MiVoice Business – Personal Data Protection and Privacy Controls

MiVoice Business Release 10.1

Version 1.0

December 2023

NOTICE

Trademarks

Contents

List of Tables

1 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 Mitel MiVoice Business customers that are putting security processes and security controls in place to comply with data security regulations.

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

- Identifying the types of personal data that are processed by MiVoice Business
- Listing the MiVoice Business Security Features that customers may require to achieve compliance with data security regulations
- Providing a description of the MiVoice Business Security Features
- Providing information about where the MiVoice Business 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 New in this Release

The following security related changes are included in Release 10.1:

- MiVoice Business Release 10.1 includes support for TLS 1.3.

2 Personal Data Collected by MiVoice Business

MiVoice Business is made available as both on-premises and hosted offerings. Both offerings process only personal data that is required for the delivery of communication services including call control, billing services, and technical support services. There are no end-user opt-in consent mechanisms implemented in MiVoice Business.

During the course of installation, provisioning, operation, and/or maintenance, MiVoice Business collects data related to several types of users, including:

- End-users of MiVoice Business – typically Mitel customer employees using Mitel phones.
- Customers of Mitel customers – for example, voicemail recordings might contain personal content of both parties in a call; end-user personal contact lists may contain personal data of their business contacts.
- System administrators and technical support personnel – logs and audit trails contain records of the activities of system administrators and technical support personnel.

3 Personal Data Processed by MiVoice Business

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

- **Provisioning Data:**
  - The end-user's name, business extension phone number, mobile phone number, location, department, and email address.
- **Maintenance, Administration, and Technical Support Activity Records:**
  - System and content backups, logs, and audit trails.
- **End-User Activity Records:**
  - Call history and call detail records.
- **End-User Personal Content:**

Voice mail recordings and personal contact lists.

4 Personal Data Transferred by MiVoice Business

Depending on the customer's configuration, and specific use requirements, the personal data collected may be processed and/or transferred between the MiVoice Business 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 configured to be shared between clustered MiVoice Business systems, Mitel MiCollab, and management systems such as the Mitel Performance Analytics system.
- Voice quality logs, phone inventory, username, and phone number may be configured to be read by Mitel Performance Analytics system and other customer-authorized systems.
- System logs, login and logout audit logs for the desktop tool, voice quality logs, customer databases, call detail records (also known as CDR or SMDR), and voice quality statistics may be configured to be transferred to Mitel product support or transferred to customer-authorized log collecting systems.
- Call Detail Records may be configured to be transferred to third-party call accounting systems.
- When MiVoice Business is part of a Hospitality solution (hotel/motel) the system may be configured to transfer the end-user's personal data between the MiVoice Business system and other customer authorized Property Management Systems.

5 How the Security Features Relate to Data Security Regulations

MiVoice Business 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 summaries the security features Mitel customers can use when implementing both customer policy and technical and organizational measures that the customer may require to achieve compliance with data security regulations.

Table 1 MiVoice Business 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 Data Protection, and Identity and Authentication	Access to personal data is limited with the following controls.	Details are available in the document, *MiVoice Business Security Guidelines* and in the *MiVoice Business System Administration Tool* Help files.
	Management Tool Access to the Management Tool is limited by allowing only authorised access that is authenticated using username/password login combinations that use strong password mechanisms. Failed logins are logged and restricted to a maximum of three attempts.	In the MiVoice Business System Administration Tool Help files go to the: *System Security Management Form* to configure administrative access controls. This form is used to:
	Passwords are stored securely using strong encryption. The encryption mechanism used is the Advanced Encryption Standard - AES 256-bit encryption.	Set/reset the password Establish the password strength rules Set the user session inactivity timer Set the password expiry interval Enable/disable the Login Banner Set the Phone Administrator's Password
	Communications to the system are performed over authenticated, encrypted communications channels using HTTPS (TLS). The MiVB supports TLS 1.2 & TLS 1.3.	
	A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs), and firewalls.	*System IP Properties Form* to configure VLANs and DNS settings. *External FTP Server Form* to configure data base backups/restores, scheduled software downloads, and file transfers.
	In all cases, physical access to systems should be restricted by the customer.	

