Mitel Alarm Server

RELEASE 4.1

VERSION 1.2

SECURITY GUIDELINES

NOTICE

TRADEMARKS

Mitel Alarm Server
Security Guidelines
Release 4.1
Version 1.2
January 2021

Overview/Introduction

This document provides an overview of the security mechanisms available to protect the Mitel Alarm Server from network threats and maintain user data privacy. This document will be of interest to personnel who are responsible for ensuring the secure deployment and the secure operation of the Mitel Alarm Server.

Every organization should have a clearly defined IT security policy in place, defining goals, assets, trust levels, processes, incident handling procedures, and so on. The security mechanisms available in the Mitel Alarm Server should be covered by and configured according to this policy.

Security is an integral part of the Mitel Alarm Server system design; this document describes the Mitel Alarm Server security features and provides recommendations on how the administrator should configure the security features to ensure a secure Mitel Alarm Server deployment.

The Mitel Alarm Server security features are enabled in the system by default, enabled during the installation/configuration phase of the system, or need to be enabled manually by the system admin when the Mitel Alarm Server system is initialized.

The Mitel Alarm Server security measures are mainly based on the following open standard technologies and access management mechanisms:

- TLS – Transport Layer Security provides secure access to Email and secure signaling between the Email Server and the Mitel Alarm Server.
- Correct configuration of identity and access management policies to secure all end-user and administrator accounts, roles, permissions and password policies.

Other mechanisms that can be employed to protect the Mitel Alarm Server are based on the following:

- Configuration of external public facing routers and firewalls

An important security measure is to establish and maintain physical security. Only authorized personnel should have access to server locations because many data-exposure attacks can be mounted by having physical access to a host. Further, the IT data infrastructure should be designed with security in focus; security mechanisms and protocols should be enabled, and all components of the whole system must be correctly configured, maintained, and updated, as necessary.

About the Mitel Alarm Server Documentation Set

Documents for Mitel Alarm Server are available after installing administration tool.

The following documents provide complete information about the Mitel Alarm Server*:*

- Alarm Server System Manual (depl-2544)
- Alarm Server System Manual Addendum (depl-2607)
- Alarm Server EULA (depl-2608)

The Mitel Alarm Server provides an integrated, web-based system administration tool and an installable administration tool.

Product Architecture

The Mitel Alarm Server is an IP-based server for professional use. The system can be expanded with interfaces and licenses.

The current releases 3.1 and 4.0 are available for the general market as ready to run hardware appliances with preinstalled software or as virtual machine images.

Release 4.1 of the Mitel Alarm Server is an industry-specific release for cruise ships that are primarily used for tourist purposes. This release is available only as a virtual machine image to be used in a VMware environment. The Mitel Alarm Server covers the growing demand for solutions in the cruise business. It is an open system that supports global standards and can therefore be easily integrated into a VMware infrastructure. Mitel Alarm Server supports the integration of Mitel and third-party systems and protocols: SIP-DECT, GPS (NMEA), Email, ESPA 4.4.4, ESPA-X, SIP, and ModBus with all their advantages. Additional gateways (for example, IP/RS232) may be needed to connect to legacy system.

Security Overview

The Mitel Alarm Server has been designed in accordance with Mitel's Secure Development Life Cycle (MiSDLC). For further details, see the section called Secure Development Life Cycle in this document. The Mitel Alarm Server has security features that address identity, authentication, encryption, and access and authorization.

Mitel Alarm Server also supports access and alarm and event logs.

The Mitel Alarm Server security features are configured via the configurator, an installable system administration tool on client side.

Securing the Operating System

Operating System Overview

- Mitel Alarm Server software is installed on top of the CentOS Linux release 7.9.2009. The kernel version is 3.10.0-1160.6.1.el7.x86_64.
- Mitel Alarm Server software (RPM) can be installed and updated.
- The installed rpm runs in a docker container.

As with all systems, the location of the solution must be physically secured from unauthorized access.

Operating System Related Network Controls

In their default initial state, the configuration of the Mitel Alarm Server offers only the minimum required access to set up and configure the system. The Administration of Mitel Alarm Server is via a browser which allows access to the system using a default username and password that the customer (administrator) must change when first accessing the system.

