
UNMS Network Management System

Schnellstartanleitung

Copyright Statement for Intellectual Property and Confidential Information

The information contained in this manual is non-conditional and may be changed without due notice. Although GENEREX has attempted to provide accurate information within this document, GENEREX assumes no responsibility for the accuracy of this information.

GENEREX shall not be liable for any indirect, special, consequential, or accidental damage including, without limitations, lost profits or revenues, costs of replacement goods, loss or damage to data arising out of the use of this document

GENEREX the manufacturer of this product undertakes no obligations with this information. The products that are described in this brochure are given on the sole basis of information to its channel partners for them to have a better understanding of the GENEREX products.

GENEREX allows its channel partners to transfer information contained in this document to third persons, either staff within their own Company or their own customers, either electronically or mechanically, or by photocopies or similar means. GENEREX states that the content must not be altered or adapted in any way without written permission from GENEREX.

It is agreed that all rights, title and interest in the GENEREX's trademarks or trade names (whether or not registered) or goodwill from time to time of GENEREX or in any intellectual property right including without limitation any copyright, patents relating to the Products, shall remain the exclusive property of GENEREX.

GENEREX will undertake to deal promptly with any complaints about the content of this document. Comments or complaints about the document should be addressed to GENEREX Systems GmbH.

Copyright of the European Union is effective (Copyright EU).
Copyright (c) 1995-2016 GENEREX GmbH, Hamburg, Germany. All rights reserved.

Bevor Sie beginnen....

→ Dokumentieren Sie Ihre Konfigurationen

Die UNMS ist ein flexibles System, welches individuell an Ihre Anforderungen anpassbar ist. Einige Funktionen hängen dabei von Vorarbeiten ab, die durchgeführt werden müssen, um eine die gewünschte Funktion freizuschalten.

→ Überlegen Sie sich, was Sie tun möchten

Die UNMS kann Szenariobedingt sehr unterschiedliche Funktionen erfüllen. Sie können Gerätedaten mit zugehörigen Kundendaten nach Service-Leveln und Verfügbarkeit sortiert eintragen, Sie können verschachtelte Subscreens erstellen, Redundanzgruppen und Eskalationslevel abbilden, Automatische Alarmlevel für Einzelaspekte von Geräten definieren, Sammelstörungen und Masteralarme einstellenm ...

Nicht jede Funktion muss zwangsläufig konfiguriert werden, entscheidend ist, was Sie in Ihrem Netzwerk erreichen möchten und wofür Sie das System benutzen wollen.

→ Machen Sie 1 – 2 Testinstallationen

Die UNMS II von der Grundstruktur her sehr logisch aufgebaut, aber gerade dann, wenn Sie mit IIS arbeiten müssen, kommt es immer wieder zu seltsamen Ergebnissen, deren Ursache auf eine Fehlkonfiguration im IIS zurückzuführen ist. In einigen Fällen muss man wissen, welches Konfigurationsmenü im IIS dafür zuständig ist und entsprechend dokumentieren.

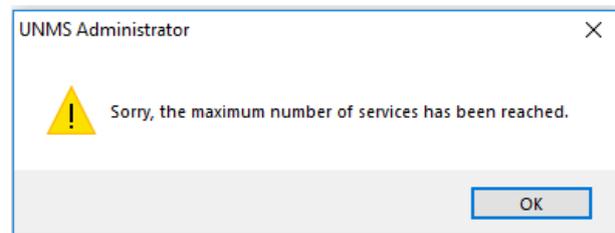
→ Fertigen Sie regelmäßig Backups an

Insbesondere dann, wenn Sie eine größere Änderung vorhaben, sollten Sie ein Backup erstellen, um jederzeit auf den originalzustand zurück zu kommen. Ansonsten könnten Sie bei Ihren Änderngen in Gefahr laufen, das aktuelle Betsandssystem zu verlieren.

→ Überprüfen Sie, ob Ihre Version der UNMS II die gewünschte Funktion unterstützt

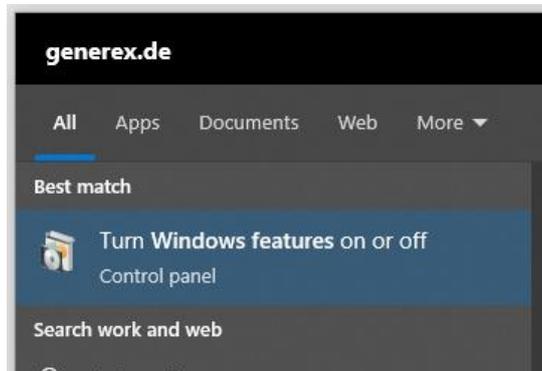
Der Funktionsumfang und die Möglichkeiten der UNMS ist Versionsabhängig. Wenn eine Funktion nicht ausführbar ist, kann es dem entsprechend zwei Gründe haben:

1. Ihre Version der UNMS II kann diese Funktion von der Softwarelizenzierung her nicht.
2. Die Rahmenbedingung für diese Funktion ist nicht erfüllt.



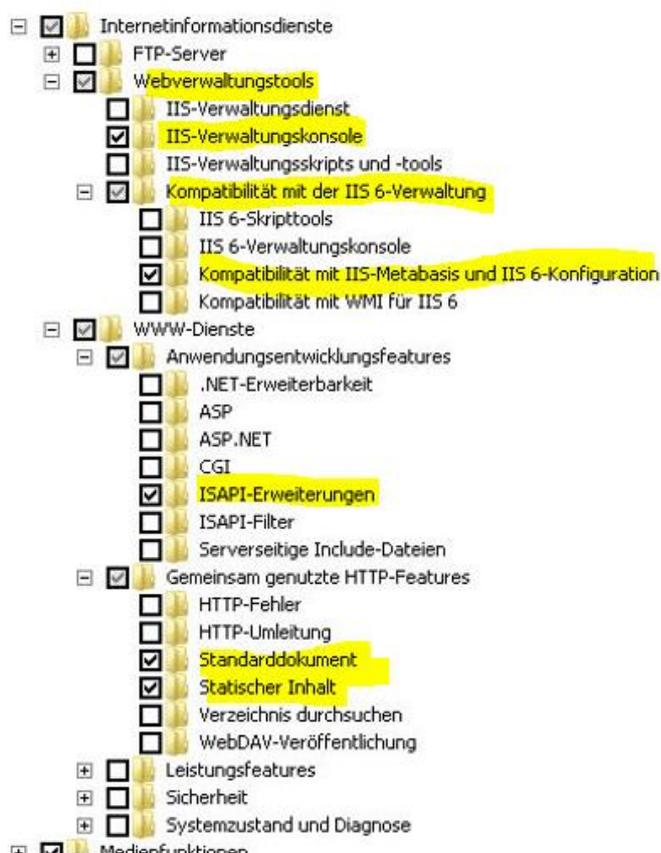
Quick Install

Preparation Windows Features – Add the IIS



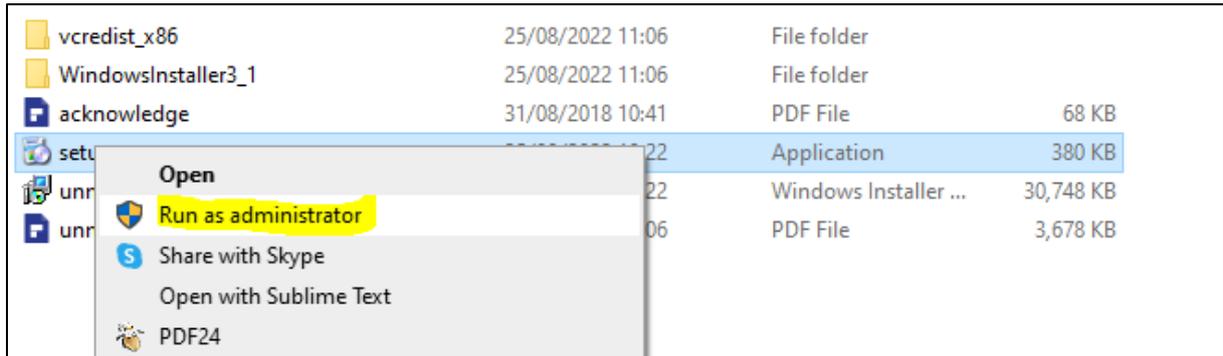
Die UNMS II setzt auf den sog. Internet Information Service (IIS) von Microsoft auf, um die notwendigen Informationen über http ausliefern zu können. Bevor Sie die UNMS II installieren können, müssen Sie also entsprechend kontrollieren, ob diese sog. Windows Features auch zur Verfügung stehen. Die Quickstartanleitung verwendet hierbei Windows 10 Professional, bei der der IIS und die notwendigen Komponenten über die Programmfeatures installiert werden können. **Andere Betriebssysteme sind weiter unten in diesem Handbuch beschrieben.**

Folgende Windows-Features sind für den Betrieb der UNMS II mindestens notwendig:

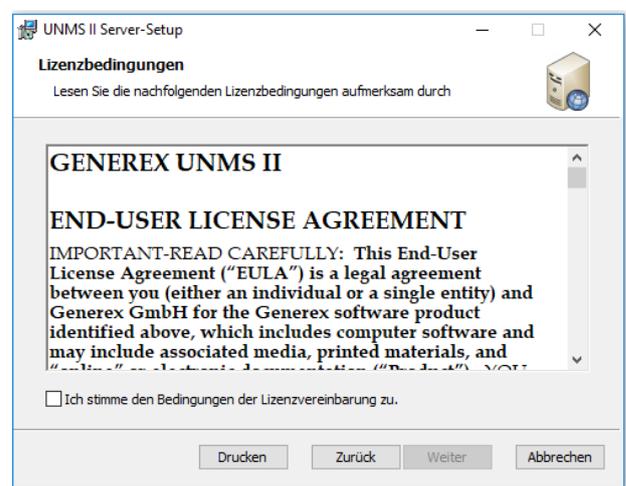
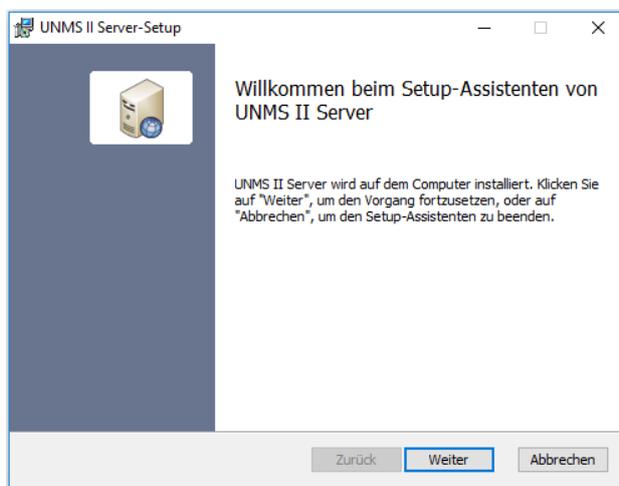


Außerdem benötigt die Installation der UNMS II erhöhte Systemrechte, da u.a. auch im Hintergrund laufende Dienste installiert werden, die unabhängig von einer Benutzer- oder Administratorkonsole laufen.

Daher kann die Installation nur gestartet werden, wenn sie über das Windows-Kontextmenü "Als Administrator" ausgeführt wird:

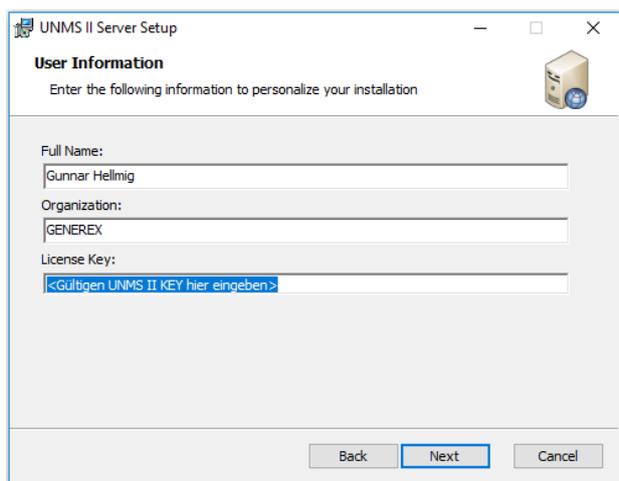


Der Installationsdialog führt Sie einmal durch de Installationsprozess

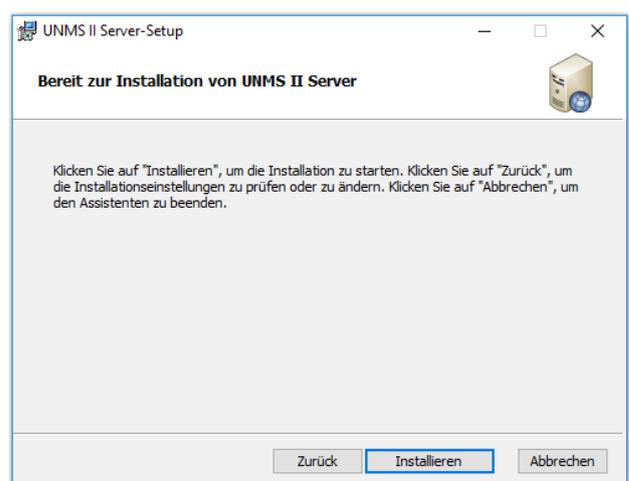


Weiter klicken ...

... Lizenzbedingungen akzeptieren ...

