A MITEL
PRODUCT
GUIDE

Mitel InAttend and CMG

Security Guidelines

Release 9.3

November 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

Overview 1

This document provides an overview of the security mechanisms used to protect the Mitel InAttend and Collaboration Management (CMG) solutions from network threats and maintain user data privacy. It will be of interest to personnel responsible for ensuring the secure deployment and operation of the Mitel InAttend and CMG.

Every organization should have a clearly defined IT security policy that defines goals, assets, trust levels, processes, incident handling procedures, etc. This policy should cover and configure the security mechanisms available in the Mitel InAttend and CMG solutions.

Security is an integral part of the Mitel InAttend and CMG system design. This document describes the security features of these systems and provides recommendations on how the administrator should configure them to ensure a secure deployment.

The Mitel InAttend and CMG security features are either enabled in the system by default, enabled during the installation/configuration phase of the system, or need to be enabled manually by the system administrator when the Mitel InAttend and CMG system is initialized.

The Mitel InAttend and CMG security measures are mainly based on the following open standard technologies and access management mechanisms:

- TLS – Transport Layer Security (TLS) 1.3 provides secure administration access and secure signaling between InAttend clients and the InAttend Server(s). The Transport Layer Security (TLS) provides secure web access to Mitel InAttend and CMG.
- SRTP – Secure Real-time Transport Protocol (SRTP) protects the voice media streams between IP phones and between IP phones and call managers.
- LDAPS – Secure LDAP is used for connectivity to LDAP Servers
- OAuth2.0 (Open Authorization) - The authentication protocol for Calendar Integration with Office365 can be the Open Standard for Authentication 2.0 (OAuth 2.0) or the Basic Authentication protocol.
- Advanced security features, including forced password changes, expiration policies, and password complexity requirements, are available for user authentication and password management.

Other mechanisms that can be employed to protect the Mitel InAttend and CMG are based on the following:

- A securely designed corporate Local Area Network (LAN) infrastructure
- Configuration of internal and external public-facing routers and firewalls

In addition to the security recommendations described in this document, the system administrator and/or the Information Technology (IT) security officer should address a number of general security aspects.

An important security measure is to establish and maintain physical security. Only authorized personnel should have access to server locations since many data-exposure attacks can be mounted by having physical access to a host. Further, the IT data infrastructure should be designed with security in mind, security mechanisms, and protocols should be enabled, and all components of the whole system should be correctly configured, maintained, and updated as necessary.

About the Mitel InAttend and CMG Documentation Set

2

This chapter contains the following sections:

The Mitel Document Center website (https://www.mitel.com/document-center) offers documents for Mitel InAttend, Collaboration Management, and other Mitel® products. The documentation set is available in PDF format that can be viewed and downloaded using an Internet browser.

The following documents provide the complete information about the Mitel InAttend and CMG:

- *CMG Installation Guide, InAttend Installation and Configuration Guide*: describes the installation, upgrade, maintenance, and troubleshooting instructions.
- *InAttend and CMG Solution Engineering Guide*: describes the hardware specifications.
- *InAttend User Guide*: provides the procedure for configuring the InAttend.
- *CMG Web User Manual*: provides the procedure for configuring the CMG Web.
- *CMG Speech Attendant User Guide*: provides the procedure for configuring the CMG Speech Attendant.
- *Virtual Reception Installation and Configuration Guide*: provides the procedure for configuring the Virtual Reception.
- *InAttend System Overview, CMG System Overview*: describes the general product overview, including deployments, architecture, products, and features.
- *Virtual Reception System Overview*: describes the general product overview, including deployments, architecture, products, and features.

Additional guides and help systems are available that contain instructions on how to configure and use the individual Mitel applications supported on Mitel InAttend and CMG.

To access the Mitel InAttend and CMG product documentation set: Mitel InAttend and Collaboration Management.

The following document discusses security and toll fraud prevention:

- Security Toll Fraud and Installation Checklist - EM004472

The following documents are available in the Mitel Document Center to address network and product security:

- Mitel Technical Paper - Intrusion Detection and Prevention Systems
- Mitel Technical Paper - Securing Mitel Cloud-Based Unified Communications

2.1 Additional Security Related Documentation

The End User Security Related Documentation are:

- *InAttend Installation and Configuration Guide*
- *CMG Configuration Guide*
- *InAttend Administration and Maintenance Guide*

2.2 What is New in this Release

The following security enhancements are included in Release 9.3:

- **CMG Virtual Reception: Google ASR/TTS Integration**

To address the upcoming end of support for Nuance ASR and TTS (June 2026), CMG Virtual Reception introduces support for Google Cloud Text-to-Speech (TTS) and Automatic Speech Recognition (ASR).

The integration uses the existing MRCP interface and a local Google Backend service that connects CMG Virtual Reception to Google Cloud for speech processing.

In this release, the local connection between CMG Virtual Reception and Google Backend uses HTTP (port 9002) and is intended to operate inside a trusted internal network. Communication between Google Backend and Google Cloud uses encrypted HTTPS channels to protect voice and text data during transmission.

Reference:

- *Virtual Reception Installation and Configuration Guide* > Steps to Follow Post VR Package Installation.
- *Virtual Reception Installation Preparation Guide* > Google Cloud Dialogflow Account creation.

- **Federated Authentication for CMG Web using Keycloak and Azure AD**

This release introduces support for secure authentication to CMG Web through OpenID Connect (OIDC) via Keycloak. Keycloak serves as an OpenID Connect (OIDC) Identity Provider for CMG Web, brokering authentication from Azure Active Directory (Azure AD) using SAML 2.0. This enhancement strengthens federated authentication by enabling centralized identity and access management through Azure AD. It allows organizations to extend existing Azure AD Single Sign-On (SSO) and Multi-Factor Authentication (MFA) policies seamlessly to CMG Web.

