MiCollab – Personal Data Protection and Privacy Controls

MiCollab Release 9.7 SP1

Version 1.0

July 2023

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

List of Tables

1 Introduction

This document is one in a series of product-specific documents that discuss the product security controls and features available on Mitel products.

This document will be of interest to MiCollab customers that are putting security processes and security controls in place to comply with data security regulations.

This document is intended to assist Mitel MiCollab customers with their data security regulations compliance initiatives by:

- Identifying the types of personal data that are processed by MiCollab
- Listing the MiCollab Security Features that customers may require to achieve compliance with security regulations
- Providing a description of the MiCollab Security Features
- Providing information on where the MiCollab Security Features are documented

This document is not intended to be a comprehensive product-specific security guideline. For information on product security guidelines, product engineering guidelines or technical papers, refer to Mitel's Web Site.

1.1 What is New in this Release

In MiCollab Release 9.7 SP1, no new security features were added.

2 Personal Data Collected by MiCollab

During installation, provisioning, operation, and maintenance, MiCollab **collects** data related to several types of users, including:

- End-users of Mitel products and services – typically Mitel customer employees using Mitel phones, voice mail, and collaboration tools.
- Customers of Mitel customers – for example, conference recordings and call recordings contain personal content of both parties in the call; personal contact lists may contain personal data of business contacts.
- System administrators and technical support personnel – logs contain records of the activities of system administrators and technical support personnel.
- For USA deployments with MiCollab softphones 911 dispatchable location information is cached locally on the user's device.
- Optionally, the MiTeam Classic component of MiCollab provides the ability to store documents and recordings that may contain personal data in data centers located in the USA, China, and Europe. The customer's data is stored within the local geographic regional data center; for example, European customer data is stored in a European data center.
- Optionally, the MiTeam Meeting application launched from MiCollab clients also provides the ability to store documents, share location, maintains meeting chats history, and meeting recordings that may contain personal data in data centers located in the USA and Europe. The customer's data is stored within the local geographic regional data center; for example, European customer data is stored in a European data center.
- The CloudLink (CL) Chat component synchronizes chat conversations, file transfer, and group chat across a user's devices. The CloudLink server stores the files until the CL account is deleted.

3 Personal Data Processed by MiCollab

MiCollab **processes** the following types of data:

- **Provisioning Data**:
  - The user's name, business extension phone number, mobile phone number, location (this is the user's static location, not the user's mobile location), department, business email address, password, MiCollab Client user credentials, active directory photo, and mailbox number.
- **Maintenance, Administration, and Technical Support Activity Records**:
  - System and content backups and logs.
  - Audit trails for MiCollab Unified Messaging admin console are recorded (Not Applicable for MiCloud Flex in Google Cloud deployments).
  - Audit Logs for admin are available. Personal data is not captured in these logs.
- **User Activity Records**:
  - Call and Instant Messaging history, voicemail usage, MiCollab Audio, Web and Video Conference call recordings, and call detail records.
  - MiCollab Client chats are secured with admin access.
  - MiCollab Audio, Web and Video Conferencing (AWV)
    - AWV Public chats are stored and encoded on the MiCollab Server but cannot be accessed from the Admin portal.
    - AWV Public chats are secured with Admin access.
    - AWV Private chats are not stored on the MiCollab Server at all.
    - Access to AWV recordings and uploaded files is password-secured.
  - MiCollab Client
    - Legacy MiCollab chats (that is, non CloudLink server chats) between users are stored in an encrypted file on the MiCollab Server that is secured with administrator access privileges.
- **User Personal Content**:
  - Voice mail, call recordings, chat messages, video images, photos, content sharing, and personal contact lists.
  - CloudLink Chat is a work stream communications and collaboration tool that is available with MiCollab for PC Client, MiCollab MAC Client, MiCollab Web Client, MiCollab for Mobile Client (Android and iOS), and MiCollab Web Client. CloudLink Chat provides the ability to store documents and recordings that may contain personal data in data centers located in the USA and Europe. The customer's data is stored within the local geographic regional data center; for example, European customer data is stored in a European data center.

