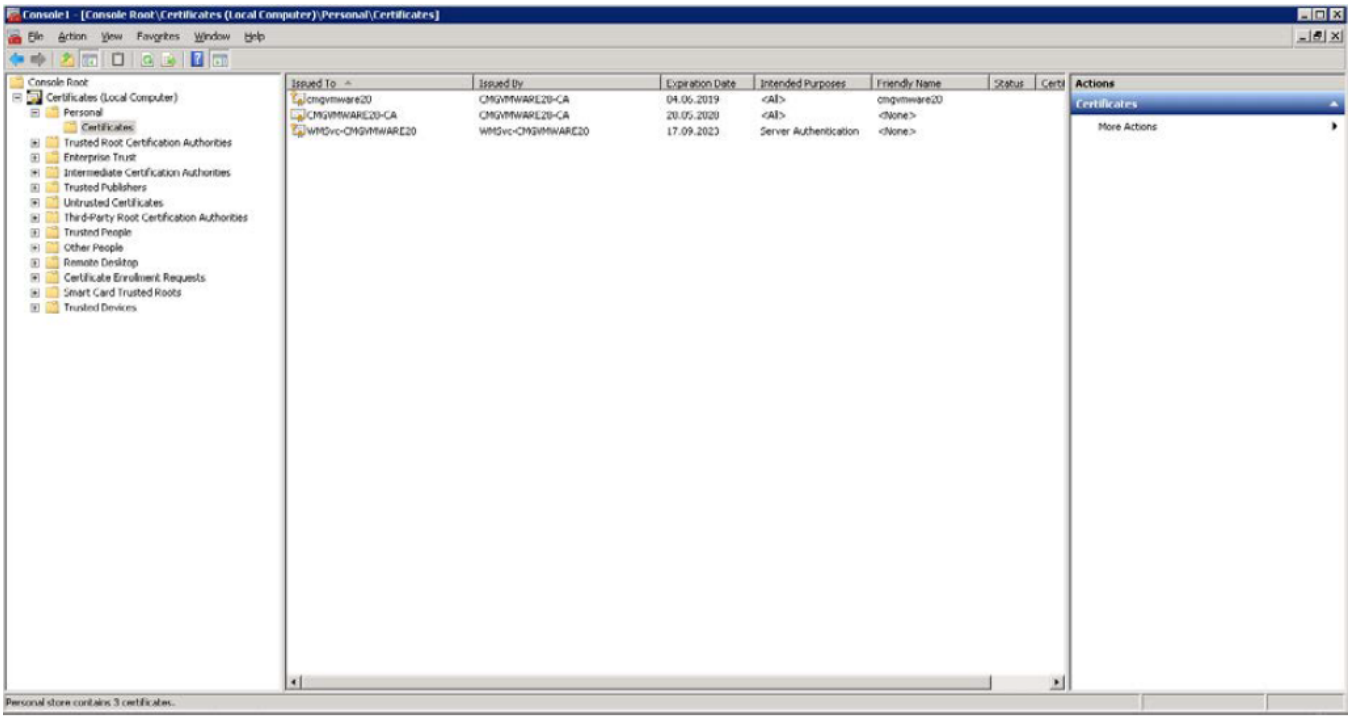
TLS Certificates Installation

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.

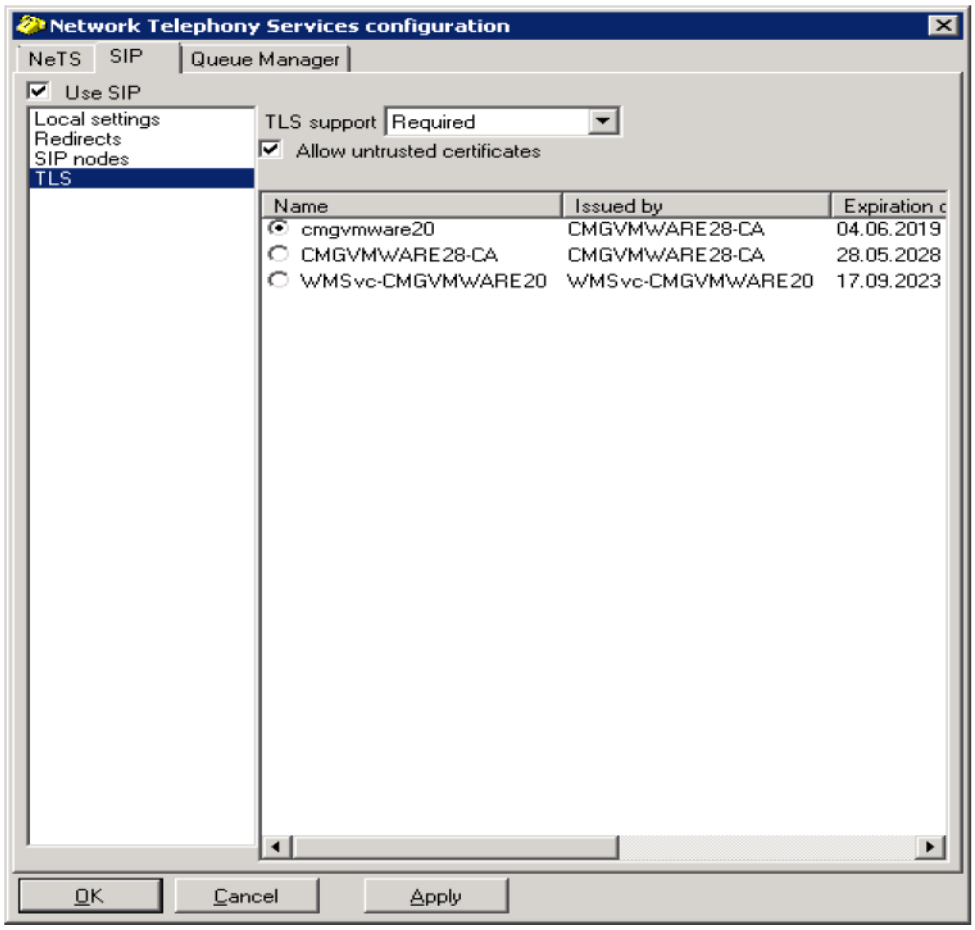
The Certificate snap-in allows you to browse the contents of the certificate stores.

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**.
10. 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**.



On the ACS server activate TLS with the imported certificate using NETS config.



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.

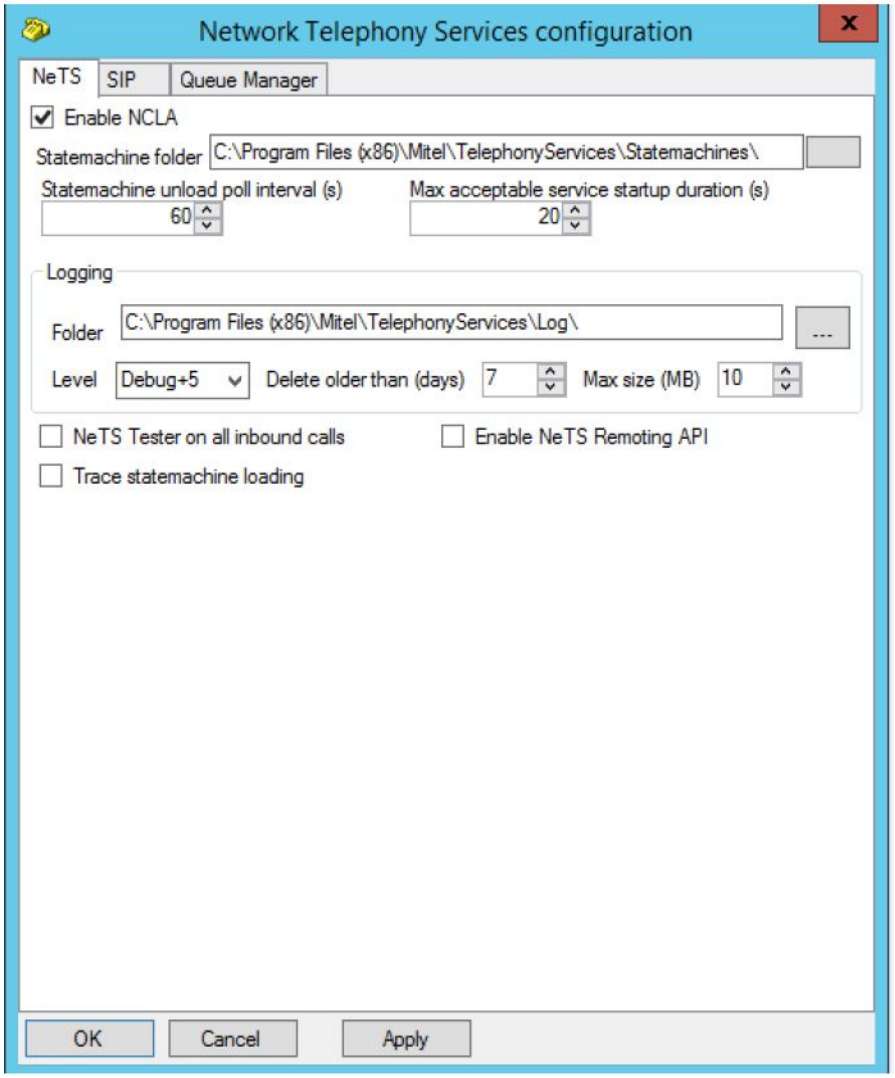
Configuring the NeTS telephony system

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:

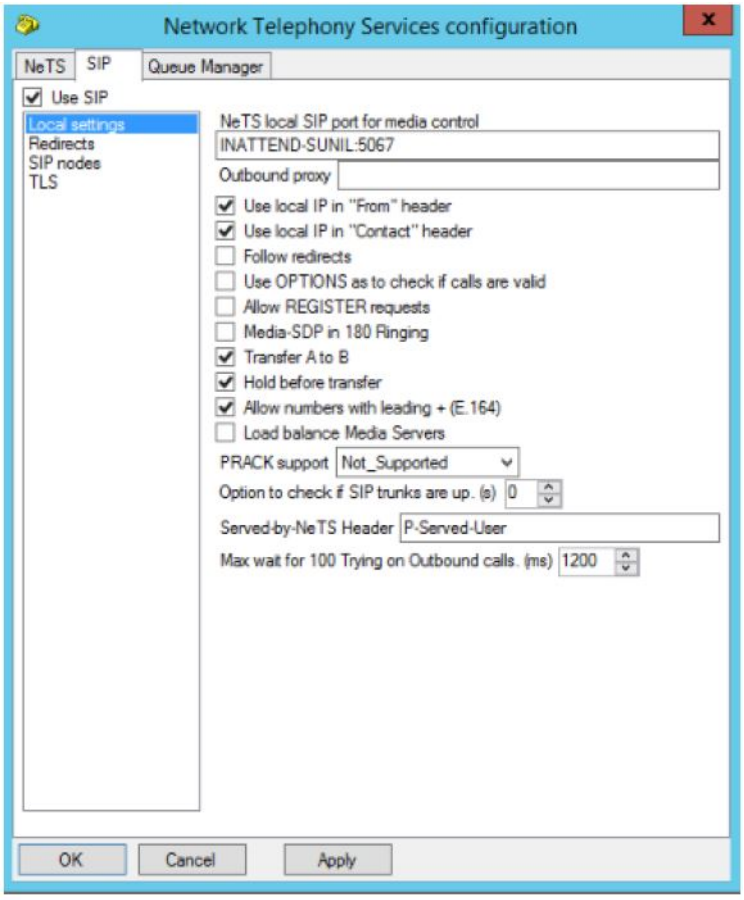
1. Open the NeTS configuration tool (**Start -> Programs -> Mitel -> NeTS**).
2. Select the **NeTS** tab.



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.



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.)
   l. **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.

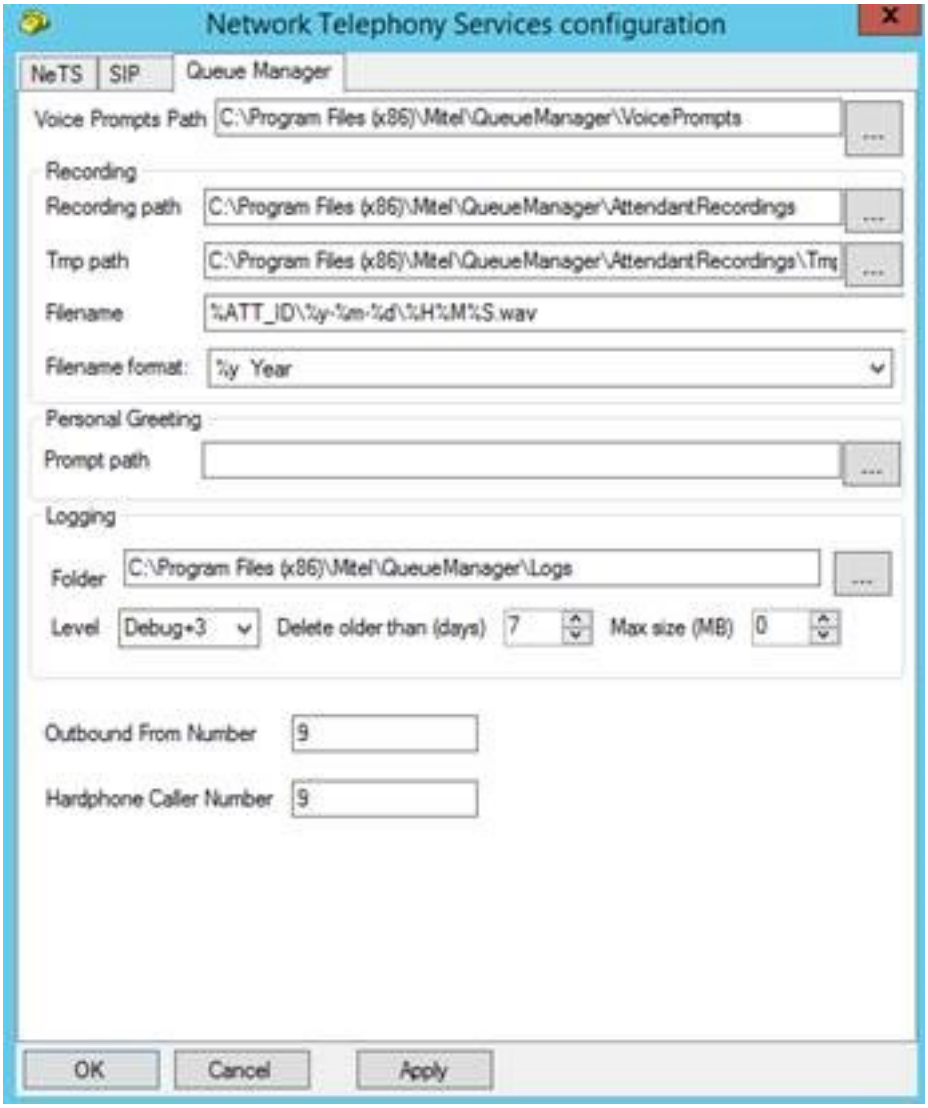
- **Required**: Both TLS and non-TLS ports are open. If a non-TLS request is received, NeTS responds with a 301 Moved Permanently message, with the new Contact the same as the request URI, but with the port and transport changed to TLS.

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.



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, File-name 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.

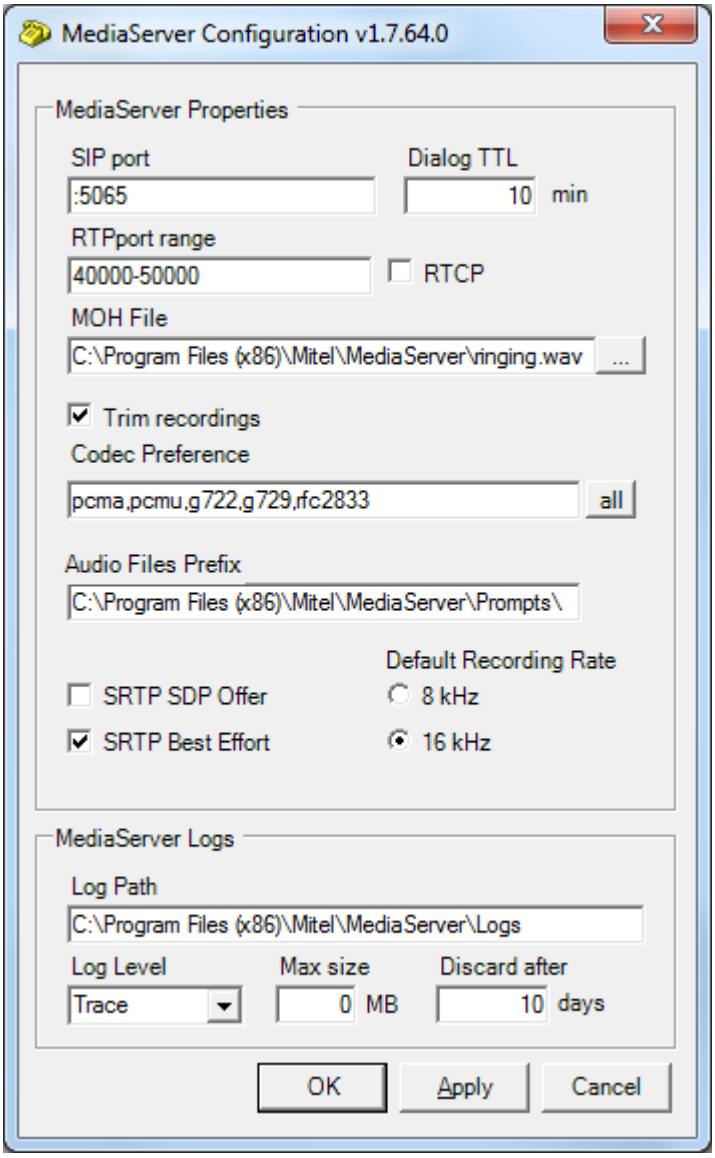
– **Hardphone Caller Number**: Sets the number for the operator's device; that is, when NeTS calls the operator's device, this number is displayed on the operator device. If this parameter is not set, the NeTS/ QueueManager uses 0 as calling number.

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**).



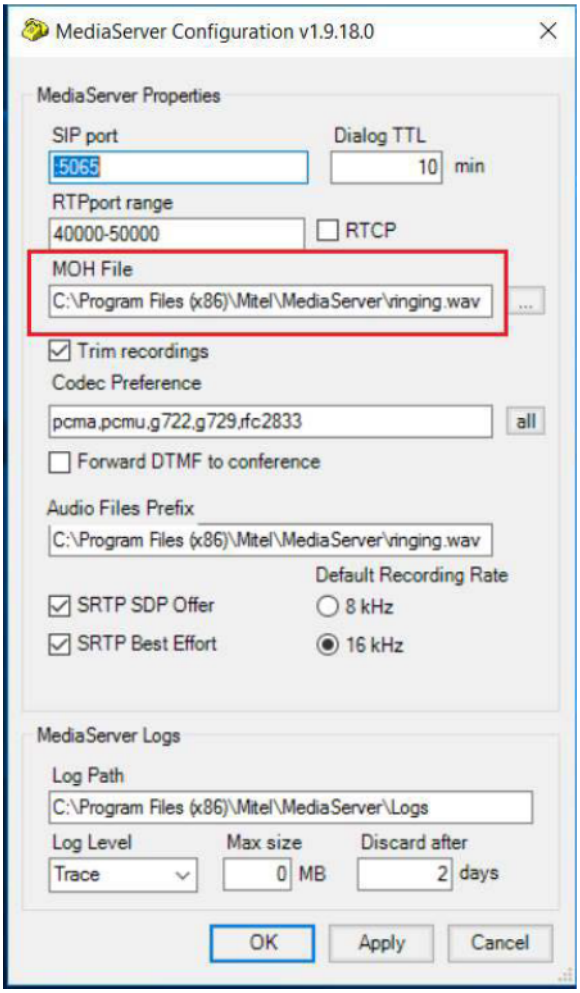
2. Enter or change the values for the following parameters as required:
   - **SIP port**: The port number where the Media Server listens for SIP sessions, and optionally Ethernet interface.

