EIN MITEL-
PRODUKTLEITFADEN

Mitel SIP-DECT 10.0 Event Manager

Systemhandbuch

Version 1.0

Mitel

HINWEIS

Wir gehen davon aus, dass die in diesem Dokument enthaltenen Informationen in jeder Hinsicht korrekt sind, übernehmen jedoch keine Garantie für die Mitel Networks™ Corporation (MITEL®). Die Informationen können ohne Vorankündigung geändert werden und sind in keiner Weise als Verpflichtung von Mitel oder einer seiner Tochtergesellschaften oder Niederlassungen zu verstehen. Mitel und seine verbundenen Unternehmen und Tochtergesellschaften übernehmen keine Verantwortung für Fehler oder Auslassungen in diesem Dokument. Überarbeitungen dieses Dokuments oder Neuauflagen können herausgegeben werden, um solche Änderungen zu berücksichtigen.

WARENZEICHEN

Mitel SIP-DECT 10.0 Event Manager

System Manual

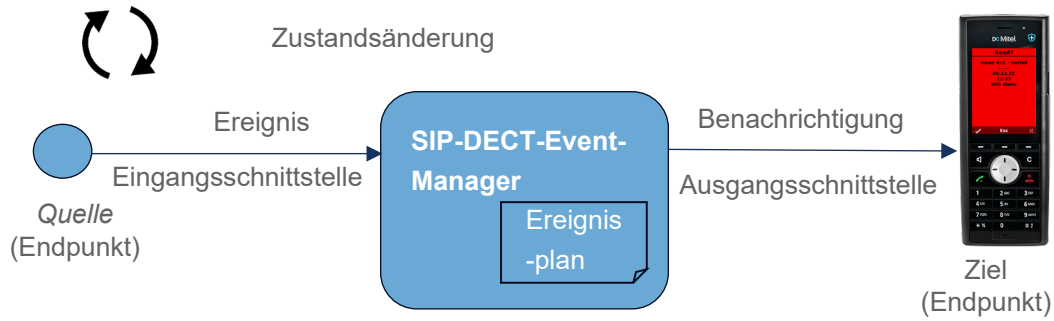
Release 10.0 – April 25

Inhaltsverzeichnis

Überblick

Einleitung

Der SIP-DECT-Event-Manager ist eine integrierte Softwarekomponente eines Mitel SIP-DECT-Systems. Es wird für die automatisierte Verarbeitung eingehender Ereignisse und das Versenden von ausgehenden Benachrichtigungen verwendet. Der SIP-DECT-Event-Manager kann Ereignisse aus verschiedenen Quellen verarbeiten, darunter SIP-DECT-Telefone, das SIP-DECT-System selbst und andere externe Systeme. Die Verarbeitung der Ereignisse erfolgt nach benutzerdefinierten Regeln, die vom Administrator festgelegt werden.



Der primäre Ablauf besteht darin, Benachrichtigungen als Textnachrichten an SIP-DECT-Telefone zu senden, die durch eingehende Ereignisse ausgelöst werden. Auf diese Weise unterstützt SIP-DECT Kunden-Workflows über Sprachanrufe hinaus, z.B. können Textnachrichten an DECT-Telefone gesendet werden, um über Ereignisse von Schwesternrufsystemen zu informieren, ohne dass zusätzliche Hardware erforderlich ist.

Verarbeitungsregeln für verschiedene Arten von Ereignissen bestehen aus Ereignisplänen, deren Ereignisphasen, Meldungsprofilen und verschiedenen Arten von Bestätigungsanfragen.

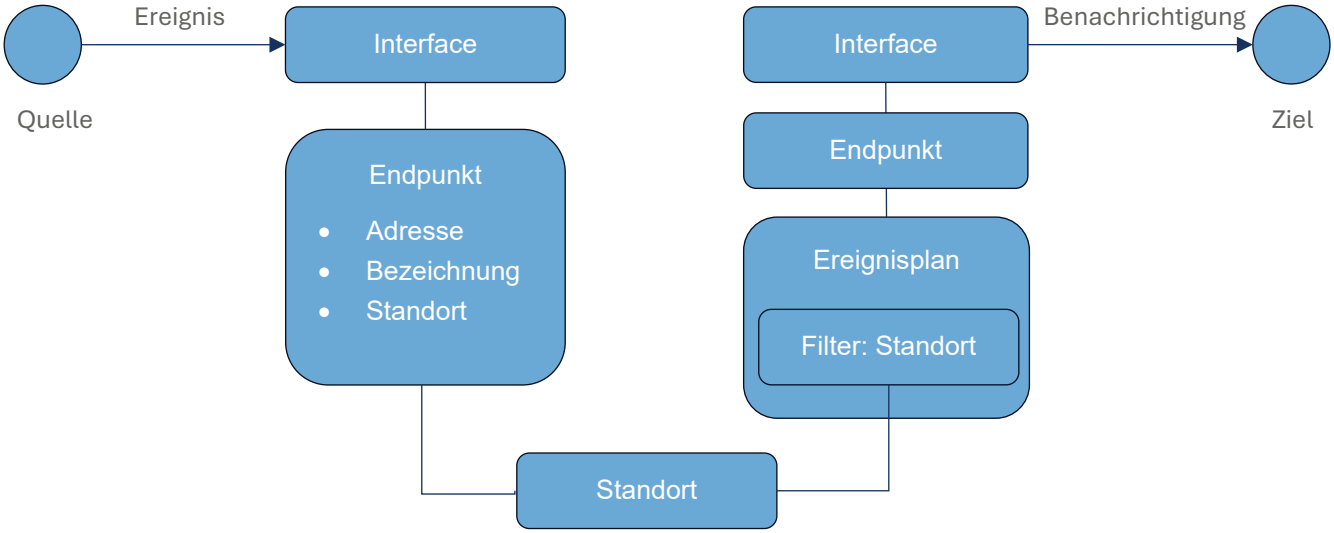
Kommt es zu einer Statusänderung, z.B. einem Tastendruck, sendet eine Quelle über eine Eingangsschnittstelle ein Ereignis an den SIP-DECT-Event-Manager. Der SIP-DECT-Event-Manager generiert Benachrichtigungen, z.B. Textnachrichten, und sendet diese über ausgehende Schnittstellen nach einem geeigneten Ereignisplan an Ziele, z.B. SIP-DECT-Telefone.

Bei einigen Schnittstellentypen handelt es sich nur um eingehende oder nur ausgehende Schnittstellen, und einige können sowohl eingehend als auch ausgehend sein. Schnittstellen werden im Kontext des Event Managers als Interfaces bezeichnet.

Quellen und Ziele werden als Endpunkte bezeichnet. Sie sind den Schnittstellen zugeordnet, über die sie mit dem SIP-DECT-Event-Manager kommunizieren. Endpunkte haben eine eindeutige Identifikation, z. B. eine Telefonnummer.

Endpunkte werden auch Standorten zugewiesen. Je nach Standort kann ein bestimmter Ereignisplan ausgewählt werden. Auf diese Weise kann ein und dasselbe Ereignis unterschiedlich behandelt werden, je nachdem, wo es entstanden ist.

In der folgenden Abbildung sollen die Beziehungen zwischen dem Endpunktstandort und dem Standortfilter des Ereignisplans visualisiert werden.



Der Event Manager DECT Lokalisierung ergänzt die oben beschriebene Event Manager Funktionalität um eine textliche und grafische Anzeige der Position eines DECT-Gerätes basierend auf der DECT-Funkabdeckung durch eine Basisstation (typischerweise ca. 30 bis 50 Meter in Gebäuden je nach baulichen Gegebenheiten und ca. 300 Meter im freien Feld) im Falle eines Notrufes, ausgelöst durch Drücken der SOS-Taste am Mitel DECT-Telefon (722dt, 732d, 742d, 632d(t V2)). 300 Meter im freien Feld) im Falle eines Notrufs, ausgelöst durch Drücken der SOS-Taste am Mitel DECT-Telefon (722dt, 732d, 742d, 632d(t) V2) oder durch einen Sensoralarm des DECT-Gerätes (732d, 742d, 632d(t) V2) sowie Feature Access Codes für kundenspezifisch konfigurierbare Alarmauslöser. Darüber hinaus kann die Position eines ortbaren DECT-Gerätes auch unabhängig von einem Ereignis abgefragt werden.

Die grafische Darstellung erfolgt in einer Detail- und einer Übersichtsansicht.

Für die grafische Darstellung der Position eines DECT-Gerätes im Ereignisfall muss ein geeigneter Ereignisplan konfiguriert werden und somit das auslösende DECT-Telefon als Endpunkt eingerichtet werden. Im Monitor wird im Lokalisierungsbereich eine Lokalisierungstaste angeboten, die die grafische Darstellung öffnet.

Achtung! Der entsprechende Ereignisplan wird anhand des konfigurierten Standorts und nicht anhand der über DECT ermittelten Position ausgewählt.

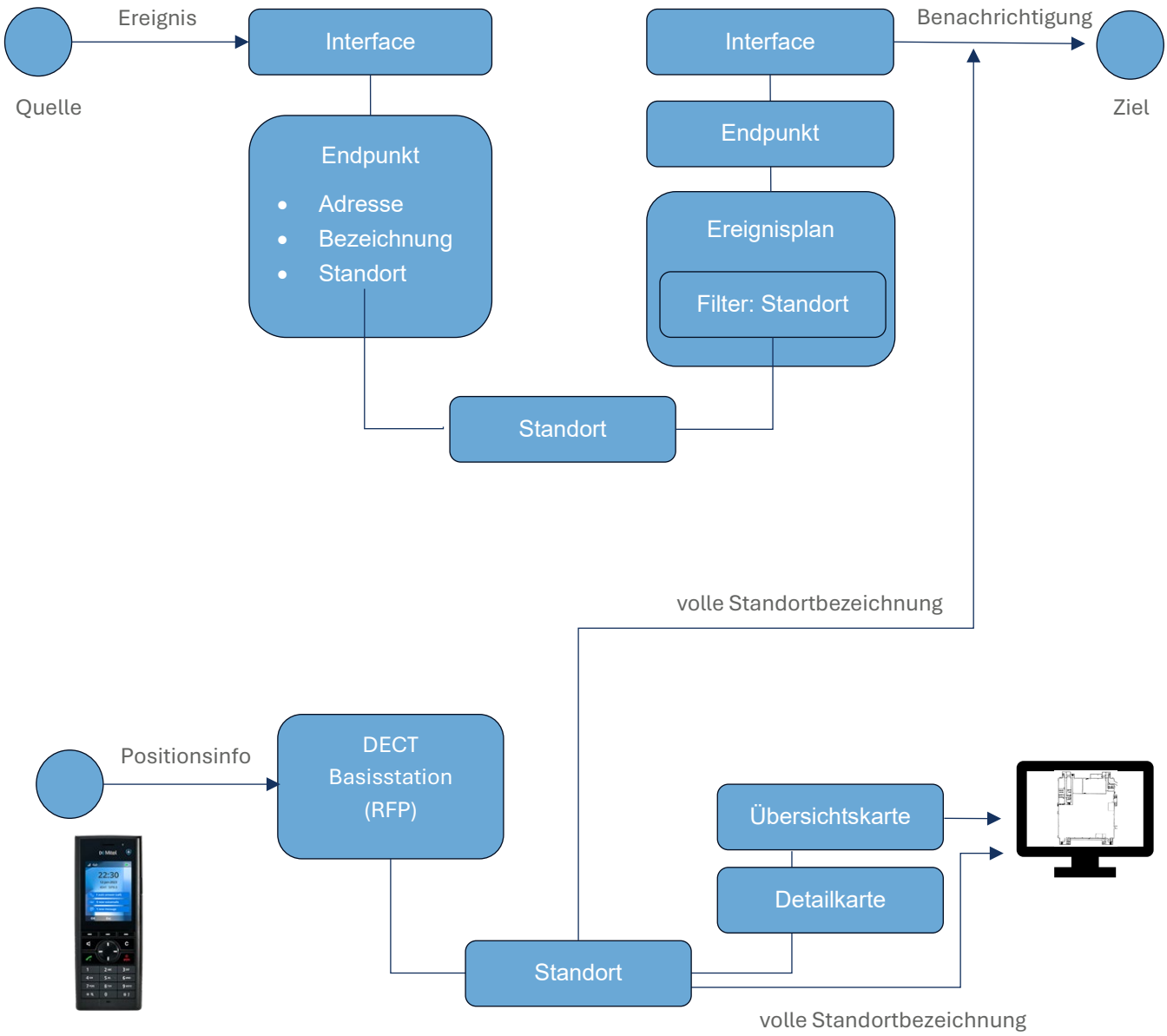
Für eine ereignisunabhängige Ermittlung und Anzeige der Position des DECT-Endgerätes eines ortbaren und ggf. verfolgbaren Teilnehmers ist kein Ereignisplan erforderlich. Hierfür kann die Telefonbenutzerliste im Bereich Ortung verwendet werden, die alle ortbaren Benutzer enthält. Auch hier ist eine Lokalisierungstaste vorhanden.

Um den Standort eines DECT-Telefons zu bestimmen, müssen die DECT-Basisstationen Standorten zugewiesen werden. Außerdem muss dem Standort eine Karte zugeordnet werden und der Standort muss auf einer Detailkarte und auf einer Übersichtskarte zur grafischen Darstellung positioniert werden.

Wenn die SIP-DECT-Lokalisierung verwendet wird, wird in der Benachrichtigung der vollständige Standortname aus dem Event Manager anstelle der im OMM konfigurierten Basisstationsdaten Standort,

Gebäude, Korridor usw. verwendet. Dadurch wird sichergestellt, dass der Standort in den Benachrichtigungen mit den Angaben in der Weboberfläche des Event Managers übereinstimmt.

Die folgende Abbildung veranschaulicht die Beziehungen zwischen Basisstationen, Karten und Standorten sowie die Ereignisbehandlung im Ereignis-Manager.



Um DECT-Lokalisierung nutzen zu können, ist eine Linux-Server-Installation des Event Managers erforderlich.

Achtung! Es wird empfohlen, Standorte nicht zu granular zu planen und einzurichten, da DECT mit größeren und überlappenden Funkfeldern arbeitet.

Wo läuft der SIP-DECT-Event-Manager?

RFP der 4. Generation

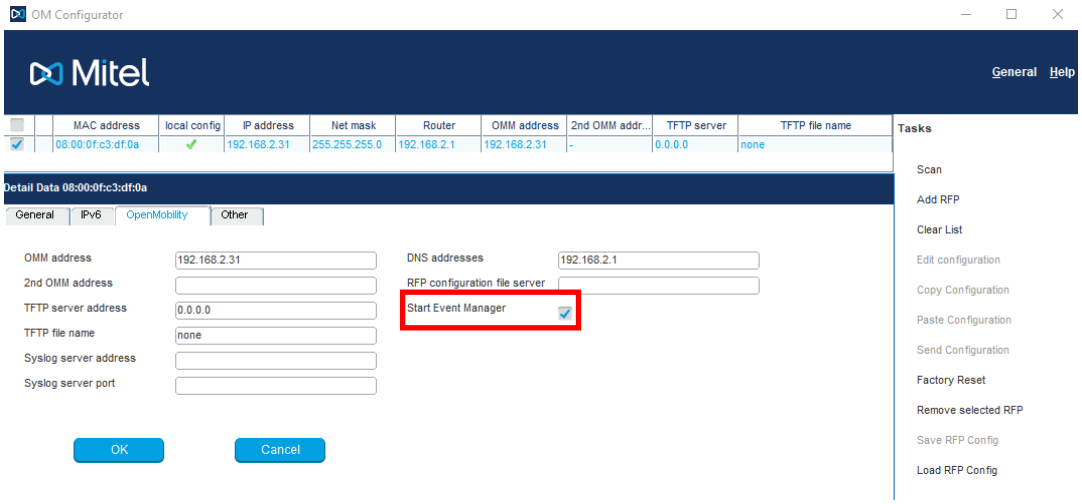
Der SIP-DECT-Event-Manager kann auf einem RFP der 4. Generation (RFP44, RFP45, RFP47 oder RFP48

WLAN) laufen und ist Teil des SW-Pakets iprfp4G.dnld.

Der SIP-DECT-Administrator legt im OMC (OM Configurator) fest, auf welchem RFP der SIP-DECT-Event-Manager gestartet wird. Dadurch kann ein anderer RFP als der OMM verwendet werden, so dass OMM und SIP-DECT-Event-Manager nicht um die gleichen Ressourcen konkurrieren.

Dies impliziert auch, dass der SIP-DECT-Event-Manager-RFP (der RFP, auf dem der SIP-DECT-Event-Manager ausgeführt wird) über eine lokale statische IP-Konfiguration verfügt. Dadurch wird sichergestellt, dass der SIP-DECT-Event-Manager unabhängig von anderen Diensten gestartet werden kann und immer unter der gleichen IP-Adresse erreichbar ist, wie es bei Diensten üblich ist. Es wird nur ein SIP-DECT-Event-Manager pro SIP-DECT-Installation unterstützt.

Um den SIP-DECT-Event-Manager zu starten, muss das Flag "Start Event Manager" wie unten gezeigt gesetzt werden.



Wenn dieses "Start Event Manager"-Flag über den OMC wieder von einem RFP entfernt wird, wird der Event Manager gestoppt und seine Datenbank wird beim nächsten Start des RFPs entfernt.

Bitte beachten Sie: Der Event Manager auf einem RFP kann nur Konfigurationen innerhalb der Konfigurationsgrenzen eines RFP OMM verarbeiten, d.h. max. 256 RFPs und max. 1024 DECT-Benutzer. Wenn der OMM auf einem Linux-Server läuft, muss der Event Manager ebenfalls auf einem Linux-Server laufen

Linux Server

Der Event Manager kann auch als Anwendung auf einem Rocky Linux® 9 installiert werden. Hierfür steht eine rpm-Datei zur Verfügung. Die rpm-Datei ist auch Bestandteil der SIP-DECT VM-Images. Nach dem ersten Start einer VM kann der OMM, MOM oder der Event Manager installiert werden. Informationen dazu finden Sie in der Administrationsanleitung zur SIP-DECT LINUX Server Installation.

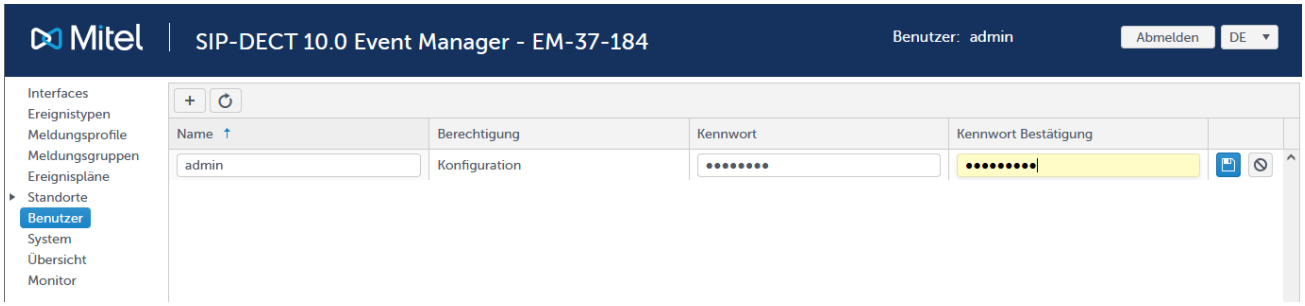
Die Linux Server Installation des Event Managers unterstützt die DECT-Lokalisierung mit einer textlichen und grafischen Darstellung der Position eines DECT-Gerätes. Siehe dazu den Abschnitt DECT-Lokalisierung. Ansonsten unterscheidet sich der EM auf einem Linux Server hinsichtlich des Funktionsumfangs nicht von einem EM auf einem RFP.

Da der Mitel CloudLink-Daemon für Serverinstallationen des Event Managers nicht zur Verfügung steht, ist das Remote-Management in diesem Fall nicht verfügbar.

Zugriff auf den SIP-DECT-Event-Manager

Der SIP-DECT-Event-Manager verfügt über eine eigene Web-Administrationsoberfläche, die über https://<RFP-IP-Adresse>:8444 erreichbar ist.

Verwenden Sie **admin** als Benutzernamen und Passwort, um sich zum ersten Mal anzumelden. Bei der ersten Anmeldung wird der Benutzer aufgefordert, das Passwort zu ändern.



Lizenzvoraussetzungen für den SIP-DECT-Event-Manager

Der SIP-DECT-Event-Manager benötigt eine Lizenz für die konfigurierten und aktivierten Endpunkte. Es ist eine integrierte Lizenz für 5 Endpunkte enthalten.

Für zusätzliche Endpunktlizenzen ist eine SIP-DECT-Lizenz erforderlich, die die Anzahl der konfigurierten SIP-DECT-Event-Manager-Endpunkte abdeckt. Es wird dringend empfohlen, diese Lizenz vor der Konfiguration des Event Managers in den OMM zu importieren.

Wenn die Anzahl der konfigurierten SIP-DECT-Event-Manager-Endpunkte die Anzahl der lizenzierten Endpunkte überschreitet, wird eine Warnung auf der Administrator-Weboberfläche angezeigt und alle 15 Minuten werden Benachrichtigungen an verschiedene zufällig ausgewählte SIP-DECT-Endpunkte gesendet. Diese Benachrichtigungen werden nicht vom Event Manager überwacht und können nicht aus der Anwendung gelöscht werden (auch nicht für den Fall, dass die Lizenz aktualisiert wird, um die konfigurierte Anzahl von Endpunkten abzudecken). Die Benachrichtigungen sind auf den SIP-DECT-Endgeräten sichtbar, solange sie nicht auf den Endgeräten selbst gelesen und gelöscht werden.

Der SIP-DECT-Event-Manager nutzt erweiterte SIP-DECT-Messaging- und Alarmierungsfunktionen, ohne dass eine "Mitel SIP-DECT Messaging & Alerting License Enterprise"-Lizenz erforderlich ist.

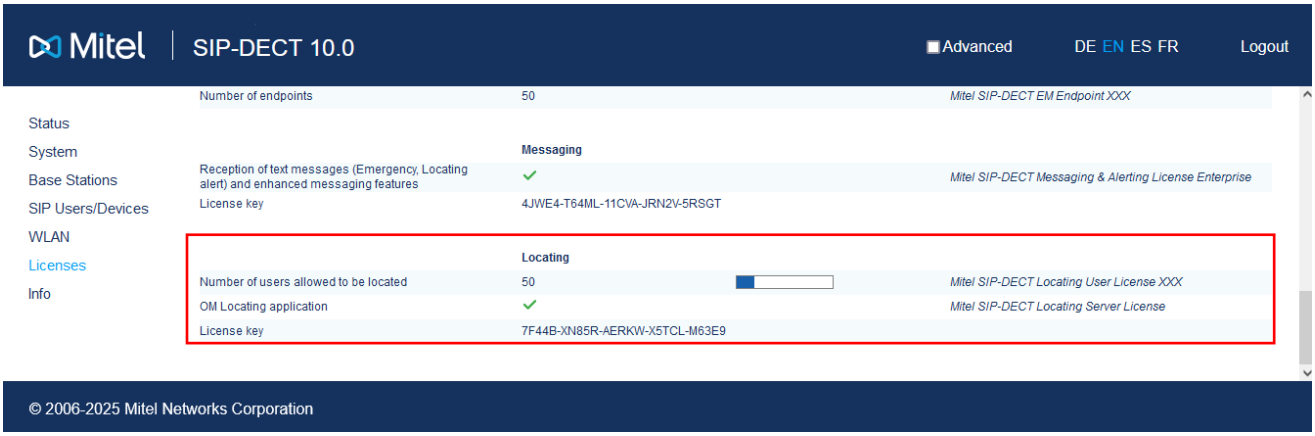
Der SIP-DECT-Event-Manager liefert automatisch Standortinformationen für SIP-DECT-Alarmauslöser, z. B. SOS-Key oder Man-Down, ohne dass eine Lokalisierungslizenz "Mitel SIP-DECT Locating User License XXX" erforderlich ist. Die Anwendung ‚OM Locating' wird auch nicht benötigt, um den SIP-DECT-Event-Manager zu betreiben.

Lizenzvoraussetzungen für die SIP-DECT Lokalisierungsfunktionalität

Für die Nutzung der Lokalisierungsfunktionalität sind folgende SIP-DECT-Lizenzen erforderlich:

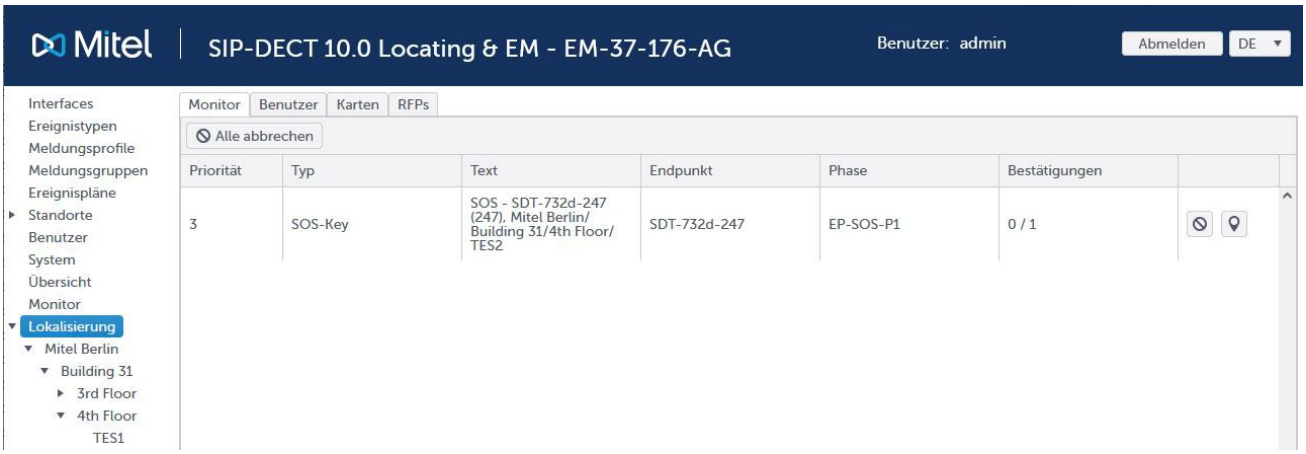
- Mitel SIP-DECT Locating User License XXX

- Mitel SIP-DECT Locating Server License



Die Mitel SIP-DECT Locating Server-Lizenz muss in den OMM importiert werden, bevor die Lokalisierungsfunktionalität auf der EM Weboberfläche sichtbar wird.

Sobald die Lizenz angewendet und der EM-Anwendung zur Verfügung gestellt wurde, ändert sich der Name in der oberen Leiste, Lokalisierung erscheint in der Navigationsleiste und ermöglicht den Zugriff auf die Lokalisierungsfunktionalität, wie z. B. eine Liste der lokalisierbaren Benutzer.



Bitte beachten Sie, dass nur lokalisierbare Benutzer angezeigt werden und dass für diese die Mitel SIP-DECT Locating User License erforderlich ist.

Solange Benutzer keine Ereignisse auslösen oder Benachrichtigungen erhalten sollen, müssen sie nicht aus dem OMM in den EM importiert worden sein und als Endpunkt in der SIP-DECT-Schnittstelle existieren. Sie erscheinen trotzdem in der Liste der lokalisierbaren Benutzer. Das bedeutet, dass für diese Benutzer keine Endpunktlizenz erforderlich ist.

Wenn Benutzer als Endpunkte importiert wurden, aber nur lokalisiert werden sollen, ohne Ereignisse auszulösen oder Benachrichtigungen zu erhalten, können diese Endpunkte auf inaktiv gesetzt werden. Sie sind dann immer noch in der Liste der lokalisierbaren Benutzer aufgeführt, werden aber nicht auf die Endpunktlizenz angerechnet.

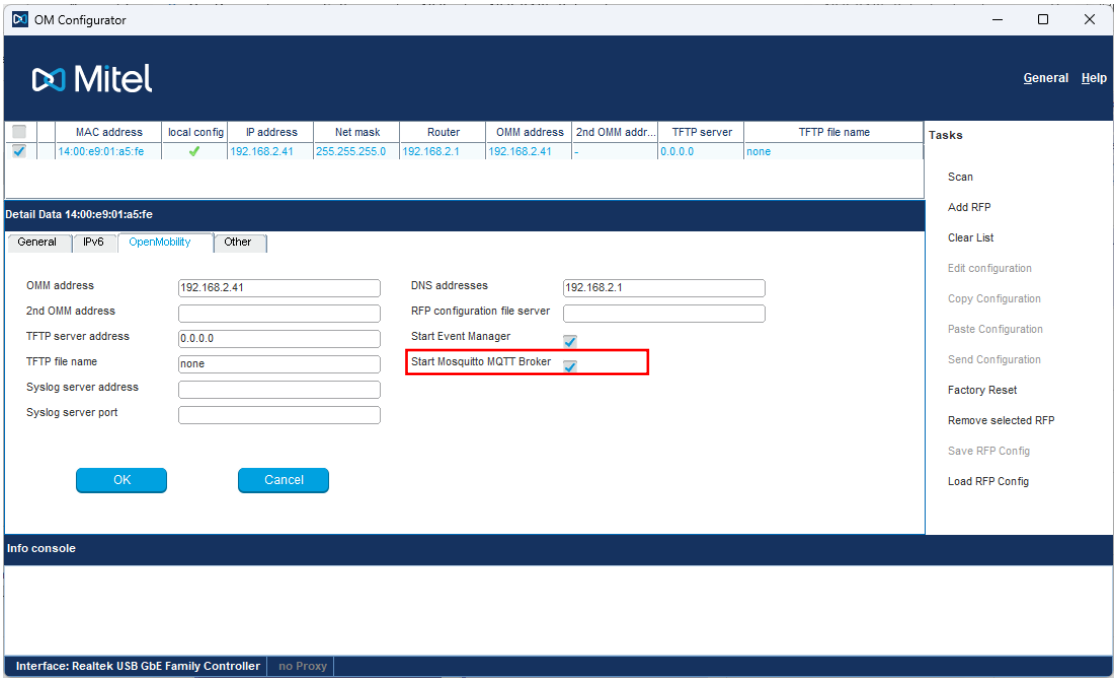
Unterstützte DECT-Telefone

Der SIP-DECT-Event-Manager unterstützt die 700d DECT-Telefonfamilie. Die DECT-Telefonfamilie SIP-DECT 600d V2 wird ebenfalls unterstützt. Ältere Generationen der 600d-Gerätefamilie oder deren ältere SW-Versionen unterstützen möglicherweise nicht alle SIP-DECT-Messaging-Funktionen und können daher Einschränkungen aufweisen. Bitte beachten Sie auch die Informationen im ‚Benutzerhandbuch für Mitel 600/700 DECT Phone Messaging and Alerting Applications'.

Eclipse Mosquitto™ Opensource MQTT broker auf RFP4G

Es ist möglich, einen funktional eingeschränkten Eclipse Mosquitto™ Open Source MQTT Broker auf einem RFP4G zu starten. Dies ermöglicht den Betrieb von MQTT in Verbindung mit dem Event Manager und MQTT-fähigen Geräten hauptsächlich zu Testzwecken.

Der SIP-DECT-Administrator legt im OMC (OM Configurator) fest, auf welchem RFP der MQTT Broker gestartet wird. Dazu muss das Flag "Start Mosquitto MQTT Broker" wie unten gezeigt gesetzt werden



Wenn die folgenden Einschränkungen akzeptiert werden, ist der Einsatz in betrieblichen Umgebungen möglich.

- Maximal 150 Clients werden parallel unterstützt.
- keine Unterstützung für zurückbehaltene Nachrichten (Clients, die das Retain-Flag in Veröffentlichungsnachrichten setzen, werden getrennt).
- QoS 0 wird empfohlen. Bitte vermeiden Sie MQTT QoS Level 1 und 2, da zusätzliche Einschränkungen gelten.
- Die maximale Paketgröße für einzelne MQTT-Nachrichten beträgt 4096 Byte (Clients, die größere Pakete senden, werden getrennt). Eine MQTT-Nachrichtengröße von ~1200 Byte wird empfohlen, um Fragmentierung und zusätzliche CPU- und Speicherbelastung zu vermeiden.
- keine Unterstützung für persistente Sitzungen.
- keine Unterstützung für WebSocket-Verbindungen.
- keine Unterstützung für TLS, nur Port 1883 wird unterstützt.
- keine Client-Authentifizierung, anonymer Zugriff ist möglich.

Der Broker sollte nicht zusammen mit dem OMM oder dem Event Manager auf einem 4G RFP laufen. Wenn eine ausreichende Anzahl von RFPs verfügbar ist, sollte der Broker auf einem separaten RFP aktiviert werden.

Zusätzliche Hinweise:

Der Mosquitto Broker veröffentlicht alle 10s Statistiken und Nutzungsinformationen unter der Topic-Hierarchie '$SYS/broker/#'.

Das Tool MQTT-Explorer (https://mqtt-explorer.com/) zeigt diese Informationen standardmäßig an.

Mit mosquitto_sub können die Informationen auch abgerufen und in einer Datei gespeichert werden:

```
mosquitto_sub -h <Broker-ip-address> -p 1883 -t '$SYS/#' -v
```

Das Broker-Logging kann unter der Topic-Hierarchie '$SYS/broker/log/#' abgerufen werden. Die Nachrichten werden hier vom Broker gesendet, wenn das entsprechende Ereignis eintritt. Es ist nicht möglich, Protokollmeldungen für Ereignisse in der Vergangenheit abzurufen, der Broker speichert diese Informationen nicht.

Nur die Logmeldungen des Brokers werden mit dem folgenden Befehl abgerufen.

```
mosquitto_sub -h <Broker-IP-Adresse> -p 1883 -t '$SYS/Broker/log/#' -v
```

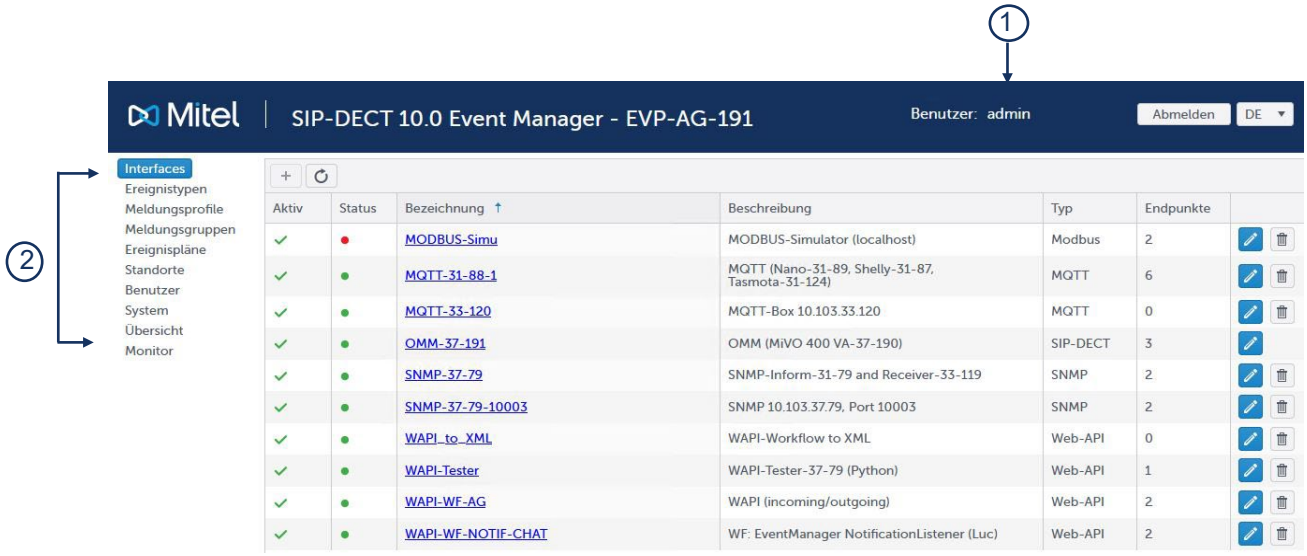
Hinweis: MQTT-Explorer und mosquitto_sub können parallel auf demselben Broker laufen, der MQTT-Explorer eignet sich gut zur Anzeige von Status- und Statistikinformationen und mosquitto_sub kann zur Aufzeichnung der Log-Ausgaben des Brokers verwendet werden.

Verwenden des SIP-DECT-Event-Managers

Um so schnell wie möglich die ersten praktischen Schritte mit dem SIP-DECT-Event-Manager zu machen, können Sie mit dem Abschnitt Schnellstart-Konfigurationshandbuch SIP-DECT-Event-Manager beginnen.

Benutzeroberfläche des SIP-DECT-Event-Managers

Der SIP-DECT-Event-Manager verfügt über eine eigene Web-Administrationsoberfläche, die über https://<RFP-IP-Adresse>:8444 erreichbar ist. Die Weboberfläche besteht aus einer Reihe von Administrationsbereichen, auf denen die verschiedenen Einstellungen des SIP-DECT-Event-Managers konfiguriert werden können und auf die von jedem Computer oder Gerät mit einem Webbrowser im selben Netzwerk oder über Remote-Management (wenn für den EM auf einem RFP4G konfiguriert) zugegriffen werden kann. Der Web-Service ist als Single-Page-Application (SPA) realisiert.



1 Login-Bereich

2 Administrationsbereiche

Login-Bereich

Sprachauswahl

Folgende Sprachen stehen zur Verfügung: Deutsch, Englisch, Französisch und Spanisch. Beim Anlegen der Konfiguration werden eine Reihe von Standardwerten (z.B. Ereignistypen) in der zu diesem Zeitpunkt ausgewählten Sprache eingerichtet. Die in der Konfiguration enthaltenen Werte werden durch das Umschalten der Sprache nicht beeinflusst.

