SIP-DECT

RELEASE 9.1SP1

VERSION 1.0

SECURITY GUIDELINES

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 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

SIP-DECT
Security Guidelines
Release 9.1SP1
Version 0.1
June, 2024

List of Figures

List of Tables

Overview/Introduction

This document provides an overview of the security mechanisms available to protect the SIP-DECT solution 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 SIP-DECT.

Every organization should have a clearly defined IT security policy in place, defining goals, assets, trust levels, processes, incident handling procedures, etc. The security mechanisms available in the SIP-DECT solution should be covered by and configured according to this policy.

Security is an integral part of the SIP-DECT system design; this document describes the SIP-DECT security features and also provides recommendations as to how the administrator should configure the security features to ensure a secure SIP-DECT deployment.

The SIP-DECT security features are enabled in the system by default for new installations. After upgrading SIP-DECT software, the software might support some enhanced or additional security controls. The administrator may need to change the configuration to take advantage of the advanced secure settings.

The SIP-DECT security measures are mainly based on the following open standard technologies and access management mechanisms:

- TLS – Transport Layer Security (TLS) provides secure signaling between SIP-DECT and call server nodes. The Transport Layer Security (TLS) provides secure web access to SIP-DECT administration of the OpenMobility Manager (OMM) and the Multi OMM Manager (MOM).
- SSH - Secure Shell (SSH) provides secure console-based access to the OMM and IP-RFP.
- SRTP - Secure Real-time Transport Protocol (SRTP) is used to protect the voice media streams between SIP-DECT IP-RFP and the other voice party.
- DSC – DECT Standard Cipher provides secure signaling and voice media streams between a SIP-DECT IP-RFP and a DECT phone.
- DSAA – DECT Standard Authentication Algorithm secures the authentication of a DECT Phone by the OMM for each connection establishment over the air.
- Blowfish encryption – Used for SIP-DECT internal communication between the different hardware entities OpenMobility Manager (OMM) and IP-RFP (radio base stations) for configuration and voice signaling. The OMM and the IP-RFP share an individual key on the first registration of the IP-RFP in the OMM.

The SIP-DECT product is designed to be installed in a Local Area Network (LAN) or a secure corporate network only. One important security measure is to establish and maintain physical security. Only authorized personnel must have access to server locations because many data-exposure attacks can be perpetrated by unauthorized physical access to a host device. Further, the IT data infrastructure should be designed with security in mind.

Other mechanisms that can be employed to protect the SIP-DECT are based on the following:

- A securely designed corporate Local Area Network (LAN) infrastructure
- Configuration of internal and external public facing routers and firewalls
- Security mechanisms and protocols must be enabled, and all components of the whole system must be correctly configured, maintained, and updated as necessary.

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 SIP-DECT solution should be covered by and configured according to this policy.

In addition to the security recommendations described in this document, there are a number of general security aspects that should be addressed by the system administrator and/or the Information Technology (IT) security officer.

An important security measure is to establish and maintain physical security. Only authorized personnel should have access to server locations, since 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 mind, security mechanisms and protocols should be enabled, and all components of the whole system should be correctly configured and maintained and updated as necessary.

About the SIP-DECT Documentation Set

Documents for SIP-DECT and other Mitel® products are available on the Mitel Document Center web site.

https://www.mitel.com/document-center

The Mitel Document Center web site can also be accessed by anyone with a miaccess.mitel.com account via the MiAccess Portal.

The following documents provide complete information about the SIP-DECT:

- Mitel 600 DECT Phone User Guide
- Mitel 600 DECT Phone Messaging and Alerting Applications User Guide
- SIP-DECT Personal Data Protection and Privacy Control
- SIP-DECT Integrated Message and Alerting Application Administration Guide
- SIP-DECT OM System Manual Administration Guide
- SIP-DECT LINUX Server Installation Administration Guide
- SIP-DECT Phone Sharing and Provisioning Administration Guide
- SIP-DECT User Monitoring Administration Guide
- SIP-DECT Multi OM Manager Administration Guide
- SIP-DECT Event Manager System Manual

The following documents are available via the Mitel Solutions Alliance (MSA).

- SIP-DECT OM Application XML Interface
- SIP-DECT XML Terminal Interface for Mitel 600 DECT Phone Family

What is New in this Release

With Release 9.1SP1, Mitel introduces the SIP-DECT Event Manager as an integrated software component of the SIP-DECT system. It is used for the automated processing of incoming events and the sending of outgoing notifications. The SIP-DECT Event Manager can process events from various sources, including SIP-DECT end devices, the SIP-DECT system itself and other external systems. .

Product Architecture

Mitel® SIP-DECT is a VoIP SIP solution for the on-site business voice mobility market and uses the **D**igital **E**nhanced **C**ordless **T**elephony technology. It includes the following main components:

- SIP-DECT base stations: Also called Radio Fixed Parts (RFPs). These are distributed over an IP network and offer DECT, WLAN, and IP interfaces via Ethernet
- DECT phones (wireless DECT devices)
- Open Mobility Manager (OMM): Management and signaling software for the SIP-DECT solution, which runs on one of the DECT base stations (Figure 1), or OMM, which runs on a Linux server (VM or dedicated HW) (Figure 2)
- Multi-OMM Manager (MOM): Management software to combine up to 500 OMMs to provide a central user and device management of up to 50000 users/devices. This enables user and device roaming between OMMs. The MOM provides configuration file generation for centralized OMM provisioning. The MOM runs on a Linux server (VM or dedicated HW) (Figure 4).

The OMM and the RFPs communicate through the IP infrastructure with a call server, media server, media gateway, or endpoints.

The MOM communicates through the IP infrastructure mainly with OMMs and in some scenarios with other applications that manage SIP-DECT.

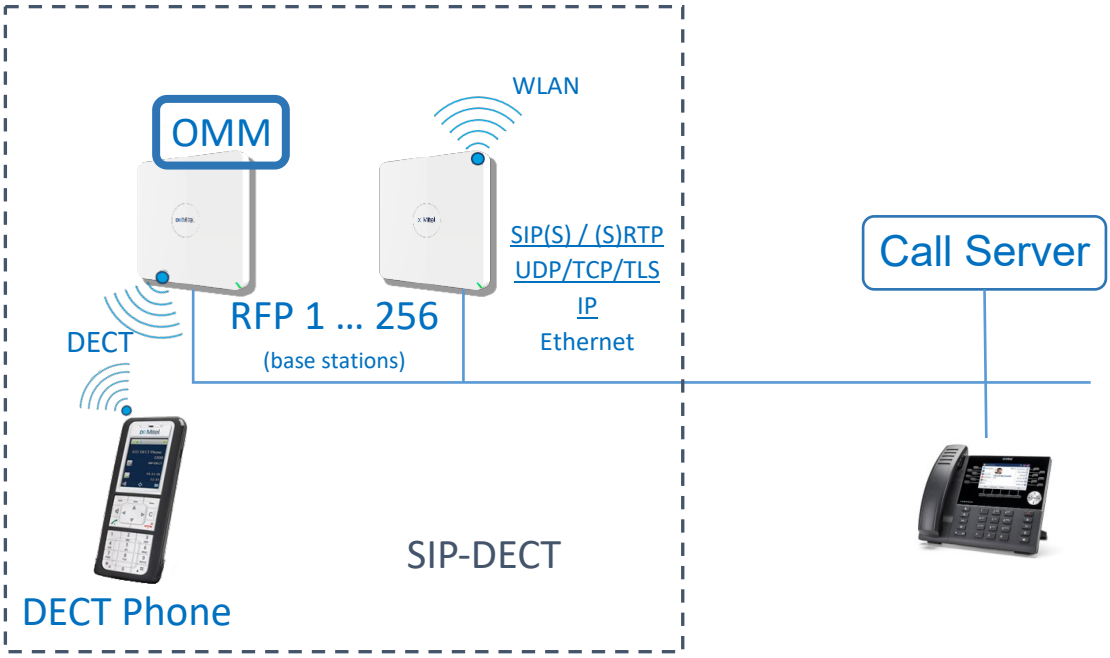


Figure 1: SIP-DECT Architecture Overview - OMM Running on RFP

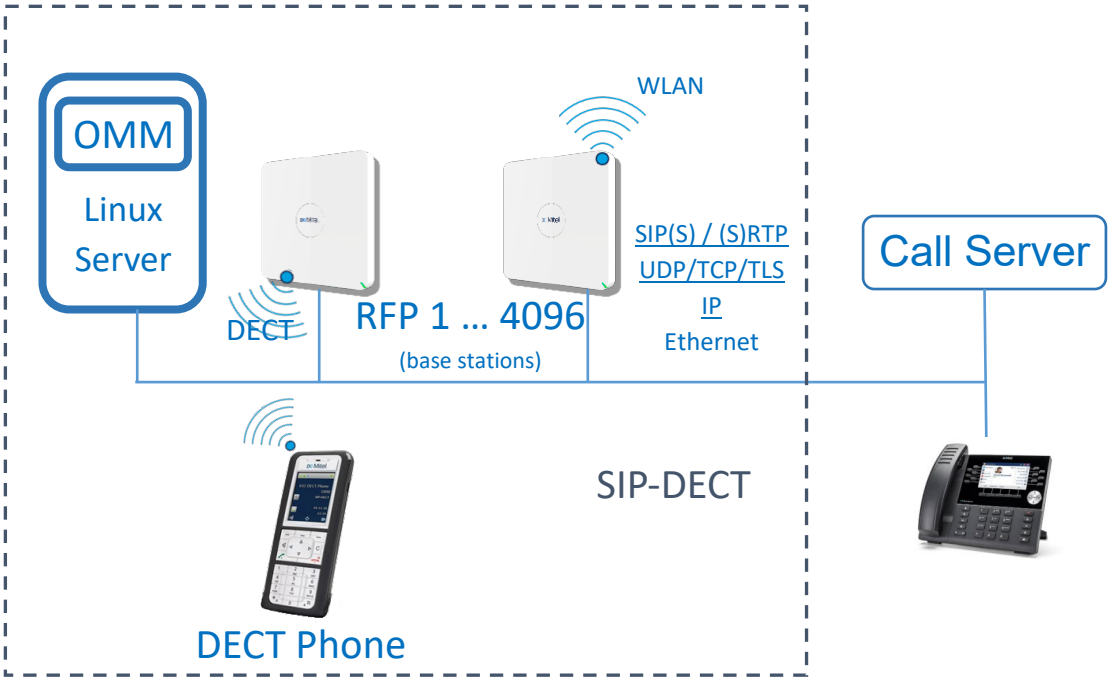


Figure 2: SIP-DECT Architecture Overview - OMM Running on Linux Server

The base station provides the lower layer DECT interface and acts as a DECT / RTP media gateway. It is also the platform to host the OMM. The bases station's OS is a proprietary embedded Linux®, which has been hardened by removal of unnecessary components on a proprietary hardware.

Some DECT base stations available with the solution also integrate an embedded 802.11XX WLAN access point (AP) that forwards the traffic between the WLAN and the Ethernet interface.

The OMM performs amongst other things, the following tasks:

- Signaling gateway (SIP <-> DECT)
- Central Management of the base stations and DECT phones
- Provides a Web service for system configuration
- Provides additional services such as:
  - Central corporate directory (LDAP, SIP-DECT XML terminal interface, and Broadworks® XSI (eXtended Services Interface))
  - OM Application XML interface (AXI) for OAM&P, messaging, alerting service, and locating
  - Integrated Messaging and Alerting Service (IMA)
  - Data backup and provisioning services
  - SIP-DECT XML terminal interface

The SIP-DECT XML terminal interface adapts Mitel's "XML API for SIP Phones" for the Mitel 600 and 700 DECT phone family.