     :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



- **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)

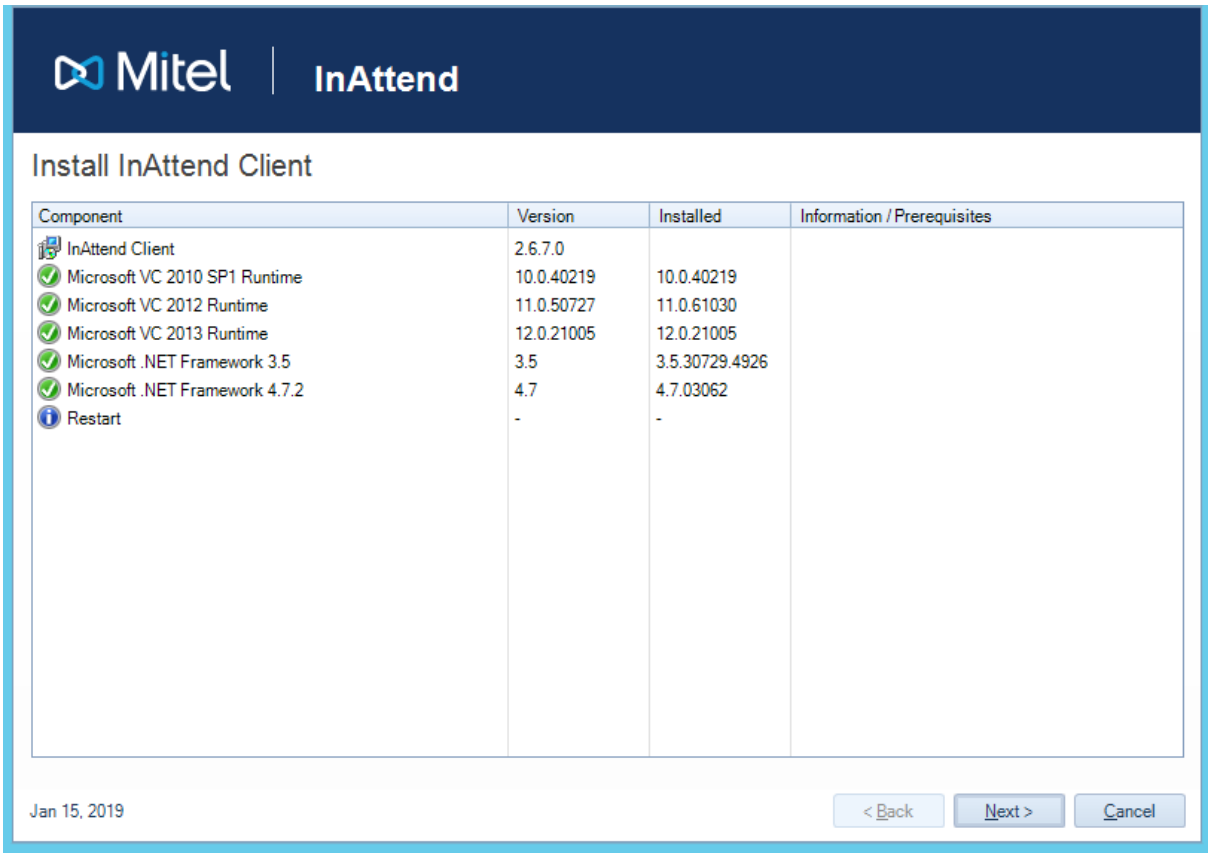
  This default setting is used if there is no other value specified by NeTS.
  - If you select the recording rate as 8.000 samples per second, Media Server saves the data in PCMA (also known as A-law).
  - If you select the recording rate as 16.000 samples per second, Media Server saves the data in L16 (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

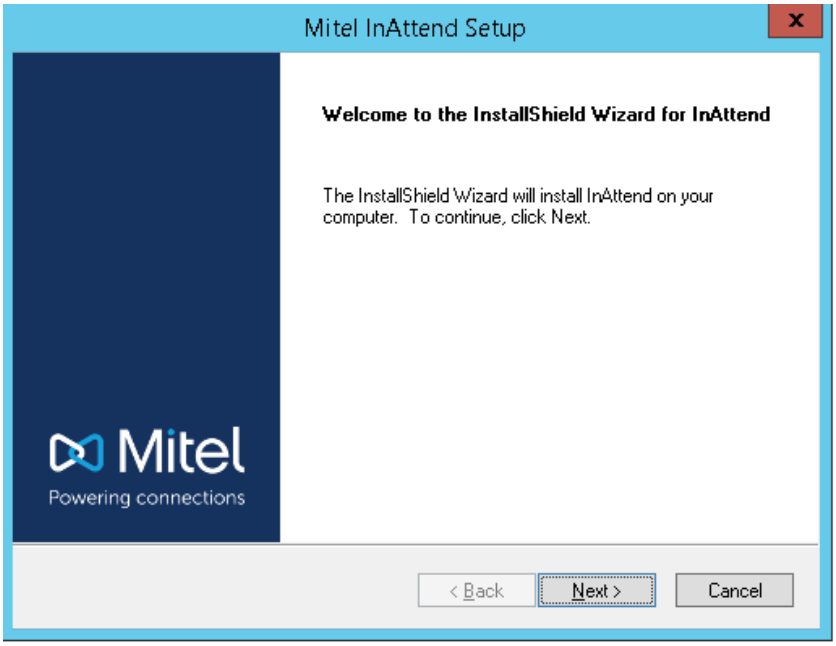
After you have completed configuration of the InAttend server, you can install and configure the InAttend Client for your users. The InAttend Client provides the user interface for the InAttend application.

To install the InAttend client software on each client machine:

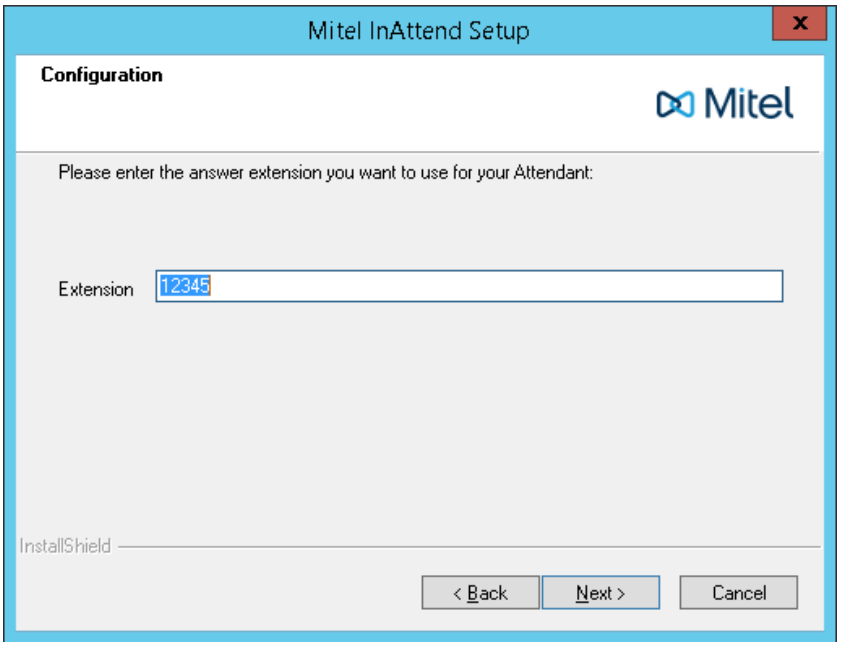
1. Double-click the **Install.exe** file in the top-level directory of your software package to launch the Mitel Installer.
2. In the Installer main window, click **Install**.
3. In the Install Wizard, select **Install InAttend Client**.
4. In the Installation window, review the components that are being installed. Components with a green check mark are already installed. Click **Next**.



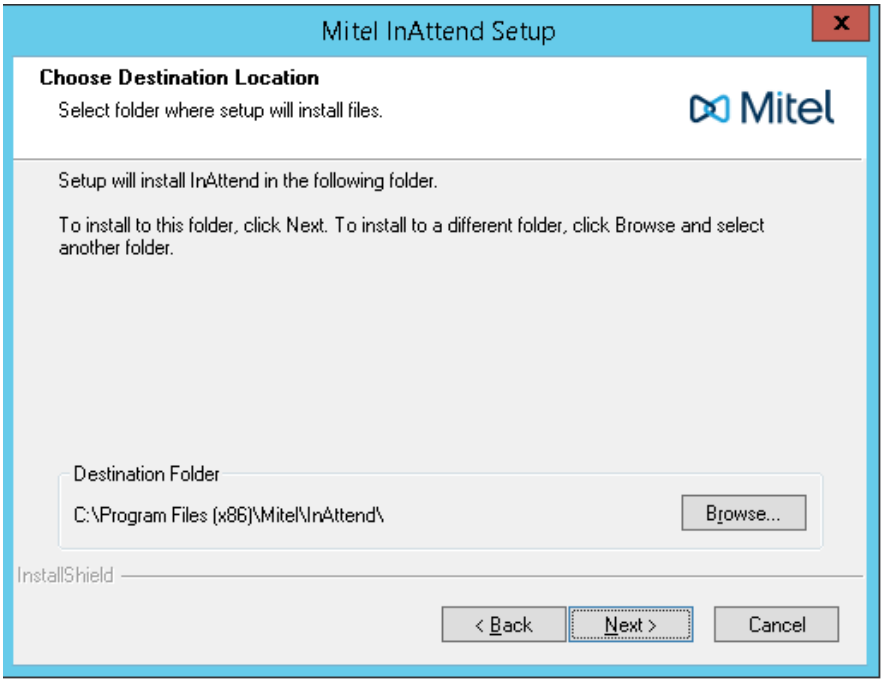
5. On the Welcome page for InAttend Client Setup, click **Next**.



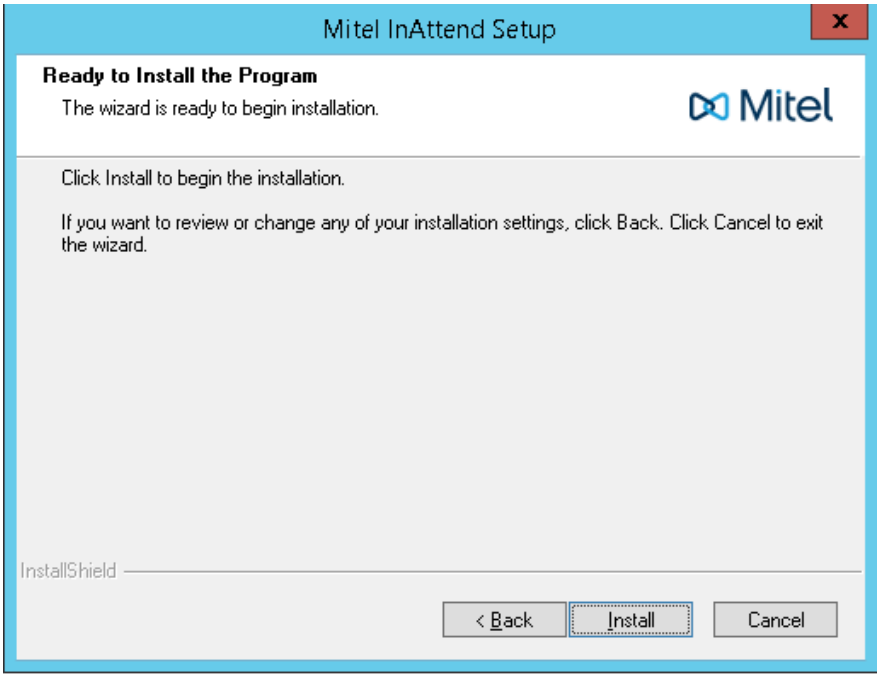
6. On the Configuration page, enter the server address for the Data Access Service in the **Hostname** field. (In single-server deployments, this is the hostname or IP of the InAttend server.) If a backup server is used, enter the address for the Data Access Server backup server in the **Backup** field. Click **Next** to continue.
7. On the Configuration page, enter the **Extension** number for the attendant and click Next.



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.



9. Click **Install** to start the InAttend Client installation.



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.

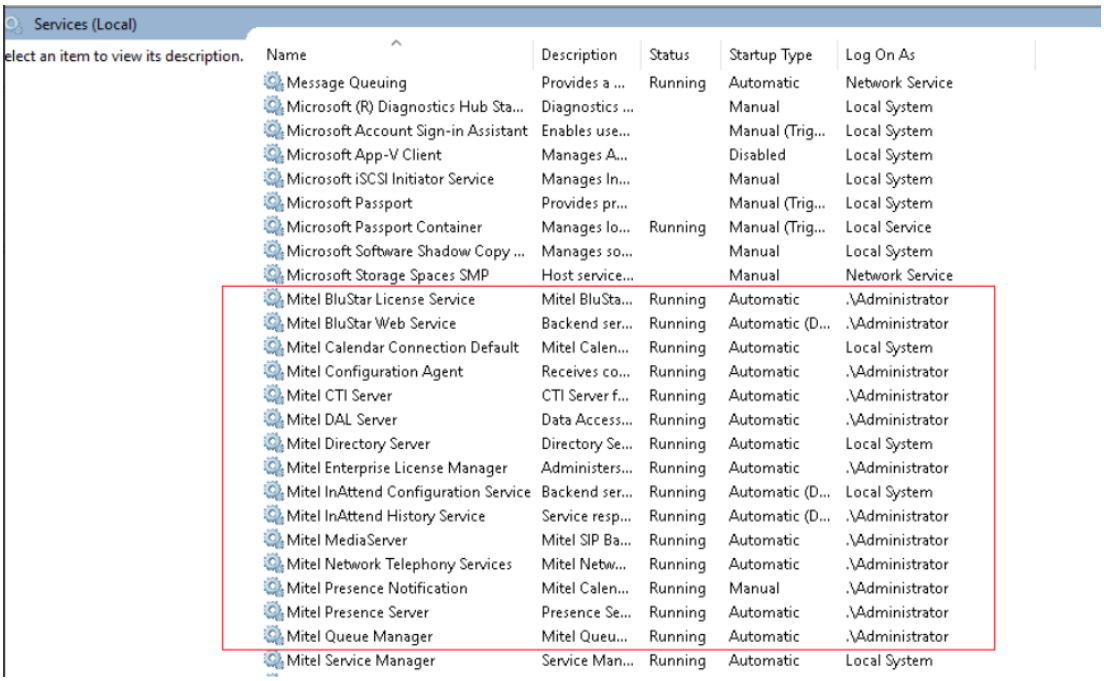
It is recommended to enable EFS on the folders where the application log, trace files and database backups are stored. This will ensure that prevention of unauthorized access

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



Setting up Quality Manager

You can extend InAttend functionality with the installation of optional components. The **Browse Packages** 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:

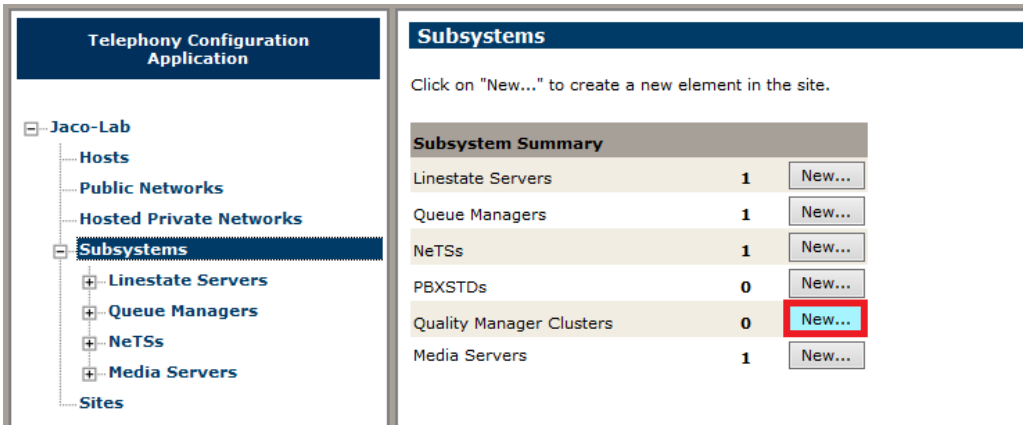
- configure the InAttend Server to recognize the Quality Manager service
- populate the Quality Manager database with the InAttend configuration information
- configure the Quality Manager service using the QM Configuration Manager tool

Configuring the InAttend Server for Quality Manager

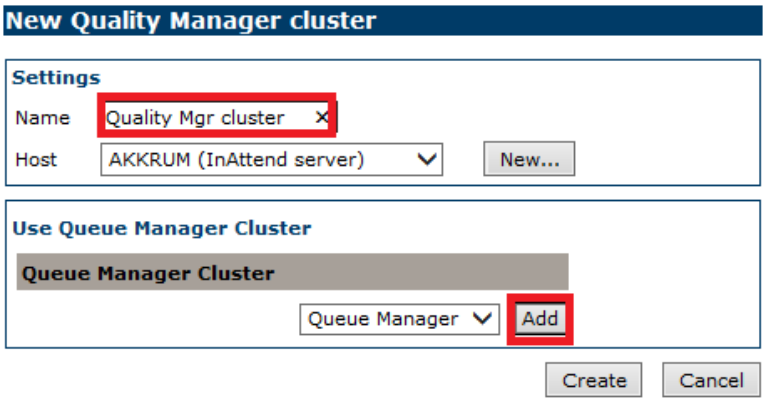
The InAttend Server has to be aware of Quality Manager for call information to be delivered to Quality Manager. To configure the InAttend Server for Quality Manager, you have to create a new Quality Manager cluster in the Telephony Configuration Application (TCA).

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.



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**.



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.

1. 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:

1. 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.

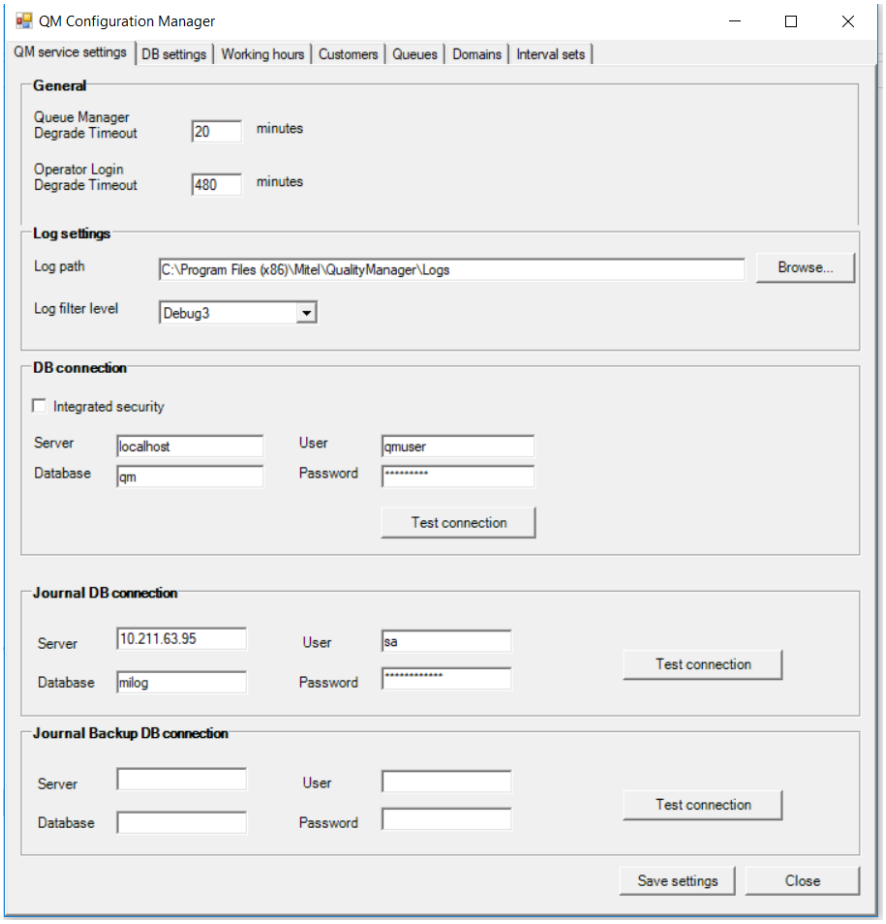
     Note that deleted data is permanently lost.
   - **Clear data after <x> days**: days before data being cleared (default is 730 days).
4. Click **Save DB settings** to apply your changes.