Security Feature	**Relationship to Data Security Regulations**	**Where the Feature is Documented**
System Data Protection, and Identity and Authentication	**Embedded Voice Mail Box** User access to their Voice Mail Box is limited with a passcode that can be set to between 4 and 10 digits. OpenSSL's AES 256-bit encryption is used to encrypt passcodes. The Mailbox lockout timer can be set from 0 to 60 minutes, where 0 refers to lock mailbox "forever".	*VM Options Form* to configure the passcode length and lock out rules.
Communications Protection	Communications protection is provided with the following controls. **Voice Streaming** MiVoice Business may be configured to encrypt all IP voice call media streams with either Mitel SRTP or SRTP using AES 128 encryption. Note that not all SIP trunks service providers and third-party SIP devices support encryption. Legacy technologies such as analog and digital trunks and devices do not support encryption. In such cases, if permitted, the communications will negotiate to no encryption. Note: The 6900 series of MiNET IP sets have the ability to indicate on their displays that a call is secured with end-to-end encryption.	Details are available in the document *MiVoice Business Security Guidelines* and in the *MiVoice Business System Administration Tool* Help files. In the MiVoice Business System Administration Tool, go to: *System Options Form* and also see information entry on *Voice Streaming Security.* The Secure Call Icon feature must be enabled by the Administrator. The feature is enabled via the MiVoice Business System Administration Tool. Within the System Administration Tool, the system option called Voice/Video SRTP Encryption Enabled field must be set to Yes for the SRTP security to be negotiated.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
Communications Protection	**Voice Call Signaling** Only authenticated devices may connect to the MiVoice Business. Call signaling between the MiVoice Business and IP phones may be secured with TLS. Legacy analog and digital trunks and devices do not support encryption. **Call Privacy** Only authenticated devices may connect to the MiVoice Business. All IP communications are encrypted by Mitel by default. Additional Caller privacy is controlled with a number of option settings and Class of Service settings including: Call Privacy settings Caller ID settings on Trunks Call Display settings HCI/CTI/TAPI settings IP Phone Peripheral settings for Bluetooth, USB, and PC port.	See the information entry on *Call Signaling Security.* For Release 9.1 and later, the system can be configured to support only TLS 1.2. For details, refer to the *Knowledge Based Article SO4819 - How to enable TLS 1.2 only for MiVB 9.1.* For Release 10.1 the system can be configured to support TLS 1.2 and TLS 1.3. If TLS 1.2 and TLS 1.3 are enabled on the MiVB, the MiVB will attempt to connect to the endpoint with TLS 1.3, if the endpoint does not support TLS 1.3, the MiVB will negotiate down to TLS 1.2 and attempt to communicate. *Class of Service Options Form* and the *Calling Line ID Restriction Form.*