The OMM processes SIP(S) and the base station processes (S)RTP. The DECT signaling between the OMM and the DECT telephone is forwarded to the base station via IP and sent from there by radio.

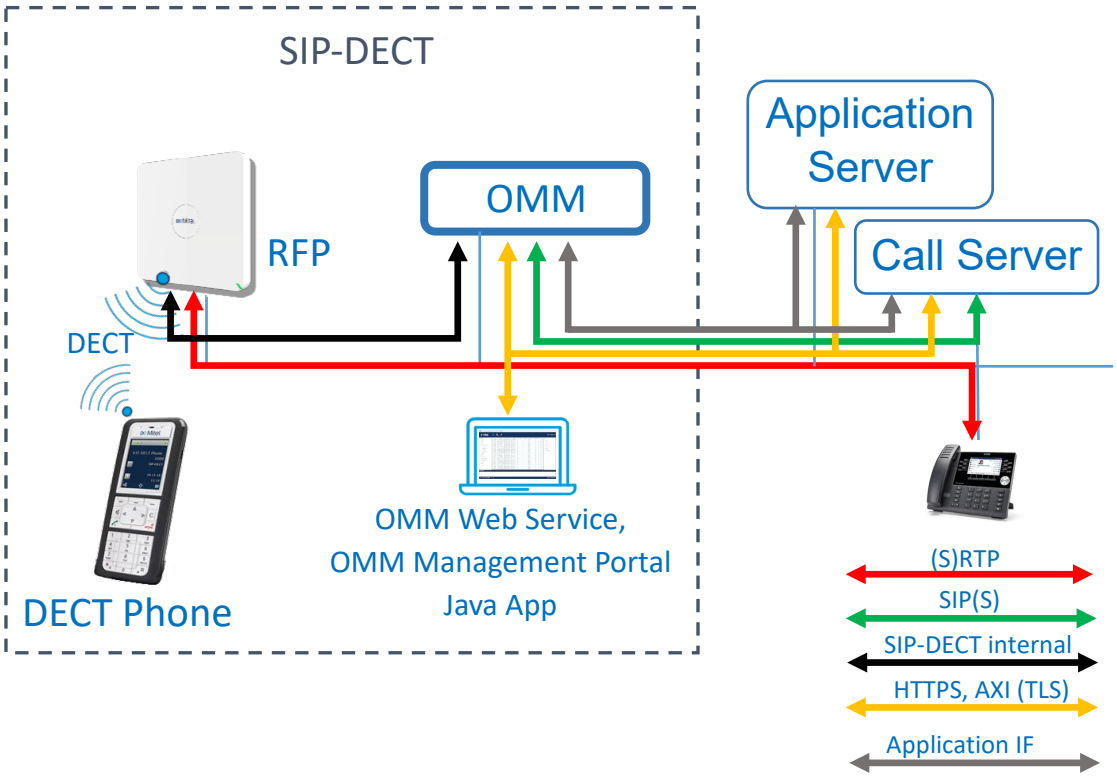


Figure 3: SIP-DECT Protocols

The OMM management takes place via the OMM web service or via the Java application OMP (OMM Management Protocol). The OMP uses the OM Application XML interface (AXI).

The AXI interface is also used by applications. Further application interfaces include: XML terminal interface, LDAP(S), and Broadworks® XSI.

The OMM can also fetch configuration files from an external file server to import configuration data including, but not limited to, user data. Such a configuration or provisioning service can be part of a call server or a separate service.

The Multi-OMM Manager (MOM) fulfills the following tasks, among others:

- Maintains a central user and DECT Phone DB for all connected OMMs including the synchronization of data between OMMs and MOM
- Supports the roaming of user and DECT phones between OMMs
- Provides configuration files for OMMs as a means for central management of multiple OMMs
- Provides a MOM Application XML interface (MAXI) for OAM&P, messaging, alerting service, and locating, which is derived from the OM Application XML interface (AXI)

The MOM is not involved in any telephony related signaling or media stream processing.

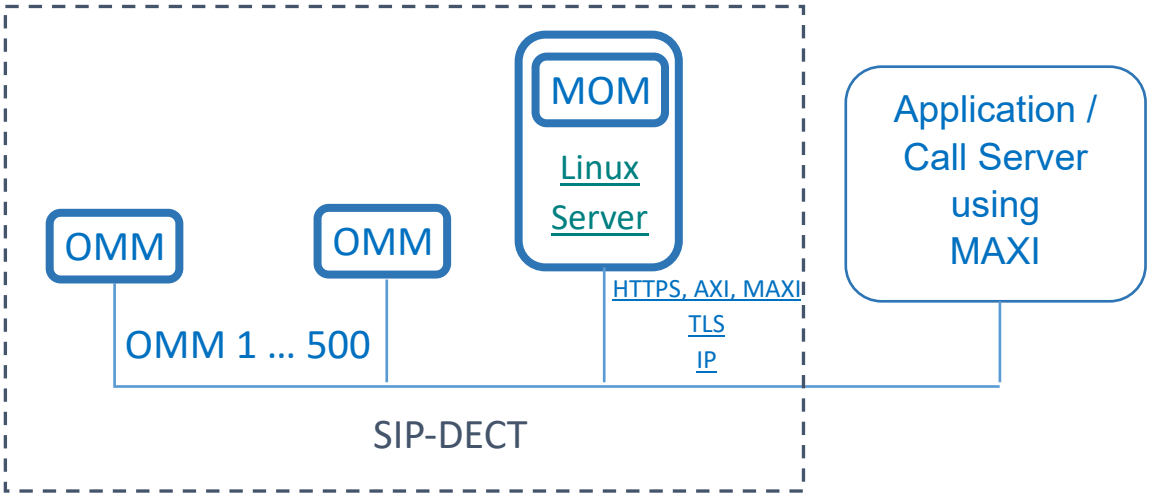


Figure 4: SIP-DECT Architecture Overview - Multi-OMM Installation

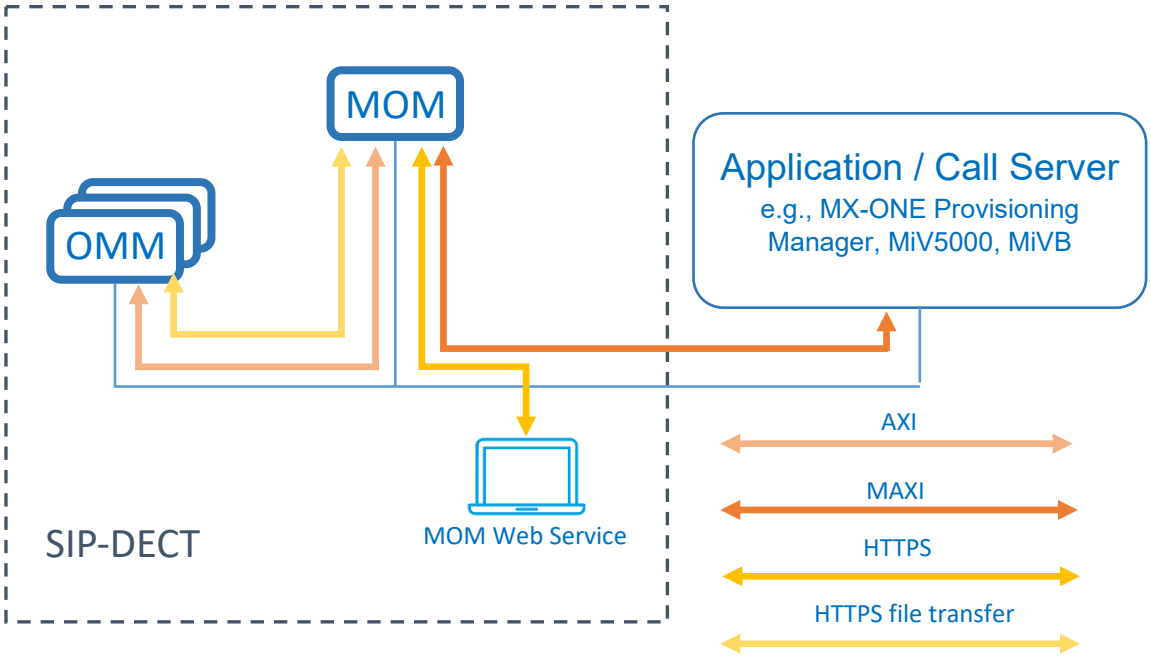


Figure 5: SIP-DECT Protocols with MOM

Security Overview

The SIP-DECT 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 SIP-DECT has security features that address identity, authentication, encryption, access and authorization.

SIP-DECT also supports audit trails, logs, and enterprise security certificates.

The SIP-DECT security features are configured via various management forms, which are accessed with the SIP-DECT System Administration Tool. The SIP-DECT System Administration Tool OMP contains embedded help files that will assist the administrator with forms configuration.

Securing the Operating System

Operating System Overview

The SIP-DECT software runs on an embedded Linux OS of the SIP-DECT RFPs. The Linux OS is part of the RFP firmware deliverables.

The OMM and MOM can be installed on a Rocky 9 Linux server (dedicated hardware or VM). The Linux OS software is only part of an OVA deliverable. If you do not want to run OMM or MOM in a virtual environment, you must have an appropriate Rocky 9 installation in place before installing the application as an RPM package.

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

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.

Operating System Related Network Controls

In their default initial state, SIP-DECT RFP provides only a minimum network access for setting up and configuring an RFP as part of a whole SIP-DECT system. The Web UI is started only on the RFP running the OMM.

Network access is reduced to the minimum and can be configured by the customer (admin) through activation/deactivation of specific features in the OMM:

- All unused IP ports are disabled by default. Unconfigured RFP has SSH activated by default.
- Only TLS 1.3 and 1.2 are enabled by default.
- TLS 1.1 and TLS 1.0 are no longer supported.
- Unencrypted HTTP connections are redirected to the Web UI to HTTPS by default.

As of SIP-DECT Release 9.1SP1, Mitel has introduced the Event Manager, whose Web UI (port 8444) is started on the RFP on which the OMM is not running (for performance reasons). The Event Manager provides additional interfaces if configured by the customer:

- ESPA v4.4.4 IP interface (TCP server socket with configurable port) for incoming event messages. This interface is not encrypted.
- SIP-DECT interface (AXI on TCP port 12622)
- SNMPv2c TCP interface for outgoing TRAPS. This interface is not encrypted.
- Unencrypted HTTP connections (port 8082) are redirected to HTTPS (port 8444) by default.

Securing Operating System User Interfaces

Each SIP-DECT RFP provides an SSH “User shell” and SSH “Root (SSH only)” shell for maintenance and diagnostic purposes. Whether these shells are available or not depends on the RFP’s state and the according OMM configuration. The SSH is version SSHv2.

The root shell allows access to the running OS.

In initial factory default state, both ssh shells are enabled with following login/password credentials:

- User shell: “omm” / “omm”
- Root shell: “root” / “22222”

As soon as an RFP is connected to an OMM, the OMM overwrites the RFP’s ssh settings and login/password credentials with its own configuration and enables or disables the SSH access. After first connection to an OMM, the root shell is no longer available to log in. The administrator must first log in to a regular user shell to get access and then start a root shell in the RFP.

