



A MITEL  
PRODUCT  
GUIDE

# Mitel SIP-DECT 9.2 Event Manager

System Manual

Version SIP-DECT 9.2

Document Version 1.2



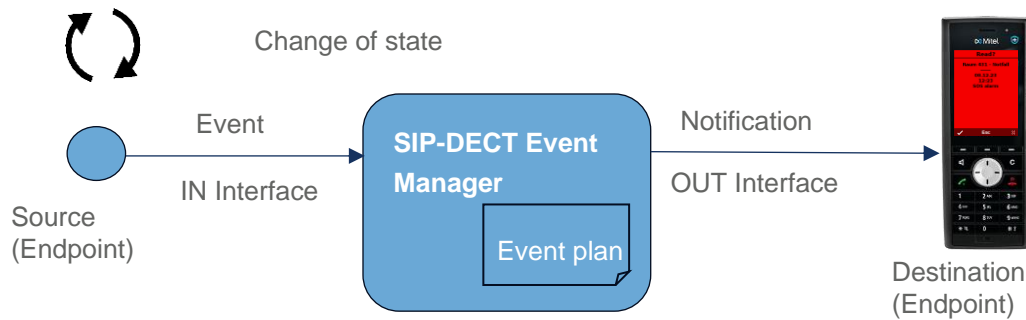
## Table of Contents

Overview .....	3
Introduction .....	3
Where is the SIP-DECT Event Manager running? .....	4
Accessing the SIP-DECT Event Manager .....	5
License Requirements for the SIP-DECT Event Manager.....	5
Supported DECT Phones .....	5
Using the SIP-DECT Event Manager .....	6
SIP-DECT Event Manager GUI .....	6
1 Login Area .....	6
2 Configuration panes.....	6
Interfaces .....	7
SIP-DECT (OMM) Interface.....	8
ESPA Interface .....	10
Modbus interface .....	15
SNMP interface.....	18
Event types .....	21
Notification profiles.....	21
Notification groups .....	22
Event plans .....	22
Locations.....	24
User.....	25
System .....	25
Monitor .....	26
Quick Start Configuration Guide SIP-DECT Event Manager .....	27
Configuring SOS alarm trigger from a DECT phone.....	27
Configuring ESPA interface .....	30
Appendix.....	33
Sitemap .....	33
Web UI Parameter, Action & Status Information overview .....	35

## Overview

### Introduction

The SIP-DECT Event Manager is an integrated software component of a Mitel 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 terminals, the SIP-DECT system itself, and other external systems. The processing of the events is carried out according to user-defined rules set by the administrator.



The primary flow is to send notifications as text messages to SIP-DECT phones, which are triggered by incoming events. In this way, SIP-DECT supports customer workflows beyond voice calls, e.g., text messages can be sent to DECT phones to inform about events from nurse call systems without the need for additional hardware.

Processing rules for different types of events consist of event plans, their event phases, notification profiles and different types of confirmation requests.

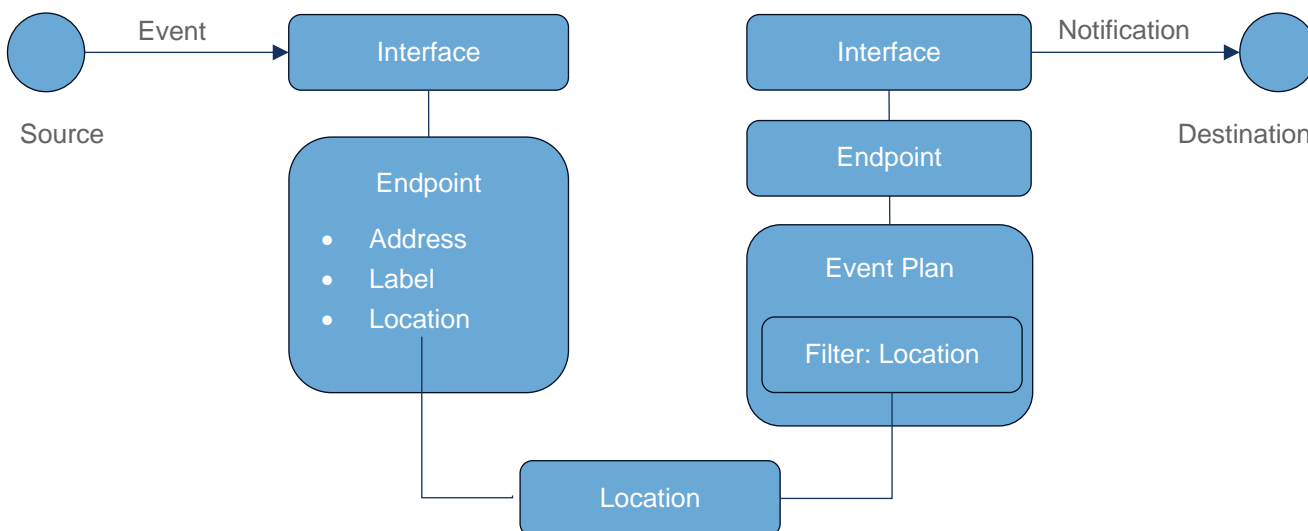
If there is a change in status, e.g., a key press, a source sends an event to the SIP-DECT Event Manager via an input interface. The SIP-DECT Event Manager generates notifications, e.g., text messages, and sends them to destinations, e.g., DECT telephones via outgoing interfaces according to a suitable event plan.

Some interface types are only incoming or only outgoing interfaces, and some can be both incoming and outgoing.

Sources and destinations are called endpoints. They are assigned to the interfaces through which they communicate with the SIP-DECT Event Manager. Endpoints have a unique identification e.g. a telephone number.

Endpoints are also assigned to locations. Depending on the location, a specific event plan can be selected. This allows the same event to be treated differently depending on where it originated.

The following illustration is intended to visualize the relationships between endpoint location and the event plan location filter.



## Where is the SIP-DECT Event Manager running?

The SIP-DECT Event Manager may run on a 4th generation RFP (RFP44, RFP45, RFP47 or RFP48 WLAN) and is part of the iprfp4G.dnld SW package.

The SIP-DECT administrator determines in the OMC (OM Configurator) on which RFP the SIP-DECT Event Manager is started. This allows a different RFP to be used than the RFP used by the OMM, so that the OMM and SIP-DECT Event Manager do not compete for the same resources.

This also implies that the SIP-DECT Event Manager RFP (the RFP on which the SIP-DECT Event Manager runs) has a local static IP configuration. This ensures that the SIP-DECT Event Manager can be started independently of other services and is always accessible under the same IP address, as is usual for services. Only one SIP-DECT Event Manager per SIP-DECT installation is supported.

To start the SIP-DECT Event Manager the “Start Event Manager” flag must be set as shown below.

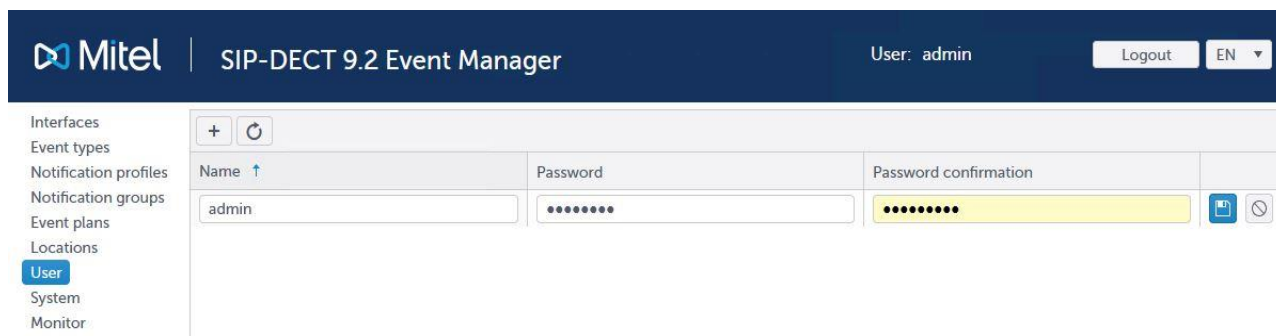
The screenshot shows the 'OM Configurator' window. At the top, there's a table with columns: MAC address, local config, IP address, Net mask, Router, OMM address, 2nd OMM address, TFTP server, and TFTP file name. Below this, there's a 'Detail Data' section for MAC address 08:00:0f:c3:df:0a. The 'General' tab is selected, showing fields for OMM address, 2nd OMM address, TFTP server address, TFTP file name, Syslog server address, and Syslog server port. A red box highlights the 'Start Event Manager' checkbox, which is checked. To the right, there's a 'Tasks' panel with various actions like Scan, Add RFP, Clear List, etc.

If this “Start Event Manager” flag is removed again from an RFP via the OMC, the Event Manager will be stopped, and its database will be removed only during the next start of this RFP.

## Accessing the SIP-DECT Event Manager

The SIP-DECT Event Manager has its own web administration interface which is available via `https://<RFP IP address>:8444`.

Use **admin** as the username and password to login for the first time. During login for the first time, the user is asked to change the password.



The screenshot shows the Mitel SIP-DECT 9.2 Event Manager web interface. The top header bar is dark blue with the Mitel logo on the left, the title 'SIP-DECT 9.2 Event Manager' in the center, and 'User: admin' on the right. To the right of the user name are 'Logout' and 'EN' buttons. A left sidebar contains a list of navigation items: Interfaces, Event types, Notification profiles, Notification groups, Event plans, Locations, User (highlighted in blue), System, and Monitor. The main content area shows a form for creating or editing a user. It has a table with columns: Name (with an up arrow icon), Password, and Password confirmation. The 'Name' field contains 'admin'. The 'Password' and 'Password confirmation' fields are masked with dots. There are '+' and 'refresh' icons at the top of the table. On the right side of the table, there are icons for a document and a lock.

## License Requirements for the SIP-DECT Event Manager

The SIP-DECT Event Manager requires a license for the configured and activated endpoints. There is a built-in license available already for 5 endpoints.

For additional endpoint licenses a SIP-DECT license is required which covers the amount of configured SIP-DECT Event Manager endpoints. It is strongly recommended to import this license into the OMM before the configuration of the Event Manager.

If the number of configured SIP-DECT Event Manager endpoints exceed the number of licensed endpoints, a warning is displayed on the administrator web interface and notifications are sent to various randomly selected SIP-DECT endpoints every 15 minutes. These notification messages are not monitored by the Event Manager and could not be deleted from within the application (also in case the license would be updated to cover the configured number of endpoints). The notifications will be visible on the SIP-DECT terminals as long they are not read and deleted on the terminals itself.

The SIP-DECT Event Manager uses advanced SIP-DECT messaging and alerting features without requiring a “Mitel SIP-DECT Messaging & Alerting License Enterprise” license.

The SIP-DECT Event Manager provides location information for SIP-DECT alarm trigger e.g. SOS-Key or Man-Down automatically without requiring locating license “Mitel SIP-DECT Locating User License XXX”. The OM Locating application is also not needed to operate SIP-DECT Event Manager.

