MiVoice Border Gateway as Deployed in Google Cloud – Personal Data Protection and Privacy Controls

MiVoice Border Gateway Release 11.1

Version 1

May 2020

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 Border Gateway as deployed in Google Cloud customers that are putting security processes and security controls in place to comply with GDPR in a MiCloud Flex, as delivered on Google Cloud, hosted offering. For onsite and hosted VMware based solutions, refer to version 11.0 in the Mitel Documentation Center.

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 as deployed in Google Cloud Security Features that customers may require to achieve GDPR compliance
- Providing a description of the MiVoice Border Gateway as deployed in Google Cloud Security Features
- Providing information on where the MiVoice Border Gateway as deployed in Google Cloud 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.

2 Personal Data Collected by MiVoice Border Gateway as deployed in Google Cloud

MiVoice Border Gateway Release 11.1 is made available only in a MiCloud Flex, as delivered on Google Cloud, hosted deployment. MiVoice Border Gateway only processes 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 as deployed in Google Cloud

The MiVoice Border Gateway processes the following types of data:

- **Provisioning Data:**
  - The end user's business extension phone number, MAC address or SIP username and password. A descriptive free-text field may include the user's name or other identifiers.
  - User credentials may be processed through the 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 usernames, 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 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 as deployed in Google Cloud

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, MiCollab End User services, Initial Configuration Wizard and Mitel Performance Analytics.
  - 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.

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 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 that Customers May Require to Achieve GDPR Compliance

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 through the Solution Manager, and communication channel encryption is enforced with TLS 1.2. **API Access** Provisioning API access is limited to clients providing a shared secret stored in the Kubernetes distributed key-value store (Etcd) as an encrypted secret. The Provisioning API is unavailable to third-party applications. Only Mitel Interaction Recording is authorized to connect to the Secure Recording Connector component of the MiVoice Border Gateway. Communication between Mitel's call recorders and MiVoice Border Gateway is encrypted based on AES-256 with shared secret.	The administrator account and access are described in the Solution Manager online Help. .
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. For TLS, high-grade ciphers are used. All low, medium, and export-grade cipher suites are disabled by default.	See the section "Update Configuration Settings" in the online Help for instructions on disabling plaintext transports.

	Voice Media Use of SRTP on both the WAN and LAN sides of calls being processed by the MiVoice Border Gateway can be enforced. **Web UI Access** High-grade ciphers are 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** The Provisioning API communication between clients and MiVoice Border Gateway is encrypted with TLS 1.2. The Provisioning API is unavailable to third-party applications. Communication between Mitel's call recorders and MiVoice Border Gateway is encrypted based on AES-256 with shared secret.	
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.	The administrator account and access are described in the Solution Manager online Help.
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. Access to date files on disk requires execution permission through Google's RBAC system for Kubernetes. SSH is not available and cannot be enabled. Sensitive data within disk files is encrypted at rest. Provisioning API is unavailable to third-party applications.	The administrator account and access are described in the Solution Manager online Help.

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 7 files are retained. User information stored in MiCloud Flex solution backup files is not removed. Contact Mitel in the event of a backup purge and create 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. • 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 Mitel Interaction Recording documentation. • Logs that are transferred to external or third-party systems, including Solutions Manager, are not deleted by this step. For information on how to delete logs from these systems, refer to the application specific documentation.	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.
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 contains the IP address, administrator name or application token identifier, information about which objects were added, changed, or	MiVoice Border Gateway audit logs are available as part of the MiVoice Border Gateway Fetch Logs and the Solution Manager logs bundle.

	removed, and the details of that operation. As such, the Audit Log may contain personal end-user information.	
End Customer Guidelines	MiVoice Border Gateway Security Guidelines are available to assist with installation, upgrades, and maintenance.	Details are available in various sections of the MiCloud Flex on Google Cloud Installation and Maintenance Guide and Engineering Guidelines and the MiVoice Border Gateway online Help. The latest versions of these documents are available in the Mitel Document Center 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, 'processing 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 organizations measures are used to appropriately 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