The SSH access can be enabled/disabled via “OMP > System > Basic settings > Remote access”.

For Linux server installations the administrator is in charge and is responsible for preventing unauthorized access to the system. An SSH shell must be secured at the operating system level.

Recommendation

- Disable the “Remote access” in the OMM when not needed. The default is Off.
- For Linux server installations, it is recommended to run OMM and MOM on different (VM) servers.
- On the Linux server, prevent SSH access for user “root”. Install a local administrator user who can switch to root privileges if needed and secure login of this user with a strong password.

Administration

Administration and Management Tools

The SIP-DECT provides personnel with following integral administration and management tools:

- MOM Web UI
- OMM Web UI
- Event Manager Web UI
- OM Management Platform (OMP)
- OM Configurator

MOM Web UI

The MOM acts as an HTTP/HTTPS server. The Web interface allows HTTPS only. Any request to HTTP port 80 is redirected to HTTPS on port 443.

The MOM Web interface is used for administration of the MOM application itself (for example add administrative users) and for the administration and supervision of the connected OMMs. Before the MOM can connect to an OMM, the connection must be defined in the MOM.

OMM Web UI

The OMM acts as an HTTP/HTTPS server. The HTTP server binds to port 80 and HTTPS binds to port 443 by default. An HTTP request on port 80 will be redirected to HTTPS on port 443.

In contrast to the OMP, the interface allows the basic configuration of the system but does not offer the full configuration scope with all expert settings.

Event Manager Web UI

The Event Manager Web UI acts as an HTTP/HTTPS server on the RFP (not OMM). By default, the HTTP server is bound to port 8082 and HTTPS to port 8444. An HTTP request on port 8082 will be redirected to HTTPS on port 8444.

The Event Manager Web interface is used for administration of the Event Manager application itself.

OM Management Platform (OMP)

The OM Management Portal (OMP) is a Java tool used to manage the SIP-DECT solution. OMP can be used to view and configure OMM system data and has integrated monitoring and other maintenance features. It offers the full configuration scope.

OMP accesses the OMM via the OM Application XML Interface (OM AXI). The OM AXI is an application programming interface that also allows third-party software to configure the OMM. This interface is encrypted by TLS depending on the OMM TLS configuration.

OM Configurator

The OM Configurator (OMC) is a Java tool and offers as an alternative to DHCP configuration the statically network settings of DECT base stations (RFP). The settings configured through the OM Configurator tool are saved permanently in the internal flash memory of the RFP.

An initial configuration of RFPs through the OM Configurator tool requires a login ID and password. The default login ID and password are “omm” and “omm”. If the RFP is configured by the OMM later on, the OMM also sets the configuration password. You must enter the OMM’s full access user and password in the OM Configurator tool then.

Administration and Web Server Certificate

By default, MOM and OMM use a hardcoded self-signed MOM or OMM certificate as the local certificate for encrypted Web UI and MAXI and AXI (for example, OMP) access.

However, self-signed certificates are inherently untrusted by the web browser. This can be mitigated by installing the self-signed certificate on the local computer or bypassed by making an exception.

The recommendation though is to install a certificate obtained from a Certificate Authority (CA) that the customer already owns (that is, an enterprise CA). The web browser will then trust the SIP-DECT access. Note that certificates do expire and the customer, therefore, must be aware of the expiry date and renew it when needed. The certificates to import use PEM files.

Administration/Management Tool Encryption

The administration is accessed through

- HTTPS on TCP port 443 (OMM Web UI) and 8444 (Event Manager Web UI)
- AXI on TCP port 12622
- MAXI on TCP port 12624

which must be allowed through any data network local access control list or firewall.

SIP-DECT utilizes Transport Layer Security (TLS) version 1.3 or 1.2.

As of SIP-DECT Release 8.3, a system-wide “TLS security level” configuration parameter was introduced for the OMM and the MOM. This parameter allows the Administrator to differentiate between the levels High, Medium, and Legacy. Each security level is associated to a set of cipher suites and TLS version (see the following tables). This security level will be used for all TLS interfaces except the 802.1x interface.

Note: The IEEE 802.1x interface allows only authorized devices to be IP-routed on a specific LAN socket. In LAN infrastructure in public places any user could plug a device to an accessible RJ45 LAN socket. The infrastructure must prevent illegal use of such LAN access and must be able to verify a device using 802.1x in conjunction with certificates to determine that a device is authorized to use this LAN socket. Once authorized typically by a radius server, the switch serving that socket is set up to forward packets of this device (MAC address) only. If one unplugs an already authorized device, the switch will block any traffic from this socket except for 802.1x interface mechanism, and the 802.1x authorization process is run again.

When updating a system without security level, the system-wide security level "Legacy" is used to ensure operability, while with a new SIP-DECT installation, the system-wide security level “High” is used to achieve the highest security.

The recommendation though is to use the security level High whenever the used environment allows this.

For the MOM to OMM connections the TLS version is always 1.2 or 1.3. It cannot be switched to a lower TLS version.

Table 1 gives an overview of the Ciphers Suites that are used as default values in the individual security levels. Table 2 shows the corresponding default cipher strings in OpenSSL notation. The lists are ordered preference lists in which the most preferred cipher suite is at the top.

Table 1: Default Cipher Suites per Security Level

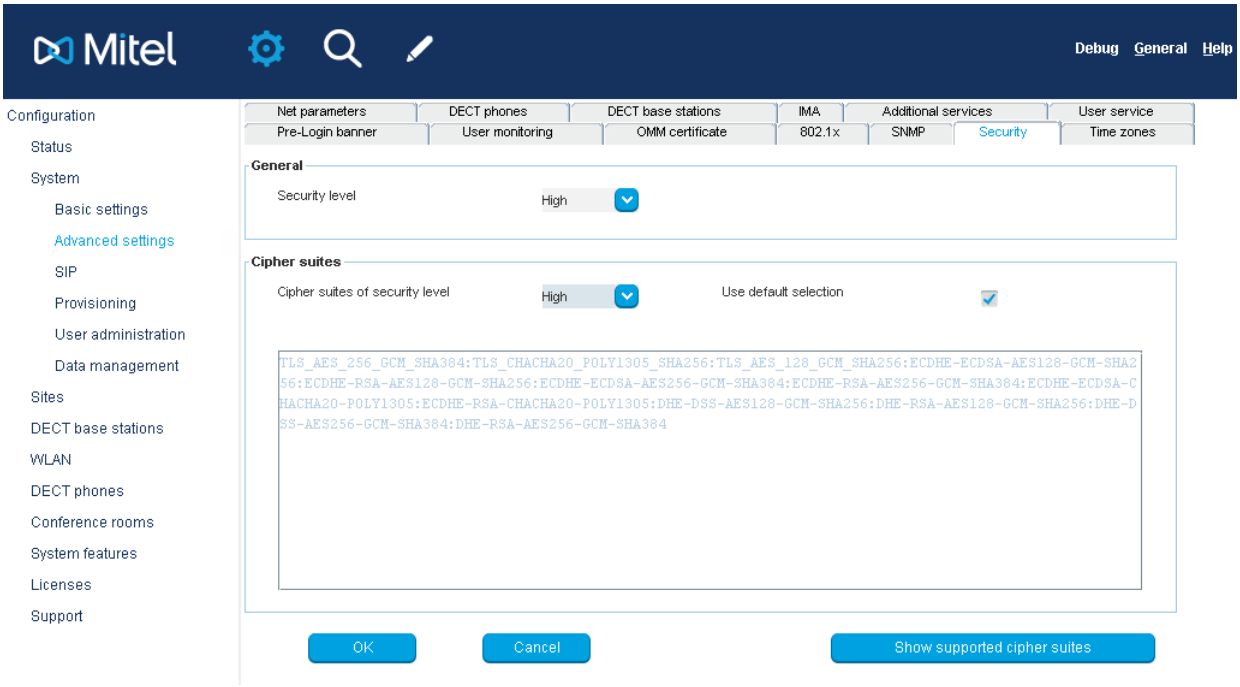
Hex Code	Cipher Suite Name (OpenSSL)	Protocol	Strength	Security level		
				High	Medium	Legacy
0x13,0x02	TLS_AES_256_GCM_SHA384	1.3	High	✓	✓	✓
0x13,0x03	TLS_CHACHA20_POLY1305_SHA256	1.3	High	✓	✓	✓
0x13,0x01	TLS_AES_128_GCM_SHA256	1.3	High	✓	✓	✓
0xC0,0x2B	ECDHE-ECDSA-AES128-GCM-SHA256	1.2	High	✓	✓	✓
0xC0,0x2F	ECDHE-RSA-AES128-GCM-SHA256	1.2	High	✓	✓	✓
0xC0,0x2C	ECDHE-ECDSA-AES256-GCM-SHA384	1.2	High	✓	✓	✓
0xC0,0x30	ECDHE-RSA-AES256-GCM-SHA384	1.2	High	✓	✓	✓
0xCC,0xA9	ECDHE-ECDSA-CHACHA20-POLY1305	1.2	High	✓	✓	✓
0xCC,0xA8	ECDHE-RSA-CHACHA20-POLY1305	1.2	High	✓	✓	✓
0x00,0xA2	DHE-DSS-AES128-GCM-SHA256	1.2	High	✓	✓	✓
0x00,0x9E	DHE-RSA-AES128-GCM-SHA256	1.2	High	✓	✓	✓
0x00,0xA3	DHE-DSS-AES256-GCM-SHA384	1.2	High	✓	✓	✓
0x00,0x9F	DHE-RSA-AES256-GCM-SHA384	1.2	High	✓	✓	✓
0xC0,0x23	ECDHE-ECDSA-AES128-SHA256	1.2	Medium		✓	✓
0xC0,0x27	ECDHE-RSA-AES128-SHA256	1.2	Medium		✓	✓
0xC0,0x24	ECDHE-ECDSA-AES256-SHA384	1.2	Medium		✓	✓
0xC0,0x28	ECDHE-RSA-AES256-SHA384	1.2	Medium		✓	✓
0x00,0x9C	AES128-GCM-SHA256	1.2	Medium		✓	✓
0x00,0x9D	AES256-GCM-SHA384	1.2	Medium		✓	✓
0x00,0x3C	AES128-SHA256	1.2	Medium		✓	✓
0x00,0x3D	AES256-SHA256	1.2	Medium		✓	✓
0xC0,0x09	ECDHE-ECDSA-AES128-SHA	1	Low			✓
0xC0,0x13	ECDHE-RSA-AES128-SHA	1	Low			✓
0xC0,0x0A	ECDHE-ECDSA-AES256-SHA	1	Low			✓
0xC0,0x14	ECDHE-RSA-AES256-SHA	1	Low			✓
0x00,0x2F	AES128-SHA	SSLv3	Low			✓
0x00,0x35	AES256-SHA	SSLv3	Low			✓
0x00,0x0A	DES-CBC3-SHA	SSLv3	Low			✓