## Supported DECT Phones

The SIP-DECT Event Manager supports the 700d DECT phone family. The SIP-DECT 600d V2 DECT phone family is also generally supported. Older generations of the 600d device family or their older SW versions may not support all SIP-DECT messaging features and may therefore have limitations. Please also note the information in the Mitel 600/700 DECT Phone Messaging and Alerting Applications user guide.

## Using the SIP-DECT Event Manager

To take the first practical steps with the SIP-DECT Event Manager as quickly as possible, you can start with the section [Quick Start Configuration Guide SIP-DECT Event Manager](#).

### SIP-DECT Event Manager GUI

The SIP-DECT Event Manager has its own web administration interface which is available via <https://<RFP IP address>:8444>. The web interface consists of a series of web pages that are used to configure the various settings of the SIP-DECT Event Manager and can be accessed from any computer or device with a web browser on the same network. The web service is implemented as a single-page application (SPA).



### 1 Login Area

#### Language Selection

The following languages are available: German, English, French and Spanish. When creating the configuration there are numbers of standard values (e.g. event types) set up in the language selected at this time. These values contained in the configuration are not affected by switching the language.

Use 'admin' as the username and password to login for the first time. During login for the first time, the user is asked to change the password.

### 2 Configuration panes

The SIP-DECT Event Manager includes multiple panes that contain different information about the SIP-DECT Event Manager.

Configuration Pane	Description
<b>Interfaces</b>	The Interfaces pane provides an overview of the status of systems connected to the SIP-DECT Event Manager. Currently only ESPA, SIP-DECT (OMM), Modbus (e.g. WAGO), and SNMP interfaces are available. The number of interfaces to be set up is currently limited to 5 interfaces.
<b>Event types</b>	<p>The Event types pane allows to create new or change existing Event types. There are <b>5 default</b> Event types ('Man Down', 'No Move', 'Escape', 'SOS-key' and 'System Info') available. These types cannot be deleted.</p> <p>The Event type serves as a kind of filter in an Event plan to control the escalation of an event. Based on the assigned priority, the system can be informed in which order the event should be processed.</p>

Configuration Pane	Description
Notification profiles	The display and acoustic signaling of an event on the SIP-DECT terminals can be configured within a notification profile.
Notification groups	Endpoints that can receive notifications (e.g. SIP-DECT terminals) can be combined into a notification group. This simplifies the configuration.
Event plans	The Event plans pane allows to create, edit and delete event plans. An Event plan specifies how received events should be handled depending on the location of the originating endpoint. The plan specifies which endpoints should receive notifications and how to react if acknowledgements are not received. An event plan can include one or more event types and one or more locations. It means that the event plan will only be used for events of the configured type and if the originating endpoint belongs to the specified location.
Locations	<p>The Event Manager supports the management of locations to which endpoints are assigned as sources of events. Locations are assigned to event plans too.</p> <p>This allows the location-specific definition of event plans, i.e. it is possible to notify different recipients depending on the location of the sender of an event.</p>
User	The Users pane allows to create, edit and delete users. The default user <b>admin</b> cannot be deleted.
System	The System pane includes different tabs for naming the system, showing the current software version, for the configuration of a Watchdog and to activate the CloudLink daemon for the remote management. Here can also be performed functions such as Restart, Restart with factory defaults, Export log, Import config, and Export config. The import of SSL certificates is available as well as the configuration of a security level and the used Cipher Suites. In case of activated CloudLink daemon the detailed configuration and displaying the status of it is available.
Monitor	The Monitor pane shows a list of active event handlings and allows the administrator to end a single event or all events.

## Interfaces

Interfaces connect the SIP-DECT Event Manager to other devices and services. Depending on the type, these interfaces support receiving events or sending notifications, sometimes both.

The following types of interfaces can be configured:

- SIP-DECT (OMM)
- ESPA
- Modbus (e.g. WAGO/MOXA)
- SNMP

Under the **Interfaces** configuration pane, all configured interfaces are displayed, and can be selected and edited.

<b>Interfaces</b> Event types Notification profiles Notification groups Event plans Locations User System Monitor	<div> <div>+</div> <div>↺</div> </div>							
	Active	State	Label ↑	Description	Type	Endpoints		
	✓	●	<a href="#">ESPA-37-79-10002</a>	ESPA-37-79-10002	ESPA	7		
	✓	●	<a href="#">MODBUS-MOXA-33-116</a>	MODBUS-MOXA-33-116	Modbus	3		
	✓	●	<a href="#">MODBUS-WAGO-33-109</a>	MODBUS-WAGO-33-109	Modbus	5		
	✓	●	<a href="#">OMM-37-182</a>	OMM-37-182	SIP-DECT	4		
	✓	●	<a href="#">SNMPO-37-197-Inform</a>	SNMP-37-79-162 (inform)	SNMP	1		

## SIP-DECT (OMM) Interface

The SIP-DECT (OMM) interface is already created by default and cannot be deleted. It contains the following tabs:

### General Tab

The **General** tab is used to configure the OMM IP address(es), user and password. With this configuration the SIP-DECT Event Manager will be able to connect with the OMM. A successful connection is indicated by the interface status turning to green in the interfaces overview tab. The 'User defined event text' box must be selected to take effect the settings under the tab 'User defined event text'.

<

Interface: OMM-37-182

General

Endpoints

User defined event text

Import endpoints

Save

Refresh

OMM 1

10.103.37.182

OMM 2

User

omm

Password

●●●●●●●●

User defined event text

☒

### Endpoints Tab

The **Endpoints** tab is used to define the destinations or receivers of messages in the SIP-DECT event. To simplify the setting up of the endpoints on the SIP-DECT interface, these endpoints can be imported via the 'Import endpoints' tab.

Please be aware that an endpoint which is not marked as active, cannot be used to trigger an alarm and is not counted as a licensed endpoint. Inactive endpoints are marked with (\*) in other configuration panes as shown below.

<div> <div>&lt;</div> <div>Interface: defaultOMM</div> </div>				
<div> <div>General</div> <div>Endpoints</div> <div>User defined event text</div> <div>Import endpoints</div> </div>				
<div> <div>+</div> <div>↺</div> <div>🔍</div> <div>🗑️</div> </div>				
Active	Address (Phone number) ↑	Label	Location	
✗	118	User 118		
✓	120	User 120		





<
Location: root

Endpoints assigned	Endpoints available
defaultOMM / User 118 (*) / 118	
defaultOMM / User 120 / 120	
defaultOMM / User 126 / 126	
defaultOMM / User 141 / 141	
ESPA -IF-1 / ESPA EP 9000 / 9000	

### **User defined event text Tab**

The **User defined event text** tab is used to customize special types of text to be sent to the DECT phones when an event is handled.

This function allows organizations, agencies, or individuals to create and send messages with specific details or instructions that are relevant for a special situation.

The texts defined in this section only take effect when the checkbox 'User defined event text' under tab 'General' is selected.

The message text is normally made up of the event type and the location of the originating endpoint. The composition of alarm texts can be flexibly configured for each interface with user defined alarm texts.

The text delivered by the interface during the triggering of the event can be changed before the further editing by replacing individual character strings. The character strings to be replaced should be entered in 'Text' and 'Replaced by'.

Up to four texts can be used for the composition of the final alarm text. A maximum length should be defined for each of these texts. Either a space or a line feed can be used as a spacer between these texts. Since line feeds cannot be displayed on all endpoints, they are automatically replaced with spaces where necessary.

The following texts are available:

- Event type
- Event type short – max 8 characters
- Priority – Priority of the alarm defined by the alarm type
- Originating endpoint (name) – Name of the endpoint at which the alarm has been triggered
- Originating endpoint (address) – Address (e.g. phone number) for the endpoint at which the alarm has been triggered
- Location of originating endpoint – Environment to which the alarm which has been triggered is assigned by the configuration or by DECT locating
- Received text from interface – Permits the use of composed alarm texts based on special interface settings (e.g. ESPA)
- Event phase – The designation of the current escalation phase

### **Import endpoints Tab**

The **Import endpoints** tab allows the automatic import of the SIP-DECT devices configured in the SIP-DECT system as endpoints to the SIP-DECT Event Manager configuration. This function can only be used if a connection has been established between the SIP-DECT Event Manager and the SIP-DECT system (OMM).

If the number of endpoints permitted by the license is exceeded during the import, a warning will be displayed.

Only those endpoints should be imported that are really needed.

The imported endpoints can be deleted under the Endpoints tab.

## ESPA Interface

The ESPA interface enables the connection of devices that support data exchange in accordance with the ESPA 4.4.4 protocol. This protocol was defined by the European Selective Paging Manufacturer's Association for controlling radio paging equipment and for connecting fire alarm and light signaling systems.

The SIP-DECT Event Manager supports the ESPA 4.4.4 protocol over IP. This permits the exchange of messages with fire alarm systems, light signaling systems, radio paging equipment and similar systems which also support this interface. An ESPA interface can only operate as an input interface (where the SIP-DECT Event Manager receives messages) and not as an output interface (where the SIP-DECT Event Manager sends messages).

If supported by the other side, the SIP-DECT Event Manager facilitates monitoring of the ESPA connection protocol-wise.

Components are connected directly via TCP/IP byte stream or via RS-232 / IP converter. The SIP-DECT Event Manager acts as a TCP client in an ESPA slave mode.

An ESPA message contains information organized in numbered fields. The following fields are important for configuring the SIP-DECT Event Manager

No.	Designation	ESPA Standard Designation	Remarks
1	Call address	Call Address	16 characters max.
2	Display message	Display Message	128 characters max.
3	Ringtone	Beep coding	
4	Ring type	Call type	
6	Priority	Priority	

Please note: ESPA messages in a wrong format will not be processed. Unknown fields will be ignored. 'Call address' (1) and 'Display message' (2) must always be present in an ESPA record.

The fields 'Beep coding' (3), 'Call type' (4), and 'Priority' (6) have no direct influence on the notifications to the SIP-DECT phones. They are only used to select the right event type.

The ESPA interface contains the following tabs:

- General
- Endpoints
- User defined event text
- Event assignment
- Simulator/Trace

### General Tab

The **General** tab allows configuring the basic settings of the ESPA interface. The following settings can be configured:

- **IP address:** IP address to which the SIP-DECT Event Manager should connect to
- **IP port:** The IP port to which the SIP-DECT Event Manager should connect to
- **Interface supervision:** Select this check box if this interface should be supervised.
- **Determine endpoint by:** Select the method for determining the endpoint. Available

options are 'Call address' (which is the default setting) and 'Message text'.

- **Default event type:** Select the default event type. A specific event type must be created for it in the Event type section. This default event type is used as fallback if nothing else is defined in the Event assignment tab or if nothing fits to the made configuration.
- **Call type 1 (Field 4) terminates event:** Select this check box to terminate the event.
- **User defined event text:** Select this check box if 'User defined event text' should be used.