Network access is reduced to a minimum and can be configured by the customer (administrator):

- The Administration access to the operating system is secured with TLS v1.2 as standard.

Note: Mitel strongly recommends that you use network security mechanisms in the VMware host to restrict access only to devices that require these services; for example, Access Control Lists and Firewall rules.

Administration

Administration and Management Tools

The Mitel Alarm Server provides the customer with the following server-/client-administration and management tools:

Administration via browser:

- Web-based, integrated configuration tool for monitoring the Mitel Alarm Server system:
  - System- and alarm protocols
- Switch GUI languages: DE, DA, EN, FR, NL
- Limited configuration:
  - Supervision alarm
  - Alarm activation, cancelling and information
  - Handle DECT frequency switch of connected Mitel SIP-DECT system
  - User and user groups
- Access control with user accounts
- Managing user data such as email address, password
- Integrated in the server software package

Configurator (client installation):

- Client-based executable for admins
- Expert and Default view
- Security configuration (TLS Cipher Suites)
- Configuration of several interfaces:
  - Mitel SIP-DECT
  - Audio Unit
  - E-Mail
  - ESPA, ESPA-X
  - ModBus
  - Sip Phones
  - GPS
  - Web Alarm
- Configuration of:
  - Alarm/Event types
  - Notification profiles
  - Notification groups
  - Escalation plans
  - WEB alarm templates
  - Supervision alarms
  - Environments

These two different management tools are provided in order to meet the needs of technicians, administrators, and the Mitel Alarm Server users themselves.

Administration Encryption

The Administration via browser is accessed through HTTP on TCP port 80, which must be allowed through any data network local access control list or firewall. Mitel Alarm Server utilizes Transport Layer Security (TLS).

Note: By default, Mitel Alarm Server is initially configured to support only TLS 1.2 for the entire system (E-Mail). If older Email Server, are to be used, TLS 1.1 will also need to be activated in configurator (TLS Cipher Suites).

The following encryption modules are available in the Cipher Suite of Mitel Alarm Server by default:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_SEED_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM

In the unlikely situation that requires a cipher to be removed, contact Mitel technical support.

Identity, Authentication, Profiles, and Password Policies

To ensure privacy and maintain system integrity, access to the Mitel Alarm Server is restricted by a login password to those users that can be correctly identified and authenticated. Users will be forced to change the factory default password to a password of their choosing.

The Administration via browser is used to create or change a user account.

Recommendation

It is recommended to restrict physical access to the Mitel Alarm Server system to authorized personnel.

Each user account must be linked with an authorization profile. Authorization profiles determine the users' access rights. A series of standard profiles are available. The admin can change and create new authorization profiles.

There is one predefined user account that is required for certain applications. This account cannot be deleted. For example, the predefined user account “admin” is intended for operating WEB access. The predefined user account cannot be deleted.

The password strength rules are fixed and cannot be changed:

- A password must consist of a minimum of 8 and a maximum of 255 characters.
- Unlike the user names, the passwords are case sensitive.
- The default password “admin” is not permitted.

Recommendation

It is recommended that a strong password is used. The password should be changed regularly (for example, every 30 or 60 days).

If the user (admin) login for the first time after installation, the user has to change the default password.

If a user fails a log in attempt, the event is recorded in the access log.

Access and Authorization

For privacy, all personal data processing is protected with role-based access and authorization controls, which include personal data processing by data subjects, administrators and technical support. For system integrity and reliability, including the controls that protect privacy, all system data processing, and all access to databases, files and operating systems, are protected with role-based access and authorization controls.

In the Mitel Alarm Server, there are two forms used to administer access and authorization: The *User Account* form and the *User Groups* form. A description of these two forms follows.