   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.



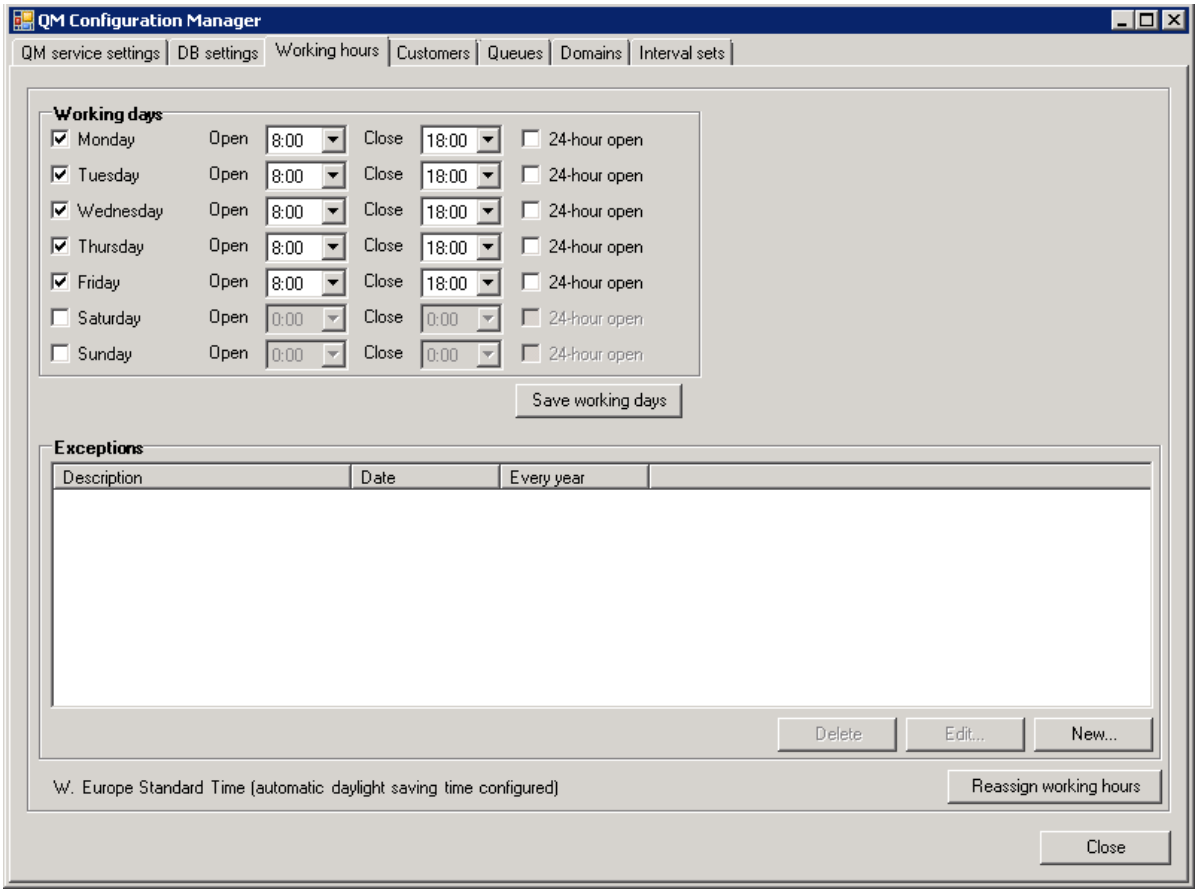
Configuring Working Hours in Quality Manager

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.



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.

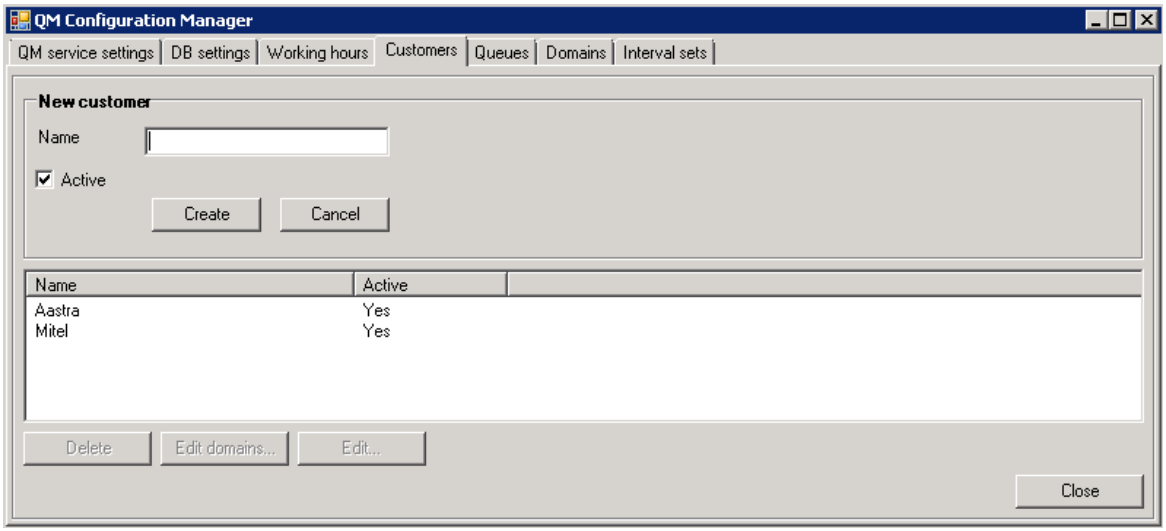
Configuring customers in Quality Manager

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.



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.

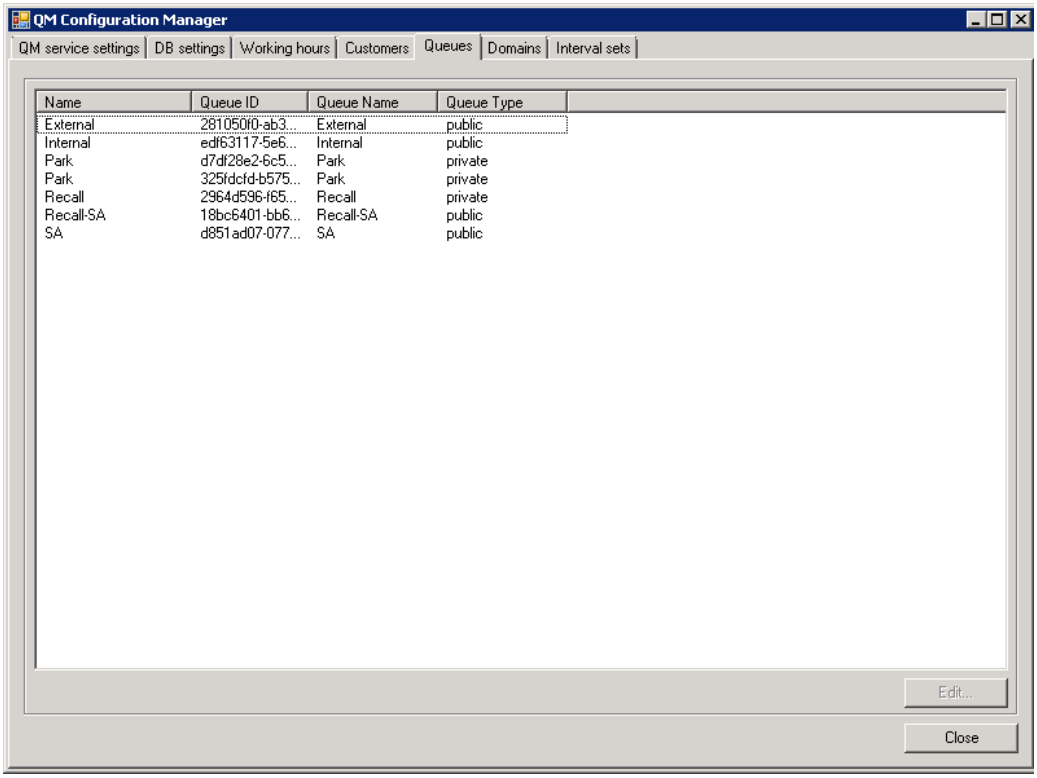
Viewing queues in Quality Manager

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).



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.

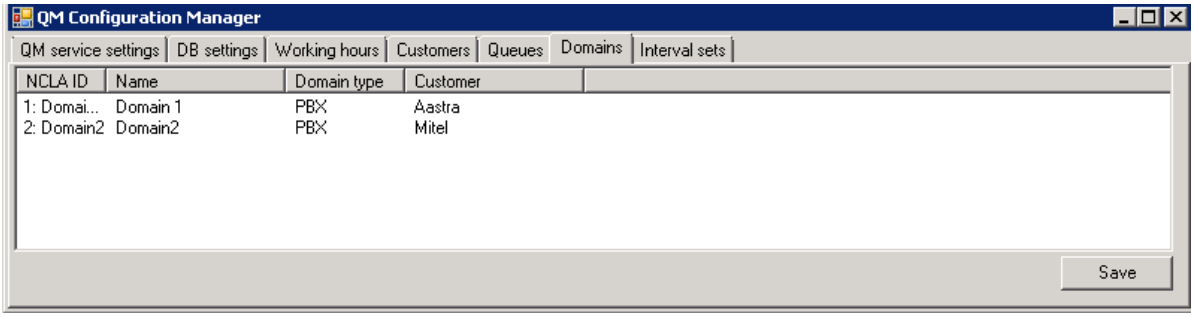
Assigning customers to a domain in Quality Manager

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.



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).

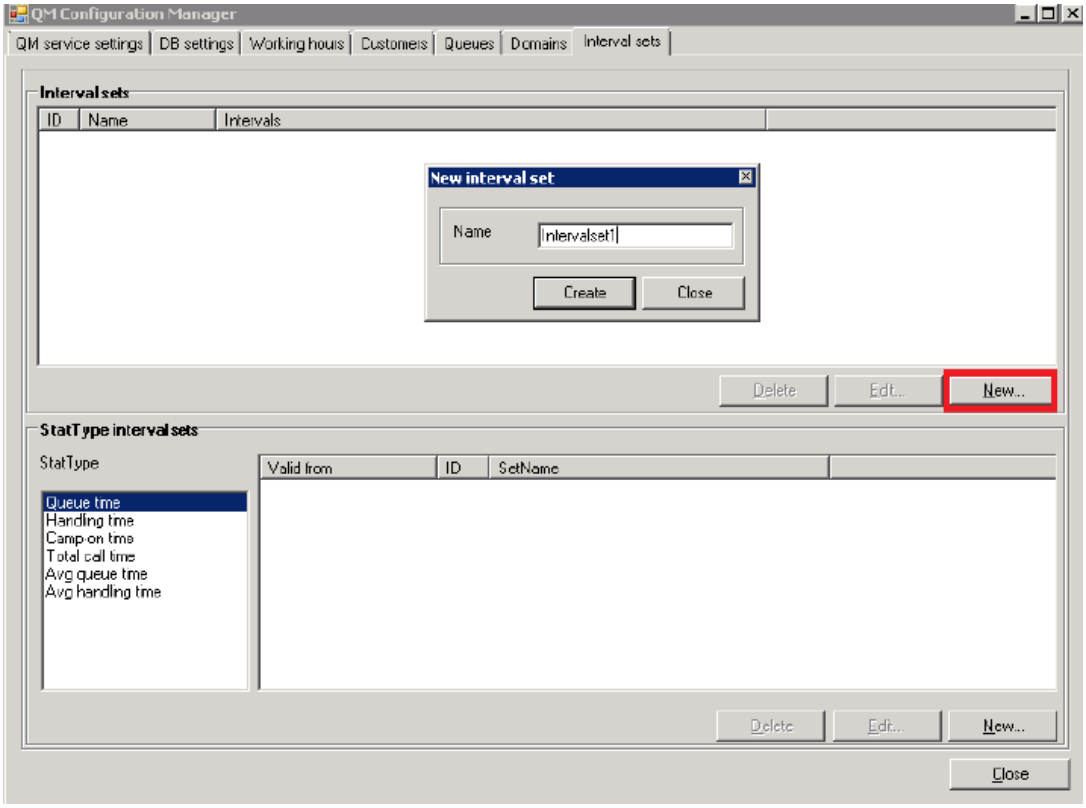
NOTE: Once intervals have been added to an interval set, you cannot change them, as this could compromise statistics that have already been collected.

When you configure the interval sets, consider which interval sets you need for each statistic type (StatType). 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**.

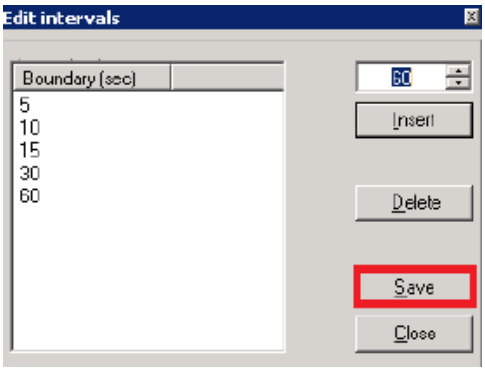
   In the **New interval set** dialog, specify a name for the new interval set and click Create to save your changes. The new interval set appears in the list.



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.)

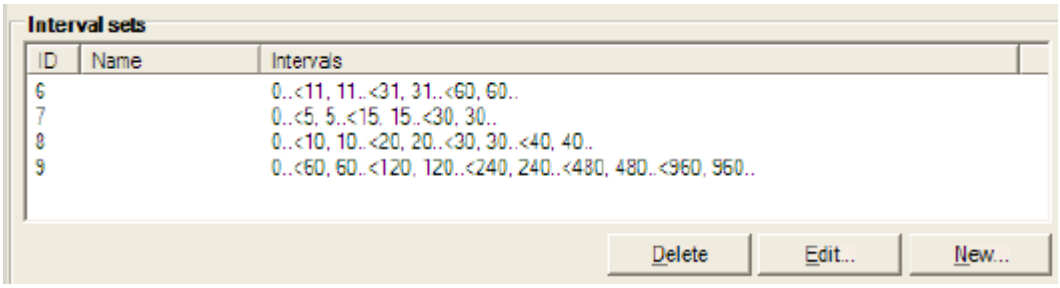
   NOTE: Once intervals have been added to an interval set, you cannot change them.
5. In the **Edit intervals** window, do the following:

   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.



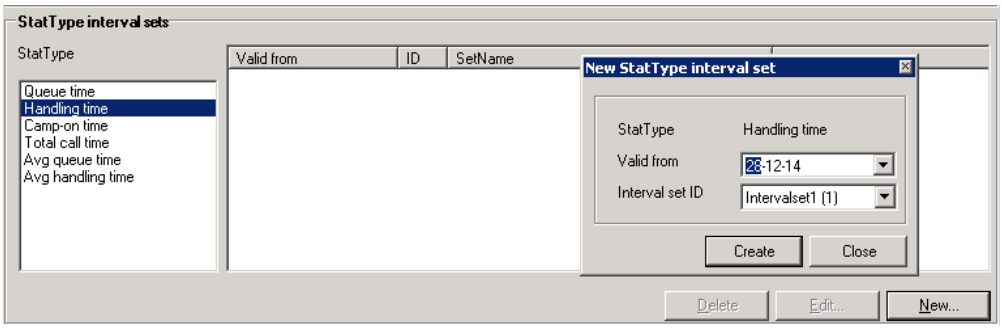
   e. Click **Close** to exit the dialog.

The new interval set and intervals are displayed in the Interval sets area of the main tab.



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:



   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 StatType 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.
4. 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:

1. 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**.

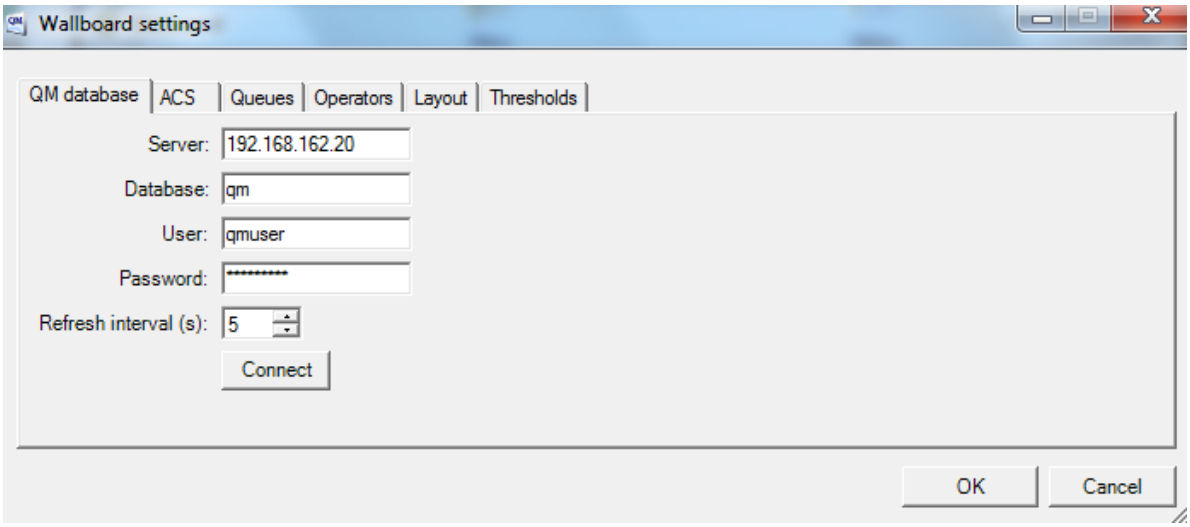
   The application displays the Wallboard Settings page.

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.

