A MITEL
PRODUCT
GUIDE

Mitel InAttend

Administration and Maintenance Guide

Release 9.2

BOOK PART NUMBER: 2/1553-ANF 901 89 Uen
May 2025

Mitel
Powering connections

Notices

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), its affiliates, parents, or 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

Introduction 1

InAttend is a powerful, user-friendly attendant application designed for handling high volumes of internal and external calls in an efficient way. Call and activity handling, presence and availability with line status information are all integrated into one single application.

The Attendant Connectivity Server (ACS) is the Telephony server providing the telephony functionalities over IP. The InAttend client works in combination with ACS to provide an advanced attendant platform for the supported SIP enabled call managers. See InAttend Compatibility Matrix [3] for a list of the supported call managers.

Note:

The Compatibility Matrix document is available on Mitel PowerUp.

This document describes how to administer and maintain the InAttend system. To get an overview and better understanding of InAttend and ACS, refer to InAttend System Overview [1].

Backup and Restore 2

This chapter contains the following sections:

This section includes information on how to backup and apply the InAttend system configuration and database.

2.1 System Configuration

The InAttend telephony server configuration is performed from Telephony Configuration Application (TCA). Each time a new configuration is deployed, a new local backup file is created in the `C:\ProgramData\Netwise\NCLA\1.0\Configurations\backups` directory.

See InAttend Installation and Configuration Guide [2] for configuration steps.

2.1.1 Backup System Configuration

Always backup your system configuration when a change in configuration has been done. Do the following:

1. Make a copy of the following directory:`C:\ProgramData\Netwise\NCLA\1.0\`
2. Store the copy on a separate media.

2.1.2 Restore System Configuration

In the unlikely event of a system hardware crash, you can re-apply a backed up configuration file after a system reconstruction:

1. Make sure that the InAttend installation is complete.
2. Copy the backed up configuration to:

```
C:\ProgramData\Netwise\NCLA\1.0\
```

The configuration is now available for activation in TCA.

Note:

If problems occurs when activating a backed up configuration in a Windows Server 2008 environment, make sure that the IUSR user has read and write access to the configuration file.

2.2 System Database

The database is named AastraConfig in an InAttend 2.x installation.

Note:

If the system has been upgraded from InAttend 1.0, the database name is TsConfig.

2.2.1 Backup System Database

The backup procedure can be done during normal use of the InAttend Server. To perform a backup, do the following:

1. Open the **BluStar Server Administration** tool and select **Tools -> Database backup -> Database.**
2. Click on **Database backup active**and enter the file path and name of the backup file as well as a favored time to activate the backup function. You can also select how many backup files you want to have and if a backup of the log database AastraLog/TsLog should also be created.
3. To create an immediate backup, enter the favored path and name and click the button **Start backup** when finished.

In a new InAttend installation, the created backup file contains the SQL database <AastraConfig.mdf> and its transaction file <AastraConfig.ldf>.

If running on an upgraded InAttend system, the files are named<TsConfig.mdf> and <TsConfig.ldf>.

2.2.2 Restore System Database

After activated the automatic database backup, you can restore the different databases from this dialog. Do the following:

1. Select the favored backup file from the drop down box and load it by clicking**Read** . The backup database will be restored to a temporary database.
2. Select which kind of restore you want to do (complete database, links, users, profiles) and select the favored parts of the backup.

3. With **Restore data** the restore will be initiated (can take some seconds depending on the backup size)

2.2.3 Rename Server

In the **BluStar Server Administration** tool, there is an option for renaming the server when the configuration database is moved from an existing server to a new server. Perform the following steps to rename the server:

1. After restoring the database from the existing server to the new server, use the **Rename Server** option to rename the server. This will change the hostname in several places.
2. After renaming the server, log off from the **BluStar Server Administration** tool, log in again and check the server name/IP address in the following places:

    a. **User Configuration** > **Configuration Profiles** > **Attendant Directories**
    b. **User Configuration** > **Configuration Profiles** > **Attendant PBX**
    c. **Presence Server** > **Configuration** > **Linestate** > **Connection Data**
    d. **Presence Server** > **Configuration** > **Presence Interface**
3. Wherever the earlier hostname/IP addressvalue exists, change it to the new hostname/IP address in the above places.
4. After verification by the **BluStar Server Administration** tool, use **SQL Server Management Studio** to search for the **dbo.ServerData** table in the configuration database.
5. Change any earlier values in the columns for **ServerName** and **IPAddress** to the new values.