Verwenden Sie "admin" als Benutzernamen und Passwort, um sich zum ersten Mal anzumelden. Bei der ersten Anmeldung wird der Benutzer aufgefordert, das Passwort zu ändern.

Administrationsbereiche

Der SIP-DECT-Event-Manager enthält mehrere Bereiche, die unterschiedliche Informationen über den SIP-DECT-Event-Manager enthalten.

Administrationsbereich	Beschreibung
Interfaces	Der Bereich "Interfaces" bietet einen Überblick über den Status von Systemen, die mit dem SIP-DECT-Event-Manager verbunden sind. Derzeit sind die Interfaces ESPA, SIP-DECT (OMM), MODBUS (z.B. WAGO) und SNMP verfügbar. Die Anzahl der einzurichtenden Interfaces ist derzeit auf 5 Interfaces begrenzt.
Ereignistypen	Im Bereich Ereignistypen können Sie neue Ereignistypen erstellen oder vorhandene ändern. Es stehen **5 Standard-Ereignistypen** ('Man-Down', ‚No Move', ‚ESCAPE' 'SOS-Key' und 'Systeminfo') zur Verfügung. Diese Typen können nicht gelöscht werden. Der Ereignistyp dient als eine Art Filter in einem Ereignisplan, um die Eskalation eines Ereignisses zu steuern. Anhand der zugewiesenen Priorität kann dem System mitgeteilt werden, in welcher Reihenfolge das Ereignis abgearbeitet werden soll.
Meldungsprofile	Die Anzeige und akustische Signalisierung eines Ereignisses an den SIP-DECT-Endgeräten kann innerhalb eines Meldungsprofils konfiguriert werden.
Meldungsgruppen	Endpunkte, die Benachrichtigungen empfangen können (z. B. SIP-DECT Telefonendpunkte), können zu einer Meldungsgruppe zusammengefasst werden. Das vereinfacht die Konfiguration.
Ereignispläne	Der Bereich Ereignispläne ermöglicht das Erstellen, Bearbeiten und Löschen von Ereignisplänen. Ein Ereignisplan gibt an, wie empfangene Ereignisse in Abhängigkeit vom Standort des Ursprungsendpunkts behandelt werden sollen. d.h. welche Endpunkte Benachrichtigungen erhalten sollen und wie reagiert werden soll, wenn keine Bestätigungen empfangen werden. Ein Ereignisplan kann einen oder mehrere Ereignistypen und einen oder mehrere Standorte enthalten. Dies bedeutet, dass der Ereignisplan nur für Ereignisse des konfigurierten Typs verwendet wird und wenn der Ursprungsendpunkt zum angegebenen Standort gehört.
Standorte	Der Event Manager unterstützt die Verwaltung von Standorten, denen Endpunkte als Quellen von Ereignissen zugewiesen sind. Auch Ereignispläne werden Standorten zugewiesen. Dies ermöglicht die ortsspezifische Definition von Ereignisplänen, d.h. es ist möglich, je nach Standort des Absenders eines Ereignisses unterschiedliche Empfänger zu benachrichtigen.
Benutzer	Der Benutzerbereich ermöglicht das Erstellen, Bearbeiten und Löschen von Benutzern. Der Standardbenutzer **admin** kann nicht gelöscht werden.
System	Der Bereich "System" umfasst verschiedene Registerkarten zur Konfiguration des Systemnamens sowie der Anzeige der aktuellen Softwareversion. Darüber hinaus ist hier die Konfiguration eines Watchdogs und das Aktivieren des CloudLink Daemons für die Fernwartung des Systems möglich. Ein Neustart des Systems (gegebenenfalls mit Werkseinstellungen), das Exportieren von Protokollen und Datensicherungen sowie der Import von Datensicherungen kann hier angefordert werden. Auch der Import von SSL-Zertifikaten, die Einstellung eines Security levels und die Konfiguration von Cipher suites ist hier möglich. Bei aktiviertem CloudLink Daemon, ist über eine spezielle Registerkarte eine

Administrationsbereich	Beschreibung
	Oberfläche zur detaillierten Konfiguration und Statusanzeige des CloudLink Daemons verfügbar.
Overview	Der Übersichtsbereich zeigt eine kurze Zusammenfassung der Event Manager-Konfiguration (mit verschiedenen Tabellen zu Ereignisfluss, Benachrichtigungsgruppen, MQTT-Zuordnungen und Beziehungen zwischen Schnittstellen und Endpunkten).
Monitor	Im Bereich "Monitor" wird eine Liste der aktiven Ereignisbehandlungen angezeigt, und der Administrator kann ein einzelnes Ereignis oder alle Ereignisse beenden.

Monitoransicht

Die Monitoransicht ist die Ansicht für Benutzer mit der Berechtigung "Monitor". In dieser Ansicht ist keine Konfiguration möglich. Der einzige Zweck dieser Ansicht ist die Anzeige laufender Ereignisflüsse. Der Benutzer kann einen einzelnen laufenden Ereignisplan oder alle laufenden Ereignispläne abbrechen.

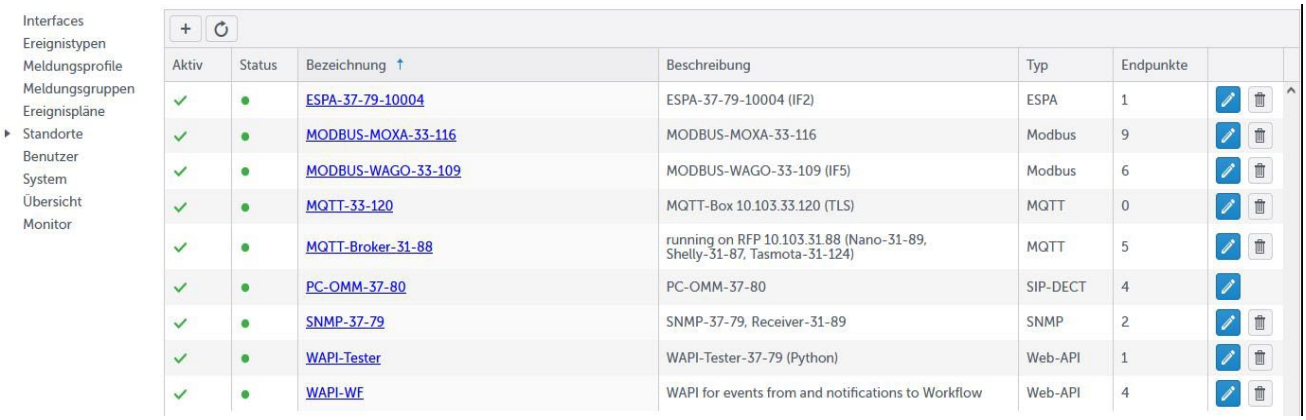
Interfaces

Interfaces verbinden den SIP-DECT-Event-Manager mit anderen Geräten und Diensten. Je nach Typ unterstützen diese Interfaces das Empfangen von Ereignissen oder das Senden von Benachrichtigungen, manchmal beides.

Die folgenden Arten von Interfaces können konfiguriert werden:

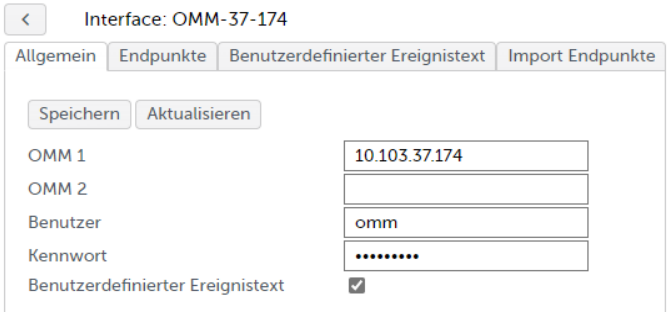
Typ	Maximale Anzahl
SIP-DECT (OMM)	1
ESPA	4
Modbus (e.g. WAGO or MOXA)	2
SNMP	2
MQTT	2
Web-API	4

Im Konfigurationsbereich Interfaces werden alle konfigurierten Interfaces angezeigt und können ausgewählt und bearbeitet werden.



SIP-DECT (OMM) Interface

Dieses Interface wird standardmäßig erstellt und kann nicht gelöscht werden.



Für das SIP-DECT-Interface können in den nachfolgend beschriebenen Registerkarten verschiedenste Einstellungen vorgenommen werden.

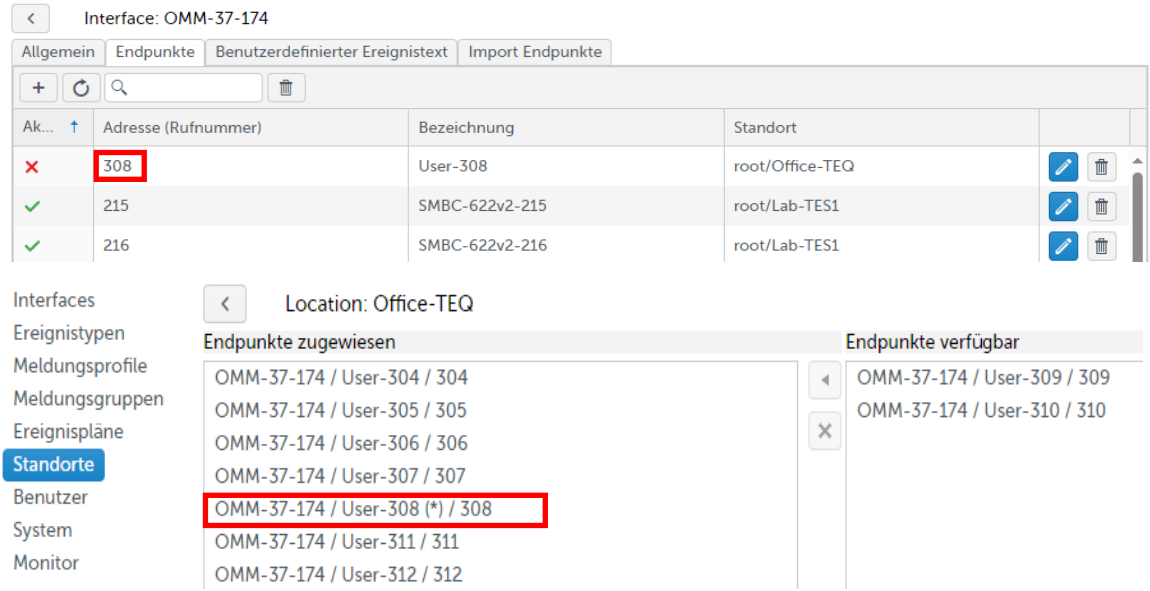
Registerkarte "Allgemein"

Auf der Registerkarte Allgemein können Sie die OMM-IP-Adresse(n), den Benutzer und das Kennwort eingeben, damit sich der SIP-DECT-Event-Manager mit dem OMM verbinden kann. Dies wird dadurch angezeigt, dass der Interfacestatus grün wird. Aktivieren Sie das Kontrollkästchen "Benutzerdefinierter Ereignistext", wenn die Änderungen unter dem Reiter "Benutzerdefinierter Ereignistext" wirksam werden sollen.

Registerkarte "Endpunkte"

Auf der Registerkarte Endpunkte werden die Quellen oder Empfänger von Nachrichten im SIP-DECT-System definiert. Um die Einrichtung der Endpunkte auf dem SIP-DECT-Interface zu vereinfachen, können die im OMM eingerichteten Endpunkte importiert werden.

Bitte beachten Sie, dass ein Endpunkt, der nicht als aktiv gekennzeichnet ist, nicht zum Auslösen eines Alarms verwendet werden kann und nicht als lizenzierter Endpunkt gezählt wird. Inaktive Endpunkte werden in anderen Konfigurationsbereichen mit (*) gekennzeichnet, wie unten dargestellt.



Registerkarte Benutzerdefinierter Ereignistext

Die Registerkarte Benutzerdefinierter Ereignistext wird verwendet, um spezielle Texttypen anzupassen, die an die DECT-Telefone gesendet werden, wenn ein Ereignis verarbeitet wird.

Diese Funktion ermöglicht es, Organisationen, Behörden oder Einzelpersonen, Notfallnachrichten mit bestimmten Details oder Anweisungen zu erstellen und zu versenden, die für eine spezielle Situation relevant sind.

Die in diesem Abschnitt definierten Texte werden nur wirksam, wenn die Checkbox 'Benutzerdefinierter Ereignistext' auf der Registerkarte Allgemein aktiviert ist.

Der Meldungstext setzt sich normalerweise aus dem Ereignistyp und der Position des Ursprungsendpunkts zusammen. Die Zusammenstellung von Alarmtexten kann aber hier auch mit benutzerdefinierten Alarmtexten flexibel konfiguriert werden.

Der Text, der während des Auslösens des Ereignisses von dem Interface geliefert wird, kann vor der weiteren Bearbeitung durch Ersetzen einzelner Zeichenketten geändert werden. Die zu ersetzenden Zeichenketten sollten in die Felder "Text" und "Ersetzt durch" eingetragen werden.

Für die Zusammenstellung des Alarmtextes können bis zu vier Texte verwendet werden. Für jeden dieser Texte sollte eine maximale Länge definiert werden. Als Abstandshalter zwischen den Texten kann entweder ein Leerzeichen oder ein Zeilenvorschub verwendet werden. Da Zeilenvorschübe nicht auf allen Endpunkten angezeigt werden können, werden sie bei Bedarf automatisch durch Leerzeichen ersetzt.

Folgende Texte stehen zur Verfügung:

- Art des Ereignisses
- Ereignistyp kurz – max. 8 Zeichen
- Priorität – Priorität des Alarms, die durch den Alarmtyp definiert wird
- Auslösender Endpunkt (Name) – Name des Endpunkts, an dem der Alarm ausgelöst wurde
- Auslösender Endpunkt (Adresse) – Adresse (z. B. Telefonnummer) für den Endpunkt, an dem der Alarm ausgelöst wurde
- Standort des auslösenden Endpunktes – Umgebung, der der ausgelöste Alarm durch die Konfiguration oder durch die DECT-Ortung zugewiesen wird
- Phase – Die Bezeichnung der aktuellen Phase des aktiven Ereignisplanes
- Empfangener Text vom Interface – ermöglicht die Verwendung von zusammengesetzten Alarmtexten, die auf speziellen Interfaceeinstellungen (z. B. ESPA) basieren

Registerkarte "Import Endpunkte"

Die Registerkarte Import Endpunkte ermöglicht den automatischen Import der im SIP-DECT-System konfigurierten DECT-Geräte als Endpunkte in die SIP-DECT-Event-Manager-Konfiguration. Diese Funktion kann nur verwendet werden, wenn eine Verbindung zwischen dem SIP-DECT-Event-Manager und dem SIP-DECT-System (OMM) hergestellt wurde.

Wenn die von der Lizenz erlaubte Anzahl von Endpunkten durch den Import überschritten wird, wird eine Warnung angezeigt.

Es sollten nur diejenigen Endpunkte importiert werden, die als auslösende oder zu notifizierende Endpunkte benötigt werden (es werden EM Endpunkt-Lizenzen benötigt).

Die importierten Endpunkte können auf der Registerkarte Endpunkte gelöscht werden.

ESPA-Interface

Das ESPA-Interface ermöglicht den Anschluss von Geräten, die den Datenaustausch nach dem ESPA 4.4.4-Protokoll unterstützen. Dieses Protokoll wurde von der ‚European Selective Paging Manufacturer's Association' für die Steuerung von Funkrufgeräten und für den Anschluss von Brandmelde- und Lichtsignalsystemen festgelegt.

Der SIP-DECT-Event-Manager unterstützt das ‚ESPA 4.4.4 Protokoll over IP'. Dies ermöglicht den Austausch von Meldungen mit Brandmeldeanlagen, Lichtsignalanlagen, Funkrufanlagen und ähnlichen Systemen, die diese Schnittstelle ebenfalls unterstützen. Ein ESPA-Interface kann nur als Eingang (SIP-DECT-Event-Manager empfängt Nachrichten) und nicht als Ausgang (SIP-DECT-Event-Manager sendet Nachrichten) arbeiten.

Sofern von der Gegenseite unterstützt, ermöglicht der SIP-DECT Event Manager die protokollmäßige Überwachung der ESPA-Verbindung.

Der Anschluss der Komponenten erfolgt direkt über TCP/IP-Bytestream oder über RS-232/IP-Konverter. Der SIP-DECT-Event-Manager fungiert als TCP-Client in einem ESPA-Slave-Modus.

Eine ESPA-Nachricht enthält Informationen, die in nummerierten Feldern organisiert sind. Die folgenden Felder sind wichtig für die Konfiguration des SIP-DECT-Event-Managers

Nr.	Bezeichnung	ESPA-Standardbezeichnung	Bemerkungen
1	Anrufadresse	Anrufadresse	max. 16 Zeichen
2	Nachrichtentext	Nachrichtentext	max. 128 Zeichen
3	Klingelton	Piepton-Codierung	
4	Ruftyp	Typ des Anrufs	
6	Priorität	Priorität	

Bitte beachten Sie: ESPA-Nachrichten im falschen Format werden nicht verarbeitet. Unbekannte Felder werden ignoriert. Die Felder "Anrufadresse" (1) und " Nachrichtentext " (2) müssen in einem ESPA-Datensatz vorhanden sein.

Die Felder ‚Klingelton' (3), 'Ruftyp' (4) und 'Priorität' (6) haben keinen direkten Einfluss auf die Benachrichtigungen an die SIP-DECT-Telefone. Sie werden nur verwendet, um den richtigen Ereignistyp auszuwählen.

Die ESPA-Oberfläche enthält die folgenden Registerkarten:

- Allgemein
- Endpunkte
- Benutzerdefinierter Ereignistext
- Ereignis zuweisen
- Simulator/Trace

Hinweis: Die Änderungen, die auf der Registerkarte **Benutzerdefinierter Ereignistext** vorgenommen werden, werden nur wirksam, wenn das Kontrollkästchen auf der Registerkarte **Allgemein** aktiviert ist.

Registerkarte "Allgemein"

Auf der Registerkarte Allgemein können Sie die Grundeinstellungen des ESPA-Interfaces konfigurieren. Die

folgenden Einstellungen können konfiguriert werden:

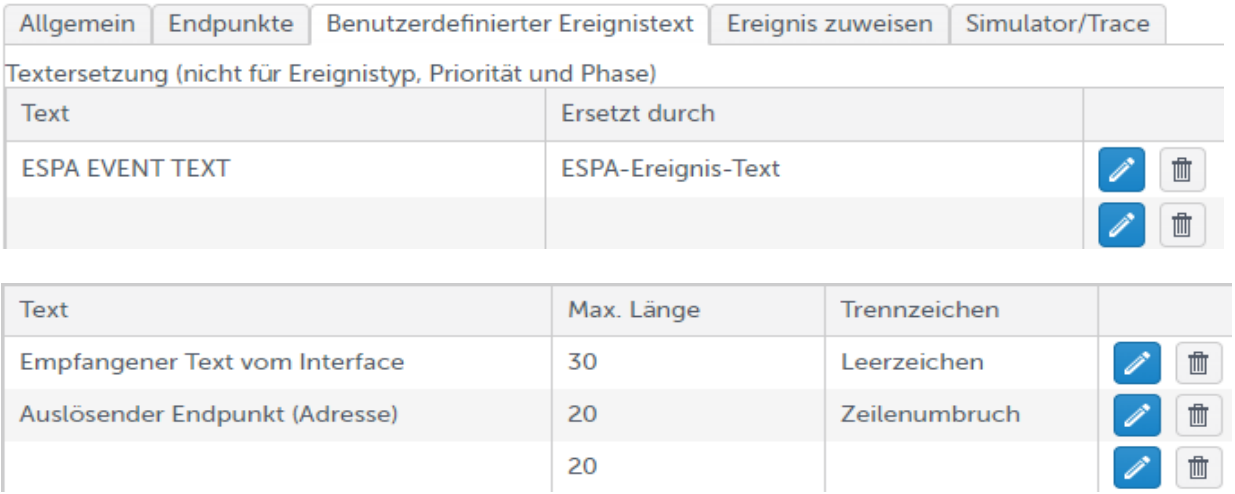
- **IP Adresse**: IP-Adresse, mit der sich der SIP-DECT-Event-Manager verbinden soll
- **IP Port**: Der IP-Port, mit dem sich der SIP-DECT-Event-Manager verbinden soll
- **Interface Überwachung**: Aktivieren Sie dieses Kontrollkästchen, wenn dieses Interface überwacht werden soll.
- **Endpunkt bestimmen durch**: Wählen Sie die Methode aus, mit der der Endpunkt bestimmt werden soll. Verfügbare Optionen sind "Ruf Adresse" (Standardeinstellung) und "Nachrichtentext".
- **Standard Ereignistyp**: Wählen Sie den Standardereignistyp aus. Hierfür muss im Abschnitt Ereignistyp ein bestimmter Ereignistyp erstellt werden. Dieser Standard-Ereignistyp wird als Fallback verwendet, wenn im Reiter Ereigniszuweisung nichts anderes definiert ist oder wenn nichts zur vorgenommenen Konfiguration passt.
- **Ruftyp 1 (Feld 4) beendet Ereignis**: Aktivieren Sie dieses Kontrollkästchen, um das Ereignis zu beenden.
- **Benutzerdefinierter Ereignistext**: Aktivieren Sie dieses Kontrollkästchen, wenn "Benutzerdefinierter Ereignistext" verwendet werden soll.

Registerkarte "Endpunkte"

Auf der Registerkarte Endpunkte können Sie Absender von ESPA-Nachrichten definieren. Die Zuordnung eines Endpunkts zu einer ESPA-Nachricht erfolgt anhand der Anrufadresse. Die Rufadresse kann über das ESPA-Feld 1 (Anrufadresse) oder über das ESPA-Feld 2 (Nachrichtentext) ermittelt werden. Wenn 'Endpunkt ermitteln durch: Meldungstext' gesetzt ist, dann darf der Meldungstext nur die Rufadresse enthalten und sonst nichts.

Registerkarte "Benutzerdefinierter Ereignistext"

Auf der Registerkarte Benutzerdefinierter Ereignistext ist es möglich, spezielle Inhalte für die Benachrichtigungen an adressierte Endpunkte (z.B. SIP-DECT Mobilteile) zu definieren. Wenn diese Funktion auf der Registerkarte Allgemein nicht aktiviert ist, wird der ESPA-Nachrichtentext (Feld 2) für die Benachrichtigung verwendet. Unter dieser Registerkarte stehen zwei Tabellen zur Verfügung, in denen eine einfache Textersetzung und/oder eine vollständige Textdefinition in Abhängigkeit von einigen bekannten Parametern möglich ist.



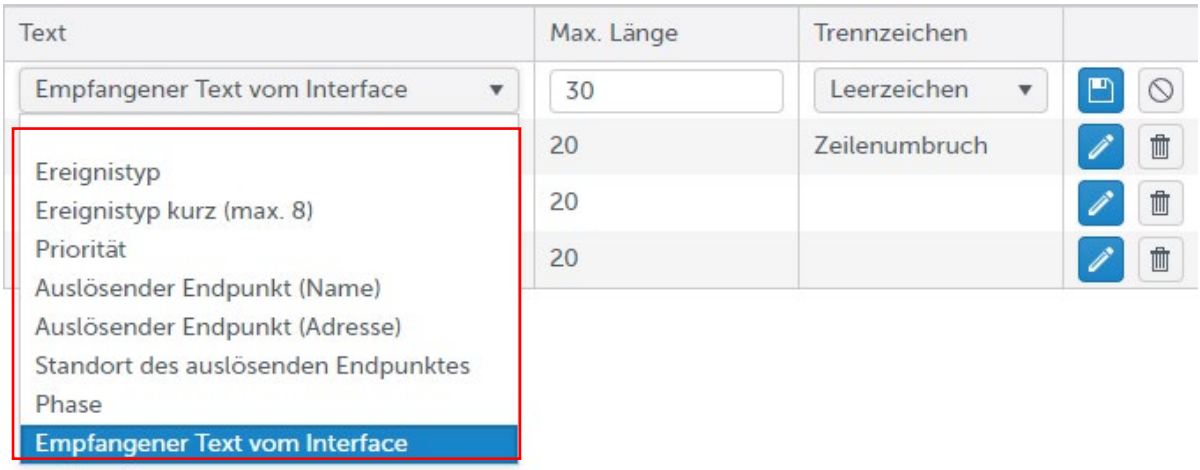
Einfaches Ersetzen von Text

In der Tabelle oben auf dieser Registerkarte kann der empfangene Text (Feld 2) aus der ESPA-Nachricht geändert werden.

Text (Feld 2) der ESPA-Meldung	Ersetzungsregel		Resultierender Benachrichtigungstext
ESPA EVENT TEXT	Text	Ersetzt durch	ESPA-Ereignis-Text
	ESPA EVENT TEXT	ESPA-Ereignis-Text	

Verfassen eines neuen Ereignistextes auf Basis einer ESPA-Nachricht

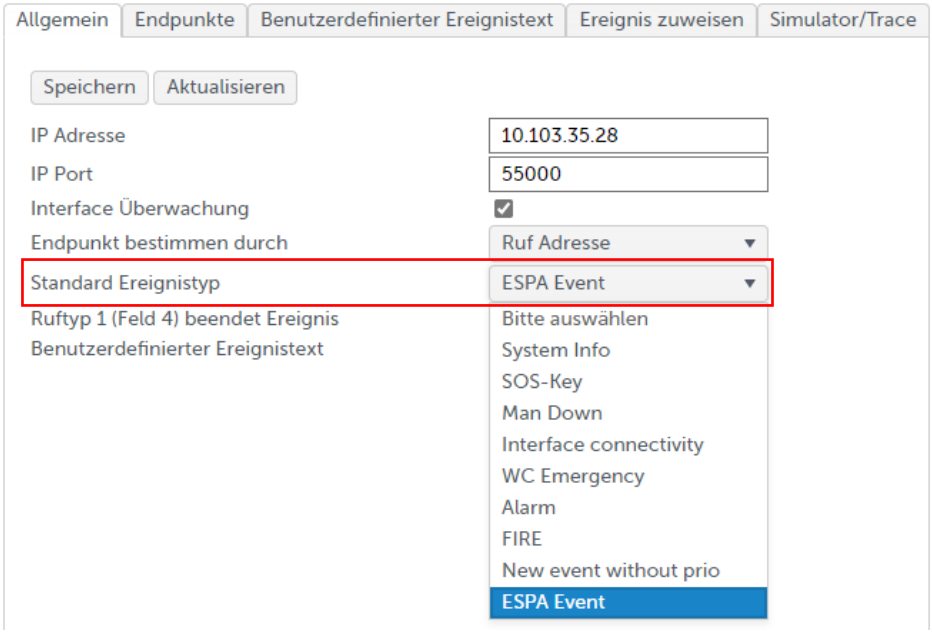
In der Tabelle am unteren Rand dieses Tabs kann der Ereignistext aus bis zu 4 Elementen neu zusammengesetzt werden. Diese 4 Elemente können aus 8 verschiedenen Ereignisinformationselementen ausgewählt werden. Diese Informationselemente werden im folgenden Beispiel gezeigt.



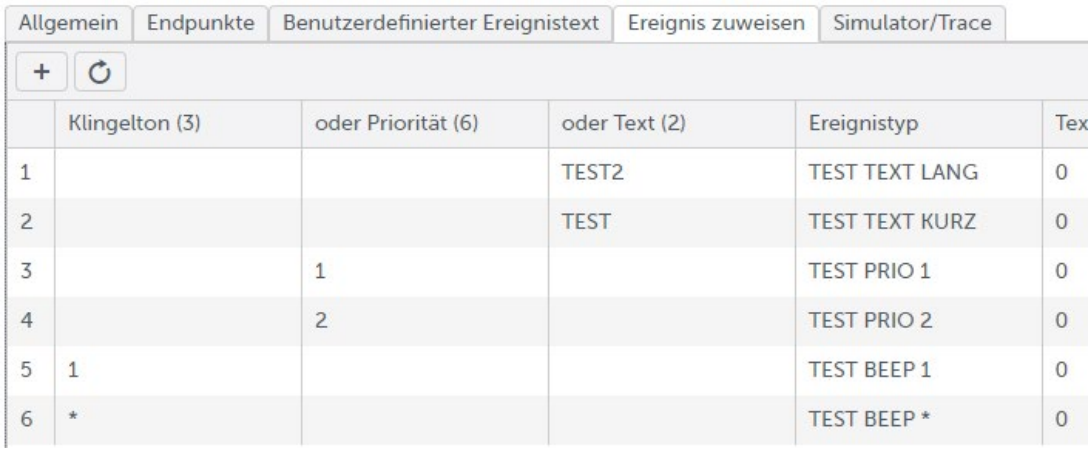
Registerkarte "Ereignis zuweisen"

Auf der Registerkarte Ereignis zuweisen können Sie den Prozess der Zuweisung bestimmter Aufgaben, Rollen oder Verantwortlichkeiten an Einzelpersonen oder Teams als Reaktion auf ein Notfallereignis definieren. Sie ist ein entscheidender Bestandteil der Koordinierung einer wirksamen Reaktion auf Notfälle.

Ein Ereignistyp wird für eingehende ESPA-Nachrichten basierend auf dem Klingelton (Feld 3), der Priorität (Feld 6) oder dem Text (Feld 2) zugewiesen. Darüber hinaus muss für nicht zugewiesen Typen auf der Registerkarte Allgemein ein Standardereignistyp eingetragen werden.



Regeln können auf der Registerkarte Ereigniszuweisung der ESPA-Interfacekonfiguration definiert werden, wie nachfolgend gezeigt.



	Klingelton (3)	oder Priorität (6)	oder Text (2)	Ereignistyp	Tex
1			TEST2	TEST TEXT LANG	0
2			TEST	TEST TEXT KURZ	0
3		1		TEST PRIO 1	0
4		2		TEST PRIO 2	0
5	1			TEST BEEP 1	0
6	*			TEST BEEP *	0

Die Regeln werden in der Reihenfolge der Erstellung angezeigt und auch in dieser Reihenfolge abgearbeitet: von oben nach unten. Die erste Abgleichsregel wird angewendet. Daher müssen die spezifischeren Regeln zuerst konfiguriert werden.

Die Felder sind mit "ODER" verknüpft, nicht mit "UND"!

Ein "*" kann als Platzhalter in den Feldern "Klingelton" und "Priorität" verwendet werden. Die Zuordnung erfolgt dann für alle Werte, die in diesen Feldern verwendet werden.

Führende oder nachfolgende Leerzeichen im Textfeld werden automatisch entfernt.

Ein Ereignis wird in der folgenden Reihenfolge gesucht:

1. Es wird nach übereinstimmenden Werten ohne Platzhalter gesucht.
2. Wenn keine Regel zutrifft, sucht das System nun nach Platzhaltern in den Feldern Klingelton und Priorität.
3. Wenn es nicht möglich ist, einen Ereignistyp zuzuordnen, wird der Standardereignistyp verwendet.

Beispielsweise ist TEST2 spezifischer als TEST. Um zu vermeiden, dass der TEST immer vor TEST2 angewendet wird, muss zuerst die TEST2-Regel wie oben gezeigt konfiguriert werden.

Die folgende Tabelle zeigt, wie diese Regeln auf einige Beispiele für die Eingabe von ESPA-Nachrichten angewendet werden.

Eingabe von ESPA-Nachrichten			**Abgleichs-Regel**			**Resultierender Ereignistyp**	**Kommentar**
Klingelton (3)	**Priorität (6)**	**Text (2)**	**Klingelton**	**Priorität**	**Text**		
Beliebig oder nicht zur Verfügung gestellt	Beliebig oder nicht zur Verfügung gestellt	TEST2			TEST2	TEST TEXT LANG	Regel 1
Beliebig oder nicht zur Verfügung gestellt	Beliebig oder nicht zur Verfügung gestellt	TEST3			TEST	TEST TEXT KURZ	Regel 2

Eingabe von ESPA-Nachrichten			Abgleichs-Regel			Resultierender Ereignistyp	Kommentar
Klingelton (3)	Priorität (6)	Text (2)	Klingelton	Priorität	Text		
1	1	Hallo!		1		TEST PRIO 1	Regel 3
1	3	Hallo!	1			TEST BEEP 1	Regel 5
Beliebig, außer 1	Beliebig (außer 1 und 3) oder nicht angegeben	Hallo!	*			TEST BEEP *	Regel 6
Nicht vorgesehen	Nicht vorgesehen	Hallo!				ESPA Event	Keine Übereinstimmung, Standardereignistyp

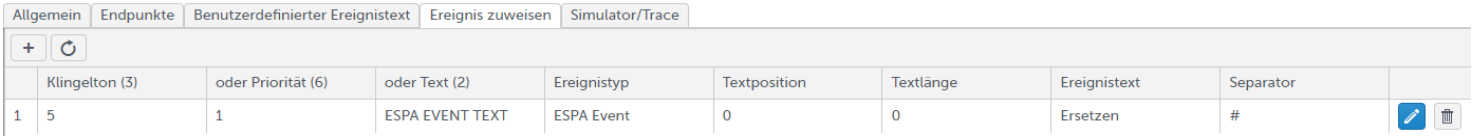
Ersetzen von Ereignistext

Normalerweise wird der Text (Feld 2) der ESPA-Nachricht als Benachrichtigungstext verwendet. Führende und nachfolgende Leerzeichen in diesem Textfeld werden nicht unterstützt und bei der Konfiguration automatisch entfernt.

Wenn ein Ereignistext definiert ist, ersetzt der Ereignistext den Inhalt des Textes (Feld 2) der ESPA-Nachricht.

Wenn eine Textposition > 0 gesetzt ist, dann wird der Text (Feld 2) der ESPA-Nachricht ab der angegebenen Position auch in den Benachrichtigungstext aufgenommen.

Wenn zusätzlich eine Textlänge eingestellt ist, dann wird nur der angegebene Teil des Textes (Feld 2) der ESPA-Nachricht auch in den Benachrichtigungstext aufgenommen.

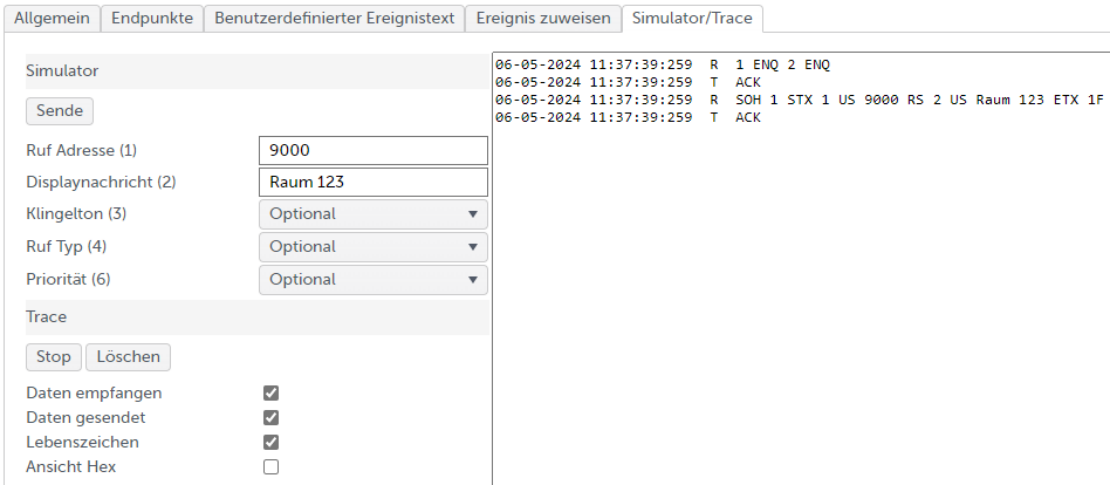


Einstellungen – Textposition, Textlänge und Ereignistext					Resultierender Benachrichtigungstext
oder Text (2)	Ereignistyp	Textposition	Textlänge	Ereignistext	Ersatz
ESPA EVENT TEXT	ESPA Event	0	0	Ersatz	
oder Text (2)	Ereignistyp	Textposition	Textlänge	Ereignistext	ESPA EVENT TEXT
ESPA EVENT TEXT	ESPA Event	0	0		
oder Text (2)	Ereignistyp	Textposition	Textlänge	Ereignistext	Zusatz - ESPA EVENT TEXT
ESPA EVENT TEXT	ESPA Event	1	0	Zusatz	
oder Text (2)	Ereignistyp	Textposition	Textlänge	Ereignistext	Zusatz - EVENT TEXT
ESPA EVENT TEXT	ESPA Event	6	0	Zusatz	

<table>
<tr><th>Einstellungen – Textposition, Textlänge und Ereignistext</th><th>Resultierender Benachrichtigungstext</th></tr>
<tr><td>
<table>
<tr><th>oder Text (2)</th><th>Ereignistyp</th><th>Textposition</th><th>Textlänge</th><th>Ereignistext</th></tr>
<tr><td>ESPA EVENT TEXT</td><td>ESPA Event</td><td>6</td><td>5</td><td>Zusatz</td></tr>
</table>
</td><td>Zusatz - EVENT</td></tr>
<tr><td>
<table>
<tr><th>oder Text (2)</th><th>Ereignistyp</th><th>Textposition</th><th>Textlänge</th><th>Ereignistext</th></tr>
<tr><td>ESPA EVENT TEXT</td><td>ESPA Event</td><td>6</td><td>5</td><td></td></tr>
</table>
</td><td>EVENT</td></tr>
</table>

Registerkarte "Simulator/Trace"

Mit der Simulator-Funktion kann überprüft werden, ob eine gesendete ESPA-Nachricht korrekt eskaliert wurde. Daher muss es nur für einen ESPA-Endpunkt mit einem Standort erstellt werden. Außerdem muss auf der Registerkarte Allgemein ein Standardereignistyp ausgewählt werden, indem eine beliebige IP-Adresse und ein beliebiger Port konfiguriert werden. Das ESPA-Interface selbst muss dazu selbst nicht laufen (Status: grün), um die Simulator-Funktion nutzen zu können.