< Interface: ESPA -IF-1

General Endpoints User defined event text Event assignment Simulator/Trace

Save Refresh

IP address 192.168.2.71

IP port 10001

Interface supervision ☒

Determine endpoint by Call address ▼

Default event type ESPA-Event ▼

Call type 1 (Field 4) terminates event ☐

User defined event text ☒

### Endpoints Tab

The **Endpoints** tab allows the definition of senders of ESPA messages. The assignment of an endpoint to an ESPA message is done based on the call address. The call address can be determined either by the ESPA field 1 (Call address) or by the ESPA field 2 (Message text). If 'Determine endpoint by: Message Text' is set, the message text must contain only the call address and nothing else.

### User defined event text Tab

In the **User defined event text** tab, it is possible to define special content for the notification messages to addressed endpoints (e.g. SIP-DECT terminals). If this feature is not enabled in the **General** tab, the ESPA field 2 (Message text) is used for the notification message. There are two tables available under this tab where a simple text replacement and/or a complete text definition depending on some known parameters is possible.

<
Interface: ESPA

General
Endpoints
User defined event text
Event assignment
Simulator/Trace

Text replacement (not for event type, priority and phase)

Text	Replace by	
ESPA EVENT TEXT	ESPA event text	

Text	Max. length	Spacer	
	20		
	20		
	20		
	20		

### Simple Text replacement

In the table at the top of this tab the received text (field 2) from the ESPA message can be modified.

Text (field 2) of the ESPA message	Replacement rule	Resulting notification text
ESPA EVENT TEXT	ul	ESPA event text

### Compose a new event text based on an ESPA message

In the table at the bottom of this tab the event text can be recomposed from up to 4 elements. These 4 elements can be selected from 8 different event information elements. These information elements are shown in the following example.

<
Interface: ESPA

General
Endpoints
User defined event text
Event assignment
Simulator/Trace

Text replacement (not for event type, priority and phase)

Text	Replace by	

Text	Max. length	Spacer	
<div> Event type Event type short (max. 8) Priority Originating endpoint (name) Originating endpoint (address) Location of originating endpoint Phase Received text from interface </div>	20		
	20		
	20		
	20		

## Event assignment Tab

The **Event assignment** tab allows to define the process of designating or assigning specific tasks, roles, or responsibilities to individuals or teams in response to an emergency event. It is a crucial part of coordinating an effective response to emergencies.

An event type is assigned for incoming ESPA messages based on the Ringtone (field 3), Priority (field 6) or Text (field 2). In addition, a Default event type must be configured for non-assigned types in the **General** tab.

**Interface: ESPA**

General | Endpoints | User defined event text | **Event assignment** | Simulator/Trace

Save Refresh

IP address: 192.168.2.71

IP port: 10001

Interface supervision: ☒

Determine endpoint by: Message text

**Default event type: ESPA**

Call type 1 (Field 4) terminates event

User defined event text

Please select  
System Info  
SOS-Key  
Man Down  
New ESPA Type  
**ESPA**

Rules can be defined in the **Event assignment** tab of the ESPA interface configuration, as following shown.

**Interface: ESPA**

General | Endpoints | User defined event text | **Event assignment** | Simulator/Trace

+ ↺

	Ringtone (3)	or Priority (6)	or Text (2)	Event type
1			TEST2	TEST_TEXT_LONG
2			TEST	TEST_TEXT_SHORT
3		1		TEST_PRIO_1
4		2		TEST_PRIO_2
5	1			TEST_BEEP_1
6	*			TEST_BEEP_*

Rules are displayed in the order of their creation and are also processed in this order (top down). The first matching rule will be applied. Hence, the more specific rules need to be configured first.

The fields are linked 'OR', not 'AND'!

A '\*' can be used as a wildcard in the fields 'Ringtone' and 'Priority'. The assignment is then made for all values used in these fields.

Leading or trailing spaces in the Text field will be removed automatically.

The search for an event will be done in the following order:

1. A search is made for matching values without wildcards.
2. If no such rule applies, the system then searches for wildcards in the 'Ringtone' and 'Priority' fields.
3. If it is also then not possible to assign an event type, the default event type is used.

For example, a rule with 'TEST2' as text is more specific than a rule with text 'TEST'. To avoid that the 'TEST' will always be applied before 'TEST2', the rule with text 'TEST2' needs to be configured first as shown below.

The following table shows how these rules are applied to some ESPA message input examples.

ESPA message input			Matching rule			Resulting event type	Comment
Ringtone (3)	Priority (6)	Text (2)	Ringtone	Priority	Text		
Any or not provided	Any or not provided	TEST2			TEST2	TEST_TEXT_LONG	Rule 1
Any or not provided	Any or not provided	TEST3			TEST	TEST_TEXT_SHORT	Rule 2
1	1	Hello!		1		TEST_PRIO_1	Rule 3
1	3	Hello!	1			TEST_BEEP_1	Rule 5
Any, except 1	Any (except 1 and 3) or not provided	Hello!	*			TEST_BEEP_*	Rule 6
Not provided	Not provided	Hello!				ESPA	no match, default event type

### Event Text Replacement

Normally the 'Message text' (field 2) of an ESPA message is used as the notification text. Leading and trailing spaces in this text field are not supported and will be removed automatically during the configuration.

If there is an event text defined, then the event text will replace the content of the received 'Message text' (field 2) of the ESPA message.

If 'text position > 0' is set, then the 'Message text' (field 2) of the ESPA message is also included in the notification text starting at the specified text position.

If there is additionally a text length set, then only the specified portion of the 'Message text' (field 2) of the ESPA message is also included in the notification text.

<

Interface: ESPA

General

Endpoints

User defined event text

Event assignment

Simulator/Trace

+

↺

	Ringtone (3)	or Priority (6)	or Text (2)	Event type	Text position	Text length	Event text	Separator	
0	5	1	ESPA EVENT TEXT	New ESPA Type	0	0	Replacement	#	<div>✎</div> <div>🗑</div> <div>↑</div>

Settings – Text position, Text length and Event text					Resulting notification text
Text (2)	Event type	Text position	Text length	Event text	Replacement
ESPA EVENT TEXT	New ESPA Type	0	0	Replacement	
Text (2)	Event type	Text position	Text length	Event text	ESPA EVENT TEXT
ESPA EVENT TEXT	New ESPA Type	0	0		
Text (2)	Event type	Text position	Text length	Event text	Addition - ESPA EVENT TEXT
ESPA EVENT TEXT	New ESPA Type	1	0	Addition -	
Text (2)	Event type	Text position	Text length	Event text	Addition - EVENT TEXT
ESPA EVENT TEXT	New ESPA Type	6	0	Addition -	
Text (2)	Event type	Text position	Text length	Event text	Addition - EVENT
ESPA EVENT TEXT	New ESPA Type	6	5	Addition -	
Text (2)	Event type	Text position	Text length	Event text	EVENT
ESPA EVENT TEXT	New ESPA Type	6	5		

### Simulator/Trace Tab

The **Simulator** function can be used to check if a received ESPA message would be escalated correctly. The ESPA interface itself does not need to be running (state: green) for the Simulator function to work. There must only have been created an ESPA endpoint with a location, and in the **General** tab, a Default event type must be selected, and any IP address and port must be configured.

The communication between the SIP-DECT Event Manager and the ESPA interface can be recorded at the protocol level as needed. The **Trace** function can be used to monitor the data sent and received by the ESPA interface. The trace functionality can be started and stopped by the same button.

**Interfaces**  
Event types  
Notification profiles  
Notification groups  
Event plans  
Locations  
User  
System  
Monitor

Interface: ESPA-IF-1

General
Endpoints
User defined event text
Event assignment
Simulator/Trace

Simulator

Send

Call address (1)9000
Display message (2)Room 123
Ringtone (3)Optional
Call type (4)Optional
Priority (6)Optional

Trace

Stop
Clear

Data received☒
Data sent☒
Vital sign☒
View Hex☐

19-02-2024 08:51:40:709 R 1 ENQ 2 ENQ  
19-02-2024 08:51:40:709 T ACK  
19-02-2024 08:51:40:709 R SOH 1 STX 1 US 9000 RS 2 US Room 123 ETX 0B  
19-02-2024 08:51:40:710 T ACK

### Modbus interface

The Modbus interface enables the connection of devices e.g. WAGO or MOXA which provides input ports (e.g. buttons or switches) and output ports (e.g. lights) via Modbus-TCP protocol. The

Modbus protocol is a client / server data protocol in the application layer of the OSI model which was originally published by Modicon (now Schneider Electric) in 1979 for use with programmable logic controllers via RS232/RS485 interfaces (Modbus-RTU). For data transmission over Ethernet the protocol was adapted to Modbus-TCP. Meanwhile Modbus has become a de facto standard communication protocol for communication between industrial electronic devices in a wide range of buses and networks.

Reading digital input ports and setting digital output ports of Modbus-TCP devices is supported by the Event Manager.

The following devices have been approved for correct interoperability with the Event Manager:

- WAGO I/O System 750 ("Fieldbus Coupler Modbus TCP 4th generation" Item no. 750-362)
- MOXA ioLogik E1200 Series (ioLogik E1212)

Analog inputs and outputs and other sensor ports are not supported by the Event Manager.

**Note: Functionality cannot be guaranteed with other devices and must be checked separately before use. The following conditions must be observed.**

- Only digital inputs/outputs supported (no analog inputs/outputs or other sensors)
- IO addresses must not be remapped by device configuration, Event Manager only supports address range starting with address 1 for input/output ports.

### General Tab

The **General** tab is used for configuration of the IP address and port of the Modbus-TCP device which is connected through the interface.

< Interface: MODBUS-WAGO-33-109

General Endpoints

✓ Save Refresh

IP address 10.103.33.109

IP port 502



### Endpoints Tab

The **Endpoints** tab is used for configuration of incoming and outgoing endpoints. Incoming endpoints correspond to digital inputs of Modbus-TCP devices and outgoing endpoints correspond to digital

< Interface: MODBUS-WAGO-33-109

General Endpoints

+ ↺ 🔍 🗑️

Active	Direction	Address ↑	Label	Location	
✓	Incoming	1	WAGO-33-109-IN-I1-Switch	root/Lab-TES1	 
✓	Incoming	2	WAGO-33-109-IN-I2-Button	root/Lab-TES1	 
✓	Outgoing	2	WAGO-33-109-OUT-O2-White-Light	root/Lab-TES1	 
✓	Outgoing	3	WAGO-33-109-OUT-O3-Red-Light	root/Lab-TES1	 
✓	Outgoing	4	WAGO-33-109-OUT-O4-Green-Light	root/Lab-TES1	 



outputs of Modbus-TCP devices. For WAGO devices the incoming ports 1-256 are valid addresses, for MOXA only the addresses 1-16.