Table 2: Default Cipher Strings per Security Level

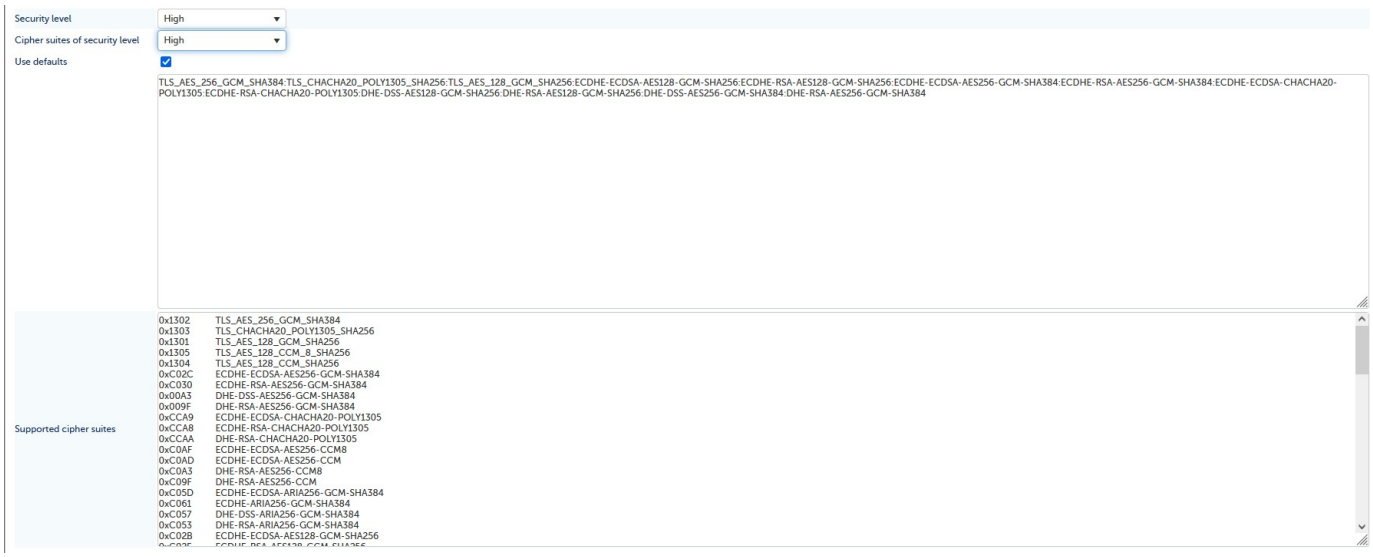
Security level	Default cipher string (OpenSSL notation)
High	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-

	POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384
Medium	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256
Legacy	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

The security level and the cipher suite selection for the different security levels can be modified using OMP. For further details, see the “SIP-DECT OM System Manual – Release 9.1”.



The security level and cipher suite selection in the MOM is in the tab “System settings”: It allows the same setting as in the OMM.



The SIP-DECT OMM supports all cipher suites listed in Table 3 while the java configuration tool, OMP, supports the listed subset.

Table 3: Supported Cipher Suites

Hex Code	OpenSSL Cipher Suite Name [IANA name]	Prot.	Mitel Default	OMP
0x13,0x02	TLS_AES_256_GCM_SHA384 [TLS_AES_256_GCM_SHA384]	1.3	H1	✓
0x13,0x03	TLS_CHACHA20_POLY1305_SHA256 [TLS_CHACHA20_POLY1305_SHA256]	1.3	H2	✓
0x13,0x01	TLS_AES_128_GCM_SHA256 [TLS_AES_128_GCM_SHA256]	1.3	H3	✓
0x13,0x05	TLS_AES_128_CCM_8_SHA256 [TLS_AES_128_CCM_8_SHA256]	1.3		
0x13,0x04	TLS_AES_128_CCM_SHA256 [TLS_AES_128_CCM_SHA256]	1.3		
0xC0,0x2C	ECDHE-ECDSA-AES256-GCM-SHA384 [TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384]	1.2	H6	
0xC0,0x30	ECDHE-RSA-AES256-GCM-SHA384 [TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384]	1.2	H7	
0x00,0xA3	DHE-DSS-AES256-GCM-SHA384 [TLS_DHE_DSS_WITH_AES_256_GCM_SHA384]	1.2	H12	✓
0x00,0x9F	DHE-RSA-AES256-GCM-SHA384 [TLS_DHE_RSA_WITH_AES_256_GCM_SHA384]	1.2	H13	✓
0xCC,0xA9	ECDHE-ECDSA-CHACHA20-POLY1305 [TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256]	1.2	H8	
0xCC,0xA8	ECDHE-RSA-CHACHA20-POLY1305 [TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256]	1.2	H9	
0xCC,0xAA	DHE-RSA-CHACHA20-POLY1305 [TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256]	1.2		✓
0xC0,0xAF	ECDHE-ECDSA-AES256-CCM8 [TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8]	1.2		
0xC0,0xAD	ECDHE-ECDSA-AES256-CCM [TLS_ECDHE_ECDSA_WITH_AES_256_CCM]	1.2		
0xC0,0xA3	DHE-RSA-AES256-CCM8 [TLS_DHE_RSA_WITH_AES_256_CCM_8]	1.2		
0xC0,0x9F	DHE-RSA-AES256-CCM [TLS_DHE_RSA_WITH_AES_256_CCM]	1.2		
0xC0,0x5D	ECDHE-ECDSA-ARIA256-GCM-SHA384 [TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384]	1.2		
0xC0,0x61	ECDHE-ARIA256-GCM-SHA384 [TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384]	1.2		

Hex Code	OpenSSL Cipher Suite Name [IANA name]	Prot.	Mitel Default	OMP
0xC0,0x57	DHE-DSS-ARIA256-GCM-SHA384 [TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384]	1.2		
0xC0,0x53	DHE-RSA-ARIA256-GCM-SHA384 [TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384]	1.2		
0xC0,0x2B	ECDHE-ECDSA-AES128-GCM-SHA256 [TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256]	1.2	H4	
0xC0,0x2F	ECDHE-RSA-AES128-GCM-SHA256 [TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256]	1.2	H5	
0x00,0xA2	DHE-DSS-AES128-GCM-SHA256 [TLS_DHE_DSS_WITH_AES_128_GCM_SHA256]	1.2	H10	✓
0x00,0x9E	DHE-RSA-AES128-GCM-SHA256 [TLS_DHE_RSA_WITH_AES_128_GCM_SHA256]	1.2	H11	✓
0xC0,0xAE	ECDHE-ECDSA-AES128-CCM8 [TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8]	1.2		
0xC0,0xAC	ECDHE-ECDSA-AES128-CCM [TLS_ECDHE_ECDSA_WITH_AES_128_CCM]	1.2		
0xC0,0xA2	DHE-RSA-AES128-CCM8 [TLS_DHE_RSA_WITH_AES_128_CCM_8]	1.2		
0xC0,0x9E	DHE-RSA-AES128-CCM [TLS_DHE_RSA_WITH_AES_128_CCM]	1.2		
0xC0,0x5C	ECDHE-ECDSA-ARIA128-GCM-SHA256 [TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256]	1.2		
0xC0,0x60	ECDHE-ARIA128-GCM-SHA256 [TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256]	1.2		
0xC0,0x56	DHE-DSS-ARIA128-GCM-SHA256 [TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256]	1.2		
0xC0,0x52	DHE-RSA-ARIA128-GCM-SHA256 [TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256]	1.2		
0xC0,0x24	ECDHE-ECDSA-AES256-SHA384 [TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384]	1.2	M3	
0xC0,0x28	ECDHE-RSA-AES256-SHA384 [TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384]	1.2	M4	
0x00,0x6B	DHE-RSA-AES256-SHA256 [TLS_DHE_RSA_WITH_AES_256_CBC_SHA256]	1.2		✓
0x00,0x6A	DHE-DSS-AES256-SHA256 [TLS_DHE_DSS_WITH_AES_256_CBC_SHA256]	1.2		✓
0xC0,0x73	ECDHE-ECDSA-CAMELLIA256-SHA384 [TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384]	1.2		
0xC0,0x77	ECDHE-RSA-CAMELLIA256-SHA384 [TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384]	1.2		
0x00,0xC4	DHE-RSA-CAMELLIA256-SHA256 [TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256]	1.2		
0x00,0xC3	DHE-DSS-CAMELLIA256-SHA256 [TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256]	1.2		
0xC0,0x23	ECDHE-ECDSA-AES128-SHA256 [TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256]	1.2	M1	
0xC0,0x27	ECDHE-RSA-AES128-SHA256 [TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256]	1.2	M2	
0x00,0x67	DHE-RSA-AES128-SHA256 [TLS_DHE_RSA_WITH_AES_128_CBC_SHA256]	1.2		✓
0x00,0x40	DHE-DSS-AES128-SHA256 [TLS_DHE_DSS_WITH_AES_128_CBC_SHA256]	1.2		✓
0xC0,0x72	ECDHE-ECDSA-CAMELLIA128-SHA256 [TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256]	1.2		
0xC0,0x76	ECDHE-RSA-CAMELLIA128-SHA256 [TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256]	1.2		
0x00,0xBE	DHE-RSA-CAMELLIA128-SHA256 [TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256]	1.2		
0x00,0xBD	DHE-DSS-CAMELLIA128-SHA256 [TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256]	1.2		
0xC0,0x0A	ECDHE-ECDSA-AES256-SHA [TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA]	1	L3	
0xC0,0x14	ECDHE-RSA-AES256-SHA [TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]	1	L4	

Hex Code	OpenSSL Cipher Suite Name [IANA name]	Prot.	Mitel Default	OMP
0x00,0x39	DHE-RSA-AES256-SHA [TLS_DHE_RSA_WITH_AES_256_CBC_SHA]	SSLv3		✓
0x00,0x38	DHE-DSS-AES256-SHA [TLS_DHE_DSS_WITH_AES_256_CBC_SHA]	SSLv3		✓
0x00,0x88	DHE-RSA-CAMELLIA256-SHA [TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA]	SSLv3		
0x00,0x87	DHE-DSS-CAMELLIA256-SHA [TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA]	SSLv3		
0xC0,0x09	ECDHE-ECDSA-AES128-SHA [TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA]	1	L1	
0xC0,0x13	ECDHE-RSA-AES128-SHA [TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]	1	L2	
0x00,0x33	DHE-RSA-AES128-SHA [TLS_DHE_RSA_WITH_AES_128_CBC_SHA]	SSLv3		✓
0x00,0x32	DHE-DSS-AES128-SHA [TLS_DHE_DSS_WITH_AES_128_CBC_SHA]	SSLv3		✓
0x00,0x45	DHE-RSA-CAMELLIA128-SHA [TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA]	SSLv3		
0x00,0x44	DHE-DSS-CAMELLIA128-SHA [TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA]	SSLv3		
0x00,0x9D	AES256-GCM-SHA384 [TLS_RSA_WITH_AES_256_GCM_SHA384]	1.2	M6	✓
0xC0,0xA1	AES256-CCM8 [TLS_RSA_WITH_AES_256_CCM_8]	1.2		
0xC0,0x9D	AES256-CCM [TLS_RSA_WITH_AES_256_CCM]	1.2		
0xC0,0x51	ARIA256-GCM-SHA384 [TLS_RSA_WITH_ARIA_256_GCM_SHA384]	1.2		
0x00,0x9C	AES128-GCM-SHA256 [TLS_RSA_WITH_AES_128_GCM_SHA256]	1.2	M5	✓
0xC0,0xA0	AES128-CCM8 [TLS_RSA_WITH_AES_128_CCM_8]	1.2		
0xC0,0x9C	AES128-CCM [TLS_RSA_WITH_AES_128_CCM]	1.2		
0xC0,0x50	ARIA128-GCM-SHA256 [TLS_RSA_WITH_ARIA_128_GCM_SHA256]	1.2		
0x00,0x3D	AES256-SHA256 [TLS_RSA_WITH_AES_256_CBC_SHA256]	1.2	M8	✓
0x00,0xC0	CAMELLIA256-SHA256 [TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256]	1.2		
0x00,0x3C	AES128-SHA256 [TLS_RSA_WITH_AES_128_CBC_SHA256]	1.2	M7	✓
0x00,0xBA	CAMELLIA128-SHA256 [TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256]	1.2		
0x00,0x35	AES256-SHA [TLS_RSA_WITH_AES_256_CBC_SHA]	SSLv3	L6	✓
0x00,0x84	CAMELLIA256-SHA [TLS_RSA_WITH_CAMELLIA_256_CBC_SHA]	SSLv3		
0x00,0x2F	AES128-SHA [AES128-SHA]	SSLv3	L5	✓
0x00,0x41	CAMELLIA128-SHA [TLS_RSA_WITH_CAMELLIA_128_CBC_SHA]	SSLv3		
0x00,0x0A	DES-CBC3-SHA [TLS_RSA_WITH_3DES_EDE_CBC_SHA]	SSLv3	L7	

Administration/Management Tool Interfaces - Physical Characteristics

Most SIP-DECT base stations have a 100Mb/s Ethernet interface. IP-RFPs with Wi-Fi have a 1000Mb/s Ethernet interface. The earlier 3G RFP hardware also has a USB interface. The USB interface of the 3G RFP is primarily used to do a factory reset or to copy files for error research reasons. The USB interface cannot be disabled.

