MiVoice Office 400 – Personal Data Protection and Privacy Controls

MiVoice Office 400 Release 6.3

Version 1.0

March 2021

NOTICE

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 MiVoice Office 400 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 Office 400 customers with their data security regulations compliance initiatives by:

- Identifying the types of personal data that are processed by MiVoice Office 400
- Listing the MiVoice Office 400 Security Features that customers may require to achieve compliance with security regulations
- Providing a description of the MiVoice Office 400 Security Features
- Providing information on where the MiVoice Office 400 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

In this release, Automatic keylock has been introduced for SIP-DECT terminals.

2 Personal Data Collected by MiVoice Office 400

MiVoice Office 400 is made available as both on-premise and hosted offerings. Both offerings collect 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 Office 400.

During the course of installation, provisioning, operation, and maintenance, the MiVoice Office 400 collects data related to several types of users, including:

- End-users of MiVoice Office 400 – typically Mitel customer employees using Mitel phones.
- Customers of Mitel customers – for example, voice mail and call recordings contain personal content of both parties in the call; the end-user's personal contact lists may contain personal data of 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 Office 400

The MiVoice Office 400 processes the following types of data:

- **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.
- **User Personal Content:**
  - Voice mail, call recordings, personal contact lists

4 Personal Data Transferred by MiVoice Office 400

Depending on the customer's configuration, and specific use requirements, the personal data collected may be processed and/or transferred between the MiVoice Office 400 and other related systems and applications (such as directory systems, voice mail systems, and billing systems.) For example:

- User provisioning data, such as name, office phone number, and mobile phone number are shared between MiVoice Office communication servers, Mitel MiVoice Office 400, and other customer authorized systems.
- Maintenance, administration, and technical support activity records, such as configuration data backups 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 Office 400 is part of a Hospitality solution (hotel/motel) the system may be configured to transfer the end-user's personal data between the MiVoice Office 400 and other customer authorized Property Management Systems. Personal content such as call recordings and voice mail messages can be sent automatically by email to different destinations. Voice mail messages and personal greeting can be manually saved in a backup.

5 How the Security Features Relate to Data Security Regulations

MiVoice Office 400 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 Office 400 Security Features that customers may require to achieve Compliance with Data Security Regulations.

Security Feature	Feature Details	Where the Feature is Documented
System and Data Protection	Access to personal data is limited with administrative controls. Access to the system is limited by allowing only authorized access that is authenticated using encrypted username/password login combinations. For system integrity and reliability, all provisioning interfaces use secure channels. Communications to the system are performed over authenticated, encrypted communication channels using HTTPS in most cases. Some applications such as the Open Interfaces Platform (OIP) or hotel management systems use different communication channels that are authenticated, but not encrypted. Failed access logins are logged and after 15 failed attempts, the user account is locked for 10 minutes and the teleworker account is locked for 30 minutes. These accounts are automatically unlocked and do not need an administrator to unlock them. The end-user's voice mail data is encrypted and pseudonymized when stored on the system to prevent reading/listening of the data by third parties, including the administrator. 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 the system should be restricted by the customer.	Details are given in the chapter "User access control" in the system manual of the appropriate MiVoice Office 400 communication server. OR In the online Help of the views under "Access control" in WebAdmin, the web-based administration tool for MiVoice Office 400. See "Configuration > User access control > WebAdmin User accounts and authorization profiles > Passwords".
Communications Protection	All personal data transmissions may use secure channels. There may be unsecured channels available, but the administrator has the choice to use secure channels only. For system integrity and reliability, all provisioning interfaces use secure channels.	

	A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists, and firewalls. **Voice Streaming** MiVoice Office 400 may be configured to encrypt all IP voice call media streams with SRTP using AES 128 encryption. **Note:** 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. If permitted, the communication will negotiate to no encryption. **Voice Call Signaling** Only authenticated devices may connect to the MiVoice Office 400. Call signaling between the MiVoice 400 and the IP phones may be secured with TLS 1.2. Legacy analog and digital trunks and devices do not support encryption. **Call Privacy** Only authenticated IP devices can connect to the MiVoice Office 400. All IP communications may be secured with TLS 1.2 when configured. The user of a device may further secure their device with a PIN to protect the device. The Call Privacy settings on the MiVoice Office 400 allow restriction of the user identity and/or the presentation of the phone number during call establishment as well as during a conversational. **Email** The email channel may be secured and authenticated using an SMTP connection encrypted using TLS 1.2.	For details, see the document MiVoice Office 400 Security Guidelines.
Access and Authorization	**Role-Based Access** The MiVoice Office 400 system supports a total of 25 predefined Role Based Access (RBA) accounts and authorization profiles. For each RBA account, an authorization profile is assigned, which defines permissions and allows limited access to certain interfaces. There is one default RBA account with administrator rights, which allows the	Details are given in the chapter “User Accounts” in the system manual of the appropriate MiVoice Office 400 communication server And in the online Help of the view “User accounts” in the WebAdmin, the web-based administration tool for MiVoice Office 400.