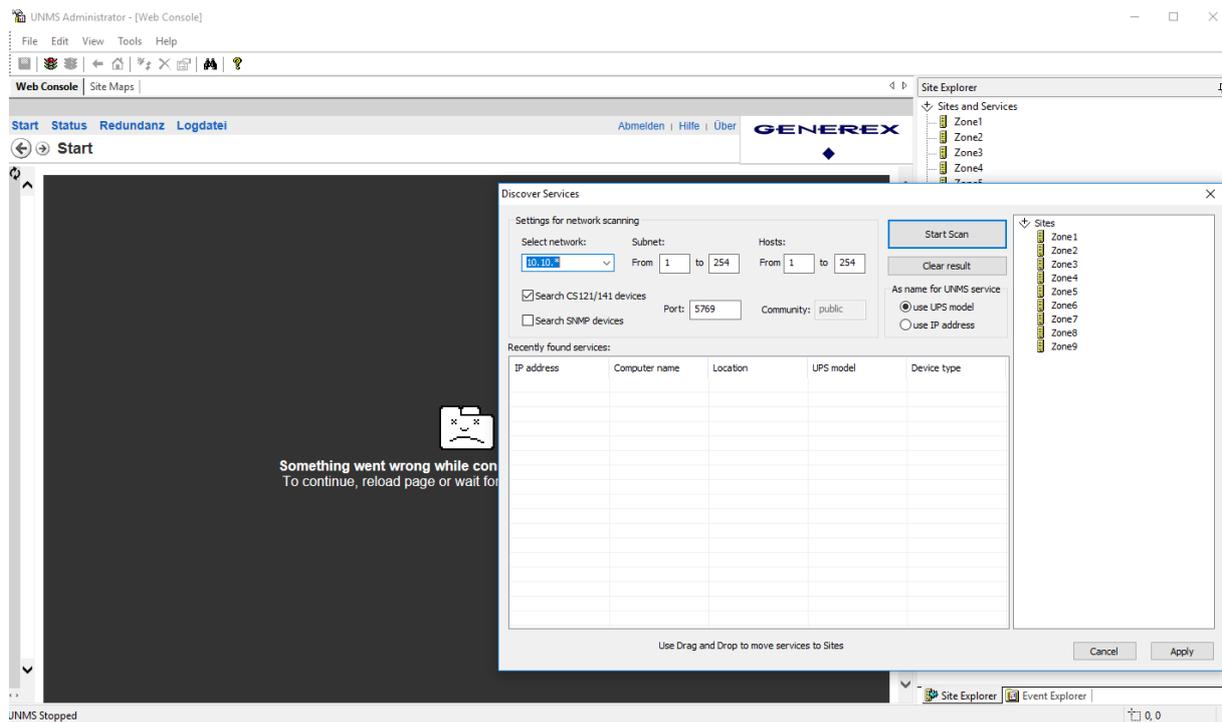


... Lizenzkey eingeben...



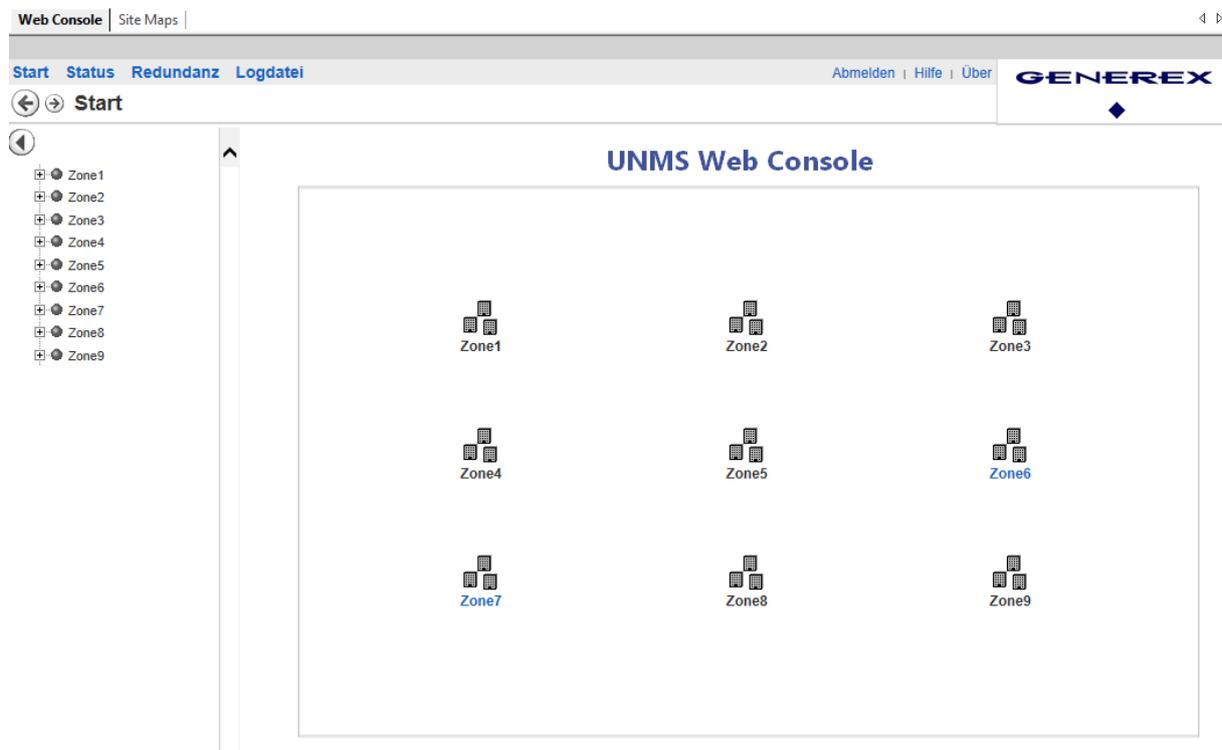
Installation abschließen.

Beim ersten Start der UNMS II werden Sie mit folgendem Screen begrüßt:



Um zu überprüfen, ob die UNMS II richtig installiert wurde und der IIS Service auch richtig läuft, drücken Sie bei Discover services zunächst auf Cancel und anschließend auf die kleine rote Ampel oben links, um die UNMS regulär zu starten.

Wenn Sie folgenden Screen sehen, ist die UNMS richtig eingerichtet und Sie können mit der Konfigurationsarbeit beginnen:

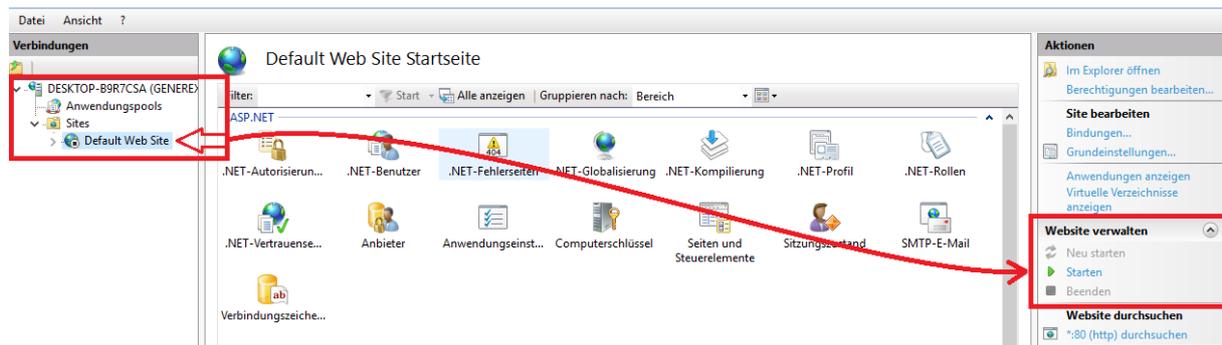


Das Webinterface zeigt eine noch unkonfiguriertes Standardlayout mit 9 vordefinierten Zonen. Da noch keine Geräte hinterlegt sind

Tipp: Wenn die UNMS beim Start kein Webinterface anzeigt: Überprüfen Sie den IIS

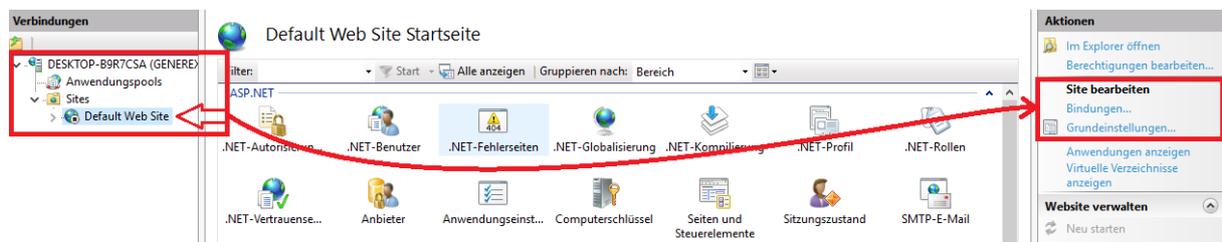
Der Internet Information Service ist ein sehr filigranes Werkzeug innerhalb einer Windowsinstallation.

1. Überprüfen Sie, ob die Webseitenverwaltung aktiv ist:



Gegenüber von Default Web Site findet sich der Punkt Webseite verwalten. Dieser Dienst muss gestartet sein, ansonsten liefert der IIS keine Webseiten an einen Webbrowser aus.

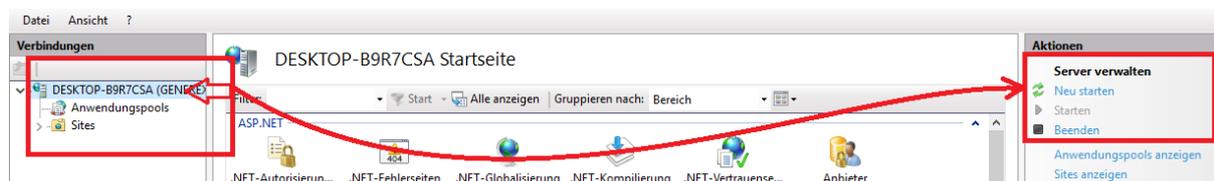
2. Überprüfen Sie die Bindungen im IIS



Wenn Sie dieses Fenster auf machen, finden Sie Portbindungen. Hier muss mindestens http Port 80 mit der IP-Adresse * zu finden sein, wenn Sie https nutzen möchten, entsprechend auch der Port 443:

Typ	Hostname	Port	IP-Adresse	Bindungsinform...
http		80	*	
https		443	*	

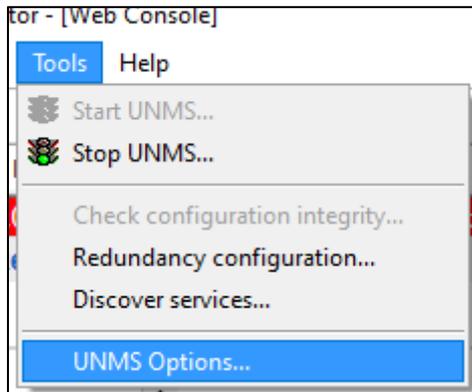
3. Starten Sie den IIS Service neu



Nach jeder Änderung im IIS selber sollten Sie den IIS Service neu starten damit alle Ihre Änderungen auch richtig eingelesen und initialisiert werden. Achten Sie darauf, noch einmal zu überprüfen, ob Punkt 1 im Fall eines Neustarts auch erfüllt wurde, da Sie ansonsten wieder in den selben Fehler laufen.

4. HTTPS für IIS und die UNMS aktivieren

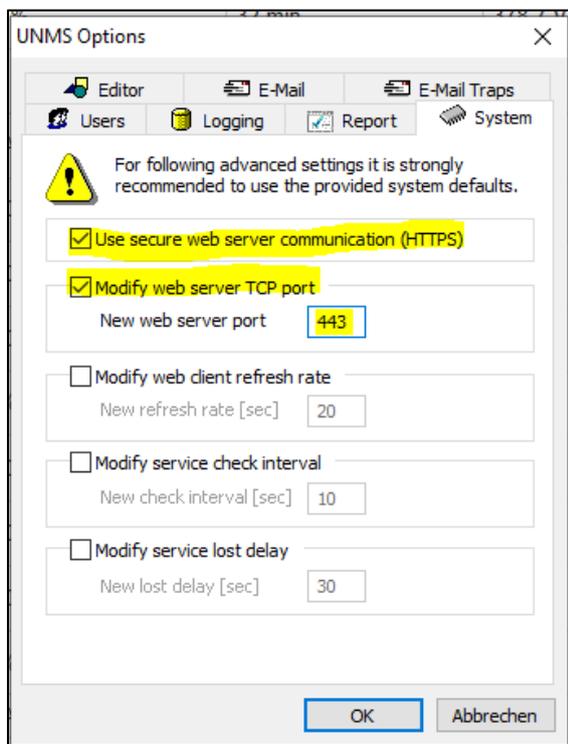
Für diesen Konfigurationsschritt benötigen Sie folgendes Menü:



Schritt 1: UNMS umstellen

Zunächst müssen Sie sicherstellen, dass die UNMS auch gewillt ist, über https zu kommunizieren. Öffnen Sie hierzu die UNMS Options und gehen dort auf den Reiter „System“:

Dort angekommen modifizieren Sie die Einstellungen „Use secure web server communication (HTTPS)“ und „Modify web server TCP port“:



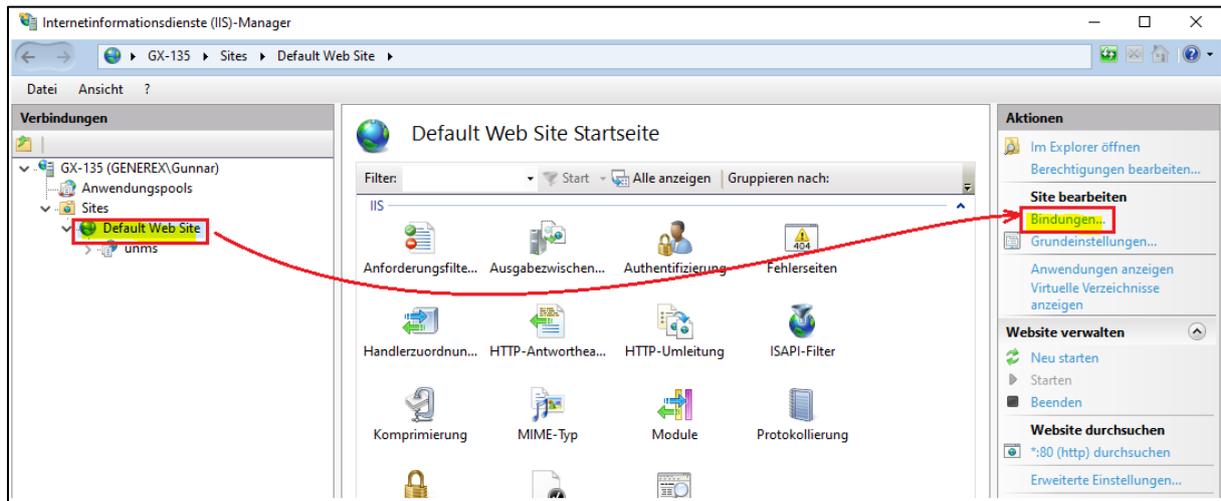
In diesem Beispiel wurde der Port 443 ausgewählt und die UNMS angewiesen, HTTPS zu verwenden.