Note: The 4G RFP utilizes a button for different settings. Depending on when and how long the button is pressed the 4G RFP performs a factory reset. For more details, see *SIP-DECT OM System Manual Administration Guide*.

The Ethernet interface is used for administration and maintenance, and it is also used for telephony (SIP).

In addition to the Ethernet interface, DECT radio connection can be used for limited administration of the OMM system after login authentication and input of an additional administration PIN in the device.

The OC based OMM and MOM Ethernet interfaces depend on the host hardware used.

Separation of Network Functionality

SIP-DECT does not separate network functionality. Therefore, all system management, call control handling, and media stream use the same network. It is possible to assign a VLAN ID to the device to separate the SIP-DECT network traffic from another productive network traffic.

Managing System Security Features

Many of the SIP-DECT's security features can be managed or configured by the administrator or by authorized personnel. Management of these security features is performed by accessing the SIP-DECT Web UI or Event Manager Web UI or the administration tool OMP. This section describes the security features that the administrator can configure, and recommendations on how to configure the security features are also provided.

Identity, Authentication and Password Policies

To ensure privacy and maintain system integrity, access to the SIP-DECT is restricted by a login password to those users that can be correctly identified and authenticated. Access must be granted to the Administrator with (write) full access and for the application with read-only access.

On first login, the system forces the user to change the default credentials. The password must comply with several complexity rules (see SIP-DECT OM System Manual Chapter 6.4.4 USER ADMINISTRATION).

The rules are fixed and cannot be weakened. The preconfigured users "omm" (OMM), "root" (OMM), "user" (OMM) and “admin” (Event Manager Web UI) cannot be changed or deleted. The passwords are stored in the OMM as salted hash.

Password aging is supported. Default is *no aging*.

In MOM, there is only the preconfigured user “mom”. Passwords are stored as salted hash. There is no password aging.

In Event Manager, there is the preconfigured user “admin”. Passwords are stored as salted hash. There is no password aging.

There is no mechanism to reset a forgotten password of the fully access user "omm" or “admin”. To reset the "omm" and “admin” password back to default, the OMM IP-RFP hardware must be factory reset with loss of all data.

Other forgotten passwords can be reassigned by the "omm" user, or in the MOM as the “mom” user. On a PC or VM system, a new password of the “omm” or “mom” may be set as root user of that system.

The administrator may create new users in OMP menu "System -> User administration" for each user who needs access to OMM management. Individual accounts allow restricted permissions for read/write or different permissions for messaging, locating, or monitoring.

As the OMM is intended to be installed in a secured local network; there are no further mechanisms to exclude users after failed logins. Each OMP login is logged as AXI connection in the event log.

A web session is timed out after 10 minutes of inactivity. This timer is not configurable.

Recommendation

- Create individual user accounts and assign the minimum needed permissions.
- Enable password aging for all accounts that are not used for the application or tool login. Default is *no aging* ('none'). To enable password ageing, select '3 months' or '6 months'.
- Do not activate password aging in OMM for a MOM login account.

The security features configured under the "System -> Advanced Settings" are described in the following sections. For additional details, refer to the SIP-DECT System OMP Help menu or the SIP-DECT OM System Manual.

Login Banner

In the OMP menu "System > Advanced Settings" a pre-login banner can be configured to warn users against unauthorized system access or use. The form is empty by default as the OMM is designed for installations at the customer site. The customer may publish their own security rules in this banner.

This setting is used to determine whether users will be presented with a message. The message displays on the OMP and requires the user's acknowledgment (via an OK button) before proceeding. If the banner is not accepted, the OMP will terminate. The default setting is 'not active', meaning that no banner will be displayed.

The MOM supports the login banner in the “System settings” tab. The Event Manager Web UI does not support the login banner.

Recommendation

- Use the login banner to provide the administrator with any needed information. The actual text will come from the company’s own security policy.

Access and Authorization

For privacy, all personal data processing is protected with role-based access and authorization controls. SIP-DECT supports two roles, fully access or read only access for administrators.

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 SIP-DECT OMP, there is only one form used to administer access and authorization, the "System > User administration" menu.

The administrator can allow remote access in "System > Basic setting > General". Remote access is needed only for deep inspection and debugging of the system. Remote access is off by default.

On PC or VM systems, root access is needed to get access to the file system where the data resides. This access is needed to deploy the certificate (PEM file) for the system.

Recommendation

- When an administrative user leaves, delete the user’s account from the OMM.
- Switch on remote access only for the time needed for tracing and debugging the system and switch remote access to off again after the trace has ended.

Application - Login Security

To connect different tools using the AXI interface, the tools need to log in to the OMM. Each tool connected to the OMM shall have its own account for access and have a set of permissions assigned to it. For this purpose, use the OMP "System > User administration" menu and configure the set of permissions.

The OMM has not implemented a lockout mechanism for failed logins because this would lead to inoperable service for the tools connected to that account.

Recommendation

- When a tool is no longer in use, delete that tool’s account in the OMM

Audits, Logs and Event Reporting

There are no log entries generated for administration tasks. The following logs are for system monitoring only.

Event Log

Purpose

The Event Log can be inspected via Web UI or with OMP. Switch the OMP from "Administration Mode" to "Monitor Mode" to view the Event Log. The Event Log lists for each event

- the severity,
- the subsystem which caused the entry,
- the count for how often the event occurred repeatedly,
- the time and
- the events description as text.

The Event log is not configurable. The entries list hints for maintenance in case of system failures. It shows security events as well as network events.

- running software version
- provisioning progress
- failure on config file retrieval
- certificate loading
- AXI connection login
- SIP registration failures
- failed DECT subscriptions
- IP-RFP to the OMM connection failures

The login of the SIP-DECT OMP is logged as AXI connection login.

Recommendation

- If no other log system, such as syslog, is used, inspect the Event Log periodically.

Syslog

Purpose

The SIP-DECT Syslog is used for monitoring the SIP-DECT network components and for maintenance and support such as debugging or tracing purposes only—to catch non-reproducible failure of the system over a longer time.

SIP-DECT can log events to a Syslog server. Configuration is described in "SIP-DECT OM System Manual" chapter "6.12.2 Syslog". The IP address and port of the Syslog server must be configured in the OMM. The administrator can activate or deactivate syslog generation.

By default, the syslog is unconfigured. If configured, all events are sent to the syslog server. The syslog is also used for trace purposes. The tracing feature is for debugging and research of error situations and is activated by a set of commands, each for special situations. For a complete list of trace commands, see "SIP-DECT OM System Manual" chapter "10.3.5.6 OMM Console Commands".

Recommendation

- Switch off this feature when it is not needed any longer after tracing.

User Monitoring

Purpose

User monitoring allows the follow activity of individual users and inspect the states of their DECT phones. It is often used for special purposes of connected applications for alarming or messaging scenarios.

The feature must be configured and switched on for each individual user. User monitoring is set to off by default. Once switched on for a user, the user activity is monitored and can be inspected via OMP in *Monitoring Mode*. The user's activity is listed in "DECT phones > User monitoring" page. Events of all users which are setup to be monitored are listed here. The monitored user actions are:

- user login/logout from a DECT phone,
- handset subscription (DECT subscription),
- handset registration (DECT attachment),
- handset activity status,
- silent charging status of the handset,
- handset battery status,
- call diversion status,
- SIP user registration status.

An external application can log in via AXI and register to the listed user events. For more details, see "SIP-DECT OM System Manual" chapter "9.25 User Monitoring".

Recommendation

- The customer shall inform the users about this type of monitoring and obtain the consent from the affected users.
- Do not activate User monitoring if it is not needed by an application.
- Deactivate User monitoring as soon as an application based on this feature is no longer used.

RFP Statistic

Purpose

The RFP statistic shows the DECT network utilization of the air interfaces as a statistic over a long time. The counters provide base station related information on how many events showed up after the last counter reset. The statistic allows analysis of DECT areas where call drops often occur, or bad audio quality is experienced. To monitor the DECT network capacity, DECT base station channel statistics can be evaluated or cleared for a single base station or all base stations at once. For each single base station, the following data is collected:

- event count of voice channel usage (4 categories),
- event count of air channel usage (3 categories),
- event count of page queue overflow,
- count of sync events (3 categories),
- event count of base station health states (2 categories),
- count of DECT connection (4 categories),
- count of DSP channels used (4 categories),
- event counts to frame error rate (3 categories),
- count to miscellaneous base station event (4 categories).

None of these statistic counters reflect any personal user specific data.

Recommendation

- If this feature is not needed, clear statistic counter from time to time.

Network Alarms

SIP-DECT supports the following management and alarm protocols.

SNMP Support

SIP-DECT offers SNMPv1 and SNMPv2c support. Each IP-RFP may run an SNMP agent. The agent supports the MIB II database and will give alarm information. The SIP-DECT SNMP agent does not support write access.

SNMP support on PC or VM hardware must be configured separately, if needed, on the Linux operating system and is not part of the MOM application.

Recommendation

- As community string, use other than “public” or “private”.

If trap handling is switched off, the event will be logged to the event log list. The administrator must then review the event log from time to time.

For more information, see "SIP-DECT OM System Manual" chapter "6.4.6 SNMP menu" and chapter "9.18 SNMP configuration".

Specific SNMP management systems are not verified.

Use of Antivirus Software

As SIP-DECT is a closed system, there is no Antivirus Software available or needed. It is not possible to install other software programs on the SIP-DECT IP-RFP hardware system.

Software Patch Management Policy

SIP-DECT does not provide software patches to the system. SIP-DECT software is always delivered as a bundled package to be installed on the OMM. To get the highest level of security, the customer shall always install the latest service pack or hotfix version of the release to the OMM.

SIP-DECT software for VM server (OMM or MOM) is also delivered as an OVA file for VMware virtual machine environment. This OVA file always incorporates the latest Linux updates based on the Linux OS version (CentOS 7).

Network Security

The SIP-DECT and associated components communicate using the corporate network infrastructure.

Network Access Security

It is recommended that the Ethernet LAN switches used to provide SIP-DECT 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.

Wireless networks should 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.