Reference:

- *CMG Configuration Guide* > Configuring CMG Web for Keycloak OpenID Connect Integration (Azure AD as SAML Broker).

System Architecture 3

This chapter contains the following sections:

3.1 InAttend Server Architecture Overview

InAttend is a powerful, user-friendly attendant application designed to efficiently handle high volumes of internal and external calls. Call and activity handling, presence and availability, and line status information are all integrated into one single application.

InAttend can be installed as a stand-alone solution or combined with CMG - BluStar Web:

- **InAttend stand-alone**- Any LDAP directory can be used for directory information in this scenario. 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 - BluStar Web users' extensions according to the different activities that have been set for each user.
- The **Attendant Connectivity Server** (ACS) is the Telephony server that provides telephony functionalities over IP. The InAttend client works in combination with ACS to provide an advanced attendant platform for supported SIP-enabled call managers.

  The InAttend Hard Phone support allows the attendant to use a standard desk phone for media as an alternative to the built-in Soft Phone capabilities.

InAttend can be deployed on industry-standard servers or in a virtualized computing environment.

The InAttend Server connects to call managers, groupware systems, and presence systems over TCP/IP as shown in the following figure. At start-up, the client application announces itself to the TCP/IP interface of the InAttend Server. When the client announces itself, it is authenticated by verifying the client's credentials. The client then receives information about the presence status of the monitored users over this connection.

The InAttend call control functionality uses open SIP standards and integrates with call managers using a SIP trunk. InAttend also supports TLS and SRTP.

The system architecture supports both IPv4 and IPv6 network configurations, enabling flexible deployment in modern IT infrastructure.

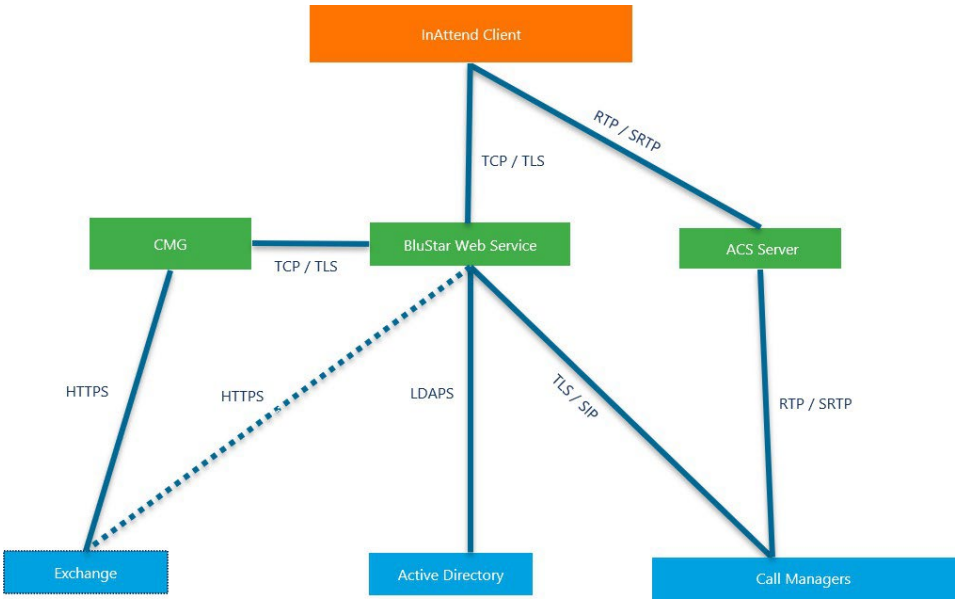

Figure 1: InAttend Server Architecture

Additional details on InAttend Server Architecture are available in the InAttend System Overview.

3.2 CMG Web Architecture Overview

Collaboration Management (CMG) is a collaboration and presence management suite that enables business users to manage their daily communication.

The CMG suite includes the CMG Web component, which enables business users to manage their activities. With the CMG website, users can perform “smart-search” directory services, use click-to-dial, set an activity timeline, and manage call-routing preferences based on the calendar/activities.

Integration with the BluStar Server (BSS) enables users to see, in real-time, their colleagues’ rich presence information, including CMG Web user presence status, calendar activity, and call manager line state from all available sources provided by the BluStar Server.

The CMG Web Server can be deployed on industry-standard servers or in a virtualized computing environment and can be accessed from desktop and mobile web browsers. CMG Web uses the CMG Server and, optionally, a BluStar Server as backend servers.

The following shows the connections between the different clients and the CMG website.

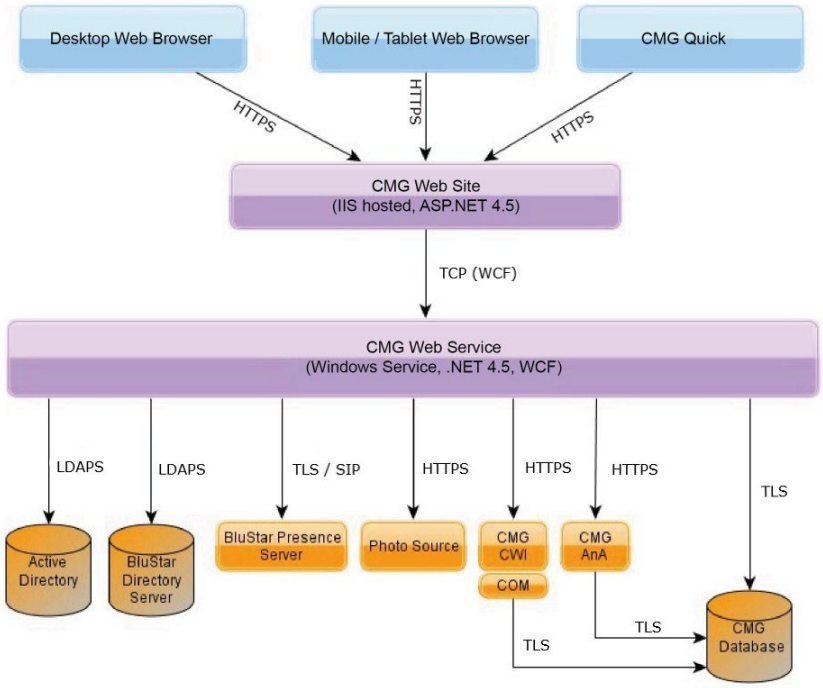

Figure 2: CMG Web Architecture

The following web services, shown in Figure 2: CMG Web Architecture on page 6, are used for communication between the CMG applications:

- **AnA Web Service** - used to check that the user is authorized to use a certain service when logging into the CMG server.
- **User Information Service (CWI)** - used by the applications to retrieve information from CMG Server.
- **Activity Service (CWI)** - used by CMG Web for activity registration.