- MiTeam Meetings is a work stream communications and collaboration tool that is available with MiCollab for PC Client, MiCollab MAC Client, MiCollab Web Client, MiCollab for Mobile Client (Android and iOS), and MiCollab Web Client. MiTeam Meetings provides the ability to store documents and recordings that may contain personal data in data centers located in the USA and Europe. The customer's data is stored within the local geographic regional data center; for example, European customer data is stored in a European data center.
- An optional work stream communications and collaboration tool that is available with MiCollab is MiTeam Classic. MiTeam Classic provides the ability to store documents and recordings that may contain personal data in data centers located in the USA, China, and Europe. The customer's data is stored within the local geographic regional data center; for example, European customer data is stored in a European data center.

Personal data processed by the MiCollab is required for the delivery of communication services, technical support services or other customer business interests. For example, call billing and reporting services.

The MiCollab Client application supports an end-user opt-in consent mechanism.

4 Personal Data Transferred by MiCollab

The types of **personal data transferred** among the MiCollab and various applications and services will depend on the specific use requirements of those applications or services, for example:

- User provisioning data such as the user's first name, last name, office phone number, and mobile phone number may be shared between MiCollab and its associated PBX, management systems such as the Mitel Performance Analytics system and other third-party systems such as Active Directory and the Mitel CloudLink Server.
- User logon credentials may be transferred between MiCollab to Active Directory (AD) / CloudLink for single sign on purposes and authenticated on AD/CloudLink before being allowed access on MiCollab.
- User-provisioning data such as Personal Ring Group (PRG) / Multi Device User group (MDUG) Directory Number, External Hot Desk Users (EHDU), MiCollab Client credentials, IM address, statuses, and so on are collected and shared between multiple MiCollab Servers and associated call control platforms.
- System management activity, such as login and logout, applicable audit logs system logs, MiCollab Client logs, logs for the desktop tool, voice quality logs, customer databases, call records, and voice quality statistics may be transferred to Mitel technical support personnel or secondary storage.
- Call Detail Records may be transferred to third-party billing systems.
- For USA deployments using MiCollab softphone clients “Dispatchable Location” information is conveyed with 911 calls when configured to do so.
- With Unified Messaging (UM) integration the Voicemail (VM) message may be transferred to the customer's email server, if opted. Mitel does offer methods where the VM is kept only on the MiCollab Server (not applicable to MiCloud Flex in Google Cloud deployments).
- Optionally, the MiCollab Server may be Federated with another server using Extensible Messaging and Presence Protocol (XMPP) for Instant Messaging and Presence sharing.
- Optionally, the MiCollab Server can share an avatar (photo) with the MiVoice Business for display on the MiVoice 6900 series IP Phones from Mitel.
- MiTeam Classic is an optional cloud component of MiCollab that allows users to transfer and share content. This uses Transport Layer Security (TLS 1.2) for data transfer, creating a secure tunnel protected by Advanced Encryption Standard (AES) encryption. The connection is authenticated by MiTeam Classic using shared secrets (stored on the MiCollab Server in an encrypted file format AES-256). End-user credentials are not transferred between these servers.
- Optionally, the MiCollab Server may be configured to share user provisioning data with the CloudLink servers. CloudLink Chat is a full featured chat function that synchronizes chat conversations, file transfer, and group chat across devices. CloudLink Chat supports server-independent mode so that the functionalities will work even when MiCollab Server is down. The connection is authenticated by CloudLink using shared secrets. MiCollab does not store Client secrets in backup. MiCollab stores access and refresh tokens in an encrypted format (using AES 128) and these are backed up with MiCollab backup.

5 How the Security Features Relate to Data Security Regulations

MiCollab provides security-related features that allow customers to secure user data and telecommunications data and to prevent unauthorized access to the user's data

Table 1 summarizes the security features Mitel customers can use when implementing both customer policy and technical and organizational measures which the customer may require to achieve compliance with data security regulations.