Certificate Management

SIP-DECT has various secured interfaces to support secure connections for file imports from local servers or provisioning servers. By default, the OMM uses the following hardcoded self-signed certificate for Web UI, encrypted AXI connections, provisioning and SIP-over-TLS connections.


```
-----BEGIN CERTIFICATE-----
MIIDpzCCAo+gAwIBAgIJAK66pBhiSgV7MA0GCSqGSIb3DQEBCwUAMIGCMQswCQYD
VQQGEwJERTEPMA0GA1UECBMGQmVybGluMQ8wDQYDVQQHEwZCZXJsaW4xHzAdBgNV
BAoTFk1pdGVsIERldXRzY2hsYW5kIEdtYkgxMDAuBgNVBAMTJ01pdGVsIERldXRz
Y2hsYW5kIFNlY3VyZSBTZXJ2ZXIgUm9vdCBDQTAeFw0yMTA2MDQwODUzNDdaFw0z
MTA2MDIwODUzNDdaMIGTMQswCQYDVQQGEwJERTEPMA0GA1UECBMGQmVybGluMQ8w
DQYDVQQHEwZCZXJsaW4xHzAdBgNVBAoTFk1pdGVsIERldXRzY2hsYW5kIEdtYkgx
IjAgBgNVBAsUGU1vYmlsaXR5ICYgSW5mcmFzdHJ1Y3R1cmUxHTAbBgNVBAMTFE9w
ZW5Nb2JpbGl0eSBNYW5hZ2VyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA8txQ+r2scQysWg9oGmcHjp8HlpOgYX1jpTfGHvD4mVg0FHVqP6rhg/rxi6Sl
leeVvrlqPYUjb7h5SLH08Ok803UpgJWTdTz7HCdob2kIQX3R/f8OIKIw71ZAEO7K
CB4fWOn7mMK6TWJ3urLzIcjENaXwYAT+NUiEPqOsvweUTVEH0Z7VV+hSRvmVKvwM
xmBHt9Eqs/scHNfQKu+zSFR7M9AiwKvQm9yXa9zY8iADlpJOrT4gbbAM1R+VZ/Tu
4RseK9B1J/HOosAF9fdRNON0d0Bv+6tSik4kR/5xE2yTDle6dcVA+9qyBAmsHdAC
33e6XCzDxyZBCZvhW4m3lvJXOQIDAQABow0wCzAJBgNVHRMEAjAAMA0GCSqGSIb3
DQEBCwUAA4IBAQBKsbOYQV4Q1zHR/a8o7vUjCnIFll7lenYeBU/B0f2U4D/GW3Ei
XFy8p4adE/Ba6SGJme15KSVLw1Iiwvb6hB6wI/5aYq5Rg62VDk5KJAxGnOqzRbZa
R+yRpn8qnZp0kP/mFJUPEUpUYFqSDa33Ccxust6ipAFw+MfFh4jdaJZyH/2ghvMj
4l7p+/K0a+ufWpptYnkHDP31wn0OncSEYOFB+FZMQhDlD2/r6yf8Bf1SUKk6tmuf
/G4QDoig8+zBDDWp0BUggIuekI21SW1DLPpBXI787LmrDcTvkQ2RPTK+2UOeN1wr
mKNEfHNuLn6BbmDgNmoR+Bl+qFHxiDUU/Gn4 -----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIJAK66pBhiSgV8MA0GCSqGSIb3DQEBCwUAMIGCMQswCQYD
VQQGEwJERTEPMA0GA1UECBMGQmVybGluMQ8wDQYDVQQHEwZCZXJsaW4xHzAdBgNV
BAoTFk1pdGVsIERldXRzY2hsYW5kIEdtYkgxMDAuBgNVBAMTJ01pdGVsIERldXRz
Y2hsYW5kIFNlY3VyZSBTZXJ2ZXIgUm9vdCBDQTAeFw0yMTA2MDQwODU0MDBaFw0z
MTA2MDIwODU0MDBaMIGQMQswCQYDVQQGEwJERTEPMA0GA1UECBMGQmVybGluMQ8w
DQYDVQQHEwZCZXJsaW4xHzAdBgNVBAoTFk1pdGVsIERldXRzY2hsYW5kIEdtYkgx
IjAgBgNVBAsUGU1vYmlsaXR5ICYgSW5mcmFzdHJ1Y3R1cmUxGjAYBgNVBAMTEU11
bHRpLU9NTSBNYW5hZ2VyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
0qGqJ849/4YXATNqpgpaxtxXpZZlyHesFZqYVIz9iePLroGuYUukVwuz8ldCLK9D
4vv/ToZ8g7QCVxVNYFL+veQUX5sR0IlPJKhSnGs41cylYrum3cYPBQfVEmhBY6uJ
UlVPYX1j2Tynr9w7Xir2H4vo9WBlCy5wPPFfd7YLMKW1yTNsNXwRIaX25hzWJUPL
XGUyq88MGUkKVnbr7Gpu7GWaWFTm9i2X8Iie745Bm26ETbKgG9tEy61q7+y20FEV
h0jG7qZjSAUzaZxm2Afe/kyVEdCWdgsc24pOb9sIXDpXRh7uQ9E1R/LcHC81ch1O
gxjpn6r93Qabccwjrw RdWwIDAQABow0wCzAJBgNVHRMEAjAAMA0GCSqGSIb3DQEB
CwUAA4IBAQATEX1rfLZCDgcnPkyfLUTb+QoNrrfFGlFCSG0mBRmxaP0cn5uSAtaX
279aa8TrIQuNk0VdW0QZi4eWrfUyshUQq1CgNGQzyPYXyulxXiEkboAkxZabnxIs
```

```
1Iwz4A4sRIRBLvGgj/PAJlWfwlkZRhxXmv9aMaUI69VnaHGwjfD2RQp8C6VAuWsb
6dISDHWnILhiDETgej9LPNcisDKeqWfbiNElOGmGpif6Tl9eOVrjfqynyYJGNiv8
PZIFDQUSDDmSBKmNkqTUCILEHQ5jbTEgF0N9m8L4g6QnP4DwEFoj5EvhFiP5BfXK
e1UhfD0JMMHwM1idrs/Pp4cXfHfW7tX5 -----END CERTIFICATE-----
```

For details on how to replace the default certificate as a PEM file, refer to the *SIP-DECT OM System Manual Administration Guide chapter 9.10 "CONSOLIDATED CERTIFICATE MANAGEMENT"*.

Recommendation

- The customer shall import his own trusted certificate (PEM files).

Using VLANs to Assist with Security

To make eavesdropping attacks or Denial of Service attacks more difficult, or less effective, traffic on the LAN should be grouped according to traffic types and trust levels. This can be achieved with the use of Virtual LANs. VLANs can be used to segregate controller to controller signaling, controller to phone signaling and voice traffic.

When VLANs are used to provide isolation between traffic types, it will make the solution more robust against virus-based and network flooding attacks. In particular, if Voice over Internet Protocol (VoIP) traffic is grouped into a single VLAN, and the nodes on this VLAN are strongly protected, a worm-based attack causing network overload that originated on a node located on another VLAN might only marginally affect the VoIP LAN.

As an example, traffic types could be segregated as follows:

1. One VLAN grouping all of the call control engines together,
2. One or several VLANs grouping all of the SIP-DECT OMM, RFPs and IP phones together
3. One or several VLANs for supporting the data traffic

When the traffic types have been segregated by VLAN, hosts or devices belonging to different VLANs can only communicate through a Layer 3 switch or router that connects the two VLANs. This means that broadcast traffic is blocked across VLANs, preventing broadcast storms from propagating network wide.

Additionally, many modern routers offer Intrusion Detection/Prevention Systems (IDS/IPS), which are able to detect and/or block more advanced types of attacks.

Creating network trust zones for security purposes and the usage of Intrusion Detection and Prevention Systems (IDPS) are discussed in detail in the Mitel Technical Papers - Intrusion Detection and Prevention Systems and Securing Mitel Cloud Based Unified Communications.

Securing Server to Server Traffic

In a modern IT infrastructure, servers are generally connected at the network core, and they are also usually placed in a common physical location. This location needs to be physically protected, and only authorized personnel should be allowed to access this area.

When servers are deployed in this way, traffic among the servers is likely to never leave the physical locations where servers are stored. Some Layer 2 and Layer 3 network devices are also located in the same locations and contribute to guarantee the physical separation of server traffic from other kinds of network traffic. Access control measures should be enabled on L2 switches housed in this location, and IDPS technology should be deployed to protect the core elements.

As a further measure to protect server to server traffic, it is recommended that a specific VLAN be used just for connecting servers to servers.

If servers are located at remote locations, it is highly recommended to connect these devices to the main location via a Virtual Private Network (VPN), and to employ firewalls with integrated IDPS to protect and monitor the traffic on these external connections.

Securing Server to Client Traffic

SIP-DECT offers a variety of client application interfaces to access services from Mitel or third-party servers. These interfaces are:

- Provisioning
- Corporate Directory
- XML applications
- DECT phone's firmware update
- Automatic DB export

Recommendation

- For all of the above client application interfaces, SIP-DECT offers the possibility to configure the different transport protocols. It is recommended to use protocols that allow encryption and authentication; such as https, sftp, ftps, or ldaps.

IP Ports

The administrator and/or network technician must open certain IP ports in the network firewalls so that SIP-DECT internal components (RFPs, OMM) can communicate with each other or with connected servers (for example, call server, provisioning). For a list of the IP ports that need to be opened on network firewalls, refer to the *SIP-DECT OM System Manual Administration Guide*.

SSH Console

Each SIP-DECT RFP offers an SSH “User shell” and SSH “Root (SSH only)” shell for maintenance and diagnostics purpose from remote. Whether the console is available or not is controlled by the connected OMM and can be enabled/disabled via the configuration parameter “*Remote access”*. The SSH is version SSHv2.

Recommendation

- It is recommended to disable the “Remote access” when not needed. It is disabled by default. For more details, refer to the SIP-DECT OM System Manual Administration Guide.

Client Security

SIP-DECT includes the following measures to ensure VoIP security:

- Network access authentication protocol (802.1X)
- Encryption of voice and call signaling streams
- Authentication to call control

Network access authentication is used to ensure that only authorized users are allowed access to the network. Encryption is used to conceal the information that is being exchanged from unauthorized users and applications.

Client Network Access Authentication

Most enterprise grade L2 switches support 802.1x access authentication on their network ports. When 802.1X access authentication is enabled on the switch, an RFP connecting to one of these ports needs to be authenticated as valid before full network connections can be established.

SIP-DECT supports the IEEE 802.1X authentication protocol for the SIP-DECT RFPs.

Recommendation

- It is recommended that the L2 switches used throughout the LAN support the IEEE 802.1X protocol and that this capability be enabled by the administrator.

Signaling Encryption - Secure Connections

SIP-DECT uses the Session Initiation Protocol (SIP) for call control signaling. The following transport protocol modes are supported:

- UDP
- TCP
- UDP/TCP
- TLS
- Persistent TLS

Recommendation

- It is recommended to use TLS or persistent TLS as transport protocol mode. The TLS security protocol provides data encryption, server authentication message integrity, and optional client authentication for a TCP/IP connection. TLS will prevent unauthorized access to administrative functions. TLS encrypts all traffic on the link to prevent sniffing of user names and passwords.
- Furthermore, it is recommended to use the TLS protocol version 1.2 and/or 1.3. The usage of earlier TLS protocol versions is not recommended and still offered only for legacy reasons.

