Open Integration Gateway – Personal Data Protection and Privacy Controls

Open Integration Gateway Release 4.2

Version 1.0

September 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 Open Integration Gateway (OIG) customers that are putting security processes and security controls in place to comply with data security regulations.

This document is intended to assist Mitel Open Integration Gateway (OIG) customers with their data security regulations compliance initiatives by:

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

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

1.2 What is New in this Release

1. EULA for the OVA deployment and while upgrading OIG from 'Blades' page of OIG Server is updated.
2. Mitel Standard Linux (MSL) has been upgraded to MSL 11. Refer to "Mitel Standard Linux Security Technical Paper" available in Doc Center of Mitel's Web Site.

2 Personal Data Collected by OIG

Mitel Open Integration Gateway runs as an application installed on an Industry Standard Server (ISS) or in a VMware® vSphere environment—in either Standalone single ESXi hypervisor or Managed by vCenter Server mode. The environment is accessed by the designated OIG administrators, using a web browser.

Mitel also offers applications that use the Mitel OIG: MiVoice Integration for Salesforce and MiVoice Integration for Google. Third-party applications can also be developed using OIG.

The security protocols are defined by Mitel Standard Linux (MSL), the base operating system on which the Mitel Open Integration Gateway resides.

During the course of installation, provisioning, operation and maintenance, the OIG **collects** data related to several types of users, including:

- End-users of the MiVoice Integration for Google application, who are typically Mitel customer employees using Mitel phones and collaboration tools.
    - Note that the MiVoice Integration for Salesforce does not collect any personal data.
- Customers of Mitel customers, who are end-users of the MiVoice Integration for Google application, and use Mitel phones and collaboration tools.
- OIG does not collect any personal data that is specific to third-party custom applications. Any data collection performed by third-party custom applications is outside of Mitel's control. End-users must consult with the application developer for guidance in understanding what personal data might get collected by the application.
- 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 OIG

The Open Integration Gateway **processes** the following types of data:

- **Provisioning Data:**
    - The end-user's name, email address, phone number, job title, geographic location, department, and language preferences.
    - OIG may require authentication to third-party services and certain permissions therein (such as access to contacts of a Google admin account).
- **Maintenance, Administration, and Technical Support Activity Records:**
    - System and content backups, logs, and audit trails.
- **User Activity Records:**
    - Call history and call detail records.
- **User Personal Content:**
    - Employment details (Job Title, Department, and Company Name) and Address (including city, state/province, and zip/postal code) of the end-user.

Personal data processed by the OIG, including name, phone number, and email address are required for the delivery of communication services, technical support services or other customer business interests, while employment and address details can be processed by the Open Integration Gateway administrator for record keeping purposes.

OIG processes third-party services and certain permissions, solely to obtain access to information stored in Google administrator’s account for the purpose of setting up or tearing down VoIP calls. MiVoice Integration for Google plugin may read and write notes you enter about your calls and contacts into your third-party accounts.

Mitel Integration for Google plugin supports end-user opt-in consent mechanism. There are no other end-user opt-in consent mechanisms implemented in Open Integration Gateway.

4 Personal Data Transferred by OIG

The types of **personal data transferred** among the Open Integration Gateway and the MiVoice Integration with Google application and services will depend on the specific use requirements of those applications or services, for example:

- **Provisioning Data:**
  - Such as name, phone number, and email address.
- **Maintenance, Administration, and Technical Support Activity Records:**
  - System logs and database records 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 (if authorized by the administrator) may be transferred to another system as part of a backup or to Mitel as part of a Diagnostics upload for Product Technical Support.

Note that MiVoice Integration for Salesforce does not query, collect, or store personal data. In addition, no personal data is queried, collected or stored by OIG from third-party applications using OIG services.

OIG may transfer personal data that is specific to third-party custom applications. Any data transfer to the third-party custom application(s) is outside of Mitel's control. End-users must consult with the application developer for guidance to understand what personal data might get transferred to the application.

5 How the Security Features Relate to Data Security Regulations

Open Integration Gateway 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: OIG 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 is limited to Administrator, who is authenticated using a user name/password login combination that uses strong password mechanisms. All communications are encrypted using OpenSSH 7.4 or HTTPS (TLS). TLS 1.2 is enabled by default. 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 log in attempts to SSH results in a temporary ban of further log in attempts from the IP address. The communication and access can be further limited over the network using standard network security techniques such as firewalls or web-proxies. **API Access** Third-party applications are individually authorized to connect to OIG with a 2-step process of identification and authorization check. 1. Each application needs to be registered as a standard or advanced application with Mitel Certificate Server (MCS) which is maintained by Mitel. Upon registration, it needs to be approved by Mitel. 2. Once approved, the application will be available under the list of "Available Applications" on the OIG Server. The	Details are available in the "Client Station Support" and the "Installing the Mitel OIG" sections of OIG Installation and Maintenance Guide available in the Mitel Document Center at www.mitel.com.