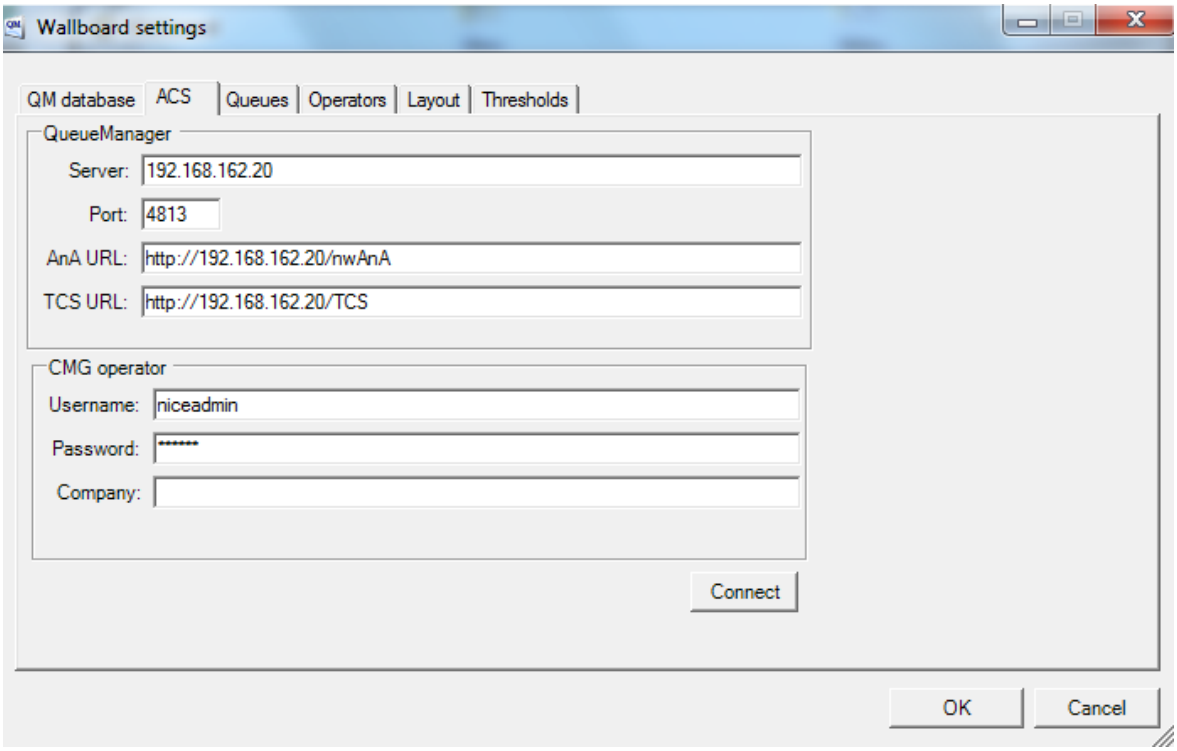


2. Specify values for the following parameters:
   - **Server**: the IP address of the server hosting the Quality Manager database.
   - **Database**: the name of the Quality Manager database (i.e., qm).
   - **User**: the name of the account configured for Quality Manager Database access. The user account “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.



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.

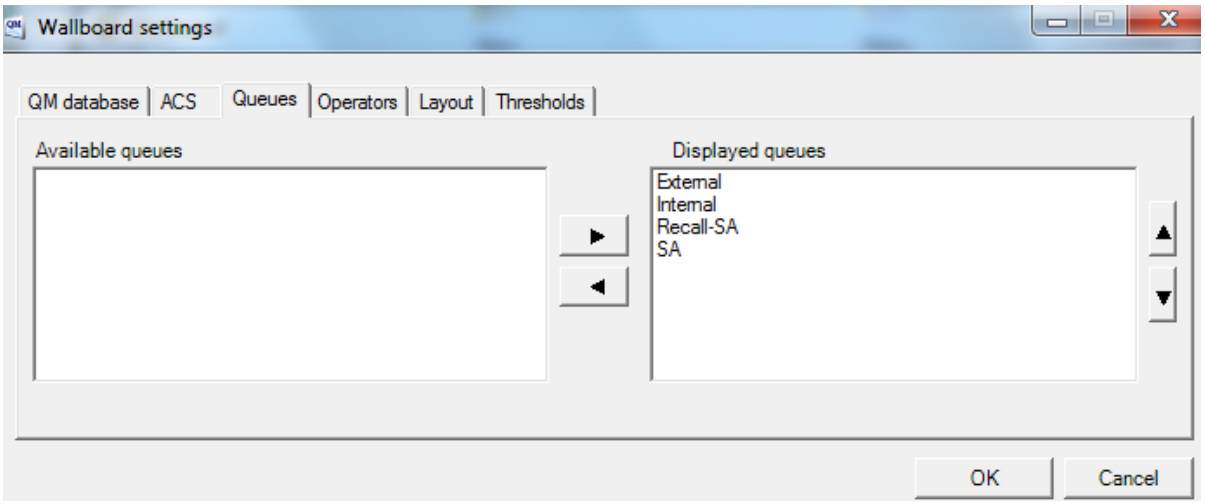
Configuring the Queues to display

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.

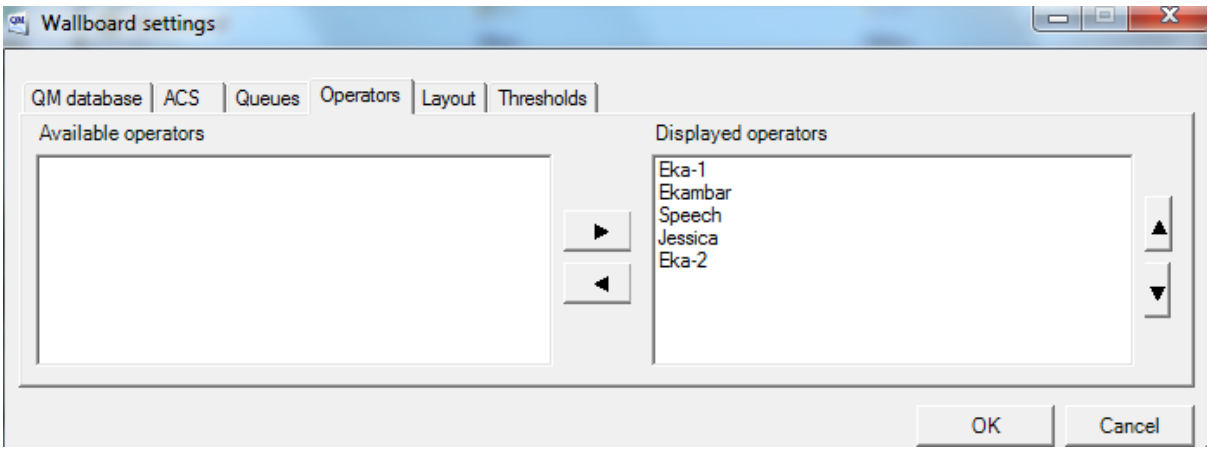


2. Select a queue from the **Available queues** list and click the right arrow to move it to the **Displayed queues** list.
3. Repeat step 2 for each additional queue you want to display.
4. To remove a queue from the Wallboard display, select the entry in the Displayed queues list and click the left 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.



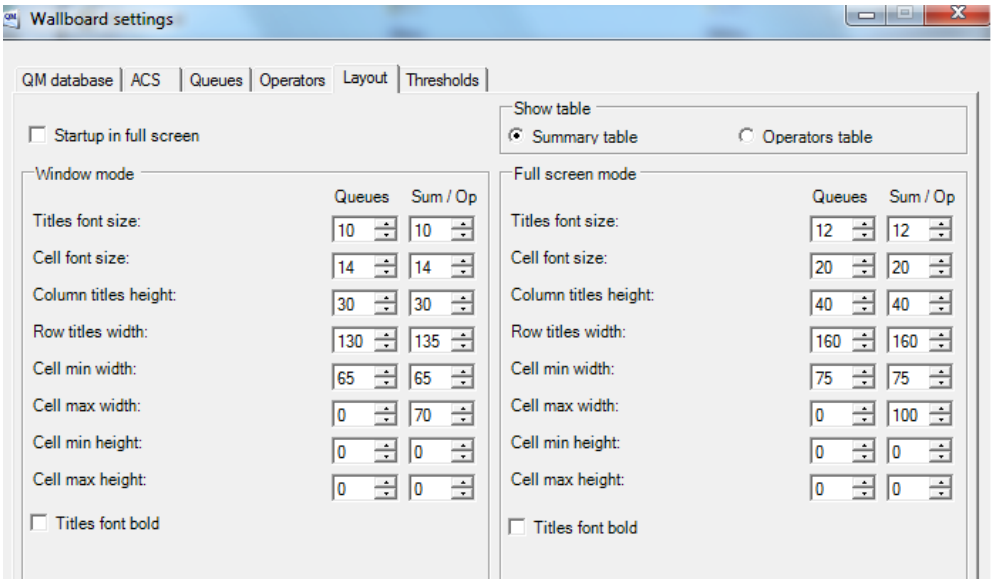
2. Select an operator from the **Available operators** list and click the right arrow to move it to the **Displayed operators** list.

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.



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.

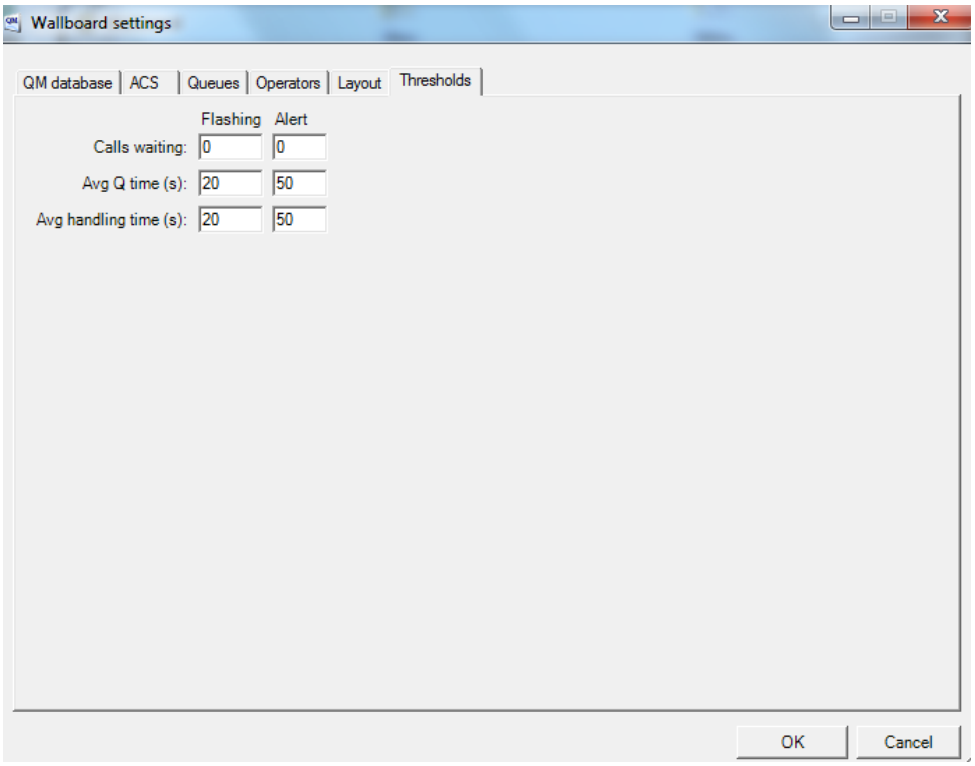
Configuring thresholds for alerts

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.



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

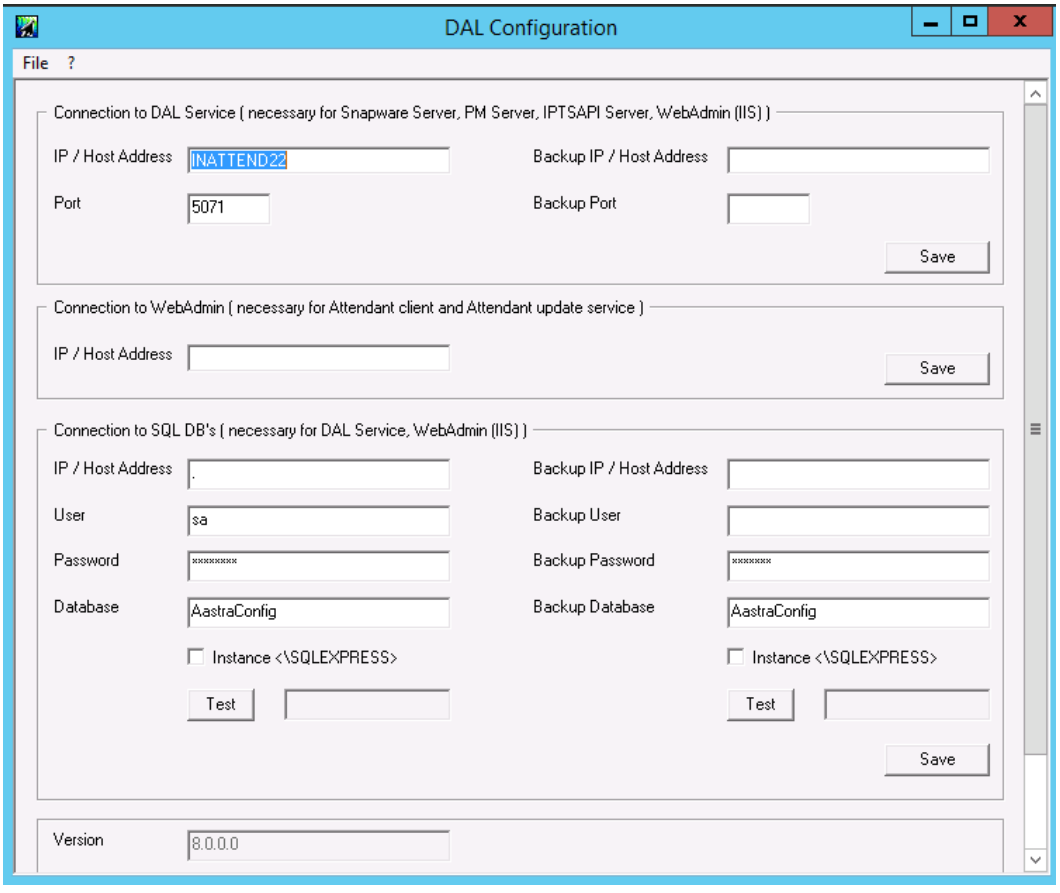
The following configuration tools are also available if you want to make changes to your system configuration after initial installation and configuration:

- **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. 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.

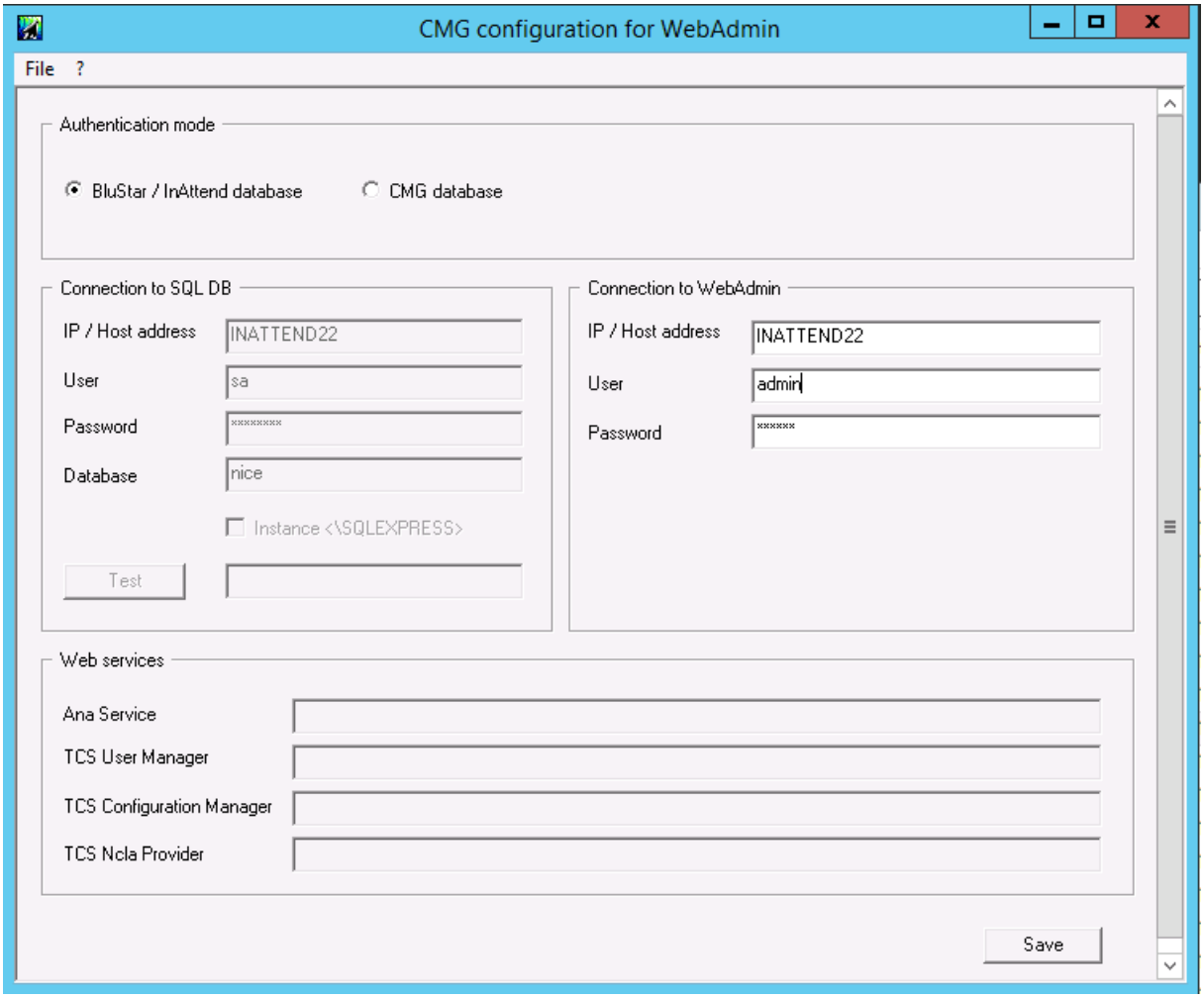
CMG configuration tool

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:

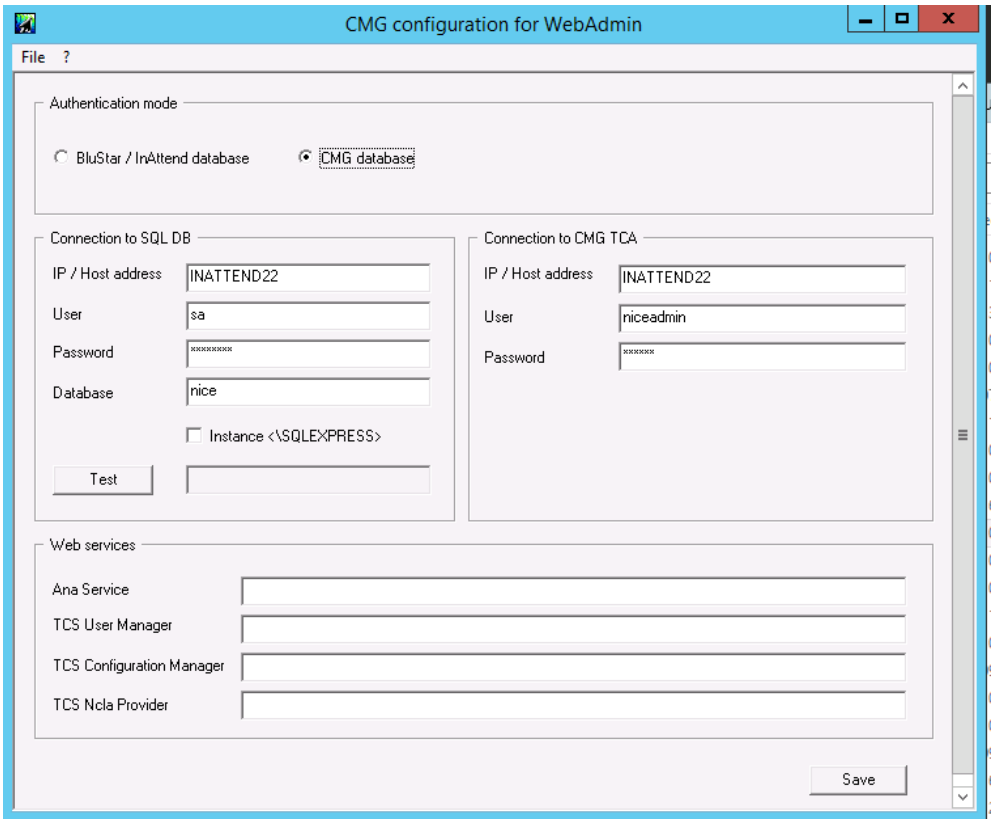
1. Navigate to the BluStar Server folder (**Start > Program Files > Mitel > BluStar Server) and double-click on the CMGConfigTool.exe** file.
The system opens the CMG configuration for WebAdmin tool.