In the Endpoints configuration (reached by the link in the overview) some special settings for the endpoint can be configured. Mandatory are 'direction' and 'event type', optionally some special settings can be configured: 'Idle current' or 'Working current' is used on the connected device, a 'Alarm delay in seconds' and the 'Behavior when returning to normal state' (not terminate, terminate immediately or terminate at the end of the current alarm phase). For outgoing endpoints can be configured no special settings.

Interface: MODBUS-MOXA-33-116 / Endpoint: 1

✓ Save
🔄 Refresh

Direction

Incoming ▼

Event type

Fire alarm ▼

Idle current

☐

Release delay (sec)

0

Behavior when returning to normal state

Do not terminate event ▼

Do not terminate event  
Terminate event immediately  
Terminate event at the

Interface: MODBUS-MOXA-33-116 / Endpoint: 2

✓ Save
🔄 Refresh

Direction

Incoming ▼

Event type

WC-Call ▼

Idle current

☐

Release delay (sec)

0

Behavior when returning to normal state

Terminate event at the end of phase ▼

### Simulator/Trace Tab

The **Simulator/Trace** tab is used for simulation of the Modbus interface endpoints and for tracing changes on input/output ports. Each time the tab will be opened the trace window will show TCP/IP related connection information and the simulation window will show the actual status of the configured ports. By pressing the "Show all inputs" button the state of all inputs between address 1 and highest configured incoming endpoint address is shown. It is not recommended to open more than one browser window with active Simulator/Trace tab. Only one session is handled by the system.

For configured incoming endpoints a small button  is drawn beside each input state. If such button is pressed, the event configured for this endpoint will be generated and processed with defined event plan,

Please note that the configured endpoint attributes "Alarm delay", "Idle Current" and "Behavior when returning to normal state" don't apply if this button is pressed, the configured event will be generated immediately. If needed the executed event plan can be canceled via Monitor section of the Event Manager web frontend.

<

Interface: MODBUS-MOXA-33-116

General

Endpoints

Simulator/Trace

23-04-2024 13:52:15:550 TCP connected

23-04-2024 13:52:19:019 trigger event on addr 1 success - Fire alarm

Delete trace

Show all inputs

Inputs

1

2

8

0

0

0

Outputs

1

2

3

4

5

8

1

0

0

0

0

0

In the Outputs part of the **Simulator/Trace** tab the activity on output port 1 (in this example there is a light connected) is visible and in the trace part of the tab the handled trigger event at the incoming port 1 (triggered by the switch connected physically to this port or by pressing the button 1 in the Inputs part) is documented.

For simulation of the Modbus interface without a connection to a physical device it is possible to configure the interface with local host IP address (127.0.0.1).

## SNMP interface

### General Information

The SNMP interface enables the Event Manager to send SNMP notifications to the configured IP address with the assigned trap-community. Notifications are either sent as Traps or Inform-Requests.

Interfaces

Event types  
Notification profiles  
Notification groups  
Event plans  
Locations  
User  
System  
Monitor

<

Interface: SNMP-37-197-Inform

General

Save

Refresh

IP address10.103.37.79

IP port162

TypeInform

CommunityTrapInform

Traps are notifications that are sent once without the Event Manager checking whether the configured recipient actually receives them. In the case of Inform-Requests however, the Event Manager waits for a correct Get-Response from the target. Should a correct Get-Response not be received after 5 seconds, the Inform-Request will be resent. The Event Manager will only resend an Inform-Request once.

Currently, only SNMPv2c Traps and Inform-Requests are supported. Receiving and answering SNMP Get-Requests, Set-Requests and other SNMP notifications are not supported.

### SNMP Notifications

Once an SNMP interface has been added, a corresponding endpoint is automatically created. This endpoint may be added to event plan phases like any other endpoint.

### Interface Status Change

Should the event plan be triggered by the predefined event type “System Info”, the notification will contain data about the interface that triggered it and its current status. A “System Info” event is triggered by any interface when its status changes. This event is always triggered in the location “root”. If an SNMP interface is supposed to send notifications about interface status changes, an event plan handling the predefined “System Info” should be configured in that location with a phase containing the SNMP system endpoint as an assigned endpoint. Modifying the event type “System Info” has no influence on this functionality.

Notification name	Data field name	Object Identifier (OID)	Comment
interfaceStatusChange	---	.1.3.6.1.4.1.1027.4.1.1337.0.4	the trap OID
	interfaceType	.1.3.6.1.4.1.1027.4.1.1337.1.1.3.1.4	the interface's type
	interfaceLabel	.1.3.6.1.4.1.1027.4.1.1337.1.1.3.1.2	the interface's name
	interfaceState	.1.3.6.1.4.1.1027.4.1.1337.1.1.3.1.6	the state the interface has now changed to
	InterfaceDescription	.1.3.6.1.4.1.1027.4.1.1337.1.1.3.1.3	description of the interface

### Event Plan Processing

When a phase with an SNMP endpoint is activated, the corresponding SNMP interface will send a notification to the configured target. This notification will contain a notification ID, the event text, data about what triggered the plan and information on the triggered plan and phase. Once the phase has ended by any means, a notification with a matching notification ID will be sent to the target, informing it that the phase has ended. This trap does not contain the reason for ending the event plan. The current implementation is offered for evaluation of use cases. Accordingly, this functionality may be further developed and may be subject to technical changes in future software updates.

Notification name	Data field name	Object Identifier (OID)	Comment
activateEventPhase	---	.1.3.6.1.4.1.1027.4.1.1337.0.5	exact same fields as deactivateEventPhase
deactivateEventPhase	---	.1.3.6.1.4.1.1027.4.1.1337.0.6	exact same fields as activateEventPhase

Notification name	Data field name	Object Identifier (OID)	Comment
	trapEventID	.1.3.6.1.4.1.1027.4.1.1337.0.3.1	this ID matches in corresponding activate and deactivate notifications
	trapEventText	.1.3.6.1.4.1.1027.4.1.1337.0.3.2	the event text
	locationLabel	.1.3.6.1.4.1.1027.4.1.1337.2.1.3.1.2	location where the event plan was triggered
	endpointLabel	.1.3.6.1.4.1.1027.4.1.1337.4.1.3.1.5	name of the endpoint that triggered the event
	endpointCallNumber	.1.3.6.1.4.1.1027.4.1.1337.4.1.3.1.3	call number of the endpoint that triggered the event
	eventTypeLabel	.1.3.6.1.4.1.1027.4.1.1337.3.1.3.1.2	name of the event type
	eventPlanLabel	.1.3.6.1.4.1.1027.4.1.1337.6.1.3.1.2	name of the event plan
	phaseLabel	.1.3.6.1.4.1.1027.4.1.1337.6.1.4.1.3.1.2	name of the phase
	phaseDuration	.1.3.6.1.4.1.1027.4.1.1337.6.1.4.1.3.1.6	Duration of phase in seconds

### ***coldStart Notification***

Once an SNMP interface is correctly configured, it will send a coldStart notification to its configured target. This notification will get sent every time the SNMP interface is modified in such a way that it can work correctly or when it is activated after being toggled off. This notification will also be sent when the event manager starts or gets rebooted, if they are configured correctly. These coldStart notifications make the interface visible to SNMP management systems. They are however only supposed to inform the recipient that the SNMP interface itself is configured correctly and ready to send notifications. They do not yield concrete information about the state of the event manager itself or other interfaces. Furthermore, the event manager does not send warmStart notifications, even if the configuration of the interface did not change.

### ***Additional Notification Fields***

Each notification contains MIB undefined data fields in addition to their defined ones. These hold information about the EVM itself or data which is too specific for the more generic notification type. They are appended after the MIB defined data fields.

Notification name	Data field name	Object Identifier (OID)	Comment
Additional fields	---	---	data fields that get appended to notifications after their MIB defined data types
	espaDestinationIP	.1.3.6.1.4.1.1027.4.1.1337.1.3.1.1.1	for interfaceStatusChange, IP address where the ESPA interface is trying to connect to
	espaDestinationPort	.1.3.6.1.4.1.1027.4.1.1337.1.3.1.1.2	for interfaceStatusChange, Port where the ESPA interface is trying to connect to
	modbusDestinationIP	.1.3.6.1.4.1.1027.4.1.1337.1.5.1.1.1	for interfaceStatusChange, IP address where the Modbus is trying to connect to
	modbusDestinationPort	.1.3.6.1.4.1.1027.4.1.1337.1.5.1.1.2	for interfaceStatusChange, Port where the Modbus is trying to connect to

Notification name	Data field name	Object Identifier (OID)	Comment
	sipdectOMM1	.1.3.6.1.4.1.1027.4.1.1337.1.2.1.1.1	for interfaceStatusChange, the IP address of the first OMM
	sipdectOMM2	.1.3.6.1.4.1.1027.4.1.1337.1.2.1.1.2	for interfaceStatusChange, the IP address of the second OMM
	snmpDestinationIP	.1.3.6.1.4.1.1027.4.1.1337.1.4.1.1.1	for interfaceStatusChange, IP address where the SNMP interface is trying to connect to
	snmpDestinationPort	.1.3.6.1.4.1.1027.4.1.1337.1.4.1.1.2	for interfaceStatusChange, IP address where the SNMP interface is trying to connect to
	sysName	.1.3.6.1.2.1.1.3	appended to all notifications, EVM's name
	systemIPAddress	.1.3.6.1.4.1.1027.4.1.1337.10.3	appended to all notifications, EVM's IP address
	systemMACAddress	.1.3.6.1.4.1.1027.4.1.1337.10.4	appended to all notifications, EVM's MAC address
	systemVersion	.1.3.6.1.4.1.1027.4.1.1337.10.2	appended to all notifications, EVM's version number
	snmpTrapEnterprise	.1.3.6.1.6.3.1.1.4.3	always last data field, contains MITEL's Enterprise OID

### Management Information Base

In order to interpret these messages and their data fields correctly, two MIB files are supplied together with the Event Manager. The first Management Information Base (MIB) is MITEL's root MIB file (MITEL-MIB.mib). It is necessary for the second MIB, the MITEL-EVM-MIB.mib, to work. Both .mib files together contain all the proprietary information that an SNMP agent needs to correctly interpret the specific data and notifications of the Event Manager.

Other RFC defined MIB files that the event manager utilizes are SNMPv2-SMI (RFC 2578), SNMPv2-TC (RFC 2579), SNMPv2-CONF (RFC-2580) and SNMPv2-MIB (RFC 3418).

### Event types

There are five default Event types ('Man Down', 'No Move', 'Escape', 'SOS-Key' and 'System Info') available. These types can be changed but cannot be deleted. The default Event types 'Man Down', 'No Move', 'Escape' and 'SOS-Key' correspond to the Alarm triggers which are also available as standard in SIP-DECT.

To handle additional Alarm triggers that may be defined in SIP-DECT OMP, Event types with the same name or short name as the name of the Trigger ID in OMP must be configured in the SIP-DECT Event Manager.

All Event types serve as a kind of filter in an Event plan to control the escalation of an event. Based on the assigned priority the system knows in which order the events should be processed. Important events should therefore be configured with a higher priority.