Die Kommunikation zwischen dem SIP-DECT-Event-Manager und des ESPA-Interfaces kann bei Bedarf auf Protokollebene aufgezeichnet werden. Mit der Trace-Funktion können die von dem ESPA-Interface gesendeten und empfangenen Daten überwacht werden. Die Trace-Funktionalität kann mit der gleichen Schaltfläche gestartet und gestoppt werden.

Modbus-Interface

Die Modbus-Schnittstelle ermöglicht den Anschluss von Geräten wie z.B. WAGO oder MOXA, die über das Modbus-TCP-Protokoll Eingangsports (z.B. Taster oder Schalter) und Ausgangsports (z.B. Leuchten) zur Verfügung stellen. Das Modbus-Protokoll ist ein Client/Server-Datenprotokoll in der Anwendungsschicht des OSI-Modells, das ursprünglich 1979 von Modicon (heute Schneider Electric) für den Einsatz mit speicherprogrammierbaren Steuerungen über RS232/RS485-Schnittstellen (Modbus-RTU) veröffentlicht wurde. Für die Datenübertragung über Ethernet wurde das Protokoll zu Modbus-TCP angepasst. Inzwischen hat sich Modbus zu einem De-facto-Standard-Kommunikationsprotokoll für die Kommunikation zwischen industriellen elektronischen Geräten in einer Vielzahl von Bussen und Netzwerken entwickelt.

Das Lesen von digitalen Eingangsports und das Setzen von digitalen Ausgangsports von Modbus-TCP-Geräten wird vom Event Manager unterstützt.

Die folgenden Geräte wurden für die korrekte Interoperabilität mit dem Event Manager zugelassen:

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

Analoge Ein- und Ausgänge und andere Sensoranschlüsse werden vom Event Manager nicht unterstützt.

Hinweis: Die Funktionstüchtigkeit mit anderen Geräten kann nicht garantiert werden und muss vor der Verwendung separat geprüft werden. Die folgenden Bedingungen müssen beachtet werden.

- Nur digitale Ein-/Ausgänge werden unterstützt (keine analogen Ein-/Ausgänge oder andere Sensoren)

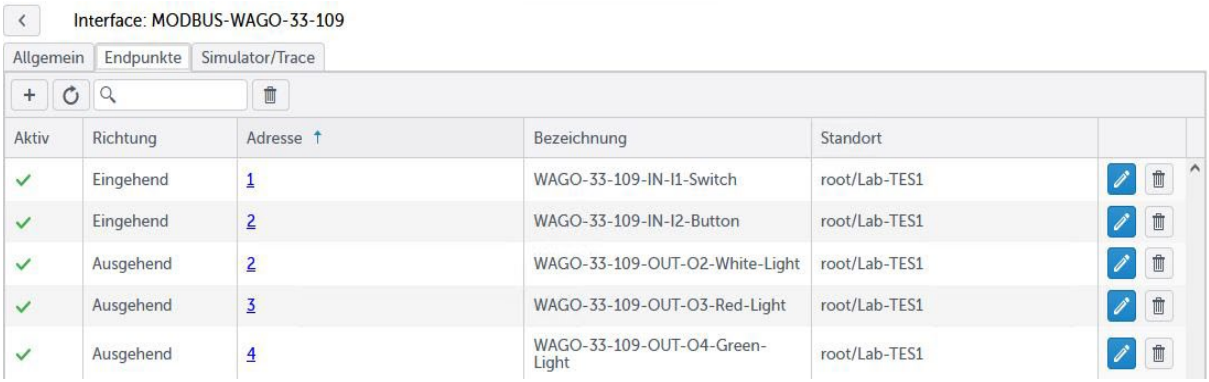
- IO-Adressen dürfen nicht durch die Gerätekonfiguration neu belegt werden, Event Manager unterstützt nur den Adressbereich ab Adresse 1 für Ein-/Ausgänge.

Registerkarte Allgemein

Die Registerkarte Allgemein wird für die Konfiguration der IP-Adresse und des Ports des Modbus-TCP-Geräts verwendet, das über die Schnittstelle angeschlossen wird.

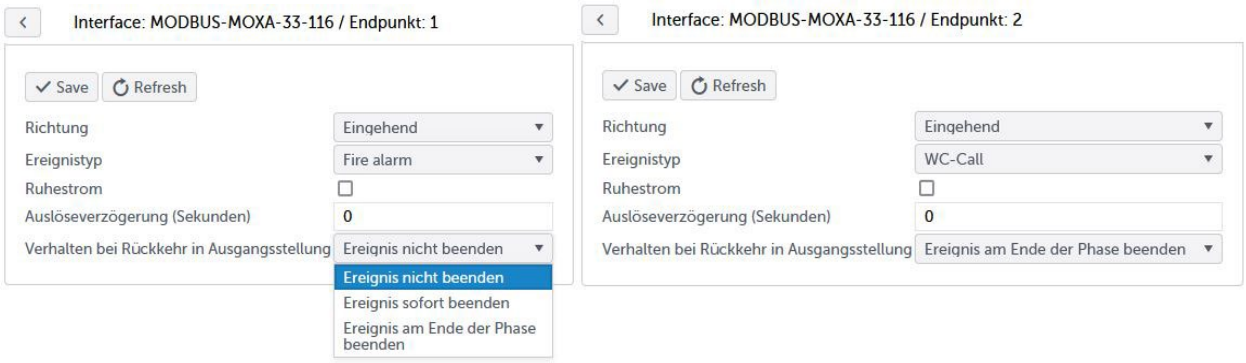
Registerkarte Endpunkte

Die Registerkarte Endpunkte wird für die Konfiguration der eingehenden und ausgehenden Endpunkte verwendet. Eingehende Endpunkte entsprechen den digitalen Eingängen von Modbus-TCP-Geräten und ausgehende Endpunkte entsprechen den digitalen Ausgängen von Modbus-TCP-Geräten. Für WAGO-Geräte sind die Eingangsports 1-256 gültige Adressen, für MOXA nur die Adressen 1-16.



In der Endpunktkonfiguration (erreichbar über den Link in der Übersicht) können einige spezielle Einstellungen für den Endpunkt konfiguriert werden. Obligatorisch sind 'Richtung' und 'Ereignistyp', optional können einige spezielle Einstellungen konfiguriert werden: 'Ruhestrom' oder 'Arbeitsstrom' wird am angeschlossenen Gerät verwendet, eine 'Alarmverzögerung in Sekunden' und das 'Verhalten bei Rückkehr in

den Normalzustand' (nicht beenden, sofort beenden oder am Ende der aktuellen Alarmphase beenden). Für ausgehende Endpunkte können keine speziellen Einstellungen konfiguriert werden.



Registerkarte Simulator/Trace

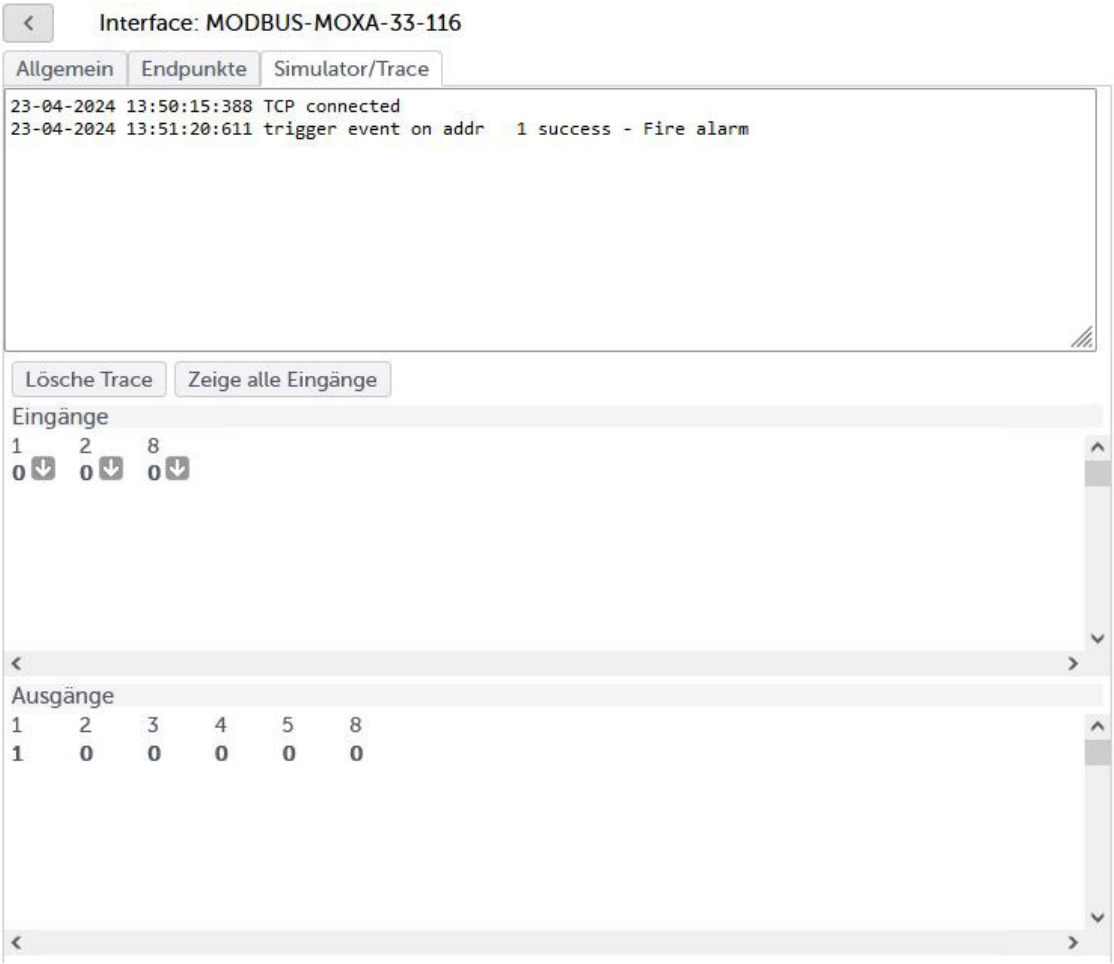
Die Registerkarte "Simulator/Trace" dient zur Simulation der Modbus-Schnittstellenendpunkte und zur Verfolgung von Änderungen an den Eingangs-/Ausgangsports. Jedes Mal, wenn die Registerkarte geöffnet wird, zeigt das Trace-Fenster TCP/IP-bezogene Verbindungsinformationen und das Simulationsfenster den aktuellen Status der konfigurierten Ports an. Durch Drücken der Schaltfläche "Alle Eingänge anzeigen" wird der Status aller Eingänge zwischen Adresse 1 und der höchsten konfigurierten eingehenden Endpunktadresse angezeigt. Es wird nicht empfohlen, mehr als ein Browserfenster mit aktiver Simulator/Trace-Registerkarte zu öffnen. Es wird nur eine Sitzung vom System verarbeitet.

Für konfigurierte eingehende Endpunkte wird neben jedem Eingangsstatus eine kleine Schaltfläche angezeigt. Wenn diese Schaltfläche gedrückt wird, wird das für diesen Endpunkt konfigurierte Ereignis erzeugt und mit dem definierten Ereignisplan verarbeitet,

Bitte beachten Sie, dass die konfigurierten Endpunktattribute "Alarmverzögerung", "Ruhestrom" und "Verhalten bei Rückkehr in den Normalzustand" nicht gelten, wenn diese Schaltfläche gedrückt wird; das konfigurierte Ereignis wird sofort generiert. Bei Bedarf kann der ausgeführte Ereignisplan über die Sektion Monitor im Web-Frontend des Event Managers abgebrochen werden.

Im Teil "Ausgänge" der Registerkarte "Simulator/Trace" ist die Aktivität am Ausgangsanschluss 1 (in diesem Beispiel ist ein Licht angeschlossen) sichtbar, und im Teil "Trace" der Registerkarte wird das behandelte Triggerereignis am Eingangsanschluss 1 (ausgelöst durch den physisch an diesen Anschluss angeschlossenen Schalter oder durch Drücken der Taste 1 im Teil "Eingänge") dokumentiert.

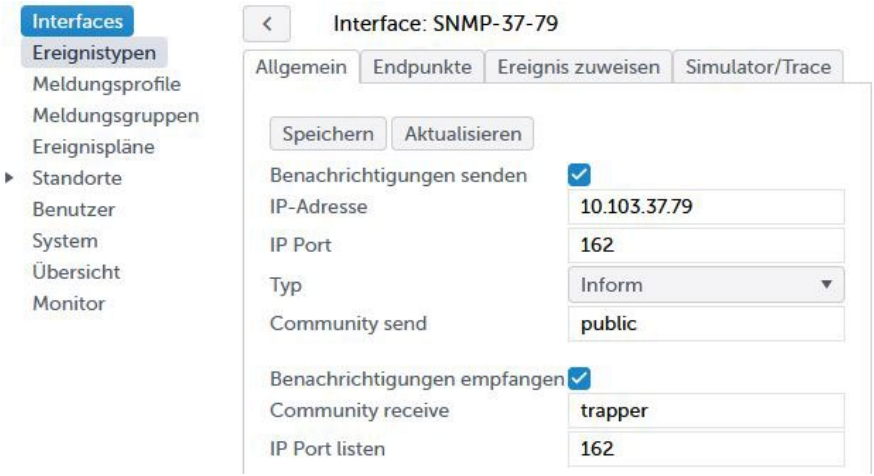
Für die Simulation der Modbus-Schnittstelle ohne Verbindung zu einem physikalischen Gerät kann die Schnittstelle mit der lokalen Host-IP-Adresse (127.0.0.1) konfiguriert werden.



SNMP-Interface

Allgemeine Informationen

Die SNMP-Schnittstelle ermöglicht dem Event Manager das Senden und Empfangen von SNMP-Benachrichtigungen an und von konfigurierten IP-Adressen mit korrekten Community-Strings. Sowohl gesendete als auch empfangene Benachrichtigungen können Traps oder Inform-Requests sein. Nur SNMP v2c wird für das Senden von Benachrichtigungen unterstützt, während SNMP v1 und SNMP v2c für den Empfang von Benachrichtigungen unterstützt wird.

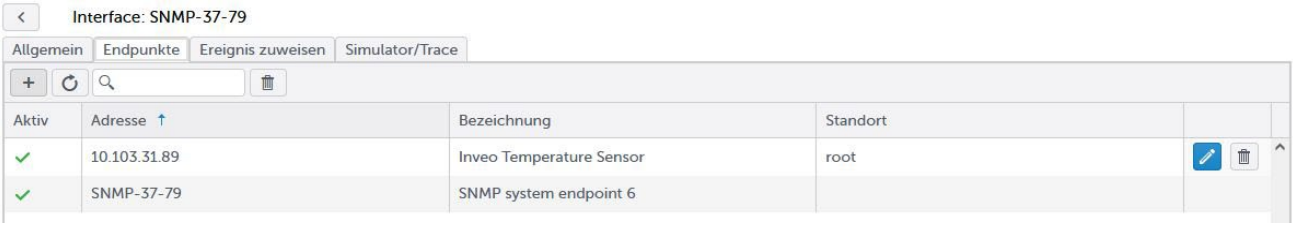


SNMP Notifikationen

Um Benachrichtigungen senden zu können, müssen "IP-Adresse", "IP-Port", "Typ" und "Community senden" korrekt konfiguriert sein. Soll die gewählte SNMP-Schnittstelle nur Benachrichtigungen senden, können Sie das Häkchen bei "Benachrichtigungsempfang" entfernen.

"IP-Adresse" und "IP-Port" bestimmen, wohin eine Benachrichtigung gesendet Mit "Typ" wird festgelegt, ob die Schnittstelle Traps oder Inform-Requests senden soll. Traps sind Benachrichtigungen, die einmalig gesendet werden, ohne dass der Event Manager überprüft, ob der konfigurierte Empfänger sie erhalten hat. Bei Inform-Requests hingegen wartet der Event Manager auf eine korrekte Get-Response vom Ziel. Sollte nach 5 Sekunden keine korrekte Get-Response empfangen worden sein, wird der Inform-Request erneut gesendet. Der Event Manager sendet einen Inform-Request nur einmal (also insgesamt zweimal), bevor er die Zeit verlässt.

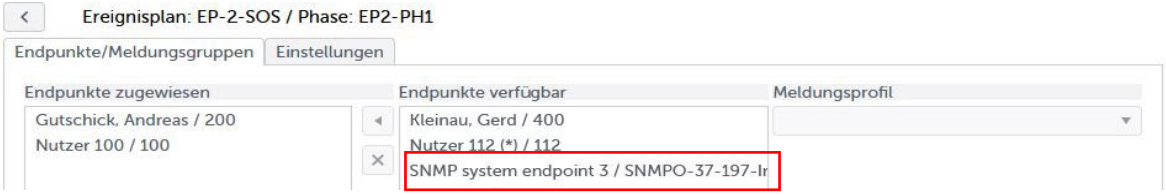
"Community send" legt die Community-Zeichenfolge für gesendete Benachrichtigungen fest. Dieser Community-String muss mit dem Community-String übereinstimmen, den der konfigurierte Empfänger konfiguriert hat. Andernfalls wird der Empfänger unsere gesendete Benachrichtigung nicht verarbeiten.



Sobald eine SNMP-Schnittstelle hinzugefügt wurde, wird automatisch ein entsprechender Endpunkt erstellt.

Dieser Endpunkt zählt zur Anzahl der lizenzierten Endpunkte, solange das Kontrollkästchen "Benachrichtigung senden" in der SNMP-Schnittstelle aktiviert bleibt. Dieser Endpunkt kann in keiner Weise bearbeitet oder gelöscht werden und kann keinem Standort zugewiesen werden.

Um der SNMP-Schnittstelle die Möglichkeit zu geben, Benachrichtigungen zu senden, müssen Sie diesen Systemendpunkt wie jeden anderen Benachrichtigungsendpunkt in die Phase eines Ereignisplans einfügen. Sobald diese Phase aktiviert ist, sendet die entsprechende SNMP-Schnittstelle eine entsprechende Benachrichtigung an den konfigurierten Empfänger.



Interface Status Änderungen

Wird der Ereignisplan durch den vordefinierten Ereignistyp "System Info" ausgelöst, enthält die Benachrichtigung Daten über die auslösende Schnittstelle und deren aktuellen Status. Ein "System Info"-Ereignis wird von jeder Schnittstelle ausgelöst, wenn sich ihr Status ändert. Dieses Ereignis wird immer an der Stelle "root" ausgelöst. Wenn eine SNMP-Schnittstelle Benachrichtigungen über Statusänderungen der Schnittstelle senden soll, sollte ein Ereignisplan, der das vordefinierte Ereignis "System Info" behandelt, an diesem Ort mit einer Phase konfiguriert werden, die den SNMP-Systemendpunkt als zugewiesenen Endpunkt enthält. Das Ändern des Ereignistyps "System Info" hat keinen Einfluss auf diese Funktionalität.

Notifikationsname	Datenfeldname	Object Identifier (OID)	Kommentar
interfaceStatusChange	---	.1.3.6.1.4.1.1027.4.1.1337.0.4	die Trap OID
	interfaceType	.1.3.6.1.4.1.1027.4.1.1337.1.1.3.1.4	Der Interface Typ
	interfaceLabel	.1.3.6.1.4.1.1027.4.1.1337.1.1.3.1.2	Der Interface Name
	interfaceState	.1.3.6.1.4.1.1027.4.1.1337.1.1.3.1.6	Der Status, welcher das Interface angenommen hat
	InterfaceDescription	.1.3.6.1.4.1.1027.4.1.1337.1.1.3.1.3	Beschreibung des Interfaces

Ereignisplanverarbeitung

Wenn eine Phase mit einem SNMP-Endpunkt aktiviert wird, sendet die entsprechende SNMP-Schnittstelle eine Benachrichtigung an das konfigurierte Ziel. Diese Benachrichtigung enthält eine Benachrichtigungs-ID, den Ereignistext, Daten über den Auslöser des Plans und Informationen über den ausgelösten Plan und die Phase. Sobald die Phase auf irgendeine Weise beendet wurde, wird eine Benachrichtigung mit der entsprechenden Benachrichtigungs-ID an das Ziel gesendet, um dieses über das Ende der Phase zu informieren. Dieser Trap enthält nicht den Grund für die Beendigung des Ereignisplans. Die derzeitige Implementierung wird zur Evaluierung von Anwendungsfällen angeboten. Dementsprechend kann diese Funktionalität weiterentwickelt werden und in zukünftigen Software-Updates technischen Änderungen unterliegen.

Notifikationsname	Datenfeldname	Object Identifier (OID)	Kommentar
activateEventPhase	---	.1.3.6.1.4.1.1027.4.1.1337.0.5	Exakt gleiche Felder wie deactivateEventPhase
deactivateEventPhase	---	.1.3.6.1.4.1.1027.4.1.1337.0.6	Exakt gleiche Felder wie activateEventPhase
	trapEventID	.1.3.6.1.4.1.1027.4.1.1337.0.3.1	Diese ID ist gleich in zusammengehörigen Aktivierungs-

Notifikationsname	Datenfeldname	Object Identifier (OID)	Kommentar
			und Deaktivierungs-notifikationen
	trapEventText	.1.3.6.1.4.1.1027.4.1.1337.0.3.2	Der Eventtext
	locationLabel	.1.3.6.1.4.1.1027.4.1.1337.2.1.3.1.2	Standort, wo der Ereignisplan ausgelöst wurde
	endpointLabel	.1.3.6.1.4.1.1027.4.1.1337.4.1.3.1.5	Name des Endpunkts, welcher das Ereignis ausgelöst hat
	endpointCallNumber	.1.3.6.1.4.1.1027.4.1.1337.4.1.3.1.3	Rufnummer des Endpunkts, welcher das Ereignis ausgelöst hat
	eventTypeLabel	.1.3.6.1.4.1.1027.4.1.1337.3.1.3.1.2	Name des Ereignistypen
	eventPlanLabel	.1.3.6.1.4.1.1027.4.1.1337.6.1.3.1.2	Name des Ereignisplans
	phaseLabel	.1.3.6.1.4.1.1027.4.1.1337.6.1.4.1.3.1.2	Name der Phase
	phaseDuration	.1.3.6.1.4.1.1027.4.1.1337.6.1.4.1.3.1.6	Dauer der Phase in Sekunden

coldStart Benachrichtigung

Sobald eine SNMP-Schnittstelle korrekt konfiguriert ist, sendet sie eine coldStart-Benachrichtigung an ihr konfiguriertes Ziel. Diese Benachrichtigung wird jedes Mal gesendet, wenn die SNMP-Schnittstelle so geändert wird, dass sie korrekt funktioniert, oder wenn sie aktiviert wird, nachdem sie zuvor ausgeschaltet war. Diese Benachrichtigung wird auch gesendet, wenn der Event-Manager gestartet oder neu gebootet wird, sofern die Schnittstelle korrekt konfiguriert ist. Diese coldStart-Benachrichtigungen machen die Schnittstelle für SNMP-Management-Systeme sichtbar. Sie sollen den Empfänger jedoch nur darüber informieren, dass die SNMP-Schnittstelle selbst korrekt konfiguriert und bereit ist, Benachrichtigungen zu senden. Sie liefern keine konkreten Informationen über den Zustand des Event-Managers selbst oder anderer Schnittstellen. Außerdem sendet der Event-Manager keine warmStart-Benachrichtigungen, auch wenn sich die Konfiguration der Schnittstelle nicht geändert hat.

Zusätzliche Meldungselemente

Jede Meldung enthält neben ihrer definierten auch in der MIB nicht definierte Datenfelder. Diese enthalten Informationen über die EVM selbst oder Daten, die zu spezifisch für den allgemeineren Benachrichtigungstyp sind. Sie werden nach den definierten MIB-Datenfeldern angehängt.

Notifikationsname	Datenfeldname	Object Identifier (OID)	Kommentar
Zusätzliche Felder	---	---	Datenfelder, welche nach den MIB definierten Datenfeldern, an Notifikationen angehangen werden
	espaDestinationIP	.1.3.6.1.4.1.1027.4.1.1337.1.3.1.1.1	für interfaceStatusChange, IP-Adresse wohin sich das ESPA-Interface versucht zu verbinden
	espaDestinationPort	.1.3.6.1.4.1.1027.4.1.1337.1.3.1.1.2	für interfaceStatusChange, Port wohin sich das ESPA-Interface versucht zu verbinden
	modbusDestinationIP	.1.3.6.1.4.1.1027.4.1.1337.1.5.1.1.1	für interfaceStatusChange, IP-Adresse wohin sich das MODBUS-Interface versucht zu verbinden
	modbusDestinationPort	.1.3.6.1.4.1.1027.4.1.1337.1.5.1.1.2	für interfaceStatusChange, Port wohin sich das MODBUS-Interface versucht zu verbinden
	sipdectOMM1	.1.3.6.1.4.1.1027.4.1.1337.1.2.1.1.1	für interfaceStatusChange, Die IP-Adresse des ersten OMMs

Notifikationsname	Datenfeldname	Object Identifier (OID)	Kommentar
	sipdectOMM2	.1.3.6.1.4.1.1027.4.1.1337.1.2.1.1.2	für interfaceStatusChange, Die IP-Adresse des zweiten OMMs
	snmpDestinationIP	.1.3.6.1.4.1.1027.4.1.1337.1.4.1.1.1	für interfaceStatusChange, IP-Adresse wohin das SNMP-Interface versucht Notifikationen zu senden
	snmpDestinationPort	.1.3.6.1.4.1.1027.4.1.1337.1.4.1.1.2	für interfaceStatusChange, Port wohin das SNMP-Interface versucht Notifikationen zu senden
	sysName	.1.3.6.1.2.1.1.3	Angehängt an alle Notifikationen, Name des Event-Managers
	systemIPAddress	.1.3.6.1.4.1.1027.4.1.1337.10.3	Angehängt an alle Notifikationen, IP-Adresse des Event-Managers
	systemMACAddress	.1.3.6.1.4.1.1027.4.1.1337.10.4	Angehängt an alle Notifikationen, MAC-Adresse des Event-Managers
	systemVersion	.1.3.6.1.4.1.1027.4.1.1337.10.2	Angehängt an alle Notifikationen, Versionsnummer des Event-Managers
	snmpTrapEnterprise	.1.3.6.1.6.3.1.1.4.3	Immer das letzte Datenfeld, enthält MITELs Enterprise OID

Management Information Base

Um die Meldungen und ihre Datenfelder richtig interpretieren zu können, werden zwei MIB-Dateien mit dem Event Manager mitgeliefert. Die erste Management Information Base (MIB) ist die Stamm-MIB-Datei von MITEL (MITEL-MIB.mib). Sie ist notwendig, damit die zweite MIB, die MITEL-EVM-MIB.mib, funktioniert. Beide „.mib“-Dateien zusammen enthalten alle proprietären Informationen, die ein SNMP-Agent benötigt, um die spezifischen Daten und Benachrichtigungen des Event Managers korrekt zu interpretieren.

Andere per RFC definierte MIB-Dateien, die der Event Manager verwendet, sind SNMPv2-SMI (RFC 2578), SNMPv2-TC (RFC 2579), SNMPv2-CONF (RFC-2580) und SNMPv2-MIB (RFC 3418).

Empfang von Benachrichtigungen

Um SNMP-Benachrichtigungen zu empfangen und zu verarbeiten, muss "Benachrichtigung empfangen" aktiviert und die Felder "Community empfangen" und "IP-Port abhören" konfiguriert werden. Soll diese Schnittstelle nur Benachrichtigungen empfangen, kann "Benachrichtigungen senden" deaktiviert werden.

Mit "Community receive" wird der Community-String konfiguriert, den alle empfangenen Benachrichtigungen haben müssen, um verarbeitet werden zu können. Bei falschem Community-String ignoriert der Event Manager die zugehörige Benachrichtigung und es findet keine weitere Verarbeitung statt.

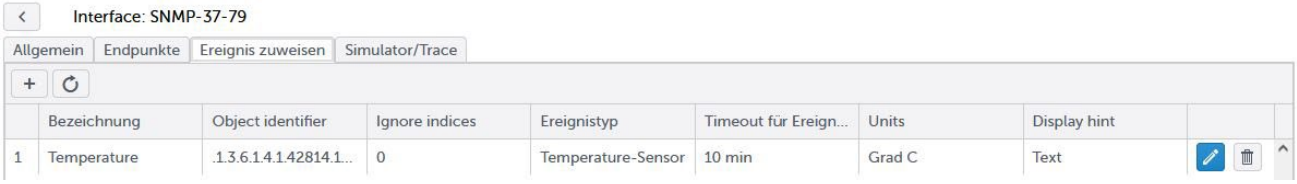
"IP port listen" ist der Port, auf dem diese SNMP-Schnittstelle auf Traps/Inform-Requests lauscht. Sollte die SNMP-Schnittstelle aus irgendeinem Grund nicht in der Lage sein, diesen Port zu öffnen, wird ihr Status auf "Inaktiv" (rot) geändert. In diesem Fall wählen Sie bitte einen anderen Listening Port! Beachten Sie, dass zwei verschiedene SNMP-Schnittstellen nicht denselben Listening Port verwenden dürfen!

Der Event Manager verarbeitet empfangene Benachrichtigungen (Traps und Inform-Requests), um Ereignisse auszulösen. Empfangene Inform-Requests werden mit korrekten Get-Responses beantwortet, empfangene Traps werden nicht beantwortet, sondern nur verarbeitet. Alle anderen Arten von Anfragen oder PDUs werden ignoriert, lösen kein Ereignis aus und werden nicht beantwortet.

Damit Meldungen zu Ereignissen verarbeitet werden können, muss ein Empfangsendpunkt konfiguriert sein. Es werden nur Benachrichtigungen von konfigurierten und aktiven Endpunkten verarbeitet. Das Feld „Adresse“ enthält die IP-Adresse des SNMP-Benachrichtigungsabsenders, von dem Sie Benachrichtigungen

verarbeiten möchten. Eingehende Benachrichtigungen, die nicht von einem konfigurierten Endpunkt stammen, werden nicht zu einem Ereignis verarbeitet.

Wenn eine Benachrichtigung von einem konfigurierten und aktiven Endpunkt mit einer korrekten Community-Zeichenfolge empfangen wird, wird ein Ereignis am zugewiesenen Standort des Endpunkts ausgelöst. Der ausgelöste Ereignistyp wird durch die erste passende Ereigniszuweisung bestimmt. Sollte keine gültige Ereigniszuweisung gefunden werden, wird kein Ereignis ausgelöst.



Feldname	Erläuterung
Nr.	Die Reihenfolge, in der die Ereigniszuweisungen erstellt wurden, wobei die niedrigste Nummer die früheste ist. Die erste passende Ereigniszuweisung löst das entsprechende Ereignis aus, beginnend mit der niedrigsten Nummer.
Label	Der Name dieser Ereigniszuweisung.
Object Identifier	Der Objektidentifikator (OID), dem diese Ereigniszuweisung entspricht. Enthält eine empfangene SNMP-Benachrichtigung ein Feld mit genau dieser OID oder ist ihr zweites Feld snmpTrapOID (definiert: SNMPv2-MIB) und enthält genau diese OID als Wert, wird diese Ereigniszuweisung gewählt und das entsprechende Ereignis am Standort des empfangenden Endpunkts ausgelöst.
Ignore Indices	Die Anzahl der OID-Indizes vom Ende (rechts), die bei den Objektbezeichnern der eingehenden Benachrichtigung ignoriert werden. Die gekürzte empfangene OID muss immer noch genau mit der konfigurierten OID im Feld „Object Identifier“ übereinstimmen.
Ereignistyp	Der Ereignistyp, der ausgelöst werden soll, wenn diese Ereigniszuordnung ausgewählt wird.
Timeout bis zum Neuauslösen des Ereignisses	Die Zeitspanne, in der ein Ereignis NICHT erneut von demselben Endpunkt ausgelöst wird, wenn diese Ereigniszuweisung gewählt wird. Dies ist besonders nützlich, wenn ein SNMP-Benachrichtigungssender zu viele SNMP-Benachrichtigungen in einer kurzen Zeitspanne sendet. Alle Timeouts werden zurückgesetzt, wenn die entsprechende Schnittstelle deaktiviert, aktiviert oder in irgendeiner Weise verändert wird.
Units	Ein kurzer Text, der an die interpretierten Daten der definierten OIDs angehängt wird. Entspricht der UNITS-Klausel in MIB-Definitionen.
Display-Hint	Wählen Sie aus, wie der definierte OIDs-Wert im generierten Ereignistext angezeigt werden soll. Werte, die zu unbrauchbaren Ergebnissen führen würden, werden bei der Erzeugung des Ereignistextes verworfen. Entspricht der DISPLAY-HINT-Klausel in MIB-Definitionen, wurde aber zu einem Dropdown-Menü vereinfacht. Es wird empfohlen, diese Option auf "Automatisch" zu belassen, es sei denn, Sie sind sich 100%ig sicher, welchen Wert Sie nach dieser OID erhalten werden. "Text" = 'a'; "Dezimal" = 'd'; "Dezimal mit Nachkommastellen: X" = 'd-X'

Eine gültige Ereigniszuweisung wird ermittelt, indem versucht wird, die konfigurierte OID mit allen empfangenen OIDs sowie mit der OID im vordefinierten snmpTrapOID-Wertfeld abzugleichen. Dies ist das zweite Feld in jeder SNMP v2c-Nachricht mit der OID „.1.3.6.1.6.3.1.1.4.1(.0)“. Die erste übereinstimmende Ereigniszuweisung bestimmt das ausgelöste Ereignis, und der Wert der ersten übereinstimmenden OID in der

empfangenen Benachrichtigung wird im Ereignistext angezeigt.

Der Ereignistext enthält den ausgelösten Ereignistyp, den auslösenden Endpunkt und dessen Adresse, die Bezeichnung der gewählten Ereigniszuweisung und den interpretierten Wert hinter dem "Object Identifier"-Feld der Ereigniszuweisung entsprechend dem "Display-Hint"-Feld, wobei das "Units"-Feld einfach angehängt wird.

Handelt es sich bei dem Feld "Object Identifier" um eine snmpTrapOID, wird im Ereignistext angegeben, dass es sich bei dem empfangenen Wert um einen "TRAP TYPE" und nicht um den interpretierten Wert handelt.

Es folgen einige Beispiele für die Auswahl der Ereigniszuweisungen, um sie besser zu veranschaulichen.

Received OIDs	Received values	Event assignment	What gets checked *)	Final result
.1.3.6.1.2.1.1.3.0 .1.3.6.1.6.3.1.1.4.1.0 .7.6.4.12.5.9.8.8	37652723 .1.3.6.1.4.5.5.2.4 “Example Text”	OID: .1.3.6.1.2.1.1.3 Ignore indices: 0	.1.3.6.1.2.1.1.3.0 .1.3.6.1.6.3.1.1.4.1.0 .1.3.6.1.4.5.5.2.4 .7.6.4.12.5.9.8.8	• No exact match • No event trigger • The next event assignment will be tried
.1.3.6.1.2.1.1.3.0 .1.3.6.1.6.3.1.1.4.1.0 .7.6.4.12.5.9.8.8	37652723 .1.3.6.1.4.5.5.2.4 “Example Text”	OID: .1.3.6.1.2.1.1.3 Ignore indices: 1	**.1.3.6.1.2.1.1.3**.0 .1.3.6.1.6.3.1.1.4.1.0 .1.3.6.1.4.5.5.2.4 .7.6.4.12.5.9.8.8	• Exact match because 1 index ignored • Event trigger!
.1.3.6.1.2.1.1.3.0 .1.3.6.1.6.3.1.1.4.1.0 .7.6.4.12.5.9.8.8	37652723 .1.3.6.1.4.5.5.2.4 “Example Text”	OID: .1.3.6.1.2.1.1.3 Ignore indices: 2	.1.3.6.1.2.1.1.3.0 .1.3.6.1.6.3.1.1.4.1.0 .1.3.6.1.4.5.5.2.4 .7.6.4.12.5.9.8.8	• No exact match • No event trigger • The next event assignment will be tried
.1.3.6.1.2.1.1.3.0 .1.3.6.1.6.3.1.1.4.1.0 .7.6.4.12.5.9.8.8	37652723 .1.3.6.1.4.5.5.2.4 “Example Text”	OID: .7.6.4.12.5.9.8.8 Ignore indices: 0	.1.3.6.1.2.1.1.3.0 .1.3.6.1.6.3.1.1.4.1.0 .1.3.6.1.4.5.5.2.4 **.7.6.4.12.5.9.8.8**	• Exact match • Event trigger!
.1.3.6.1.2.1.1.3.0 .1.3.6.1.6.3.1.1.4.1.0 .7.6.4.12.5.9.8.8 .1.3.6.1.2.1.1.4.0	37652723 .1.3.6.1.4.5.5.2.4 “Example Text” 50	OID: .1.3.6.1.2.1.1 Ignore indices: 2	**.1.3.6.1.2.1.1**.3.0 .1.3.6.1.6.3.1.1.4.1.0 .1.3.6.1.4.5.5.2.4 .7.6.4.12.5.9.8.8 .1.3.6.1.2.1.1.4.0	• Exact match • The first matching OID’s value will be used for the event text • Event trigger

*) Die roten Zahlen innerhalb der empfangenen OIDs werden mit der Ereigniszuweisungs-OID abgeglichen. Schwarze Zahlen innerhalb der empfangenen OIDs werden beim Abgleich mit der Ereigniszuweisungs-OID ignoriert. Unterstrichene OIDs werden mit der Ereigniszuweisungs-OID abgeglichen. Die fett unterstrichenen OIDs werden für den Ereignistext verwendet.