	administrator to create additional user and RBA accounts, and authorization profiles. All administrative and API-based accounts are forced to use a strong password in combination with the user name. **End-User Access** For each end-user, a specific personal account exists, for example, to access the Self Service Portal (SSP). The end-user has the permission to set, update, or delete the data belonging to the individual account. End-user account is allowed to use the user name or the extension number in combination with a PIN when the user is located within the LAN. In cases where the end-user is remotely located and connects through a WAN, as with Teleworkers, the end-users are forced to use a strong password in combination with the user name. **Number of Users Allowed Access** Access to the system is limited depending on the type of account. For the end-user accounts the maximum allowed number of end-users depends on the system platform. For the system configuration accounts, such as Administrator, System Assistant or Hospitality Manager accounts, two sessions are allowed in parallel. **Authorization** MiVoice Office 400 supports authorization profiles. The system supports default authorization profiles for the administrator and for certain application programming interfaces; for example, for third - party CTI users. An authorization profile has a related set of permissions that can be configured individually. The profile determines whether the user has the correct permissions to access a specific functionality or a certain interface. The authorization profile with its associated permissions can be assigned to a specific user account. Only the Administrator can create new system user accounts.	Details are given in the chapter “WebAdmin Configuration Tool” in the system manual “System Functions and Features”. The online Help of the view “Authorization profiles” in WebAdmin, the web-based administration tool for MiVoice Office 400 has detailed information about: Administration rights, interface access, WebAdmin access, and predefined authorization profiles.

Data Deletion	The system provides an administrator with the ability to erase the end-user's personal data. **Deleting a User and Phone Service** The MiVoice Office 400 allows the administrator to delete a user, or a user and all of the users associated phone services. **Deleting a User 's Embedded Voice Mail Box** The MiVoice Office 400 allows the administrator to delete a user's embedded voice mail box. **Deleting a User from the Telephone Directory** The MiVoice Office 400 allows the administrator to delete a user from the telephone directory. **Deleting Logs** Certain types of user data cannot be deleted such as the Access Detail Record logs. Certain types of logs cannot be deleted on a per user basis. However, MiVoice Office 400 provides the administrator with the ability to delete the entire content from all logs. The Call Detail Record (CDR) logs are not stored on the MiVoice Office 400 at all, but if configured, they can be sent to a customer authorized external call accounting server. The system supports hospitality functionality. It logs the call data information of the user/guest for the purpose of the invoice. The information is stored in a file which the administrator / hospitality manager is able to delete. **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. **Deleting Voice Mail Messages** The voice mail data belonging to an end-user can be deleted by the end-user. Furthermore, automatic deletion of voice mail messages after e-mail sending is configurable by the end-user.	Details are given in the online Help of the view "User list" in WebAdmin, the web-based administration tool for MiVoice Office 400. The Access Detail Record data can be retrieved in the online Help of the view "Access logs" in WebAdmin, the web-based administration tool for MiVoice Office 400. Details are given in the online Help of the "Hospitality Manager". Details are given in the user guide "Voice Mail System" for MiVoice Office 400 and in the user guide for each phone system.

	The MiVoice Office 400 allows the administrator to delete a user's embedded voice mail box. The administrator can delete all of an end-user's voice mail data by deleting the end-user from the system.	
Audit	Audit trails are supported to maintain records of data processing activities. **Audit Trail Logs** Audit Trail Logs provide a historical record of changes made to the system from the System Administration Tool (Web Administration) and various other user interfaces and applications. The administrator may use the logs to determine who in a multi-administrator system is responsible for a particular change. **Call Detail Record Logs** The system allows the administrator to configure what details will be recorded for internal and external calls.	Details are given in the chapter "Access logs" in the system manual of the appropriate MiVoice Office 400 communication server And in the online Help of the view "Access log" in WebAdmin, the web-based administration tool for MiVoice Office 400. Details are given in the online Help of the view "Charges - General" in WebAdmin, the web-based administration tool for MiVoice Office 400.
End Customer Guidelines	MiVoice Office 400 Security Guidelines are available to assist with installation, upgrades, and maintenance.	The MiVoice Office 400 Security Guidelines (Product Information) provide recommendations on how the MiVoice Office 400 security-based features can be used to help the customer achieve GDPR compliance.

6 Data Security Regulations

This section provides an overview of the security regulations that MiVoice Office 400 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 MiVoice Office 400 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 Product Security Publications are available at:
https://www.mitel.com/support/security-advisories

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 Office 400 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.