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
Communications Protection	**WAN Security** Some Mitel MiVoice Business 3300 ICP appliances have a WAN port on them. The WAN interface is secured with an integral firewall that examines all packets attempting to access the internal network from the Internet. Unless a packet is part of an existing connection or matches a specific TCP or UDP port programmed for forwarding, it is declared as *unknown*. All unknown packets are logged in System Diagnostics and then either dropped or rejected.	Details are available in the document *MiVoice Business Security Guidelines* and in the *MiVoice Business System Administration Tool* Help files. *Port Forward Table Form* to configure the MiVoice Business's integral router. *IP Routing Form* to configure routing capabilities. *Firewall Control Form* to configure the integral Internet gateway. Note: The above-mentioned forms are applicable only to MiVoice Business 3300 ICP appliances that are equipped with a WAN interface.
	Remote Access Security The firewall can also be programmed to allow Virtual Private Network (VPN) tunnels with PPTP and IPSec pass-through and inbound connections with IP Port Forwarding.	*Remote Access (PPTP) Form* to configure the internet gateway. **Note**: The above-mentioned forms are applicable only to MiVoice Business 3300 ICP appliances that are equipped with a WAN interface.
	IMAP Server Transmission of usernames and passwords PINs) between the MiVoice Business and an IMAP server may be secured with TLS or with OAuth2.0. 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.	*Embedded UM (Unified Messaging) Settings Form* to configure the IMAP Server connection.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
Communications Protection	**Voice Mail - Authentication with Other Applications** The MiVoice Business embedded voice mail application can use OAuth2.0 to authenticate with a number of applications such as: • Microsoft Office 365 • Microsoft Graph • IMAP • SMTP **Voice Mail – Forward to Email** The forward to email feature which forwards a voicemail message to the user's email account supports the following transmission and authentication methods: A non-secure / Cleartext method of forwarding to email via Port 25. This method is not supported in the MiCloud Flex Solution. It is available only with the MiVB Enterprise solutions. The STARTTLS method of authentication for forwarding to email via Port 587. This method is supported for MiVB Enterprise solutions and is mandatory for MiCloud Flex solutions. The SSL / TLS method of authentication for forwarding to email via Port 465. This method is supported for MiVB Enterprise solutions and is mandatory for MiCloud Flex solutions.	*Embedded UM (Unified Messaging) Settings Form* to configure the Server connection. Details are available in the document *MiVoice Business Security Guidelines* and in the *MiVoice Business System Administration Tool* Help files. *Forward Voice Mail to Email Form* to configure this feature.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
Access and Authorization	**Role-Based Access** MiVoice Business supports up to five System Administration Tool users, five Group Administration Tool users, and 10 Desktop Tool users at a time. Only the root Administrator can program access to the System Administration Tool and use the Import and Export functions in this form. Other administrators can only manage user profiles that do not have System Administrator Tool access rights. 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.	Details are available in the document *MiVoice Business Security Guidelines* and in the *MiVoice Business System Administration Tool* Help files. In the MiVoice Business System Administration Tool, the following forms are used to establish role-based access controls: *User Authorization Profiles Form*. This form is to create, modify, and delete user profiles which are required to access the following MiVoice Business management interfaces: System Administration Tool Group Administration Tool Desktop Tool The *Admin Policies Form.* This form is used to add, modify, and delete policies that are used to establish permissions for various user profiles. These permission policies dictate which System Administration Tool forms a user is allowed to access or modify.
Data Deletion	The system provides the Administrator with the ability to delete a user, or to delete a user and all phone services and MiCollab services associated with that user. **Deleting a User and Phone Services** The MiVoice Business allows the Administrator to delete a user, or a user and all of the user's associated phone services.	Details are available in the document *MiVoice Business Security Guidelines* and in the *MiVoice Business System Administration Tool* Help files. In the MiVoice Business System Administration Tool, the following forms and procedures are used to erase a personal data: The *User and Services Configuration Form.* This form is used to delete a user or to delete a user and all associated phone services.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
Data Deletion	**Deleting a User's Embedded Voice Mail Box** The MiVoice Business allows the administrator to delete a user's embedded voice mail box.	The *User and Services Configuration Form* is also used to delete a user's embedded voice mailbox. Alternately, the administrator's mailbox can be used to delete a user's mailbox.
	Deleting a User from the Telephone Directory The MiVoice Business allows the Administrator to delete a user from the telephone directory.	The *Telephone Directory Form.* This form is used to delete a user from the telephone directory.
	Deleting Logs Certain types of logs cannot be deleted on a per user basis such as Call Detail Record logs, CESID logs, and Hot Desking Logs. However, MiVoice Business 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 method. For information about how to delete logs from these systems, refer to the vendor's documentation.	MiVoice Business supports several logs. For a complete list of logs and the forms that are used to manage the logs, refer to the *MiVoice Business System Administration Tool Help* files. The System Administrator can delete Property Management System occupancy logs from the MiVoice Business, for details refer to the *MiVoice Business Security Guidelines, in the section Audits and Logs.* In the *MiVoice Business System Administration Tool* Help files, look under *Property management System (PMS)* for additional information about PMS logs.
	Deleting Voicemail Messages The system provides the Administrator with the ability to erase a voicemail message that was left in the end-user's voicemail box by a customer of the end-user the end-user. The system Administrator can, once authenticated, log in to the shell and locate and delete the file that contains the voicemail message based on the user's extension number and the time that the recording was left in the user's voicemail box.	

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
Audit	**Audit Trail Logs** Audit trails are supported to maintain records of data processing activities. Audit Trail Logs provide a historical record of changes made to the system from the System Administration Tool and various other user interfaces and applications. It does this by recording certain actions (such as who logged in and when) and storing this information in a log. Use the logs to help with troubleshooting when problems arise and to determine who in a multi-administrator system is responsible for a particular change. **SMDR Logs** Station Message Detail Recording (SMDR) is the Mitel name for Call Detail Recording (CDR) logs on the MiVoice Business platform. The system allows the Administrator to configure the details that will be recorded for internal calls, external calls and details related to location-based accounting.	Details are available in the document *MiVoice Business Security Guidelines* and in the *MiVoice Business System Administration Tool* Help files. In the MiVoice Business System Administration Tool, go to the following forms: *Audit Trails Logs Form.* This form provides a historical record of changes made to the system from the System Administration Tool and various other user interfaces and applications. *SMDR Options Form* (Station Management Detail Recording). This form is used to configure SMDR options.
End Customer Guidelines	MiVoice Business Security Guidelines are available to assist with installation, upgrades, and maintenance.	The MiVoice Business Security Guidelines provide detailed recommendations on how the MiVoice Business security-based features can be used within the customer GDPR compliance initiatives. The MiVoice Business Security Guidelines are available at Mitel online.

6 Data Security Regulations

This section provides an overview of the security regulations that MiVoice Business 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. Section 5 of this document explains what personal data is processed by Mitel’s MiVoice Business 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 and 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 centre security.

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

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 MiVoice Business 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.