CMG configuration for WebAdmin
File ?
Authentication mode
BluStar / InAttend database
CMG database
Connection to SQL DB
IP / Host address
INATTEND22
User
sa
Password
Database
nice
Instance <\SQLEXPRESS>
Test
Connection to WebAdmin
IP / Host address
INATTEND22
User
admin
Password
Web services
Ana Service
TCS User Manager
TCS Configuration Manager
TCS Ncla Provider
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.



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://<host-name>/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	PASSED	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.

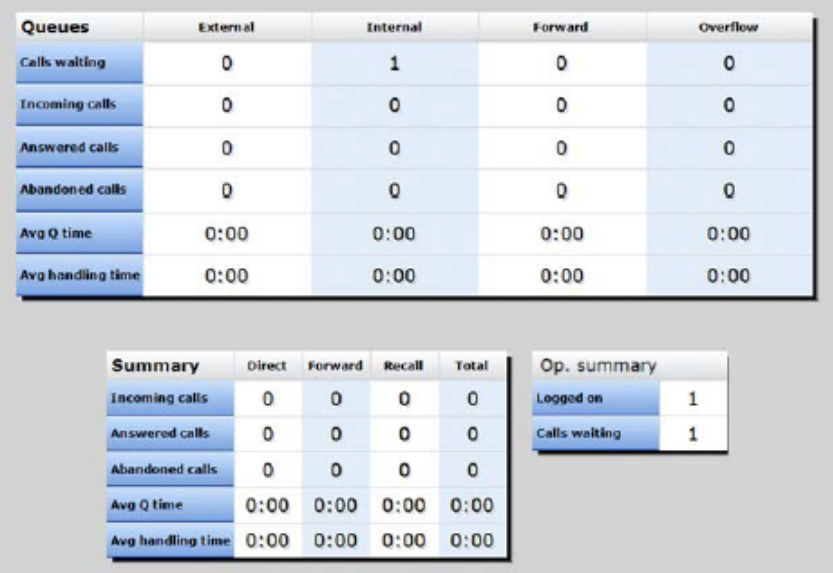
   The generated report contains a graph and a table with no data.
4. Make a call to an operator.
   a. Make a call that is routed to the switchboard.
   b. Answer the call in the InAttend client.
   c. End the call.
5. Regenerate the Quality Manager report with the same time interval and granularity. The 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:

1. 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	External	Internal	Forward	Overflow
Calls waiting	0	1	0	0
Incoming calls	0	0	0	0
Answered calls	0	0	0	0
Abandoned calls	0	0	0	0
Avg Q time	0:00	0:00	0:00	0:00
Avg handling time	0:00	0:00	0:00	0:00

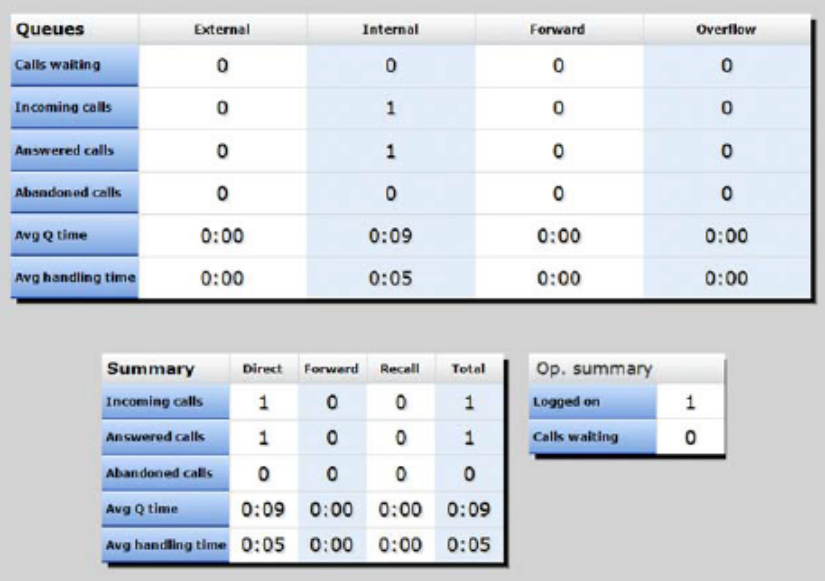
Summary	Direct	Forward	Recall	Total
Incoming calls	0	0	0	0
Answered calls	0	0	0	0
Abandoned calls	0	0	0	0
Avg Q time	0:00	0:00	0:00	0:00
Avg handling time	0:00	0:00	0:00	0:00

Op. summary	
Logged on	1
Calls waiting	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



Queues	External	Internal	Forward	Overflow
Calls waiting	0	0	0	0
Incoming calls	0	1	0	0
Answered calls	0	1	0	0
Abandoned calls	0	0	0	0
Avg Q time	0:00	0:09	0:00	0:00
Avg handling time	0:00	0:05	0:00	0:00

Summary	Direct	Forward	Recall	Total
Incoming calls	1	0	0	1
Answered calls	1	0	0	1
Abandoned calls	0	0	0	0
Avg Q time	0:09	0:00	0:00	0:09
Avg handling time	0:05	0:00	0:00	0:05

Op. summary	
Logged on	1
Calls waiting	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.

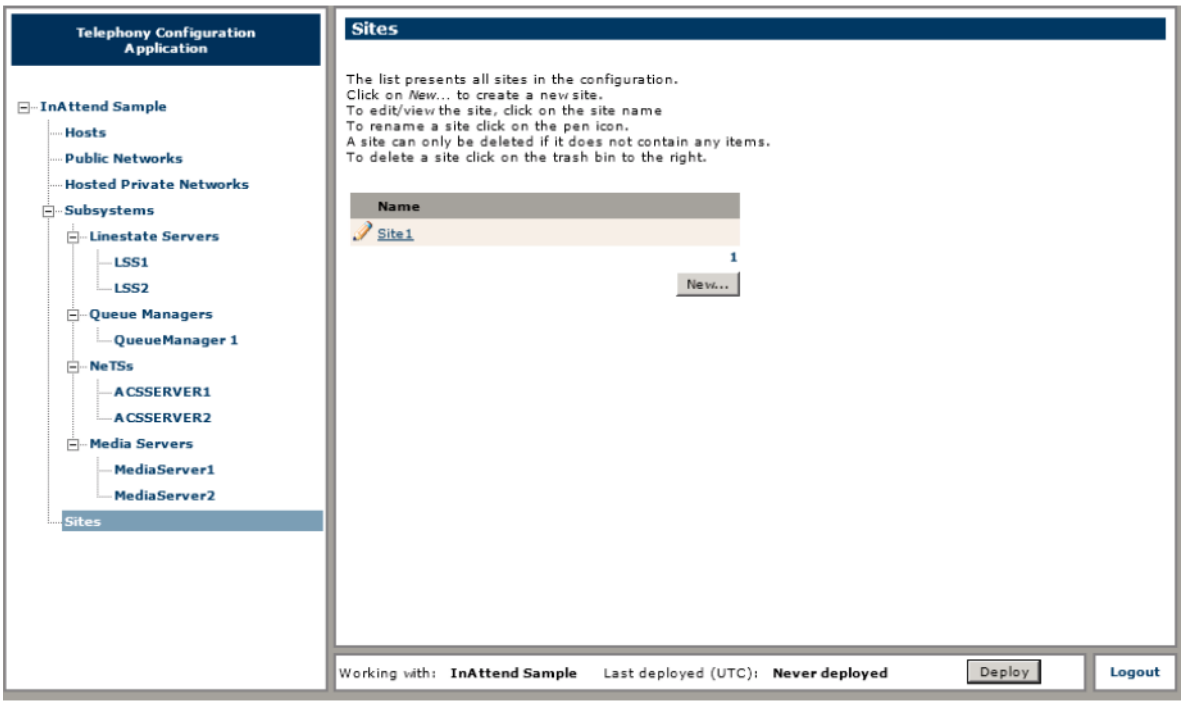
You can access the TCA tool from a supported browser (for example, Internet Explorer or Edge Chromium), using the following address: `http://<TCA web server>/TCA (where <TCA web server>` is the InAttend server address).

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.

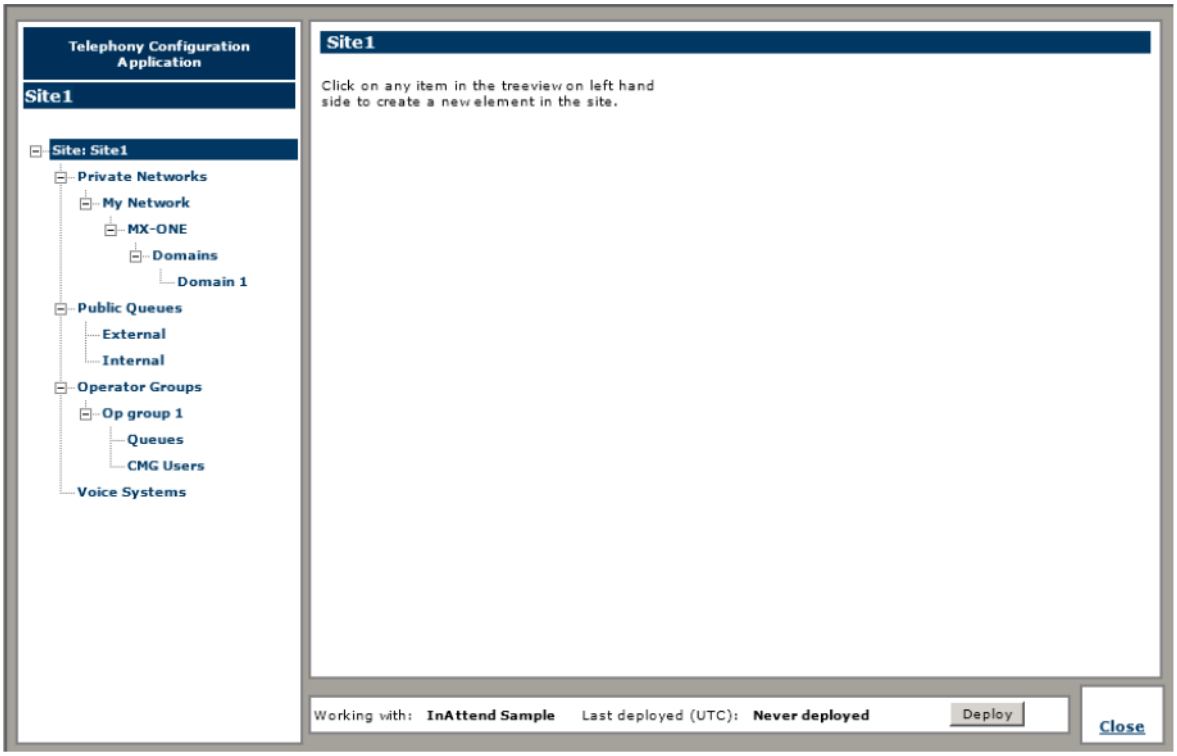
When creating a configuration, it is recommended that you use one of the predefined configuration templates. When you use a predefined template, the system automatically creates the required components for your configuration. You only need to customize the components with your specific configuration.

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



TCA Site Configuration: MX-ONE SIP Template

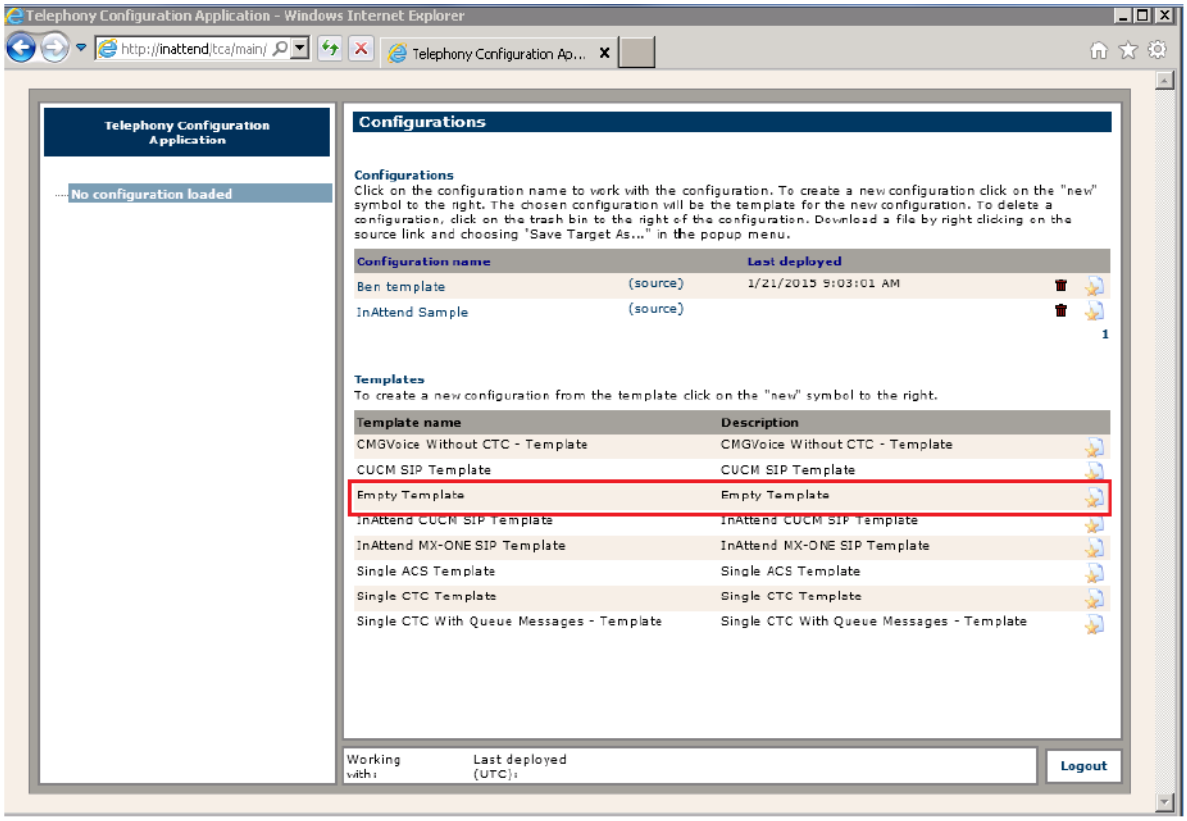


Create a TCA configuration

The configuration example described in the following sections uses the Empty Template, to describe creation and configuration of all required components.

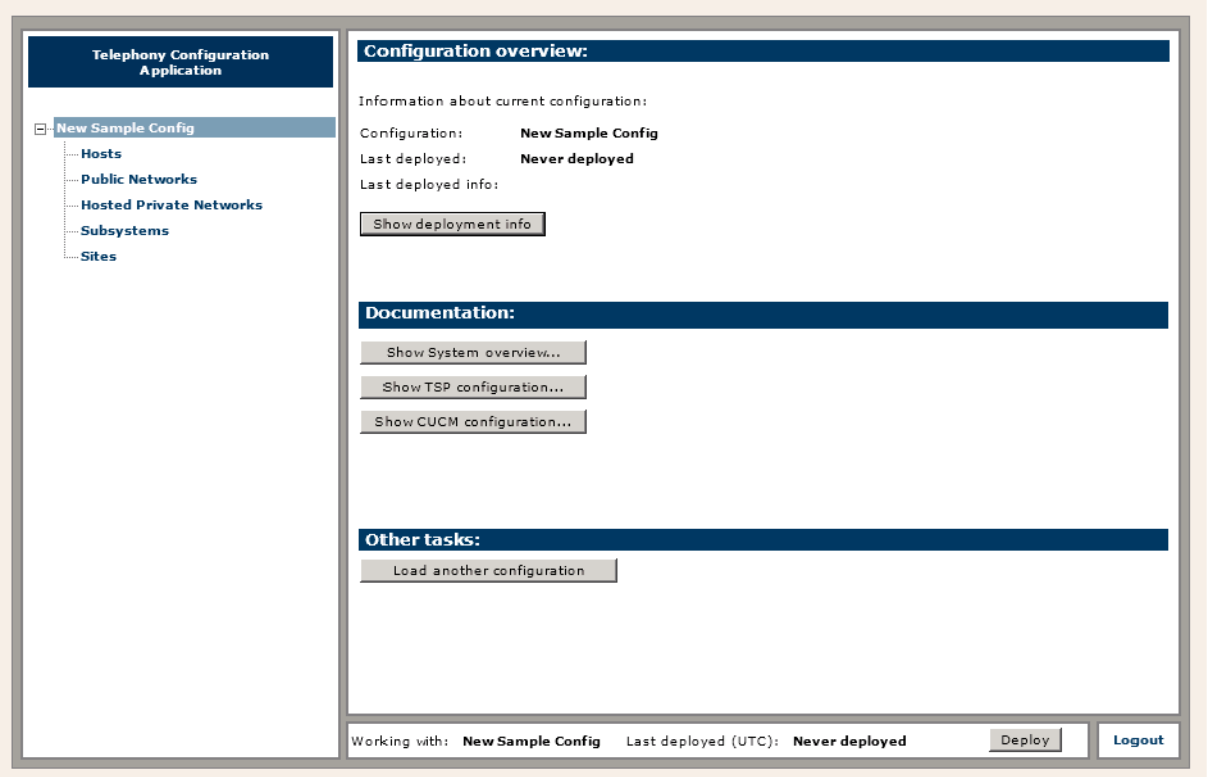
To create a new TCA configuration, do the following:

1. Open a browser and log in to the TCA tool ().
2. On the Configurations page, click on the icon beside the Empty Template.



3. Enter a name for the configuration and click Create.

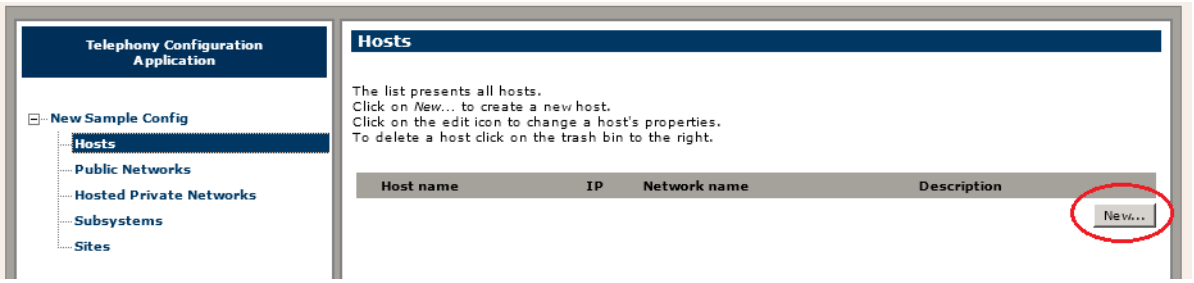
   TCA displays the Configuration overview page.