Administration 3

This section includes information on how to administer the InAttend server using the BluStar Server Administration tool (WebAdmin).

To start the BluStar Server Administration tool, enter the following address: `http://<servername>/webadmin`

where "<servername> is the name or the IP-address (IPv4/IPv6) of the InAttend server.

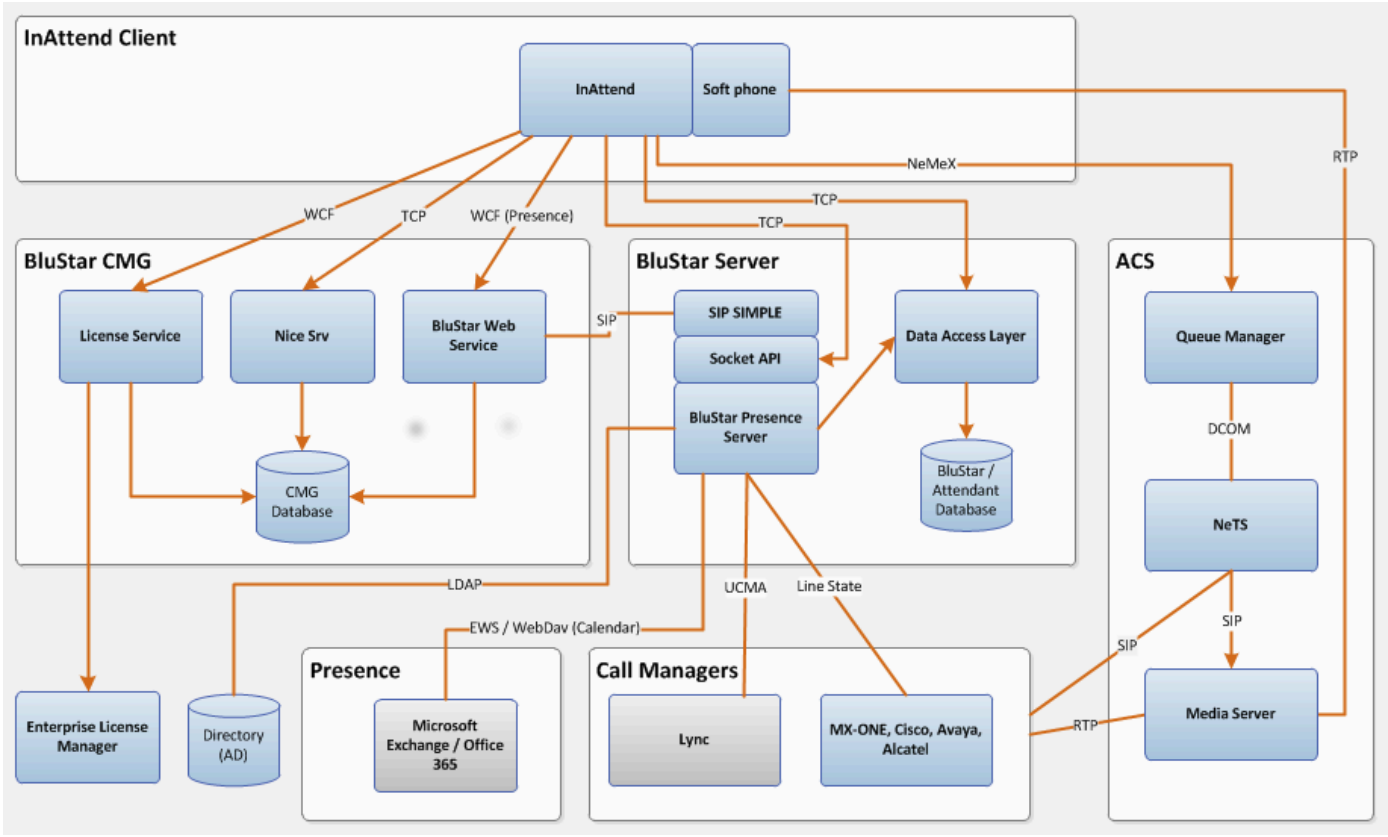
To login, use the following user ID and password:

- When using InAttend with CMG Server, the default user ID is niceadmin and the password is set during installation.
- When using InAttend with BluStar Server, the default user ID is admin and the default password is Aastra123 .

