MiVoice Border Gateway – Personal Data Protection and Privacy Controls

MiVoice Border Gateway Release 11.2

Version 1.0

July 2021

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 MiVoice Border Gateway customers that are putting security processes and security controls in place to comply with GDPR.
This document is intended to assist Mitel MiVoice Border Gateway customers with their GDPR compliance initiatives by:

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

MiNet and SIP signaling security now defaults to TLS 1.2 on a new installation. On an upgrade, the previous setting is preserved. Certain weak ciphers have also been disabled in MBG 11.2.

2 Personal Data Collected by MiVoice Border Gateway

MiVoice Border Gateway 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 technical support services. There are no end user opt-in consent mechanisms implemented in MiVoice Border Gateway.

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

- End-users of MiVoice Border Gateway – typically customers of Mitel customers using Mitel phones and collaboration tools.
- 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 Border Gateway

MiVoice Border Gateway processes the following types of data:

- **Provisioning Data**
  - The end-user's business extension phone number, MAC address or SIP user name and password. A descriptive free-text field may include the user's name or other identifiers.
  - User credentials may be processed through the web proxy or port forwarding capability of the MiVoice Border Gateway.

- **Maintenance, Administration, and Technical Support Activity Records**
  - System and content backups, logs, and audit trails
  - IP addresses of administrator PCs, administrator and user names, and passwords

- **User Activity Records**
  - When connected, the user's current IP address is logged
  - Call signaling information is included in the application logs for diagnostics

- **User Personal Content**
  - User credentials may be processed through the web proxy or port forwarding capability of the MiVoice Border Gateway
  - Packet captures including call signaling and media may be created during troubleshooting
  - Voice and video transmissions may be proxied through the MiVoice Border Gateway

MiVoice Border Gateway processes only personal data that is required for the delivery of communication services, technical support services, or other customer business interests. For example, call billing and reporting services. There are no end-user opt-in consent mechanisms implemented in the application.

4 Personal Data Transferred by MiVoice Border Gateway

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

- **Provisioning Data**
  - Provisioning data including user names, passwords, IP addresses, MAC addresses, telephone extension numbers, and device descriptions is replicated among all nodes in a MiVoice Border Gateway cluster and may be shared with other applications using the MiVoice Border Gateway Provisioning API, such as MiCollab Client Deployment, Mitel Performance Analytics and MiCloud Management Gateway.

  - Provisioning data may be transferred to other systems as part of a system backup file or to Mitel as part of a Diagnostics upload for Product Technical Support.

- **Maintenance, Administration, and Technical Support Activity Records**
  - System logs, audit trails, and information on system usage may be transferred to another system as part of a backup or to Mitel as part of a Diagnostics upload for Product Technical Support.

- **User Activity Records and Personal Content**
  - Information about calls made and received may be transferred to another system as part of a backup or to Mitel as part of a Diagnostics upload for Product Technical Support.

- **Call Recording**
  - Recordings of calls may be transferred to authorized recording applications using the MiVoice Border Gateway Secure Recording Connector functionality of the MiVoice Border Gateway.

- **Remote Proxy Service**
  - The Remote Proxy Service may collect a user's personal data for user authentication. The information may include the user's username, password, first name, last name and address.

5 How the Security Features Relate to Data Security Regulations

MiVoice Border Gateway 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 can use when implementing both customer policy and technical and organizational measures that the customer may require to achieve GDPR compliance.

Table 1: MiVoice Border Gateway Security Features which customers may require to achieve Compliance with Data Security Regulations.

Security Feature	Relationship to GDPR	Where the Feature is Documented
System and Data Protection	Access to personal data is limited with administrative controls on accounts for both personnel and Application Programming Interfaces. **Administrator Access** Administrator access is secured by a user name and password with strength validation. All access is encrypted using SSH version 2 or HTTPS (TLS). Use of TLS 1.2 can be enforced. Access to the administrator web interface by default is limited to the directly attached local network. Access may be extended to other specific networks and hosts. SSH is disabled by default and should remain so unless needed for troubleshooting. SSH access can be limited to a list of authorized networks or hosts. Repeated failed login attempts to SSH result in a temporary ban of further login attempts from this IP address. **API Access** Applications may be individually authorized to connect through the Provisioning API or Secure Recording Connector. Provisioning API access is controlled by an OAuth enrollment mechanism for each application instance. Permissions may be assigned to each access token individually. Call recorders must enroll by submitting a Certificate Signing Request to a local Certificate Authority embedded in the product for this purpose. A unique certificate is issued to each call recorder, and used for TLS authentication. The use of TLS 1.2 can be forced by the Administrator via settings within Mitel Standard Linux.	The administrator account is described in the Mitel Standard Linux Installation and Administration Guide under “Configure the Server”. For information on TLS and SSH configuration, see the same document. The MiVoice Border Gateway Provisioning API specification and Secure Recording Connector Developer’s Guide are available through the MSA program.