-> Beenden Sie die Konfiguration, indem Sie zuerst speichern, danach die UNMS beenden und anschließend wieder starten.

Schritt 2: IIS einrichten:

Öffnen Sie zunächst den IIS Manager



Öffnen Sie den Reiter [Computername]>Sites>Default Web Site>UNMS

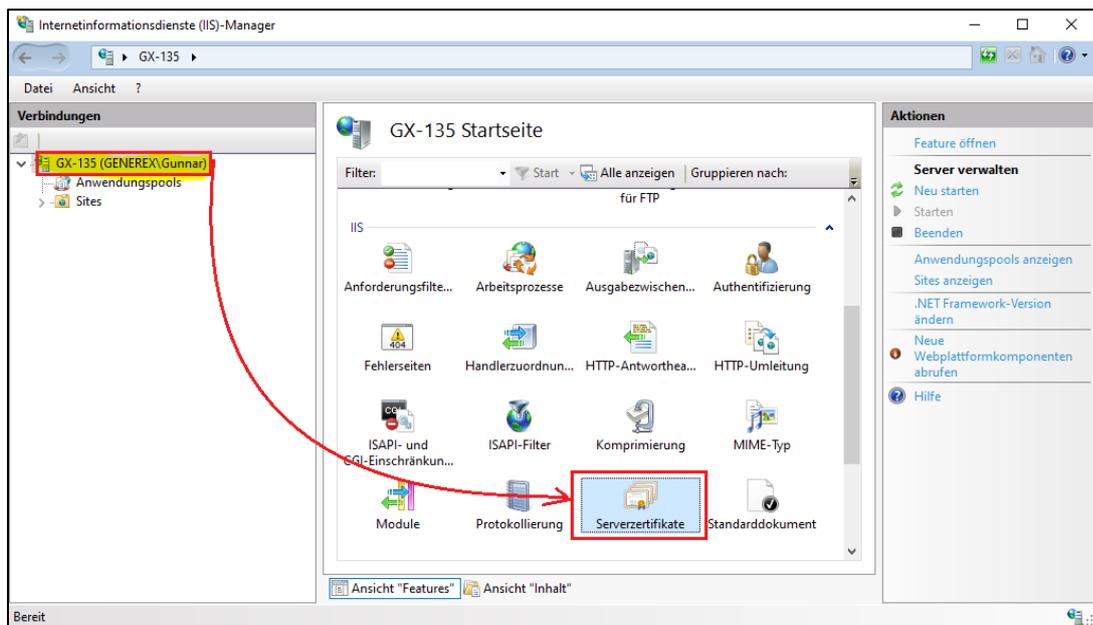
Auf der gegenüberliegenden Seite finden Sie dort unter Aktionen den Menüpunkt „Bindungen“. Hier ist normalerweise lediglich Port 80 für http – Anfragen auf die UNMS hinterlegt. Mit Hinzufügen können Sie jedoch beliebige Ports mit angeben. Wichtig hierbei ist jedoch:

1. Der Port muss frei (Verfügbar) sein
2. Der Port darf nicht von einer Firewall blockiert werden
3. Der Port muss zuvor in der UNMS bekannt gemacht worden sein

Wenn Sie ein Zertifikat zur Verfügung haben, können Sie den folgenden Schritt überspringen, ansonsten geht es hier weiter:

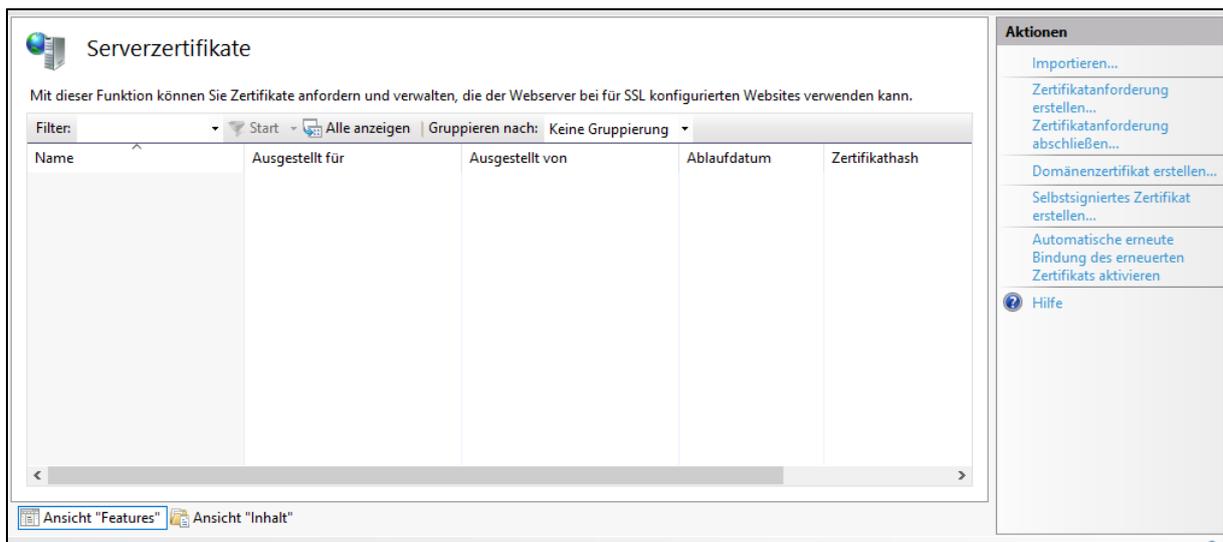
Zertifikat erstellen

Für diesen Schritt benötigen Sie folgendes Menü:



Um https nutzen zu können, benötigt man ein passendes Serverzertifikat. Wenn Sie unter Bindungen kein Zertifikat zum Auswählen zur Verfügung haben, können Sie sich dieses über den IIS relativ einfach eins erstellen. Öffnen Sie hierzu im Hauptmenü des IIS Managers den Punkt „Serverzertifikate“

Hier erhalten Sie eine Übersicht vorhandener Zertifikate und zahlreiche Verwaltungsfunktionen:

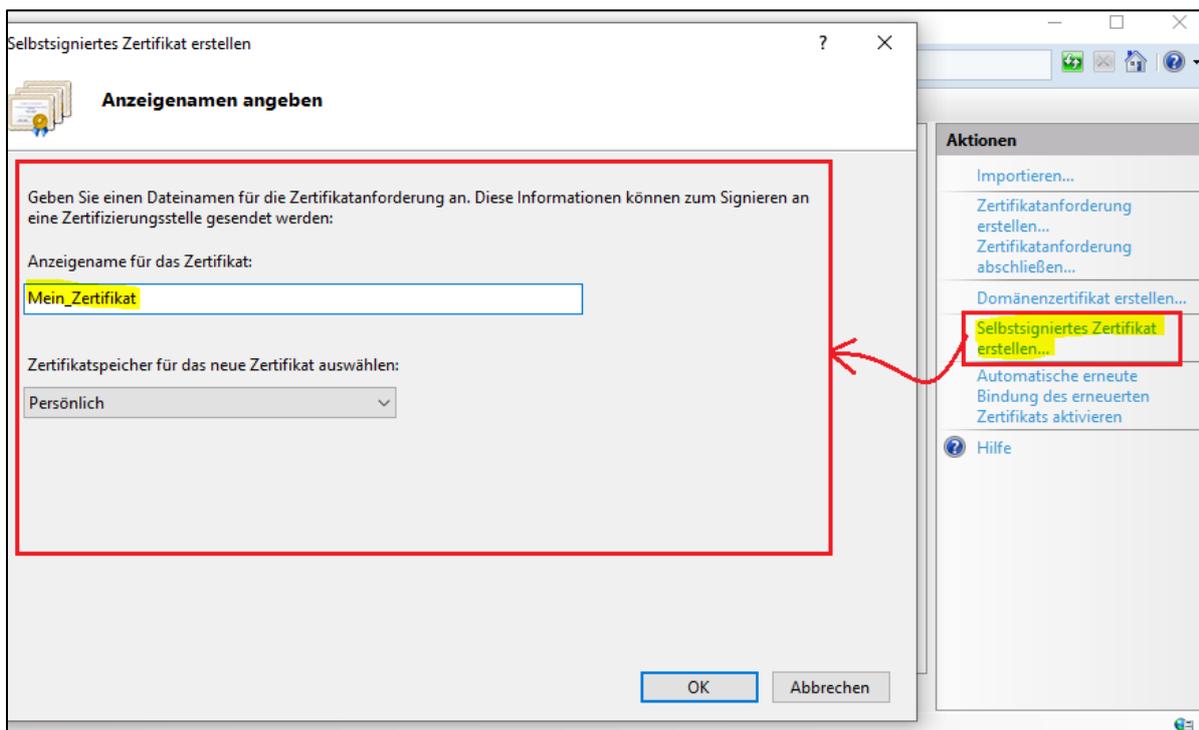


Da ein Zertifikat für die Verwendung von https zwingend notwendig ist, muss es zunächst entweder

1. Von einem Administrator bereitgestellt und von Ihnen importiert werden:
2. Von Ihnen kurzerhand selbst erstellt werden.

In diesem Beispiel reicht ein selbstsigniertes Zertifikat aus:

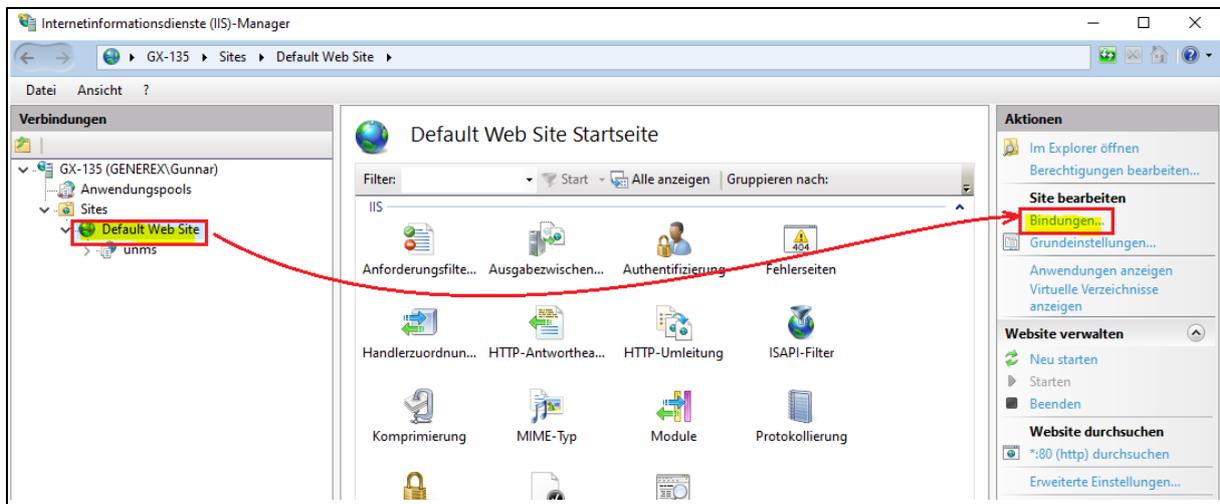
Der IIS erstellt selber ein Zertifikat und „beglaubigt“ seine Echtheit. Das geht deshalb, weil Sie als Nutzer natürlich wissen, dass der Server auch wirklich der ist, für den er sich ausgibt*. Benennen Sie Ihr Zertifikat und klicken Sie auf OK:



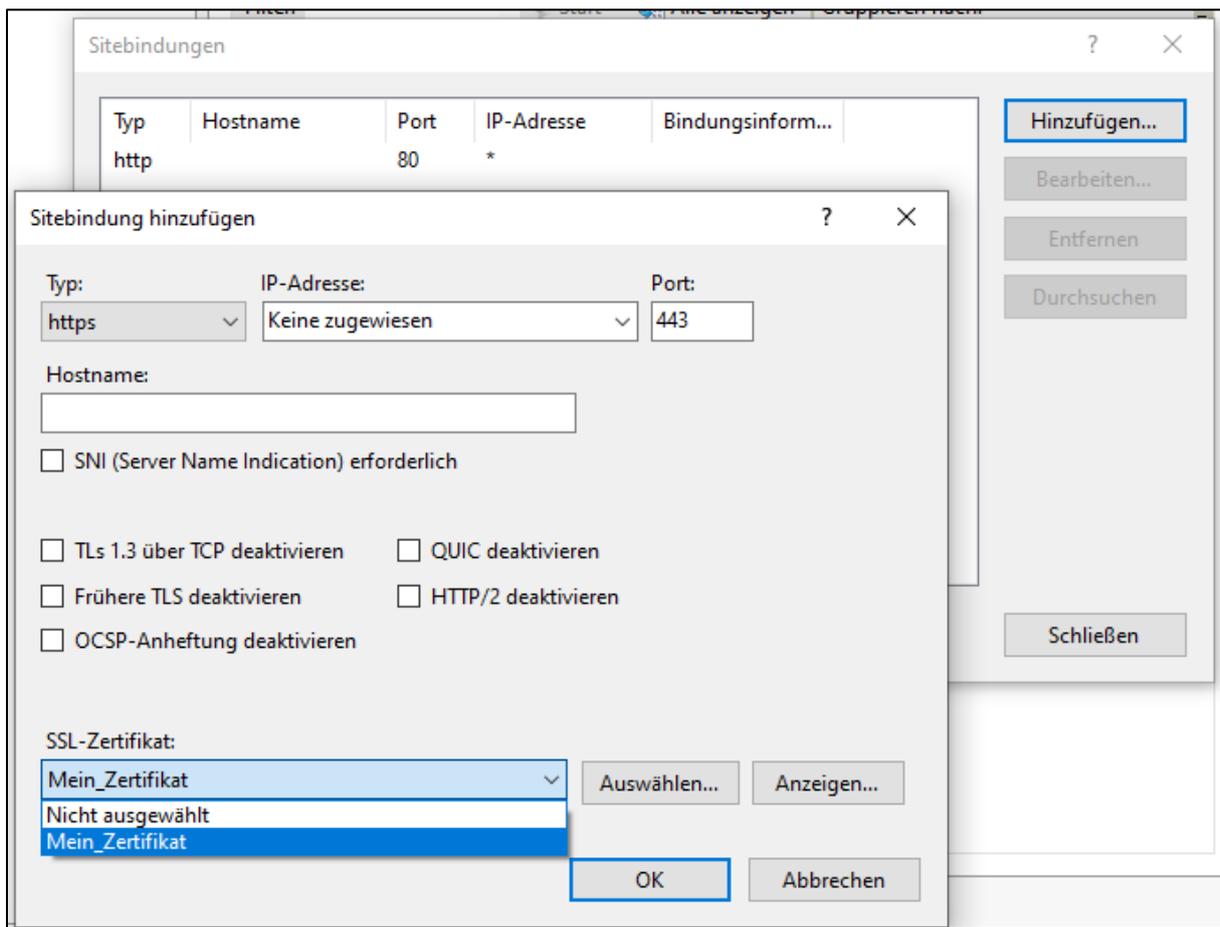
Name	Ausgestellt für	Ausgestellt von	Ablaufdatum	Zertifikathash	Zertifikatspeicher
Mein_Zertifikat	GX-135.generex.local	GX-135.generex.local	22.11.2022 01:00:00	AD7FE10457E5AD6C3A1A41B...	Personal

*)Der Webbrowser wird dennoch jammern, weil Ihr Server natürlich nicht offiziell authentifiziert wurde, aber das ist eine andere Geschichte, die mit den Sicherheitseinstellungen eines modernen Webbrowsers zusammenhängen.