Note: An event displayed on a SIP-DECT terminal will be overwritten by a higher priority event.

### Notification profiles

Notification profiles determine how a notification should be presented to the recipient. It is assigned to the receiving endpoint within the event plan. Only one notification and only the one

with the highest priority (Event type priority) is displayed on a DECT phone. Notifications with lower priority are not transmitted to the DECT phone if a message with higher priority is to be displayed. If there are several messages with the same priority at the same time, they will be transmitted one after the other to the DECT phone, with each message being displayed for at least 20 seconds before it is replaced by the next one. Selecting the interface when configuring a new notification profile displays the configurable parameters. Notification profiles are very different depending on the interface. One notification profile ('normal') is created by default, this profile cannot be deleted. Click the link under the column 'Label' to change the profile settings (Melody, Ringtone, Volume, etc.) for a profile.

A Ringtone group is a set or collection of ringtones that can be assigned to specific contacts, groups, or categories. Ringtone groups are used to customize the incoming call alert sounds for different callers or types of calls. The ringtone group can be specifically selected from all the ringtones available from SIP-DECT.

If the 'Increasing ring volume' option is used, the ringtone starts quietly and then gradually reaches the ring volume set. In addition, notification can also be signaled by telephone vibration (if supported by the phone type).

If the 'No alert tone during call' option is active, a notification is delivered without acoustic signaling while the terminal is on a call. If 'Disconnect existing call' is selected, an existing call will be disconnected at the time of the notification.

If the telephone supports 'Font color' and 'Background color', the font and color display of the message can be controlled by the SIP-DECT Event Manager.

Restrictions and behavior:

- Settings not supported by the used telephone are ignored.
- 'Priority Low': 'Ringtone group', 'Ringtone', 'Ring volume' and 'Increasing ring volume' has no effect.
- 'Priority Emergency': Pop-up window during call only available with this priority
- Further information about the behavior of displayed messages: Please see the document 'Mitel 600/700 DECT Phone Messaging and Alerting Applications'!

## Notification groups

Endpoints that can receive notifications can be combined into a notification group. This simplifies the configuration regarding the escalation of an event. If the assigned notification group address matches with the source endpoint address then the "Use call address" feature of the event phase can be used.

## Event plans

Event plans describe how to react to certain types of events that occur at different locations. Event plans can consist of up to 10 escalation phases and define the process for handling these events and the resulting notifications in the different phases.

Interfaces	+ ↺ 🔍			
Event types	Active	Label ↑	Description	Restart plan after completion
Notification profiles	✓	<a href="#">Plan</a>		✗
Notification groups				<a href="#">✎</a> <a href="#">🗑</a>
<b>Event plans</b>				
Locations				
User				
System				
Monitor				

**Please be aware that a running event plan will be stopped and replaced with a new execution of this plan when the same event from the same source endpoint is received.**

The following settings can be carried out in the **Event plans** configuration pane:

### Filter: Event type Tab

Different types of events can be assigned here to the Event plan. At least the following default Event types are available: **System Info**, **SOS-Key**, and **Man Down**.

< Event plan: Plan	
Filter: Event type	Filter: Location Phase
Event types assigned	Event types available
	<div> <div>System Info</div> <div>SOS-Key</div> <div>Man Down</div> <div>ESPA-Event</div> </div>

### Filter: Location Tab

Formerly created locations (to which endpoints are assigned) can be assigned here to the Event plan.

< Event plan: Plan	
Filter: Event type	Filter: Location Phase
Locations assigned	Locations available
	<div> <div>root</div> </div>

### Phase Tab

Up to 10 phases can be added to an Event plan in the Phase tab with the following configurations:

Interfaces	< Event plan: EP-1				
Event types	Filter: Event type Filter: Location Phase				
Notification profiles	+ ↺				
Notification groups					
<b>Event plans</b>					
Locations					
User					
System					
Monitor					
	Label	Description	Use call address	with Notification profile	
	1 <a href="#">EP1-PH1</a>	Phase 1 of Plan 1	✗		<a href="#">✎</a> <a href="#">🗑</a>
	2 <a href="#">EP1-PH2</a>	Phase 2 of Plan 1 (notification group)	✗		<a href="#">✎</a> <a href="#">🗑</a>

By editing the phase settings, the 'Use call address' flag can be enabled, and a notification profile may be assigned. With this kind of configuration, a direct assignment of call addresses to a notification group with this address can be realized. In the incoming interface (e.g. ESPA) an endpoint with this call address must be configured.

### Endpoints/Notification groups Tab

Up to 1000 endpoints and/or up to 50 notification groups can be added to a phase or deleted from a phase in the **Endpoints/Notification groups** tab. To each endpoint or notification group a

formerly created notification profile can be assigned here also.

## Settings Tab

The following settings can be carried out in the **Settings** tab for a phase:

- The duration in seconds for this phase
- Number of retries (repetitions of this phase)
- Number of confirmations (needed for successful ending of the phase)

Note: 'Individual' implies that all to this phase assigned endpoints must confirm the received notification before the phase ends successfully. If the number of confirmations is not reached, it moves on to the next phase (if configured), is repeated (if configured) or is terminated after the phase has expired.

Note: If there are assigned outgoing endpoints like Modbus or SNMP to a phase, the setting for the number of confirmations should not be set to 'Individual' to avoid unsuccessful phases (because those types of endpoints will never be able to confirm received messages).

## Locations

By defining the locations, a spatial environment can be mapped in a tree structure. A location means the origin of an event. Endpoints that should be used to trigger an event can be assigned to a location here. Endpoints that are not assigned to a location cannot trigger an event.


The root location is always present and cannot be deleted.

To create a new location, a table line must be selected, and the button must be pressed. The new location is then based on the location that was selected before.



Interfaces				
Event types				
Notification profiles				
Notification groups				
Event plans				
<b>Locations</b>				
User				
System				
Monitor				

Location	Label	Description	
root	<a href="#">root</a>		

All endpoints can be assigned to a desired location by following the link under the column 'Label'. The assignment can also be changed via the **Endpoints** tab in the **Interfaces** configuration pane.

## User

The **User** pane allows to create, edit and delete users and to change the passwords of the users. The default user 'admin' cannot be deleted.

## System

The **System** pane consist of the following tabs:

### General Tab

The following settings can be carried out in the **General** tab of the system:

- A system name which subsequently will be displayed also in the headline of the Event manager web application.
- CloudLink daemon can be enabled here (for remote management of the Event Manager)
- CloudLink status is shown here (running or not running)
- The version of the running Event manager application is shown here
- An external IP-Watchdog outside of the system can be configured here which observes a ping from the Event Manager (normally sent at regular interval every 30 seconds as long as it is working correctly). The IP-Watchdog can trigger an alert by Email, SMS or SNMP Trap, or activate a relay for interruption of power for the monitored device to restart the RFP where the Event Manager is configured in case of missing ping from the monitored device.

### Backup/Restart Tab

The following actions can be carried out in the **Backup/Restart** tab of the system:

- **Restart:** The SIP-DECT Event Manager can be re-started with this menu item. The SIP-DECT Event Manager is briefly unavailable.
- **Restart with factory defaults:** All data and settings on the SIP-DECT Event Manager are irreversibly deleted when the factory defaults are restored.
- **Export log:** Log files will be downloaded from the SIP-DECT Event Manager. The log files consist of two csv files which contain the event summary and the event execution details. Depending on the traffic on the Event Manager there are saved the logs from the last days or weeks (maximum size of the details log is 6 MByte).
- **Export config:** A running configuration of the SIP-DECT Event Manager will be downloaded and saved on the local computer of the administrator.
- **Import config:** Allows to restore an existing configuration to the SIP-DECT Event Manager as zipped file (extension '.gz') but also as normal text file. A validity check is conducted before activation. A configuration recognized as defective or incomplete will not be activated. During the import of an existing configuration the user data will be used from the running SIP-DECT Event Manager system. If the configuration file was recognized as complete the SIP-DECT Event Manager system will be restarted automatically to activate the imported data backup.

### Security Tab

The following actions can be carried out in the **Security** tab of the system:

- The import of an trusted certificate which is used in the SIP-DECT OMM (for future use).
- The import of a local certificate chain and private key (with or without a password) for the

SIP-DECT Event Manager which will then be used for the web access to the Event Manager application.

- Via a 'Delete' button formerly installed certificates and private keys can be deleted at once.
- Via a dedicated 'Restart' button the activation of newly imported certificates or private key into the system will be finalized (import into web server configuration).

If a trusted certificate or a local chain certificate has been installed the number of those certificates will be displayed. There is also visible if a private key has been imported.

***If a local certificate chain was imported, the corresponding private key (and configuration of needed password) must strongly be done also before a restart of the SIP-DECT Event Manager. Otherwise the system will possibly unreachable for further configuration via the web admin.***

## Security level Tab

The following actions can be carried out in the **Security level** tab of the system:

- Setting of a security level for the Event manager application (High, Medium, Legacy)
- Configuration of 'Used Cipher Suites' for the different Security levels

Normally there is configured as a default the security level 'High' and a default setting for 'Used Cipher Suites'. These settings may be modified here carefully. Therefore a list of the currently configured and of the general configurable cipher suites is shown here. The addition of cipher suites into the 'Used cipher suites' could be managed by selecting the cipher suites name from the table entry 'Supported cipher suites' with a semicolon in front of it at the end of the listed cipher suites in the upper list entry (Used cipher suites). An entry can simply be deleted from the 'Used cipher suites' by editing the table entry after deselection of the 'Use defaults' checkbox. In all cases of changing Cipher Suites, the configuration must be finished by pressing the 'Save' button.

## CloudLink Tab

The **CloudLink** tab is only visible if the CloudLink daemon has been enabled before. Via this tab a detailed CloudLink Daemon window will be available to connect the Event Manager with the CloudLink portal and to start the tunnel for the remote access to the Event Manager.

Information about the CloudLink Daemon portal and system inventory in the CloudLink Portal will be available with the CloudLink documentation on the Document Center at <https://www.mitel.com/document-center/technology/cloudlink>.


An account with SIP-DECT integration is needed on the CloudLink portal.

Before removing the OMM or Event Manager from an RFP, stop the tunnels and unlink the CloudLink Daemon from CloudLink.

The CloudLink Daemon connects to \*.mitel.io services via https (port 443).

## Monitor

The **Monitor** pane shows a table with the currently active event handlings. Single event lines from this table or all active event handlings can be canceled from this point.

<div>Interfaces</div> <div>Event types</div> <div>Notification profiles</div> <div>Notification groups</div> <div>Event plans</div> <div>Locations</div> <div>User</div> <div>System</div> <div>Monitor</div>	Cancel all						
	Priority	Type	Text	Endpoint	Phase	Confirmations	
	3	SOS-Key	SOS - SDT-732d-247 (247), RFP48-02	SDT-732d-247	EP2-SOS-Phase1	0 / 1	

## Quick Start Configuration Guide SIP-DECT Event Manager

The following steps need to be followed to get a basic working configuration. There are two basic scenarios.