External web, desktop, and mobile connections are recommended to terminate on a BluStar Web server placed in the customer-provided DMZ, as shown in the following figure.

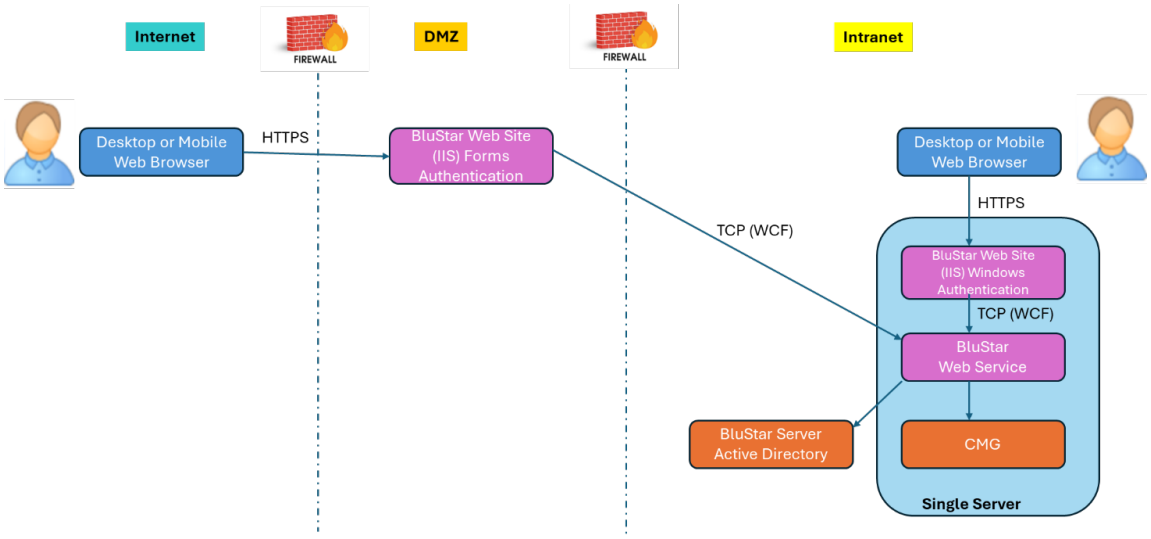

Figure 3: CMG Web Architecture with DMZ and Authentication Layers

Additional details on CMG Web Architecture are available in the CMG System Overview.

Security Overview 4

Mitel InAttend and CMG have been designed in accordance with Mitel's Secure Development Life Cycle (MiSDLC). For further details see the section called Secure Development Life Cycle in this document.

Mitel InAttend and CMG include security features that address identity, authentication, encryption, access and authorization. And they support audit trails, logs and use of enterprise security certificates.

The Mitel InAttend and CMG security features are configured via various management forms which are accessed using the Mitel InAttend and CMG System Administration Tool. The Mitel InAttend and CMG System Administration Tool contains embedded help files with extensive search capabilities that will assist the administrator with forms configuration. The help files also contain documents that discuss maintenance procedures.

With IPv6 support, all security protocols including TLS 1.3, SRTP, and LDAPS are applicable over both IPv4 and IPv6 networks, ensuring consistent protection regardless of IP version

OpenID Connect (OIDC) Integration via Keycloak

CMG Web now supports authentication using OpenID Connect (OIDC) with Keycloak as the Identity Provider. In this setup, Keycloak serves as a broker between CMG Web and Azure AD, providing secure user authentication. This configuration ensures that CMG Web does not handle user credentials directly, improving overall security.

Key Security Benefits:

- Federated authentication using SAML 2.0 to OIDC bridging.
- End-to-end TLS 1.3 encryption between CMG Web and Keycloak.
- Centralized user access control with Azure AD policies and MFA.
- Simplified user management and reduced password handling risks.

Securing the Operating System 5

This chapter contains the following sections:

5.1 Operating System Overview

Mitel InAttend and CMG software is installed on top of a Microsoft Windows Server operating system. The supported versions include Windows Server 2016, 2019, and 2022.

The Microsoft Windows Server operating system offers a range of built-in security features that help safeguard the system from unauthorized access and attacks.

The Microsoft Windows Server environment requires specific configuration to enhance security and functionality involving several recommendations to protect it from vulnerabilities and attacks. These include:

- Applying Security Patches: Ensuring that the operating system is kept up to date with the latest security patches and updates to protect against vulnerabilities.
- User Account Control (UAC): Disabling of UAC to prevent unauthorized changes. Refer to Microsoft documentation.
- Anti-malware: Use of Windows Defender or a third-party antivirus. Refer to product documentation for the recommended folder exclusions.
- Enabling Firewall: Configure firewalls to restrict unauthorized access. Refer to product documentation for the port usage.
- Role-Based Access Control (RBAC): Limit access to the operating system by enforcing role-based permissions.
- Encryption: Use BitLocker for encrypting the hard drive to protect data at rest.
- Encrypting File System (EFS) is also supported.