Media Encryption - Secure Connections

Client Media Streaming

Media path security between SIP-DECT phones or between a SIP-DECT phone and a controller/server is accomplished with the Secure Real Time Protocol (SRTP), which is a standards-based protocol that uses the 128-bit Advanced Encryption Standard (AES) and is described by RFC3711. See Figure 3 for message flow.

The following SRTP crypto suites are supported by all current RFPs:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

The SIP-DECT OMM specifies streaming connections use SRTP based on whether SRTP is enabled on the SIP-DECT OMM and the capabilities of the connection endpoints. If SRTP is enabled and supported by both end points, then SRTP is chosen.

SIP-DECT distinguishes between three different SRTP modes:

- **SRTP only**: Only SRTP calls will be accepted, all other will be rejected (the audio part of the SDP contains RTP/SAVP).
- **SRTP preferred**: All calls will be initiated as secured but accepted if they are not secured (the audio part of the SDP contain RTP/AVP—audio/video protocol).
- **SRTP disabled**: Only RTP calls will be initiated as not ciphered and incoming ciphering algorithm will be not accepted. All communications are established unencrypted.

Recommendation

- It is highly recommended to use media encryption (SRTP) in combination with signaling encryption (TLS) to ensure that the negotiated SRTP encryption keys are transferred encrypted.

RFP to RFP Media Streaming

As soon as an encrypted media stream is used, any necessary media streams between the SIP-DECT RFPs are also encrypted via SRTP.

RFP to RFP media streams can be used in case of DECT phone handover to another base station or when using SIP-DECT internal third-party conference.

DECT Encryption

The DECT air interface between a DECT handset and a base station is encrypted by default. SIP-DECT supports two levels on encryption:

- Standard DECT encryption is ON by default
- Enhanced security is OFF by default

When a DECT handset is enrolled (subscribed) to the SIP-DECT system, a standardized DECT key allocation procedure negotiates a *User Authentication Key* (UAK) with the handset. This procedure does not transmit the UAK over the air. Both entities, the OMM and the handset, calculate this key from the *Authentication Code* and a random value is administered in the OMM and manually input in the handset

during this enrollment procedure. Only the random value is transmitted over the air. The calculated *User Authentication Key* is safely kept in the OMM database (encrypted) and in the handset.

Each time a handset initiates a connection to the system, the handset is authenticated. Each call control connection is ciphered, and audio and call related information is transmitted encrypted in both directions. For each new established connection, another cipher key is negotiated during authentication procedure.

SIP-DECT implements a more secure mechanism than the DECT standard requires. SIP-DECT ciphers a connection with a per connection calculated cipher key and then authenticates the handset in this ciphered connection. During authentication, a new cipher key is calculated for use to establish a subsequent connection. Some handsets that may not fully comply with the DECT GAP standard may not support this procedure. In this case, the administrator can fall back to the more unsecure DECT standard procedure by activating *Authentication before ciphering* in OMP menu “System > Basic Settings > DECT”, the default setting for which is OFF.

SIP-DECT supports a feature for *enhanced security* that allows early encryption of a DECT connection. No unencrypted information is transmitted in this mode. The cipher keys are changed every minute for the active link. This feature has an impact on the compatibility of other GAP handsets. After a handset is enrolled in enhanced security mode, the handset can no longer communicate with the system without early encryption. If early encryption fails, no communication is possible at all.

Recommendation

- Always enable the encryption in “System > Basic settings > DECT”.
- Enable enhanced encryption mode in all sites of the SIP-DECT system or do not enable this option at all.
- It is not recommended to activate *Authentication before Ciphering* procedure in “System > Basic settings > DECT”. If only a very few handsets are incompatible to operate in this mode, it can be a better approach to configure these handsets to never cipher a connection instead operating all other handsets in a less secure mode. Alternatively, the customer may replace the incompatible handsets by Mitel’s 600d DECT handsets.

User Authentication and Access Control

All DECT phones must go through a successful DECT subscription method before they can access a SIP-DECT system. For this, the subscription must be activated in the OMM and, depending on the subscription method, different user and/or device data must be configured, and different access controls are used.

The SIP-DECT solution supports the following subscription methods:

- **standard subscription with IPEI**
  The manual subscription method is characterized by user and device data with a fixed association in the OMM database. Both user and device data are configured in one step.
  Only a subscription attempt from a phone with matching IPEI (International Portable Equipment Identity) is granted.
- **wildcard subscription**
  Wildcard subscription allows the assignment of DECT phones to users without any device administration. Wildcard subscription works only for fixed associations between user and device data sets.
- **auto-create on subscription**
  Auto-create on subscription allows the automatic subscription of DECT phones, without any device administration. This subscription method creates an unbound device data set. The device is mapped to a specific user data set when the user logs in to the phone.

SIP-DECT basically distinguishes between two types of association between a DECT phone data set a user data set:

- a fixed association indicates that this user is assigned to use the specified DECT phone, and vice versa.
- a dynamic association indicates that the DECT phone can be used by more than one user. The association is established with user login. The login is authenticated by a user specific PIN.

For more details, refer to SIP-DECT Phone Sharing and Provisioning Administration Guide and SIP-DECT OM System Manual Administration Guide.

Recommendation

- Enable the DECT Subscription only when subscribing new DECT handsets and disable it when not needed anymore.
- Configure a “DECT authentication code” to secure that only granted phones can subscribe.
- Use wildcard subscription only in dedicated secure environments.
- For user logins, configure user specific PINs with sufficient complexity.

OMM – IP-RFP Encryption

During an RFP enrolment with OMM, an RFP specific random authentication key is exchanged between OMM and RFP used for authentication and encryption.

The enrolment of RFPs comprises the following 2 steps:

- Add RFP to OMM database (create DB entry for the RFP)
- First connection between RFP and OMM

Recommendation

- It is a precondition that the enrolment of the RFP takes place in a safe environment; that is, the installer ensures that an authentication key exchange between RFP and OMM during enrolment cannot be compromised: no man-in-the-middle attack possible, no tampered RFP, and so on.

For more details, refer to *SIP-DECT OM System Manual Administration Guide* chapter 2.34 “*RFP Enrolment encryption with authentication key*”.

MOM – OMM Encryption

MOM uses the OMM AXI login and data transfer for OMM administration and user and device data distribution to and from the OMMs. The connections are TLS 1.2 or 1.3 connections. The connections are used for synchronization of user and device data and to support roaming of users and devices over different OMM sites. All related data are stored in the MOM and distributed on demand to the OMM where the data are needed for telephony or messaging service. The MOM is not involved in signaling of phone calls or message signaling. A call server connection to the MOM is for provisioning user and device data only.

WLAN Security

The DECT base stations RFP 48 WLAN and RFP 43 WLAN include an integrated WLAN access point.

Refer to the *SIP-DECT OM System Manual Administration Guide chapter 9.17 “WLAN configuration”* for configuration details to allow secure operation.

Secure Development Life Cycle

Security and privacy threats are constantly being developed and exiting 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.

SIP-DECT Release 9.1 was developed in accordance with Mitel's Secure Development Life Cycle policy, as a result, SIP-DECT Release 9.1 has been designed with the best practice safeguards to mitigate risks to the confidentiality, integrity and/or availability of data contained within SIP-DECT and to the data related to the functionality provided by SIP-DECT.

Appendix A – SIP-DECT – Important Product Information for Customer GDPR Compliance Initiatives

Introduction

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 SIP-DECT customers that are putting security processes and security controls in place to comply with data security regulations.

This document is intended to assist Mitel SIP-DECT customers with their data security regulations compliance initiatives by:

- Identifying the types of personal data that are processed by SIP-DECT
- Listing the SIP-DECT Security Features that customers may require to achieve compliance with security regulations
- Providing a description of the SIP-DECT Security Features
- Providing information on where the SIP-DECT 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. Administration of SIP-DECT OM Manager(OMM) is done with the OM Management Portal application (OMP) or using the web interface.

What is New in this Release

With Release 9.1SP1, Mitel introduces the SIP-DECT Event Manager as an integrated software component of the SIP-DECT system. It is used for the automated processing of incoming events and the sending of outgoing notifications. The SIP-DECT Event Manager can process events from various sources, including SIP-DECT end devices, the SIP-DECT system itself and other external systems..

Personal Data Collected by SIP-DECT

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

- End users of SIP-DECT, typically Mitel customer employees using Mitel phones and collaboration tools.
- Customers of Mitel customers – for example, call recordings contain personal content of both parties in the call; the end-user's personal contact lists may contain personal data of business contacts; short messages may contain personal content of both parties.
- System administrators and technical support personnel – Logs and audit trails contain records of the activities of system administrators and technical support personnel.
- Other persons information contained in end user’s short messages

Personal Data Processed by SIP-DECT

SIP-DECT **processes** the following types of data:

- **Provisioning Data:**
  - The end user's name, business extension phone number, mobile phone number, location, department and email address.
- **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:**
  - Voice mail, call recordings, and personal contact lists.
- **User Personal Settings:**
  - Service settings (login password, PIN, display language and so on), and call forwarding destination and its modes.
- **User Device Related Data:**
  - User device login and device subscription data.

Personal data processed by the SIP-DECT 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.

Personal Data Transferred by SIP-DECT

The types of **personal data transferred** among the SIP-DECT and various applications and services will depend on the specific use requirements of those applications or services, for example:

- **Provisioning Data:**
  - The user's first name, last name, office phone number, user description such as department, SIP account data, user account information, and any user device data.
- **Maintenance, Administration, and Technical Support Activity Records:**
  - System and content backups, logs, diagnostic debug trace logs, and audit trails.
  - Voice quality logs and voice quality statistics.
  - System management activity, such as login and logout, and activity audit logs may be transferred to secondary storage or to technical support personnel.
- **User Activity Records:**
  - User’s call status data, location data including date and time, and text message data including date and time. These data may be shared globally between (clustered) SIP-DECT systems connected to a SIP-DECT Multi OMM Manager (MOM) application, a call server, alarming and locating application (OML), and management systems connected through Application XML Interface (AXI) synchronization protocol.

- **User Personal Content:**
  - Voice mails and personal contact lists.
  - Text message content may be shared globally between (clustered) SIP-DECT systems connected to a SIP-DECT MOM, a call server, alarming and locating application, and management systems connected through AXI synchronization protocol.
- **User Personal Settings:**
  - Service settings (login password, PIN, display language, and so on), and call forwarding destination and its modes.
- **User Device Related Data:**
  - User device login and device subscription data.
- **User account information:**
  - SIP account data may be shared between SIP-DECT and connected call server through AXI synchronization protocol.