Zurück zu den IIS Einstellungen unter „Bindungen“:



Ab jetzt ist es möglich, HTTPS einzurichten, da ein entsprechendes Zertifikat vorliegt:



Klicken Sie auf Hinzufügen, und

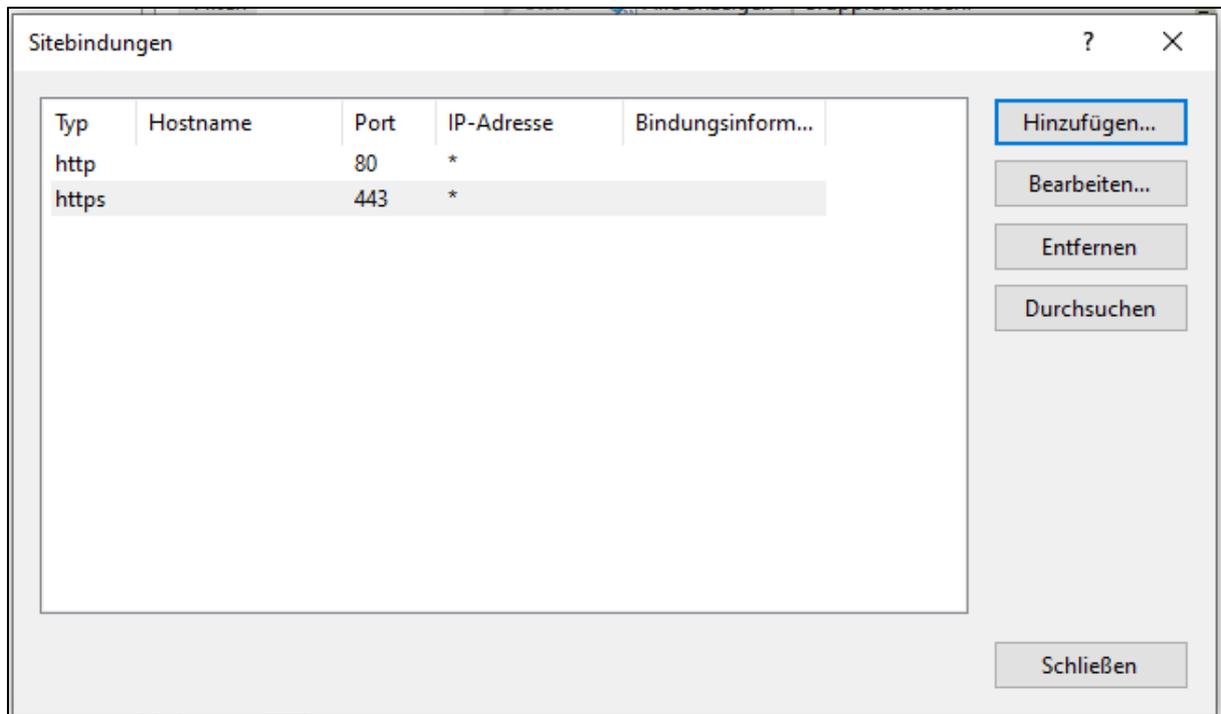
... wählen als Typ https aus

... geben den Port an, den Sie auch in der UNMS für https angegeben haben (in diesem Fall 443)

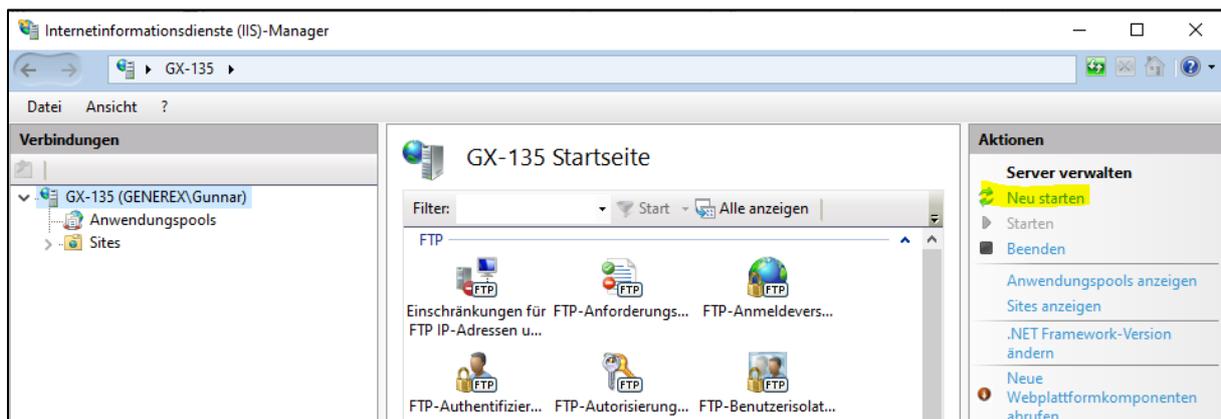
... Wählen als SSL – Zertifikat Ihr eben erstelltes Zertifikat aus

... Klicken OK, um die Einstellungen zu übernehmen.

Das Endergebnis sollte so aussehen:



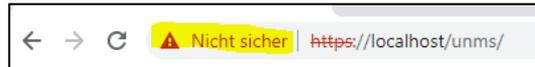
Um die Einstellungen aktiv zu schalten, klicken im IIS Managers auf „Neu starten“:



Anschließend können Sie über den Webbrowser via HTTPS auf den UNMS Server zugreifen:

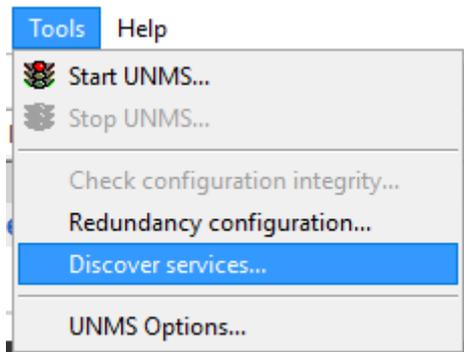


Wie bereits angedeutet: Es handelt sich um ein selbst signiertes Zertifikat. Der Webbrowser wird daher beim Start folgerichtig seine Bedenken äußern und sich auch weiterhin darauf hinweisen, bis ein offiziell authentifiziertes Zertifikat vorliegt, welches Sie an Stelle des selbst signierten Zertifikats verwenden:



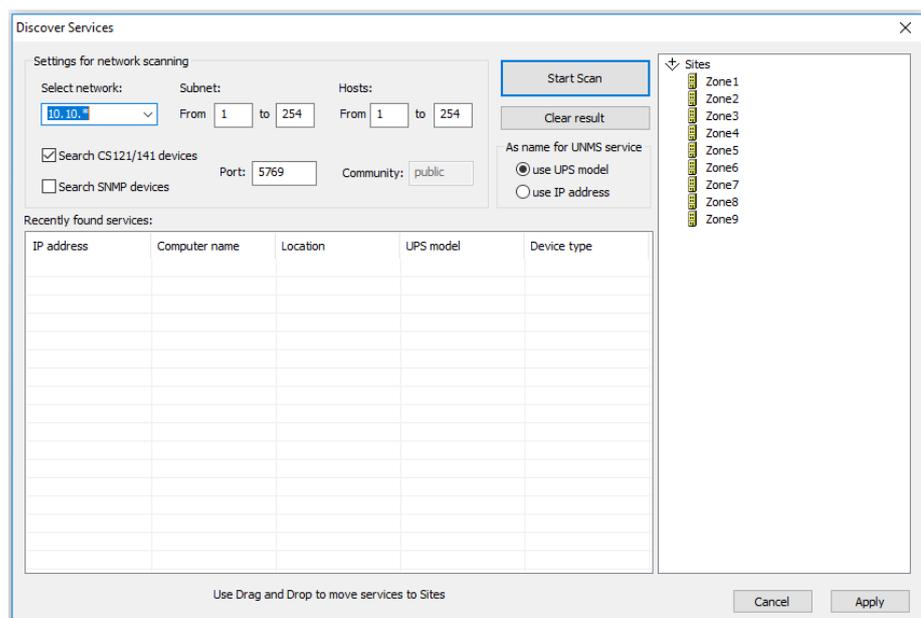
Auffinden und Einbinden von Geräten

Für diesen Konfigurationsschritt benötigen Sie folgendes Menü:



Wenn Sie die UNMS II das erste Mal starten, startet zunächst der Discovery Service. Mit diesem Service können Sie Ihr gesamtes Netzwerk auf IP-Basis nach eventuell verfügbaren Geräten scannen. Sollten Sie bereits auf Cancel gedrückt haben, um sich erst einmal zu orientieren, finden Sie diesen unter Tools wieder.

Der Discovery Service findet automatisch alle Geräte, welche sich via SNMP anzeigen lassen und bietet Ihnen diese für die weitere Konfiguration der UNMS II an.



Um Geräte zu finden, benötigt der Discovery Service ein paar weiterführende Informationen über Ihr Netzwerk, damit er weiß, wonach er suchen soll und in welchem Segment Ihres Netzwerks sich die gesuchten Geräte befinden.

Schritt 1: Netzwerkscan definieren

Geben Sie an, welcher Netzwerkbereich gescannt werden soll. Dies ist die dritte Zahl im IP-Adressbereich.

Der Bereich 15 - 27 scannt damit:

192.168.15.1 - 192.168.15.254
192.168.16.1 - 192.168.16.254
[...]

Geben Sie die ersten beiden Zahlen des IP-Netzwerks an z.B. 192.168.

Engen Sie den IP Adressbereich ein. Wenn Sie 100 - 150 eingeben, würden nur die IP-Adressen von 100-150 gescannt werden:
192.168.15.100 - 192.168.15.150
192.168.16.100 - 192.168.16.150
[...]

Geben Sie an, ob Sie nur nach CS121/CS141 - Geräten suchen möchten oder auch nach SNMP-tauglichen Geräten

Geben Sie den Port an, auf dem nach den Geräten gesucht werden soll.

Sobald Sie SNMP-Geräte konfiguriert haben, kann es notwendig sein, dass Sie der UNMS II die Community mitteilen müssen, da die Geräte ansonsten nicht antworten.

Select network

Mit den ersten beiden Oktetten definieren Sie das Basisnetzwerk, welches gescannt werden soll. Da die Anzahl der vorhandenen IP-Adressen sehr groß werden kann, ist die Eingabemöglichkeit eingeschränkt:

Geben Sie bitte die ersten beiden Zahlen Ihres Netzwerks ein:

192.168.
17.15.
158.75.

Subnet

Geben Sie hier den Bereich ein, der gescannt werden soll. Dieser definiert das dritte Oktett innerhalb der IP-Adresse. Anders als bei Select network geben Sie hier einen Adressbereich ein. Wenn Sie z.B. von netzwerksegment 100 – 103 scannen möchten, geben Sie diese beiden Werte ein. Die UNMS wird im Anschluss folgende Netzwerksegmente überprüfen:

192.168.100.xxx
192.168.101.xxx
192.168.102.xxx
192.168.103.xxx

Hosts

In großen Netzwerken werden IP-Adressbereiche traditionell aufgeteilt, um einen unkontrollierten Wildwuchs zu vermeiden. Die Art der Aufteilung ist dabei sehr unterschiedlich. Beispielsweise wird gerne der Host-Bereich 1-30 für Router und Switches verwendet, 31-50 dabb für Server, 51-60 für Drucker, ...

Wenn Ihnen die genaue IP-Adresse nicht bekannt ist, Sie jedoch wissen, dass es nur innerhalb eines bestimmten Bereichs sein kann, geben Sie hier die Startadresse und die entsprechende Endadresse ein. Wenn Sie z.B. von IP 100- 150 definieren, wird die UNMS im Anschluss wie folgt das Netzwerk scannen:

192.168.100.100
192.168.100.101
192.168.100.102
[...]
192.168.101.100
192.168.101.101
192.168.101.102
[...]

Bis letztendlich die IP-Adresse 192.168.103.150 erreicht wurde.

Tipp:

Achten Sie bei der Angabe der Adressbereiche unbedingt auf die richtige Voreinstellung, da die UNMS ansonsten sehr lange brauchen kann, da jede angegebene IP-Adresse exklusiv überprüft wird.

As name for UNMS service

As name for UNMS service

use UPS model

use IP address

Mit dieser Einstellung definieren Sie, ob die UNMS im nächsten Schritt die USV oder die IP-Adresse als Anzeigenahme übernehmen wird. Für den Scan-vorgang selber hat diese Einstellung eine untergeordnete Rolle.