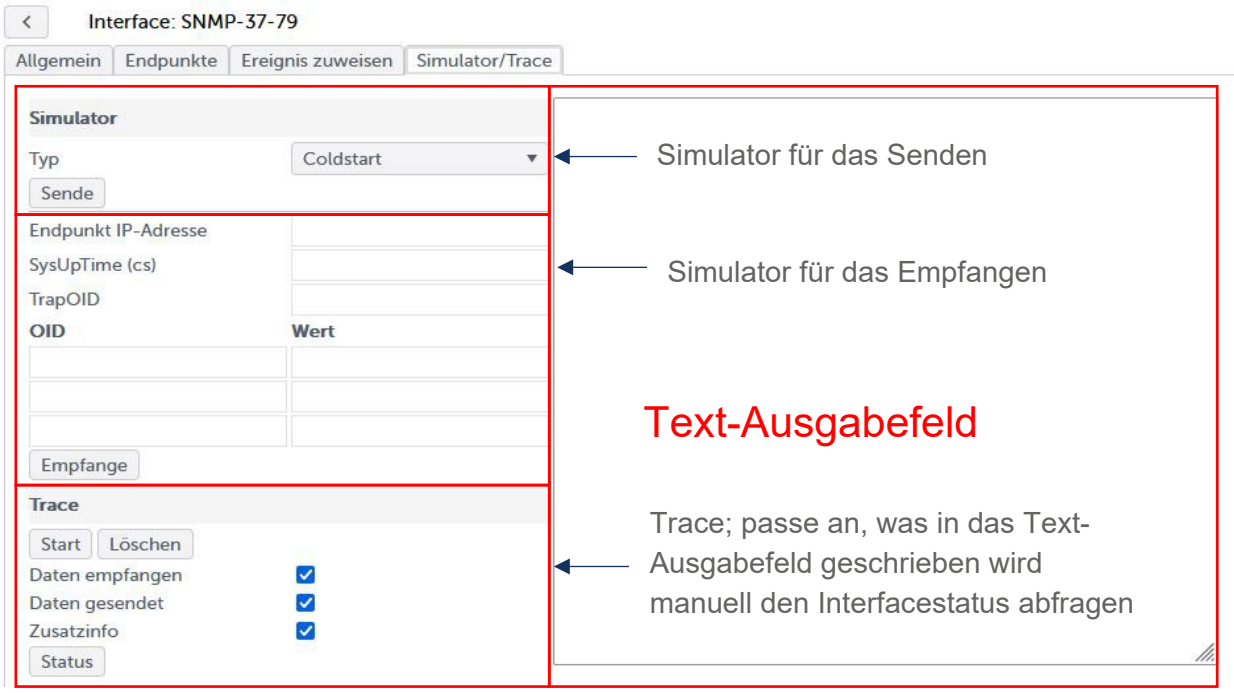
Simulator/Trace

Auf der Registerkarte Simulator/Trace können Sie den Empfang und das Senden von Traps simulieren.

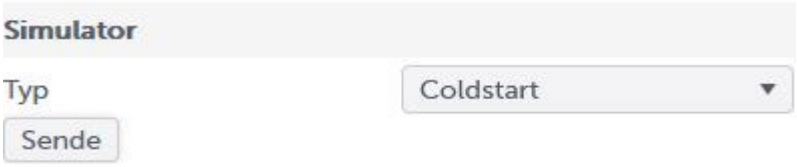
Trace wird verwendet, um anzuzeigen, was die SNMP-Schnittstelle sendet und empfängt, sowie andere Informationen zu internen Aktivitäten. „Start“ startet die Trace-Ausgabe und wird durch ‚Stop‘ ersetzt, was wiederum die Trace-Ausgabe stoppt. Mit „Clear“ wird die gesamte Trace-Ausgabe gelöscht. Mit „Status“ wird

der Status dieser SNMP-Schnittstelle in das Textausgabefeld gedruckt. Die Checkboxen „Data received“, „Data sent“ und „Additional info“ bestimmen, welche Informationen automatisch in das Textausgabefeld gedruckt werden, wenn der Trace gestartet wurde. „Data received“ ermöglicht die Anzeige von empfangenen Traps und den dazugehörigen Informationen, ‚Data sent‘ ermöglicht die Anzeige von gesendeten Traps und den dazugehörigen Informationen und ‚Additional info‘ ermöglicht die Anzeige von Informationen darüber, wie die Daten verarbeitet wurden und was das Ergebnis war. Fehlermeldungen werden immer gedruckt, unabhängig davon, welche Kontrollkästchen aktiviert oder deaktiviert sind, solange der Trace gestartet wurde.

Mit dem Simulator können Sie die SNMP-Schnittstelle zwingen, vordefinierte Traps mit der Schnittstellenkonfiguration zu senden, und Sie können testen, was passiert, wenn die SNMP-Schnittstelle einen anpassbaren Trap empfängt.

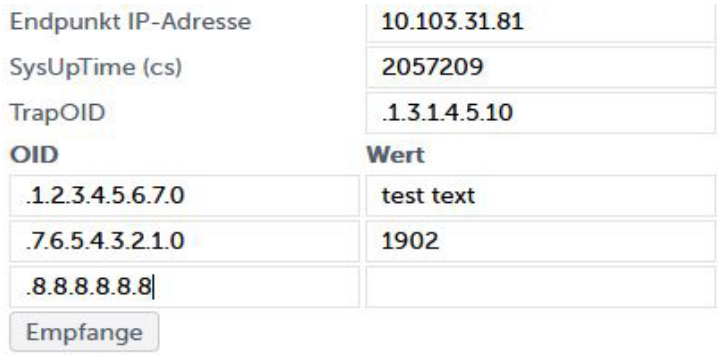


Um einen vordefinierten Trap zu senden, wählen Sie den Typ des Traps aus, den die Schnittstelle senden soll, und drücken Sie dann die Schaltfläche "Senden". Der Event Manager wird dann diesen Trap-Typ entsprechend seiner eigenen Konfiguration senden. Gegenwärtig sendet der Event Manager nur Traps für ColdStart, ereignisbezogene Traps und Statusänderungen.



Um zu sehen, was der Event Manager sendet, starten Sie den Trace und überprüfen Sie "Data sent". Dies ist nützlich, um festzustellen, ob diese SNMP-Schnittstelle korrekt für das Senden von Traps konfiguriert ist, und um zu prüfen, ob der Trap-Empfänger außerhalb des Event Managers Traps korrekt verarbeitet. Die vom Simulator gesendeten Daten haben das korrekte Format, aber die Daten selbst können korrekt sein oder auch nicht.

Der Simulator kann auch dazu verwendet werden, den Empfang eines Traps zu simulieren, um zu testen, ob die "Ereigniszuordnung" und die "Endpunkte" korrekt vorgenommen wurden.



Zunächst müssen Sie eine IP-Adresse eingeben, von der aus der Trap angeblich gesendet wurde.

Zweitens benötigen die obligatorischen SNMP-Felder "SysUpTime" und "snmpTrapOID" einen gültigen Zehntelsekundenwert bzw. eine korrekt formatierte OID. Die OIDs müssen nicht real oder MIB-definiert sein.

Schließlich können Sie dem simulierten Trap bis zu 3 zusätzliche OID-Wertepaare hinzufügen. Schreiben Sie einfach eine reale oder imaginäre OID in die linke Spalte und einen entsprechenden Wert in die rechte Spalte.

Wenn Sie auf die Schaltfläche "Empfangen" klicken, generiert diese Schnittstelle einen Trap mit den angegebenen Werten (wenn möglich) und sendet ihn an sich selbst. Um diesen generierten Trap zu sehen, starten Sie den Trace und aktivieren Sie "Daten empfangen". Im Ausgabefenster wird der generierte Trap sowie das Ergebnis der Verarbeitung dieses Traps angezeigt. Damit tatsächlich ein Ereignis ausgelöst wird, muss ein Ereignisplan für den richtigen Standort vorhanden sein.

MQTT-Interface

Die MQTT-Schnittstelle verbindet den Event Manager mit einem MQTT-Broker. Die Schnittstelle ermöglicht das Abonnieren von benutzerdefinierten Themen beim MQTT-Broker, um Nachrichten von IoT-Geräten zu empfangen, die ihre Ereignisse an diesen Broker veröffentlichen. Der Event Manager verarbeitet die vom MQTT-Broker empfangenen MQTT-Nachrichten und löst Ereignisse aus, wenn in der Konfiguration des Event Managers eine Übereinstimmung mit einer benutzerdefinierten Bedingung für ein zugewiesenes Thema gefunden wird. Die Schnittstelle ist auch in der Lage, Nachrichten an den MQTT-Broker zu veröffentlichen, die vom Event Manager-Benachrichtigungsmechanismus generiert wurden, um Aktionen auf anderen IoT-Geräten auszulösen, die mit demselben MQTT-Broker verbunden sind. Es können bis zu zwei MQTT-Schnittstellen konfiguriert werden.

Nur in sicheren Inhouse-Umgebungen (aufgrund der fehlenden TLS-Unterstützung und Benutzerauthentifizierung) kann ein interner MQTT-Broker als interne Anwendung auf einem dedizierten RFP4G des SIP-DECT-Systems betrieben werden. Die Leistung dieses internen Brokers ist für QoS 0 und den üblichen IoT-Geräteverkehr (kurze Nachrichten alle paar Sekunden) ausreichend, die Verwendung von QoS 1 und 2 wird nicht empfohlen, da bei hoher Last ein höheres Risiko für verloren gegangene Nachrichten durch die Broker-Anwendung besteht. Aus diesem Grund ist die Broker-Konfiguration standardmäßig begrenzt.

Registerkarte Allgemein

Auf der Registerkarte **Allgemein** können die folgenden Grundeinstellungen der MQTT-Schnittstelle konfiguriert werden:

- **IP-Adresse:** IP-Adresse des MQTT-Brokers
- **IP-Port:** IP-Port des MQTT-Brokers (Standard: 1883)
- **Benutzer:** auf dem Broker konfigurierter Benutzername

- **Passwort:** Passwort des im Broker konfigurierten Benutzers
- **TLS verwenden:** Setzen Sie dies, wenn TLS als Protokoll verwendet werden soll (Standard-IP-Port: 8883).

Wenn die richtigen Einstellungen konfiguriert wurden, stellt der Event Manager eine Verbindung zum MQTT-Broker her.

Bitte beachten Sie: Der interne MQTT-Broker unterstützt kein TLS und ist durch die Standardkonfiguration eingeschränkt.

Bitte beachten Sie: Wenn "TLS verwenden" nicht aktiviert ist, werden nur unverschlüsselte Verbindungen ohne Authentifizierung hergestellt (normalerweise wird Port 1883 vom Broker für solche Verbindungen verwendet). Eventuell muss die Konfiguration des Brokers geändert werden, um solche Verbindungen zuzulassen. Es wird nicht empfohlen, Verbindungen zu einem MQTT-Broker (ohne TLS-Konfiguration) außerhalb des LANs aufzubauen, da die Datenübertragung dann unverschlüsselt erfolgt.

Registerkarte Endpunkte

Auf der Registerkarte **Endpunkte** können die IoT-Geräte angelegt werden, die über den MQTT-Broker mit dem Event Manager interagieren sollen.

Registerkarte Benutzerdefinierte Ereignistexte

In der Registerkarte **Benutzerdefinierte Ereignistexte** ist es möglich, spezielle Inhalte für die Benachrichtigungsmeldungen an adressierte Endpunkte (z. B. SIP-DECT-Endgeräte) zu definieren. Wenn diese Funktion auf der Registerkarte **Allgemein** nicht aktiviert ist, besteht der von der MQTT-Schnittstelle generierte Benachrichtigungstext aus dem Endpunkt-Label und der Beschreibung des Ereignistyps (oder dem Namen des Ereignistyps, wenn das Label leer ist) und wird für die Benachrichtigungsnachricht verwendet. In der Regel ist die MQTT-Nutzlast von IoT-Geräten nicht dafür gedacht, für Menschen lesbar zu sein. Daher kann diese Einstellung und Konfiguration verwendet werden, um spezielle Teile der empfangenen Nachrichten zu extrahieren und besser lesbare Benachrichtigungen für die empfangenden SIP-DECT-Endpunkte zu erzeugen.

Registerkarte Topics

Auf der Registerkarte **Topics** können Topics erstellt werden, die der Event Manager beim MQTT-Broker abonnieren oder bei der Veröffentlichung für Benachrichtigungen verwenden soll. In der Spalte **Typ** kann ausgewählt werden, ob das Topic für die Subskription beim MQTT-Broker oder für die Veröffentlichung von Nachrichten bei Event Manager-Benachrichtigungen verwendet werden soll. Jedes Topic muss einem zuvor erstellten MQTT-Endpunkt zugewiesen werden. Es ist möglich, mehrere Topics für einen Endpunkt zu konfigurieren. Alle Topics müssen für eine Schnittstelle eindeutig sein, es ist nicht möglich, einen zweiten Eintrag mit demselben Topic für einen anderen Endpunkt zu erstellen.

MQTT erlaubt im Allgemeinen die Verwendung von einstufigen ('+') und mehrstufigen ('#') Platzhaltern in Topics bei der Anmeldung bei einem Broker.

Im Event Manager ist es möglich, eine beliebige Textzeichenfolge als Topic zu konfigurieren, einschließlich Wildcards.

Es liegt jedoch in der Verantwortung des Event Manager-Administrators, nur gültige Topics zu konfigurieren, die mit den vollständigen Topics übereinstimmen, in denen ein bestimmtes Gerät seine Daten veröffentlichen wird.

Ein Mapping von MQTT-Nachrichten, die aus einem abonnierten Topic mit Wildcards resultieren, ist

nicht möglich, da sich das empfangene Topic von dem abonnierten Topic unterscheidet.

Vorübergehend könnte es nützlich sein, ein Wildcard-Topic für ein bestimmtes Gerät zu konfigurieren, um Wissen über Topics und Payloads zu erhalten, die ein bestimmtes Gerät im Event Manager Trace veröffentlicht.

Wenn überhaupt, wird dringend empfohlen, ein Wildcard-Topic auf ein bestimmtes Gerät zu beschränken, da sonst der Event Manager mit MQTT-Nachrichten von vielen Geräten überflutet werden könnte und instabil wird, wenn viele Geräte mit dem MQTT-Broker verbunden sind.

Registerkarte Subscribe mapping

Die Registerkarte **Subscribe mapping** ermöglicht die Konfiguration von Mappings für empfangene Payloads der MQTT-Nachrichten auf Ereignistypen. Für jedes MQTT-Topic können ein oder mehrere Mappings mit einer Bedingung für die Payload hinzugefügt werden. Eine Bedingung wird verwendet, um zu entscheiden, ob ein Ereignisauslöser erzeugt werden soll oder nicht. Verschiedene Bedingungen für dasselbe MQTT-Topic werden verwendet, um verschiedene Ereignisauslöser für verschiedene MQTT-Nutzdateninhalte zu erzeugen.

Beim Empfang einer MQTT-Nachricht muss zunächst das Topic der Nachricht mit einem konfigurierten Topic im Event Manager übereinstimmen (das in der Konfiguration nicht deaktiviert sein darf). Zusätzlich muss für dieses Topic ein 'Subscribe mapping' existieren, das eine Bedingung enthält, die zur Überprüfung der Payload der MQTT-Nachricht verwendet wird. Der zugewiesene Ereignistyp wird nur ausgelöst, wenn die Bedingung erfüllt ist und nicht auf das Verlassen des konfigurierten Hysteresebereichs oder ein Retrigger-Event-Timeout gewartet wird.

Beim Empfang einer MQTT-Nachricht werden alle konfigurierten Bedingungen, die dem empfangenen Topic zugeordnet sind, überprüft. Wenn mehr als eine Bedingung auf die empfangene Nachricht zutrifft, kann bei nur einer empfangenen MQTT-Nachricht auch mehr als ein Ereignis ausgelöst werden.

Je nach Konfiguration eines 'json_key' für eine Bedingung wird entweder der json-Wert des durch den Schlüssel angegebenen json-Attributs oder die vollständige Nutzlast der MQTT-Nachricht mit den Bedingungen geprüft. Um auf Attribute in verschachtelten json-Strukturen zuzugreifen, können mehrere Attributnamen mit '/' konkateniert werden, ähnlich der Syntax, die für MQTT-Topics verwendet wird (siehe folgendes Beispiel):

Beispiele:

```
Json key:     'foo'
Json data:    {"foo":"bar"}
result:       "bar" will be processed by the Event Manager condition

Json key:     'foo/bar'
Json data:    {"foo":{"bar":10.27}}
result:       10.27 will be processed by the Event Manager condition
```

Bitte beachten Sie, dass Json-Arrays vom Event Manager nicht unterstützt werden!

Eine Bedingung kann eine der folgenden sein:

- Text gleich
  Der zu prüfende Inhalt stimmt genau mit dem angegebenen Text überein
- Text enthalten
  Der angegebene Text ist Teil des zu prüfenden Inhalts
- Wert identisch
  Der zu prüfende Inhalt wird als numerischer Wert angenommen und bei erfolgreicher Konvertierung

auf Gleichheit mit dem konfigurierten Wert geprüft
Das Ereignis wird ausgelöst, wenn der empfangene Wert mindestens einmal nicht mit dem konfigurierten Wert übereinstimmt und mit einer späteren Nachricht wieder gleich wird oder wenn die Zeit abgelaufen ist, die durch den „Timeout für Ereignis neu auslösen“ konfiguriert wird.

- Wert kleiner / größer
  Der zu prüfende Inhalt wird als numerischer Wert angenommen und bei erfolgreicher Konvertierung auf einen Wert kleiner / größer als der konfigurierte Wert geprüft. Wenn diese Art von Bedingung ausgewählt wird, muss ein Hysteresewert konfiguriert werden. Ein neues Ereignis wird normalerweise nicht bei jedem Empfang einer MQTT-Nachricht ausgelöst (was durchaus häufig vorkommen kann). Das Ereignis wird ausgelöst, sobald die Bedingung das erste Mal erfüllt ist. Um eine erneute Auslösung desselben Ereignisses zu ermöglichen, muss eine Nachricht empfangen werden, die einen Wert übe bzw. unter dem Hysteresewert der Bedingung enthält.

Für jede der Bedingungen kann ein „Timeout für Ereignis neu auslösen" mit vorkonfigurierten Werten zwischen 1 Minute und 2 Stunden konfiguriert werden. In diesen Fällen wird bei jeder Erzeugung des konfigurierten Ereignistyps ein Zeitgeber gestartet. Ein neues Ereignis wird nur dann ausgelöst, wenn dieser Zeitgeber bereits abgelaufen ist.

Registerkarte Publish mapping

Die Registerkarte **Publish mapping** ermöglicht die Konfiguration von MQTT-Topics und Payloads, die einer Publish message an einen MQTT-Endpunkt hinzugefügt werden sollen abhängig vom Ereignistyp, der den die Benachrichtigung erzeugenden Ereignisplan ausgelöst hat.

In einem zweiten Konfigurationsschritt muss die Payload für die Publish message konfiguriert werden. Für ein bestimmtes Topic können mehrere Payloads konfiguriert werden, die durch den Ereignistyp ausgewählt werden und die den Ereignisplan auslösen, um die Benachrichtigung (auch an MQTT-Endpunkte) zu erzeugen. Da nicht mehr als genau eine Publish message für einen bestimmten Ereignistyp ausführbar ist, ist es nicht sinnvoll, denselben Ereignistyp und dieselbe Nutzlast mit verschiedenen Topics auf derselben MQTT-Schnittstelle abzubilden. In solchen Fällen würde nur das erste gefundene Publish mapping zu einer ausgehenden Publish message führen. Um solche Konflikte zu vermeiden, kann es sinnvoll sein, verschiedene Endpunkte zu konfigurieren, die sich auf spezifischere Topics beziehen (siehe das folgende Beispiel):

Endpunkte: tasmota_AF7B08_P1, tasmota_AF7B08_P2 und tasmota_AF7B08_P3

Publish mit unterschiedlichen Publish messages für POWER1, POWER2 und POWER3 (Payload kann 'ON' oder 'OFF' sein).

Normalerweise ist die vom Event Manager erzeugte Benachrichtigungstextnachricht dazu gedacht, von Menschen gelesen zu werden, und es macht in den meisten Fällen wenig Sinn, sie als Payload in einer MQTT-Nachricht zu verwenden.

Wenn ein Consumer-Client mit dem MQTT-Broker verbunden ist, der in der Lage und angepasst ist, die vom Event Manager generierten Benachrichtigungstextnachrichten zu verarbeiten (z. B. Node Red), dann kann ein MQTT-Topic so konfiguriert werden, dass es die Benachrichtigungstextnachricht als Payload anstelle der Payload verwendet, die durch ein 'Publish mapping' vorgegeben ist.

Um die Benachrichtigungstextnachricht als Payload für die MQTT-Publish-Mesaage zu verwenden, muss das Flag ‚Nachricht als Payload' in der 'Topic'-Konfiguration aktiviert worden sein.

Löschen von MQTT-Interfaces, Topics und Endpunkten

Wenn MQTT-Endpunkte, Topics und Schnittstellen vom Administrator gelöscht werden, gelten die folgenden Regeln:

- Eine MQTT-Schnittstelle kann nur gelöscht werden, wenn für diese Schnittstelle keine Endpunkte mit Zuordnung zu einem Standort konfiguriert sind.
- Beim Löschen einer MQTT-Schnittstelle werden alle zugehörigen Endpunkte, Topics, Subscribe mappings und Publish mappings implizit gelöscht
- Beim Löschen eines MQTT-Endpunktes werden alle zugehörigen Topics, Subscribe mappings und Publish mappings implizit gelöscht.
- Beim Löschen eines MQTT-Topics werden alle zugehörigen Subscribe mappings und Publish mappings implizit gelöscht

Web-API-Interface

Der SIP-DECT Event Manager bietet eine Web-API an, die es anderen Anwendungen, einschließlich Mitel CloudLink Workflow, ermöglicht, mit dem Event Manager zu interagieren und z.B. Ereignisse auszulösen oder Benachrichtigungen vom Event Manager zu erhalten.

Die folgenden ereignisbezogenen Aktionen werden unterstützt:

- Senden eines Ereignisses an den Event Manager ("reqType": "**event**") und dadurch Auslösen der Ausführung eines Ereignisplans
- Abbrechen der Ausführung eines Ereignisplans ("reqType": "**eventcancel**")
- Empfang des Ergebnisses eines ausgeführten Ereignisplans vom Event Manager ("reqType": "**eventresult**")

Die folgenden benachrichtigungsbezogenen Aktionen werden unterstützt

- Empfang einer Benachrichtigung vom Ereignismanager ("reqType": "**notification**")
- Bestätigung einer Meldung an den Ereignismanager ("reqType": "**confirmation**")
- Stornierung einer Meldung durch den Ereignismanager ("reqType": "**cancel**"), z. B. wenn alle erforderlichen Bestätigungen eingegangen sind, der Ereignisplan abgesagt wurde oder eine Zeitüberschreitung vorliegt

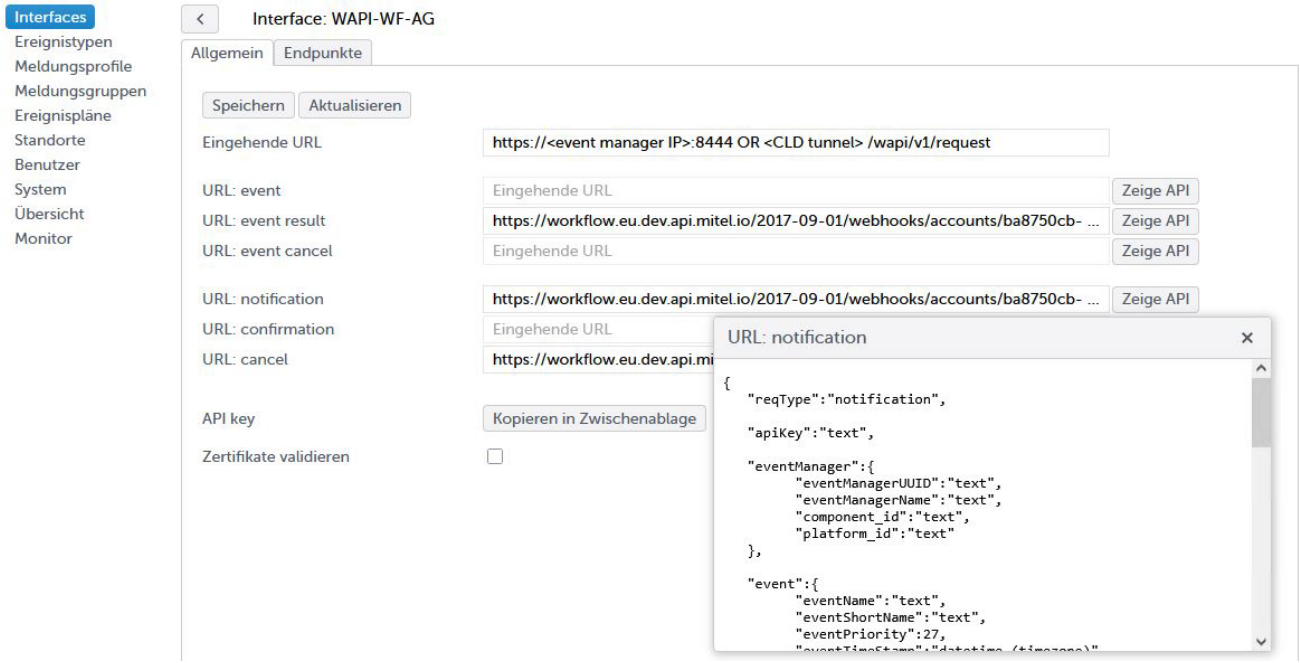
Mitel CloudLink Workflow kommuniziert mit dem Event Manager über den Mitel CloudLink Daemon, der in die Basisstation der vierten Generation integriert ist. Der Mitel CloudLink Daemon ist derzeit noch nicht für Server-Installationen des Event Managers verfügbar, d.h. Workflow kann den Event Manager nicht erreichen, wenn dieser auf einem Rocky Linux® Server für DECT-Lokalisierung installiert ist.

Die Web-API unterstützt eingehende Webanfragen mit einer URL in einer der folgenden Formen:

- https://<event manager IP>:8444/wapi/v1/request
- https://<CLD tunnel>/wapi/v1/request

Der Event Manager akzeptiert http GET und POST Anfragen.

Die Json-Body-Definition ist über die EM Web-GUI verfügbar, indem Sie auf die Schaltfläche "Show API" für die jeweilige Anfrage klicken.



Es gibt auch eine vereinfachte Form für das Auslösen eines Ereignisses, bei der die obligatorischen Parameter der Anfrage als URL-Parameter hinzugefügt werden und ein JSON-Body nicht erforderlich ist. Dies bedeutet, dass ein Ereignis sogar von einem Webbrowser ausgelöst werden kann, z. B. zu Testzwecken.

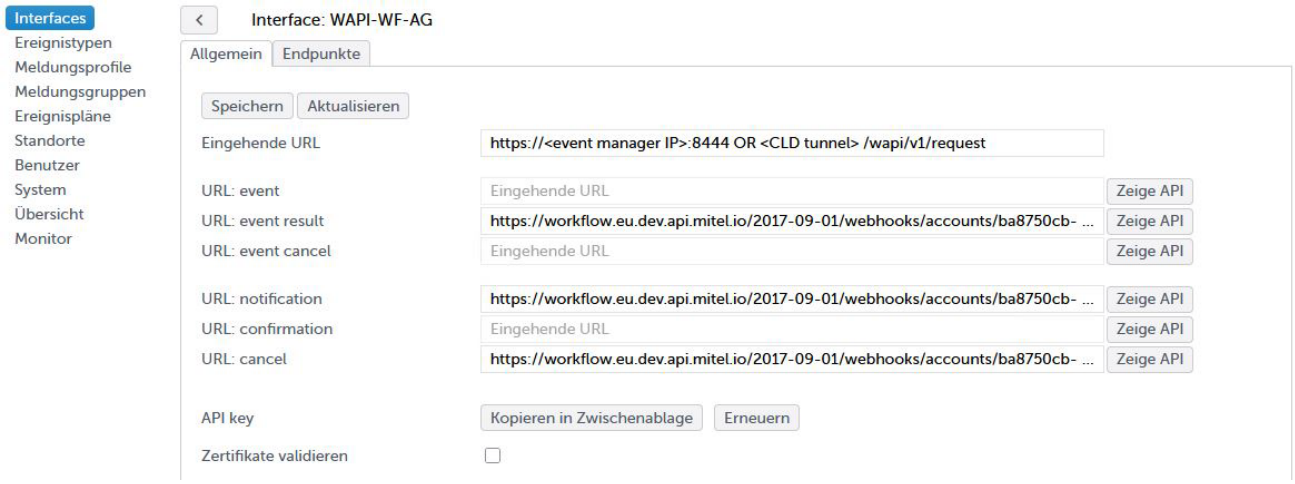
```
https://192.168.2.41:8444/wapi/v1/request?type=event&apiKey=5gDem3N3QS6XcTtViujWwiiO5usOJhDoIQ5NocONjMQMmvwezUEFrIntsTjPFGyz&eventName=SOS&eventText=Test&sourceEndpointAddress=118
```

Beispiel für eine Anfrage mit URL-Parametern zum Auslösen eines Ereignisses anstelle von

```
{
	"reqType":"event",
	"apiKey":"5gDem3N3QS6XcTtViujWwiiO5usOJhDoIQ5NocONjMQMmvwezUEFrIntsTjPFGyz",
	"eventName":"SOS",
	"sourceEndpoint":{
		"sourceEndpointAddress":"118"
	},
	"eventText":"Test"
}
```

Beispiel für einen JSON-Body für die Anfrage https://192.168.2.41:8444/wapi/v1/request Content-Type application/json nur mit notwendigen Parametern

Die eingehenden Anfragen (**eventresult**, **eventcancel**, **confirmation**) erfordern einen API-Schlüssel, der durch Klicken auf die Schaltfläche "In die Zwischenablage kopieren" in die Zwischenablage kopiert werden kann.



Ausgehende Anfragen (**eventresult**, **notification**, **cancel**) werden als POST-Anfragen mit dem Json-Body gesendet, dessen Definition über die EM Web-GUI durch Klicken auf die entsprechende Schaltfläche "Show API" verfügbar ist.

Der JSON-Body der Benachrichtigung enthält Event Manager CloudLink Daemon-Informationen, die für die Befriedigung der CloudLink-Tunnel-API erforderlich sind, um von dort Bestätigungen zurück an den Event Manager senden zu können. Sie sind nicht relevant für andere Anwendungen, die über die Web-API mit dem

Event Manager verbunden sind.

```
"eventManager":{
          "eventManagerUUID":"text",
          "eventManagerName":"text",
          "component_id":"text",
          "platform_id":"text"
},
```

POST https://tunnel.dev.api.mitel.io/wapi/v1/request

Headers | Body | Authorization | Testing

Key	Value
Content-Type	application/json
x-mitel-tunnel-service	adminportal
x-mitel-tunnel-platform-id	{{eventManagerPlatformID}}
x-mitel-tunnel-component-id	{{eventManagerComponentId}}
x-mitel-tunnel-component	dectevp

Mit der Option "Zertifikate validieren" können Sie die Validierung der Zertifikate der Server aktivieren, an die die ausgehenden Anfragen gesendet werden. Weitere Informationen zum Umgang mit Zertifikaten finden Sie im Abschnitt System / Registerkarte Sicherheit.

Registerkarte Allgemein

Auf der Registerkarte **Allgemein** können die folgenden Grundeinstellungen der Web-API-Schnittstelle konfiguriert werden:

- **URL: event result:** URL für ausgehende Antworten auf die Ereignisanfragen
- **URL: notification:** URL einer externen Webanwendung (z.B. Workflow) als Empfänger von Benachrichtigungen aus dem Event Manager
- **URL: cancel:** URL einer externen Webanwendung als Empfänger von Event Manager-Benachrichtigungen

Beispiele:

- für die Workflow-API:
  https://workflow.eu.dev.api.mitel.io/2017-09-01/webhooks/accounts/ba8750cb-3032-4015-8fde-feddf81da52f/activities/420ed198-5c77-4c14-9117-7330d64b3343/workers
- für den WAPI-Tester (eine Python-Applikation unter Windows oder Linux für den Test der Web-API-Schnittstelle):
  http://10.103.37.79:8000
  Dieses Tool kann auf Anfrage zu Testzwecken zur Verfügung gestellt werden, ohne jegliche Garantie oder Unterstützung.

Die JSON-Body-Definitionen für die Anfragen sind über die jeweiligen Schaltflächen "Zeige API" verfügbar.

Die Schaltflächen "Kopieren in Zwischenablage " und "Erneuern" können hier verwendet werden, um den API-Key zu kopieren oder zu erneuern, der zur Authentifizierung bei der Web-API für eingehende Anfragen verwendet wird.

Mit der Option "Zertifikate validieren" wird die Validierung der Zertifikate der Server aktiviert, an die die ausgehenden Anfragen gesendet werden.

Registerkarte Endpunkte

Auf der Registerkarte **Endpunkte** können Sie Endpunkte erstellen, die als Ereignisauslöser oder Benachrichtigungsempfänger fungieren können.

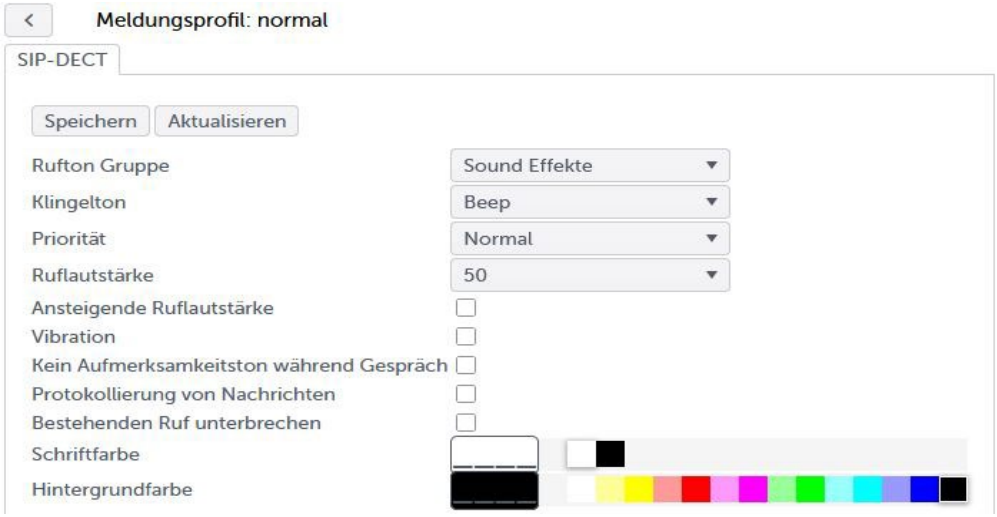
Ereignistypen

Es stehen fünf Standard-Ereignistypen ('Man Down', ‚No Move‘, ‚ESCAPE‘, 'SOS-Key' und 'System Info') zur Verfügung. Diese Typen können geändert, aber nicht gelöscht werden. Die Standard-Ereignistypen 'Man Down' und 'SOS-Key' entsprechen den standardmäßig in SIP-DECT verfügbaren Alarm-Triggern.
Um zusätzliche Alarm-Trigger zu verarbeiten, die in SIP-DECT OMP definiert werden können, müssen Ereignistypen mit dem gleichen Namen oder Kurznamen wie der Name der Trigger-ID in OMP im SIP-DECT-Event-Manager konfiguriert werden.
Alle Ereignistypen dienen als eine Art Filter in einem Ereignisplan, um die Eskalation eines Ereignisses zu steuern. Anhand der zugewiesenen Priorität weiß das System, in welcher Reihenfolge die Ereignisse abgearbeitet werden sollen. Wichtige Ereignisse sollten daher mit einer höheren Priorität konfiguriert werden.

Hinweis: Ein auf einem DECT-Telefon angezeigtes Ereignis wird durch ein Ereignis mit höherer Priorität überschrieben.

Meldungsprofile

Meldungsprofile legen fest, wie eine Benachrichtigung dem Empfänger angezeigt werden soll. Er wird dem empfangenden Endpunkt innerhalb des Ereignisplans zugewiesen. Auf einem DECT-Telefon wird nur eine Benachrichtigung und nur die mit der höchsten Priorität (Priorität des Ereignistyps) angezeigt. Benachrichtigungen mit niedrigerer Priorität werden nicht an das DECT-Telefon übertragen, wenn eine Nachricht mit höherer Priorität angezeigt werden soll. Liegen mehrere Nachrichten mit gleicher Priorität gleichzeitig vor, werden diese nacheinander an das DECT-Telefon übertragen, wobei jede Nachricht mindestens 20 Sekunden lang angezeigt wird, bevor sie durch die nächste ersetzt wird. Wenn Sie das Interface bei der Konfiguration eines neuen Meldungsprofils auswählen, werden die konfigurierbaren Parameter angezeigt. Meldungsprofile sind je nach Interface sehr unterschiedlich. Standardmäßig wird ein Meldungsprofil ('normal') erstellt, dieses Profil kann nicht gelöscht werden. Klicken Sie auf den Link unter der Spalte "Bezeichnung", um die Profileinstellungen (Melodie, Klingelton, Lautstärke usw.) für ein Profil zu ändern.



Eine Rufton Gruppe ist ein Satz oder eine Sammlung von Klingeltönen, die bestimmten Kontakten, Gruppen oder Kategorien zugewiesen werden können. Rufton Gruppen werden verwendet, um die Alarmtöne für eingehende Anrufe für verschiedene Anrufer oder Anruftypen anzupassen. Die Rufton Gruppe kann aus allen bei SIP-DECT verfügbaren Klingeltönen gezielt ausgewählt werden.

Wenn die Option "Ansteigende Ruflautstärke" verwendet wird, beginnt der Klingelton leise und erreicht dann allmählich die eingestellte Ruflautstärke. Darüber hinaus kann die Benachrichtigung auch durch Vibration des Telefons signalisiert werden (sofern dies vom Telefontyp unterstützt wird).