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.



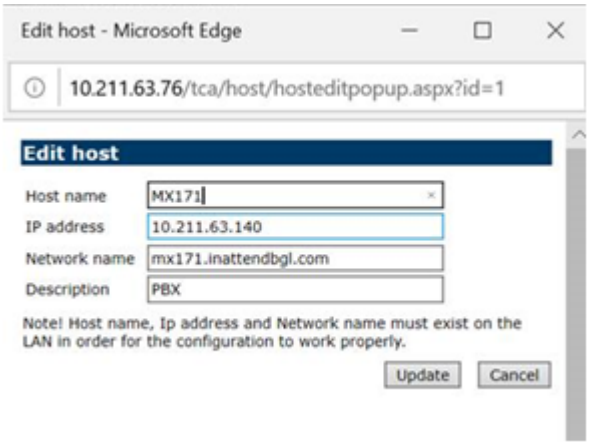
3. In the **New Host** window, specify values for the following fields:
   - **Host name**: the hostname (known in the network) of the server. The host name is used by software to identify the machine on which it is running.
   - **IP address**: the IP address of the server. This field is optional when 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.

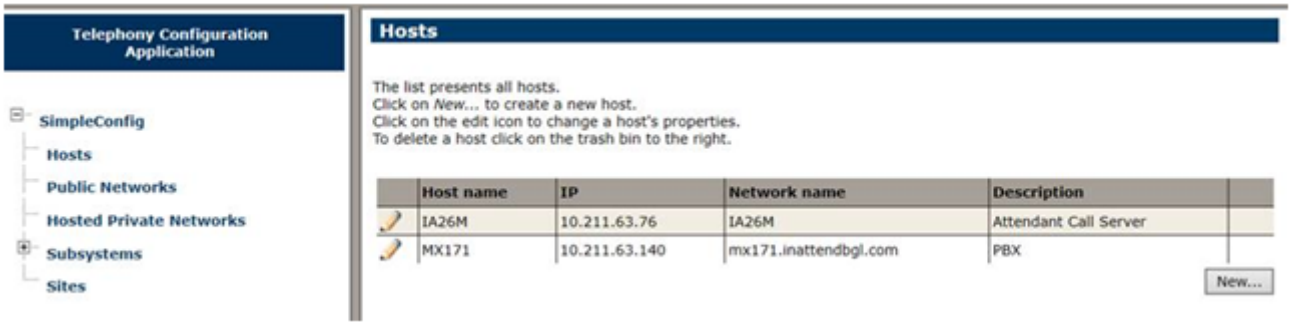
  If only when no IP address is specified, then NeTS does DNS SRV lookup on the specified "networkName".

  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).



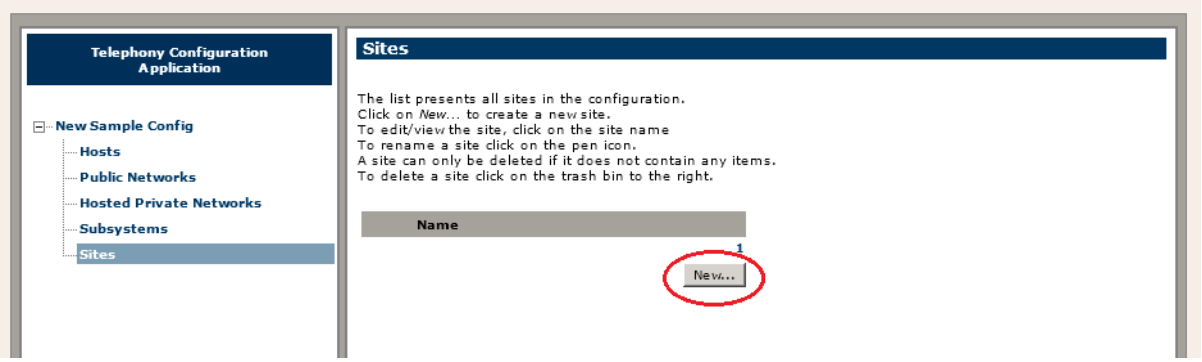
4. Click **Create** to save your changes.
5. Repeat steps 2 to 4 to create the call manager host (with the appropriate parameter values for the call manager). The system displays the new hosts on the Hosts page



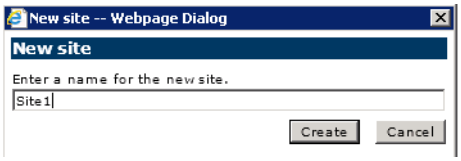
Add a site

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.

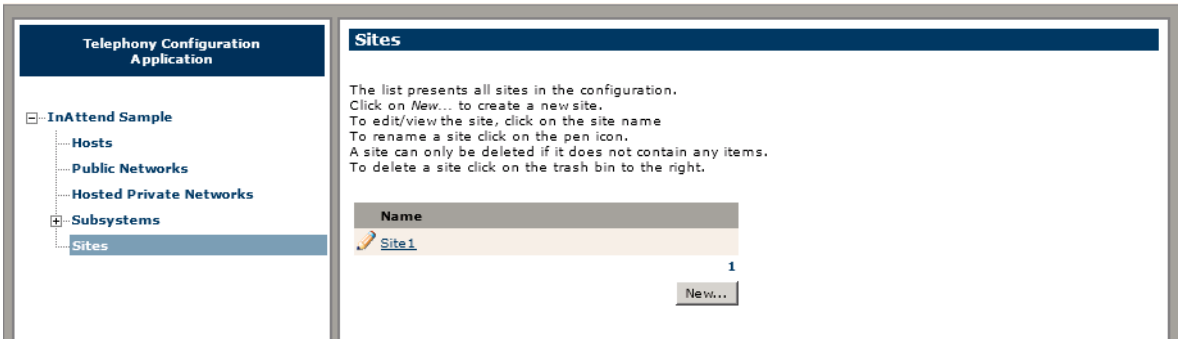
1. In the left panel of the TCA interface, click on Sites.TCA displays the Sites page in the main window.
2. Click on the **New** button to create a new site.



3. In the **New site** dialog, enter a name for the site and click Create.



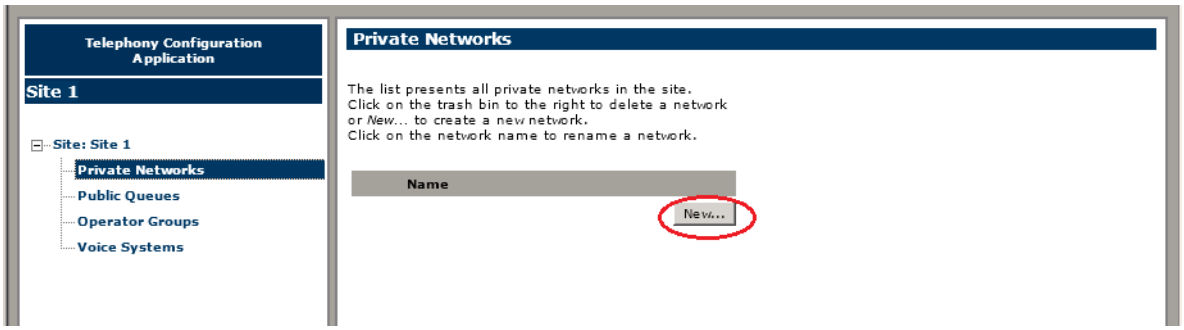
TCA creates the new site and displays the new site on the Sites page.



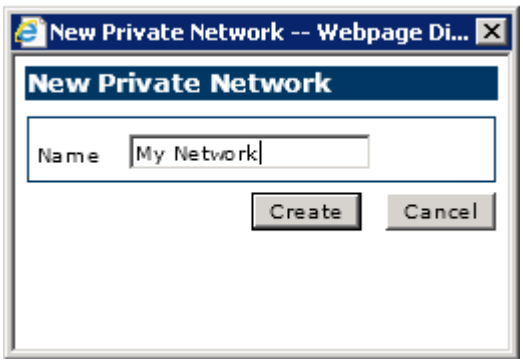
Configure a network for the site

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.

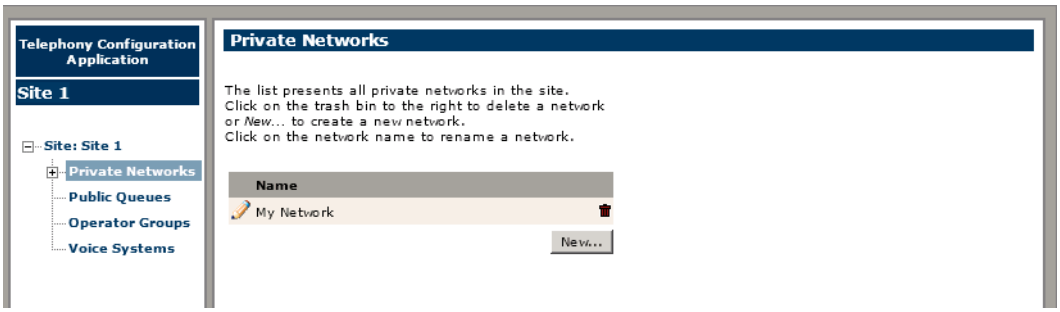
1. Click on the site entry to open the site configuration.
   TCA opens the Site page in a new window.
2. On the Site page, click on **Private Networks** in the left panel to display the Private Networks page in the main window.
3. Click the **New** button to create a network.



4. In the **New network** dialog, enter a name for the network and click **Create**.



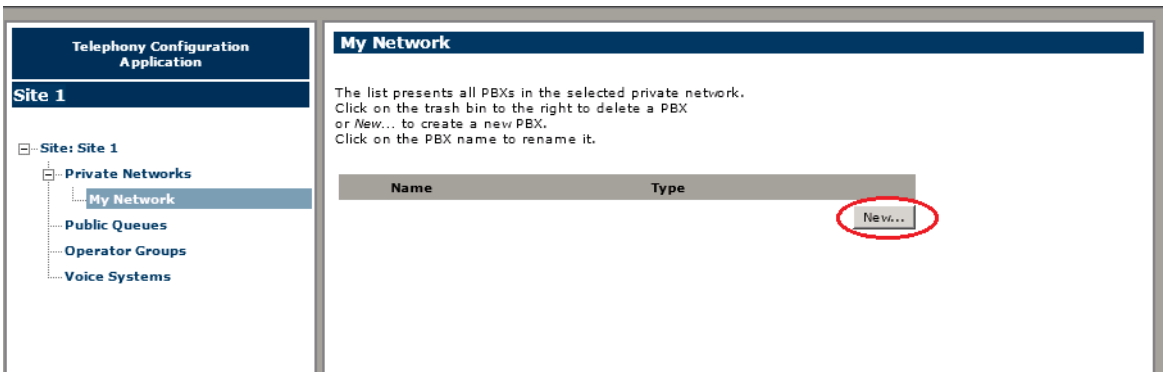
TCA creates the network component and displays the network on the Private Networks page.



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.



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.

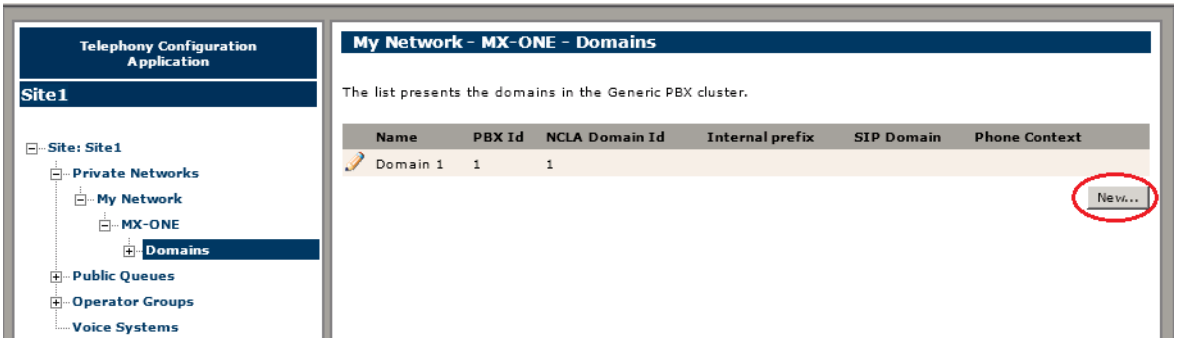
5. Click Create to create the PBX.

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.

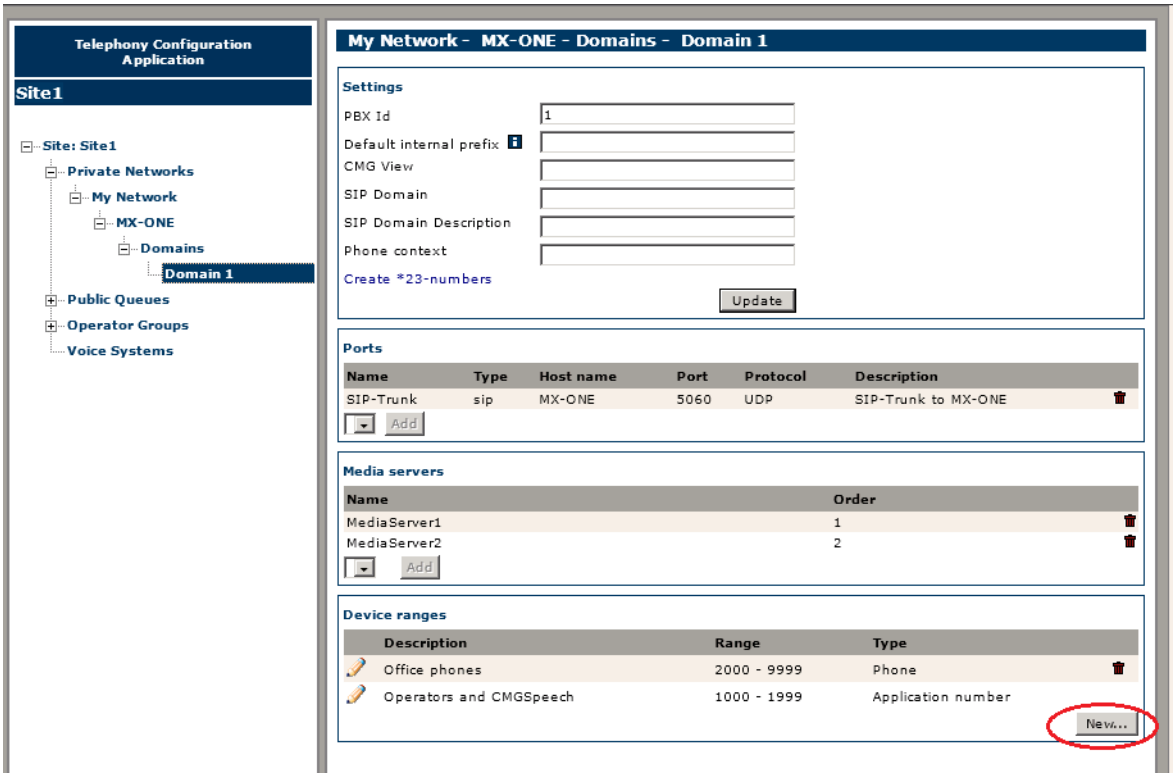
5. Click **Create** to create the domain.

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.

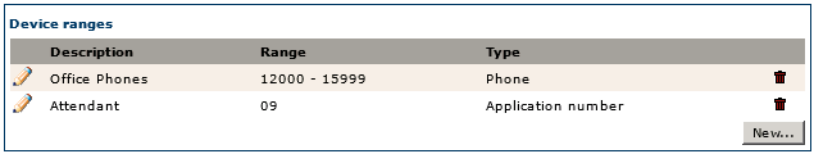


4. In the **New device range** window, specify values for the following fields:
   - **Type**: the device range type; select Phone.
   - **Description**: optional information to describe the device type (e.g., “Office phones”).
   - **Internal prefix**: leave blank.
   - **Range**: specify the number 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.

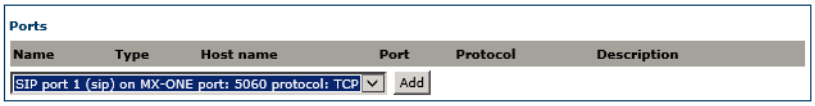
7. In the **New device range** window, specify values for the following fields:
   - **Type**: the device range type; select Application Number.
   - **Description**: optional information to describe the device type (e.g., “Attendant”).
   - **Internal prefix**: leave blank.

     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.



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**.

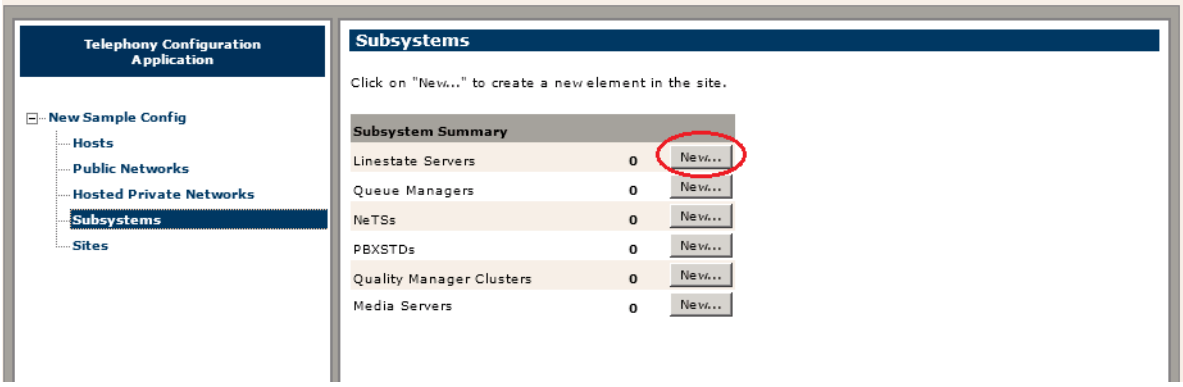


10. Click **Close** to complete the site configuration.

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.



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.

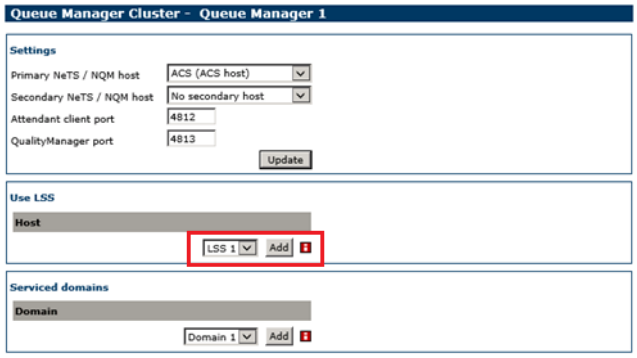
4. Click **Create** to add the Linestate Server.

Add a Queue Manager

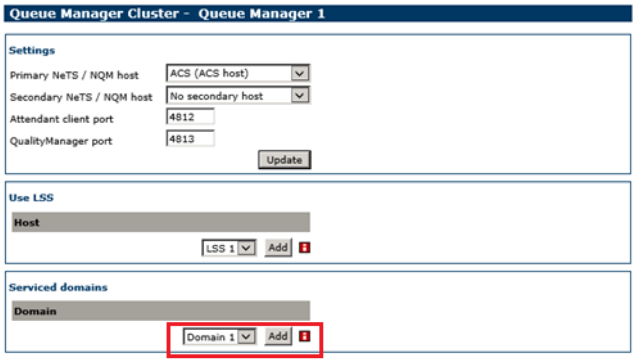
Do the following:

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**.



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).



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.

1. 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.