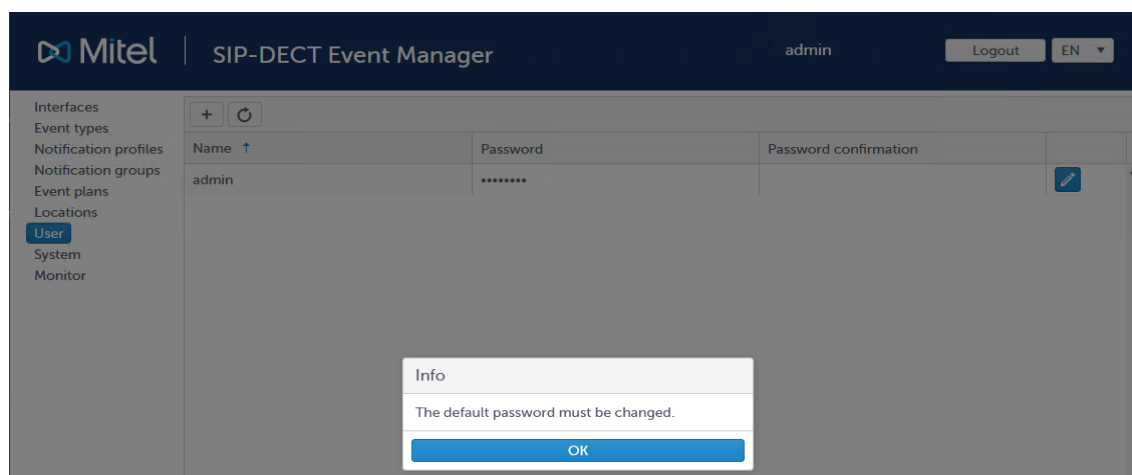
- Configuring a SOS alarm trigger from a SIP-DECT phone
- Configuring an ESPA message

The prerequisite for the following steps is a functioning SIP DECT installation with several Mitel SIP-DECT 602d v2 / 700d terminals. The SIP-DECT terminals are already updated to the SW provided with the SIP-DECT system.

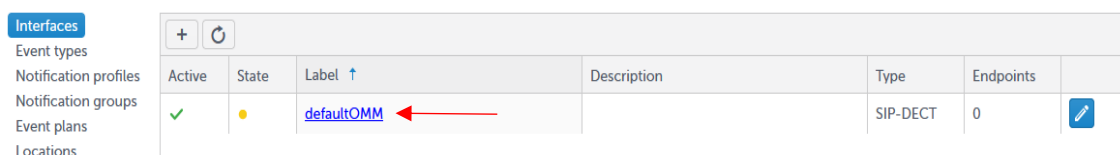
The SIP-DECT Event Manager was started on an RFP using the OM Configurator (OMC) and has the default configuration.


### Configuring SOS alarm trigger from a DECT phone

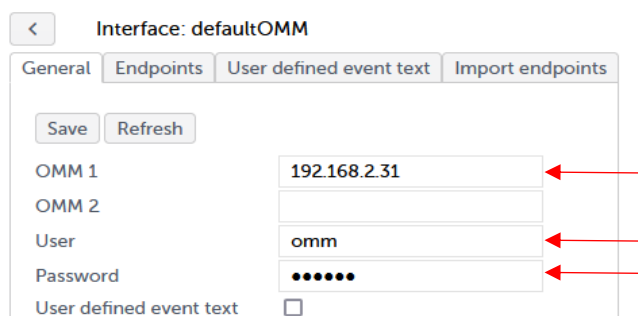
1. Log in to the SIP-DECT Event Manager web service <https://<RFP IP address>:8444> with default login “admin” and password “admin”.
2. Change the default password.



3. Open OMM interface configuration dialog by selecting the link as shown below.



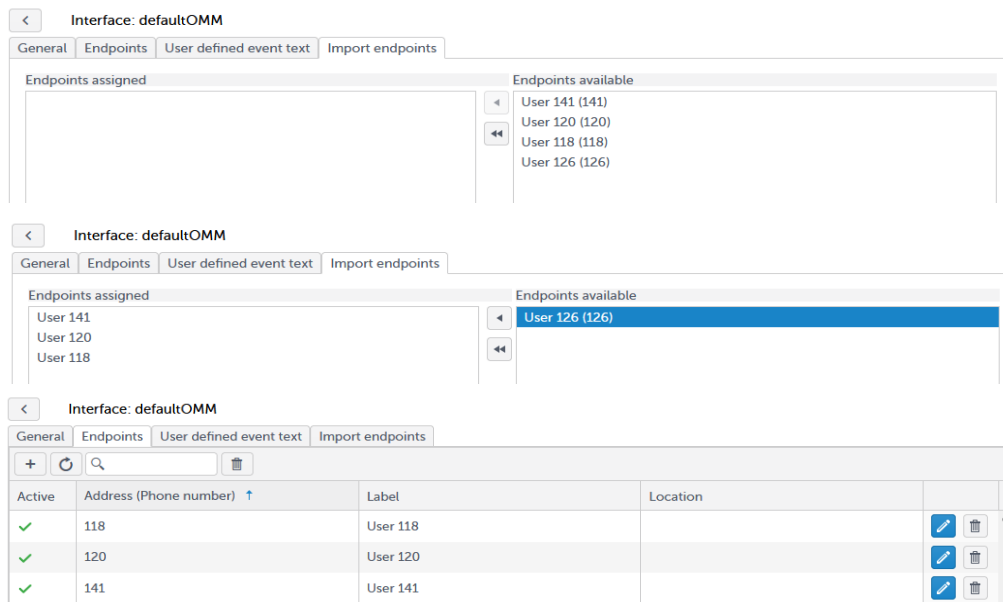
4. Enter the OMM IP address(es), user and password and confirm with ‘Save’. Return to the interface overview by clicking the Back button .



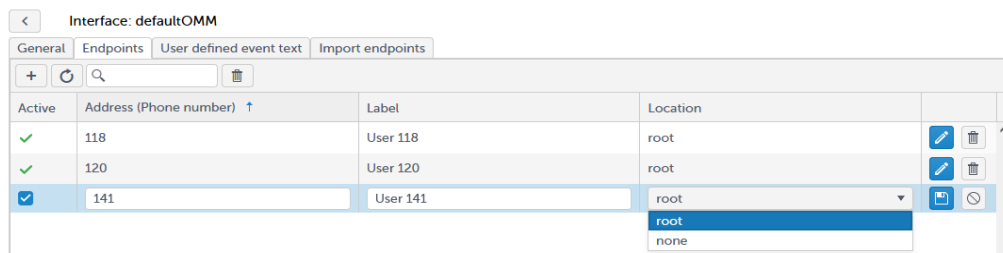
- The interface status should change to green, indicating that the SIP-DECT Event Manager could connect with the OMM.



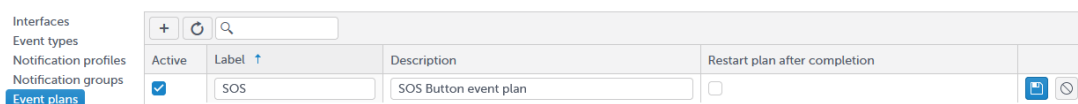
- Go back into the OMM interface configuration dialog, click the **Import endpoints** tab and transfer the SIP-DECT endpoints into the SIP-DECT Event Manager configuration by selecting one by one and clicking or all by clicking . As a result the endpoints should now appear in the endpoints list.



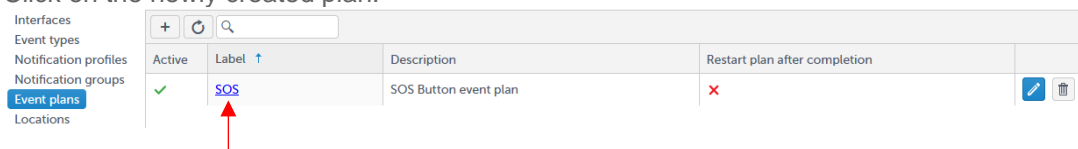
- Assign the endpoints to the default location root as shown below.



- Click the **Event plans** configuration pane and create a new event plan by clicking . Set a name and description for the plan and confirm with .



- Click on the newly created plan.



10. Under the **Filter: Event type** tab, add the default event type SOS-Key to the event type filter.

Event plan: SOS

Filter: Event type | Filter: Location | Phase

Event types assigned: SOS-Key

Event types available: System Info, Man Down


11. Click **Filter: Location** tab and add the default location root to the location filter.

Event plan: SOS

Filter: Event type | Filter: Location | Phase

Locations assigned: root

Locations available:

12. Click the **Phase** tab and create a phase for the event plan by clicking New. Set a name and description for the phase and confirm with .

Event plan: SOS

Filter: Event type | Filter: Location | Phase

+ New

	Label	Description	Use call address
	Phase 1	this is the plan's 1st phase	<input type="checkbox"/>


13. Open the Phase configuration dialog by selecting the link as shown below.

Event plan: SOS

Filter: Event type | Filter: Location | Phase

+ New

	Label	Description	Use call address
1	<a href="#">Phase 1</a>	this is the plan's 1st phase	<input checked="" type="checkbox"/>

14. Transfer the endpoints you want to be notified into the endpoints list by selecting one by one (to select more than one use additionally the Ctrl key) and press . The default notification profile 'Normal' will automatically be assigned.

Event plan: SOS / Phase:

Endpoints/Notification groups | Settings

Endpoints assigned: User 118 / 118, User 120 / 120

Endpoints available: User 141 / 141

Notification profile: Please select

15. No further phase settings need to be changed. Return to the main level dialog by .

Interfaces

Event types

Notification profiles

Notification groups

Event plans


Active	Label	Description	Restart plan after completion
✓	SOS	SOS button event plan	<input checked="" type="checkbox"/>




16. If now the SOS button is pressed on one of the Mitel SIP-DECT phones, a notification should appear on those SIP-DECT terminals that have been assigned as endpoints to the event plans phase.





## Configuring ESPA interface

Execute the same steps to setup the ESPA interface, add the ESPA interface endpoints and assign the default location “root” as described in the Configuring SOS alarm trigger from a DECT phone section. Before a new event plan is created, the ESPA interface must be set up and a new event type must be created.

1. Click the **Event types** configuration pane.
2. Add a new entry by clicking **+**. Set a unique label and short text and confirm with .

Label	Short text	Priority	Description	
ESPA-Event	ESPA	10	New event type for ESPA	 
System Info	Sys Info	3		

3. Click the **Interfaces** configuration pane.
4. Add a new entry by clicking **+**. Set a unique label and description and confirm with . Ensure that the interface type ‘ESPA’ is selected under ‘Type’.