Wenn die Option "Kein Aufmerksamkeitston während Gespräch" aktiv ist, wird eine Benachrichtigung ohne akustische Signalisierung zugestellt, während das Endgerät telefoniert.

Wenn die Option "Protokollierung von Nachrichten" aktiviert ist, bleiben beantwortete Benachrichtigungen (angenommen oder abgelehnt) in der Liste der Textnachrichten auf dem Mitel DECT-Telefon für bis zu fünfzehn Nachrichten verfügbar. Weitere Nachrichten überschreiben die ältesten Nachrichteneinträge in der Liste. Nicht beantwortete Nachrichten (weder angenommen noch abgelehnt) werden nicht in der Liste der Textnachrichten auf dem Mitel DECT-Telefon protokolliert.

Wenn "Bestehenden Ruf unterbrechen" ausgewählt ist, wird ein bestehender Anruf zum Zeitpunkt der Benachrichtigung getrennt.

Wenn das Telefon 'Schriftfarbe' und 'Hintergrundfarbe' unterstützt, kann die Schrift- und Farbdarstellung der Nachricht über den SIP-DECT-Event-Manager gesteuert werden.

Einschränkungen und Verhalten:

- Einstellungen, die vom verwendeten Telefon nicht unterstützt werden, werden ignoriert.
- **'Priorität: Low':** 'Rufton Gruppe', 'Klingelton', 'Ruflautstärke' und 'Ansteigende Ruflautstärke' haben keine Auswirkungen.
- **'Priorität: Emergency':** Pop-up-Fenster während des Anrufs nur mit dieser Priorität verfügbar
- Weitere Informationen zum Verhalten der angezeigten Meldungen: Bitte beachten Sie das Dokument 'Mitel 600/700 DECT Phone Messaging and Alerting Applications'!

Meldungsgruppen

Endpunkte, die ein Ereignis empfangen können, können in einer Meldungsgruppe zusammengefasst werden.

Dies vereinfacht die Konfiguration bezüglich der Eskalation eines Ereignisses. Wenn die zugewiesene Adresse der Benachrichtigungsgruppe mit der Adresse des Ursprungsendpunkts übereinstimmt, kann die Funktion "Rufadresse verwenden" der Ereignisphase verwendet werden.

Ereignispläne

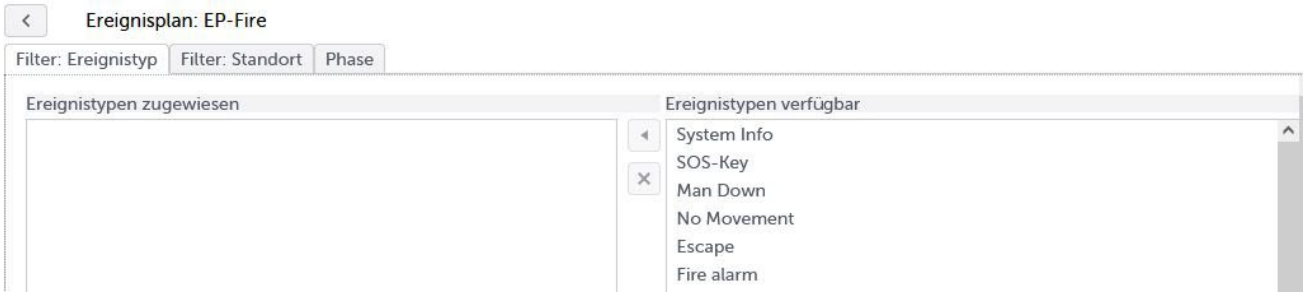
Ereignispläne beschreiben, wie auf bestimmte Arten von Ereignissen reagiert werden soll, die an verschiedenen Standorten auftreten. Ereignispläne können aus bis zu 10 Eskalationsphasen bestehen und definieren den Prozess für den Umgang mit diesen Ereignissen und den daraus resultierenden Benachrichtigungen in den verschiedenen Phasen.

Ein laufender Ereignisplan wird abgebrochen und neu gestartet, wenn das gleiche Ereignis erneut vom gleichen Endpunkt gesendet wird. Dies kann die Ausführung weiterer Phasen verhindern. Mit SIP-DECT 10.0 wird die Option eingeführt, dass ein laufender Ereignisplan weiterläuft und weitere Ereignisse des gleichen Typs vom gleichen Endpunkt ignoriert werden, bis der laufende Plan beendet wird.

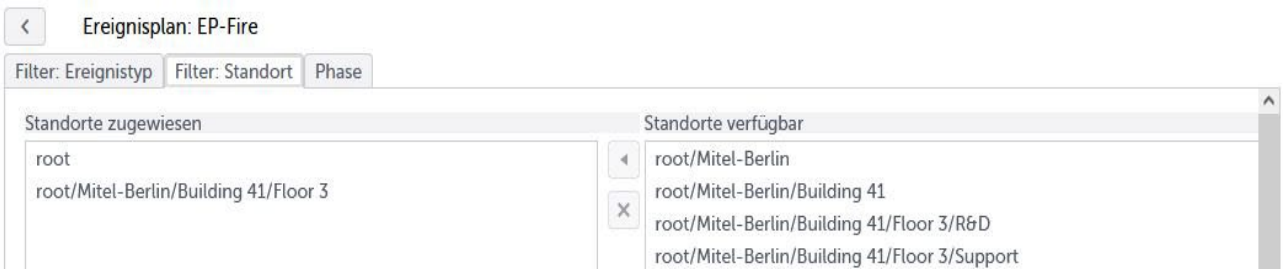
Die folgenden Einstellungen können im Konfigurationsbereich **Ereignispläne** vorgenommen werden:

Registerkarte "Filter: Ereignistyp"

Dem Ereignisplan können hier verschiedene Arten von Ereignissen zugeordnet werden. Mindestens die folgenden Standard-Ereignistypen sind verfügbar: **System Info**, **SOS-Key, Man Down, No Movement** und **Escape.**



Registerkarte "Filter: Standort"

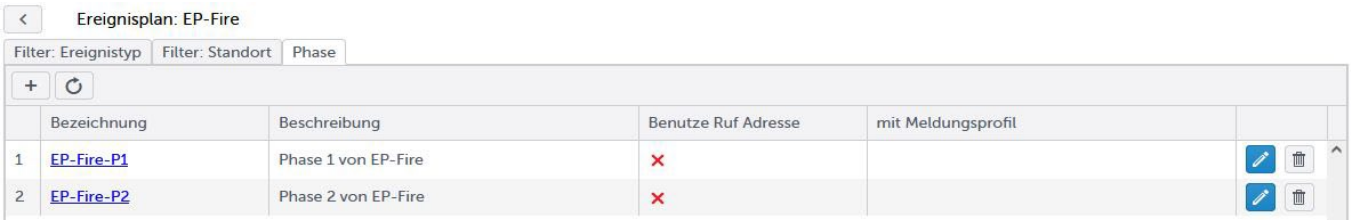


Zuvor angelegte Standorte (denen Endpunkte zugewiesen sind) können hier dem Ereignisplan zugewiesen

werden.

Registerkarte "Phase"

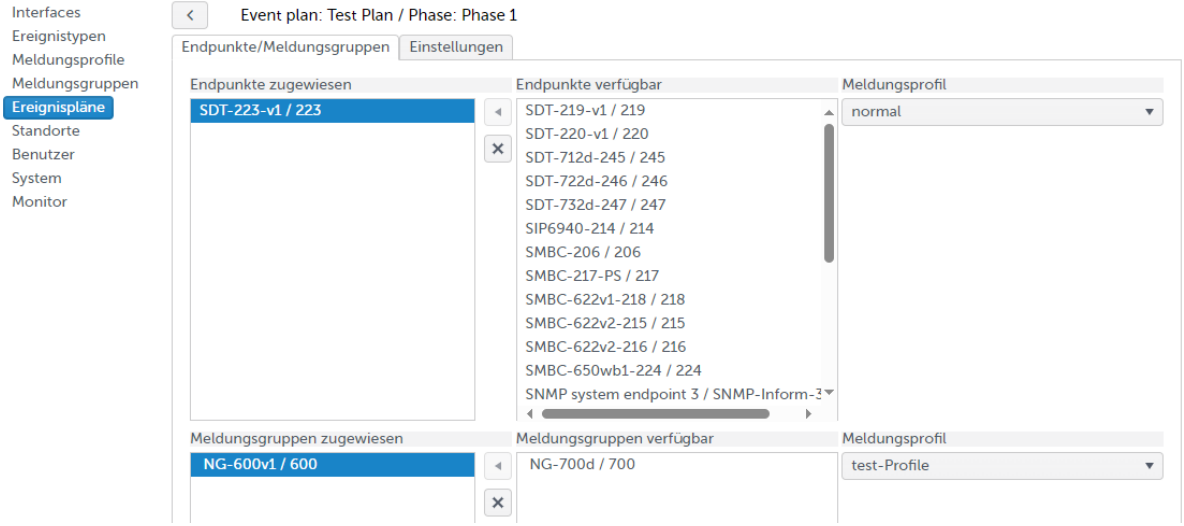
Mit den folgenden Konfigurationen können bis zu 10 Phasen zu einem Ereignisplan auf der Registerkarte "Phase" hinzugefügt werden:



Durch Bearbeiten der Phaseneinstellungen kann der Schalter "Benutze Ruf Adresse" aktiviert und ein Meldungsprofil zugewiesen werden. Mit dieser Art der Konfiguration kann eine direkte Zuordnung von Rufadressen zu einer Meldungsgruppe mit dieser Adresse realisiert werden. In dem Eingangsinterface (z.B. ESPA) muss ein Endpunkt mit dieser Aufrufadresse konfiguriert werden.

Registerkarte "Endpunkte/Meldungsgruppen"

Auf der Registerkarte Endpunkte/Meldungsgruppen können bis zu 1000 Endpunkte und/oder bis zu 50 Meldungsgruppen zu einer Phase hinzugefügt oder aus einer Phase gelöscht werden. Jedem Endpunkt oder jeder Meldungsgruppe kann auch hier ein zuvor erstelltes Meldungsprofil zugewiesen werden.



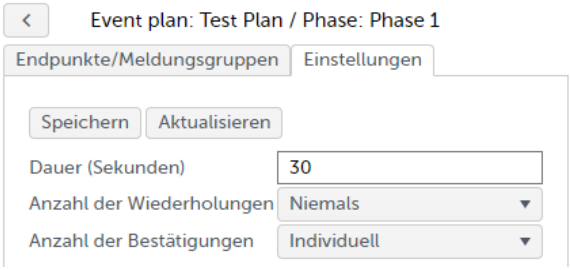
Registerkarte "Einstellungen"

Folgende Einstellungen können auf der Registerkarte Einstellungen für eine Phase vorgenommen werden:

- Dauer für diese Phase (in Sekunden)
- Anzahl der Wiederholungen (Wiederholungen dieser Phase)
- Anzahl der Bestätigungen (erforderlich für das erfolgreiche Beenden der Phase)

Hinweis: "Individuell" bedeutet, dass alle dieser Phase zugewiesenen Endpunkte die empfangene Benachrichtigung bestätigen müssen, bevor die Phase erfolgreich beendet wird. Wenn die Anzahl der Bestätigungen nicht erreicht wird, geht sie in die nächste Phase über (falls konfiguriert), wird wiederholt (falls konfiguriert) oder wird nach Ablauf der Phase beendet.

Hinweis: Wenn einer Phase ausgehende Endpunkte wie Modbus oder SNMP zugeordnet sind, sollte die Einstellung für die Anzahl der Bestätigungen nicht auf "Individuell" gesetzt werden, um erfolglose Phasen zu vermeiden (da diese Arten von Endpunkten niemals in der Lage sind, empfangene Nachrichten zu bestätigen).



Standorte

Durch die Definition der Standorte kann eine räumliche Umgebung in einer Baumstruktur abgebildet werden. Ein Standort ist der Ursprung eines Ereignisses. Endpunkte, die zum Auslösen eines Ereignisses verwendet werden sollen, können hier einem Standort zugewiesen werden. Endpunkte, die keinem Standort zugewiesen sind, können kein Ereignis auslösen.

Der Stammstandort 'root' ist immer vorhanden und kann nicht gelöscht werden.

Um einen neuen Standort anzulegen, muss eine Tabellenzeile ausgewählt und die Schaltfläche + gedrückt werden. Der neue Standort basiert dann auf dem Standort, der zuvor ausgewählt wurde.

Alle Endpunkte können einem gewünschten Standort zugewiesen werden, indem Sie dem Link unter der Spalte "Bezeichnung" folgen. Die Zuweisung kann auch über die Registerkarte **Endpunkte** im Konfigurationsbereich **Interfaces** geändert werden.

Benutzer

Der Benutzerbereich ermöglicht das Erstellen, Bearbeiten und Löschen von Benutzern sowie das Ändern der Passwörter der Benutzer. Der Standardbenutzer admin mit der Berechtigung ‚Konfiguration' kann nicht gelöscht werden. Darüber hinaus gibt es zwei weitere Berechtigungsstufen ‚Monitor' und ‚Lokalisierung', die dafür benutzt werden können, Benutzer mit eingeschränkten Berechtigungen hinzuzufügen.

System

Der Bereich "System " besteht aus den folgenden Registerkarten:

Registerkarte „Allgemein"

Auf der Registerkarte **Allgemein** können die folgenden Konfigurationen vorgenommen werden:

- ein Systemname, der dann auch in der Kopfzeile der Eventmanager-Webanwendung angezeigt wird.
- Hier kann der CloudLink-Daemon aktiviert werden (für die Fernverwaltung des Event Managers)
- Der CloudLink-Status wird hier angezeigt (läuft oder läuft nicht)

- Die Version der laufenden Eventmanager-Anwendung wird hier angezeigt.
- Hier kann ein externer IP-Watchdog außerhalb des Systems konfiguriert werden, der einen Ping vom Event Manager beobachtet (der normalerweise in regelmäßigen Abständen alle 30 Sekunden gesendet wird, solange er korrekt funktioniert). Der IP-Watchdog kann einen Alarm per E-Mail, SMS oder SNMP-Trap auslösen oder ein Relais für die Unterbrechung der Stromversorgung des überwachten Geräts aktivieren, um den RFP, in dem der Event Manager konfiguriert ist, neu zu starten, falls ein Ping vom überwachten Gerät ausbleibt.

Registerkarte „Datensicherung/Neustart"

- **Neustart**: Mit diesem Menüpunkt kann der SIP-DECT-Event-Manager neu gestartet werden. Der SIP-DECT-Event-Manager ist kurzzeitig nicht verfügbar.
- **Neustart mit Grundeinstellungen**: Alle Daten und Einstellungen am SIP-DECT-Event-Manager werden unwiderruflich gelöscht, wenn die Werkseinstellungen wiederhergestellt werden.
- **Export Log**: Protokolldateien können vom SIP-DECT-Event-Manager heruntergeladen werden. Die Protokolldateien bestehen aus zwei CSV-Dateien, die die Ereigniszusammenfassung und die Details zur Ereignisausführung enthalten. Je nach Traffic auf dem Event Manager werden die Logs der letzten Tage oder Wochen gespeichert (maximale Größe des Detaillogs beträgt 6 MByte).
- **Export Konfiguration**: Eine laufende Konfiguration des SIP-DECT-Event-Managers kann heruntergeladen und auf dem lokalen Rechner des Administrators gespeichert werden.
- **Import Konfiguration**: Ermöglicht die Wiederherstellung einer bestehenden Konfiguration im SIP-DECT-Event-Manager als ZIP-Datei (.gz) aber auch als normale Textdatei. Vor der Aktivierung wird eine Gültigkeitsprüfung durchgeführt, eine als fehlerhaft oder unvollständig erkannte Konfiguration wird nicht aktiviert. Beim Import werden die Benutzerdaten aus dem laufenden SIP-DECT-Event-Manager System verwendet. Wenn die Konfigurationsdatei als vollständig erkannt wurde, wird das SIP-DECT-Event-Manager System automatisch neu gestartet, um die Datensicherung zu aktivieren.

Registerkarte „Sicherheit“

Auf der Registerkarte "Sicherheit" des Systems können die folgenden Aktionen durchgeführt werden:

- Der Import eines vertrauenswürdigen Zertifikats, das im SIP-DECT OMM verwendet wird (für die zukünftige Verwendung).
- Der Import einer lokalen Zertifikatskette und eines privaten Schlüssels (mit oder ohne Passwort) für den SIP-DECT Event Manager, der dann für den Webzugriff auf die Event-Manager Anwendung verwendet wird.
- Über eine Schaltfläche "Löschen" können zuvor installierte Zertifikate und private Schlüssel auf einmal gelöscht werden.
- Über einen dedizierten 'Restart'-Button wird die Aktivierung von neu importierten Zertifikaten oder privaten Schlüsseln in das System abgeschlossen (Import in die Webserver-Konfiguration).

Wenn ein vertrauenswürdiges Zertifikat oder eine lokale Zertifikatkette installiert wurde, wird die Anzahl dieser Zertifikate angezeigt. Es wird auch angezeigt, ob ein privater Schlüssel importiert wurde. Die Namen der Dateien mit vertrauenswürdigem(n) Zertifikat(en) werden auch in einer separaten Tabelle auf dieser Seite angezeigt. Vertrauenswürdige Zertifikate können aus dieser zusätzlichen Tabelle wieder gelöscht werden. Die lokale Zertifikatskette und der private Schlüssel können nur gemeinsam wieder gelöscht werden.

Wurde eine lokale Zertifikatskette importiert, muss der entsprechende private Schlüssel (und die Konfiguration des benötigten Passwortes) unbedingt auch vor einem Neustart des SIP-DECT Event Managers erfolgen. Andernfalls ist das System möglicherweise für die weitere Konfiguration über den

Web-Admin nicht mehr erreichbar.

Registerkarte „Sicherheitsstufe“

Auf der Registerkarte "Sicherheitsstufe" des Systems können folgende Aktionen durchgeführt werden:

- Einstellung einer Sicherheitsstufe für die Eventmanager-Anwendung (Hoch, Mittel, Legacy)
- Konfiguration der "benutzten Cipher Suites" für die verschiedenen Sicherheitsstufen

Normalerweise ist als Standard die Sicherheitsstufe "Hoch" und eine Standardeinstellung für "Benutzte Cipher Suites" konfiguriert. Diese Einstellungen können hier vorsichtig modifiziert werden. Dazu wird hier eine Liste der aktuell konfigurierten und der allgemein konfigurierbaren Cipher Suites angezeigt. Das Hinzufügen von Chiffriersuiten in die 'Benutzten Cipher Suites' kann durch Auswahl des Chiffriersuiten-Namens aus dem Tabelleneintrag 'Unterstützte Chiffriersuiten' mit vorangestelltem Semikolon am Ende der aufgelisteten Suites im oberen Listeneintrag (Benutzte Cipher Suites) erfolgen. Ein Eintrag kann einfach aus den 'Benutzten Cipher Suites' gelöscht werden, indem der Tabelleneintrag nach Abwahl des Kontrollkästchens 'Standardwerte verwenden' bearbeitet wird. In allen Fällen, in denen Cipher Suites geändert werden, muss die Konfiguration durch Drücken der Schaltfläche 'Speichern' abgeschlossen werden.

Registerkarte CloudLink

Die Registerkarte CloudLink ist nur sichtbar, wenn der CloudLink-Daemon zuvor aktiviert wurde. Über diese Registerkarte ist ein detailliertes CloudLink Daemon-Fenster verfügbar, um den Event Manager mit dem CloudLink Portal zu verbinden und den Tunnel für den Fernzugriff auf den Event Manager zu starten.

Informationen über das CloudLink Daemon-Portal und die Systeminventarisierung im CloudLink-Portal finden Sie in der CloudLink-Dokumentation im Document Center unter

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

Ein Konto mit ‚SIP-DECT-Integration‘ ist für das CloudLink-Portal erforderlich.

Bevor Sie den OMM oder Event Manager aus einem RFP entfernen, stoppen Sie die Tunnel und trennen Sie die Verbindung des CloudLink Daemon zu CloudLink.

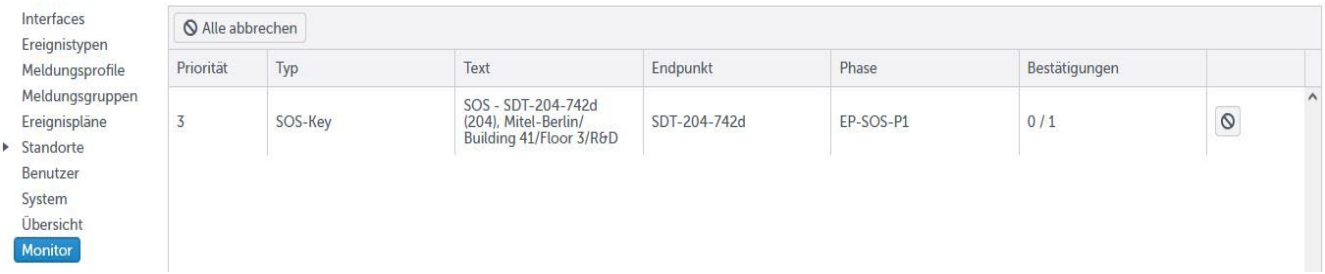
Der CloudLink Daemon verbindet sich mit *.mitel.io-Diensten über https (Port 443)

Übersicht

Der Übersichtsbereich zeigt den aktuell konfigurierten Ereignisfluss, die Benachrichtigungsgruppen, die MQTT-Zuordnungen und die Schnittstellenendpunktbeziehungen an.

Monitor

Im Bereich "Monitor" wird eine Tabelle mit den derzeit aktiven Ereignisbehandlungen angezeigt. Einzelne Ereigniszeilen aus dieser Tabelle oder alle aktiven Ereignisbehandlungen können von hier aus abgebrochen werden.



Event Log (Summary and Details)

Die Zusammenfassung und die Details der Ereignisprotokolle können über den Web-Admin als .csv-Dateien heruntergeladen werden
Ab SIP-DECT 10.0 wurden die Informationen verbessert, so dass nun klar ersichtlich ist, dass eine Benachrichtigung beim DECT-Telefon eingegangen ist.

Spalte	Information	Bedeutung
Status	Notify	Benachrichtigung wurde zum DECT-Telefon gesendet
	Notification received	Benachrichtigung wurde vom DECT-Telefon empfangen
	Confirmed	Benutzer hat die Nachricht bestätigt (positiv oder negativ)
	Notification terminated	Benachrichtigung wurde vom EM beendet
Confirmation	Accepted	Benutzer hat die Nachricht positiv bestätigt
	Rejected	Benutzer hat die Nachricht negativ bestätigt
	Not confirmed	Benutzer hat noch nicht auf die Nachricht geantwortet
	Not received	Nachricht wurde (noch) nicht vom DECT-Telefon empfangen

Darüber hinaus wurden die Spaltenüberschriften weitgehend an die Begriffe auf der EM-Webschnittstelle angepasst, wo dies angebracht war.

Time	Event-Id	Phase-Id	Notification-Id	Status	Source	Address	Event	Priority	Text	Location	Plan	Phase	Phase-Count	Destination	Address_	Profile	Confirmation
27.01.2025 13:48:14	2			New Event	Patient 118	118	SOS	2	Emergency Call								
27.01.2025 13:48:14	2	1		New Phase	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1				
27.01.2025 13:48:14	2	1	4	Notifiy	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Supervisor 1	120	SOS	
27.01.2025 13:48:14	2	1	5	Notifiy	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Caregiver 1	118	SOS	
27.01.2025 13:48:14	2	1	6	Notifiy	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Caregiver 2	119	SOS	
27.01.2025 13:48:16	2	1	4	Notification received	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Supervisor 1	120	SOS	
27.01.2025 13:48:16	2	1	5	Notification received	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Caregiver 1	118	SOS	
27.01.2025 13:48:18	2	1	4	Confirmed	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Supervisor 1	120	SOS	Accepted
27.01.2025 13:51:14	2	1	5	Notification terminated	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Caregiver 1	118	SOS	Not confirmed
27.01.2025 13:51:14	2	1	6	Notification terminated	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Caregiver 2	119	SOS	Not received
27.01.2025 13:51:14	2			Event Finished: Timeout	Patient 118	118	SOS	2	Emergency Call								
27.01.2025 14:13:45	3			New Event	Patient 118	118	SOS	2	Emergency Call								
27.01.2025 14:13:45	3	1		New Phase	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1				
27.01.2025 14:13:45	3	1	7	Notifiy	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Supervisor 1	120	SOS	
27.01.2025 14:13:45	3	1	8	Notifiy	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Caregiver 1	118	SOS	
27.01.2025 14:13:45	3	1	9	Notifiy	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Caregiver 2	119	SOS	
27.01.2025 14:13:47	3	1	7	Notification received	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Supervisor 1	120	SOS	
27.01.2025 14:13:47	3	1	8	Notification received	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Caregiver 1	118	SOS	
27.01.2025 14:13:51	3	1	7	Confirmed	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Supervisor 1	120	SOS	Rejected
27.01.2025 14:13:53	3	1	8	Confirmed	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Caregiver 1	118	SOS	Rejected
27.01.2025 14:16:45	3	1	9	Notification terminated	Patient 118	118	SOS	2	Emergency Call	root	SOS	Phase 1	1	Caregiver 2	119	SOS	Not received
27.01.2025 14:16:45	3			Event Finished: Timeout	Patient 118	118	SOS	2	Emergency Call								

DECT Lokalisierung

Einführung

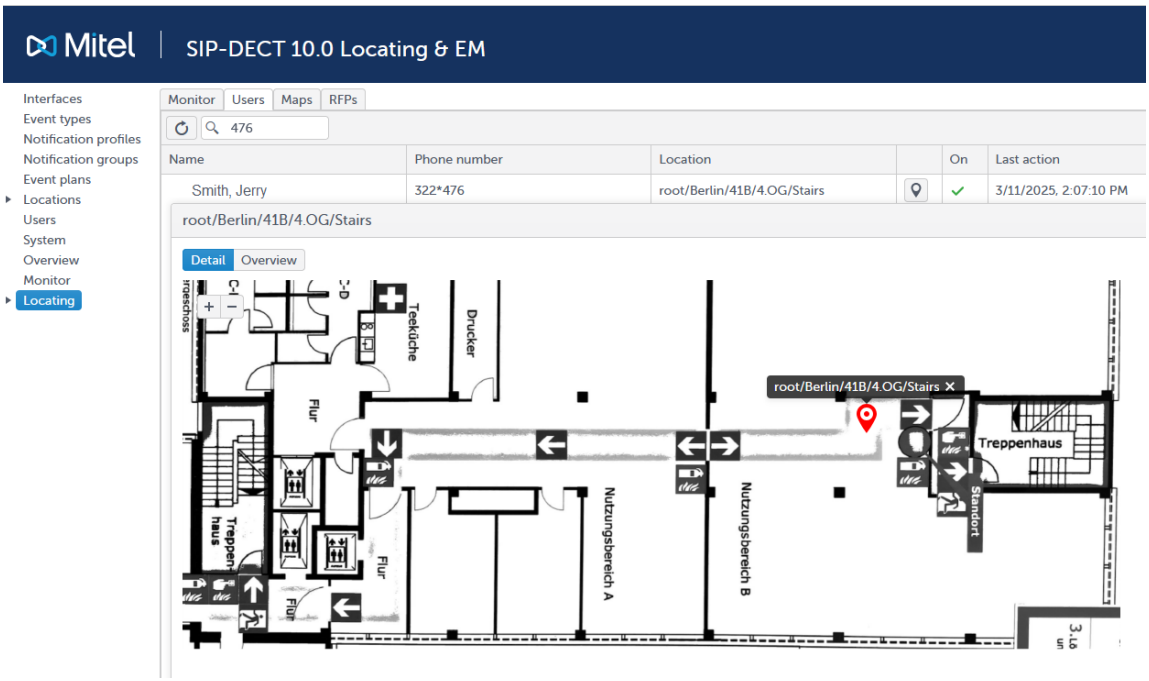
Der Event Manager DECT Lokalisierung ergänzt die oben beschriebene Event Manager Funktionalität um eine textliche und grafische Anzeige der Position eines DECT-Gerätes basierend auf der DECT-Funkabdeckung durch eine Basisstation (typischerweise je nach baulichen Gegebenheiten ca. 30 bis 50 Meter in Gebäuden und ca. 300 Meter im freien Feld) im Falle eines Notrufes, ausgelöst durch Drücken der SOS-Taste am Mitel DECT-Telefon (722dt, 732d, 742d, 632d(t V2)). im Falle eines Notrufes, ausgelöst durch Drücken der SOS-Taste am Mitel DECT-Telefon (722dt, 732d, 742d, 632d(t) V2) oder durch einen Sensor-Alarm des DECT-Gerätes (732d, 742d, 632d(t) V2) sowie Feature Access Codes für kundenspezifisch konfigurierbare Alarmauslöser. Darüber hinaus kann die Position eines ortbaren DECT-Gerätes auch unabhängig von einem Ereignis abgefragt werden.

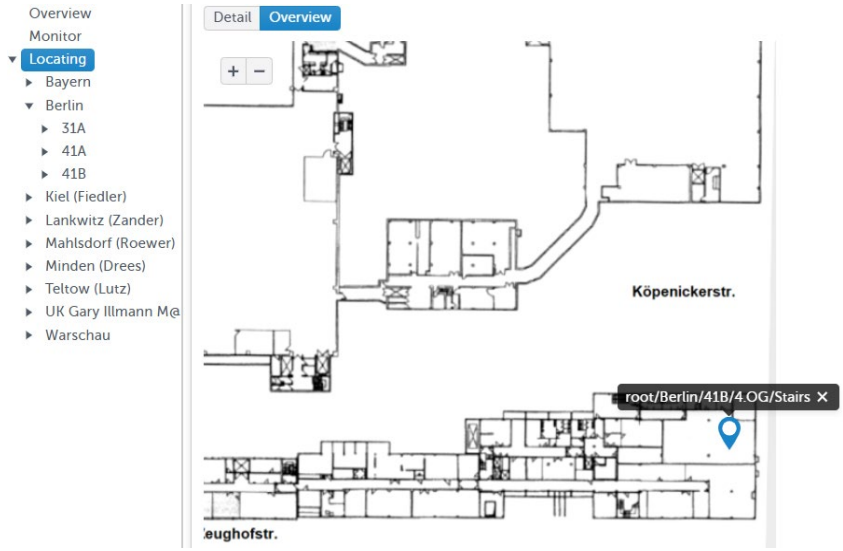
Die Hauptvoraussetzungen für die Ortungsanwendung sind:

- Installation des Event Managers auf einem Rocky-Linux-Server (in einer Microsoft® Hyper-V-Serverumgebung, einer VMware®-Umgebung oder in einer KVM/QEMU-basierten Virtualisierungsumgebung) mit dem Installationstyp EM.
- Upload einer Lokalisierungslizenz und der Lokalisierungslizenz für eine Anzahl lokalisierbarer DECT-Teilnehmer in den Open Mobility Manager
- Konfiguration der Attribute 'DECT locatable' (und 'Trackable') für diejenigen Benutzer, die von der Lokalisierungsanwendung verfolgt und/oder lokalisiert werden sollen
- Die Konfiguration erfordert die Bereitstellung von Gebäudeplänen und Grundrissen in Form von Grafikdateien (unterstützt werden die Dateiformate ".png" und ".jpg").

Da der Mitel CloudLink-Daemon für Serverinstallationen des Event Managers nicht zur Verfügung steht, ist die Fernverwaltung des Event Managers und der DECT Lokalisierungsanwendung in diesem Fall nicht möglich.

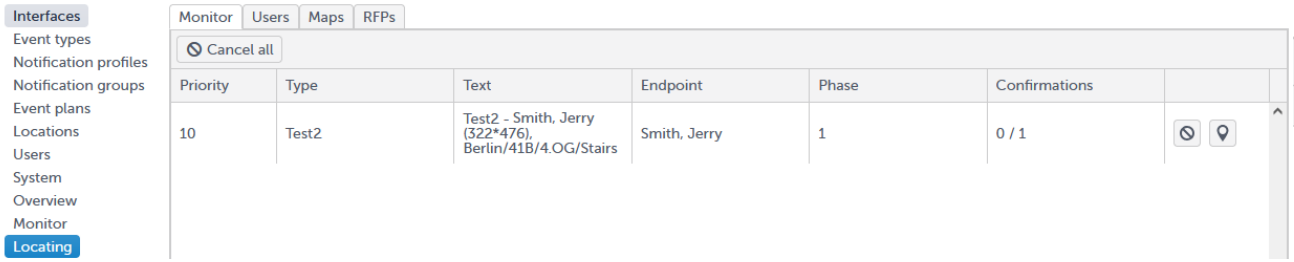
Die grafische Darstellung ist im Lokalisierungsmonitor und in der Lokalisierungsbenutzerliste in einer Detail- und in einer Übersichtsansicht verfügbar, wenn die Karten auf den Server hochgeladen wurden und die Standorte auf diesen Karten platziert wurden.



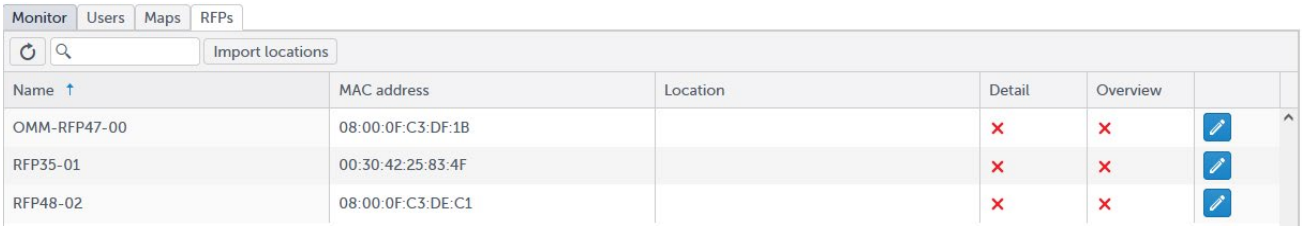


Schritte zur Konfiguration der Lokalisierungsanwendung

Die Konfiguration muss von einem Administrator-Benutzer des Event Managers durchgeführt werden. Der zusätzliche Menüpunkt **Lokalisierung**, eine neue Seite mit verschiedenen Registerkarten (Monitor, Benutzer, Karten und RFPs), ist nur verfügbar, wenn der Event Manager auf einem Linux-Server läuft und eine Lokalisierungslizenz im angeschlossenen SIP-DECT-System vorhanden ist.

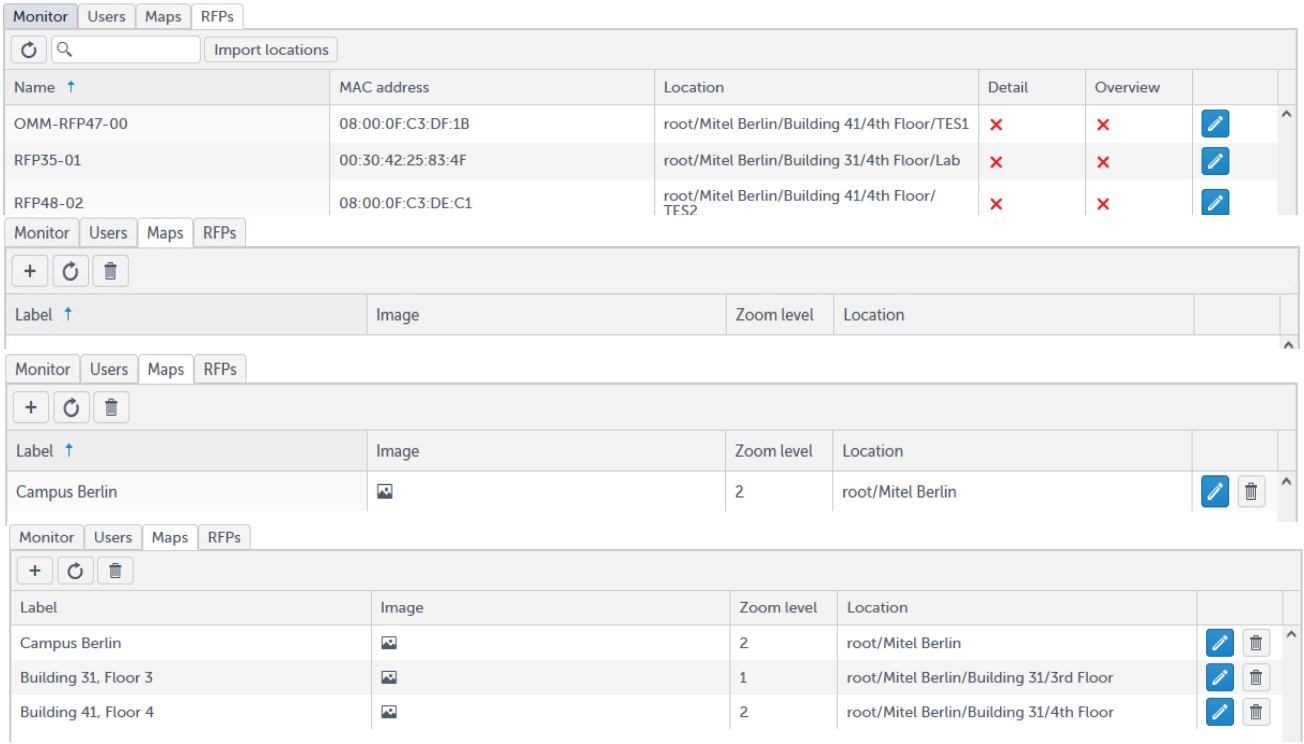


In der Registerkarte **RFPs** sind alle konfigurierten Radio Fixed Parts des SIP-DECT-Systems sichtbar. Sie werden automatisch in die Datenbank des Event Managers importiert. Die Tabelle enthält den Namen und die MAC-Adresse der Radio Fixed Parts, wie sie aus dem OMM importiert wurden.