By adhering to these recommendations for the CMG environment a secure configuration minimizing potential vulnerabilities and ensuring optimal performance is maintained.

The above measures are based on well-known security best practices. In general, a platform that is both physically secure and installed in network that has been securely designed will have a lower likelihood of being infected compared to a platform that lacks physical security and/or is installed in a network lacking security controls.

5.2 Use of Antivirus Software

InAttend and CMG are deployed on Microsoft Operating systems. A customer may implement their own preferred anti-malware solution. However, the following trace folders should be excluded from local virus scanning due to performance issues:

- If Attendant Server Services are installed on the same server as CMG Server: `<path>\nicesrv`
- For BluStar Server: `<path>\BluStar Server`
- For Calendar Connection (if installed): `<path>\Calendar Connection`

Mitel cannot guarantee that third-party antivirus software will not affect the performance of the application, and Mitel does not offer any endorsements of antivirus software vendors or evaluate particular antivirus products. Consequently, anti-malware software may also require additional server resources to be allocated to accommodate performance differences.

If the customer requires technical support from Mitel related to a system with antivirus software installed, Mitel may require that the software be removed before Mitel can start troubleshooting the problem.

5.3 Software Patch Management Policy

The administrator must ensure that the Mitel InAttend and CMG are always updated and equipped with all critical patches to guarantee the highest level of security. Mitel has developed best practices for the management and installation of security patches released by operating system vendors, aiming to guarantee the highest level of security and the correct functioning of the system.

In addition, the Microsoft Operating system must be kept up to date.

5.4 Operating System Related Network Controls

Mitel recommends implementation of TLS for administration and client signaling to defend against interception of usernames and passwords. Access to the management interface requires a use name and password.

Administrator access can be restricted to certain IP addresses or subnets, and only secure-based web connections from permitted IP addresses can be accepted using network controls to minimize network access.

A default self-signed TLS certificate is provided with the server at no additional cost, but for additional security, customers are recommended to provide their own certificate

Firewall Configuration

Details on the ports used for firewall configuration are available in the following documents:

- *InAttend Installation Preparation Guide* > Firewall Ports section
- *CMG Installation Preparation Guide* > Firewall Ports section

TLS 1.3 support on Windows Server

Details on Configuring TLS 1.3 are available in the following documents:

- *InAttend Installation Preparation Guide* > Configuring TLS 1.3 support on Windows Server section
- *CMG Installation Preparation Guide* > Configuring TLS 1.3 support on Windows Server section

Note:
TLS 1.3 requires the use of Microsoft Windows 11 and Windows Server 2022.

Network Segmentation for Enhanced Security

A customer can further limit access over the network by implementing standard network security techniques, including Virtual Local Area Networks (VLANs), Access Control Lists (ACLs), and firewalls. These measures help isolate different network segments to reduce the risk of unauthorized access to sensitive data or services.

In all cases, physical access to systems should be restricted by the customer.

5.5 Securing Operating System User Interfaces

Access to the system is restricted to authorized users through username/password login combinations, with support for local and Active Directory (AD) authentication support. Passwords must adhere to the customer's strong password policy.

The Windows OS enforces strong password policies through Group Policy settings, ensuring that passwords meet length, complexity, and periodic expiration requirements to maintain security.

All communications with the system are performed over authenticated, encrypted channels using HTTPS (TLS), ensuring data security during transmission.

Customers can also secure network access using standard network security techniques, such as VLANs, Access Control Lists (ACLs), and firewalls.

In all cases, the customer should restrict physical access to the systems to prevent unauthorized access.

Google Service Account Key Protection

The Google Backend used by CMG Virtual Reception requires a Google Cloud service account key file. Download this key file from the Google Cloud Console, rename it to **speechattendant.json**, and place it in the following directory:

C:\Program Files (x86)\Mitel\GoogleBackend\speechattendant.json

This key file must be protected using NTFS file permissions so that only authorized service accounts and administrators can read it. To safeguard credentials at rest, encrypt the folder or volume using **BitLocker** or **EFS**.

Reference:

- *Virtual Reception Installation Preparation Guide* > Google Cloud Dialogflow Account Creation.

5.6 Hard Drive and Mass Storage Systems

Disk space

Details on Disk space are available in the following document:

- *InAttend and CMG Solution Engineering Guide* > Disk space section

Data Protection

Information that resides in InAttend and CMG is password protected. The data backups can be stored as encrypted files using Microsoft EFS to protect against unauthorized data access and as protection of stored user data at rest. Data can be manually removed from the database if it is not used.

The call recordings of the calls handled by the attendant are stored in an encrypted format on the media server. Each call can be identified, retrieved, and deleted by an authorized system administrator using standard Windows file manager processes if required.

The call recordings stored on the media server are encrypted using AES (Advanced Encryption Standard) with key lengths of 128, 192, or 256 bits.

- *InAttend Install and Configuration Guide* > Configuring the Media Server section

Configuring EFS

Encrypting File System (EFS) is a feature that provides file system-level encryption. It is recommended to enable EFS in the folders where the application log, trace files, and database backups are stored. This will help prevent unauthorized access.

Details on securing log locations, CDRs, and recordings are available in the following documents:

- *InAttend Install and Configuration Guide* > Configuring EFS section
- *CMG Configuration Guide* > Configuring EFS section

Refer to Microsoft documentation for assistance in enabling EFS in the operating system.

Note:
Customers may also enable Bitlocker for full disk encryption (FDE).

Hard drive space for Logging

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 the number of days) for the logging.

Details on Logs and Log's Management are in the following documents:

- *InAttend Administration and Maintenance Guide* > Logging section
- *CMG Configuration Guide* > Logging section

5.7 Securing Databases

1. **Regular Backups**: Perform frequent backups and store them securely, ensuring they are protected from unauthorized access.