	OIG administrator needs to create a local password for the application before adding it as one of the Allowed applications. Only then can the application access the OIG server services by providing the local password. Thereafter, applications can access API services as well. A unique certificate is issued to OIG and used for TLS authentication.	
Communications Protection	Personal data transmissions use secure channels. The security protocols are defined by Mitel Standard Linux (MSL), the base operating system on which the Mitel Open Integration Gateway resides. The authentication mechanism for the MiVoice Integration for Google application attempting connection with the Open Integration Gateway server is controlled and maintained by the Open Integration Gateway administrator. • MiVoice Integration for Google must be added to the list of Allowed Applications by the Open Integration Gateway administrator to the Open Integration Gateway server and configured with a local password to authenticate the application. • Mitel Open Integration Gateway server must be configured to use a CA certificate when end-users are using the MiVoice Integration for Google application. For system integrity and reliability, all provisioning interfaces use secure channels. Channels that are not secured can be disabled by the administrator. Remote access to the OIG Server can be limited using security techniques such as firewalls or web proxies. **API Access** For communications security Mitel recommends that the OIG administrator enforces the use of TLS 1.2 if the connecting applications support it.	• See the "Application Accounts Tab" section of OIG Installation and Maintenance Guide available in the Mitel Document Center at www.mitel.com. • See the "Use Third-Party Trusted CA Certificates" section of OIG Installation and Maintenance Guide available in the Mitel Document Center at www.mitel.com. • See the "Manage TLS Protocol" section of Mitel Standard Linux Installation and Administration Guide available in the Mitel Document Center at www.mitel.com.

	Third-party applications are individually authorized to connect to OIG with a two-step process of identification and authorization check. 1. Each application needs to be registered as a standard or advanced application with Mitel Certificate Server (MCS) which is maintained by Mitel. Upon registration, it needs to be approved by Mitel. Once approved, the application will be available under the list of "Available Applications" on the OIG Server. OIG administrator needs to create a local password to the application before adding it as one of the Allowed applications. Only then can the application access the OIG server services by providing the local password. Hereafter, applications can access API services as well. A unique certificate is issued to OIG and used for TLS authentication.	
Access and Authorization	There is no end-user (data subject) access to OIG allowed. Only the administrator is allowed to access the OIG server. All personal data processing, system data processing, and all access to databases, files, and operating systems are protected with administrative access and authorization controls. Passwords are encrypted with AES-128. Failed log in attempts is logged. A customer can further limit access over the network using standard network security techniques such as firewalls and web-proxies. In all cases, physical access to systems should be restricted by the customer.	Details are available in the "Client Station Support" and the "Installing the Mitel OIG" sections of OIG Installation and Maintenance Guide available in the Mitel Document Center at www.mitel.com.
Data Deletion	The system provides the administrator with the ability to erase the end-user's personal data. The Users tab contains the functions for importing and exporting user lists. To remove any row of end-user's details from the directory, the User's list is exported (as a CSV file) and then uploaded (as a CSV file) with the "mark_as_delete" column set to Yes for the respective row for which details must be deleted.	Details are available in the "Users Tab" section of OIG Installation and Maintenance Guide available in the Mitel Document Center at www.mitel.com.

	User information in system logs is not removed by deleting an account. Log files are purged after a configurable retention period. 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.	
Audit	The security protocols are defined by Mitel Standard Linux (MSL), the base operating system on which the Mitel Open Integration Gateway resides. MSL includes a syslog server for message logging. When a system event occurs, such as a failed authentication attempt or a login failure, the affected service generates a message, which is recorded in a log file. These logs can be accessed only by the Open Integration Gateway server administrator.	See the "Syslog Server" section of Mitel Standard Linux Installation and Administration Guide available in the Mitel Document Center at www.mitel.com.
End-Customer Guidelines	• Open Integration Gateway Guidelines are available to assist with installation, upgrades, and maintenance of MSL. • The security protocols are defined by Mitel Standard Linux (MSL), the base operating system on which the Mitel Open Integration Gateway resides. To keep updated with security features, MSL distributes security patches through the Blades panel.	• See the "Installing Mitel OIG", "Configure Mitel OIG" and the "Upgrading Mitel OIG" sections of OIG Installation and Maintenance Guide available in the Mitel Document Center at www.mitel.com. • See the "What's New In This Release" section of Mitel Standard Linux Installation and Administration Guide available in the Mitel Document Center at www.mitel.com.

6 Data Security Regulations

This section provides an overview of the security regulations that OIG 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 Open Integration 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 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, 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 OIG 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.