MiVoice Business Console – Personal Data Protection and Privacy Controls

MiVoice Business Console Release 9.2

Version 1

October 2021

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.

Trademarks

Contents

1 Introduction 1
1.1 Overview 1
1.2 What is New in this Release 1
2 Personal Data Collected by MiVoice Business Console 2
3 Personal Data Processed by MiVoice Business Console 3
4 Personal Data Transferred by MiVoice Business Console 4
5 How the Security Features Relate to Data Security Regulations 5
6 Data Security Regulations 8
6.1 The European Union General Data Protection Regulation (GDPR) 8
6.1.1 What do Businesses need to know about GDPR? 8
7 Product Security Information 9
7.1 Mitel Product Security Vulnerabilities 9
7.2 Mitel Product Security Advisories 9
7.3 Mitel Security Documentation 9
8 Disclaimer 10

List of Tables

Table 1: MiVoice Business Console Security Features which customers may require to achieve Compliance with Data Security Regulations. 5

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, and will be of interest to Mitel MiVoice Business Console customers who are putting security processes and security controls in place to comply with GDPR.

This document is intended to assist MiVoice Business Console customers with their GDPR compliance initiatives by:

- Identifying the types of personal data that are processed by MiVoice Business Console
- Listing the MiVoice Business Console Security Features that customers may require to achieve GDPR compliance
- Providing a description of the MiVoice Business Console Security Features
- Providing information on where the MiVoice Business Console Security Features are documented

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

1.2 What is New in this Release

From a security standpoint, the 9.2 MIVB Console will authenticate directly with CloudLink for CloudLink Chat-related services. The Operator will be offered a web-based window controlled by the CloudLink server to perform this authentication. Note that the Console does not require CloudLink authentication to perform normal Call Handling operations.

The MiCollab Server provides the console with Presence information (as it has done in earlier releases as well). New for the 9.2 release, the console must comply with a further security check when logging into the MiCollab Server. MiCollab 9.3 now accepts and validates a CloudLink token when the console authenticates for MiCollab services.

2 Personal Data Collected by MiVoice Business Console

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

- End-users of MiVoice Business Console, typically receptionists or anyone handling incoming business calls.
- Customers of Mitel customers – Call information such as caller ID (name and number), call times, and duration of call are recorded in software logs.
- System administrators and technical support personnel – Windows user name of users starting MiVoice Business Console are recorded in software logs. PC logins are recorded by the Windows operating system and can be viewed in Windows Event Viewer.
- MiVoice Business Console can be configured to collect Call History records. These records are stored on a customer-provided or customer-owned PostgreSQL database that resides on either the same PC as the Console or a remote computer (also customer provided or owned).
- In *ADF Mode,* the console has a local copy of the MiVB Telephone Directory in CSV format. This file is normally created by exporting the telephone directory from the MiVoice Business. Additional fields that are not supported by the MiVB (for example, Automotive License Plate, Home Phone, and so on) may be added by this file.
- User Messaging when used with large customer databases will contain a “Contacts” file obtained from the MiCollab Server.

3 Personal Data Processed by MiVoice Business Console

MiVoice Business Console **processes** the following types of data:

- **Provisioning Data:**
  - User directory numbers stored in Windows Registry.
- **Maintenance, Administration, and Technical Support Activity Records:**
  - System Logs may contain usernames, numbers, call times, and duration.
- **End User Activity Records:**
  - Call activity may be recorded in software logs.
- **End User Personal Content:**
  - The Scratch Pad feature and comment files can be used to store personal information.
- **User Specified Data:**
  - **Additional Data Field(ADF) Mode**

    This mode of operation has all Telephone Directory data stored in a CSV file on the PC running MiVoice Business Console. This file is normally created by exporting the telephone directory from MiVoice Business. The user is then able to add additional fields to the CSV file and have them displayed on MiVoice Business Console. There are no restrictions on the data stored and the file is not encrypted, or password protected.

  - **Comments File**

    The user may add user-specific comments to directory entries. These are stored in a file on the PC and may be protected with BitLocker.

  - **Scratch Pad**

    MiVoice Business Console has a Scratch Pad that allows the user to store user defined information. The information can be saved in a local plain text file.

NOTE: Data files are accessible to authorized attendants having the appropriate Windows credentials to log in to the PC running MiVoice Business Console. It is recommended that Windows accounts be assigned only to authorized attendants.

Personal data processed by MiVoice Business Console is required for the delivery of communication services, technical support services, or other customer business interests such as call billing and reporting services.