2. **Access Control**: Limit database access based on user roles, providing the least privilege necessary for each role. Access control to the database is achieved by assigning appropriate roles to users, such as replacing excessive privileges like sysadmin with more restrictive roles like db_owner. This ensures users have the least privileges necessary for their tasks. SQL admin rights can be lowered through scripts, and further restrictions can be applied using IIS Manager settings.

   For detailed instructions, refer to **Section 9.4.3** in *CMG Installation Guide*, which explains how to lower SQL database admin rights. **Regular Updates**: Keep your database management system and any associated software up to date to protect against vulnerabilities.
3. **Encrypt Data**: Implement encryption for both data at rest and in transit to protect sensitive information

   SQL Server editions

   Multiple components within the InAttend and CMG solutions use Microsoft SQL Server. The solution supports both Microsoft SQL Server Express (for some configurations) and all the full editions of Microsoft SQL Server.

   Details on SQL Server editions are in the following document:

   - *InAttend and CMG Solution Engineering Guide* > SQL Server editions section

   Data backup and restoration

   Details on data backup and restoration, configuring database backups/restores, scheduled software downloads, and file transfers are available in the following document:

   - *InAttend Administration and Maintenance Guide* > Backup and Restore section

SQL Server authentication

Mixed Mode Authentication is used, which supports both Windows Authentication and SQL Server Authentication (using SQL logins). This mode is selected during installation, and the SA account password is configured. Ensure a strong password that meets the customer's password policies is used.

Details on SQL Server authentication is available in the following documents:

- *InAttend Installation Preparation Guide* > SQL Server Installation section
- *CMG Installation Preparation Guide* > SQL Server Installation section

Database Auditing

Audit trails are supported to maintain records of data processing activities.

Detailed logging for user data management in CMG: When a user record is added, modified, or deleted in CMG DM, detailed log information will be available for the admin ID or email that added, modified, or deleted the user record. The log will also include details of the changed information - name, phone number, phonetics, organization, keyword, activity, and the timestamp.

Data Protection

Data backups can be stored as encrypted files using Microsoft's EFS to protect against unauthorized access and ensure the security of user data at rest. If data is no longer needed, it is manually removed from the database to maintain data hygiene.

The **Encrypting File System (EFS)** is used to encrypt both stored files and backup files, providing an additional layer of security for stored data.

Details on securing log locations, CDRs, and recordings are available in the following documents:

- *InAttend Installation and Configuration Guide* > Configuring EFS section
- *CMG Configuration Guide* > Configuring EFS section

Administration 6

This chapter contains the following sections:

6.1 Administration and Management Tools

InAttend and CMG provide secure administration access by using TLS encrypted web user interface.

Access to InAttend and CMG is restricted by a secure login password, allowing only authorized users to authenticate via username/password combinations. Support for local authentication, Active Directory (AD) authentication, and Single Sign-On (SSO) or Multi-Factor Authentication (MFA) via AD, ensuring robust access control and enhanced security is available.

Further details on Password Management are available in the following documents:

- *CMG Configuration Guide* > Configuring Advanced Security section and setting up Users Authentication section
- *InAttend Installation and Configuration Guide* > Configuring InAttend Users section
- Details On User level authorization are in the *CMG Configuration Guide* > Setting up User Authentication section.

Passwords must adhere to the customer's password policy.

All communications with the system are conducted over authenticated, encrypted channels using HTTPS (TLS), providing robust security during data transmission. The system validates certificates for all TLS connections, ensuring the integrity of secure communications.

OpenID Connect (OIDC) Integration via Keycloak

Administrators can enable Keycloak-based OIDC authentication by configuring the CMG Web application settings in the web.config file. The following configuration keys are available:

- Keycloak:Authority – URL of the Keycloak realm (HTTPS endpoint)
- Keycloak:ClientId – Registered client ID for CMG Web
- Keycloak:RedirectUri – Post-login redirect URL
- Keycloak:Enabled – Enables or disables Keycloak authentication

All communication between CMG Web and Keycloak must be secured with HTTPS using a CA-signed certificate.

Further details on Keycloak-based OIDC authentication Configuration are available in the following documents:

- *CMG Configuration Guide* > Configuring CMG Web for Keycloak OpenID Connect Integration (Azure AD as SAML Broker).

6.2 Administration/Management Tool Encryption

Administration access is through HTTPS on TCP port 443, which must be allowed through the data network's local access control list or firewall rules. Mitel InAttend and CMG support the use of Transport Layer Security (TLS) version 1.3 when installed on Windows Server 2022 or later.

6.3 Web Server Certificate

By default, The Mitel InAttend and CMG create a self-signed certificate to authenticate the Mitel InAttend and CMG to web browsers. The system validates certificates on all TLS connections. However, self-signed certificates are inherently untrusted by the web browser. Mitel recommends installing a certificate obtained from a Certificate Authority (CA) that the customer already owns (an Enterprise CA). The MiCollab Clients will then trust the MiCollab Web server access. Note that certificates do expire, and therefore, the customer must be aware of the expiry date and renew them when needed

Details on certificates are available in *InAttend Installation and Configuration Guide* > Security Certificates section.

Refer to Microsoft OS documentation for additional information about supported cipher suites.

Communications Protection 7

Most personal data transmissions use secure channels. Channels that are not secured can be disabled by the administrator.

Secured Channels

- **Voice Streaming**: Protected using SRTP (Secure Real-time Transport Protocol) with AES encryption.

The supported SRTP ciphers are:

- AES_256_CM_HMAC_SHA1_80
- AES_256_CM_HMAC_SHA1_32
- AES_192_CM_HMAC_SHA1_80
- AES_192_CM_HMAC_SHA1_32
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

Details on SRTP support are available in the *InAttend Installation and Configuration Guide* > Configuring the Media Server section.

- **Voice Call Signaling**: Is secured with TLS. Encryption of call signaling between InAttend and the call managers may be secured with TLS 1.3.
- **HTTPS Communications**: All non-voice data is transmitted via encrypted HTTPS channels using TLS for secure and authenticated exchanges.