Hier kann jedem Radio Fixed Part ein Standort zugewiesen werden oder über die Schaltfläche "Importiere Standorte" für alle RFP importiert werden. Das Ergebnis ist in der Abbildung unten zu sehen. Die roten Kreuze in den Spalten für "Detail" und "Übersicht" zeigen, dass diese Standorte derzeit weder auf einer Detail- noch auf einer Übersichtskarte positioniert sind.

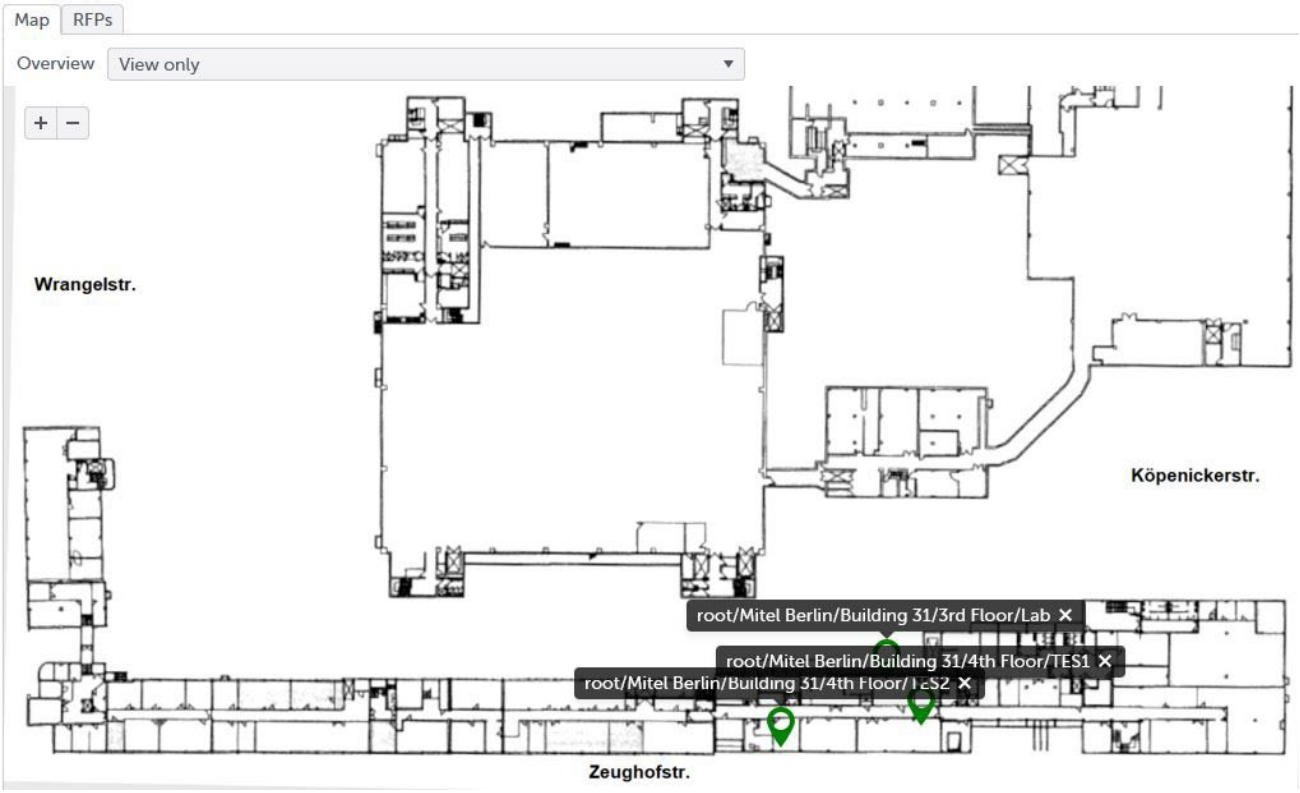
Im nächsten Schritt müssen diese notwendigen Karten über die Registerkarte **Karten** in den Event Manager hochgeladen werden. Es wird empfohlen, mindestens eine Übersichtskarte z.B. für den Campus und möglichst viele Detailkarten für spezielle Etagen oder Gebäudeteile hochzuladen. Unterstützte Grafikformate sind PNG und JPG mit Auflösungen von 1024, 2048, 4096 oder 8192 Pixel, was zu den Zoomstufen 1, 2, 3 oder 4 führt.



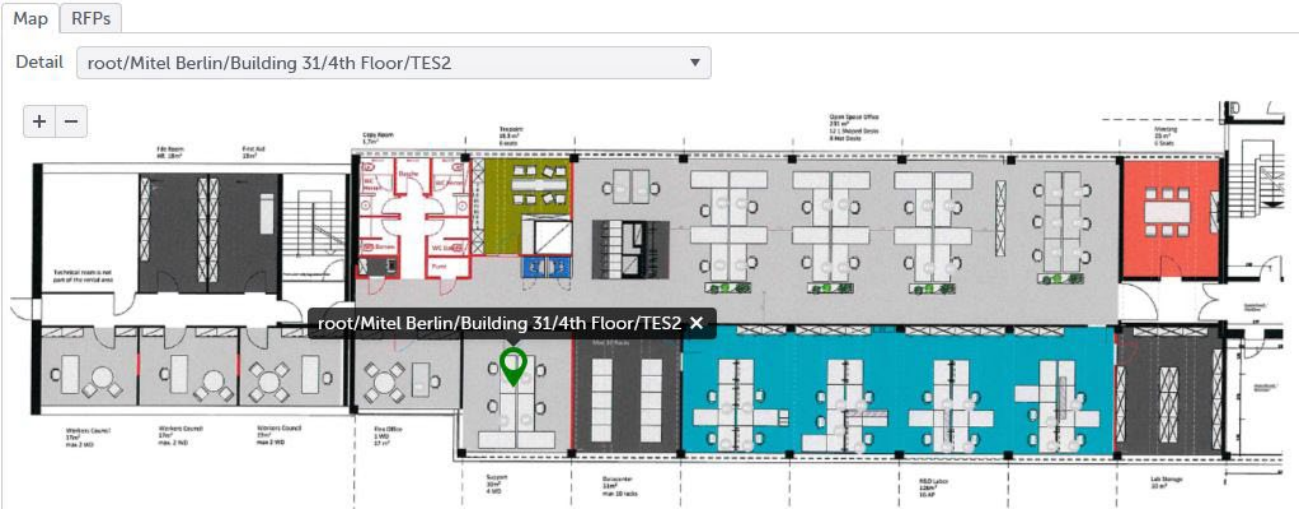
Während des Hochladens der Karten ist die direkte Zuordnung zu einem bestimmten Standort (bereits konfiguriert oder über die Registerkarte RFPs im Schritt zuvor importiert) möglich, andernfalls muss dies in einem separaten Schritt nach dem Kartenupload erfolgen. Als Ergebnis zeigt die endgültige Tabelle dann alle verfügbaren Karten mit Links zu den hochgeladenen Bildern, mit dem Wert der verfügbaren Zoomstufen (abhängig von der Auflösung der hochgeladenen Karten) und mit dem zugewiesenen Standort.

Nun müssen die Standorte noch auf den Karten positioniert werden. Dies geschieht im Standortbaum unterhalb des Menüeintrags "Lokalisierung" auf den verschiedenen Ebenen (im Beispiel von oben sind dies die Einträge "Campus Berlin" für die Übersicht und "Gebäude 31, 3. Etage" und "Gebäude 41, 4. Flur“.

Für die Übersicht müssen die entsprechenden Standorte schrittweise aus dem Dropdown-Menü ausgewählt und dann die Positionsmarkierung auf der Karte gesetzt werden. Am Ende sieht die Übersicht (nur Ansicht) wie im folgenden Bild aus.



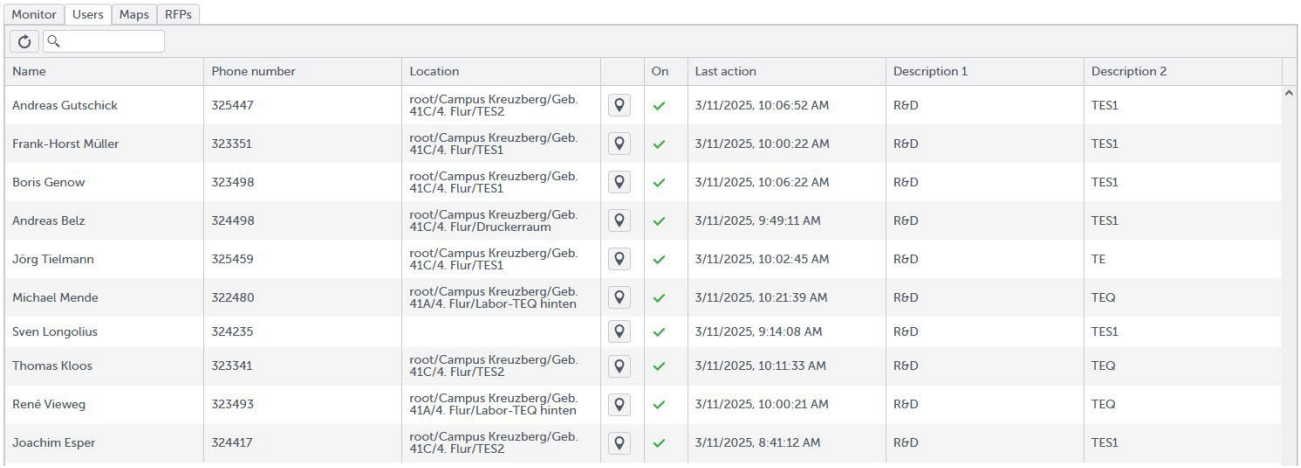
Eine ähnliche Handhabung ist für die Einstellung der Standortpositionen auf den Detailkarten erforderlich, z.B. für eine spezielle Etage.



Wenn alle Standorte mit ihren Positionsmarkierungen auf den Detail- und Übersichtskarten zugewiesen sind, zeigt die Tabelle auf der Registerkarte **RFPs** im Menüpunkt ‚Lokalisierung' nun grüne Häkchen in den Spalten für 'Detail' und 'Übersicht', wie im folgenden Bild zu sehen ist. Wenn in einer der Spalten immer noch ein rotes Kreuz anstelle eines grünen Häkchens zu sehen ist, bedeutet dies, dass die Standortmarkierung auf der genannten Karte für den betreffenden Standort noch fehlt.

Wenn alle Standorte die grünen Häkchen in den Spalten 'Detail' und 'Übersicht' haben, ist die Konfiguration abgeschlossen, und die Registerkarte 'Benutzer' im Menüeintrag 'Lokalisierung' zeigt nun die vollständige Liste all jener SIP-DECT-Benutzer, die im SIP-DECT-System mindestens mit dem Attribut 'DECT locatable' und eventuell auch mit dem Attribut 'Trackable' konfiguriert sind.

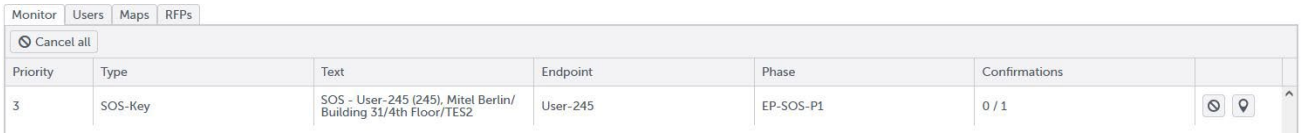
Die Tabelle enthält die Attribute "Name", "Telefonnummer", "Standort" (nur für verfolgbare Benutzer), einen grafischen Link zur Standortkarte, den Status des Benutzertelefons und den Zeitstempel der letzten Aktion sowie zwei aus dem SIP-DECT-System importierte Beschreibungsfelder mit Informationen wie Abteilung oder Team.



Name	Phone number	Location		On	Last action	Description 1	Description 2
Andreas Gutschick	325447	root/Campus Kreuzberg/Geb. 41C/4. Flur/TES2		✓	3/11/2025, 10:06:52 AM	R&D	TES1
Frank-Horst Müller	323351	root/Campus Kreuzberg/Geb. 41C/4. Flur/TES1		✓	3/11/2025, 10:00:22 AM	R&D	TES1
Boris Genow	323498	root/Campus Kreuzberg/Geb. 41C/4. Flur/TES1		✓	3/11/2025, 10:06:22 AM	R&D	TES1
Andreas Belz	324498	root/Campus Kreuzberg/Geb. 41C/4. Flur/Druckerraum		✓	3/11/2025, 9:49:11 AM	R&D	TES1
Jörg Tielmann	325459	root/Campus Kreuzberg/Geb. 41C/4. Flur/TES1		✓	3/11/2025, 10:02:45 AM	R&D	TE
Michael Mende	322480	root/Campus Kreuzberg/Geb. 41A/4. Flur/Labor-TEQ hinten		✓	3/11/2025, 10:21:39 AM	R&D	TEQ
Sven Longolius	324235			✓	3/11/2025, 9:14:08 AM	R&D	TES1
Thomas Kloos	323341	root/Campus Kreuzberg/Geb. 41C/4. Flur/TES2		✓	3/11/2025, 10:11:33 AM	R&D	TEQ
René Vieweg	323493	root/Campus Kreuzberg/Geb. 41A/4. Flur/Labor-TEQ hinten		✓	3/11/2025, 10:00:21 AM	R&D	TEQ
Joachim Esper	324417	root/Campus Kreuzberg/Geb. 41C/4. Flur/TES2		✓	3/11/2025, 8:41:12 AM	R&D	TES1

Der Inhalt der Tabelle wird automatisch durch die Aktionen der Benutzerhandys aktualisiert.

In der Registerkarte 'Monitor' des Menüeintrags 'Lokalisierung' wird zusätzlich zum 'normalen' Monitor ein Lokalisierungslink angezeigt, wenn ein Ereignis von einem lokalisierbaren Benutzer ausgelöst wird, z.B. bei einer SOS-Taste oder einem Man-Down-Alarm, ausgelöst an einem SIP-DECT-Telefon.



Priority	Type	Text	Endpoint	Phase	Confirmations	
3	SOS-Key	SOS - User-245 (245), Mitel Berlin/ Building 31/4th Floor/TES2	User-245	EP-SOS-P1	0 / 1	

Sicherung und Wiederherstellung der Event Manager-Daten einschließlich der installierten Grafikdateien

Die Event Manager-Datenbank, die über den EM-Webdienst gesichert und wiederhergestellt werden kann, enthält nicht die hochgeladenen Grafikdateien zum Auffinden, da die Grafikdateien sehr groß sein können.

Da jedoch eine Abhängigkeit zwischen den Konfigurationsdaten und den Grafikdateien besteht, müssen diese gemeinsam gesichert und wiederhergestellt werden, z. B. bei der Übertragung einer bestehenden Konfiguration auf eine neue Installation.

Außerdem sollte die EM-Anwendung während des Sicherungs- und Wiederherstellungsprozesses nicht laufen, um zu vermeiden, dass durch parallele Aktivitäten unerwünschte Inkonsistenzen entstehen.

Damit diese Prozesse nicht manuell durchgeführt werden müssen, stellt der Event Manager automatisch zwei Shell-Skripte zur Verfügung, die eine einfache Erstellung einer vollständigen Sicherung und eine Wiederherstellung ermöglichen. Beide Skripte müssen auf der Kommandozeilenschnittstelle vom Benutzer root ausgeführt werden.

Das Skript `sip-dect-em-create-backup.sh` wird verwendet, um eine Datensicherung zu erstellen. Das Skript benötigt als Argument ein Zielverzeichnis, in dem die Datensicherung gespeichert werden soll. Dieses Verzeichnis muss bereits existieren.

Die erzeugte Datei hat dann den Namen sip-dect-em-backup_<Zeitstempel>.tar.gz mit dem aktuellen Zeitstempel aus Datum und Uhrzeit z.B. 20250121_162259. Während der Ausführung des Skriptes wird der sip-dect-em-Dienst beendet, der Benutzer wird nochmals zur Bestätigung aufgefordert, um ein versehentliches Beenden zu verhindern. Nach Abschluss der Backup-Erstellung wird der sip-dect-em-Dienst automatisch neu gestartet.

```
[root@deberrndws5090 10.0]$ sip-dect-em-create-backup.sh  /root/Downloads/
User: root
OK, you are root
check service sip-dect-em:
active
The service 'sip-dect-em' is running. Would you like to stop it? (y/Y): y
Service sip-dect-em successfully stopped.
Create achive: /root/Downloads//sip-dect-em-backup_20250121_162259.tar.gz
…
Achive /root/Downloads//sip-dect-em-backup_20250121_162259.tar.gz created
Start service sip-dect-em
[root@deberrndws5090 10.0]$
```

Das Skript `sip-dect-em-restore-backup.sh` wird zur Wiederherstellung einer Datensicherung verwendet. Das Skript benötigt den Namen der Sicherungsdatei als erstes Argument und einen Zielpfad als zweites. Der Zielpfad ist immer das Stammverzeichnis /, es sei denn, Sie möchten, dass die Sicherung an einem anderen Ort entpackt wird.

```
[root@deberrndws5090 10.0]$ sip-dect-em-restore-backup.sh /root/Downloads/sip-dect-
em-backup_20250121_162259.tar.gz /
User: root
OK, you are root
OK. Unpack file /root/Downloads/sip-dect-em-backup_20250121_162259.tar.gz to target
directory /
check service sip-dect-em:
active
The service 'sip-dect-em' is running. Would you like to stop it? (y/Y): y
Service sip-dect-em successfully stopped.
retore backup from /root/Downloads/sip-dect-em-backup_20250121_162259.tar.gz to /
OK. Unpack file /root/Downloads/sip-dect-em-backup_20250121_162259.tar.gz to target
directory /
…
Start service sip-dect-em
[root@deberrndws5090 10.0]$
```

Um die Daten langfristig zu sichern, empfiehlt es sich, die Datensicherung auf ein externes Sicherungsmedium zu kopieren. Da auf den sicheren Virtualisierungs-Images keine weiteren Dienste vorinstalliert sind, muss hierfür ein externer Kopierprotokoll-Client, zum Beispiel SCP, verwendet werden.

Schnellstart-Konfigurationshandbuch SIP-DECT-Event-Manager

Die folgenden Schritte müssen befolgt werden, um eine grundlegende funktionierende Konfiguration zu erhalten. Es gibt zwei grundlegende Szenarien.

- Konfigurieren eines SOS-Alarmauslösers von einem DECT-Telefon
- Konfigurieren einer ESPA-Nachricht

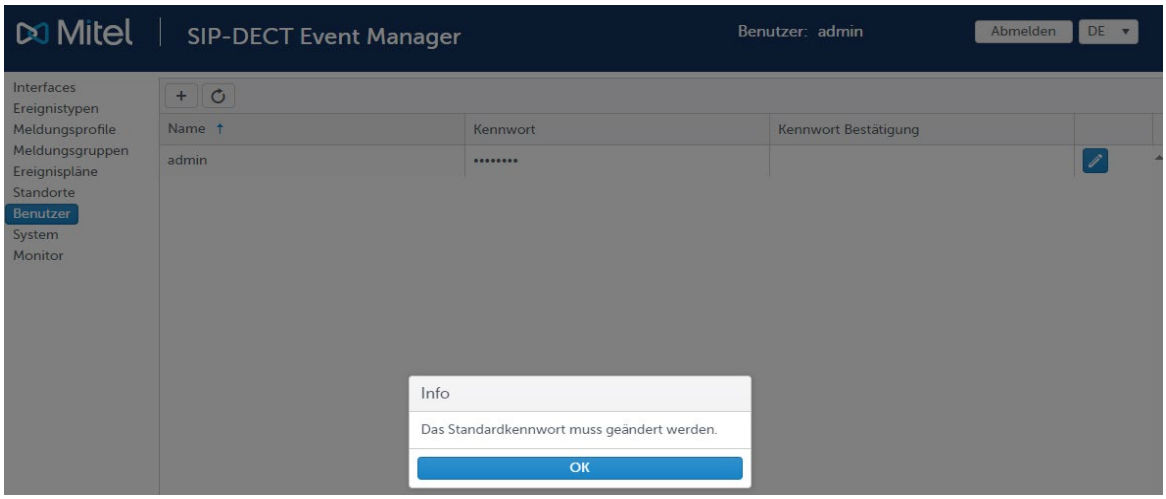
Voraussetzung für die folgenden Schritte ist eine funktionierende SIP-DECT-Installation mit mehreren Mitel DECT 602d v2 / 700d Telefonen. Die DECT-Telefone sind bereits auf die mit der SIP-DECT SW gelieferte SW aktualisiert.

Der SIP-DECT-Event-Manager wurde auf einem RFP mit dem OM Configurator (OMC) gestartet und hat die Standardkonfiguration.

Konfigurieren des SOS-Alarmauslösers von einem DECT-Telefon aus

1. Melden Sie sich beim SIP-DECT-Event-Manager-Webdienst an https://<RFP-IP-Adresse>:8444 mit dem Standard-Login "admin" und dem Passwort "admin".

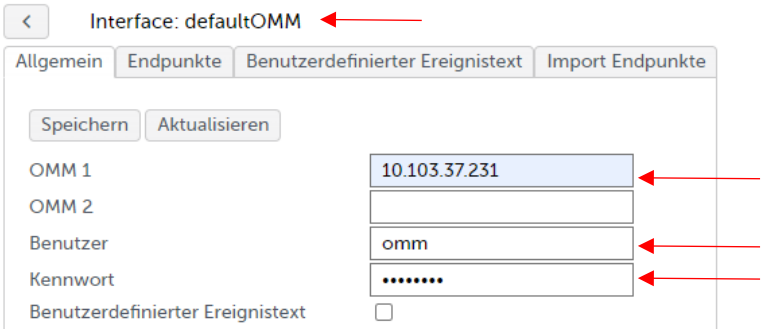
2. Ändern Sie das Standardkennwort.



3.

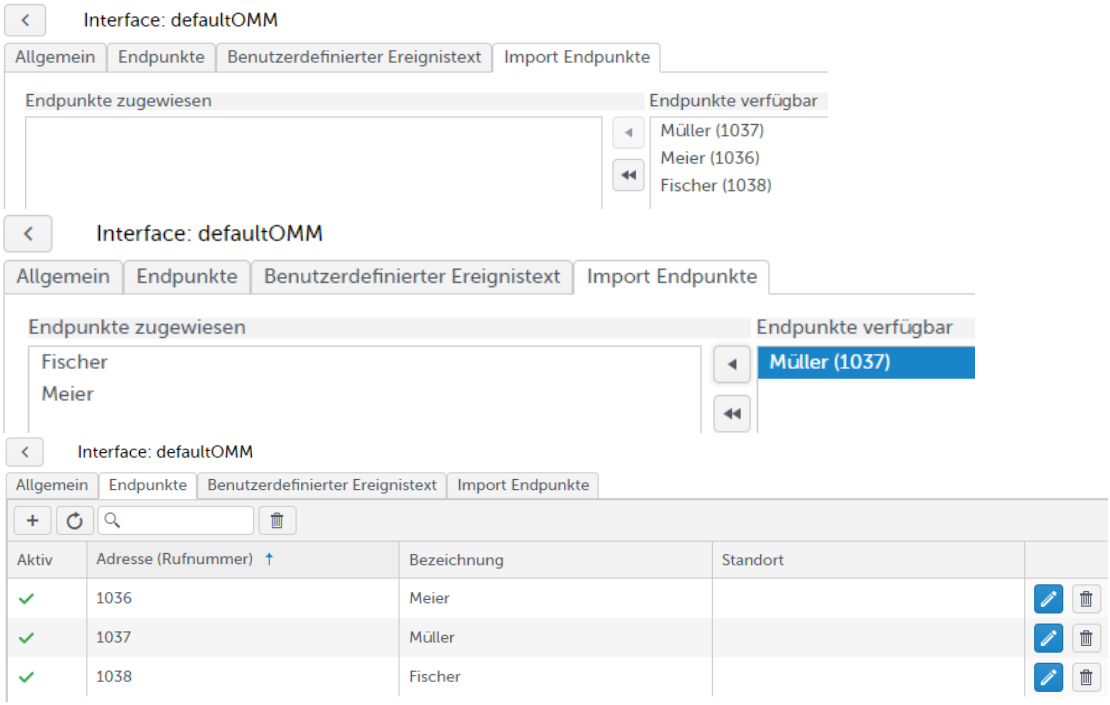
4. Öffnen Sie den Konfigurationsdialog für das OMM-Interface, indem Sie auf den unten gezeigten Link klicken.

5. Geben Sie die OMM-IP-Adresse(n), den Benutzer und das Passwort ein und bestätigen Sie mit Speichern. Kehren Sie zur Interface Übersicht zurück, indem Sie auf die Schaltfläche < klicken.



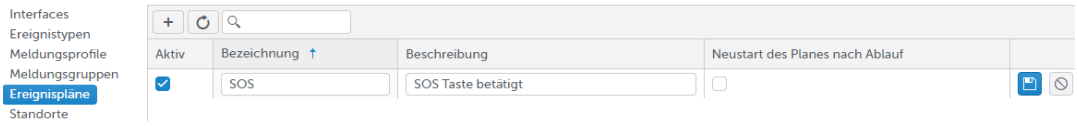
6. Der Interfacestatus sollte sich in Grün ändern, was darauf hinweist, dass der SIP-DECT-Event-Manager eine Verbindung mit dem OMM herstellen konnte.

7. Gehen Sie zurück in den Konfigurationsdialog des OMM-Interface, klicken Sie auf die Registerkarte Endpunkte importieren und übertragen Sie die SIP-DECT-Benutzer in die Konfiguration des SIP-DECT-Event-Managers, indem Sie einen nach dem anderen auswählen und auf ◂ oder auf ◂◂ um alle auf einmal zu importieren. Die Endpunkte werden anschließend in der Endpunktliste angezeigt.

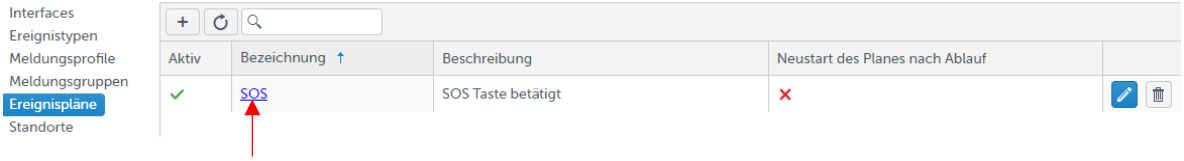


8. Weisen Sie die Endpunkte dem Standardstandort root zu, wie unten gezeigt.

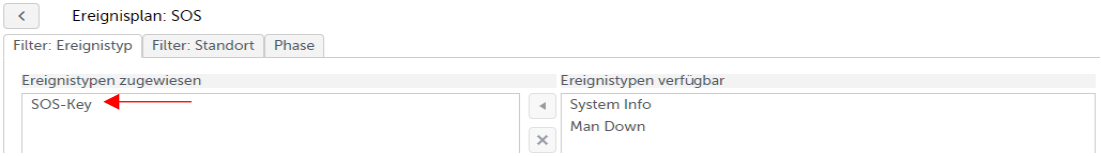
9. Klicken Sie auf den Konfigurationsbereich Ereignispläne, und erstellen Sie einen neuen Ereignisplan, indem Sie auf + klicken. Legen Sie den Namen und die Beschreibung fest und bestätigen Sie mit .



10. Klicken Sie auf den neu erstellten Plan.

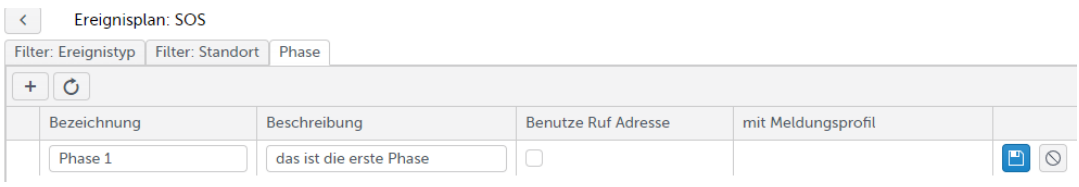


11. Fügen Sie auf der Registerkarte Filter: Ereignistyp den Standardereignistyp SOS-Key zum Ereignistypfilter hinzu.

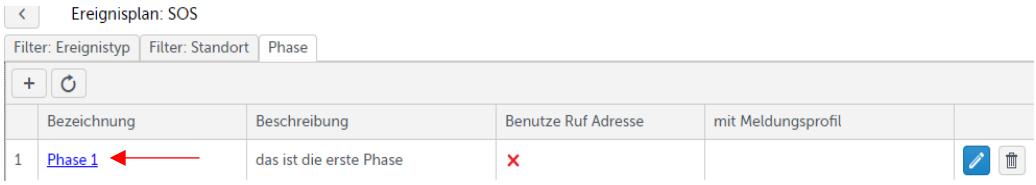


12. Klicken Sie auf die Registerkarte Filter: Standort und fügen Sie dem Standortfilter den Standardstandort root hinzu.

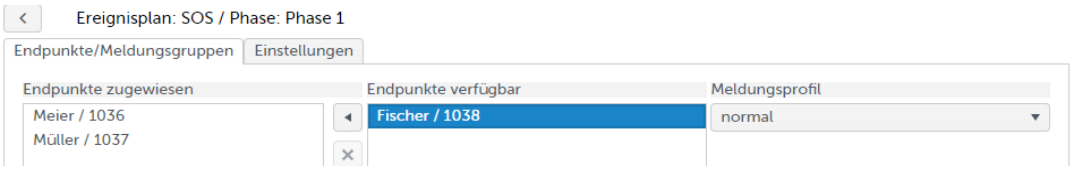
13. Klicken Sie auf die Registerkarte Phase, und erstellen Sie eine Phase für den Ereignisplan, indem Sie auf Neu klicken. Legen Sie den Namen und die Beschreibung fest und bestätigen Sie mit .



14. Öffnen Sie das Dialogfeld Phasenkonfiguration, indem Sie auf den Link klicken, wie unten gezeigt.



15. Übertragen Sie die Endpunkte, die Sie benachrichtigen möchten, in die Endpunktliste, indem Sie einen nach dem anderen auswählen und auf klicken. Das Standard-Meldungsprofil normal wird automatisch zugewiesen.



16. Es müssen keine weiteren Phaseneinstellungen geändert werden. Kehren Sie zum Dialogfeld der Hauptebene zurück, indem Sie drücken.

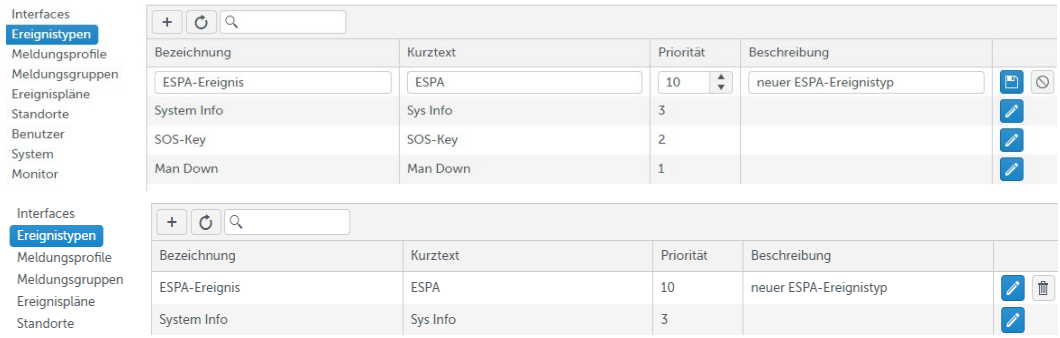
17. Wenn die SOS-Taste auf einem der Mitel DECT-Telefone (im Beispiel unten von SDT-204-742d mit der Nummer 204) gedrückt wird, sollte nun eine Benachrichtigung auf den Telefonen erscheinen, die dem Ereignisplan zugewiesen wurden.

ESPA-Interface konfigurieren

Führen Sie die gleichen Schritte aus, um das ESPA-Interface einzurichten wie im Abschnitt Konfigurieren des SOS-Alarmauslösers eines DECT-Telefons beschrieben. Bevor ein neuer Ereignisplan erstellt werden kann, muss das ESPA-Interface eingerichtet und ein neuer Ereignistyp angelegt werden.

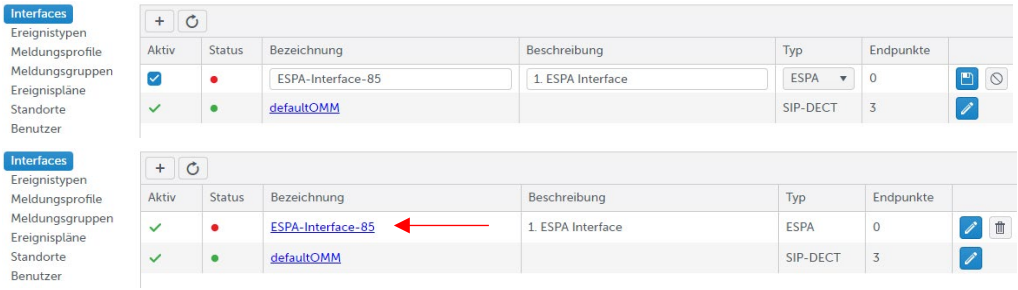
1. Klicken Sie auf den Konfigurationsbereich Ereignistypen.

2. Fügen Sie einen neuen Eintrag hinzu, indem Sie auf + klicken. Legen Sie eine eindeutige Beschriftung und einen Kurztext fest und bestätigen Sie mit .



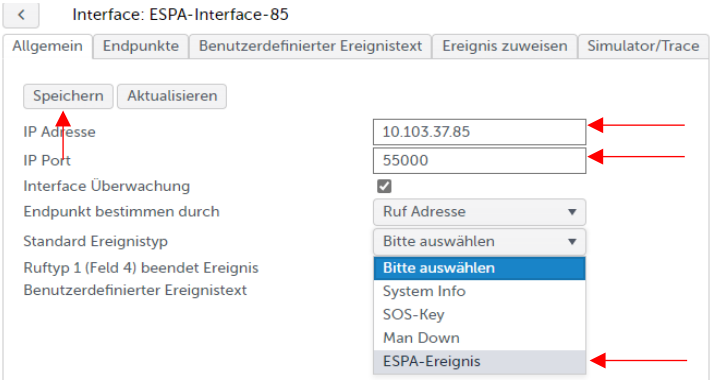
3. Klicken Sie auf den Konfigurationsbereich Interfaces.

4. Fügen Sie einen neuen Eintrag hinzu, indem Sie auf + klicken. Legen Sie eine eindeutige Bezeichnung und Beschreibung fest und bestätigen Sie mit . Stellen Sie sicher, dass unter Typ der Interfacetyp ESPA ausgewählt ist.



5. Öffnen Sie den Dialog Interfacekonfiguration, indem Sie auf den Link klicken.

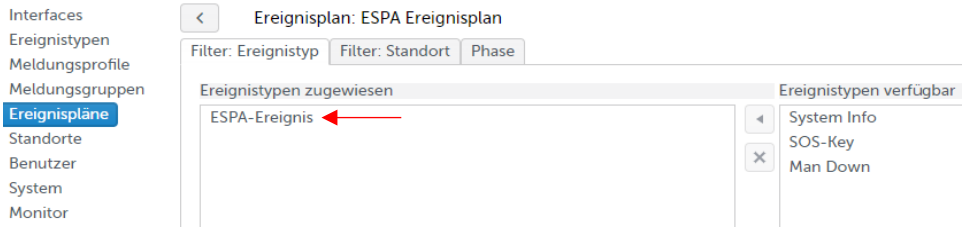
6. Geben Sie die IP-Adresse und den Port ein, mit dem sich der ESPA 4.4.4 des SIP-DECT-Event-Managers verbinden soll, wählen Sie den gerade erstellten Ereignistypen aus und bestätigen Sie mit Speichern.



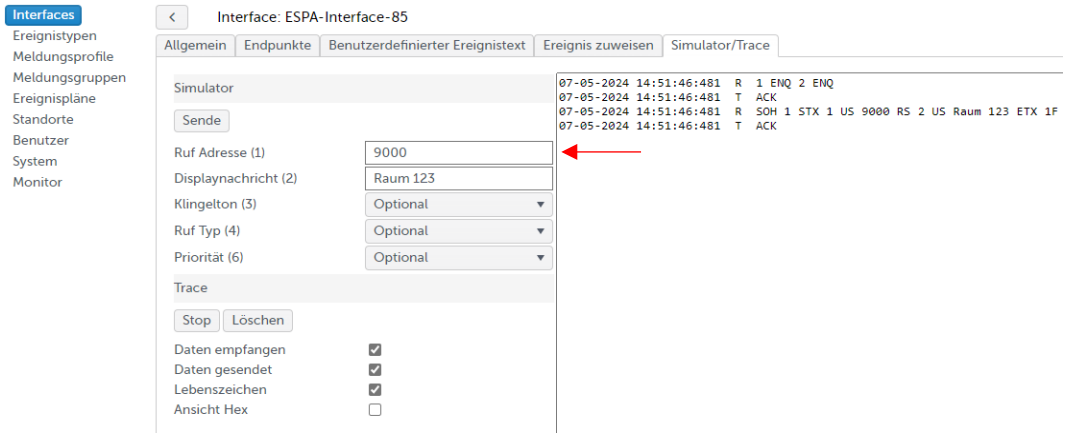
7. Fügen Sie auf der Registerkarte Endpunkte einen ESPA-Endpunkt hinzu. Legen Sie die Endpunktadresse fest (ESPA-Feld 1 – Anrufadresse), vergeben Sie einen Namen und den Standardstandortstamm und bestätigen Sie mit .

8. Kehren Sie zur Interfaceübersicht zurück, indem Sie auf klicken. Wenn sich der SIP-DECT-Event-Manager mit dem Schwesternrufsystem o.ä. verbinden konnte, wechselt der Interfacestatus auf grün.