For new installation of BluStar Server 3.2 (or higher) the default password is Mitel123 .

The next sections describe the different parts of BluStar Server Administration that are used for administration of the InAttend Server.

InAttend Architecture 4



For more information on the architecture, see InAttend System Overview [1].

Logging 5

This chapter contains the following sections:

All components in InAttend 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 BluStar Web Service can reach 900 MB in size each.

5.1 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 behavior.
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.

5.2 Configuring Log Files for each Component

This section describes how to configure and 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\...
```

5.2.1 BluStar License Manager

The default log directory for BluStar License Manager is:

```
C:\Program Files (x86)\Mitel\BluStarLicensemanager\
```

5.2.2 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
```

```
C:\Program Files (x86)\Mitel\BluStar Server\PresenceServer\logs
```

5.2.3 BluStar Web and BluStar Web Service

The default log directories for BSW Web respective BSW Service are:

```
C:\ProgramData\Mitel\BluStarWeb.Web\
```

```
C:\ProgramData\Mitel\BluStarWeb.Service
```

Change of log level (1-7, default 3) for Blustar Web Service:

```
C:\Program Files (x86)\Mitel\BluStarWebService\BluStarWebServiceConfig.xml
```

5.2.4 Enterprise License Manager (Server and Client)

The default log directory for ELM server and client is:

```
C:\Program Files (x86)\Mitel\License Manager\log
```

5.2.5 InAttend Client

Log levels and directory are configured in the Attendant System Configuration tool

The default log directory for the InAttend client log files is:

```
%LocalAppData%\Mitel\Attendant
```

5.2.6 InAttend History Service

The default log directory for InAttend History Service is:

```
C:\ProgramData\Mitel\InAttendHistoryService\
```

To change the log path settings for the InAttend History Service:

1. **Locate the Configuration File**
   - Navigate to the installation directory of the InAttend History Service, typically:

     ```
     C:\Program Files (x86)\Mitel\InAttendHistoryService\
     ```
   - Find the **AttendantHistoryServiceConfig.xml** file in this directory.
2. **Modify the Log Path Setting**
   - Open **AttendantHistoryServiceConfig.xml**.
   - Locate the **<LogPath>** section within the file. By default, this section is commented out:

     ```
     <!--<LogPath></LogPath>-->
     ```
   - Uncomment this line and specify your desired log file path. For example:

     ```
     <LogPath>D:\Logs\InAttendHistoryService\</LogPath>
     ```
   - Save the changes.
3. **Restart the InAttend History Service**.

5.2.7 InAttend Quick Configuration Service

The default log directory for InAttend Quick Configuration Service is:

```
C:\inetpub\wwwroot\AttendantConfigurationWeb\
```

5.2.8 InAttend Quick Configuration Web

The default log directory for InAttend Quick Configuration Web is:

```
C:\ProgramData\Mitel\AttendantConfig.Web\
```

5.2.9 Line State Servers

Use the line state server's configuration tool to configure the logging. Specify the logging path, a log filter level, the maximum size of log files, and for how many days to keep logs.

5.2.9.1 ACS Cisco LSS

When connecting InAttend to Cisco Call Manager the ACS Cisco Line State Server is used. Log levels and directory are configured in the ACS Cisco LSS configuration tool.

The default log directory for ACS Cisco LSS log files is:

```
C:\ProgramData\Mitel\AcsCiscoLSS\
```

5.2.9.2 CTI Server

The default log directory for MX-ONE CSTA 3 (from WEBAdmin, Traceconfig.exe):

```
C:\Program Files (x86)\Mitel\BluStar Server\Trace
```

Example log:

```
C:\Program Files (x86)\Mitel\BluStar Server\Trace\Trace_SERVERNAME.txt
```

5.2.10 Media Server

Log levels and directory are configured in the MediaServer Configuration tool.

The default log directory for Media Server log files is:

```
C:\Program Files (x86)\Mitel\MediaServer\Logs
```

5.2.11 Mobile Status Connection and Web Proxy

The default log directories for Mobile Status Connection and Web Proxy are:

```
C:\ProgramData\Aastra\MobileStatusConnection\Service
```

```
C:\ProgramData\Aastra\MobileStatusConnection\Proxy
```

5.2.12 Network Telephony Services (NeTS)

Use the NeTS configuration tool to configure the logging for NeTS.