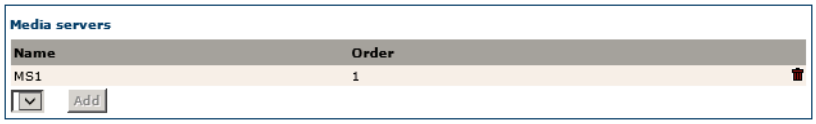
Create a media server and add it to the site

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.



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).

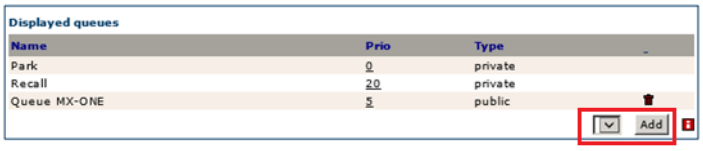
iii. **Recalls from Consult Calls**: enable or disable. Determines whether calls are sent back to the attendant in case of no answer on a consult call.

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**.



NOTE: If you make any change in Operator Groups, restart the InAttend Client.

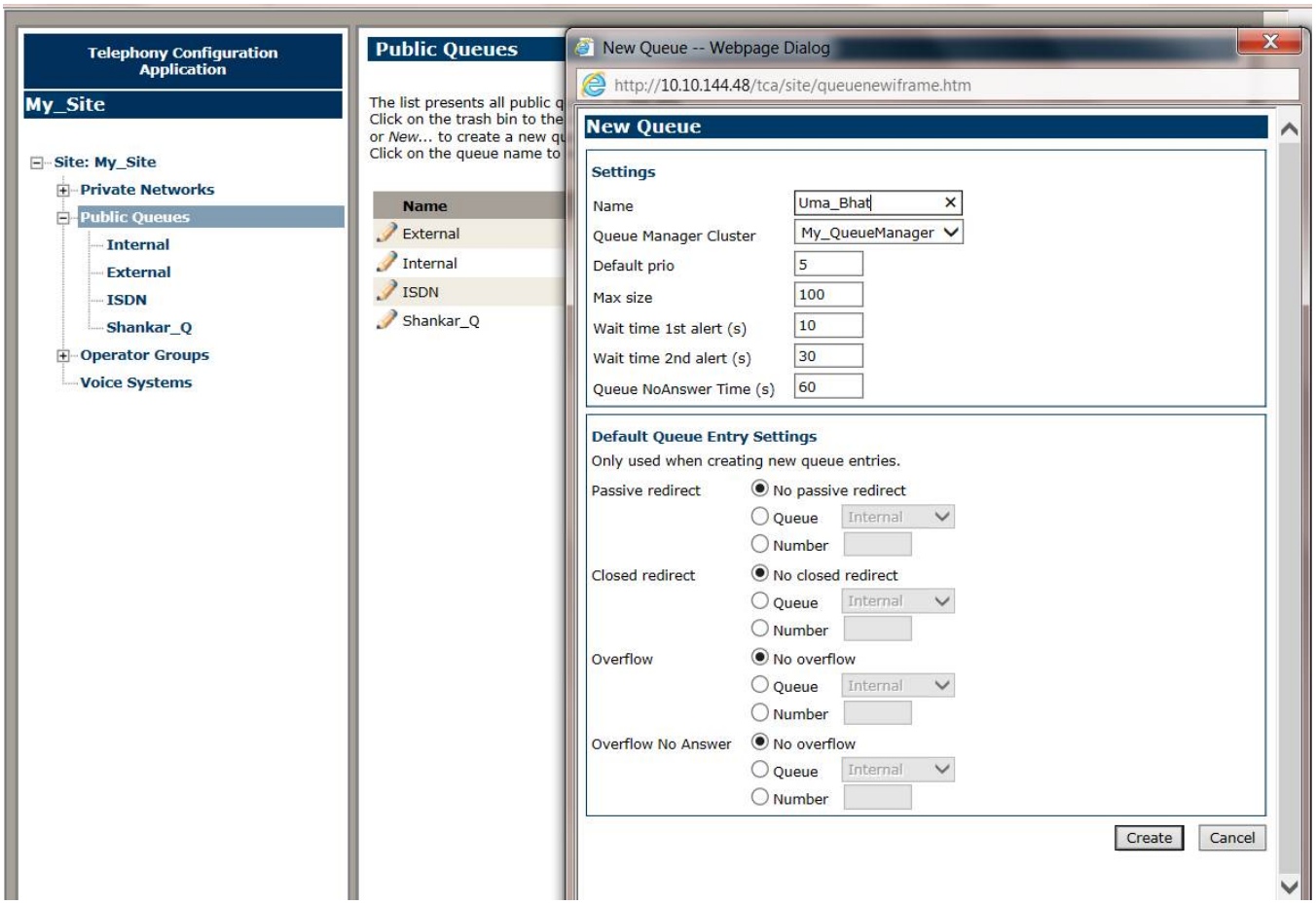
Configuring public recall queues

To assign a public recall queue, a Public Queue is added under “Public Queues” first.

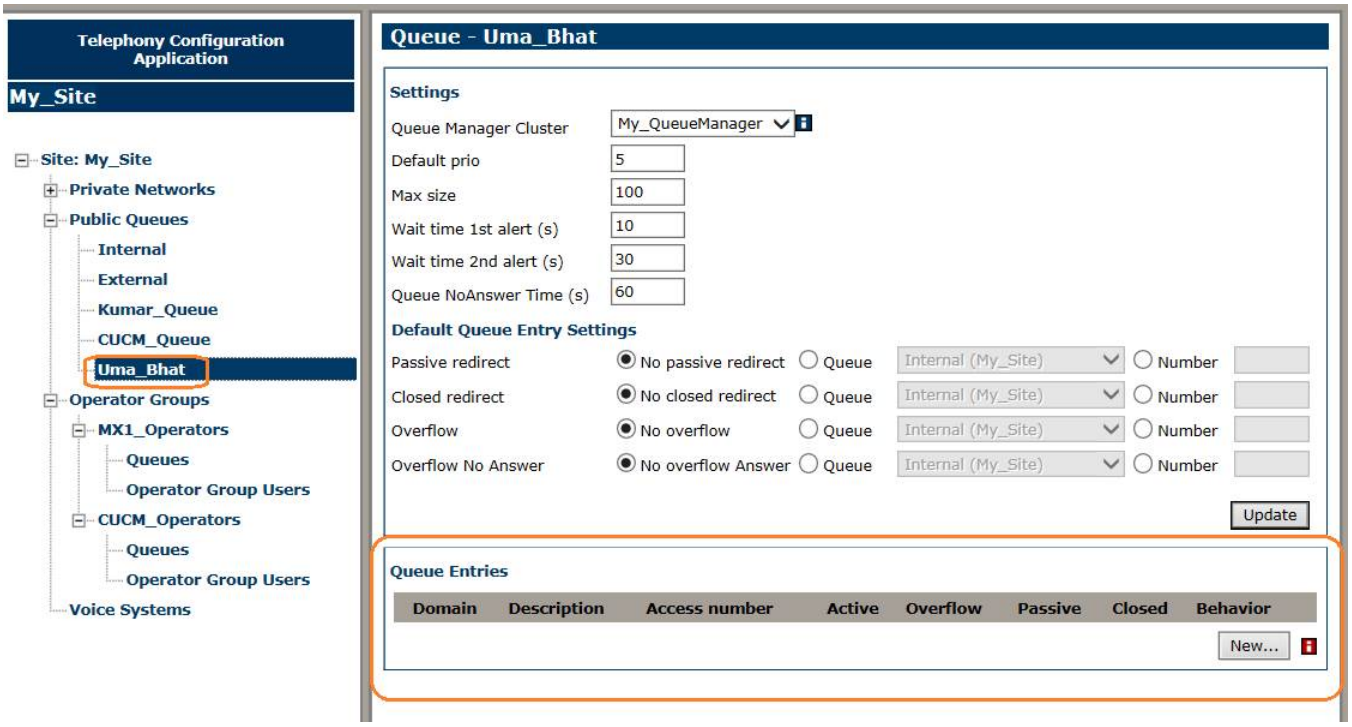
NOTE: It is not allowed to use a "public operator queue" i.e. reached by an access number as a public recall and/or park queue.

For example: If we want to create a new queue – Uma_Bhat, follow the below steps:

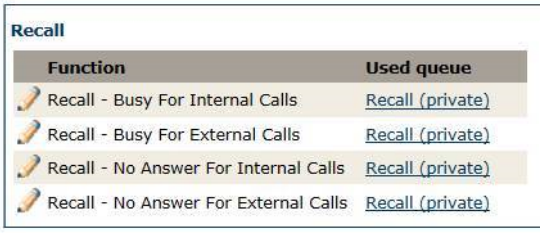
1. Go to **Public Queues**.
2. Select **New Queue**.
3. Enter a desired **Name** for the new queue.
4. The values for Queue manager cluster, Default prio, Max size, Wait time 1st alert, Wait time 2nd alert, and Queue NoAnswer Time is taken by default.
5. Click **Create**.



A New Queue – Uma_Bhat is created. This queue does not have an access number.

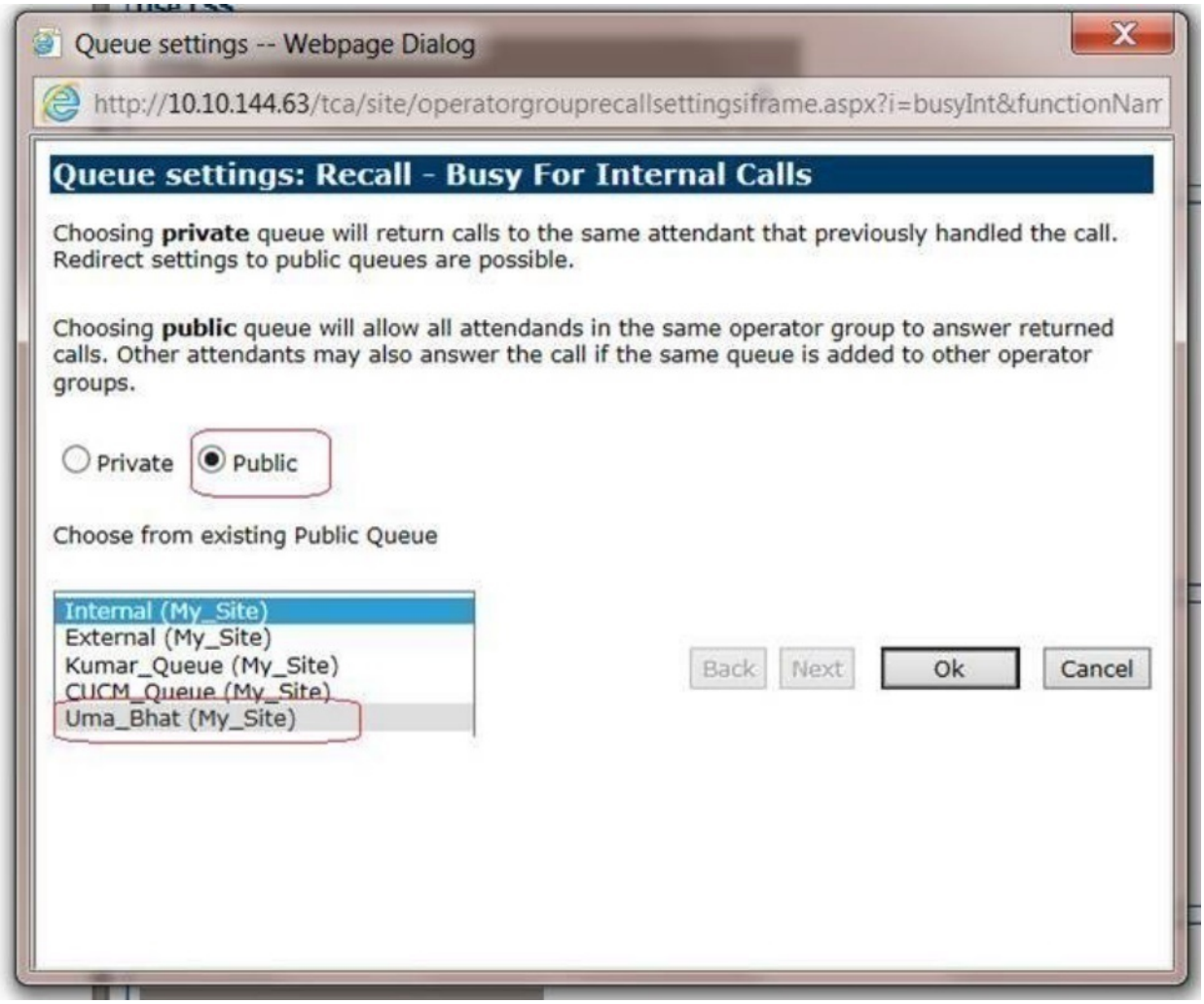


Queue entry without an access number
The Call queues are Private by default under the Recall and Park.



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**.



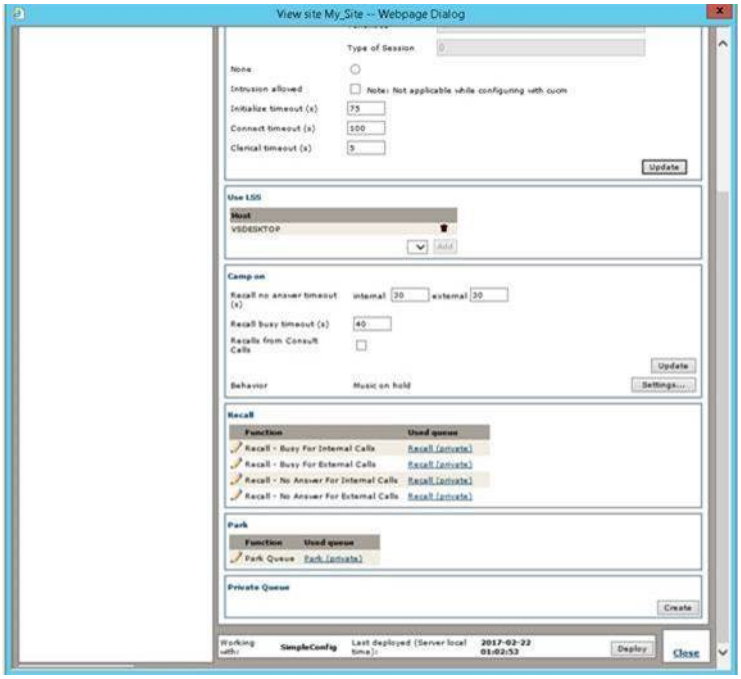
e. The **Queue Settings Recall – Busy for Internal Calls**window is displayed.
f. 2 radio buttons for Public and Private are displayed.
g. Choose the queue (Uma_Bhat) to be changed to public.
h. Select **Public**.
i. Click **Ok**.

The private queue Uma_Bhat is changed to public queue.

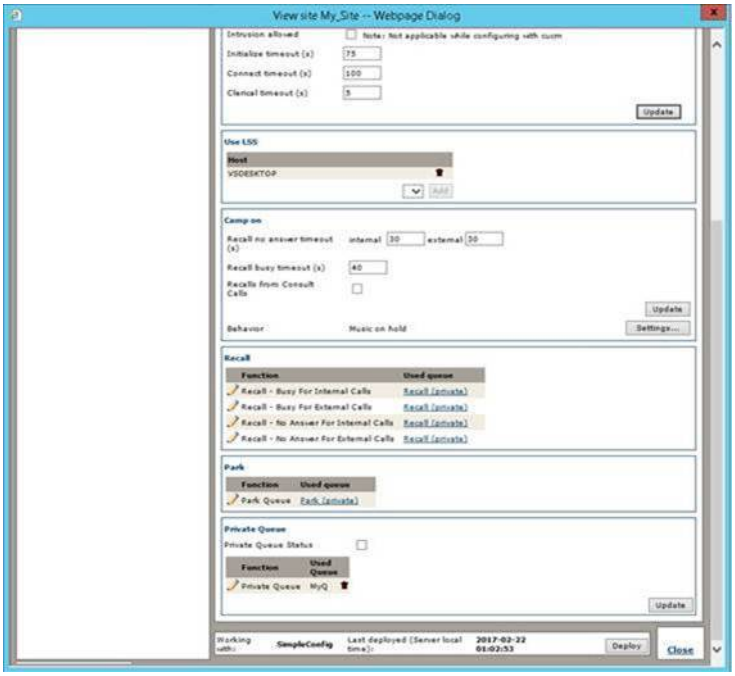
Private Queue Number for Individual Attendants

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.*



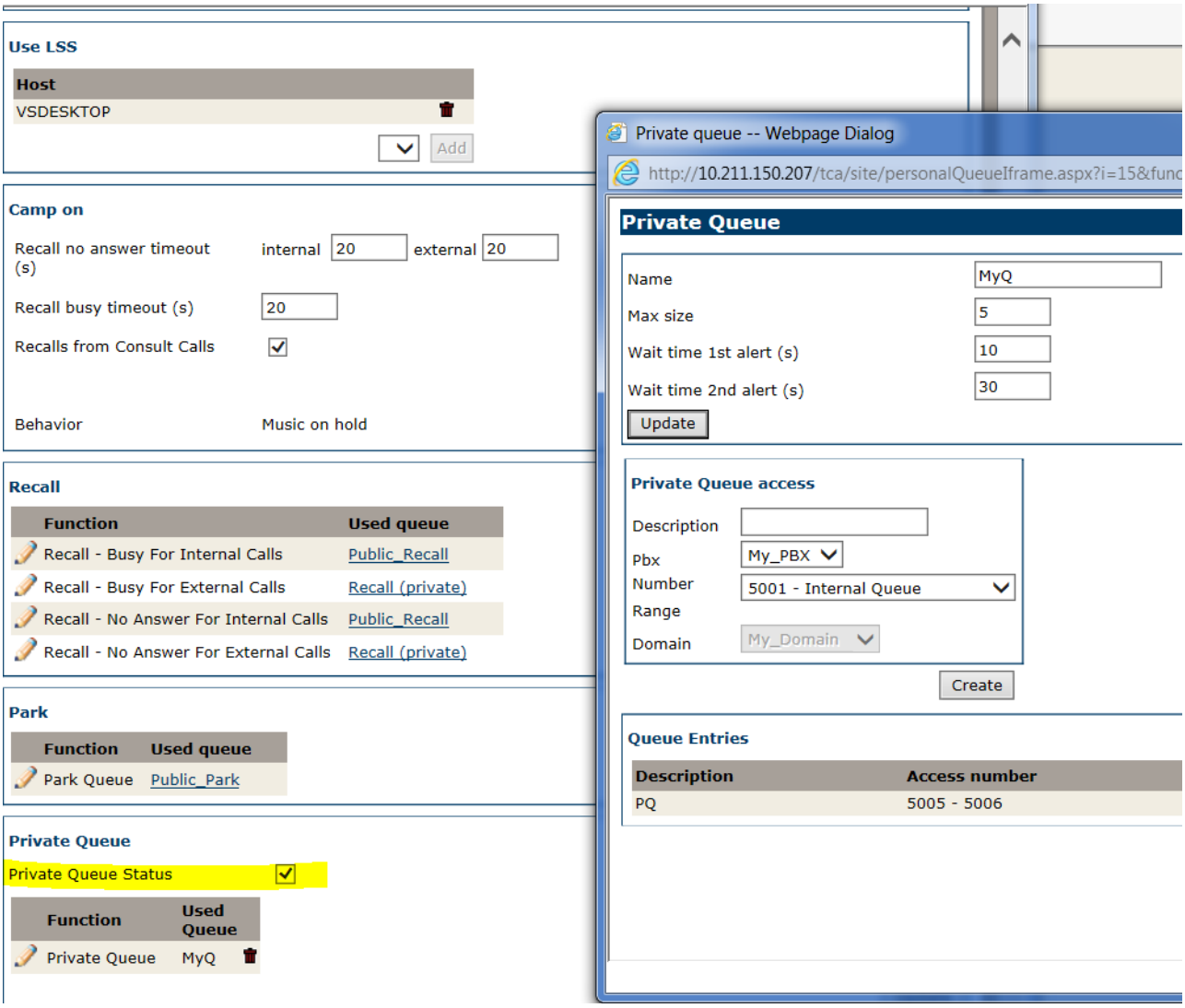
Private Queue before creation



Private Queue after creation

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.

