Mitel Alarm Server– Personal Data Protection and Privacy Controls

Mitel Alarm Server Release 4.1

Version 1.3

January 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

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information.

For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/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 Mitel Alarm Server customers that are putting security processes and security controls in place to comply with with data security regulations.

This document is intended to assist Mitel Alarm Server customers with their data security regulations compliance initiatives by:

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

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

1.2 What is New in this Release

The cipher suites / TLS versions used for encryption of incoming and outgoing E-Mails can be configured.

2 Personal Data Collected by Mitel Alarm Server

During the course of installation, provisioning, operation and maintenance, the Mitel Alarm Server collects data related to several types of users, including:

- End-users of Mitel Alarm Server – typically Mitel customer employees or customers using Mitel phones or other devices that may trigger or process alarms and related notifications.
- System administrators and technical support personnel – logs and traces contain records of the activities of system administrators and technical support personnel.

3 Personal Data Processed by Mitel Alarm Server

The Mitel Alarm Server processes the following types of data:

- **Provisioning Data:**
    - The end-user's name, business extension phone number, mobile phone number, email address, and the location in site hierarchy; for example, the user's role or title, team, department, and the building or room that the user is located in.
- **Maintenance, Administration, and Technical Support Activity Records:**
    - System and content backups (secured with password), logs, and diagnostic debug trace logs.
- **User Activity Records:**
    - Data on user-generated events that trigger alarms or indicate activity. This can include physical location information.
    - Data on the delivery of alarm messages.
- **User Personal Settings:**
    - Service settings (login password, PIN, and display language).
- **User Personal Content:**
    - Alarm related data (text messages and voice recordings).
- **User Device Related Data:**
    - User device login, language, position of DECT handset (based on closes DECT base station), and charger status of DECT handset.

The Mitel Alarm Server processes only personal data that is required for the delivery of alarm handling and messaging services, technical support services, or other customer business interests.

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

4 Personal Data Transferred by Mitel Alarm Server

The types of personal data transferred among the Mitel Alarm Server and various applications and services will depend on the specific use requirements of those applications or services, for example:

- **Alarm Notifications**
    - Messages that indicate that an alarm has been sent to users. Depending on the configuration, these messages contain information about the event that triggered the alarms. (User-related information such as name, phone number, current location, type of the alarm, and additional user-defined text.)

- **Provisioning data**
  - The Alarm Server reads provisioning data from connected call managers (name, phone number, language, and phone type) and this data can be used to create alarm notifications.
- **Activity data**
  - The Alarm Server monitors phone activity (for example, busy, logon/logoff, in charger, and location). This data is used for alarm processing.
- **Maintenance, Administration, and Technical Support Activity Records**
  - System and content backups, logs, and diagnostic debug trace logs.
  - System management activity such as login and logout records may be transferred to a customer authorized secondary storage or to technical support personnel.
- **Protocol export**
  - A protocol containing alarm events, alarm responses, event time stamps, name or phone number of the user who triggered the alarm, type of alarm and the user's physical location can manually be exported in a machine-readable format by users having the rights to do this. For each alarm, one or many notifications may be sent to users or devices. The protocol contains information about the delivery of the notifications and potential user responses (accept, reject).
- **Automated backup**
  - A scheduled automated backup can be used to transfer a copy of the configuration and the alarm protocol data to a customer-authorized external storage system.

5 How the Security Features Relate to Data Security Regulations

The Mitel Alarm Server 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 compliance with data security regulations.

Table 1: Mitel Alarm Server 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 on accounts. The Mitel Alarm Server has a role-based access control system. This allows controlling who can view or edit personal data, export data change access rights.	Mitel Alarm Server—System Manual Release 4.0, *Chapter 7.3*
Communications Protection	Most personal data transmissions use secure channels. Channels to external systems that are not secured have to be explicitly enabled by the administrator. The exchange of data with connected systems is done through the following secure channels: • Mitel SIP-DECT (TLS) • E-Mail (TLS 1.1/1.2, version can be configured with configurable cipher suits) Communications over legacy interfaces may be unsecured.	Mitel Alarm Server—System Manual Release 4.0, *Chapter 5* Mitel Alarm Server — System Manual Addendum Release 4.1, Chapter *5.2*

	The administrator must explicitly enable these interfaces. Unsecured communication is used on the following interfaces: • ESPA 4.4.4, ESPA-X • NMEA for incoming GPS data • SIP connection to call manager • AudioUnit • ModBus • SIP Phones • WEB Alarm • GPS Access to the web portal of the Alarm Server is handled with HTTP.	
Identity and Authentication	Access to the Mitel Alarm Server is restricted by a login password. Access to the system is limited by allowing only authorized access that is authenticated using strong username/password login combinations. Failed login attempts are logged but are not restricted to a maximum of attempts. Access to phone menus is restricted with PINs.	Mitel Alarm Server—System Manual Release 4.0, *Chapter 7.3*
Access and Authorization	All personal data processing is protected with role-based access and authorization controls, this includes personal data processing by data subjects, administrators, and technical support. A strong password is required, and failed login attempts are logged. All system data processing and all access to databases, files, and	Mitel Alarm Server—System Manual Release 4.0, *Chapter 7.3*

	operating systems, are protected with role-based access and authorization controls. A strong password is required, and failed login attempts are logged. 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 systems (server with virtual machine) should be restricted by the customer.	
Data Deletion	The system provides an administrator with the ability to erase the end-user's personal data. Technical logs and traces cannot be deleted explicitly. A rotation mechanism ensures that old data is removed if a maximum storage size for logs is reached. The Alarm Server can be configured to automatically delete protocol data that is older than a configurable number of days. All user (alarm protocol, log files) and configuration data can be deleted using the function to restore Factory Defaults. VMware snapshots can be used to save and restore machine states including software, configuration and data.	**Protocol Maintenance** Mitel Alarm Server—System Manual Release 4.0, *Chapter 4.3.3* **Restore Factory Defaults** Mitel Alarm Server—System Manual Release 4.0, *Chapter 4.1.2* Mitel Alarm Server — System Manual Addendum Release 4.1, Chapter *2.4*
Audit	Information about user authentication (including failed attempts) and actions concerning user management are written to the log file of the	Mitel Alarm Server — System Manual Addendum Release 4.1, *Chapter 5.1*

	Alarm Server. This includes any changes of groups and their assignment to users. Logins via the configuration and changes or actions initiated via this tool are also logged. This includes configuration updates, software updates and the restart of the Alarm Server.	
End-Customer Guidelines	Information about security configuration is available to assist with installation, upgrades, and maintenance in the guide.	Mitel Alarm Server — System Manual Addendum Release 4.1

6 Data Security Regulations

This section provides an overview of the security regulations that Mitel Alarm Server 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 Mitel's Alarm Server 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 Mitel Alarm Server 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.