Active	State	Label	Description	Type	Endpoints	
<input checked="" type="checkbox"/>	●	ESPA -IF-1	1st ESPA interface	ESPA	0	 
<input checked="" type="checkbox"/>	●	defaultOMM		SIP-DECT	0	

5. Open the Interface configuration dialog by selecting the created link.

Active	State	Label	Description	Type	Endpoints	
<input checked="" type="checkbox"/>	●	ESPA -IF-1	1st ESPA interface	ESPA	0	 
<input checked="" type="checkbox"/>	●	defaultOMM		SIP-DECT	0	

6. Enter the IP address and port that the ESPA 4.4.4 of the SIP-DECT Event Manager should connect to, select the Default event type and confirm with Save.

Interface: ESPA-IF-1

General Endpoints User defined event text Event assignment Simulator/Trace

Save Refresh

IP address 192.168.2.71

IP port 10001

Interface supervision ☒

Determine endpoint by Call address

Default event type Please select

Call type 1 (Field 4) terminates event Please select

User defined event text System Info SOS-Key Man Down ESPA-Event

7. Add an ESPA endpoint in the **Endpoints** tab. Set the endpoint address (ESPA field 1 – Call address), assign a name and the default location 'root' and confirm with

Interface: ESPA-IF-1

General Endpoints User defined event text Event assignment Simulator/Trace

Active	Address (Field 1)	Label	Location
<input checked="" type="checkbox"/>	9000	ESPA EP 9000	root

8. Return to the interfaces overview by clicking . If the SIP-DECT Event Manager could connect with the nurse call system or similar the interface status turns to green.

Active	State	Label	Description	Type	Endpoints
<input checked="" type="checkbox"/>		defaultOMM		SIP-DECT	4
<input checked="" type="checkbox"/>		ESPA-IF-1	1st ESPA interface	ESPA	1

9. Create an event plan. Follow steps 8-15 as described in the Configuring SOS alarm trigger from a DECT phone section. However, this time the newly created event type should be assigned to the ESPA interface as the default event type to use.

Interfaces

Event types

Notification profiles

Notification groups

Event plans

Locations

User

System

Monitor

Event plan: ESPA event plan

Filter: Event type Filter: Location Phase

Event types assigned

ESPA-Event

Event types available

System Info

SOS-Key

Man Down

10. To trigger an event even without a connected system, there is useable the simulator function of the ESPA interface.

Interface: ESPA-IF-1

General Endpoints User defined event text Event assignment Simulator/Trace

Simulator

Send

Call address (1) 9000

Display message (2) Room 123

Ringtone (3) Optional

Call type (4) Optional

Priority (6) Optional

Trace

Stop Clear

Data received ☒

Data sent ☒

Vital sign ☒

View Hex ☐

19-02-2024 08:51:40:709 R 1 ENQ 2 ENQ

19-02-2024 08:51:40:709 T ACK

19-02-2024 08:51:40:709 R SOH 1 STX 1 US 9000 RS 2 US Room 123 ETX 08

19-02-2024 08:51:40:710 T ACK

11. When an ESPA message is received, a notification with the received text message should now appear on the Mitel SIP-DECT terminal assigned to the event plans phase.





## Appendix

### Sitemap

The following table provides an overview of the Event Manager Web service structure.

Interfaces			
	Interface SIP-DECT	General	
		Endpoints	
		User defined event text	Text replacement
			Event text structure
		Import endpoints	Endpoints assigned
			Endpoints available
	Interface ESPA	General	
		Endpoints	
		User defined event text	Text replacement
			Event text structure
		Event assignment Simulator/Trace	Simulator
			Trace
	Interface SNMP		
	Interface Modbus	General	
		General	
		Endpoints	Endpoint config
		Simulator/Trace	Inputs
			Outputs
Event types			
Notification profiles			
	SIP-DECT profile		
	Notification groups		
	Notification group		
		Endpoints assigned	
		Endpoints available	
Event plans			

Plan		Filter: Event type	Event types assigned Event types available	
		Filter: Location	Locations assigned Locations available	
		Phase	Endpoints	Endpoints assigned  Endpoints available Notification groups assigned Notification groups available
Locations			Settings	
	Location	Endpoints assigned Endpoints available		
User				
System	General Backup/Restart Security Security level	Security level Cipher suites	Used cipher suites Supported cipher suites	
	CloudLink			
Monitor				

## Web UI Parameter, Action & Status Information overview

Web UI Parameter, Action & Status Information		Description
<b>Interfaces</b>		Configuration pane to administrate the Event Manager's interfaces. Up to 5 interfaces are supported. There is always one SIP-DECT interface which cannot be deleted. Up to 4 incoming ESPA interfaces can be configured.
	<b>Active</b>	Switch to activate or deactivate the interface
	<b>State</b>	Shows the state of the interface (running, misconfigured, inactive)
	<b>Label</b>	Name to identify the interface
	<b>Description</b>	Additional information
	<b>Type</b>	SIP-DECT, ESPA, SNMP, MODBUS
	<b>Endpoints</b>	Shows the number of configured endpoints for the interface. Up to 2000 endpoints in total are supported across all interfaces.
<b>Type SIP-DECT</b>		There is one interface to connect with the SIP-DECT OMM. Standby-OMM configuration is supported. Via this interface, messages are sent to SIP-DECT telephones, confirmations as well as alarm triggers are received from telephones, e.g., SOS, Man Down or Alarm Trigger.
	<b>General</b>	General settings for the SIP-DECT interface
	<b>OMM 1</b>	OMM IP address
	<b>OMM 2</b>	Standby OMM IP address
	<b>User</b>	Username to authenticate with the OMM
	<b>Password</b>	Password to authenticate with the OMM
	<b>User defined event text</b>	Switch to activate or deactivate the user defined event text function
	<b>Endpoints</b>	Via SIP-DECT reachable endpoints (SIP-DECT users)
	<b>Active</b>	Switch to activate or deactivate the endpoint
	<b>Address</b>	Endpoint identifier e.g., telephone number
	<b>Label</b>	Endpoint name
	<b>Location</b>	Location to which the endpoint is assigned
	<b>User defined event text</b>	The user defined event text feature allows to modify or replace the received event text to generate an appropriate notification.
	<b>Text replacement</b>	Simple text replacement function. Up to 10 text replacement rules can be defined.
	<b>Text</b>	Text to be replaced
	<b>Replace by</b>	Replacing text

Web UI Parameter, Action & Status Information		Description
	<b>Event text structure</b>	Function to create a new text from predefined elements. The user defined event text can be composed of up to 4 elements.
	<b>Text</b>	One of the following elements: Event type, Event type short, Priority, Originating endpoint (name), Originating endpoint (address), Location of originating endpoint, Event phase, Received text from interface
	<b>Max. length</b>	Maximum length of text to be inserted
	<b>Spacer</b>	Separator to separate the text elements
	<b>Import endpoints</b>	Function to simplify the setup of SIP-DECT endpoints
	<b>Endpoints assigned</b>	Endpoints which are already imported from SIP-DECT into EVM
	<b>Endpoints available</b>	SIP-DECT endpoints that can still be imported
<b>Type ESPA</b>	Incoming Interface to connect with a nurse call system, fire alarm system or similar via ESPA 4.4.4 over IP.	
	<b>General</b>	General settings for the ESPA interface.
	<b>IP address</b>	IP address of the nurse call system or similar or of the serial IP converter to connect with
	<b>IP port</b>	IP port of the nurse call system or similar or of the serial IP converter to connect with
	<b>Interface supervision</b>	Switch to enable or disable interface monitoring
	<b>Determine endpoint by</b>	Switch for defining the method for determining the endpoint. One of the two options: Call address, Message text
	<b>Default event type</b>	Event type that should be used if no other event type was determined
	<b>Call type 1 (Field 4) terminates event</b>	Switch to activate or deactivate the option that Call type 1 (ESPA Field 4) shall terminate the event
	<b>User defined event text</b>	Switch to activate or deactivate the user defined event text function
	<b>Endpoints</b>	Endpoints that can send events to the Event Manager via the ESPA interface.
	<b>Active</b>	Switch to activate or deactivate the endpoint
	<b>Address</b>	Endpoint identifier e.g., ESPA call address
	<b>Label</b>	Name to identify the endpoint
	<b>Location</b>	Location to which the endpoint is assigned

Web UI Parameter, Action & Status Information		Description
	<b>User defined event text</b>	The user defined event text feature allows to modify or replace the received event text to generate an appropriate notification.
	<b>Text replacement</b>	Simple text replacement function. Up to 10 text replacement rules can be defined (not usable for event type, priority and phase)
	<b>Text</b>	Text to be replaced
	<b>Replace by</b>	Replacing text
	<b>Event text structure</b>	Function to create a new text from predefined elements. The user defined event text can be composed of up to 4 elements.
	<b>Text</b>	One of the following elements: Event type, Event type short, Priority, Originating endpoint (name), Originating endpoint (address), Location of originating endpoint, Phase, Received text from interface
	<b>Max. length</b>	Maximum length of text to be inserted
	<b>Spacer</b>	Separator to separate the text elements
	<b>Event assignment</b>	Function for assigning an event type based on different ESPA 4.4.4 message contents.
	<b>Position</b>	Position of the rule in the list of rules. First matching rule will be applied.
	<b>Ringtone (3)</b>	Ringtone value (ESPA field 3) which should be mapped to the specified event type.
	<b>Priority (6)</b>	Priority value (ESPA field 6) which should be mapped to the specified event type.
	<b>Text (2)</b>	Text value (ESPA field 2) which should be mapped to the specified event type.
	<b>Event type</b>	Event type to be used.
	<b>Text position</b>	Start position in the received event text from which the event text should be copied. 0 - the original event text will be used.
	<b>Text length</b>	Number of characters that should be taken over from the received event text from the start position.
	<b>Event text</b>	Alternative text to replace or add the original event message text.
	<b>Separator</b>	Delimiter which will be followed by a phone number, e.g. for callback
	<b>Simulator/Trace</b>	

Web UI Parameter, Action & Status Information		Description
	<b>Simulator</b>	The simulator function allows to send ESPA messages into the Event Manager to emulate traffic even when the interface is not connected to another system.
	<b>Call address</b>	ESPA Field 1 Call address (mandatory field)
	<b>Display message</b>	ESPA Field 2 Display message (mandatory field)
	<b>Ring tone</b>	ESPA Field 3 Ringtone
	<b>Call type</b>	ESPA Field 4 Call type
	<b>Priority</b>	ESPA Field 6 Priority (1 – alarm, 2 – high, 3 – normal)
	<b>Trace</b>	Function to display traffic on the ESPA interface
	<b>Data received</b>	Switch to enable display of received data
	<b>Data sent</b>	Switch to enable display of sent data
	<b>Vital sign</b>	Switch to enable display of keep alive messages / ESPA polling messages
	<b>View Hex</b>	Switch to enable display of data additionally in hexadecimal format
	<b>Trace window</b>	ESPA traffic display window
<b>Type SNMP</b>	The SNMP interface allows to send SNMPv2c trap or inform messages to a trap destination.	
	<b>General</b>	General settings of the SNMP interface.
	<b>IP address</b>	IP address of the trap receiver.
	<b>IP port</b>	IP port address of the trap receiver.
	<b>Type</b>	Either trap or inform message can be selected.
	<b>Community</b>	SNMP trap community, e.g. 'public'.
<b>Type Modbus</b>	The Modbus interface allows to connect external devices (WAGO/MOXA) with incoming and outgoing ports.	
	<b>General</b>	General settings of the Modbus interface.
	<b>IP address</b>	IP address of the Modbus device.
	<b>IP port</b>	IP port address of Modbus device.
	<b>Endpoints</b>	Endpoints of the Modbus interface.
	<b>Active</b>	Switch to activate or deactivate the endpoint