The default log directory for NeTs log files is:

```
C:\Program Files (x86)\Mitel\TelephonyServices\Logs\NeTS
```

5.2.13 Quality Manager

The default log directory for Quality Manager log files is:

```
C:\Program Files (x86)\Mitel\QualityManager\Logs
```

5.2.14 Queue Manager

Use the NeTS configuration tool to configure the logging for Queue Manager.

The default log directory for Queue Manager log files is:

```
C:\Program Files (x86)\Mitel\QueueManager\Logs\QueueManager
```

5.2.15 Telephony Configuration Agent (TCA)

When deploying a configuration in TCA, the configuration agent receives the NCLA configurations and stores them in the directory:

```
C:\ProgramData\Netwise\NCLA\1.0
```

To change the log settings for CfgAgent:

1. In the registry, find `HKEY_LOCAL_MACHINE\SOFTWARE\Netwise\CfgAgent\Log`
2. Right-click on **LogDetailLevel** and select **Modify**.
3. Change the log level by entering a new number in the **Value data** field.

The default log directory for Telephony Configuration Agent log files is:

```
C:\ProgramData\Mitel\CfgAgent\Logs
```

5.2.16 Telephony Configuration Service (TCS)

The default log directory for Telephony Configuration Service log files is:

```
C:\Logs\TCS_YYMMDD.log
```

Troubleshooting 6

This chapter contains the following sections:

This section describes what kind of information that is useful and should be kept ready when troubleshooting the InAttend Server applications.

6.1 Check Line State Server(s)

This view gives a survey of the telephone extensions for which the line state server has started a monitor. This information indicates whether a particular monitor is permanently configured, or is currently started. It also identifies the call manager (PBX) link the monitor was started on. The total number of permanently and currently started monitors is displayed.

Note:

These numbers are important, especially when you are using a call manager telephony system with limited monitor counts. If you cannot start a new monitor on the call manager, the monitor count or the number of licenses on the call manager has probably exceeded. In this view, you can check the number of started monitors.

All telephone extensions for which a monitor has been started are shown in this list. In the normal case, all monitors are started when they are needed and stopped if they are no longer required. For performance reasons, some monitors may be started permanently. These monitors are always started.

The Monitor list is automatically sorted by extension numbers, by the line state server. By clicking on another column header, the administrator can change this default sort type to another sort based on the selected column.

You can start and stop permanent and non-permanent Monitors by using the buttons **Add Monitor** and **Remove Monitor**. Select a telephony link for the monitor.

The different monitor states are:

	Monitor is started (green)
	Out of service (yellow)
	Monitor is stopped (red)

Note:

If the database connection goes down, the line state information in the A/B fields and search result list in the InAttend client is lost and the line state information in the Busy Lamp Field becomes unreliable.

6.2 Check Call Manager Link(s)

The “PBX Link” view displays all configured links to various telephony servers and call managers (PBXs).

The individual links can be started and stopped in this view and the link settings can be changed. It is also possible to add or delete a link. Time for starting / stopping a link depends on the number of monitors to be started / stopped.

Changes to existing links can be made by using the same dialog as the one for adding a new link. The different link states are:

	Link is up (green)
	Link is initialising (yellow)
	Link is down (red)
	Link state unknown

6.3 Check CSTA Messages

This CSTA Messages view shows the messages being exchanged between the line state server and the telephony server (or the call manager itself).

The list contains all messages that the line state server has received for the monitor points set on the telephony server, or call manager. Each message is displayed on a single line. The line state server translates the raw message data into readable text.

The exact meaning of the various CSTA messages can be drawn from the industry standard specification documents for the ECMA 179 and ECMA 217 standards. The main purpose of this view is to check the messages coming from the call manager.

6.4 Check Server Messages

This view contains messages regarding the actions carried out by the server and their status. The page can be refreshed automatically using the check box “Automatic refresh view”. The messages are refreshed every 5 seconds.

The upper part of the window shows information regarding the current uptime of the server and the software version number.

6.5 Check Service States

You can start and stop the single services of the InAttend Server on a server from the BluStar Server Administration tool. Therefore, the Service Manager (`TsServiceManager.exe`) must be installed as a service and running on the server.

The different service states are:

	Service is running (green)
	Service is starting (yellow)
	Service is stopped (red)
	Service is stopping (orange)
	Service is disabled (black)

6.6 Enterprise License Manager (ELM)

The ELM setup contains software for both Server and Client (if required).