In diesem Handbuch verwenden wir die Einstellung „use IP address“ – der innerhalb der UNMS angezeigte Name ist jedoch frei bestimmbar.

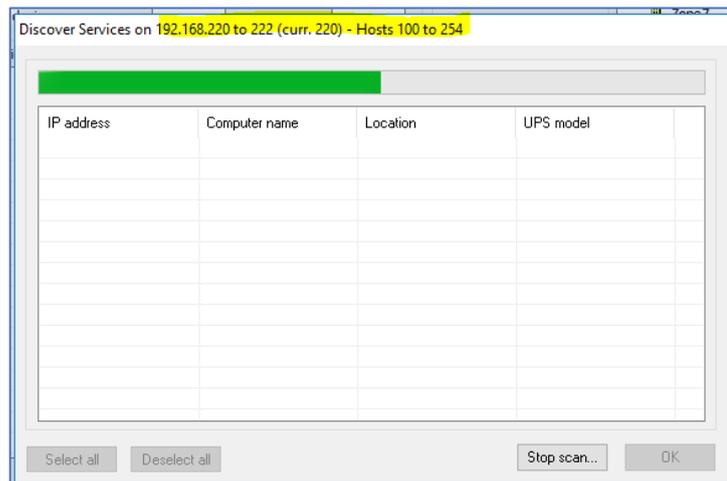
Scanfortschritt beobachten

Sobald Sie auf Start drücken, beginnt die UNMS mit dem Netzwerkskan. Im Scanfortschritt können Sie erkennen

- In welchem Netzwerksegment gerade der Scan durchgeführt wird
- Welcher IP-Adressbereich konkret gescannt wird.

In dem Screenshot können Sie z.B. folgendes ablesen:

- Gescannt wird das Netzwerk von 192.168.220.XXX bis 192.168.222.XXX
- Es werden jeweils die IP-Adressen 100 – 254 überprüft
- Mit (curr.220) befindet sich der Netzwerkskan im Netzwerk 192.168.220.XXX



Der grüne Indikatorbalken gibt Aufschluss über den Scanfortschritt des aktuellen Netzwerksegments (curr. 220). Der grüne Indikatorbalken zeigt den Fortschritt über bereits gescannte IP-Adressen.

Die Ergebnisse des Scans werden in der Liste darunter angezeigt:

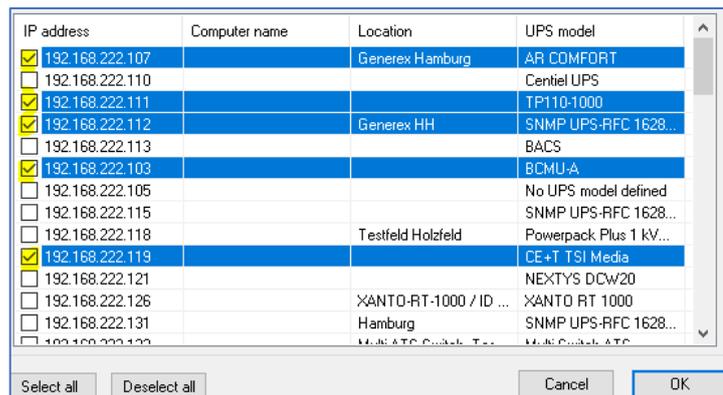
IP address	Computer name	Location	UPS model
<input type="checkbox"/> 192.168.222.107		Generex Hamburg	AR COMFORT
<input type="checkbox"/> 192.168.222.110			Centiel UPS
<input type="checkbox"/> 192.168.222.111			TP110-1000
<input type="checkbox"/> 192.168.222.112		Generex HH	SNMP UPS-RFC 1628...
<input type="checkbox"/> 192.168.222.113			BACS
<input type="checkbox"/> 192.168.222.103			BCMILA

Übernahme der Scanergebnisse in die UNMS

Im nächsten Schritt müssen die gefundenen Geräte an die UNMS übergeben werden.

Wählen Sie hierzu einfach die gewünschten Geräte aus, indem Sie bei der entsprechenden Checkbox den Haken setzen.

Wenn Sie alle Geräte ausgewählt haben, drücken Sie OK.



Die ausgewählten Geräte werden anschließend im Hauptfenster des Discovery Services unter Recently found services angezeigt:

IP address	Computer name	Location	UPS model	Device type
192.168.222.103			BCMU-A	CS121 compatible
192.168.222.107		Generex Hamburg	AR COMFORT	CS121 compatible
192.168.222.111			TP 110-1000	CS121 compatible
192.168.222.112		Generex HH	SNMP UPS-RFC 16...	CS121 compatible
192.168.222.119			CE+T TSI Media	CS121 compatible

Sie können jetzt einen neuen Scan mit einem anderen IP-Adressbereich durchführen, um weitere Geräte, die Sie mit der UNMS überwachen können, zu suchen und in diese Liste zu übernehmen.

Tipp:

Sie müssen nicht jedes Mal neu scannen, sobald Sie den Discovery Service schließen. Alle Geräte, die von Ihnen unter Recently found services abgelegt wurden, bleiben dort in der Liste, bis Sie entweder von Ihnen mit Clear Result entfernt oder aber auf die entsprechenden UNMS-Services verteilt wurden.

Geräte in die UNMS einbinden

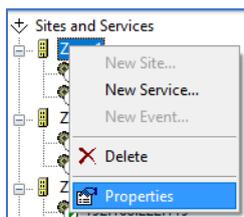
Die UNMS bietet bei der Installation als Grundeinstellung 9 sog. Zonen an, in die Sie via Drag'n'Drop die Geräte hineinschieben können.

Halten Sie einfach das gewünschte Gerät mit der linken Maustaste gedrückt, und ziehen Sie diese auf die entsprechende Zone.

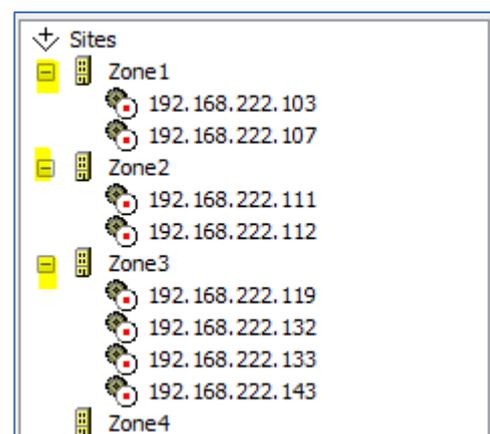
Dadurch wird das Gerät aus der Liste der Recently found Services entfernt und der entsprechenden Zone hinzugefügt.

Wenn alle Geräte verteilt wurde, drücken Sie auf Apply, um die Einstellungen entsprechend zu übernehmen.

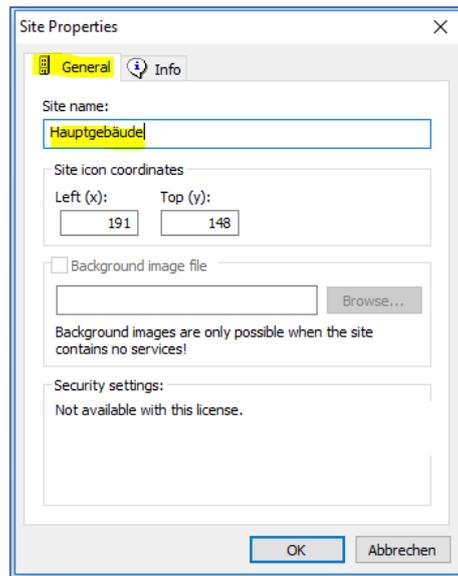
Anpassen der Zonen



Da das Wort „Zone 1“ nur bedingt aussagekräftig ist, bietet die UNMS kontextbezogen die Möglichkeit an, den Namen entsprechend anzupassen. Klicken Sie hierzu mit der rechten Maustaste auf die Zone und wählen anschließend im Kontextmenü die Option „Properties“ aus.



Es öffnet sich eine neue Registerkarte, welche die Eigenschaften dieser Zone anzeigt. Ändern Sie hier den Namen Zone 1 auf ein entsprechend angepassten Begriff.



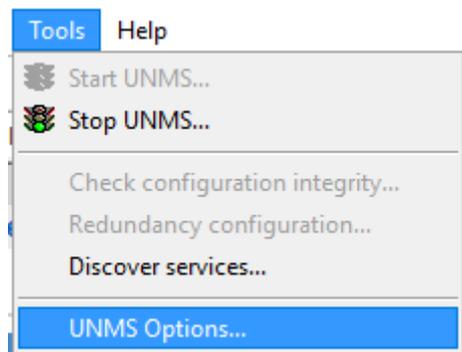
Wenn Sie fertig sind, drücken Sie OK, um die Einstellung zu übernehmen.

Speichern und erster UNMS Start



Sobald Sie alle Zonen unbenannt haben, drücken Sie oben links auf das Diskettensymbol zum Speichern und anschließend auf die rote Ampel, um den aktuellen Zustand – UNMS ist gestoppt – zu beenden. Die UNMS wird dann die neuen Daten permanent einspielen und die notwendigen Services wieder starten.

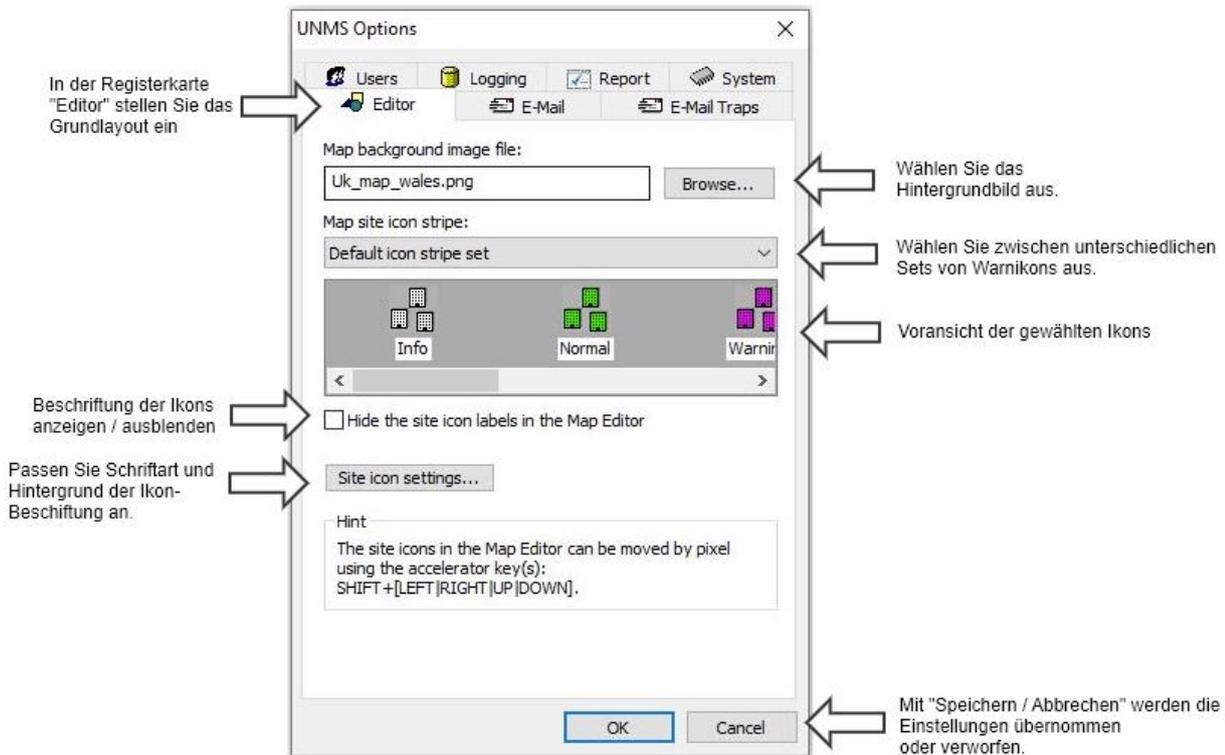
Optik der UNMS anpassen



Die UNMS II bietet Ihnen die Möglichkeit, die überwachten Geräte zu sortieren und entsprechend in geordnete Untergruppen abzulegen. Zusätzlich können Sie die überwachten Stationen auch mit beliebigen Hintergrundbildern erweitern und frei positionieren, um die Funktion einer überwachten Anlage entsprechend zu verdeutlichen.

Das erleichtert im Problemfall die Zuordnung zu einer Halle, einem Gebäudekomplex, einer bestimmten Systemkomponente, etc.

Öffnen Sie zunächst unter Tools die UNMS Options. In dieser Sammlung von Registerkarten können Sie zahlreiche Grundeinstellungen durchführen, unter anderem auch das Bild anpassen. In der Registerkarte Editor können Sie das allgemeine Grundlayout Ihren Vorstellungen anpassen:



Das Basisbild anpassen

Wählen Sie eins der bereits enthaltenen Bilder aus oder erstellen Sie sich eine eigene Grafik die zu dem Anwendungsszenario entsprechend passt. Beachten Sie bitte, das Bild muss von den Systemrechten her im entsprechenden Bildverzeichnis der UNMS II abgelegt sein, da Sie ansonsten zwar das Bild ausgewählt, jedoch letztendlich nicht verwendet werden kann.