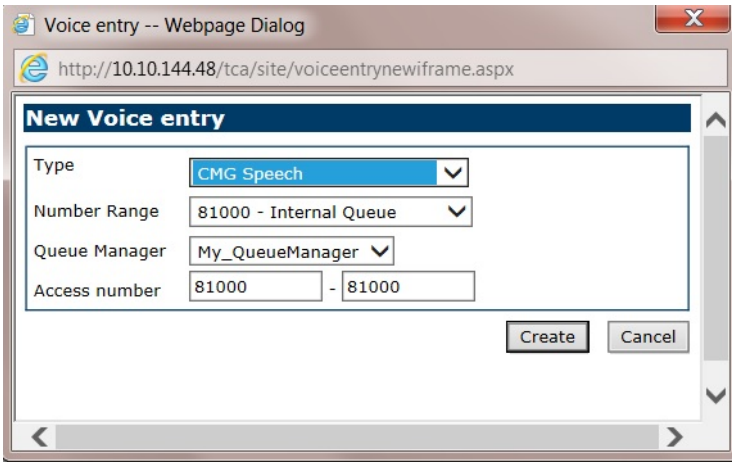


Private Queue Access page

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.



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.

1. 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.

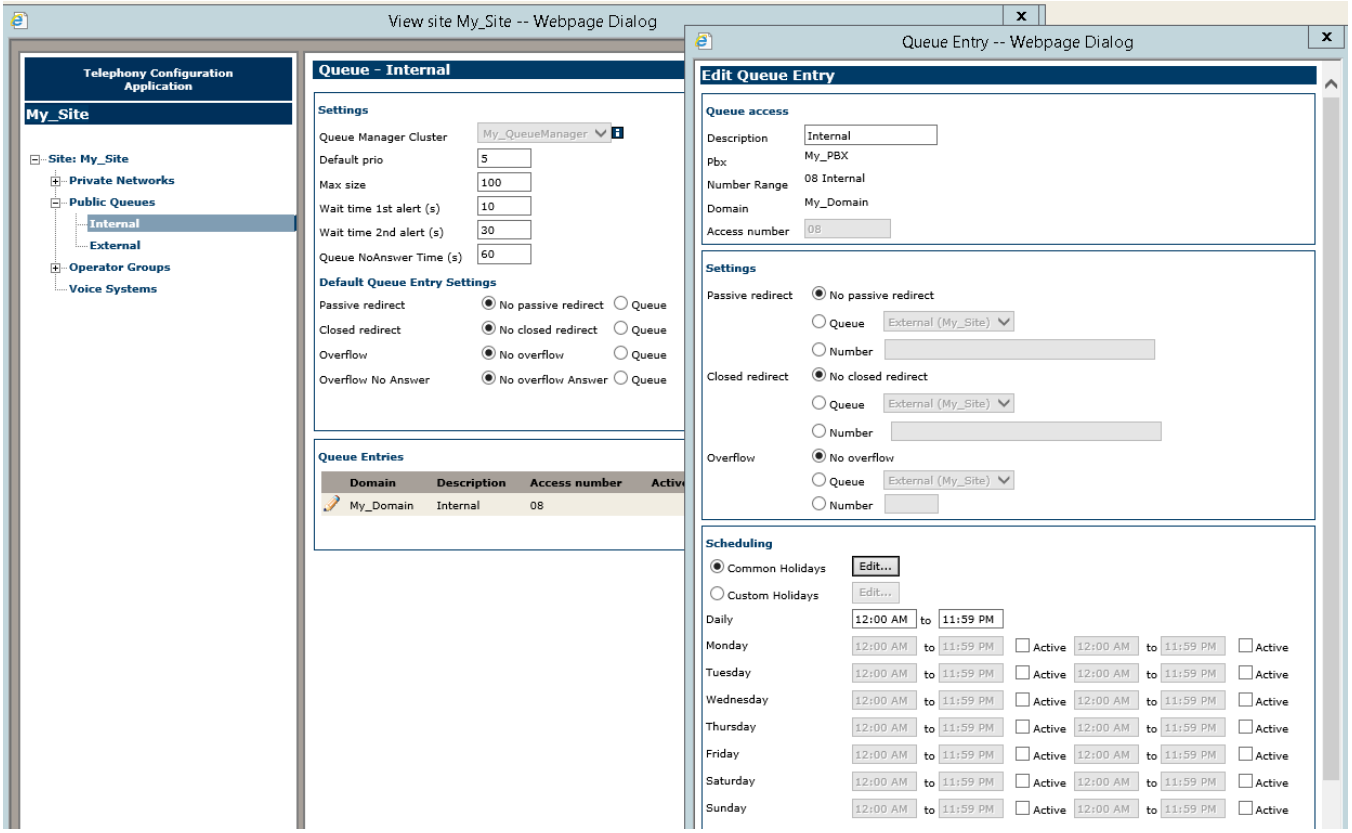
   The system deploys the selected configuration.
3. Click **Close** to exit the TCA.

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.



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.

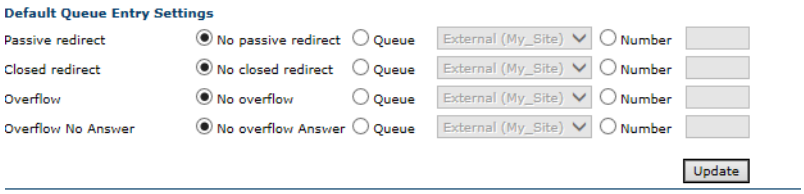
- When **No Overflow on no answer** is selected :

  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

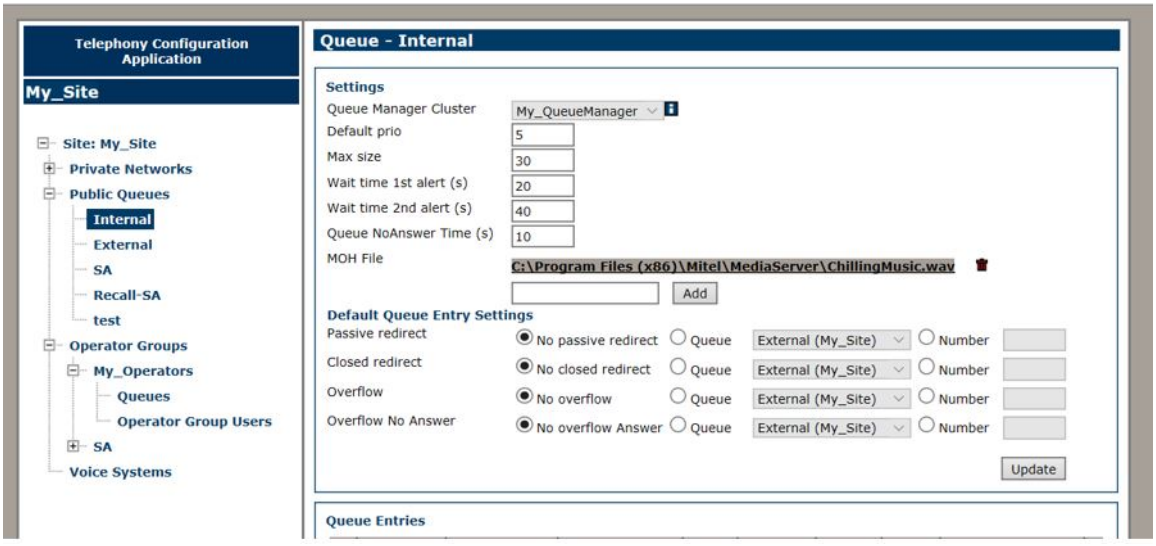
  An edit box is enabled and user can write the number to divert the call on "Overflow No Answer time" timeout.

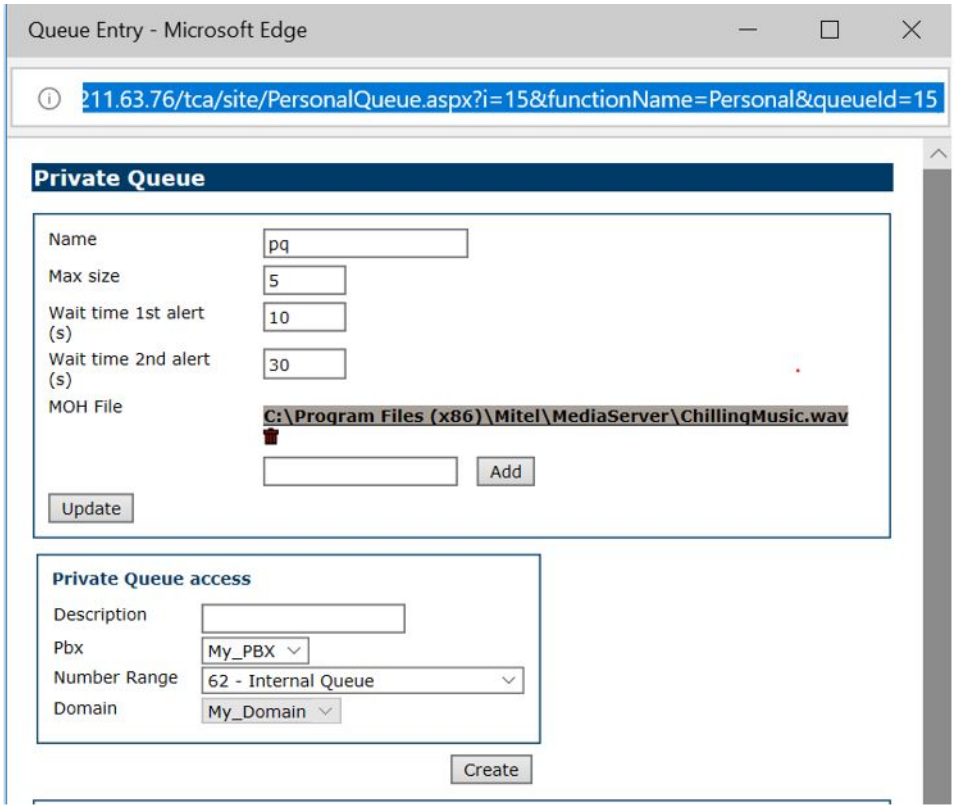
  The behavior is same as that of "Overflow" but not for recall queues.



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.




Queue Entry - Microsoft Edge
211.63.76/tca/site/PersonalQueue.aspx?i=15&functionName=Personal&queueId=15
Private Queue
Name
pq
Max size
5
Wait time 1st alert (s)
10
Wait time 2nd alert (s)
30
MOH File
C:\Program Files (x86)\Mitel\MediaServer\ChillingMusic.wav
Add
Update
Private Queue access
Description
Pbx
My_PBX
Number Range
62 - Internal Queue
Domain
My_Domain
Create

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).

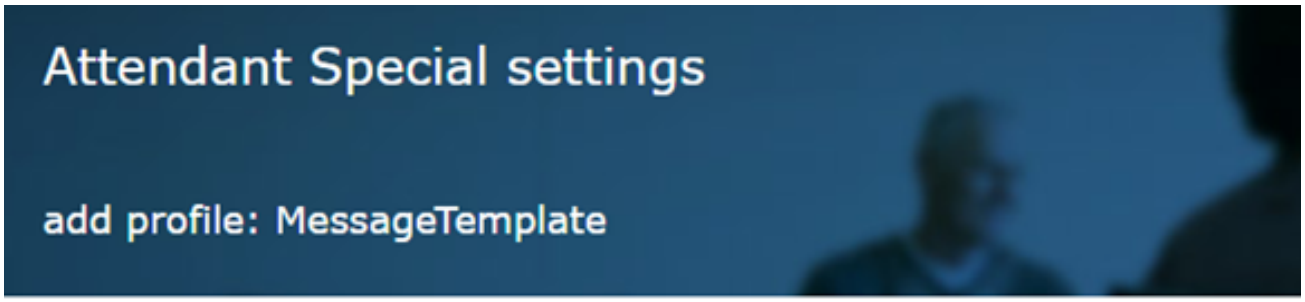
To add the CMG administrator to the operator group, do the following:

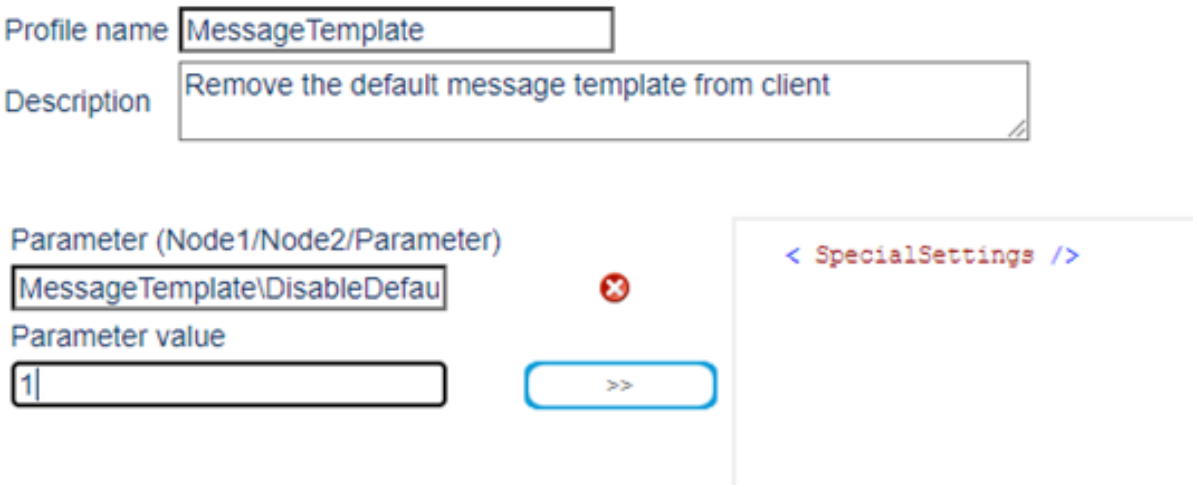
1. Log in to the TCA.
2. Open your TCA configuration and click on **Sites** in the left panel.

   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.
5. 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.

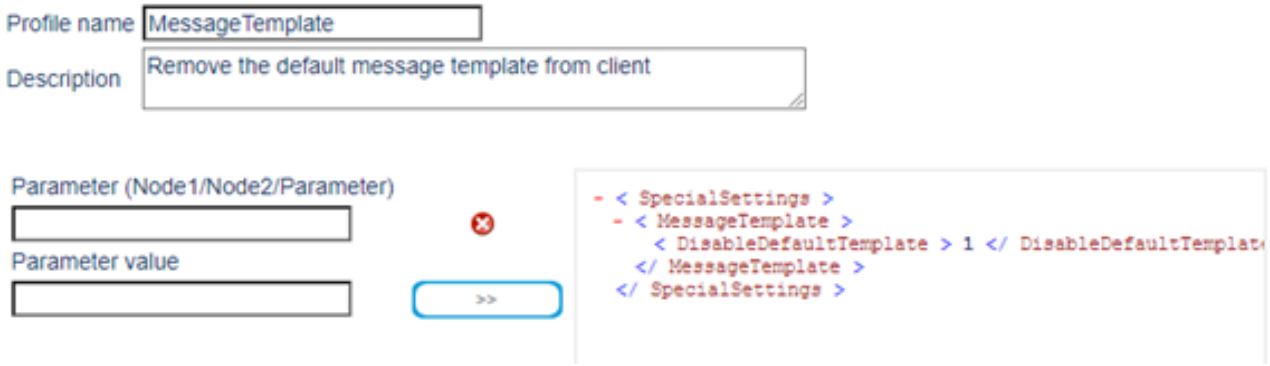




2. Add Attendant Special setting **Profile name** as **MessageTemplate**.
3. Add the **Parameter**:

   MessageTemplate/DisableDefaultTemplate
4. Add the **Parameter value** to 1.

5. Add **Profile name** and **Description** then click **Save**.



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.

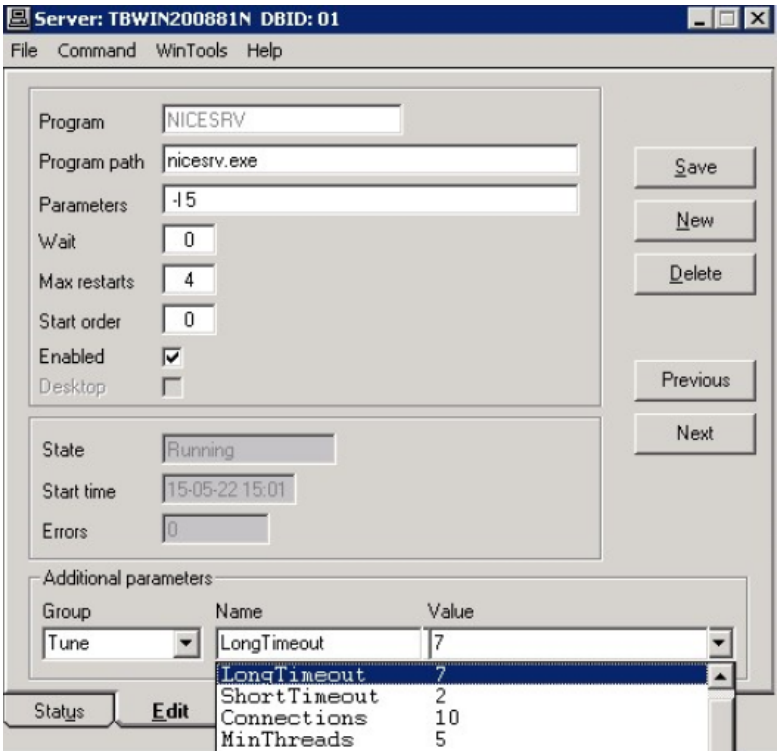
Optimizing Nicesrv

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:



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.

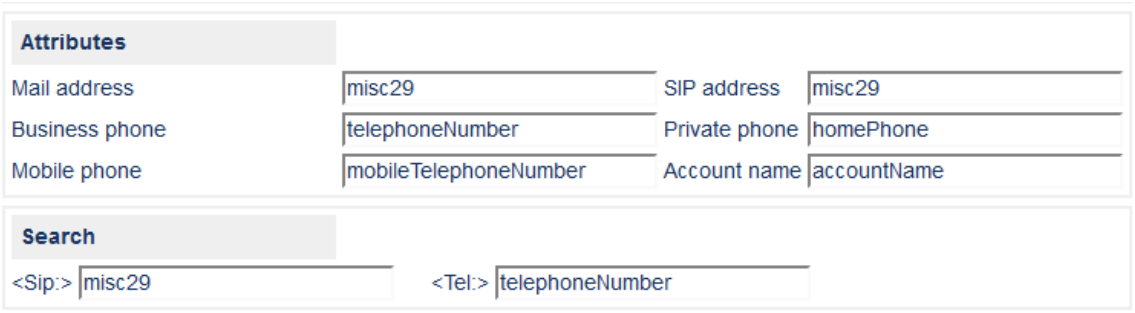
Prerequisite

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:

1. 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:



2. 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:

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