9. Erstellen Sie einen Ereignisplan. Führen Sie die Schritte 8 bis 15 aus, wie im Abschnitt Konfigurieren des SOS-Alarmauslösers von einem DECT-Telefon beschrieben. Dieses Mal sollte jedoch der neu erstellte Ereignistyp des ESPA-Interfaces als zu verwendender Standard-Ereignistyp zugewiesen werden.



10. Um ein Ereignis auch ohne angeschlossenes System auszulösen, steht die Simulator-Funktion des ESPA-Interfaces zur Verfügung.



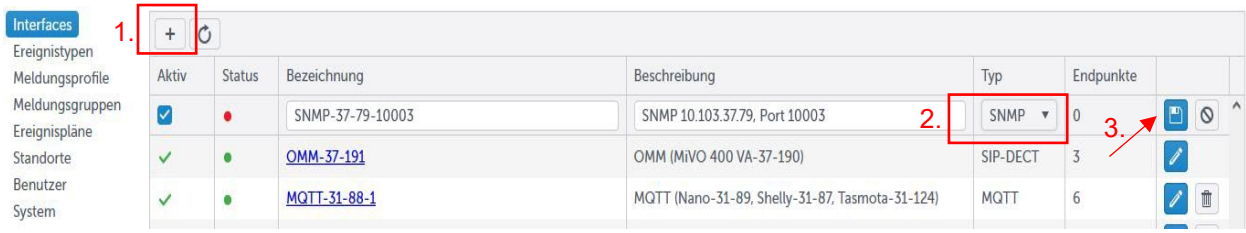
11. Wenn eine ESPA-Nachricht empfangen wird, sollte nun eine Benachrichtigung mit der empfangenen Textnachricht auf den Mitel DECT-Telefonen erscheinen, die dem Ereignisplan zugewiesen sind.


Normale Nachricht
Raum 123
14.04.25
14:15
Esc

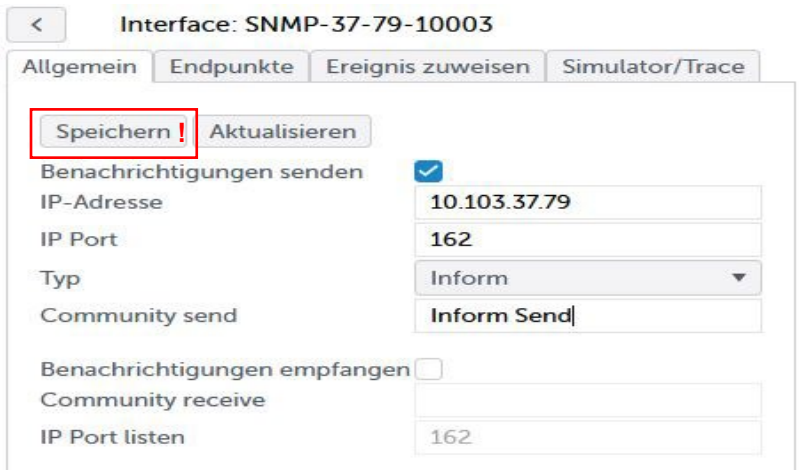
Konfigurieren einer SNMP-Schnittstelle

In diesem Kapitel wird Schritt für Schritt erklärt, wie eine SNMP-Schnittstelle zum Senden und Empfangen von Traps und Inform-Requests konfiguriert wird. Bevor Sie dieser Anleitung folgen, stellen Sie sicher, dass Sie eine funktionierende SIP-DECT-Schnittstelle mit Endpunkten haben. Als Beispiel für einen Trap-Sender, dessen Benachrichtigungen der Event Manager empfängt und verarbeitet, wird der Inveo Nano Temperatursensor verwendet.

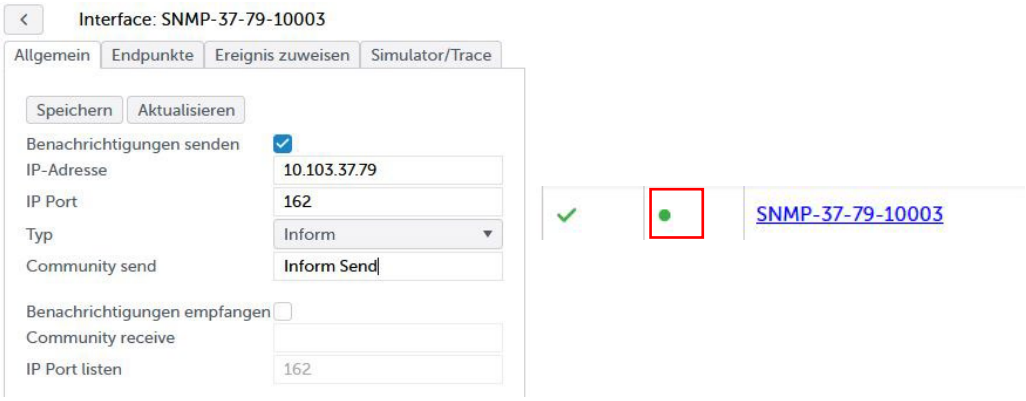
1. Öffnen Sie den Dialog "Schnittstellen". Erstellen und benennen Sie eine neue SNMP-Schnittstelle. Vergewissern Sie sich, dass die Schnittstelle auf aktiv gesetzt ist.



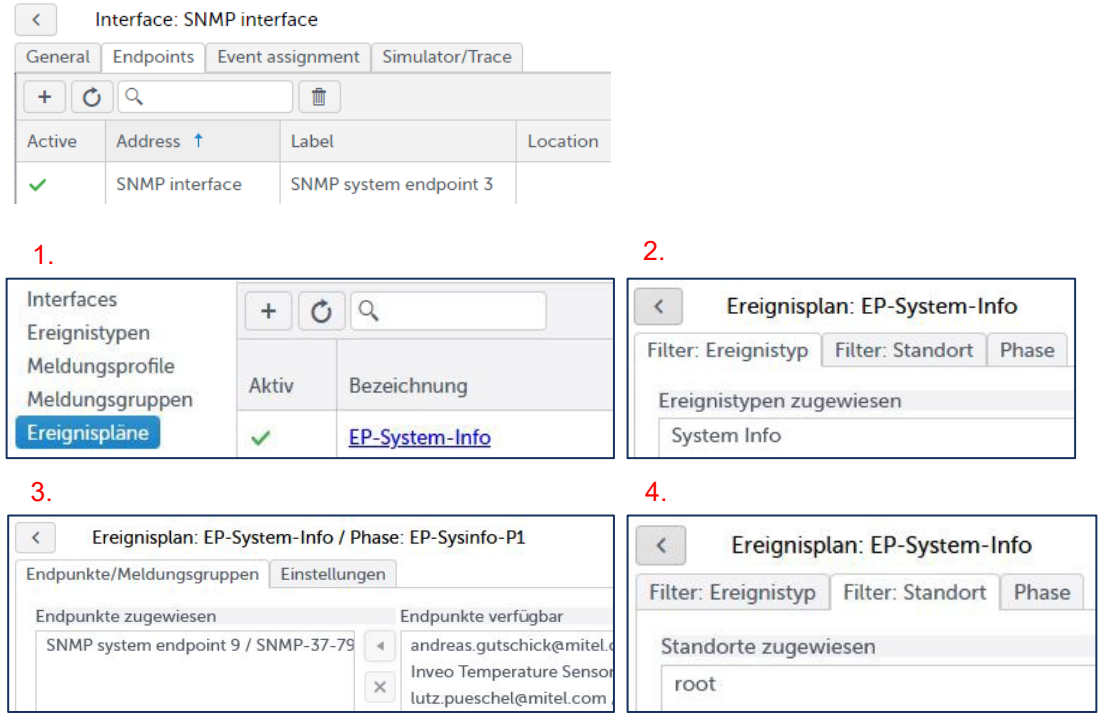
2. Klicken Sie auf den Namen der neu erstellten SNMP-Schnittstelle. Sie sollten sich nun auf der Registerkarte "Allgemein" befinden. Aktivieren Sie das Kontrollkästchen "Benachrichtigung senden" und geben Sie die IP-Adresse und den IP-Port des Trap-Empfängers, an den Sie Traps senden möchten, in die entsprechenden Felder ein. Wählen Sie im Dropdown-Menü "Typ" aus, ob Sie Inform-Requests oder einfache Traps senden möchten, und geben Sie im Feld "Community send" eine gültige Community-Zeichenfolge ein. Vergewissern Sie sich, dass das Kästchen "Benachrichtigungsempfang" vorerst nicht angekreuzt ist. Klicken Sie auf die Schaltfläche "Speichern" oben links..



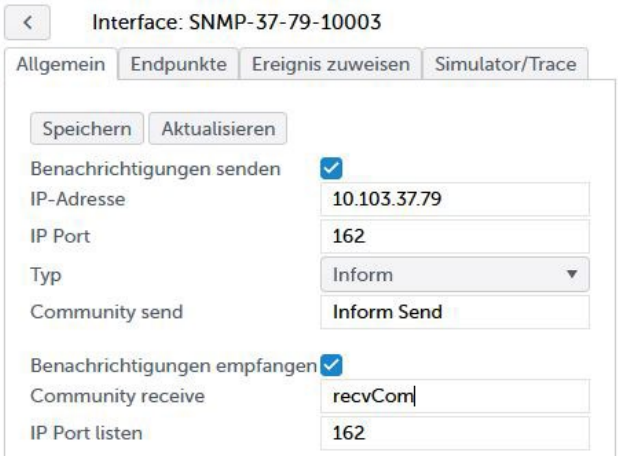
3. Klicken Sie auf den Pfeil oben links. Sie sollten sich nun wieder in dem Dialog "Schnittstellen" vom Anfang befinden. Stellen Sie sicher, dass der Status der SNMP-Schnittstelle jetzt aktiv (grün) ist. Wenn Sie etwas falsch gemacht oder vergessen haben zu speichern, sollte sie entweder rot (inaktiv) oder gelb (falsch konfiguriert) sein. Wenn er grün ist, fahren Sie mit den nächsten Anweisungen fort. Wenn er eine andere Farbe hat, wiederholen Sie 2.



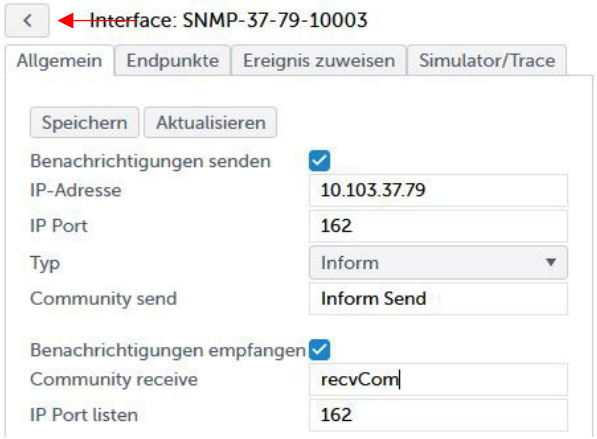
4. Nachdem Sie auf den Namen der SNMP-Schnittstelle geklickt und deren Konfigurationsfenster geöffnet haben, klicken Sie auf die Registerkarte "Endpunkte". Ein Endpunkt mit der Bezeichnung "SNMP-Systemendpunkt X" (wobei X eine Zahl ist) sollte dort zu finden und aktiv sein. Wenn er nicht aktiv ist, überprüfen Sie, ob Sie auf der Registerkarte "Allgemein" das Kontrollkästchen "Benachrichtigung senden" aktiviert haben. Wenn Sie möchten, dass die SNMP-Schnittstelle Traps/Inform-Requests sendet, müssen Sie diesen Systemendpunkt in die Phase eines Ereignisplans aufnehmen. Wenn dieser Ereignisplan durch ein Ereignis ausgelöst wird und die Phase mit dem SNMP-Systemendpunkt darin erreicht, sendet die Schnittstelle eine Benachrichtigung an ihr konfiguriertes Ziel. In diesem Beispiel fügen wir den SNMP-Systemendpunkt in einen Ereignisplan an der Position "root" ein, der durch den vordefinierten Ereignistyp "System Info" ausgelöst wird. Dies führt dazu, dass unsere SNMP-Schnittstelle interfaceStatusChange-Benachrichtigungen sendet, wenn eine Schnittstelle ihren Status ändert.



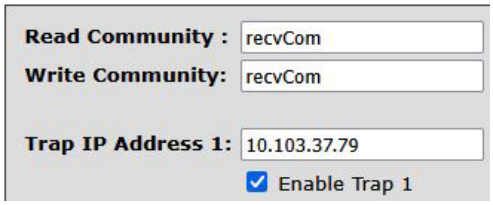
5. Als nächstes werden wir den Empfang und die Verarbeitung von Benachrichtigungen konfigurieren. Dazu gehen wir wieder auf die Registerkarte "Allgemein" unserer SNMP-Schnittstelle. Aktivieren Sie das Kontrollkästchen "Benachrichtigungsempfang", geben Sie in das Textfeld "Community receive" den Community-String ein, den wir erwarten, und tragen Sie in das Feld "IP port listen" den IP-Port ein, an dem diese SNMP-Schnittstelle auf Benachrichtigungen warten soll. Drücken Sie "Speichern".



6. Verlassen Sie die Registerkarte "Allgemein" über den Pfeil oben links. Prüfen Sie im Schnittstellenübersichtsfenster, ob die SNMP-Schnittstelle noch aktiv ist (grün). Wenn sie aktiv ist, fahren Sie mit den nächsten Anweisungen fort. Wenn sie rot (inaktiv) ist, bedeutet dies, dass der IP-Port, den Sie zum Abhören konfigurieren wollten, bereits von einem anderen Prozess oder einer anderen Schnittstelle belegt ist. Er kann nicht verwendet werden. Geben Sie die Konfiguration der SNMP-Schnittstelle erneut ein, wählen Sie einen anderen Port und drücken Sie auf "Speichern". Überprüfen Sie den Status der Schnittstelle erneut. Wiederholen Sie den Vorgang, bis die SNMP-Schnittstelle aktiv (grün) ist.

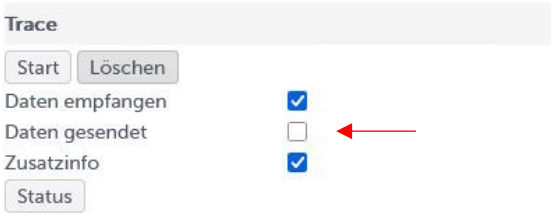


7. Konfigurieren Sie nun das Gerät, von dem Sie Benachrichtigungen erhalten möchten, so, dass es Traps/Inform-Requests an die SNMP-Schnittstelle des Event Managers senden kann. In diesem Beispiel konfigurieren wir den Inveo Nano Temperatursensor so, dass er Traps sendet. Dieser Schritt kann in Ihrem Anwendungsfall mit Ihrem Gerät ganz anders aussehen. Bitte befolgen Sie die Anweisungen des Herstellers des Geräts, das Sie konfigurieren, und bitten Sie ihn um Hilfe, wenn Sie auf Probleme stoßen. Vergewissern Sie sich, dass die Trap-Community, die das sendende Gerät sendet, mit derjenigen übereinstimmt, die in der SNMP-Schnittstelle des Event Managers im Feld "Community receive" konfiguriert wurde.



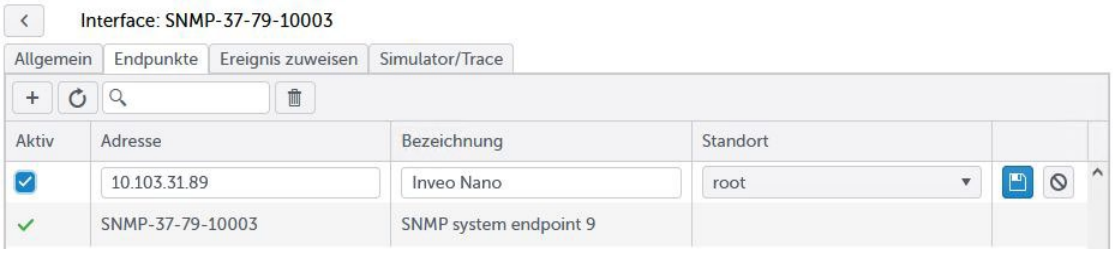
8. Um die empfangenen SNMP-Benachrichtigungen zu verarbeiten, muss ein Endpunkt mit der IP-Adresse des Absenders sowie eine Ereigniszuweisung erstellt werden, die auf den richtigen Object Identifier (OID) reagiert. Wenn Sie die IP-Adresse Ihres SNMP-Benachrichtigungssenders bereits kennen und wissen, welche OIDs er in seinen Benachrichtigungen sendet, können Sie Schritt 9 überspringen.

9. Um empfangene SNMP-Benachrichtigungen zu verarbeiten, muss ein SNMP-Endpunkt mit der IP-Adresse des Absenders sowie eine passende Ereigniszuordnung erstellt werden. Um diese einfach herauszufinden, gehen Sie in der SNMP-Schnittstelle auf den Reiter "Simulator/Trace". Kreuzen Sie die Kästchen für "Data received" und "Additional info" an und entfernen Sie das Häkchen bei "Data sent" ganz unten unter der Überschrift "Trace". Drücken Sie nun "Start". Das Trace-Fenster auf der rechten Seite zeigt nun alle auf dieser Schnittstelle eingehenden Benachrichtigungen an. Um die IP-Adresse des sendenden Geräts sowie die OIDs, die es in seinen gesendeten SNMP-Benachrichtigungen angibt, herauszufinden, lassen Sie es eine Benachrichtigung an den Event Manager senden, lesen Sie die angezeigte IP-Adresse aus und entscheiden Sie, welcher OID Sie ein Ereignis zuordnen möchten. Der Event Manager ist nicht in der Lage zu wissen, was ein empfangener Object Identifier bedeutet. Diese Information ist in den MIB-Dateien des benachrichtigenden Geräts enthalten und muss von Ihnen selbst ausgelesen werden. In diesem Beispiel enthält die OID ".1.3.6.1.4.1.42814.3.5.2.0" die aktuelle Temperatur, die vom Inveo Nano Temperatursensor gesendet wird, wenn er je nach Konfiguration zu heiß oder zu kalt ist. Wenn Sie fertig sind, drücken Sie "Stop", um die Trace-Funktion zu deaktivieren.



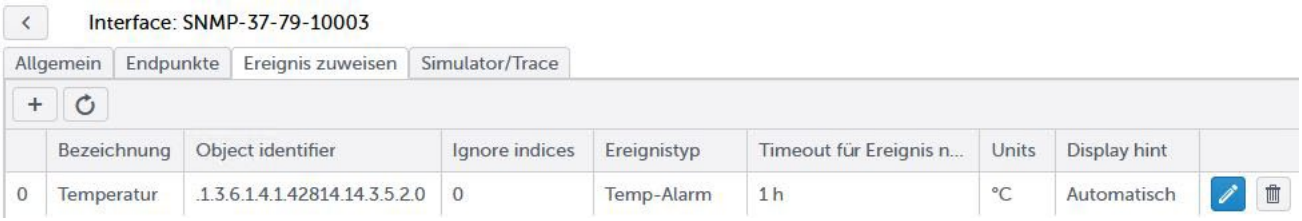

```
08-01-2025 09:40:40:358
Sender: 10.103.31.89, Endpoint: NO ENDPOINT!
Community: recvCom, Version: v2c, Type: Trap-v2
IN   <-  1 - [                          .1.3.6.1.2.1.1.3.0]: Timeticks: (133422) 0:22:14.22
IN   <-  2 - [                     .1.3.6.1.6.3.1.1.4.1.0]: OID: .1.3.6.1.4.1.42814.14
IN   <-  3 - [              .1.3.6.1.4.1.42814.14.3.5.2.0]: INTEGER: 22
Could not find an endpoint with a matching IP address on this SNMP interface.
```

10. Da wir nun die IP-Adresse des Senders haben, erstellen wir auf der Registerkarte "Endpunkte" innerhalb der SNMP-Schnittstelle einen SNMP-Endpunkt mit der IP-Adresse im Feld "Adresse" und einer leicht erkennbaren Bezeichnung. Außerdem weisen wir ihm den Standort "root" zu. Sie können ihn aber auch einem anderen, passenderen Standort, zuordnen.

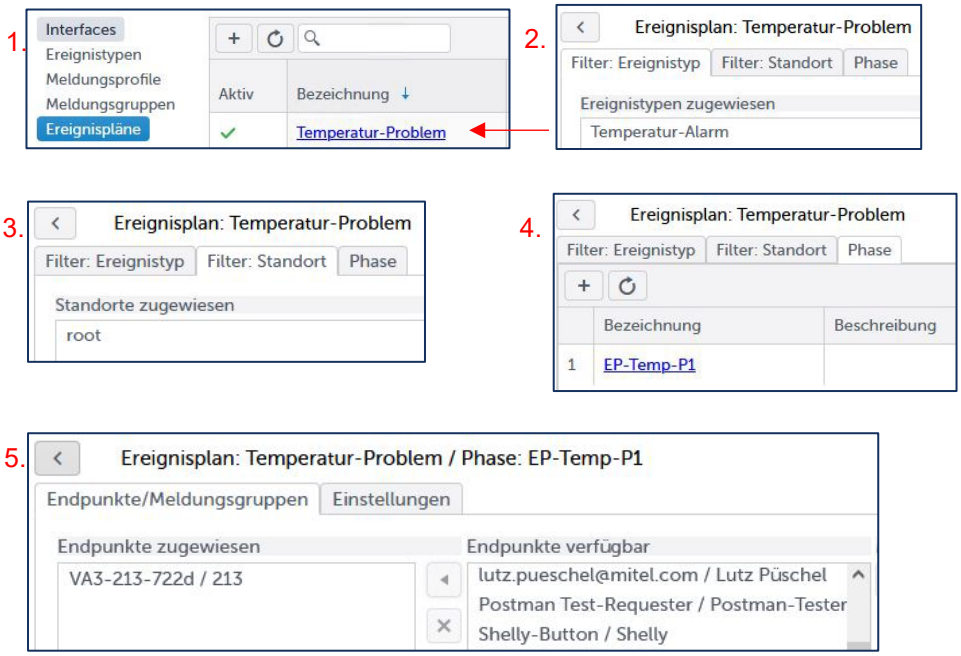


11. Erstellen Sie einen neuen Ereignistyp, der zu den Informationen passt, die Sie vom SNMP-Benachrichtigungssender erhalten.

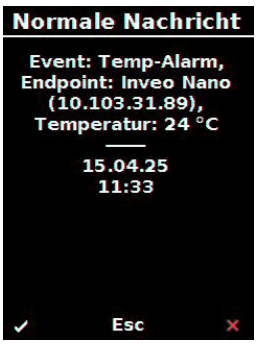
12. Erstellen Sie eine Ereigniszuweisung mit dem richtigen Object Identifier. Hinweis: Die ersten beiden OIDs einer SNMPv2-Notification sind bei allen SNMPv2-Notifications gleich. Das Erstellen einer Ereigniszuweisung, die mit den ersten beiden OIDs sysUpTime und snmpTrapOID (.1.3.6.1.2.1.1.3.0 & .1.3.6.1.6.3.1.1.4.1.0) übereinstimmt, wird daher mit ALLEN korrekten v2-Meldungen übereinstimmen. Da immer die erste übereinstimmende Ereigniszuweisung gewählt wird, würde dies dazu führen, dass alle SNMP-Benachrichtigungen das gleiche Ereignis auslösen. Deshalb wählen wir hier erst die dritte OID der empfangenen Meldung als Objekt-Identifikator.



13. Fügen Sie einen Ereignisplan an jenem Standort hinzu, dem Sie den Endpunkt zugewiesen haben ("root" in diesem Beispiel). Dieser Ereignisplan sollte auf den Ereignistyp reagieren, den Sie auf der Registerkarte "Ereigniszuweisung" der SNMP-Schnittstelle verwendet haben. Fügen Sie dem Ereignisplan eine Phase sowie SIP-DECT-Telefone als Empfänger innerhalb dieser Phase hinzu.



14. Sobald der Absender der SNMP-Benachrichtigung einen Trap/Inform-Request an uns sendet und alles korrekt eingerichtet wurde, sollte die folgende Meldung in SIP-DECT-Telefonen angezeigt werden, die einer Phase des neu erstellten Ereignisplans zugeordnet sind.



15. Sollte dies nicht der Fall sein, können Sie die Registerkarte "Simulator/Trace" der SNMP-

Schnittstelle aufrufen, unter "Trace" die Kästchen "Data received" und "Additional Info" ankreuzen und den Trace starten. Sobald eine SNMP-Meldung empfangen wurde, wird nach der empfangenen Meldung eine Meldung angezeigt, die Ihnen mitteilt, was bei der Verarbeitung der Meldung geschehen ist. Dies kann ein Hinweis darauf sein, was beim Einrichten der SNMP-Schnittstelle schiefgelaufen ist. Wenn die Meldung besagt, dass alles gut gelaufen ist, Sie aber immer noch keine Meldung im gewünschten SIP-DECT-Telefon sehen, kann das Problem in der SIP-DECT-Schnittstelle oder in dem von Ihnen eingerichteten Ereignisplan liegen.

Anhang

Sitemap

Die folgende Tabelle bietet einen Überblick über die Struktur des Event Manager-Webdienstes.

Interfaces				
	SIP-DECT-Interface			
		Allgemein		
		Endpunkte		
		Benutzer-definierter Ereignistext		
			Textersetzung	
			Struktur des Ereignistextes	
		Import Endpunkte		
			Endpunkte zugewiesen	
			Endpunkte verfügbar	
	ESPA-Interface			
		Allgemein		
		Endpunkte		
		Benutzer-definierter Ereignistext		
			Textersetzung	
			Struktur des Ereignistextes	
		Ereignis zuweisen		
		Simulator/ Trace		
			Simulator	
			Trace	
	SNMP-Interface			
		Allgemein		
	Interface Modbus	Allgemein		
		Endpunkte		
			Endpunkte konfigurieren	
		Simulator / Trace		
			Eingänge	
			Ausgänge	
	Interface MQTT	Allgemein		
		Endpunkte		
			Endpunkte konfigurieren	

		Benutzer-definierter Ereignistext		
			Textersetzung	
			Struktur des Ereignistextes	
		Topics		
		Subscribe mapping		
		Publish mapping		
		Trace		
	Interface Web-API			
		Allgemein		
		Endpunkte		
Ereignistypen				
Meldungsprofile				
	SIP-DECT Profile			
Meldungsgruppen				
	Meldungsgruppe			
		Endpunkte zugewiesen		
		Endpunkte verfügbar		
Ereignispläne				
	Plan			
		Filter: Ereignistyp		
			Ereignistypen zugewiesen	
			Ereignistypen verfügbar	
		Filter: Standort		
			Standorte zugewiesen	
			Standorte verfügbar	
		Phase		
			Endpunkte/ Meldungsgruppen	
				Endpunkte zugewiesen
				Endpunkte verfügbar
				Meldungs-gruppen zugewiesen
				Meldungs-gruppen verfügbar

			Einstellungen	
Standorte				
	Standort			
		Endpunkte zugewiesen		
		Endpunkte verfügbar		
Benutzer				
	Name			
	Berechtigung			
	Kennwort			
	Kennwort Bestätigung			
System				
	Allgemein			
	Datensicherung/ Neustart			
	Sicherheit			
	Sicherheitsstufen	Sicherheitsstufe		
		Cipher suites	Benutzte Cipher suites	
			Unterstützte Cipher suites	
	CloudLink			
Übersicht				
Monitor				

Übersicht über Web-UI-Parameter, Aktions- und Statusinformationen

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
Interfaces	Konfigurationsbereich zur Verwaltung der Interfaces des Event Managers. Es werden bis zu 5 Interfaces unterstützt. Es gibt immer ein SIP-DECT-Interface, die nicht gelöscht werden kann. Es können bis zu 4 eingehende ESPA-Interfaces konfiguriert werden.	
	Aktiv	Schalter zum Aktivieren oder Deaktivieren des Interfaces
	Status	Zeigt den Status des Interfaces an (läuft, falsch konfiguriert, inaktiv)
	Bezeichnung	Name zur Identifizierung des Interfaces
	Beschreibung	Zusatzinformation
	Typ	SIP-DECT, ESPA, SNMP, MODBUS
	Endpunkte	Zeigt die Anzahl der konfigurierten Endpunkte für das Interface an. Insgesamt werden bis zu 2000 Endpunkte über alle Interfaces hinweg unterstützt.
Typ SIP-DECT	Es gibt ein Interface, die mit dem SIP-DECT OMM verbunden werden kann. Die Standby-OMM-Konfiguration wird unterstützt. Über dieses Interface werden Nachrichten an SIP-DECT-Telefone gesendet, Bestätigungen sowie Alarmauslösungen von Telefonen empfangen, z.B. SOS, Man Down oder Alarm Trigger.	
	Allgemein	Allgemeine Einstellungen für das SIP-DECT-Interface
	OMM 1	OMM-IP-Adresse
	OMM 2	Standby-OMM-IP-Adresse
	Benutzer	Benutzername für die Authentifizierung beim OMM
	Kennwort	Passwort für die Authentifizierung beim OMM
	Benutzerdefinierter Ereignistext	Schalter zum Aktivieren oder Deaktivieren der benutzerdefinierten Ereignistextfunktion
	Endpunkte	Über SIP-DECT erreichbare Endpunkte (SIP-DECT-Benutzer)
	Aktiv	Schalter zum Aktivieren oder Deaktivieren des Endpunkts
	Adresse	Endpunktkennung, z. B. Telefonnummer
	Bezeichnung	Name des Endpunkts
	Standort	Standort, dem der Endpunkt zugewiesen ist
	Benutzerdefinierter Ereignistext	Die benutzerdefinierte Ereignistextfunktion ermöglicht es, den empfangenen Ereignistext zu ändern oder zu ersetzen, um eine entsprechende Benachrichtigung zu generieren.

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Textersetzung	Einfache Textersetzungsfunktion. Es können bis zu 10 Textersetzungsregeln definiert werden.
	Text	Zu ersetzender Text
	Ersetzt durch	Ersetzen von Text
	Struktur des Ereignistextes	Funktion zum Erstellen eines neuen Textes aus vordefinierten Elementen. Der benutzerdefinierte Ereignistext kann aus bis zu 4 Elementen zusammengesetzt werden.
	Text	Eines der folgenden Elemente: Ereignistyp, Ereignistyp kurz, Priorität, Auslösender Endpunkt (Name), Auslösender Endpunkt (Adresse), Standort des auslösenden Endpunktes, Phase, Empfangener Text vom Interface
	Max. Länge	Maximale Länge des einzufügenden Textes
	Trennzeichen	Trennzeichen zum Trennen der Textelemente
	Import Endpunkte	Funktion zur Vereinfachung der Einrichtung von SIP-DECT-Endgeräten
	Endpunkte zugewiesen	Endpunkte, die bereits aus SIP-DECT in EVM importiert wurden
	Endpunkte verfügbar	SIP-DECT-Endpunkte, die noch importiert werden können
Typ ESPA	Eingangs-Schnittstelle zur Verbindung mit einer Schwesternrufanlage, Brandmeldeanlage über ESPA 4.4.4 über IP.	
	Allgemein	Allgemeine Einstellungen für das ESPA-Interface.
	IP Adresse	IP-Adresse des Schwesternrufsystems oder ähnliches oder des seriellen IP-Konverters, mit dem eine Verbindung hergestellt werden soll
	IP Port	IP-Port des Schwesternrufsystems o.ä. oder des seriellen IP-Konverters, mit dem
	Interface Überwachung	Schalter zum Aktivieren oder Deaktivieren der Interfaceüberwachung
	Endpunkt bestimmen durch	Schalter zum Definieren der Methode zur Bestimmung des Endpunkts. Eine der beiden Optionen: Anrufadresse, Nachrichtentext
	Standard Ereignistyp	Ereignistyp, der verwendet werden soll, wenn kein anderer Ereignistyp ermittelt wurde

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Ruftyp 1 (Feld 4) beendet Ereignis	Schalter zum Aktivieren oder Deaktivieren der Option, dass Anruftyp 1 (ESPA-Feld 4) das Ereignis beenden soll
	Benutzerdefinierter Ereignistext	Schalter zum Aktivieren oder Deaktivieren der benutzerdefinierten Ereignistextfunktion
	Endpunkte	Endpunkte, die Ereignisse über das ESPA-Interface an den Event Manager senden können.
	Aktiv	Schalter zum Aktivieren oder Deaktivieren des Endpunkts
	Adresse (Feld 1)	Endpunkt-Kennung, z. B. ESPA-Anrufadresse
	Bezeichnung	Name zur Identifizierung des Endpunkts
	Standort	Standort, dem der Endpunkt zugewiesen ist
	Benutzerdefinierter Ereignistext	Die benutzerdefinierte Ereignistextfunktion ermöglicht es, den empfangenen Ereignistext zu ändern oder zu ersetzen, um eine entsprechende Benachrichtigung zu generieren.
	Textersetzung	Einfache Textersetzungsfunktion. Es können bis zu 10 Textersetzungsregeln definiert werden (nicht verwendbar für Ereignistyp, Priorität und Phase)
	Text	Zu ersetzender Text
	Ersetzen durch	Ersetzen von Text
	Struktur des Ereignistextes	Funktion zum Erstellen eines neuen Textes aus vordefinierten Elementen. Der benutzerdefinierte Ereignistext kann aus bis zu 4 Elementen zusammengesetzt werden.
	Text	Eines der folgenden Elemente: Ereignistyp, Ereignistyp kurz, Priorität, Auslösender Endpunkt (Name), Auslösender Endpunkt (Adresse), Standort des auslösenden Endpunktes, Phase, Empfangener Text vom Interface
	Max. Länge	Maximale Länge des einzufügenden Textes
	Trennzeichen	Trennzeichen zum Trennen der Textelemente
	Ereignis zuweisen	Funktion zur Zuweisung eines Ereignistyps auf Basis unterschiedlicher ESPA 4.4.4 Nachrichteninhalte.
	Position	Position der Regel in der Liste der Regeln. Die erste Abgleichsregel wird angewendet.

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Klingelton (3)	Klingeltonwert (ESPA-Feld 3), der dem angegebenen Ereignistyp zugeordnet werden soll.
	Priorität (6)	Prioritätswert (ESPA-Feld 6), der dem angegebenen Ereignistyp zugeordnet werden soll.
	Text (2)	Textwert (ESPA-Feld 2), der dem angegebenen Ereignistyp zugeordnet werden soll.
	Ereignistyp	Zu verwendender Ereignistyp.
	Textposition	Startposition im empfangenen Ereignistext, aus der der Ereignistext kopiert werden soll. 0 - Der ursprüngliche Ereignistext wird verwendet.
	Textlänge	Anzahl der Zeichen, die aus dem empfangenen Ereignistext von der Startposition übernommen werden sollen.
	Ereignistext	Alternativer Text, um den ursprünglichen Ereignismeldungstext zu ersetzen oder hinzuzufügen.
	Separator	Trennzeichen, auf das eine Telefonnummer folgt, z.B. für den Rückruf
	Simulator/Trace	
	Simulator	Die Simulatorfunktion ermöglicht es, ESPA-Nachrichten an den Event Manager zu senden, um den Datenverkehr zu emulieren, auch wenn das Interface nicht mit einem anderen System verbunden ist.
	Ruf Adresse (1)	ESPA-Feld 1 Rufadresse (Pflichtfeld)
	Displaynachricht (2)	ESPA-Feld 2 Meldung anzeigen (Pflichtfeld)
	Klingelton (3)	ESPA Field 3 Klingelton
	Ruf Typ (4)	ESPA-Feld 4 Anrufart
	Priorität (6)	ESPA-Feld 6 Priorität (1 – Alarm, 2 – hoch, 3 – normal)
	Trace	Funktion zur Anzeige des Datenverkehrs auf dem ESPA-Interface
	Daten empfangen	Schalter, um die Anzeige der empfangenen Daten zu aktivieren
	Daten gesendet	Schalter zum Anzeigen der gesendeten Daten

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Lebenszeichen	Schalter zum Aktivieren der Anzeige von Keep-Alive-Nachrichten / ESPA-Polling-Nachrichten
	Ansicht Hex	Schalter, um die Anzeige von Daten zusätzlich im Hexadezimalformat zu ermöglichen
	Fenster "Ablaufverfolgung"	ESPA-Verkehrsanzeigefenster
Typ SNMP	Das SNMP-Interface ermöglicht das Senden von SNMP-Trap- oder Inform-Nachrichten an ein Trap-Ziel.	
	Allgemein	Allgemeine Einstellungen für das SNMP-Interface.
	IP Adresse	IP-Adresse des Trap-Empfängers.
	IP Port	IP-Port-Adresse des Trap-Empfängers.
	Typ	Es kann entweder Trap oder Inform-Nachricht ausgewählt werden.
	Community	SNMP-Trap-Community, z.B. 'public'.
Typ Modbus	Das Modbus-Interface ermöglicht die Verbindung zu externen Geräten (WAGO/MOXA) mit eingehenden und ausgehenden Endpunkten	
	Allgemein	Allgemeine Einstellungen für das Modbus-Interface.
	IP Adresse	IP-Adresse des Modbus-Gerätes.
	IP Port	IP-Port-Adresse des Modbus-Gerätes.
	Endpunkte	Endpunkte des Modbus-Gerätes.
	Aktiv	Schalter zum Aktivieren oder Deaktivieren des Endpunktes
	Ausgehend	Endpunkte zu denen der Event Manager Nachrichten senden kann
	Eingehend	Endpunkte von denen der Event Manager Nachrichten empfangen kann
	Ereignistyp	Zu bearbeitender Ereignistyp
	Ruhestrom	Schalter zum Aktivieren oder Deaktivieren der Ruhestrom-Einstellung für den Endpunkt
	Alarmverzögerung	How long the endpoint needs to be activated in order to trigger an event in seconds
	Verhalten bei Rückkehr in die Ausgangsstellung	Auswahl des Verhaltens dieses Endpunktes bei dessen Rückkehr in den Normalzustand (z.B. “Ereignis nicht beenden”, “Ereignis beenden” oder “Ereignis am Ende der Phase beenden”)
	Adresse	Adresse des Endpunktes z.B. MODBUS-Adresse

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Bezeichnung	Bezeichnung des Endpunkts
	Standort	Standort, dem der Endpunkt zugewiesen ist
	Simulator/Trace	
	Trace	Das Trace-Fenster zeigt an, ob die Verbindung zu einem Modbus-Gerät hergestellt werden konnte oder nicht (Fehler) und ob es möglich ist, Trigger-Ereignisse von eingehenden Endpunkten zu empfangen
	Simulator	Die Simulatorfunktion ermöglicht die Simulation von Ereignissen an eingehenden Endpunkten im Event Manager, um den Datenverkehr zu emulieren, auch wenn die Schnittstelle nicht mit einem Gerät verbunden ist. Der Status der eingehenden und ausgehenden Endpunkte von einem real angeschlossenen Modbus-Gerät wird ebenfalls hier angezeigt.
Typ MQTT	Das MQTT-Interface ermöglicht die Verbindung zu einem MQTT-Broker über das MQTT-Protokoll.	
	Allgemein	Allgemeine Einstellungen des MQTT-Interfaces
	IP Adresse	IP-Adresse des MQTT-Brokers, zu dem verbunden werden soll
	IP Port	IP-Port des MQTT-Brokers, zu dem verbunden werden soll
	Benutzerdefinierter Ereignistext	Schalter zum Aktivieren oder Deaktivieren der benutzerdefinierten Ereignistextfunktion
	Endpunkte	IoT-Geräte, von denen der Event Manager Ereignisse über die MQTT-Schnittstelle zum MQTT-Broker empfangen kann.
	Aktiv	Schalter zum Aktivieren oder Deaktivieren des Endpunkts
	Adresse	Endpunktkennung, z. B. die Kennung des IoT-Geräts, das Ereignisse an den MQTT-Broker veröffentlicht
	Bezeichnung	Name zur Identifikation des Endpunkts
	Standort	Standort, dem der Endpunkt zugeordnet ist
	Benutzerdefinierter Ereignistext	Die benutzerdefinierte Ereignistextfunktion ermöglicht es, den empfangenen Ereignistext zu ändern oder zu ersetzen, um eine entsprechende Benachrichtigung zu generieren.