Die UNMS II erstellt keine Kopien von Bilddateien aus anderen Verzeichnissen, Bilder müssen von Hand im PNG-Format in das UNMS-Verzeichnis kopiert werden. Das Standardverzeichnis lautet:

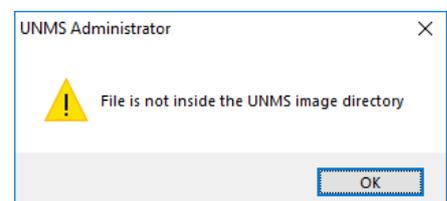
C:\UPS\unmsII\www\image

Das Ikon-Set anpassen

Im selben Verzeichnis: (C:\UPS\unmsII\www\image) finden Sie auch alle Ikonsets, die von der UNMS II angeboten werden:

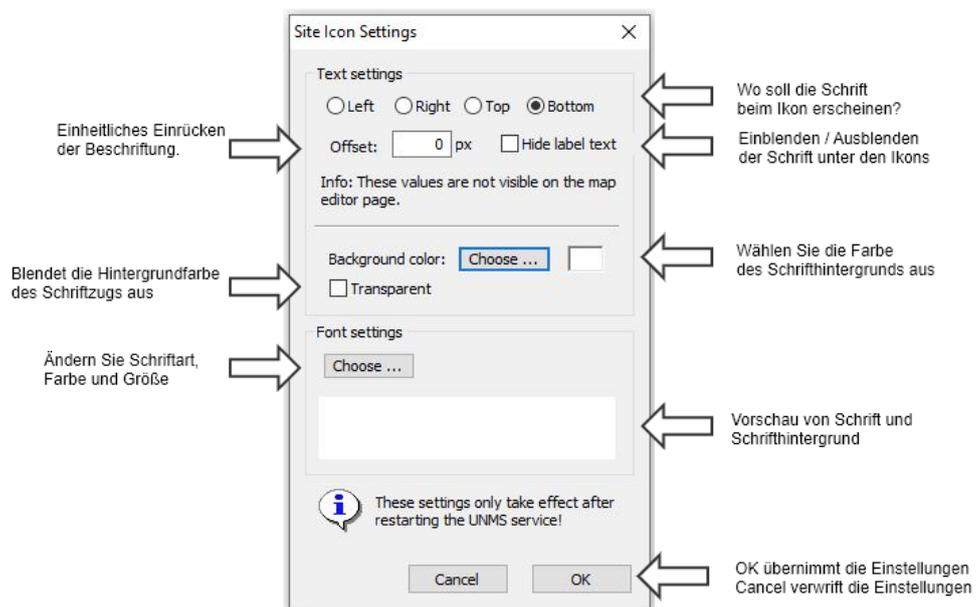


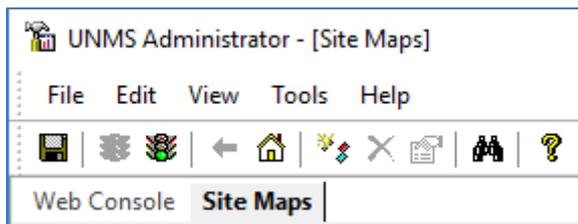
Sie können die Ikon nach belieben anpassen, indem Sie neue Ikon erstellen und die Dateinamen entsprechend umbenennen. Da es sich hierbei um Standard gif – Dateien handelt, können Sie auch beliebige animierte Ikon verwenden.



Beschriftung der Ikon anpassen

Neben dem Ikon-Set an sich können Sie zahlreiche Anpassungen an der Beschriftung der Ikon und dem Hintergrund des Schriftbildes durchführen, um die Lesbarkeit der Beschriftung anzupassen:



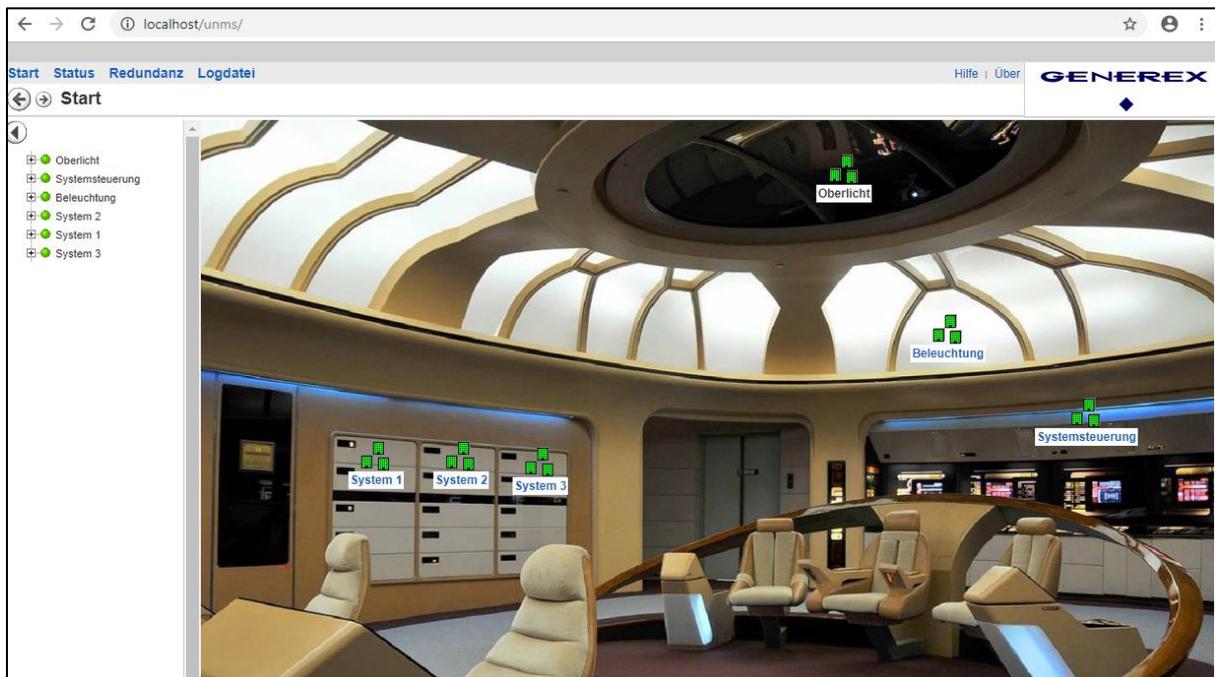
Ikons auf dem Hintergrundbild zurechtschieben

Unterhalb der Befehlszeile finden Sie die Registerkarten "Web Console" und "Site Maps". Die Webkonsole ist die Vorschau, mit der Sie den webbasierten Teil der UNMS II-Oberfläche betrachten und Funktionen testen können. Änderungen werden angezeigt, sobald Sie die Einstellungen speichern und die UNMS neu starten. Unter Site Maps können Sie die Ikons nach belieben verschieben und umbenennen. Standardmäßig ist die Webkonsole aktiv. Wechseln Sie zu den Site Maps und verschieben Sie die Ikons oder passen die Namen der Labels an:

**Tipp:**

In den Site Maps können Sie nach Belieben die Ikons verschieben, die UNMS wird erst dann die Einstellungen übernehmen, wenn Sie nach dem Speichern den UNMS Service neu starten. Sie können also die UNMS entsprechend konfigurieren während Sie über die Web Console von Außerhalb regulär arbeitet.

Speichern, beenden und Neustarten wird Ihre Einstellungen entsprechend in das System permanent übernehmen und den UNMS Service neu starten.
Den Erfolg können Sie im Administrationsbereich der UNMS II über die Web Console anschauen oder über einen Webbrowser, indem Sie die UNMS II Websicht aufrufen:



Erweiterte Grafikanpassungen Sub-Screens einrichten

Aus technischen Gründen ist es nicht möglich, eine Zone und Services – also überwachte Geräte - zusammen anzuzeigen.

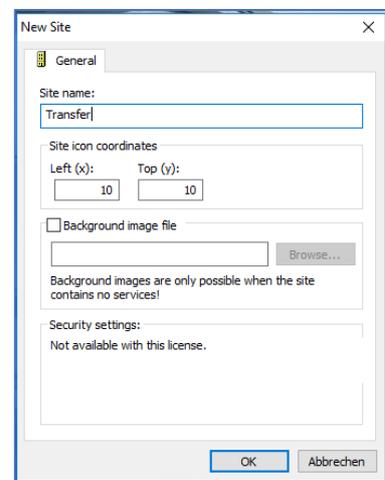
Entweder haben Sie in einer Zone weitere untergeordnete Zonen eingerichtet, in denen sich dann die Services befinden, oder aber Sie in der obersten Ebene eine Zone eingerichtet, in der sich direkt die überwachten Geräte befinden.

Um in diesem Fall die Systemsteuerung um einen Sub-Screen zu erweitern, müssen Sie also ein wenig Vorarbeit leisten:

Verschieben Sie alle Services temporär in eine andere Zone

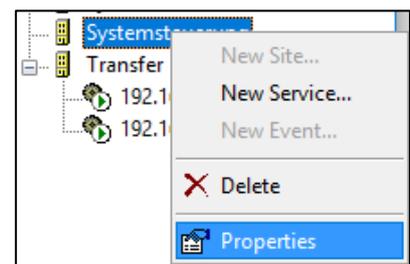
Damit Ihnen nicht versehentlich ein Gerät verloren geht, erstellen Sie sich eine eigene Zone, die Sie eindeutig benennen, z.B. „Transfer“ oder „Temporär“.

Da Sie die Zone hinterher wieder gelöscht wird, taucht sie in der aktuellen Websicht der UNMS II gar nicht erst auf.

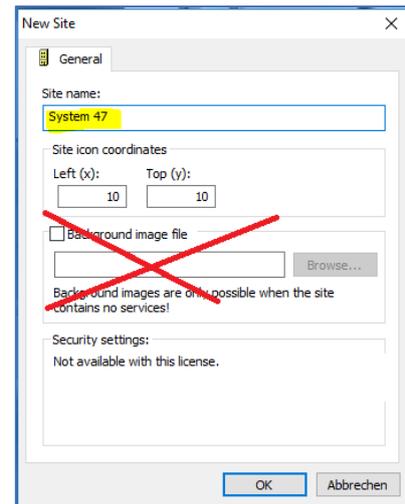


1. Klicken Sie bei der Systemsteuerung im Site Explorer auf Properties, um die Objekteigenschaften aufzu rufen. Da in dieser Zone keine Services mehr enthalten sind, können Sie jetzt ein eigenes Hintergrundbild zuweisen und damit den Charakter dieser Zone verändern:

Sobald Sie ein Bild entsprechend zugewiesen haben, können Sie untergeordnete Zonen einbinden, jedoch keine direkten Services mehr.



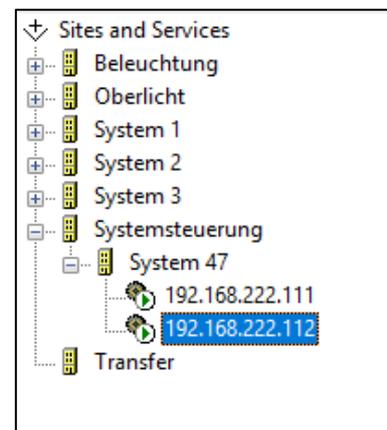
- Legen Sie jetzt in der Systemsteuerung eine neue Zone an, aber verzichten Sie auf das Vergeben eines Hintergrundbilds. Dadurch können Sie später in diese neue Unterzone die zwischengeparkten Services ziehen und entsprechend anzeigen lassen.



- Verschieben Sie anschließend die zwischengeparkten Services in die untergeordnete Zone. Im Anschluss können Sie dann die nicht mehr benötigte Transferzone löschen, da diese keine weitere Funktion mehr erfüllt.

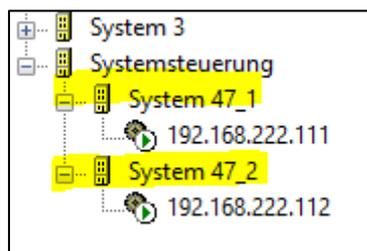
Tipp:

Bitte beachten Sie, dass diese Möglichkeit nur dann gegeben ist, wenn Sie in Schritt 3 kein Hintergrundbild definiert haben.

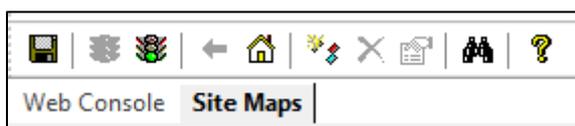


Wenn Sie die beiden Geräte nicht in einer Maske stehen haben wollen...

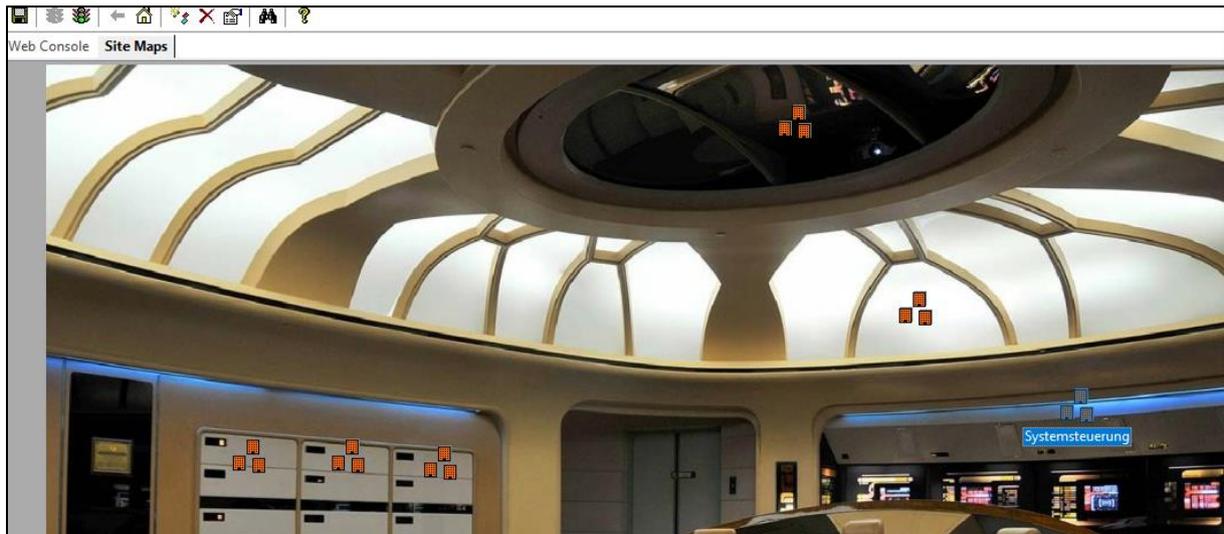
In diesem Fall erstellen Sie einfach zwei getrennte Zonen und schieben die Anlagen entsprechend in jeweils eine eigene Zone:



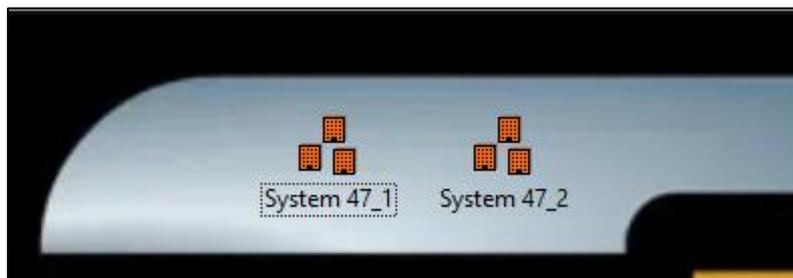
Anpassen der Ikons im Sub-Screen



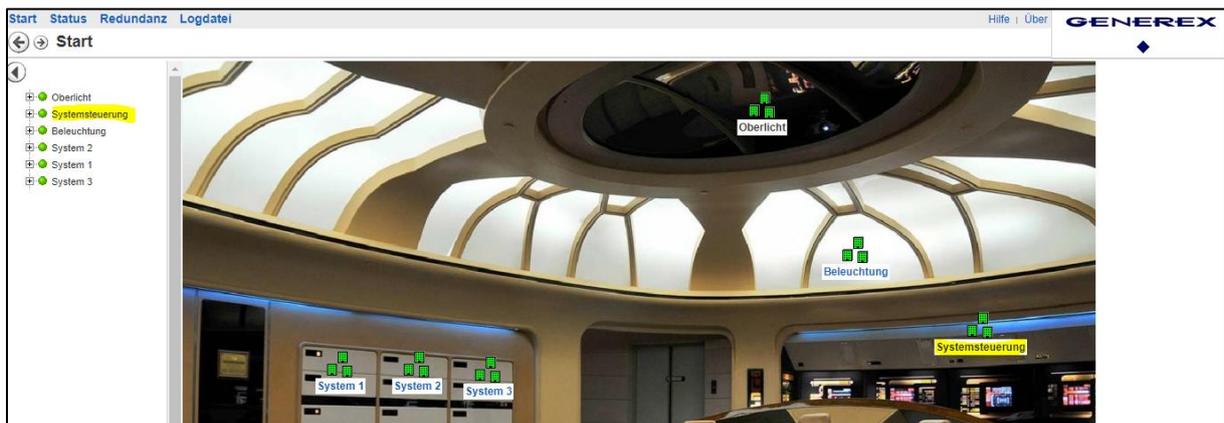
Klicken Sie hierzu oben links auf Site Maps, um Ikons verschieben zu können. Sie werden zunächst den Startbildschirm sehen:



Machen Sie jetzt einen Doppelklick auf das Icon „Systemsteuerung“, um in den entsprechenden untergeordneten Screen zu öffnen. Dabei werden Ihnen die beiden Icons – in diesem Fall System 47_1 und System 47_2 – auffallen:



Verschieben Sie diese an den Ort, an dem Sie diese haben möchten und drücken Sie auf Speichern, Beenden und Neustarten. Über die Webkonsole SubScreen zugreifen, indem Sie die Systemsteuerung öffnen. Dabei wurden die Positionen der Icons an die von Ihnen gewünschte Position angepasst.



Schriften im Subscreen anpassen

Diese Funktion wird dann interessant, wenn man z.B. einen Gebäudeplan hat, wo unterschiedliche USV-Anlagen verteilt sind und man eine Aufteilung zwischen Notfallanlagen und weniger wichtigen Anlagen wünscht. Bei einem Kreuzfahrtschiff wäre das z.B. Unterschiedliche Systeme oder aber hierarchisch aufgebaute Unterverteiler.

- Im Überblick sind alle USV-Systeme sichtbar
- In der Systembezogenen Seite befinden sich lediglich die diesem Stromkreis zugeordneten Systeme

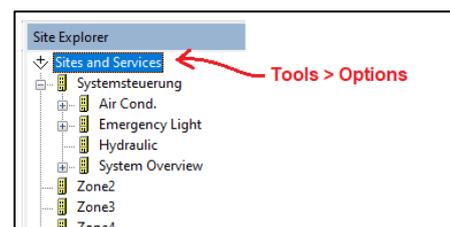
Innerhalb einem komplexen Power Distributed Network kann man auf diese Weise den Überblick behalten, da Schriftgröße und Schrift hintergrund für den jeweiligen Subscreen frei definiert werden können.

So passen Sie die Schriften im Subscreens an:

Hier ist es wichtig, die Systematik hinter dieser Funktion zu verstehen: Alles, was Sie in einer Site ändern, wirkt sich auf die Sites darunter aus.

Daraus ergibt sich folgende Anzeigelogik:

Unter Tools >Options stellen Sie global Schriftbild, Farbe, Größe, etc. ein. Von der Logik her wird das im Site Explorer bei SITES AND SERVICES aufgehängt. Was bedeutet, dass alles, was darunter zu sehen ist, die entsprechenden Einstellungen global übernimmt.



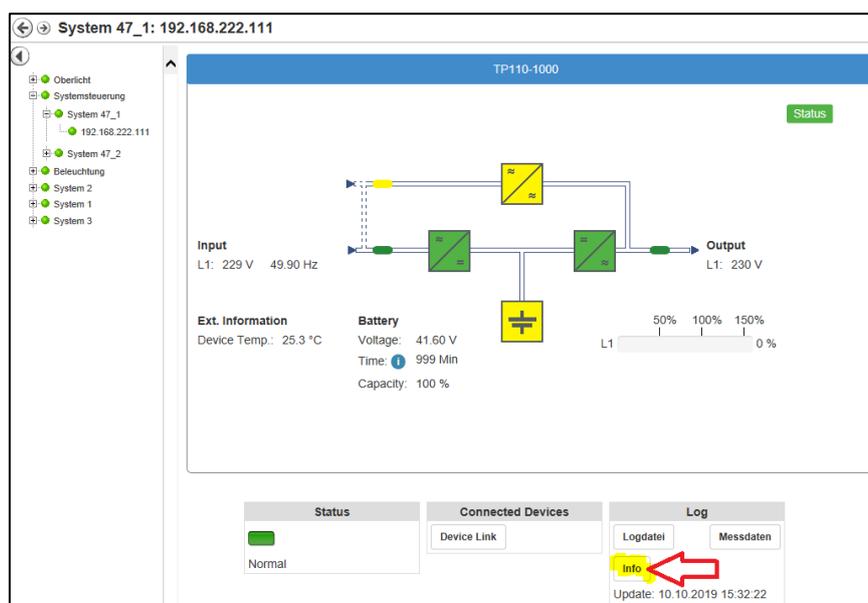
Jetzt bietet die UNMS an, Schriften für einzelne Sites lokal zu überschreiben, allerdings greifen die Änderungen immer bei der untergeordneten Site:

Wenn Sie also im Site Explorer auf „Eigenschaften“ bei der Site Systemsteuerung klicken, und dort Schriftbild, Größe, etc. anpassen, dann wirkt sich das auf alle untergeordneten Sites aus, nicht aber auf die Site „Systemsteuerung“ – für die bleibt die übergeordnete Einstellung gültig.



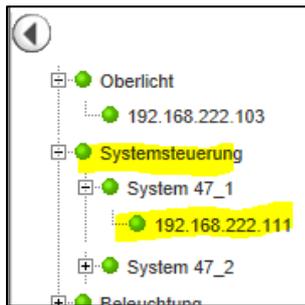
Das kann man jetzt beliebig verschachteln und nach „unten“ ändern, solange man bedenkt, dass die jeweilige Sub-Site, die die Ikon aufnehmen soll, ein Hintergrundbild hinterlegt hat und damit keine Services aufnehmen kann.

Zusätzliche Informationen hinterlegen



Wenn Sie den USV-Screen innerhalb der UNMS jetzt betrachten, wird Ihnen unter Log ein Info-Button angeboten. Hier können Sie zusätzliche Informationen zu dem überwachten Gerät einbinden. Jedes über den Discovery Service eingebundene Gerät liefert als Basis-Daten zunächst einmal das USV-Modell (sofern verwendet) sofern die eigene IP-Adresse.

Gerät im Site Explorer finden

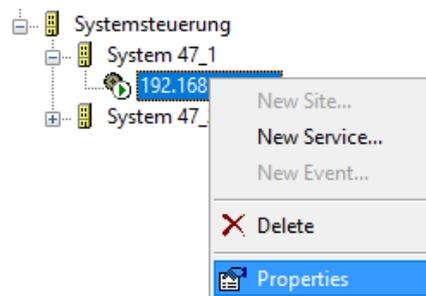


Der Verzeichnisbaum der Weboberfläche liefert Ihnen die Information, wo Sie im Site Explorer das Gerät wiederfinden können.

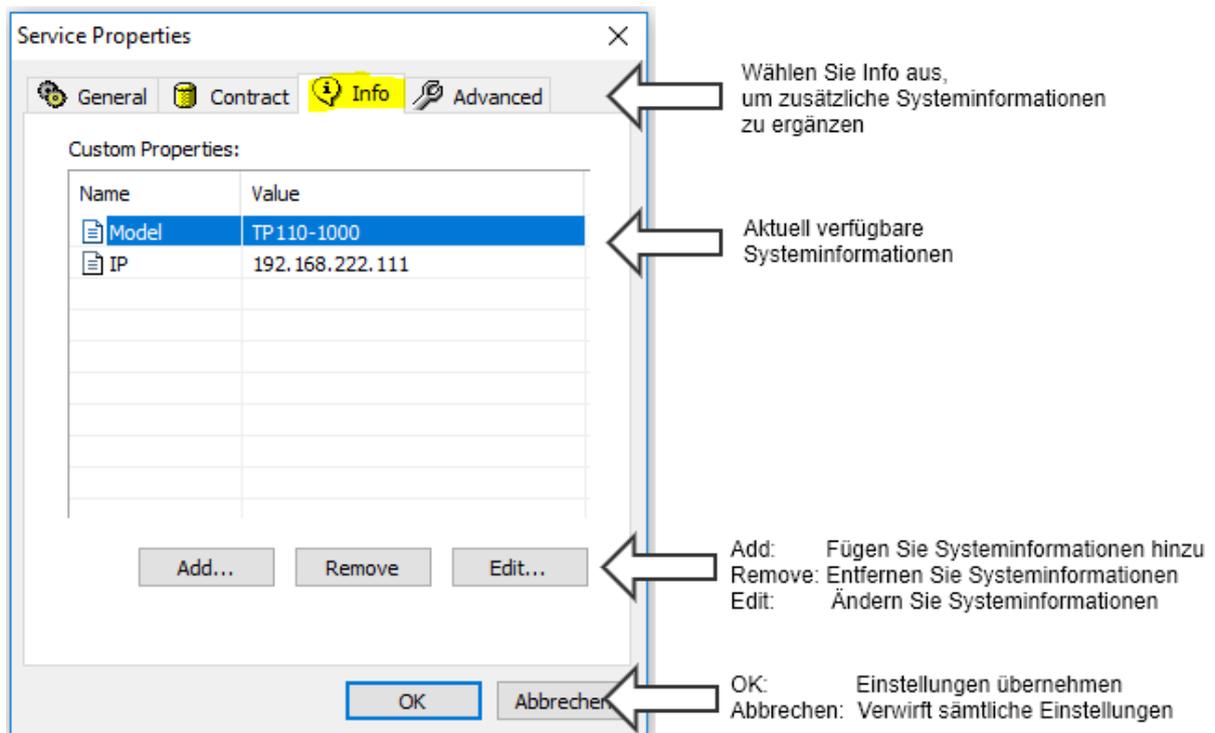
In diesem Beispiel würde das gesuchte Gerät innerhalb der Systemsteuerung zu finden sein, ganz exakt unter System 47_1

Öffnen Sie nun in der Adminkonsole auf der rechten Seite den Site Explorer und navigieren Sie zu der entsprechenden Ip- Adresse.

Wählen Sie anschließend mit der rechten Maustaste die IP-Adresse aus und wählen Sie im Kontextmenü Properties auf, um die Objekteigenschaften zu öffnen:



Wählen Sie anschließend die Registerkarte *Info* aus.



Ändern und Hinzufügen von Informationen:

Klicken Sie auf Add..., um weitere Informationen zu den Bestandsdaten hinzuzufügen:

Property type:

Die UNMS II unterstützt zwei unterschiedliche Möglichkeiten, Informationen zu hinterlegen.

Plain Text

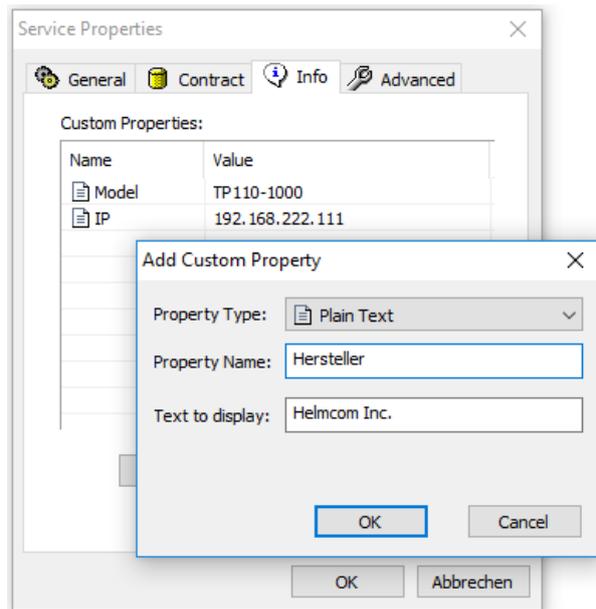
Die Information wird als Text angezeigt.
Sie können beliebige Informationen hinterlegen:

- Service-Telefonnummern
- Mail-Adressen
- Verantwortliche Fachbereiche
- Rechnungsnummern

Hyperlink

Es wird ein http-Link angezeigt, welcher entsprechend anklickbar ist. Hinterlegen Sie z.B.

- Links zu Hertsellerseiten
- Serviceformulare
- Online-Handbücher
- Downloadquellen



Wenn Sie die Einstellungen vorgenommen haben, drücken Sie auf OK, um den neuen Eintrag zu der Liste hinzuzufügen.

Tip

Wenn Sie Bestandsdaten ändern möchten wählen Sie einfach den entsprechend Listeneintrag und aus und klicken auf „Edit...“.