6.6.1 ELM Client Installation

Note:

If BluStar License Manager and ELM Server are installed on separate servers, the ELM Client must be installed on the same server as BluStar License Manager.

6.6.2 ELM Server Installation

When installing ELM on a Windows 2012 R2 server, the following error may occur:

To correct this error, make sure that the following boxes are checked in **Windows 2012 Server Manager -> Manage -> Add Roles and Features -> Web Server -> Management Tools**

If the error remains, please contact the Mitel Support.

6.7 Exchange, Lotus Notes and GroupWise

If a Mitel product encounters problems on caller identification or journaling, the existing database configurations should be deactivated successively in BluStar Server Administration to find out which configuration caused the problems. After finding such a database connection, all its configuration settings should be checked thoroughly.

You can change search method, search prefix, and search index settings for more information indicating the cause of the failure. For further analysis, a client trace tool should be activated as described below. Note that caller identification is only performed by the client software and not by the server software.

6.8 Microsoft ODBC Drivers

For problems connecting a database through ODBC drivers, verify the connection parameters using MS Query (`MSQRY32.EXE`) from MS Office.

MS Query makes it possible to access the database through ODBC and see the structure of tables, available views and field names. For advanced troubleshooting, tracing can be activated within Windows ODBC configuration.

Default update intervals:

- **Server** - The Server checks for updates in the update folder at startup and every 60 minutes thereafter.
- **Client**- The client checks for updates at startup and every 15 hours thereafter.

Please refer to the Microsoft documentation for details.

6.9 Microsoft Windows Server OS

There is no particular method for tracing the communication between Mitel products and the Windows Server operating system (OS) using only one specific trace tool. However, it is possible to activate product specific tracing, as described in this document.

6.10 Mitel LDAP Connections

For problems related to multiple database connections, disconnect one database at a time to isolate the faulty connection. Once the issue is resolved, it is likely that the issue originated with the most recently deactivated database.

For analyzing problems on LDAP connections, it is recommended to use the Mitel test tool FIRSTLDAP or a 3rd party LDAP browser. FIRSTLDAP operates in the same way as LDAP search on other Mitel products, so that you can apply FIRSTLDAP test results to the data base interface of any Mitel product.

When troubleshooting LDAP connections due to unknown or wrong connection parameters (LDAP server address, TCP port, search base, login, field attributes), use a 3rd party LDAP browser, which provides a view into the LDAP directory structure and even field data.

6.11 Telephony Configuration Application (TCA)

TCA is an ASP.NET web tool. If experiencing connection problems to the TCA web server, please log on to the web server locally and try to connect.

6.11.1 Deploy Transmission Failure

The deployment automates distribution of configuration XML files to the hybrid components. If experiencing transmission difficulties when deploying, the configuration file can be distributed manually.

1. In TCA, navigate to the **Configurations** page (the first page after you login). The Configuration page displays all configuration files.
2. Save the desired configuration file (by right-clicking on it and choosing **Save Target As**).
3. For each target computer, find the Attendant Connectivity Server configuration destination path by starting Regedit.exe and find the registry keyHKEY_LOCAL_MACHINE\SOFTWARE\Netwise \Configurations\NCLAConfigurationPath.

   The value of this key indicates the path and the filename of the configuration at the target computer.
4. Save the configuration file to disk and rename it to the name in the registry (step 3).

Note:

It is important that the same configuration file is copied to all computers with ACS components. These computers are: CMG Server, NeTS and Queue Manager.

6.12 WebAdmin – Update Status Page

Clients report their update actions to the update status page in the BluStar Server Administration tool (WebAdmin). The table can be filtered by message type (critical, error, message):

- Critical messages should be investigated as soon as possible.A critical message indicates that the client could not recover from a failed update attempt. Some files might be missing or not updated.
- Error messages indicate problems during the update.An error message indicates that the client could not be updated; all client files are untouched and not changed or updated.
- Messages inform on the update progress (e.g., that the update was installed successfully or that the client will be updated after restart).

Technical Assistance 7

Mitel provides www.mitel.com as a starting point for technical assistance regarding all products, including the CMG application suite. From here, partners can obtain online documentation, FAQs, latest software updates and request further technical assistance.

References 8

[1]InAttend System Overview

[2]InAttend Installation and Configuration Guide

[3]InAttend Compatibility Matrix (Note: Available on Mitel PowerUp)