- Details on HTTPS are in the *CMG Configuration Guide* > IIS Configuration to access CMG CM, DM, and Web applications over HTTPS section.
- Details on the Network Telephony System are in the *InAttend Installation and Configuration Guide* > Configure the NeTS section.
- Details on the administration of the InAttend server using the BluStar Server Administration tool (WebAdmin) are in the *InAttend Administration and Maintenance Guide* > Administration section.

HTTPS communications may be configured to be secured with TLS 1.3.

TLS Cipher Suite Support

The Microsoft OS provides cipher suite support for TLS Supported ciphers are therefore dependent on the OS version in use, which includes:

- TLS 1.3: TLS_AES_256_GCM_SHA384 and TLS_AES_128_GCM_SHA256
- TLS 1.2: ECDHE-RSA-AES256-GCM-SHA384 and ECDHE-RSA-AES128-GCM-SHA256,

Refer to Microsoft OS documentation for additional information about supported cipher suites.

- **Secure LDAP Support for InAttend and CMG with TLS**:

To enhance security, the InAttend and CMG systems support Secure LDAP (LDAPS) across all components. Communication between these systems and the LDAP server occurs over a secure layer utilizing TLS to ensure data integrity and confidentiality.

- **REST API Security**

  Enhancements REST API

  Communication Model

The **REST API** integration for MX-ONE 8.0+ enables secure and modern communication between CMG and the PBX system using industry-standard web protocols.

PBX Version	API Type	Protocol	Port	Security Layer
MX-ONE < 8.0 / TSW	SOAP	HTTP	80	No encryption
MX-ONE 8.0 and above	REST	HTTPS	9001	TLS 1.3 encryption

Key Security and Performance Enhancements with REST API:

- **HTTPS (TLS 1.3):** Provides encrypted communication, protecting sensitive data and authentication credentials.
- **Dedicated Port (9001):** Streamlines firewall configurations and endpoint routing.
- **Retires legacy SOAP API:** Eliminates dependency on outdated XML/SOAP libraries and insecure HTTP protocols.
- **Improved performance with JSON:** REST responses use **JSON**, a lightweight data format that's easier and faster to process than SOAP's **XML**— resulting in reduced latency and improved scalability.

Details on Enable CMG Personal Number in CMG Configuration Manager are in the **CMG Configuration Guide** > **Enable CMG Personal Number** in CMG Configuration Manager section.

- **Speech Services Integration Security**

CMG Virtual Reception uses the following internal ports for Google speech integration:

- 9002 – HTTP connection between CMG Virtual Reception and the Google Backend.
- 1544 – MRCP communication to the UniMRCP server.
- 8060 – SIP signaling for MRCP session setup.

CMG Virtual Reception ↔ Google Backend link currently uses HTTP and must be restricted to trusted internal networks. Ensure firewall rules and host controls prevent external access to ports 9002, 1544, and 8060. All communication between Google Backend and Google Cloud is protected using encrypted HTTPS channels, ensuring that voice and text data are securely transmitted during the call.

Reference:

- *Virtual Reception Installation and Configuration Guide* > Steps to Follow Post VR Package Installation (only for Google Backend).

Unsecured Channels

Sometimes, SIP trunk providers or third-party SIP devices may not support encryption, leading to a fallback to non-encrypted communication when necessary.

Details on security control of different call managers supported by InAttend and CMG are in the *InAttend Installation and Configuration Guide* > Call Manager Configuration section.

Managing System Security Features 8

This chapter contains the following sections:

Many of the Mitel InAttend and CMG security features can be managed or configured by the administrator or by authorized personnel. Management of these security features is performed by accessing Mitel InAttend and CMG Administration Tool. This section describes the security features that the administrator can configure, and recommendations on how to configure the security features are also provided.

8.1 Identity, Authentication and Password Policies

To ensure privacy and maintain system integrity, access to the Mitel InAttend and CMG is restricted by a login password to those users that can be correctly identified and authenticated.

Access to InAttend and CMG is restricted by a secure login password, allowing only authorized users authenticated via username/password combinations that adhere to strong password policies. This includes support for local authentication, Active Directory (AD) authentication, and Single Sign-On (SSO) or Multi-Factor Authentication (MFA) via AD, ensuring robust access control and enhanced security.

Password Security

As noted above, CMG and InAttend can support both Microsoft and local application accounts, depending on the configuration.

Microsoft Accounts are secured by the OS: When integrated with Microsoft Entra ID (formerly Azure AD) or using Windows Authentication, user credentials are managed and protected by the OS's security mechanisms. This setup is outlined in *CMG Configuration Guide*, which describes the configuration of Microsoft Entra ID with SAML for secure authentication.

Local Application Accounts: CMG also supports local application accounts through **Forms Authentication**, where credentials are stored separately from the OS. These passwords are encrypted and stored securely. For securing CMG and InAttend local authentication passwords on disk, encryption mechanisms such as the Encrypting File System (EFS) are employed. For information on managing local application accounts, **Changing to Domain Account** section in the *CMG Configuration Guide*.

All personal data access is protected with role-based access and authorization controls. This includes personal data processing by data subjects, administrators, technical support, and machine APIs.

OpenID Connect (OIDC) Integration via Keycloak

CMG Web now supports federated Single Sign-On (SSO) using OpenID Connect (OIDC) via Keycloak, which brokers authentication from Azure Active Directory (Azure AD) through SAML 2.0. This configuration enables the reuse of existing enterprise credentials and Azure AD conditional access policies.

Administrators must ensure that the CMG Directory Manager (DM) user email matches the Azure AD User Principal Name (UPN) or email attribute to ensure successful user mapping and login synchronization.

8.2 Security Parameters Available in Configuration Manager

For CMG users, the basic or advanced security may be set. Advanced security means that higher standards are set for users with regard to password quality, with the option of locking them out after failing to log in. Mitel recommends the use of the advanced security function.