Table 1 MiCollab Security Features that Customers May Require to Achieve Compliance with Data Security Regulations.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
System and Data Protection, and Identity and Authentication	Access to personal data is limited with administrative controls on accounts for both personnel and Application Programming Interfaces. Access to the system is limited by allowing only authorized access that is authenticated using username/password login combinations that are secured over HTTPS (TLS 1.2) communications channels. User level authorization may be accomplished locally or using single sign on with Mitel's CloudLink Auth. **Note:** MiCollab Webserver interface supports TLS 1.0, TLS 1.1, and TLS 1.2. TLS 1.1 and 1.2 are enabled by default. TLS 1.1 has been deprecated and is considered insecure and is not recommended. It is recommended that the Administrator only use TLS 1.2. Access including those by the administrator and root are logged. Failed login attempts are also logged. All user passwords that are stored locally use encryption/hash algorithms to protect the data. For user continuity credentials, Mitel recommends Active Directory (AD) integration for user login including inheriting the password mechanisms used by AD, for example, password lockout.	Details are available in the document *MiCollab Administrator Online Help*. In the MiCollab Server Manager, go to the: *Security* section for information about adding secure PPTP VPN access to your server, hosts on remote networks accessing the Server Manager. *MiCollab Settings* under *Configuration* for information about setting password strength. *Backup Server Data* section for information about backing up your server data with an encrypted password. *MiCollab Client Service > Enterprise* section for information about Presence Privacy.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
	The optional MiTeam Classic cloud service is hosted using Amazon S3. With Amazon S3, Server-Side Encryption (SSE) is used to encrypt the data stored at rest in Amazon S3. Each object is encrypted with a unique key. As an additional safeguard, this key itself is encrypted with a regularly rotated master key. Amazon S3 Server-Side Encryption uses 256-bit Advanced Encryption Standard (AES-256). MiCollab sever based chat messages are encrypted with Blowfish encryption. A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs), and firewalls. In all cases, physical access to systems should be restricted by the customer. End-users have complete control of their Presence Privacy in MiCollab Client. They can hide their presence or show it to all or to restricted users. They can also request other user's presence status and can accept or reject presence request from other users. The administrator can manage Presence privacy for the whole organization as well as for individual users. Calendar Integration with Office 365 can be performed using Basic Auth and OAuth 2.0.	*MiCollab Settings > CloudLink Integration* under Configuration for information about CloudLink integration with MiCollab.
Communications Protection	Most personal data transmissions use secure channels. Channels that are not secured can be disabled by the Administrator. For system integrity and reliability, all provisioning interfaces use secure channels. MiCollab is designed to work with multiple Mitel call control servers and is required to be on the same network LAN of the call control system. MiCollab Server allows	Details are available in the document *MiCollab Administrator Online Help*. From the MiCollab Unified Messaging Unified Messaging Web Console UI, the system superuser can assign "permission categories" for Functionally Partitioned System Administration (FPSA) users to access features and server resources based on the selected category.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
	only authenticated applications to connect to it. Voice media to and from the MiCollab Server is not encrypted. Voice signaling directly between the PBX and MiCollab Server is encrypted (AES-128) for NPM and not encrypted for AWV. **MiTeam Stream**: Communication channels between MiCollab and MiTeam Classic are authenticated using pre-shared keys saved on the MiCollab Server Data in transit between a MiTeam Stream and the hosted service is always encrypted through TLS 1.2. A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists, and firewalls. **AWV –** AWV Conferences are set up over HTTPS (TLS 1.2) communications. Video calls to AWV are not encrypted. **MiCollab Client –** Communications between the MiCollab Server and MiCollab Client, including instant messaging, are secured over HTTPS (TLS 1.2). Peer-to-peer video calls between MiCollab Clients are encrypted. Voice calls are also encrypted on the MiCollab softphone to other devices that support encryption, such as SRTP. MiCollab Client deployment is secured by TLS 1.2. **Unified Messaging Integration** **IMAP Server –** Transmission of usernames and passwords between the MiCollab Server and an IMAP server may be secured with TLS 1.2. **Office 365 (Exchange Online)** - Transmission of username and OAuth 2.0 token between the MiCollab Server and Office 365 is secured with TLS 1.2. **Microsoft Graph** - Microsoft Graph provides access to data stored across Microsoft 365 services. Custom applications can use the Microsoft Graph API to connect to data and use it in custom applications to enhance organizational productivity.	In the MiCollab Server Manager, go to the: *Security > Syslog* section for information about configuring local syslog server to accept remote syslog events from other hosts. *Security > Web Server* section for information about managing and modifying installed web server certificates. *Security > Certificate Management section for information about managing all Certificate Signing Requests (CSRs) in the queue of this server.*

