MiCollab – Important Product Information for Customer GDPR Compliance Initiatives

MiCollab Release 8.0

Version 1

July 2018

Mitel

NOTICE

Trademarks

Contents

Introduction

1.1 Overview

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

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

This document is intended to assist MiCollab customers with their GDPR 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 GDPR compliance
- 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.

1.2 What is 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, 'processing personal information' means any operation performed on personal data, such as collecting, recording, erasing, usage, transmitting, and disseminating.

1.2.1 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. This document explains what personal data is collected, processed, and transferred by MiCollab and highlights available security features to safeguard such data.

2 Personal Data Collected by MiCollab

MiCollab is made available as both on-premises and hosted offerings. Both offerings use only personal data required for the delivery of communication services including Unified Messaging, Collaboration tools, Instant Messaging, technical support services, and performance analytics. There are no end user opt-in consent mechanisms implemented in MiCollab.

During the course of installation, provisioning, operation, and/or 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.
- Optionally, the MiTeam 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. Customer's data is stored within the local geographic regional data center; for example, European customer data is stored in a European data center.

3 Personal Data Processed by MiCollab

MiCollab processes the following types of data to enable its communications features:

- **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.
  - Audit Logs for admin are available. Personal data is not captured in the logs.

- **User Activity Records:**
  - Call and Instant Messaging history, voicemail usage, MiCollab Audio, Web and Video Conference call recordings, and call detail records.
  - Administrator access to MiCollab Client chats and MiCollab Audio are secured with passwords.

  - AWV
    - AWV Public chats are stored and encoded on the MiCollab Server, but cannot be accessed from the Admin portal.
    - MiCollab Audio, Web and Video Conference (AWV) public chats are secured with Admin access.
    - AWV Private chats are not stored on the MiCollab Server.
    - Access to AWV recordings and uploaded files is password-secured.
  - MiCollab Client
    - MiCollab Client chats between users are stored in an encrypted file on the MiCollab Server that is secured with administrator access privileges.
  - Optional MiTeam:
    - The MiTeam component of MiCollab provides the ability to store documents, recordings and have a persistent chat.
    - Transfer of MiTeam Stream ownerships is password-secured, audited, and subject to administrator control.
- **User Personal Content:**
  - Voice mail, call recordings, chat messages, video images, photos, content sharing, and personal contact lists.

4 Personal Data Transferred by MiCollab

Depending on configuration, and specific use requirements, the personal data collected may be processed and/or transferred between the MiCollab and other related systems and applications (such as directory systems, voice mail systems, and billing systems.) 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, MiCollab, and management systems such as the Mitel Performance Analytics system and other third-party systems such as Active Directory.
- Logon credentials may be transferred between MiCollab to Active Directory and authenticated on AD 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.
- 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.

- 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.
- 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 is an optional cloud component of MiCollab that allows users to transfer and share content. This uses Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by Advanced Encryption Standard (AES) encryption. The connection is authenticated by MiTeam using shared secrets (stored on the MiCollab Server in an encrypted file). End user credentials are not transferred between these servers.

5 How MiCollab Security Features Relate to GDPR

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

Table 1 Summarizes the security features Mitel customers may use when implementing and evaluating both customer policy and technical and organizational measures required to achieve customer GDPR compliance.

Table 1: MiCollab Security Features that Customers May Require to Achieve GDPR Compliance

Security Feature	Feature Details	Where the Feature is Documented
System and Data Protection, and Identity and Authentication	Access to personal data is limited with administrative controls on accounts. Access to the system is limited by allowing only authorised access that is authenticated using username/password login combinations that are secured over HTTPS (TLS) communications channels. 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	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.

	recommends Active Directory (AD) integration for user log in, including inheriting the password mechanisms used by AD; for example, password lockout. MiTeam 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. Amazon S3 Server Side Encryption employs strong multi-factor encryption. 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). 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.	
Communications Protection	For system integrity and reliability, all provisioning interfaces use channels that are secured through HTTPS/TLS. MiCollab is designed to work with multiple Mitel call control servers and to be adjacent on the network to the call control system. MiCollab Server allows only authenticated applications to connect to it. Voice media to and from the MiCollab Server is not encrypted. Voice signalling is directly between the PBX and MiCollab Server and is not encrypted. **AWV –** AWV Conferences are set up	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. 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

	over HTTPS (TLS) 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). Peer-to-Peer video calls between MiCollab Clients are encrypted. Voice calls to other devices that support encryption (such as SRTP) are also encrypted on the MiCollab softphone. MiCollab Client deployment is secured by TLS. **Unified Messaging Integration** **IMAP Server –** Transmission of user names and passwords between the MiCollab Server and an IMAP server may be secured with TLS. **SMTP Server –** Transmission of user names and passwords between the MiCollab Server and a SMTP server may be secured with TLS. **MAPI Gateway –** Transmission of user names and passwords between the MiCollab Server and a MAPI server may be secured with TLS. **MiTeam –**To protect data in transit, MiTeam uses Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by Advanced Encryption Standard (AES) encryption. Communication channels between MiCollab and MiTeam are secured with TLS. Data in transit between a MiTeam client and the hosted service is always encrypted through TLS. End user credentials are not transferred between the MiCollab	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.

	Server and the MiTeam server. A customer can further limit access over the network using standard network security techniques such as VLANs; access control lists and firewalls.	
Access and Authorization	Administrator access to MiCollab is restricted by a secured login username/password combination over HTTPS/TLS. The administrator can choose to set password strength at strong. All system data processing and all access to databases, files, and operating systems are protected with administrator authorization controls. End-user portal log in allows a user to log in to the web-based interface for access to their mailbox, AWV recordings and files, and user settings only; not to other users. MiCollab Client deployment using the Redirect server is secured with TLS connections. MiCollab Client self deployment is protected by username/password combination web access before generation of a QR code that represents a randomly generated authorization token that is valid for 6 weeks or 3 download attempts. The configuration download is secured and encrypted with TLS. A customer can further limit access over the network using standard network security techniques such as	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 will see 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 > 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 on the corresponding command next to the account).

	VLANs; access control lists, and firewalls. In all cases, physical access to systems should be restricted by the customer.	In the MiCollab End-user portal, go to the: • *Portal Password* section and enter your new password and click *Save*.
Data Deletion	The system provides the administrator with the ability to add or delete a user and all phone services and MiCollab services associated with that user. 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 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. Voice mail recordings may also be deleted automatically based on a retention timer that may be configured by the administrator. End users may delete their own voice mail recordings. End user information in backup files may 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.	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 before you can complete the deletion.

Audit	Audit logs are supported for the MiCollab Unified Messaging application. The logs are for maintaining 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. **Note**: Logs that are transferred to external or third-party systems are not deleted by this step For information on how to delete logs from these systems refer to the vendor's documentation. Mitel recommends that logs are backed up regularly.	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.
End Customer Guidelines	MiCollab documents and guidelines are available to assist with installation, upgrades, and maintenance.	Details are available in the document *MiCollab Administrator Online Help*.

6 Product Security Information

6.1 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:
www.mitel.com/support/security-advisories/mitel-product-security-policy

6.2 Mitel Product Security Publications

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

7 Disclaimer