The following advanced security parameters can be set in CMG Configuration Manager:

Table 1: CMG Configuration Manager - Security Parameters

Security Parameter	Description
AdvancedSecurity	Set to **Enabled** to turn on the advanced security functions. This means that the parameters below are used.
DaysUntilLockout	Number of days an account can be inactive before it is locked. After that, the administrator unlocked the account.
ForcePasswordChangeOnReset	If set to Enabled, the user must change the password when the account is reset (i.e., activated after lockout or inactivation).
DaysUntilDelete	Number of days an account can be inactive before it is deleted. A system account cannot be deleted.
MaxLogonErrors	Number of failed login attempts before the account is locked. A system account permits an infinite number of login attempts.
PwdExpirationIntStd	Number of days a user has to change the password before the password expires. A system account never expires.
PwdExpirationIntAdm	Number of days Configuration Manager and Directory Manager user has to change the password before it expires.
UserMustChangePwdFirstLogon	If set to **Enabled**, the user must change the password when logging in for the first time.
MinPasswordLength	Minimum number of characters in the password.
MinUserNameLength	Minimum number of characters in the username.

Security Parameter	Description
PasswordRules	If set to 0, all passwords with the required number of characters are allowed. If set to 1, the password can contain only alphanumeric characters (a-z, 0-9), at least one character is numeric, and one character is a letter.

Details on setting basic and advanced security restrictions for the CMG User are in the following document:

- *CMG Configuration Guide* > Configuring Advanced Security section

Details on Password Management are available in the following documents:

- *CMG Configuration Guide* > Configuring Advanced Security section
- *InAttend Installation and Configuration Guide* > Configuring InAttend Users section
- *InAttend Installation and Configuration Guide* > Supported Characters for User Passwords in InAttend with CMG section

Details on Profiles, Users, and Calls Management are in the following documents:

- *InAttend Installation and Configuration Guide* > Configuring InAttend Profiles and Users section
- *InAttend Installation and Configuration Guide* > Working with Profile Groups section
- *InAttend Installation and Configuration Guide* > Configuring InAttend Users section
- *CMG Configuration Guide* > Setting Up User Authentication section

Details on the verification of administrator's and InAttend attendants' authorization to use certain services are in the following document:

- *InAttend Installation and Configuration Guide* > Configuring the Authentication and Authorization (AnA) Web Service section.

Details on configuring Default Voicemail PIN for new users are in the following document:

- *CMG Speech System Settings Maintenance Guide*

Details on unlocking Voicemail after max faulty attempts are in the following document:

- *Directory Manager User Guide*

Configuration Parameters for Google ASR/TTS Integration

To enable Google Cloud Speech Services for CMG Virtual Reception, ensure the required configuration entries are added. These should be included along with the registry values that are automatically set during the VR package installation when using the Speech Attendant with Google as the backend.

In dgserver.ini:

[googleBackend]
host = localhost
port = 9002

In netspeech.ini:

[googleBackend]
uniMrcpHost = localhost
uniMrcpPort = 1544
uniMrcpSipPort = 8060

These settings configure the local HTTP path and MRCP/SIP ports used by CMG Virtual Reception to communicate with the Google Backend and UniMRCP services. Communication between the Google Backend and Google Cloud uses encrypted HTTPS channels to protect voice and text data during transmission.

Reference:

- *Virtual reception Installation and Configuration Guide* > Steps to Follow Post VR Package Installation (only for Google Backend).

8.3 Access and Authorization

For privacy, all data processing is protected with role-based access and authorization controls; this includes personal data processing by data subjects, administrators, technical support, and machine APIs. Role-based access defines permissions based on user roles within a system.

For system integrity and reliability, including the controls that protect privacy, all system data processing and all access to databases, files, and operating systems are protected with role-based access and authorization controls.

Server Roles

Server roles are defined using Microsoft's Server Manager tool to add roles, e.g., Web Server (IIS).

Refer to the InAttend Installation Preparation Guide or CMG Installation Preparation Guide for more details on Mitel application requirements.

InAttend

The BluStar Server Administration tool is used 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.

Configuration Profiles include:

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

A profile group contains one or more configuration profiles that control InAttend client functionality. You can add or remove configuration profiles from a profile group. InAttend users must be assigned to a profile group containing the above configuration profiles.

Details on Profiles, Users, and Calls Management are available in the following documents:

- *InAttend Installation and Configuration Guide* > Configuring InAttend Profiles and Users section
- *InAttend Installation and Configuration Guide* > Working with Profile Groups section
- *InAttend Installation and Configuration Guide* > Configuring InAttend Users section

CMG

CMG user profiles are used for managing call-forwarding options

Details on defining roles and providing access based on the roles to different users are in the *CMG CM Online Help* > All Users section.

8.4 Audits, Logs and Event Reporting

Audit Trails Log

Audit trails are supported to maintain records of data processing activities. All components in InAttend have log files for troubleshooting and audit purposes. This includes security logs, end-user activity records, and administration activity audits.

When CMG Audit Log is enabled, each CMG logon transaction generates an Audit entry in the system application log.

The audit trails and logging mechanisms for CMG and InAttend are in the following sections:

1. **Log Levels** in the *CMG Configuration Guide* and *InAttend Administration and Maintenance Guide*:

   This section explains the different log levels (Error, Warning, Info, Trace, Debug) set in the system registry. It provides details on how each level captures different types of logs, ranging from critical errors to detailed debug logs.
2. **Log Directory for each Component** in the *CMG Configuration Guide* and *InAttend Administration and Maintenance Guide*:

   This section lists where logs for various CMG and InAttend components, including CMG Web Service, Calendar Connection, and others, are stored.
3. **Section 3.1.2.3 Configure Logging to capture deleted users from DM application** in the *CMG Configuration Guide*:

   This section describes how to configure logging to capture deleted users from the DM application.
4. **Section 4.4.2.4 Enabling logging In Configuring CMG Corporate Directory for IP Phones** in the *CMG Configuration Guide*.