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Textersetzung	Einfache Textersetzungsfunktion. Es können bis zu 10 Textersetzungsregeln definiert werden (nicht verwendbar für Ereignistyp, Priorität und Phase)
	Text	Zu ersetzender Text
	Ersetzt durch	Ersetzender Text
	Struktur des Ereignistextes	Funktion zum Erstellen eines neuen Textes aus vordefinierten Elementen. Der benutzerdefinierte Ereignistext kann aus bis zu 4 Elementen zusammengesetzt werden.
	Text	Eines der folgenden Elemente: Ereignistyp, Ereignistyp kurz, Priorität, Auslösender Endpunkt (Name), Auslösender Endpunkt (Adresse), Standort des auslösenden Endpunktes, Phase, Empfangener Text vom Interface
	Max. Länge	Maximale Länge des einzufügenden Textes
	Trennzeichen	Trennzeichen zum Trennen der Textelemente
	Topics	MQTT-Topics für Subscribe oder Publish
	Aktiv	Schalter zum Aktivieren oder Deaktivieren der Topic
	Typ	Typ der Topic (Subscribe oder Publish)
	Nachricht als Payload	Schalter zur Auswahl, ob Notifikationen als Payload in einer Publish-Nachricht an den MQTT-Broker gesendet werden sollen
	Endpunkt	Bezeichnung des Endpunkts, dem diese Topic zugewiesen ist
	Subscribe mapping	Mapping für Subscribe
	Aktiv	Schalter zum Aktivieren oder Deaktivieren des Subscribe mappings
	Ereignistyp	Typ des Ereignisses, das durch die empfangene MQTT-Nachricht ausgelöst werden soll
	Bedingung	Bedingung, die geprüft wird, um ein Ereignis auszulösen, wenn eine MQTT-Nachricht für ein abonniertes Thema empfangen wird (Text gleich, Text enthalten, Wert identisch, Wert größer, Wert kleiner)
	Publish mapping	Mapping von Ereignistypen zu Publish-Topics mit Payload-Inhalt

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Topic	Publish-Topic, welche über den MQTT-Broker an das IoT-Gerät gesendet werden soll
	Ereignistyp	Typ des Ereignisses welches die Publish-Topic für eine MQTT-Nachricht erzeugt
	Payload	Payload-Inhalt einer MQTT-Nachricht
Typ Web-API	Interface zur Kommunikation mit Web-Applikationen über das HTTPS-Protokoll (RESTapi).	
	Allgemein	Allgemeine Einstellungen für die Web-API-Schnittstelle
	Eingehende URL	Fix: ‚https://<IP Adresse des EM>/wapi/v1/request' oder ‚https://<CLD tunnel>/wapi/v1/request'
	URL: event	Eingehende URL für Ereignisanforderungen
	URL: event result	URL für ausgehende Resultate zu angeforderten Ereignissen
	URL: event cancel	Eingehende URL für das Abbrechen von Ereignissen
	URL: notification	URL für das Senden von Notifikationen
	URL: confirmation	Eingehende URL für Bestätigungen
	URL: cancel	URL zum Abbrechen ausgehender Notifikationen
	API key	Buttons für 'Kopieren in Zwischenablage' und 'Erneuern' des API key (CloudLink-API)
	Zertifikate validieren	Schalter zur Aktivierung der Zertifikatsüberprüfung bei ausgehenden Nachrichten
	Endpunkte	Interne Endpunkte für das Senden/Empfangen von Web-API-Notifikationen/Anforderungen.
	Aktiv	Schalter zum Aktivieren oder Deaktivieren des Endpunkts
	Adresse	Endpunktkennung, z. B. die Kennung des Web-API-Geräts, das Ereignisse anfordert oder Benachrichtigungen empfängt
	Bezeichnung	Bezeichnung des Endpunkts
	Standort	Standort, dem der Endpunkt zugeordnet ist
Ereignistypen	Konfigurationsbereich zur Verwaltung von bis zu 100 Ereignistypen. Einzelne Ereignisse werden diesen Ereignistypen zur weiteren Verarbeitung zugeordnet.	
	Bezeichnung	Name des Ereignistyps
	Kurztext	Kurzer (max. 8 Zeichen lang) Name des Ereignistyps

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Priorität	Priorität des Ereignisses
	Beschreibung	Zusatzinformation
Meldungsprofile	Konfigurationsbereich zur Verwaltung von bis zu 50 Meldungsprofilen. Meldungsprofile definieren die Art und Weise, wie Benachrichtigungen vom empfangenden Gerät angezeigt werden.	
	Bezeichnung	Name des Meldungsprofils
	Beschreibung	Zusatzinformation
	SIP-DECT-Profil	Das Profil enthält verschiedene Parameter, mit denen die Art und Weise gesteuert wird, wie eine Benachrichtigung auf dem Mitel 6x2d/700d DECT-Telefon angezeigt wird.
	Rufton Gruppe	Der Ereignis-Manager kann den Klingelton steuern, um die auf dem DECT-Telefon empfangene Nachricht zu warnen. Es stehen verschiedene Optionen zur Verfügung: a) Vorerst nicht zu verwenden: kein b) Verwendung der Geräteeinstellungen mit Auswahl einer bestimmten Melodieeinstellung: Lokale Einstellungen c) Auswahl eines Klingeltons aus einer Gruppe: eine der verfügbaren Klingeltongruppen
	Klingelton	a) Wenn die Klingeltongruppe auf "Lokale Einstellungen" eingestellt ist, kann eine bestimmte Melodieeinstellung des Gerätes ausgewählt werden. B) Wenn eine Klingeltongruppe eingestellt ist, kann eine Melodie oder ein Soundeffekt ausgewählt werden.
	Priorität	SIP-DECT-Nachrichtenpriorität: Niedrig, Normal, Hoch, Notfall
	Ruflautstärle	Klingeltonlautstärke, die zur Anzeige der Benachrichtigung verwendet werden soll.
	Ansteigende Ruflautstärke	Aktiviert die automatische Lautstärkeerhöhung
	Vibration	Aktiviert den Vibrator, wenn er nicht automatisch vom Telefon basierend auf der Nachrichtenpriorität aktiviert wird.
	Kein Aufmerksamkeitston während Gespräch	Schalten Sie den Schalter ein, um die akustische Anzeige (In-Band) der empfangenen Nachricht auszuschalten.
	Bestehenden Ruf unterbrechen	Wenn diese Option aktiviert ist, wird ein bestehendes Telefongespräch beendet, wenn die Nachricht eintrifft.

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Schriftfarbe	Anzeigefarbe des Meldungstextes
	Hintergrundfarbe	Hintergrundfarbe des Meldungstextes
Meldungsgruppen	Konfigurationsbereich zur Verwaltung von bis zu 50 Meldungsgruppen. (insgesamt maximal 2000 Endpunkte über alle Gruppen hinweg). Meldungsgruppen gruppieren Endpunkte, die benachrichtigt werden sollen, um die Verwaltung zu vereinfachen. Gruppen können Phasen von Ereignisplänen anstelle einzelner Endpunkte zugewiesen werden. Darüber hinaus können Meldungsgruppen Adressen haben, um die Funktion "Anrufadresse verwenden" in Ereignisplänen zu verwenden.	
	Bezeichnung	Name der Meldungsgruppe
	Beschreibung	Zusatzinformation
	Adresse	Eindeutige ID, z. B. Telefonnummer / Durchwahlnummer
	Endpunkte zugewiesen	Liste der Endpunkte, die dieser Gruppe zugewiesen sind
	Bezeichnung/Adresse	Name des Endpunkts / Adresse des Endpunkts
	Endpunkte verfügbar	Liste der Endpunkte, die dieser Gruppe zugewiesen werden können.
	Bezeichnung/Adresse	Name des Endpunkts / Adresse des Endpunkts
Ereignispläne	Konfigurationsbereich zur Verwaltung von bis zu 500 Ereignisplänen. Ereignispläne definieren Prozesse für die Verarbeitung empfangener Ereignisse, die von Endpunkten an den verschiedenen Standorten gesendet werden, um empfangende Endpunkte zu benachrichtigen	
	Aktiv	Schalten Sie um, um den Ereignisplan zu aktivieren oder zu deaktivieren.
	Bezeichnung	Name des Ereignisplans
	Beschreibung	Zusatzinformation
	Neustartplan des Planes nach Ablauf	Schalter zum Aktivieren oder Deaktivieren des Neustarts des Plans nach Abschluss (Standard: aus)
	Filter: Ereignistyp	

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Ereignistypen zugewiesen	Liste der Ereignistypen, für die der Plan angewendet wird, d.h. ausgeführt werden soll.
	Ereignistypen verfügbar	Liste der Ereignisarten, die dem Plan noch nicht zugewiesen wurden, d.h. auf die der Plan nicht angewendet wird
	Filter: Standort	
	Standorte zugewiesen	Liste der Standorte, für die der Plan gilt, d. h. der Plan wird auf Ereignisse angewendet, die von Endpunkten an diesen Standorten gesendet werden.
	Standorte verfügbar	Liste der Standorte, die dem Plan noch nicht zugewiesen wurden, d.h. für die der Plan nicht gilt
	Phase	Ereignisplanphasen: bis zu 10 Phasen in einem einzigen Plan und bis zu 1000 Phasen insgesamt über alle Ereignispläne hinweg.
	Bezeichnung	Name der Phase
	Beschreibung	Zusätzliche Beschreibung für die Phase.
	Benutze Ruf Adresse	Option zum Aktivieren der Auswahl der Meldungsgruppe basierend auf der Adresse der empfangenden Endpunkte. Es muss eine Meldungsgruppe mit derselben Adresse vorhanden sein.
	mit Meldungsprofil	Wenn die Meldungsgruppe über die Aufrufadresse der Endpunkte ausgewählt wird, wird das angegebene Meldungsprofil bei der Verarbeitung dieser Phase angewendet.
	Endpunkte/Meldungsgruppen	Registerkarte, in der der Phase Endpunkte oder Meldungsgruppen zugewiesen werden, die benachrichtigt werden sollen.
	Endpunkte zugewiesen	Endpunkte, die dieser Phase zugewiesen sind.
	Bezeichnung/Adresse	Name des Endpunkts / Adresse des Endpunkts
	Endpunkte verfügbar	Endpunkte, die dieser Phase zugeordnet werden können.
	Bezeichnung/Adresse	Name des Endpunkts / Adresse des Endpunkts
	Meldungsprofil	Meldungsprofil, das in dieser Phase für den Endpunkt verwendet werden soll
	Meldungsgruppen zugewiesen	Meldungsgruppe, die dieser Phase zugewiesen ist.
	Bezeichnung/Adresse	Name der Meldungsgruppe / Adresse der Meldungsgruppe

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Meldungsgruppe verfügbar	Meldungsgruppe, die dieser Phase zugeordnet werden könnte.
	Bezeichnung/Adresse	Name der Meldungsgruppe / Adresse der Meldungsgruppe
	Meldungsprofil	Meldungsprofil, das in dieser Phase für die Gruppe verwendet werden soll
	Einstellungen	Registerkarte für die Konfiguration allgemeiner Phaseneinstellungen.
	Dauer	Dauer in Sekunden
	Anzahl der Wiederholungen	Nie / Dauerhaft / 1..49
	Anzahl der Bestätigungen	Individuell (jeder Endpunkt) oder Wert zwischen 1 und 49
Standorte	Konfigurationsbereich zum Verwalten von bis zu 500 Endpunktstandorten. Speicherorte, an denen es Endpunkte gibt, die Ereignisse an den Ereignis-Manager senden. Diesen Standorten können auch Ereignispläne über standortbasierte Filter zugeordnet werden, so dass standortabhängige Abläufe definiert werden können.	
	Standort	Vollständige Standortinformationen mit übergeordneten Standorten
	Bezeichnung	Name des Standorts
	Beschreibung	Zusatzinformation
	Endpunkte zugewiesen	Liste der Endpunkte, die diesem Speicherort zugewiesen sind.
	Bezeichnung/Adresse	Name des Endpunkts / Adresse des Endpunkts
	Endpunkte verfügbar	Liste der Endpunkte, die keinem Standort zugewiesen sind und diesem Standort zugewiesen werden könnten.
	Bezeichnung/Adresse	Name des Endpunkts / Adresse des Endpunkts
Benutzer	Konfigurationsbereich zur Verwaltung von bis zu 10 Benutzern, die Zugriff auf den Webservice des Event Managers haben.	
	Name	Benutzername, Login-Name
	Berechtigung	Berechtigung des Benutzers (Konfiguration, Monitor, Lokalisierung)
	Kennwort	Benutzerkennwort
	Kennwort Bestätigung	Bestätigung des Benutzerpassworts
System	Administrationsbereich für verschiedene administrative Tätigkeiten für den Betrieb des Eventmanagers.	
	Allgemein	Allgemeine Systemeinstellungen

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Systemname	Systemname
	CloudLink aktiviert	Schalter zum Aktivieren oder Deaktivieren des CloudLInk Daemon
	CloudLink Status	Zeigt den Status des CloudLInk Daemon
	Version	Zeigt die aktuell laufende Softwareversion
	Watchdog	Schalter zum Aktivieren oder Deaktivieren des Auslösens eines Watchdogs
	Watchdog-IP-Adresse	IP-Adresse des Watchdogs, der ausgelöst werden soll
	Datensicherung/Neustart	Optionen zum Neustart des Event Managers, zum Sichern der Konfiguration und des Ereignisprotokolls.
	Neustart	Starten Sie den Event-Manager neu
	Neustart mit Grundeinstellungen	Starten Sie den Event Manager neu und setzen Sie die Event Manager-Konfiguration auf die Standardeinstellungen zurück
	Export Log	Ermöglicht das Speichern des Alarmprotokolls auf dem PC als <Datum>-<Zeit>_evp_summary_log.csv Datei und <Datum>-<Zeit>_evp_details_log.csv Datei
	Export Konfiguration	Ermöglicht es, die Konfiguration des Event Managers auf dem PC als <Datum>-<Uhrzeit>_evp_conf.gz Datei zu speichern
	Import Konfiguration	Ermöglicht die Wiederherstellung der Konfiguration des Event Managers von einem PC aus
	Sicherheit	Optionen zum Import von SSL-Zertifikaten und privaten Schlüsseln (mit und ohne Passwort).
	Vertrauenswürdige Zertifikate	Zeigt, wie viele vertrauenswürdige Zertifikate geladen sind
	Lokale Zertifikatketten	Zeigt, wie viele lokale Zertifikate der Event Manager geladen hat
	Privater Schlüssel	Zeigt, ob der Event Manager einen privaten Schlüssel geladen hat
	Privater Schlüssel: Kennwort	Eingabefeld für das Passwort zum privaten Schlüssel
	Privater Schlüssel: Kennwortbestätigung	Eingabefeld für die Bestätigung des Passworts zum privaten Schlüssel
	Importiere PEM-Datei mit	Definition des Typs der PEM-Datei (vertrauenswürdiges Zertifikat / lokale Zertifikatkette / privater Schlüssel)
	Importiere PEM-Datei	Importiere eine PEM-Datei

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Lösche Zertifikate/Schlüssel	Lösche alle Zertifikate und Schlüssel
	Bring es zum Laufen	Neustart des Event Managers zur Übernahme der Änderungen
	Sicherheitsstufen	Optionen zur Konfiguration einer Sicherheitsstufe und von zugehörigen benutzten Cipher suites
	Sicherheitsstufe	Auswahl der Sicherheitsstufe (Hoch, Mittel oder Legacy)
	Cipher suites der Sicherheitsstufe	Auswahl der Cipher suites zur eingestellten Sicherheitsstufe
	Benutze Grundeinstellungen	Schalter zum Aktivieren / Deaktivieren der Grundeinstellungen
	Benutzte Cipher suites	Liste der benutzten Cipher suites (kann editiert werden, wenn ‚Benutze Grundeinstellungen' nicht gesetzt ist)
	Unterstützte Cipher suites	Liste aller unterstützten Cipher suites
	CloudLink	Zeigt die aktuelle Konfiguration des CloudLink Daemon und erlaubt die Konfiguration der Verbindung zum CloudLink Portal und für die Fernwartung.
Monitor	Bereich zur Anzeige der aktuell aktiven Ereignisverarbeitungsaktivitäten und deren Status sowie der Möglichkeit, diese zu beenden.	
	Alle abbrechen	Alle aktiven Alarme abbrechen
	Priorität	Priorität des Ereignistyps
	Typ	Art des Ereignistypen
	Text	Text der Ereignismeldung
	Endpunkt	Endpunkt, der das Ereignis empfangen hat
	Phase	Aktuelle Phase des Ereignisplans
	Bestätigungen	Erhaltene Bestätigungen/Erforderliche Bestätigungen
	Abbrechen	Einen einzelnen aktiven Alarm abbrechen

Event Manager mit Lokalisierung

Im Falle eines Event Managers, der als PC-Anwendung auf einem Linux-Server läuft und mit einem OMM mit einer installierten 'Mitel SIP-DECT Locating Server License' verbunden ist, steht ein zusätzlicher Menüeintrag im Menübaum zur Verfügung: Lokalisierung.

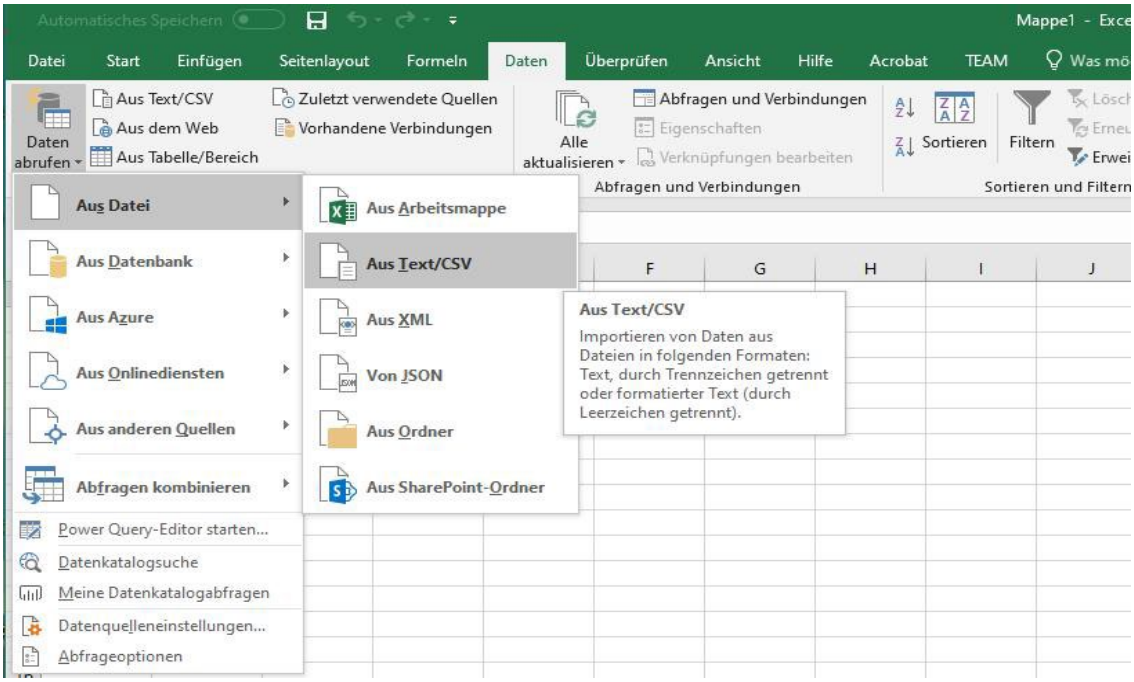
Dieser Menüeintrag ist als erweiterbarer Baum mit den im Event Manager konfigurierten Standorten realisiert und enthält verschiedene Registerkarten für Monitor, Benutzer, Karten und Radio Fixed Parts (RFPs). Hier gibt es auch eine Schaltfläche 'Standorte importieren', um Standorte zu importieren, die bereits im OMM definiert sind.

Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
Lokalisierung	Konfigurationsbereich als erweiterbarer Baum mit den im Event Manager konfigurierten Standorten	
	Monitor	Bereich zur Anzeige der derzeit aktiven Ereignisverarbeitungsaktivitäten und ihres Status sowie einer Option zum Beenden dieser Aktivitäten.
	Alle abbrechen	Abbrechen aller aktiven Ereignispläne
	Priorität	Priorität des Ereignistyps
	Typ	Ereignistyp
	Text	Ereignistext
	Endpunkt	Auslösender Endpunkt
	Phase	Aktuelle Phase des Ereignisplanes
	Bestätigungen	Erhaltene Bestätigungen / erforderliche Bestätigungen
	Abbrechen	Abbrechen des einzelnen aktiven Ereignisplanes
	Benutzer	Liste der importierten SIP-DECT Benutzer mit aktivierter Einstellung ‚lokalisierbar' und/oder ‚verfolgbar'
	Name	Benutzername eines lokalisierbaren DECT-Gerätes (in SIP-DECT)
	Rufnummer	Rufnummer des DECT-Gerätes (in SIP-DECT)
	Standort	Aktueller Standort des DECT-Gerätes (basierend auf Nachrichten vom OMM)
		Link zur Karte, die eine Markierung für den Standort zeigt
	On	Icon zur Anzeige ob der Standort des DECT-Gerätes bereits empfangen wurde
	Letzte Aktion	Datum und Zeit der zuletzt bekannten Position des DECT-Gerätes (basierend auf Nachrichten vom OMM)
	Beschreibung 1	Beschreibung zum DECT-Gerät (in SIP-DECT), z.B. Organisation

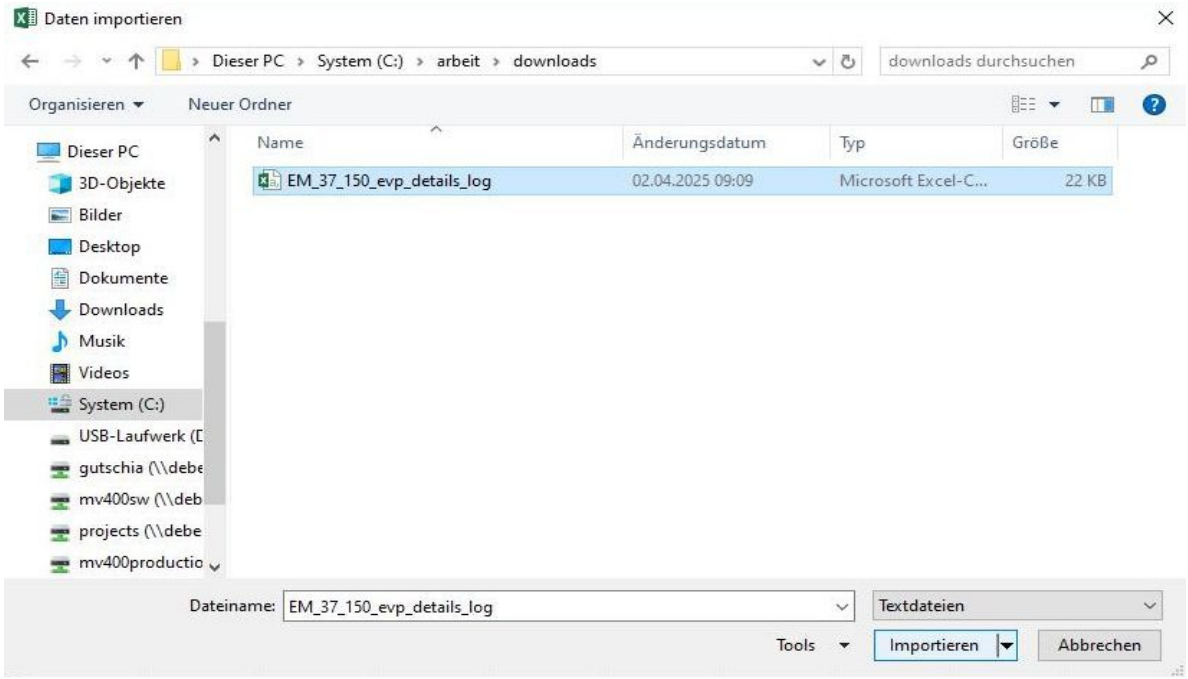
Web-UI-Parameter, Aktions- und Statusinformationen		Beschreibung
	Beschreibung 2	Beschreibung zum DECT-Gerät (in SIP-DECT), z.B. Abteilung
	Karten	Liste geladener Karten als Grundlage für Standortanzeigen
	Bezeichnung	Bezeichnung der geladenen Karte
	Bild	Link zur geladenen Karte
	Zoomstufe	Anzahl verfügbarer Zoomstufen der geladenen Karte
	Standort	Zugeordneter Standort
	Speichern / Löschen	Buttons für Ändern / Löschen von Karten
	RFPs	Liste aus SIP-DECT importierter Radio Fixed Parts (RFP)
	Name	Bezeichnung des RFP (aus SIP-DECT)
	MAC-Adresse	MAC-Adresse des Radio Fixed Part (RFP)
	Standort	Standort des zugeordneten RFP
	Detail	Icon welches anzeigt, ob der Standort des RFP bereits auf einer Detailkarte positioniert ist
	Übersicht	Icon welches anzeigt, ob der Standort des RFP bereits auf einer Übersichtskarte positioniert ist
	Speichern	Button für Speichern des Eintrags

Empfehlung für das Verfahren zum Importieren von Protokolldaten in Microsoft Excel

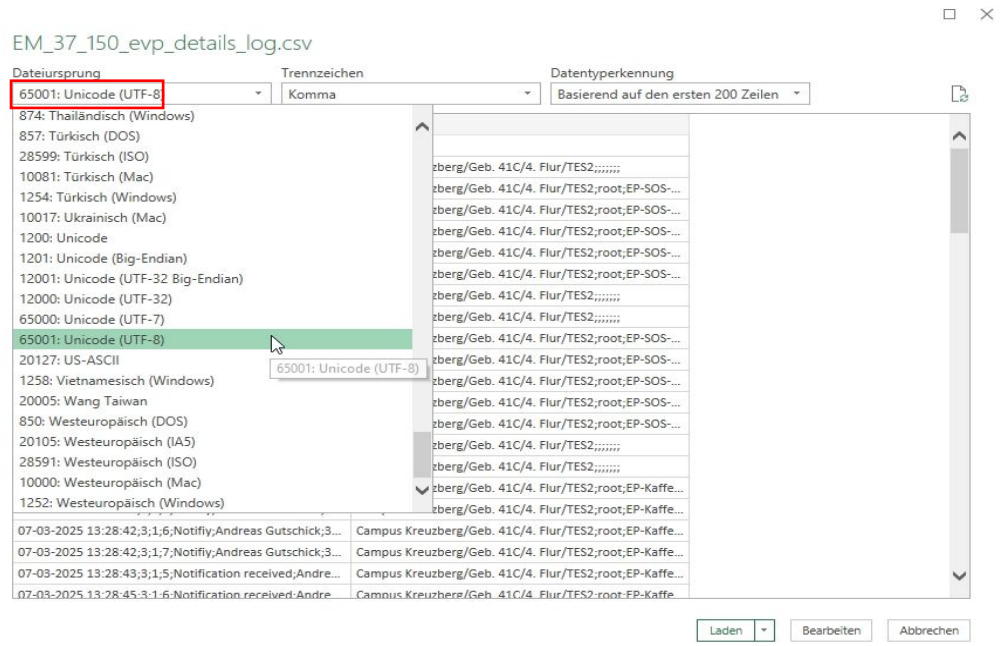
Eine bequeme Möglichkeit, die Protokolldaten aus dem Event Manager in eine Microsoft Excel-Datei zu importieren und dabei die korrekte Formatierung der Daten beizubehalten, ist der Datenimport "Daten aus Datei holen".



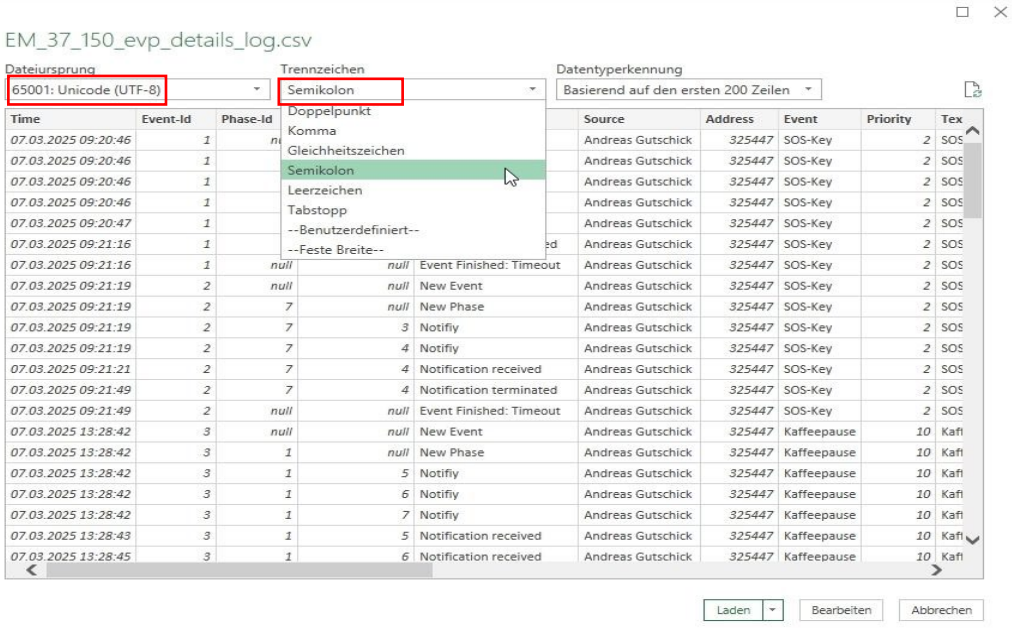
Wählen Sie die Datei, die Sie importieren möchten.



Wählen Sie "Unicode (UTF-8)" für die Kodierung, damit Nicht-ASCII-Zeichen korrekt angezeigt werden.



Wählen Sie "Semikolon" als Begrenzungszeichen.

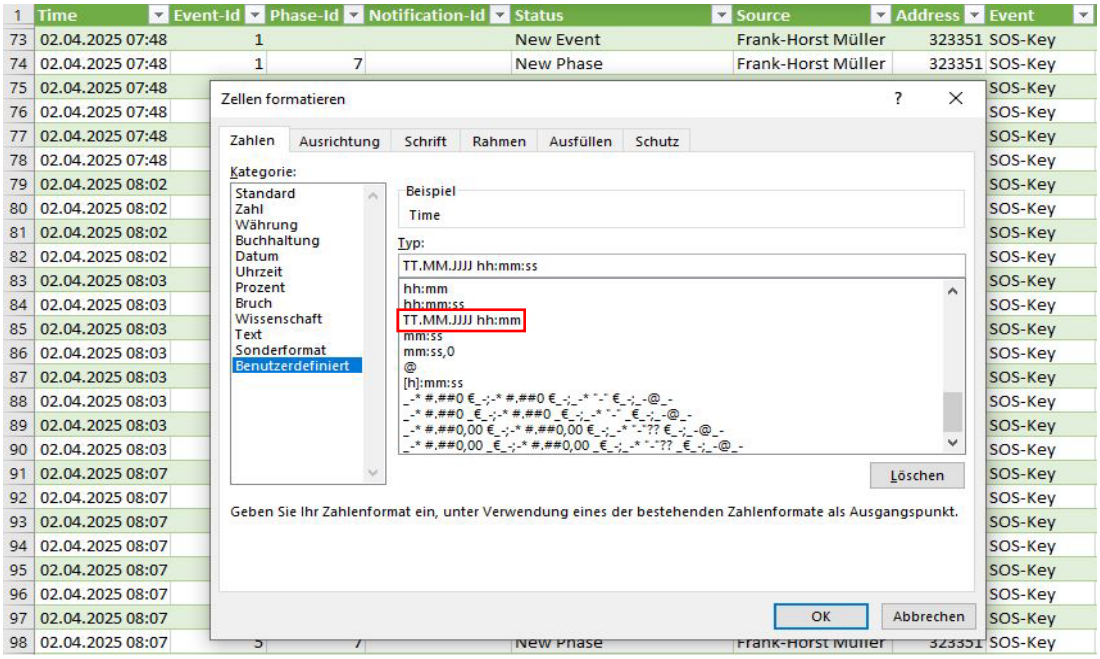


Bestätigen Sie dann mit "Laden", um die Daten zu laden.

Die Daten sollten dann folgendermaßen angezeigt werden:

	Time	Event-Id	Phase-Id	Notification-Id	Status	Source	Address	Event
73	02.04.2025 07:48:10	1			New Event	Frank-Horst Müller	323351	SOS-Key
74	02.04.2025 07:48:10	1	7		New Phase	Frank-Horst Müller	323351	SOS-Key
75	02.04.2025 07:48:10	1	7	1	Notifiy	Frank-Horst Müller	323351	SOS-Key
76	02.04.2025 07:48:13	1	7	1	Notification received	Frank-Horst Müller	323351	SOS-Key
77	02.04.2025 07:48:20	1	7	1	Confirmed	Frank-Horst Müller	323351	SOS-Key
78	02.04.2025 07:48:20	1			Event Finished: Confirmed	Frank-Horst Müller	323351	SOS-Key
79	02.04.2025 08:02:40	2			New Event	Frank-Horst Müller	323351	SOS-Key
80	02.04.2025 08:02:40	2	7		New Phase	Frank-Horst Müller	323351	SOS-Key
81	02.04.2025 08:02:40	2	7	2	Notifiy	Frank-Horst Müller	323351	SOS-Key
82	02.04.2025 08:02:42	2	7	2	Notification received	Frank-Horst Müller	323351	SOS-Key
83	02.04.2025 08:03:03	2	7	2	Confirmed	Frank-Horst Müller	323351	SOS-Key
84	02.04.2025 08:03:03	2			Event Finished: Confirmed	Frank-Horst Müller	323351	SOS-Key

Wenn die Uhrzeit immer noch keine Sekunden enthält, muss das Format der Zellen angepasst werden. Wählen Sie dazu das benutzerdefinierte Format " TT/MM/JJJJ hh:mm" und fügen Sie ":ss" hinzu, so dass die Zeit aus Stunden:Minuten:Sekunden besteht (TT/MM/JJJJ hh:mm:ss").



Da die Daten mit der Quelldatei verknüpft sind, müssen die oben genannten Schritte nicht jedes Mal wiederholt werden. Wenn aktualisierte Protokolle unter demselben Dateinamen an denselben Speicherort kopiert werden, ist eine Aktualisierung der Daten ausreichend.

	Time	Event-Id	Phase-Id	Notification-Id	Status	Source	Address	Event	Priority	Text
73	02.04.2025 07:48:10	1			New Event	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
74	02.04.2025 07:48:10	1	7		New Phase	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
75	02.04.2025 07:48:10	1	7	1	Notifiy	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
76	02.04.2025 07:48:13	1	7	1	Notification received	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
77	02.04.2025 07:48:20	1	7	1	Confirmed	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
78	02.04.2025 07:48:20	1			Event Finished: Confirmed	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
79	02.04.2025 08:02:40	2			New Event	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
80	02.04.2025 08:02:40	2	7		New Phase	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
81	02.04.2025 08:02:40	2	7	2	Notifiy	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
82	02.04.2025 08:02:42	2	7	2	Notification received	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
83	02.04.2025 08:03:03	2	7	2	Confirmed	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller
84	02.04.2025 08:03:03	2			Event Finished: Confirmed	Frank-Horst Müller	323351	SOS-Key	2	SOS - Frank-Horst Müller

Die geänderten Daten erscheinen nach der Aktualisierung.