User Account Form

Purpose

The *User Account* form is used by the system admin to create, modify, and delete additional user accounts:

- Login name
- Password / Password confirmation
- Username
- Phone
- Start page (for first view with WEB browser after logging in)

- User group
- Environment

User Group Form

Purpose

The admin uses the *user group* form to perform the following tasks:

- Creating/changing user groups
    - User Administration
    - Receive Notifications
    - Roles Operation
        - Alarms
            - Trigger alarm
            - Cancel all alarms/presences
            - Forward Alarm (operator)
        - Cameras
        - Phones
            - Trigger alarm
            - Locating Alert
        - Contacts
        - Protocol
    - Roles Administration
        - User
            - Edit User
        - User groups
            - Edit groups
        - Plans
            - Disable plan
        - Supervision Alarms
        - DECT Frequency
    - Roles System
        - Interfaces
            - Restart
        - Phones System
        - Protocol
        - Monitor

Recommendation

- It is recommended that the admin creates a user group form. The admin should establish Mitel Alarm Server user group profiles that comply with the company policy and business requirements.
- The admin must create temporary user group forms to support maintenance and/or troubleshooting activities. The authorization profiles must be deleted once the activities have completed.
- When a user is no longer an employee of the company, the admin should delete all of that user's credentials.

Audit and Log Reporting

Several audit trails and access logging capabilities are supported to maintain records of data processing activities and system accesses.

Purpose

The *Access Logs* form provides a historical record of access attempts and configuration changes from Administration via browser and various other user interfaces and applications.

- In general, login/logout attempts and any action from any user interface connected to Mitel Alarm Server that results in a change to the system database is logged.
  Access logs are included in the system backup.

The user interfaces audited for database changes and logins/logouts are as follows:

- Administration via browser (create/change/delete: user, user groups)

The user actions audited are:

- Logins and logouts, both successful and unsuccessful attempts
- Maintenance operations

Note: The Mitel Alarm Server does not allow the admin to delete the access logs.

Network Alarms, Monitoring, Supervision

The Mitel Alarm Server supports system supervision with event notifications to multiple interfaces such as SIP-DECT, GPS (NMEA), Email, ESPA 4.4.4, ESPA-X, SIP, and ModBus.

The Mitel Alarm Server generates an event message every time an event or error occurs. This message is written in the system database and can be downloaded at any time by authorized persons.

Event messages can be sent as an alarm to the endpoints of various interfaces (configurable via configurator) to the configured recipient.

Network Security

The Mitel Alarm Server and associated components communicate using the corporate network infrastructure.

Network Access Security

As with any network-attached device or application, the connection can potentially be accessed by unauthorized persons (“hackers”). If network access is not restricted, a bad actor can attempt to access the Mitel Alarm Server system and misuse it for their gain, for example, Toll Fraud. Unauthorized access can be from the outside (as from the WAN or from the Internet) when an access to the company’s data network has been permitted and also from an internal user. In both cases, the network access must be limited to only authorized personnel.

Note: Mitel Alarm Server systems are not designed to be connected directly to the Internet or a WAN. The Mitel Alarm Server must be deployed behind a reliable and secure firewall. It is strongly recommended to access control lists to limit the access to the Mitel Alarm Server.

Network components

It is recommended that the Ethernet LAN switches used to provide IP phones with LAN connectivity be managed, enterprise-grade switches that include integrated access control measures. It is also recommended that the system administrator ensure that the switch access control measures are properly configured and maintained. IP Port information follows below.

Wireless networks must also employ access control measures and user authentication mechanisms with a minimum of WPA2 encryption and a separate SSID for voice applications. SSID to VLAN mapping is recommended.

IP Ports

The following table shows the TCP/UDP ports used by the Mitel Alarm Server to communicate with IP phones and other components of the Mitel Alarm Server solution.

Port (Range)	Service	Transport Protocol	Initial data sent ←from / →to peer	Link Type AS – Alarm Server
22	Secure Shell	TCP	←	AS ← PC
25	SMTP client	TCP	→	AS → SMTP Server
80	HTTP	TCP	←	AS ← PC (Administration via browser)
110	POP3 client	TCP	→	AS → POP3 Server
143	IMAP client	TCP	→	AS → IMAP Server
465	SMTPS client	TCP	→	AS → SMTP Server
502[1]	ModBus client	TCP	→	AS → ModBus controller
993	IMAP (SSL/TLS)	TCP	→	AS → IMAP Server
995	POP3 (SSL/TLS)	TCP	→	AS → POP3 Server
2016[1]	ESPA-X server	TCP	←	AS ← ESPA-X Client
5060	SIP Service	UDP/TCP	→	AS → Call manager
12622	SIP-DECT (OMM AXI) client	TCP	→	AS → SIP-DECT OMM
68	DHCP client	UDP	→	AS → DHCP Server
2222	Secure Remote Management	TCP	→	AS → SRM Server

[1] Default port can be changed by administrator.