   Detailed logging for user data management in CMG: for user data management in CMG, When a user record is added, modified, or deleted in CMG DM, there will be detailed log information of the admin ID or email who added, modified, or deleted the user record. There will be detailed log information of what information was changed – name, phone number, phonetics, organisation, keyword, and activity along with the timestamp.

   Detailed logging features are in the *CMG DM Records > New Records* section.

   - Log details on the Main Form Tab: The user modifies the first name, last name, extension, misc. Fields, and so on, to the corresponding record ID with a date stamp
   - Log details on the Phonetic Tab: The user modifies the phonetic information to the corresponding record ID with a date stamp.
   - Log details on the Organization Tab: The User modifies the Organization to the corresponding record ID with a date stamp.
   - Log details on the Keywords Tab: The User adds, edits, and deletes keywords to the corresponding record ID with a date stamp.
   - Log details on the Recurring Activity Tab: The User adds, edits, and deletes the recurring activity to the corresponding record ID with a date stamp.
   - Log details when deleting an existing Record: The user deletes an existing record with first name, last name, Telno, and date stamp.
   - Log details when creating a new Record: The User adds a record with first name, last name, Telno, and date stamp.

Network Access Security 9

This chapter contains the following sections:

It is recommended that the Ethernet LAN switches used to provide LAN connectivity be managed with enterprise-grade switches that include integrated access control measures. The system administrator should also ensure the switch access control measures are properly configured and maintained.

Wireless networks must also employ access control measures and user authentication mechanisms with minimum WPA2 encryption and a separate SSID for voice applications. SSID to VLAN mapping is recommended.

Most businesses have a well-defined network structure that includes a secure internal network zone and an external untrusted network zone, often with intermediate security zones.

While the threat of attacks might seem daunting, the solution lies in implementing the dynamic and effective software and hardware security solutions available and enforcing strategic security provisions to guard your enterprise against evolving attacks on the network.

- **Network Hardening** must be done for all devices using strong password policies.
- **Maintain current patch levels:** Enterprises should implement adequate monitoring, ensure the timely deployment of patch releases, and keep systems up to date.
- **Limit physical access to network hardware:** Physical access to network hardware must be granted only to relevant and authorized personnel, and all equipment must be stored in a restricted and controlled environment.
- **Implement advanced intrusion detection and prevention systems:** These systems must be part of every enterprise VoIP network. They use stateful detection and prevention techniques and deep packet scanning to guard against zero-day and emerging threats.
- **Enforce security through authentication, authorization, and encryption.** Best practices include:
  - Configuring Ethernet switch ports to allow only known MAC addresses.
  - Password protection using cryptographic keys.

8.5 Using VLANs to Assist with Security

To make eavesdropping attacks or Denial of Service attacks more difficult or less effective, traffic on the LAN should be grouped according to traffic types and trust levels. This can be achieved with the use of Virtual LANs. VLANs can be used to segregate controller-to-controller signaling, controller-to-phone signaling, and voice traffic.

When VLANs are used to provide isolation between traffic types, the solution will be more robust against virus-based and network flooding attacks. In particular, if Voice over Internet Protocol (VoIP) traffic is grouped into a single VLAN and the nodes on this VLAN are strongly protected, a worm-based attack causing network overload that originated on a node located on another VLAN might only marginally affect the VoIP LAN.

When the traffic types have been segregated by VLAN, hosts or devices belonging to different VLANs can only communicate through a Layer 3 switch or router that connects the two VLANs. This means broadcast traffic is blocked across VLANs, preventing broadcast storms from propagating network-wide. Additionally, many modern routers offer Intrusion Detection/Prevention Systems (IDS/IPS), which can detect and/or block more advanced attacks. Creating network trust zones for security purposes and using Intrusion Detection and Prevention Systems (IDPS) are discussed in detail in the Mitel Technical Papers - *Intrusion Detection and Prevention Systems* and *Securing Mitel Cloud-Based Unified Communications*.

Develop a standard building of a secure desktop: Design a secured workstation configuration as the standard build of the company, make an image backup of the build, and replicate it to the company desktops.

Make sure your network is locked down tightly. Good practices, policies, and procedures can secure your WAN and telecommunication services against the most common threats. Protect your network with a complete network security solution.

Secure Development Life Cycle 10

Security and privacy threats are constantly being developed, and existing threats are always evolving. To combat these threats, product designers must continuously evaluate product security risks and ensure that robust controls are included in the design. Evaluating security risks and incorporating protective measures into the design must be an integral part of the product design process.

Mitel's Secure Development Life Cycle (SDLC) policy was created to ensure that product developers employ the latest security and privacy best practices throughout product development.

Mitel InAttend and CMG Release 9.1 were developed in accordance with Mitel's Secure Development Life Cycle policy. As a result, they have been designed with best practice safeguards to mitigate risks to the confidentiality, integrity, and/or availability of data contained within Mitel InAttend and CMG and to the data related to the functionality provided by Mitel InAttend and CMG.

The **OpenID Connect (OIDC)** login feature is built using **Mitel's Secure Development Life Cycle (MiSDLC)** process, which helps ensure the system is safe and reliable. As part of this approach, several important security steps are followed to protect user information and maintain system integrity.

- ID Token signature and claim validation.
- HTTPS/TLS 1.3-only communication enforcement.
- Use of least-privilege OAuth client configurations.
- Periodic vulnerability assessments for Keycloak and dependencies.

Appendix A - Mitel InAttend and CMG – Important Product Information for Customer GDPR Compliance Initiatives 11

Details on Mitel InAttend and CMG GDPR are in the *InAttend Release 9.3 and CMG Release 9.3 - Personal Data Protection and Privacy*.