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
	SMTP Server – Transmission of user names and passwords between the MiCollab Server and a SMTP server may be secured with TLS 1.2. End-user credentials are not transferred between the MiCollab Server and the MiTeam Classic server. For use with MiTeam Meetings the end-user CloudLink GUID is transferred between the MiCollab Server and the MiTeam Meeting server using TLS 1.2 or better.	
Access and Authorization	All personal 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. All system data processing and all access to databases, files, and operating systems, are protected with role-based access and authorization controls. Administrator access to MiCollab is restricted by a secured login username/password combination over HTTPS/TLS1.2. The administrator can choose to set password strength level at strong for enterprise deployment (not available with MiCloud Flex in Google Cloud deployments solution). End-user portal login allows a user to log in to the web-based interface for access to their mailbox, AWV recordings and files, and user's own settings only – not to other users. MiCollab Client deployment using the Redirect server is secured with TLS 1.2 connections. MiCollab Client self-deployment is protected by username/password combination web access before generation of a QR code that represents a randomly	Details are available in the document *MiCollab Administrator Online Help*. Local Administrator permission allows adding/editing users, phones, and services. The account name "local-admin" is created when MiCollab is installed. The local administrator accesses the Administrator portal in the same way as the system administrator but is restricted to a limited subset of administrative tasks. In the MiCollab Server Manager, go to the: *Create, modify, or remove user accounts* section under the *Administration* section for information about modifying, locking, or removing any account or resetting the account's password. *Provision Users and Services* section under the *Applications* section for information about creating or modifying, any end-user portal access. *Security > Web Server* section for information about managing and modifying installed web server certificates.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
	generated authorization token that is valid for 6 weeks or 3 download attempts. The configuration download is secured and encrypted with TLS 1.2 or better. A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists, and firewalls. In all cases, physical access to systems should be restricted by the customer.	*Security > Certificate Management* section for information about managing all Certificate Signing Requests (CSRs) in the queue of this server. *System users'* section for information about modifying, locking, or removing any account or resetting the account's password (by clicking the corresponding command next to the account). In the MiCollab End-user portal, go to the Portal Password section, enter your new password and click **Save**.
Data Deletion	The system provides an end-user or an administrator with the ability to erase the end-user's personal data. CloudLink (CL) chat messages are deleted on CL Account (User) deletion. The MiCollab Users and Services Provisioning application is a single, easy-to-use interface that the administrator uses to add, edit, or delete user data and to modify users' application settings. All data pertaining to a user that is stored on the MiCollab Server are deleted when the user is deleted. Data stored on MiTeam Classic is stored for 30 days after user deletion and can be transferred to another owner. When a user is deleted through the MiCollab Users and Services Provisioning application, the user's voice mail messages are automatically deleted. The system provides the administrator with the ability to erase the end-customer's personal data that may have been left in an end-user's voicemail box. Voice mail recordings may also be deleted automatically based on a retention timer that may be configured	Details are available in the document *MiCollab Administrator Online Help*. In the MiCollab Server Manager, go to the: *Users and Services Create > Users* section for information about adding, editing, or deleting any account from the Server Manager. **Note**: If MiCollab fails to delete a phone's services on the MiVoice Business, you will receive an error. You must manually delete all references to the phone's directory number/Remote Directory Number from the MiVoice Business System Administration Tool forms to complete the deletion.