Prevention of Toll Abuse

Any communication system that has a combination of Recorded Announcement Devices groups or voice mail can be susceptible to toll abuse if not configured correctly. Therefore, it is important to assign appropriate telephone privileges and restrictions to devices. The use of Direct Inward System Access (DISA) is not recommended.

In addition, publicly accessible telephones should be denied toll access unless authorized through an attendant.

Product Hardening for Security during Development

Secure Development Life Cycle

Security and privacy threats are constantly being developed and existing threats are always evolving. To combat these threats, product designers need to continuously evaluate product security risks and ensure that robust controls are included in the design. The practice of evaluating security risks and incorporating protective measures into the design must be an integral part of the product design process itself.

Mitel's Secure Development Life Cycle (SDLC) policy was created to ensure that product developers will employ the latest security and privacy best practices throughout the entire product development process.

Mitel Alarm Server Release 4.1 was developed in accordance with Mitel's Secure Development Life Cycle policy. As a result, Mitel Alarm Server Release 4.1 has been designed with best-practice safeguards to mitigate risks to the confidentiality, integrity and/or availability of data contained within Mitel Alarm Server and to the data related to the functionality provided by Mitel Alarm Server.

Miscellaneous Recommendations

System Security Options

Different configurator forms under *General Settings* are used to specify parameters that are used system-wide and contains a number of security-related settings, which are as follows:

- Delete protocol entries older than 1-300 days: The default setting is "no”
- Delete Backup files after 1-30 Days: The default setting is "no”
- Plans (Escalation-) may be switched off by user: The default setting is "No”
- Email SSL/TLS can be activated: The default setting is "no”
- Compatibility mode for TLS v1.1 and TLS v1.2 – The default setting is TLS v1.2 (TLS Cipher Suites: High security)
- Save system data – Backup interval: An automatic data backup is possible every full hour every day. The default setting is "no”

Recommendation

It is recommended that the admin review all these options and set the controls as appropriate for their network.

Anti-Virus Protection

Applications such as Mitel Alarm Server must process data in real-time. Real-time applications require unfettered access to processor resources, memory systems, disk drive accesses, and network communications. When Mitel Alarm Server is deployed on virtual machines – as per Standard Linux and Antivirus Software - Guidelines (see Mitel’s Knowledge Management System 1W05) – the machine's resources will have been sized to ensure that the applications will have unrestricted and timely access to the resources that they require. Because these real-time data processing applications execute on carefully sized computing platforms, the installation of antivirus software is not recommended.

Securing Docker container in CentOS

The Mitel Alarm Server software runs in a Docker container on a CentOS 7 based system. In this Docker container, the base is openjdk:8-jre. OpenJDK is an open-source implementation of the Java Platform. Because containers use a common kernel in most cases, namely the kernel of the operating system, there is a general risk that several containers will be compromised at the same time if a container on a host is attacked. This is less likely with VMs in which each VM uses its own operating system.

Additional measures can be taken to secure the CentOS platform and the Mitel Alarm Server application executing on the platform. These measures are based on well-known network security best practices. In general, a platform that is both physically secure and installed in network that has been securely designed will have a low likelihood of being infected compared to a platform that lacks physical security and/or is installed in a network lacking security controls.

Appendix A – Mitel Alarm Server – Personal Data Protection and Privacy Controls

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.

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 and 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.

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 Mitel 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.

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.

The following table summarizes the security features Mitel customers can use when implementing both customer policy and technical and organizational measures that customers may require to achieve GDPR compliance.

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. 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	Mitel Alarm Server—System Manual Release 4.0, *Chapter 5* Mitel Alarm Server — System Manual Addendum Release 4.1, Chapter *5.2*

	• 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 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.	Mitel Alarm Server—System Manual Release 4.0, *Chapter 7.3*

	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 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.	Mitel Alarm Server — System Manual Addendum Release 4.1, *Chapter 5.1*
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