Web UI Parameter, Action & Status Information		Description
	<b>Outgoing</b>	Endpoints to which the Event Manager can send messages
	<b>Incoming</b>	Endpoints from which the Event Manager can receive messages
	<b>Event type</b>	Event type to be used
	<b>Idle current</b>	Switch to activate or deactivate idle current for this endpoint
	<b>Alarm/Release delay</b>	How long the endpoint needs to be activated in order to trigger an event in seconds
	<b>Behavior when returning to normal state</b>	Select the behavior of this endpoint when it returns to its normal state (e.g. "Do not terminate event", "Terminate event immediately" & "Terminate event at the end of phase")
	<b>Address</b>	Endpoint identifier e.g., MODBUS call address
	<b>Label</b>	Name to identify the endpoint
	<b>Location</b>	Location to which the endpoint is assigned
	<b>Simulator/Trace</b>	
	<b>Trace</b>	The trace window shows if connection to a Modbus device could be established or not (errors) and if it is possible to received trigger events from incoming endpoints.
	<b>Simulator</b>	The simulator function allows simulation of events on incoming endpoints into the Event Manager to emulate traffic even when the interface is not connected to anything. The status of incoming and outgoing endpoints from a real connected Modbus device will also be shown.
<b>Event types</b>	Configuration pane to administrate up to 100 event types. Individual events are mapped to these event types for further processing.	
	<b>Label</b>	Event type name
	<b>Short text</b>	Short (max. 8 character long) event type name
	<b>Priority</b>	Event priority
	<b>Description</b>	Additional information
<b>Notification profiles</b>	Configuration pane to administrate up to 50 notification profiles. Notification profiles define the way notifications are presented by the receiving device.	
	<b>Label</b>	Notification profile name

Web UI Parameter, Action & Status Information		Description
	<b>Description</b>	Additional information
	<b>SIP-DECT profile</b>	The profile contains various parameter to control the way a notification is indicated on the Mitel 6x2d/700d DECT phone.
	<b>Ringtone group</b>	The Event Manager can control the ringtone to alert the message received on the DECT phone. Various options are available: a) <b>Not to be used for now: None</b> b) Using the device settings with selection of a specific melody setting: Local settings c) Selecting a ringtone from a group: one of the available ringtone groups
	<b>Ringtone</b>	a) If the ringtone group is set to “Local settings”, a specific melody setting of the device can be selected. B) If a ringtone group is set, a melody or sound effect can be selected.
	<b>Priority</b>	SIP-DECT message priority: Low, Normal, High, Emergency
	<b>Ring volume</b>	Ring tone volume which shall be used to indicate the notification.
	<b>Increasing ring volume</b>	Enables the automatic volume increase
	<b>Vibration</b>	Enables the vibration function if not automatically activated by the phone based on the message priority.
	<b>No alert tone during call</b>	Switch to turn off the audible indication (in-band) of the received message.
	<b>Disconnect exiting call</b>	If activated, ends an existing telephone conversation when the message arrives.
	<b>Font color</b>	Display color of the message text
	<b>Background color</b>	Background color of the message text
<b>Notification groups</b>	Configuration pane to administrate up to 50 notification groups. (maximum 2000 endpoints in total across all groups). Notification groups group endpoints to be notified for easier management. Groups can be assigned to	



Web UI Parameter, Action & Status Information		Description
		phases of event plans instead of individual endpoints. In addition, notification groups can have addresses to use the "Use call address" function in event plans.
	<b>Label</b>	Notification group name
	<b>Description</b>	Additional information
	<b>Address</b>	Unique id e.g., telephone number / extension number
	<b>Endpoints assigned</b>	List of endpoints assigned to this group
	<b>Label/Address</b>	Endpoint name / Endpoint address
	<b>Endpoints available</b>	List of endpoints which could be assigned to this group.
	<b>Label/Address</b>	Endpoint name / Endpoint address
<b>Event plans</b>		Configuration pane to administrate up to 500 event plans. Event plans define processes for handling received events sent by endpoints at the various locations to notify receiving endpoints
	<b>Active</b>	Switch to activate or deactivate the event plan.
	<b>Label</b>	Event plan name
	<b>Description</b>	Additional information
	<b>Restart plan after completion</b>	Switch to enable or disable the restart of the plan after completion (default: off)
	<b>Filter: Event type</b>	
	<b>Event types assigned</b>	List of Event types for which the plan is applied, i.e., should be executed.
	<b>Event types available</b>	List of Event types that have not yet been assigned to the plan, i.e., to which the plan is not applied
	<b>Filter: Location</b>	
	<b>Locations assigned</b>	List of Locations to which the plan applies, i.e., the plan is applied to events sent from endpoints assigned to these locations.
	<b>Locations available</b>	List of Locations that have not yet been assigned to the plan, i.e., to which the plan does not apply
	<b>Phase</b>	Event plan phases: up to 10 phases in a single plan and up to 1000 phases in total across all event plans.
	<b>Label</b>	Phase name
	<b>Description</b>	Additional description for the phase.

Web UI Parameter, Action & Status Information		Description
	<b>Use call address</b>	Option to enable selecting a notification group based on the receiving endpoints address. A notification group with the same address must exist.
	<b>with Notification profile</b>	If the notification group is selected by the endpoints call address, then the specified notification profile will be applied when processing this phase.
	<b>Endpoints/Notification groups</b>	Tab in which endpoints or notification groups to be notified are assigned to the phase.
	<b>Endpoints assigned</b>	Endpoints assigned to this phase.
	<b>Label/Address</b>	Endpoint name / Endpoint address
	<b>Endpoints available</b>	Endpoints which could assigned to this phase.
	<b>Label/Address</b>	Endpoint name / Endpoint address
	<b>Notification profile</b>	Notification profile to be used in this phase for the selected assigned endpoint
	<b>Notification groups assigned</b>	Notification group assigned to this phase.
	<b>Label/Address</b>	Notification group name / Notification group address
	<b>Notification groups available</b>	Notification group which could assigned to this phase.
	<b>Label/Address</b>	Notification group name / Notification group address
	<b>Notification profile</b>	Notification profile to be used in this phase for the selected assigned group
	<b>Settings</b>	Tab for configuring general phase settings.
	<b>Duration</b>	Duration in seconds
	<b>Number of retries</b>	Never / Permanently / 1..49
	<b>Number of confirmations</b>	Individual (each endpoint) or value between 1 and 49
<b>Locations</b>	Configuration pane to administrate up to 500 endpoint locations. Locations where there are endpoints that send events to the Event Manager. Event plans can also be assigned to these locations using location-based filters so that location-dependent processes can be defined.	
	<b>Location</b>	Complete location information with parent locations

Web UI Parameter, Action & Status Information		Description
	<b>Label</b>	Location name
	<b>Description</b>	Additional information
	<b>Endpoints assigned</b>	List of endpoints assigned to this location.tyt
	<b>Label/Address</b>	Endpoint name / Endpoint address
	<b>Endpoints available</b>	List of endpoints which are not assigned to any location and could assigned to this location.
	<b>Label/Address</b>	Endpoint name / Endpoint address
<b>User</b>	Configuration pane to administrate up to 10 users who have access to the Event Manager's Web service.	
	<b>Name</b>	Username, login name
	<b>Password</b>	User password
	<b>Password confirmation</b>	User password confirmation
<b>System</b>	Administration pane for various administrative activities for the operation of the Event Manager.	
	<b>General</b>	General system settings
	<b>System name</b>	System name
	<b>CloudLink enabled</b>	Switch to enable or disable the CloudLink daemon
	<b>CloudLink status</b>	Displays the status of the CloudLink daemon
	<b>Version</b>	Running software version is shown here
	<b>Watchdog</b>	Switch to enable or disable the Watchdog functionality
	<b>Watchdog IP address</b>	IP address of the watchdog that is to be triggered
	<b>Backup/Restart</b>	Options to restart the Event Manager, backup the configuration and the event log.
	<b>Restart</b>	Restart the Event Manager
	<b>Restart with factory defaults</b>	Restart the Event Manager and resets the Event Manager configuration to default
	<b>Export log</b>	Allows to store the alarm log on the PC as a <date>-<time>_evp_summary_log.csv file and <date>-<time>_evp_details_log.csv file
	<b>Export config</b>	Allows to store the Event Manager's configuration on the PC as a <date>-<time>_evp_conf.gz file

Web UI Parameter, Action & Status Information		Description
	<b>Import config</b>	Allows to restore the Event Manager's configuration from a PC
	<b>Security</b>	Options to import trusted certificate, local certificate chain and private key (with or without password).
	<b>Trusted certificate(s)</b>	Displays how many certificates the Event Manager has
	<b>Local certificate chain</b>	Displays how many local certificate chains the Event Manager has
	<b>Private key</b>	Display if the Event Manager has a working private key
	<b>Private key: password</b>	Enter the password for the imported private key
	<b>Private key: password confirmation</b>	Confirm the password for the imported private key
	<b>Import PEM file with</b>	Define the type of PEM file to be imported
	<b>Import PEM file</b>	Import a PEM file
	<b>Delete certificates/key</b>	Delete all imported certificates and keys
	<b>Make it work</b>	Restart the Event Manager to apply changes
	<b>Security level</b>	Options to configure the security level used by the Event Manager and the used cipher suites for AXI and HTTPS connections.
	<b>Security Level</b>	Select the security level (e.g. "Legacy", "Medium" or "High")
	<b>Cipher suites of security level</b>	Select the cipher suites security level (e.g. "Legacy", "Medium" or "High")
	<b>Use defaults</b>	Switch to use or not use the default settings
	<b>Used cipher suites</b>	List of all used cipher suites, can be edited
	<b>Supported cipher suites</b>	List of all supported cipher suites
	<b>CloudLink</b>	Shows the current configuration of the CloudLink Daemon and allows to configure connection to CloudLink portal and for Remote Management.
<b>Monitor</b>	Area to display the currently active event processing activities and their status and option to terminate them.	
	<b>Cancel all</b>	Cancel all active event plans
	<b>Priority</b>	Event type priority
	<b>Type</b>	Event type
	<b>Text</b>	Event message text
	<b>Endpoint</b>	Endpoint that triggered the event

Web UI Parameter, Action & Status Information		Description
	<b>Phase</b>	Current event plan phase
	<b>Confirmations</b>	Received Confirmations/Required Confirmations
	<b>Cancel</b>	Cancel a single active event plan