There are no end-user opt-in consent mechanisms implemented in the application.

4 Personal Data Transferred by MiVoice Business Console

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

- User provisioning data, such as name, phone number, location, and IP and MAC addresses are transferred between the MiVoice Business and MiVoice Business Console.
- Chat Presence and Chat Dialogs may be transferred between MiVoice Business Console and the MiCollab application server.
- User Messaging credentials are forwarded to the CloudLink Server but are not stored on the MiVoice Business Console. However, retrieved Tokens are stored to facilitate reconnecting to CloudLink on the next console start-up. MiVoice Business Console can be configured to automatically transfer software logs to Mitel product support or transferred to customer authorized log collecting systems through FTP.
- The MiVoice Business Console desktop PC can be configured to work in combination with Microsoft Active Directory to leverage Active Directory user accounts for access. The customer can then leverage Active Directory security mechanisms such as password strength and the account enable process.
- Call History information may be transferred between MiVoice Business Console and a PostgreSQL database provided/configured by the customer and residing on a remote computer.
- The PostgreSQL data transferred is not encrypted in transit.

5 How the Security Features Relate to Data Security Regulations

MiVoice Business Console provides security-related features which 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 which the customer may require to achieve compliance with data security regulations.

Table 1: MiVoice Business Console Security Features which 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 may be limited by allowing only authorised access to the Windows PC running MiVoice Business Console. Users created on the PC should use username/password login combinations that are based on strong password mechanisms. Mitel recommends using Microsoft Windows Authentication for added security measures leveraging the AD security rules; for example, account enable/disable, password rules, and login attempts. Voice Communications to the MiVoice Business system are performed over authenticated and encrypted communications channels using Secure MiNET. BitLocker (or a similar method) can be used for encryption of the local Windows desktop hard drive. A customer can further limit access over the network by using standard network security techniques such as VLANs, access control lists (ACLs), and firewalls.	Refer to the MiVoice Business Engineering Guidelines - Search for “MiVoice Business Console”. Refer to Windows OS Help. Online documentation can be found at: https://docs.microsoft.com/enus/windows/ For example: Setting the login thresholds can be found at: https://docs.microsoft.com/enus/windows/security/ threatprotection/security-policysettings/account-lockout-threshold

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
Communications Protection	**Voice Streaming** By default, MiVoice Business Console is configured to encrypt all IP voice call media streams with either Mitel SRTP or SRTP using AES 128 encryption. **Voice Call Signalling** MiVoice Business Console by default is configured to encrypt all Call Signalling with TLS/SSL. Secure Minet is also available when configured on the MIVB. **User Messaging** MiVoice Business Console may be configured to register with the Mitel MiCollab for Instant Messaging and presence updates. This mechanism uses HTTP and SIP, both of which are unencrypted when connected directly to MiCollab. These mechanisms can be encrypted by connecting MiVoice Business Console to a MiVoice Border Gateway. **User Messaging – CloudLink** MiVoice Business Console may be configured to register with Mitel CloudLink for Instant Messaging. This mechanism uses HTTPS by default.	Refer to the MiVoice Business Engineering Guidelines; search for "MiVoice Business Console".
Access and Authorization	All personal data can be protected with Windows access and authorization controls. Mitel recommends using Microsoft Windows Authentication for added security measures leveraging the AD security rules; for example, account enable/disable, password rules, and login attempts.	Refer to Windows OS Help. Online documentation can be found at: https://docs.microsoft.com/enus/windows/

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
Data Deletion	User data can be deleted either by uninstalling the MiVoice Business Console or by using Windows File Explorer to delete any logs or files that contain user data. It is possible to filter logs and disable logging completely by using the Problem Reporting settings in MiVoice Business Console. Call History records are stored on a customer configured and maintained PostgreSQL server. Data can be deleted from the PostgreSQL database. 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.	Refer to Administrator Help topics in MiVoice Business Console for details on Log Filter controls and how to delete logs files. Refer to “MiVoice Business Console Admin Help”, Section “Setting Up PostgreSQL 9.6 Database” on how to delete records.
End Customer Guidelines	MiVoice Business Console Security Guidelines are available to assist with installation, upgrades, and maintenance.	Refer to Mitel MiVoice Business Security Guidelines.

6 Data Security Regulations

This section provides an overview of the security regulations that MiVoice Business Console 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 appropriately safeguard such data. Table 1 explains what personal data is processed by Mitel's MiVoice Business Console 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 Console 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.