Communications Protection	Most personal data transmissions use secure channels. Channels that are not secured can be disabled by the administrator. **Call Signaling** Both MiNet and SIP signaling can use TLS 1.2, and plaintext transports such as UDP can be turned off or restricted to specific networks. **Voice Media** Use of SRTP (AES 128) on both the WAN and LAN sides of calls being processed by the MiVoice Border Gateway can be enforced. **Web UI Access** All access to internal web interfaces through the Remote Proxy Service must use TLS. High-grade encryption is used. All low, medium, and export-grade cipher suites are disabled by default. For system integrity and reliability, all provisioning interfaces use secure channels. **API Access** Application access through the Provisioning API uses HTTPS (TLS) with high-grade cipher suites. Use of TLS 1.2 can be enforced. Application access through the Secure Recording Connector is encrypted with TLS. Use of TLS 1.2 can be enforced. Each application instance is authenticated with a unique certificate issued by the MiVoice Border Gateway administrator.	See Mitel Standard Linux Installation and Administration Guide, section “Server Manager”. The MiVoice Border Gateway Provisioning API specification and Secure Recording Connector Developer’s Guide are available through the MSA program.
Identity and Authentication	Access to the MiVoice Border Gateway is restricted by a login password. Access to the administrator UI is controlled by a user name and password. The password is subject to strength validation. There is no end-user access to MiVoice Border Gateway. Accounts are defined locally per server. Transmission of the login credentials is protected by TLS, and the password is stored as a secure hash.	Mitel Standard Linux Installation and Administration Guide under “Server Manager”.

Access and Authorization	There is no end-user (data subject) access to MiVoice Border Gateway. All personal data processing is limited to the local administrator account. Application access through the Provisioning API can be limited to specific subsets of the data by category, such as SIP trunks or MiNet devices. Access may be read-only or read-write per application. The Remote Proxy Service may be used to authenticate a user with a target application such as MiVoice Business Contact Center or AWV. Access to data files on disk requires administrator ('root') access. Sensitive data within disk files is encrypted. Access to the system shell is disabled by default. Mitel recommends its use only for troubleshooting.	The administrator account is described in the Mitel Standard Linux Installation and Administration Guide under "Configure the Server". The MiVoice Border Gateway Provisioning API specification is available through the MSA program.
Data Deletion	The system provides an administrator with the ability to erase the end-user's personal data. User data can be removed by deleting the user's account from the administrator web interface. User information in system logs is not removed by deleting an account. Log files are purged after a configurable retention period. Similarly, information in the Concurrent Signaling Capture diagnostics is not removed until the file is rotated out; each file grows to 200 MB and a configurable number (default 14) are retained. User information in backup files is not removed. Administrators should purge old backups and make a new backup without the end-user's personal data. Any recordings made of the user's calls must be deleted from the call recording application. Certain types of logs cannot be deleted on a per user basis such as audit logs. However, Mitel provides the administrator with the ability to delete the entire contents from all logs.	See the sections "Add or Edit MiNet Devices" and "Add or Edit SIP Devices" in the online Help for instructions on deleting user device data. See the "Logging" online Help for log and capture retention settings.

	• Call recording information that has been transferred to a call recording server is not deleted by this step. For information on how to delete recordings from these systems refer to the vendor's documentation. • 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.	
Audit	Audit trails are supported to maintain records of data processing activities. All changes made by administrator accounts and connected applications (through the Provisioning API), as well as all changes originating on other nodes of a MiVoice Border Gateway cluster are logged to the Audit Log. The audit log may be sent through syslog to a central site for aggregation and analysis. The audit log contains the IP address, administrator name or application token identifier, information on which objects were added/changed/removed, and the details of that operation. As such, the Audit Log may contain personal end-user information. The Audit Log can be accessed only by the administrator unless it has been sent to another server by syslog.	For MiVoice Border Gateway Release 10.1 and later, see the Installation and Maintenance Guide, section “Accessing Log Files” for details on the Audit Log.
End Customer Guidelines	MiVoice Border Gateway Engineering Guidelines are available to assist with installation, upgrades, and maintenance.	Details are available in various sections of the MiVoice Border Gateway Installation and Maintenance Guide, MiVoice Border Gateway Engineering Guidelines, and the online Help. The latest versions of these documents are available at: https://www.mitel.com/document-center

6 Data Security Regulations

This section provides an overview of the security regulations that MiVoice Border Gateway 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 Border Gateway 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 Publications

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 Border Gateway 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.