How SIP-DECT Security Features Relate to GDPR

SIP-DECT 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 4 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 4: SIP-DECT Security Features that 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. The SIP-DECT OMM,MOM and Event Manager are not intended to allow standard telephony users to log in. OMM,MOM and Event Manager Administrators configure additional accounts only for other administrators or for tools or for machine APIs that need to log in. Access to the system is limited by allowing only authorized access that is authenticated using encrypted user name/password login combination. Failed logins are logged but are not restricted to a maximum of attempts Communications to the system are performed over authenticated, encrypted communications channels using HTTPS (TLS 1.3 or 1.2). As of Release 9.1, support for TLS 1.1 has been discontinued. A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs) and firewalls.	See the document SIP-DECT OM System Manual Administration Guide, Chapter 4.3 System Configuration, Chapter 1.6 Logins and Passwords, Chapter 6.1 Login (through web service), Chapter 7.3 Login (through OMP), Chapter 7.7.6.1 Creating New User Accounts. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide, Chapter Installation and Configuration > Additional system configuration > Managing MOM user accounts. For OML, see the document

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
	The user of a DECT phone should secure their device with a PIN to protect the access. In all cases, physical access to systems should be restricted by the customer.	SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Installation and Configuration > Administration > Managing Users.
Communications Protection	All personal data transmissions use secure channels. For system integrity and reliability, all provisioning interfaces use secure channels. **Voice Streaming** The administrator may configure SIP-DECT OMM to encrypt all IP voice media streams with AES 128. Note that not all SIP providers and third-party SIP devices support encryption; if permitted, the communications will negotiate to no encryption. The DECT protocol uses the “DECT Standard Cipher” for encryption over air by default. **Voice Call Signaling** Only authenticated DECT phone devices may connect to SIP-DECT OMM. The DECT protocol uses the “DECT Standard Cipher” for encryption over air by default. SIP call signaling between SIP-DECT OMM and the PBX for SIP phones may be secured with TLS 1.3 or 1.2 dependent from the PBX configuration. As of Release 9.1, support for TLS 1.1 has been discontinued. **Call Privacy** Only authenticated DECT devices can connect to Mitel SIP-DECT. The DECT protocol uses the “DECT Standard Authentication Algorithm” for authentication process. The user of a DECT device may secure their device with a PIN to protect device access. **Messaging** Messages sent between SIP-DECT OMM and the OML application are always encrypted using TLS 1.3 or 1.2. Messages sent between the SIP-DECT Event Manager and OMM via SIP-DECT interface are always encrypted (AXI). Messages sent between the SIP-DECT Event Manager and external applications via ESPA interface are not encrypted (ESPA v.4.4.4 TCP server socket). Messages sent between the SIP-DECT Event Manager and external applications via SNMP interface are not encrypted (SNMP V2 client via TCP)	See the document SIP-DECT OM System Manual Administration Guide, Chapter 2.5 VoIP Encryption, Chapter 4.3 System Configuration, Chapter 6.4.1.2 DECT settings, Chapter 7.7.1.2 DECT settings, Chapter 9.26 SRTP [for telephony], Chapter 9.27 SIP over TLS, Chapter 9.27.2 SIP over TLS certificates, Chapter 9.27.6 Additional Security Considerations. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide, Chapter Multi-OMM Manager Installation and Configuration > Getting started with the Multi-OMM Manager > System requirements (firewall setting). For OML, see the document SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Installation and Configuration > Administration > Managing Users. For Event Manager, see the document SIP-DECT Event Manager System Manual, Chapter Using the SIP-Dect Event Manager

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
	Communications to the system are performed over authenticated, encrypted communications channels using HTTPS or SSH (TLS 1.3 or 1.2). The SIP-DECT OMM and MOM support two restriction levels: full access and read-only access. System provisioning needs full access. The SIP-DECT OML application supports only HTTP and not HTTPS protocol; but the application is installed on a Linux server, which may provide an HTTPS proxy to secure the network interface. When installing the HTTPS proxy on the same server on which the OML application is installed, the Linux administrator configures the server firewall to forward external OML HTTP requests to the HTTPS proxy from any network address other than the *localhost* address. All URI destination configurations in SIP-DECT must be configured to use secure connections; for example, HTTPS (TLS 1.3 or 1.2). A customer can further limit access over the network using standard network security techniques such as VLANs and firewalls.	
Access and Authorization	All personal data processing is protected with access and authorization controls, this includes personal data processing by data subjects, Administrators, technical support, and machine APIs. All system data processing and all access to databases, files, and operating systems, are protected with encrypted access and authorization controls. For use of the OML application, see administration rule as described in “Communication protection” above. SIP-DECT OMM defines different permissions to an administrative account to allow limited access to the system. The administrator can have full access or read-only access. The administrator must also define permissions for machine API logging in.	See the document SIP-DECT OM System Manual Administration Guide, Chapter 1.6 Logins and Passwords, Chapter 6.1 Login (through web service), Chapter 6.4.4 User Administration (password rules) Chapter 7.3 Login (through OMP), Chapter 7.7.6.1 Creating New User Accounts. For MOM, see document SIP-DECT Multi-OMM Manager Administration Guide, Chapter Multi-OMM Manager functionality > MOM Interface [login area], Chapter Multi-OMM Manager Installation and Configuration > Additional system configuration > Managing MOM user accounts, Chapter Multi-OMM Manager and Installation > Getting started with the Multi-OMM Manager > Logging in and setting the system name. For OML, see the document SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Application Quick User Guide > Login / Logout.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
Data Deletion	The system provides an administrator with the ability to erase the end user's personal data. **Deleting a User and Phone Services** SIP-DECT allows the administrator to delete an end user and all of the end user's associated phone services. **Deleting Logs** Certain types of logs cannot be deleted on a per user basis such as messaging logs, error logs and debug trace logs. However, SIP-DECT provides the administrator with the ability to delete the entire contents from all logs. The system administrator can, once authenticated, log in to the shell, locate, and delete the entire file. **Note**: Some logs such as messaging data or debug trace logs are transferred outside of the SIP-DECT system. There is no control of the SIP-DECT system on who traces and how logs are treated outside the system. 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. **Deleting short message content** The SIP-DECT OML application generates and stores end user's short message content. This content cannot be erased in the OML application. The content must be erased by deleting the user record in the connected SIP-DECT OMM. The administrator may erase the end user's data through web interface or SIP-DECT OMP administration tool. SIP-DECT does not store any voicemail data. The administrator must erase any voicemail data in the originating call server system.	See the document SIP-DECT OM System Manual Administration Guide, Chapter 7.7.6.3 Deleting User Accounts, Chapter 7.11.2 "Users" Menu. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide, Chapter Multi-OMM Manager Installation and Configuration > Additional system configuration > Managing MOM user accounts, Chapter Multi-OMM Manager Installation and Configuration > Centralized user and device data management > Adding a new data set > Deleting a user or DECT phone record. For OML, see the document SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Installation, and Configuration > Administration > Managing Users.
Audit	Audit trails are supported to maintain records of administrator login for a limited time. Records of data processing activities are not collected in the system but may be collected by external applications.	See the document SIP-DECT OM System Manual Administration Guide, Chapter 6.4.8 Event Log Menu. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide, For OML, see the document SIP-DECT OM Locating Application Administration Guide.

Security Feature	Relationship to Data Security Regulations	Where the Feature is Documented
End Customer Guidelines	SIP-DECT Security Guidelines is available to assist with installation, upgrades, and maintenance, refer to the SIP-DECT OM System Manual Administration Guide.	See the document SIP-DECT OM System Manual Administration Guide, Chapter 4.3 System Configuration, Chapter 9.26 SRTP [for telephony], Chapter 9.27 SIP over TLS, Chapter 9.27.2 SIP over TLS certificates, Chapter 9.27.6 Additional Security Considerations. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide, Chapter Multi-OMM Manager Installation and Configuration > Additional system configuration > Managing MOM user accounts. For OML, see the document SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Installation, and Configuration > Overview > Notes on Operating Conditions.

Data Security Regulations

This section provides an overview of the security regulations that SIP-DECT customers may need to be compliant with.

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.

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 4 explains what personal data is processed by Mitel's SIP-DECT and highlights available security features to safeguard such data.

Appendix B – Secure Installation Checklist

1 System Security	Y	N
The default login credentials are replaced with sufficient complexity passwords (OMP->System->User administration)		
DECT base station capturing (OMP->DECT base stations->Capturing) is disabled after enrollment of new base stations (RFP).		
Remote access is disabled (OMP->System->Basic settings->General->Remote access)		
Security level "High" (OMP->System->Advanced settings->Security) is activated and either the default ciphers or individual ciphers with sufficient security are configured.		

2 DECT Security	Y	N
Encryption (OMP->System->Basic settings->DECT->Encryption) is activated		
Enhanced DECT security (OMP->Sites->Enhanced DECT security) is activated for all sites or for no site.		
DECT authentication code (OMP->System->Basic settings->DECT authentication code) is configured. Non-predictable and non-trivial digit sequence is used.		
Restricted subscription duration (OMP->System->Basic settings->Restricted subscription duration) is activated and/or subscription is disabled after subscribing new DECT phones		
Authentication before ciphering (OMP->System->Basic settings->DECT->Authentication before ciphering) is OFF.		
All DECT phones (OMP->DECT phones->Devices) have Encryption enabled.		
If the "user login" feature is used, user individual PINs with sufficient complexity are configured		

3 Signaling Security	Y	N
Persistent TLS or *TLS* is used as SIP *Transport protocol* (OMP->System->SIP->Transport protocol)		
TLS authentication (OMP->System->SIP->Security->TLS authentication) is enabled		
TLS common name validation (OMP->System->SIP->Security->TLS common name validation) is enabled		
All necessary TLS certificates for the caller server used have been imported (OMP->System->SIP->Security->PEM file import)		
All SIP-DECT users have individual SIP passwords with sufficiently complexity (OMP->DECT phones->Users->Password)		
A strong Security level (OMP->System->SIP-Security->Security level) with a secure cipher list selection is used		
TLS version 1.2, *1.3* or *Auto* (OMP->System->SIP-Security->TLS version) is used		

4 Media Security	Y	N
SRTP Preferred or *SRTP Only* is activated on all sites (OMP->Sites->SRTP)		

The following check lists are optional and relevant only if the underlying feature is used.

5 Provisioning Security (optional)	**Y**	**N**
Only the secure protocols FTPS, HTTPS or SFTP are used in general or specific URLs (for example, OMP->System->Provisioning->General->Protocol)		
If the TLS based protocols FTPS/HTTPS are used, following settings are enabled (OMP->System->Provisioning->General): • *Validate certificates* • *Validate expires* • *Validate hostname*		
For TLS based protocols: • All necessary TLS certificates for the provisioning server used have been imported (OMP->System->Provisioning->Provisioning certificates) • A strong Security level (OMP->System->Provisioning->General->Security level) with a secure cipher list selection is used • *TLS version 1.2*, *1.3* or *Auto* (OMP->System->Provisioning->General) is used		

6 Corporate Directory (optional)	**Y**	**N**
Secure protocols are used: • for XSI or XML: HTTPS (OMP->System features->Directory->URL->Protocol) • for LDAP: *StartTLS* or *LDAPSecure* (OMP->System features->Directory->URL->Security)		
Use common certificate configuration (OMP->System features->Directory->URL->Use common certificate configuration) is enabled and the TLS settings of checklist 5 are done		

7 XML applications (optional)	**Y**	**N**
HTTPS is used as transport (OMP->System features->XML applications->Protocol) for all activated XML applications		

8 DECT phone's firmware update (optional)	**Y**	**N**
FTPS or *HTTPS* is used as transport (OMP->Support->DECT phones firmware update->Protocol)		

9 Automatic DB export (optional)	**Y**	**N**
FTPS or *HTTPS* is used as transport (OMP->System->Data management->Protocol)		
Use common certificate configuration (OMP->System->Data management->Use common certificate configuration) is enabled and the TLS settings of checklist 5 are done		

Product Security Information

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

Mitel Product Security Advisories

Mitel Product Security Advisories are available at:

https://www.mitel.com/support/security-advisories

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 center security.

Mitel Product Security Documentation is available at:

https://www.mitel.com/document-center