Security Feature	**Relationship to Data Security Regulations**	**Where the Feature is Documented**
	by the administrator. End-users may delete their own voice mail recordings. End-user information in backup files might not be removed. When deleting a user, the administrator should purge old backups and make a new backup without the end-user's personal data.	
Audit	Audit trails are supported to maintain records of data processing activities. **Deleting Logs** Certain types of logs cannot be deleted on a per user basis such as Call Detail Record logs. However, MiCollab provides the administrator with the ability to delete the entire contents from all logs. Mitel recommends that logs are backed up regularly. **Note**: Logs that are transferred to external or third- party systems are not deleted by this step For information about how to delete logs from these systems, refer to the vendor's documentation.	Details are available in the document *MiCollab Administrator Online Help*. In the MiCollab Server Manager, go to the: *View log files* section for information about viewing or downloading the log files generated by the services running on your server. *Event viewer* section for information about displaying the current alarm state for the system, and the events recorded depending on the current age setting for the page. *Audit Trail in NuPoint Web Console* section for information about generating a report of the current audit trail.

6 Data Security Regulations

This section provides an overview of the security regulations that MiCollab customers may need to be compliant with.

6.1 The European Union General Data Protection Regulation (GDPR)

The European Union (EU) General Data Protection Regulation (GDPR) effective on 25 May 2018 replaces the previous EU Data Protection Directive 95/46/EC.

The intent of GDPR is to harmonize data privacy laws across Europe so that the data privacy of EU citizens can be ensured. GDPR requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. GDPR also addresses the export of personal data outside of the EU. Any business that processes personal information about EU citizens within the EU must ensure that they comply with GDPR. Under GDPR, 'processes personal information' means any operation performed on personal data, such as collecting, recording, erasing, usage, transmitting, and disseminating.

6.1.1 What do Businesses need to know about GDPR?

GDPR applies to businesses with a presence in any EU country, and, in certain circumstances, to businesses that process personal data of EU residents even if the businesses have no presence in any EU country.

In order to achieve GDPR compliance, businesses must understand what personal data is being processed within their organization and ensure that appropriate technical and organizational measures are used to adequately safeguard such data. Table 1 explains what personal data is processed by Mitel’s MiCollab and highlights available security features to safeguard such data.

7 Product Security Information

7.1 Mitel Product Security Vulnerabilities

The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.

Mitel's Product Security Policy is available at:
https://www.mitel.com/support/security-advisories/mitel-product-security-policy

7.2 Mitel Product Security Advisories

Mitel Product Security Advisories are available at:
https://www.mitel.com/support/security-advisories

7.3 Mitel Security Documentation

Mitel security documentation includes product-specific Security Guidelines, Important Information for Customer GDPR Compliance Initiatives and Data Protection and Privacy Controls. Mitel also has Technical Papers and White papers that discuss network security and data center security.

Mitel Product Security Documentation is available at:
https://www.mitel.com/en-ca/document-center

7.4 Mitel MiCollab Services, Terms of Service and Data Protection

MiCollab CloudLink Chat is considered a cloud service and is covered by the following documents:

- MiCloud Services – Global Terms of Service: https://www.mitel.com/en-ca/legal/mitel-cloud-services-terms-and-conditions
- DPA: https://www.mitel.com/en-ca/legal/gdpr/dpa
- Mitel Application Privacy Policy: https://www.mitel.com/en-ca/legal/mitel-application-privacy-policy

8 Disclaimer

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of MiCollab and/or other Mitel products and solutions including without limitation, laws and regulations related to call recording and data privacy. The information contained in this document is not, and should not be construed as, legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.