Entfernen von Einträgen

Wählen Sie den Eintrag aus und drücken Sie auf „Remove“. Der Eintrag wird aus der Liste entfernt.

Aktivieren der Änderungen

Die UNMS hat die Informationen zwar gespeichert, jedoch noch nicht in die aktive Konfiguration übernommen. Die Änderungen werden angezeigt, sobald Sie oben links im Administrationsbereich Speichern, Beenden und Starten geklickt haben.

Die unter Service Properties konfigurierte Liste...

Name	Value
Model	TP110-1000
IP	192.168.222.111
Hersteller	Helmcom Inc.
Link	www.generex.de

Info	
Model	TP110-1000
IP	192.168.222.111
Hersteller	Helmcom Inc.
Link	Generex

.... Anzeige im Webinterface unter *Info*

System 47_1: 192.168.222.111

TP110-1000

Status

Input
L1: 229 V 49.90 Hz

Output
L1: 230 V

Ext. Information
Device Temp.: 25.3 °C

Battery
Voltage: 41.60 V
Time: 999 Min
Capacity: 100 %

L1 50% 100% 150% 0 %

Status: Normal

Connected Devices: Device Link

Log: Logdatei, Messdaten

Info (highlighted with a red arrow)

Update: 10.10.2019 15:32:22

Tipp

Die hier abgelegten Informationen sind nicht auf dem entsprechenden Webmanager gespeichert, sie sind ausschließlich in der UNMS hinterlegt.

Vertragsdaten und Servicelevel hinterlegen

Die UNMS kann sehr vielfältig benutzt werden. Eine der interessanteren Funktionen ist der automatische Abgleich von gültigen Serviceverträgen über die Wartung von Notstromversorgungen und dem dazugehörigen Service-Level. Je nach Blickwinkel kann hierbei ein Kunde entweder sehen, bis wann ein Fehler innerhalb der USV von seinem Vertragspartner gelöst worden sein müsste oder aber wie viel Zeit ein Service-Anbieter hat, bis er einen Kunden spätestens bedient haben muss.

Service Properties

General Contract Info Advanced

Contract
ID: Vertrag: 12947 State: Active Edit...

UPS
Model: Ultramax 17 Baytech 4
Serial No.: 2834934kdhfk3849347

Customer
Company: Helmcom Inc
Address... Helms klamm 3
Rohan
More customer data...

OK Abbrechen

Wählen Sie Contract aus, um erweiterte Service- und Vertragsinformationen zu ergänzen.

Definieren Sie die Servicevertragsnummer, den Servicelevel und den aktiven Status.

Geben Sie das USV-Modell und die Seriennummer an.

Geben Sie die Kundendaten an

zusätzliche Kundendaten und Memos, interne Informationen über Standort, etc.

Nachdem Sie gespeichert, beendet und neu gestartet haben, können Sie die neuen Informationen unter Info anzeigen lassen:

Status	Connected Devices	Log
 Normal	Device Link	Logdatei Messdaten Info ← Update: 10.10.2019 15:32:22

Contract	
Contract ID	Vertrag: 12947
Contract Status	Active
UPS Model	Ultramax 17 Baytech 4
UPS Serial No.	2834934kdhfk3849347
Customer Company	Helmcom Inc
Customer Address	Helms klamm 3 Rohan
Contact Person	Max Mustermann
Contact Phone	040 1234567
Contact Fax	040 12345679
Contact E-Mail	max.mustermann@musterdorf
Notes	Dieser Kunde ist sehr schnell nervös und neigt dazu, Systemhinweise als Fehler zu interpretieren
Contract Level	4
Contract Start	08.10.2019
Contract End	11.10.2019

Ändern der Grundeinstellungen

Es kommt immer wieder vor, dass sich grundlegende Einstellungen ändern. In machen Fällen ist es lediglich die IP-Adresse, in anderen Fällen ändert sich mit der verwendeten SNMP- Karte die komplette Abfragemethodik selber.

In dem Reiter General können Sie diese grundsätzlichen Daten an die jeweiligen Umstände anpassen.

General
Contract
Info
Advanced

Site name:

Service

Name:

Group: STANDARD

Connection type:
CS121/141 compatible (UPSTCP)

DNS name or IP address: UPSTCP Port:

Schließen
Abbrechen

Wählen Sie General aus, um Grundeinstellungen dieses Geräts zu ändern.

Aktivieren / Deaktivieren Sie die Überwachung des Geräts.

Ändern Sie den Anzeigenahmen und passen Sie ggfs die Redundanzgruppen an.

Passen Sie die Abfrage des Zielgeräts an Ihre Infrastruktur an.

Definieren Sie die IP-Adresse oder den Hostnamen des Zielgeräts und passen Sie Port bzw. SNMP-Community an.

Tipp

Jeder Reiter wird grundsätzlich unabhängig von den anderen eingegebenen Informationen einzeln behandelt. Ggfs. müssen Sie also auch andere Reiter öffnen und entsprechende Service- und Vertragsdaten anpassen.

Site Name

Dieser Punkt ist nicht verhandelbar – er ändert sich, wenn Sie via Drag'n'Drop im Site Explorer dieses Gerät in eine andere Zone verschieben.

Service (On/Off)

Wenn Sie temporär ein Gerät nicht überwachen möchten, können Sie den Haken entfernen. Das Gerät wird anschließend in der UNMS aufgeführt aber entsprechend als „Deaktiviert“ angezeigt und aus der Echtzeitüberwachung ausgeschlossen. Sollte es ein Problem mit dem Gerät geben, wird kein Alarm ausgelöst.



Da die Links in der Webkonsole entweder auf das Gerät selber verweisen oder aber innerhalb der UNMS eingegeben wurden, funktionieren gibt es hier Abweichungen:

Info	Die Daten sind in der UNMS abgelegt, der Link funktioniert immer
Device Link	Öffnet einen Webbrowser, und versucht auf das Gerät zuzugreifen. Dieser Link funktioniert nur, wenn das Gerät auch erreichbar ist.
Logdatei	Liest die Logdateien vom Zielgerät aus. Dieser Link funktioniert nur, wenn das gerät auch verfügbar ist.
Messdaten	Das Datalog Chart des CS141 / CS121, nur verfügbar, so

Name / Group

Name ist der direkte Anzeigenahme innderhlab des Webinterfaces der UNMS II. Der Name kann frei angepasst werden, so dass Sie innerhalb der Webanzeige sich schnell über Standort, Funktion, etc. informieren können.

Mit Group definieren Sie spezielle Redundanzgruppen innerhlab der UNMS, welche dann ggfs. mit einer gesonderten Konfiguration ausgerüstet werden können. Näheres erfahren Sie im Kapitel „Redundanzgruppen einstellen“

Connection type

Diese Einstellung muss nur dann geändert werden, wenn Sie die Zielkarte komplett ändern, z.B. wenn Sie die USV austauschen und eine nicht mit dem CS141 kompatible Karte verwenden.

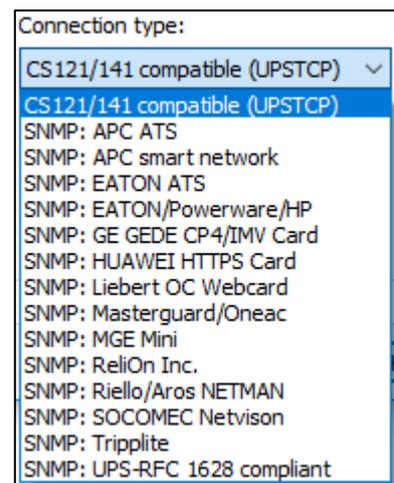
Hintergrund ist, dass es zwar ein paar allgemeine Standarts gibt, wie eine Kommunikation stattfinden sollte, es jedoch keine rechtliche Grundlage gibt, die Hersteller zwingt, sich wirklich an eine einheitliche Basis zu halten.

Viele Hersteller haben zudem eigene Produkte und Monitoringlösungen auf dem Markt und sind selbstverständlich bestrebt, ihre eigene Lösung bestmöglich zu vermarkten.

Die UNMS II ist darauf ausgelegt, möglichst offen mit anderen Systemen und Karten umzugehen, es kann jedoch notwendig sein, dass herstellerepezifische Konfigurationen auf der Zielkarte selber durchgeführt werden müssen, damit eine Kommunikation aufgebaut werden kann.

Im Zweifelsfall wenden Sie sich an das GENEREX Support Team:

support@generex.de



DNS name or IP-Adresse / UPSTCP Port (Community)

IP-Adresse und DNS

Die UNMS II unterstützt sowohl die DNS Auflösung von Hostnamen als auch die direkte Eingabe von IP-Adressen. Der Unterschied zwischen diesen beiden Möglichkeiten hat weitreichende Konsequenzen für die Konfiguration Ihres Netzwerks:

- Bei der Angabe eines DNS-Hosts ein entsprechender DNS-Server vorhanden sein, der den Namen in eine IP-Adresse auflösen kann. Ist dieser DNS-Server offline, werden Sie keine Verbindung zu dem entsprechenden Netzwerkgerät mehr haben.
- Bei der Angabe einer direkten IP-Adresse müssen Sie hingegen davon ausgehen, dass die IP-Adresse auf dem Zielgerät statisch vergeben wurde- wird diese dynamisch von einem DHCP-Server vergeben, kann sie sich auch sporadisch einmal ändern.

Wenn dies geschieht, werden Sie ebenfalls keine Verbindung mehr zum Zielgerät erhalten, bis Sie die IP-Adresse angepasst haben. Für die korrekte Einstellung wenden Sie sich in diesem Fall an Ihren lokalen Systemadministrator oder zuständigen Netzwerkbetreuer.

Tip

In der Registerkarte Info können Sie beliebige Informationen hinterlegen, die lokal innerhalb der UNMS II gespeichert vorliegen. Sie können also entsprechende Informationen in der Info-Box des entsprechenden Geräts hinterlegen. Im Störfall liegen so die entsprechenden Informationen bereits vor.

UPSTCP Port (Community)

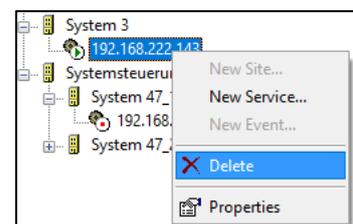
Der Standardport für den CS121 und CS141 für die UNMS ist 5769 – sofern Sie diesen nicht in Ihrem Netzwerk manuell geändert haben, müssen Sie an dieser Stelle nichts ändern.

Wenn Sie unter Connection type eine andere Karte ausgewählt haben, kann es sein, dass Sie statt Port eine SNMP Community angeben müssen. Diese Community muss entsprechend auch auf der Zielkarte konfiguriert sein und die IP-Adresse des UNMS II-Computers muss autorisiert sein, Daten lesen zu dürfen.

Löschen eines obsoleten Geräts

Wählen Sie im Site Explorer auf der rechten Seite einfach das entsprechende Gerät aus und klicken Sie im Kontextmenü auf „Delete“. Das Gerät wird sofort aus der Konfiguration entfernt und auf Wunsch sämtliche Logdateien gelöscht.

Drücken Sie anschließend wie gewohnt auf Speichern, Beenden Starten, und das Gerät wird in der Webanzeige nicht mehr angezeigt oder überwacht.

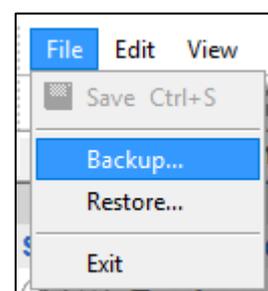


UNMS um zusätzliche Funktionen erweitern

Wenn Sie die UNMS II heruntergeladen und ohne einen Lizenzkey installieren, wird automatisch die UNMS Free installiert. Die UNMS kann jederzeit um weitere Module erweitert werden. Die hierfür notwendige Lizenz kann innerhalb der UNMS aktualisiert werden, indem Sie eine neue Lizenzkeydatei einbinden.

1. Fertigen Sie ein Backup an.

Sollte es Probleme wider Erwarten mit der Key-Datei geben (Tippfehler, Formatfehler, etc) , können Sie jederzeit auf den letzten Stand wieder zurückkehren und ggfs. das UNMS System auch von Hand neu installieren.



2. Vorbereiten der Key-Datei

Die Key-Datei können Sie jederzeit selber erstellen. Starten Sie hierzu einen Standard Text-Editor und geben Sie folgendes ein:

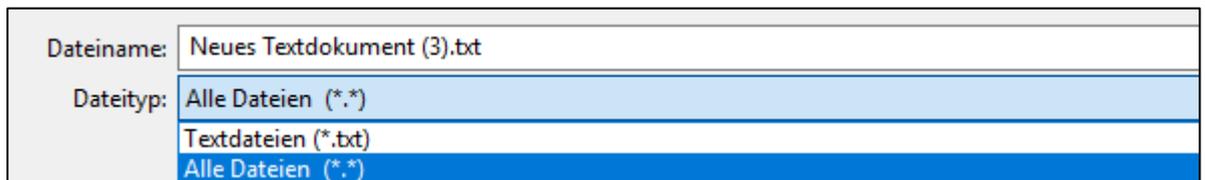
```
unms2.key.txt - Editor
Datei Bearbeiten Format Ansicht ?
[Install]
KeyCode=12H123DE...
```

Achten Sie hier unbedingt auf das genaue Format, da ansonsten die Schlüsseldatei nicht funktionieren wird. Klicken Sie anschließend auf Datei und dann auf Speichern Unter.

Der Texteditor wird Ihnen standardmäßig alles zunächst als Textdatei mit der Endung .txt abspeichern wollen. Wenn Sie jetzt einfach den Dateinamen unms2.key verwenden würden, würde ihnen der Texteditor daraus folgendes machen:

unms2.key.txt

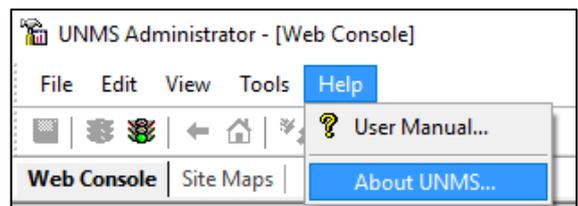
Um das zu verhindern, ändern Sie bitte den Dateityp von Textdateien auf alle Dateien:



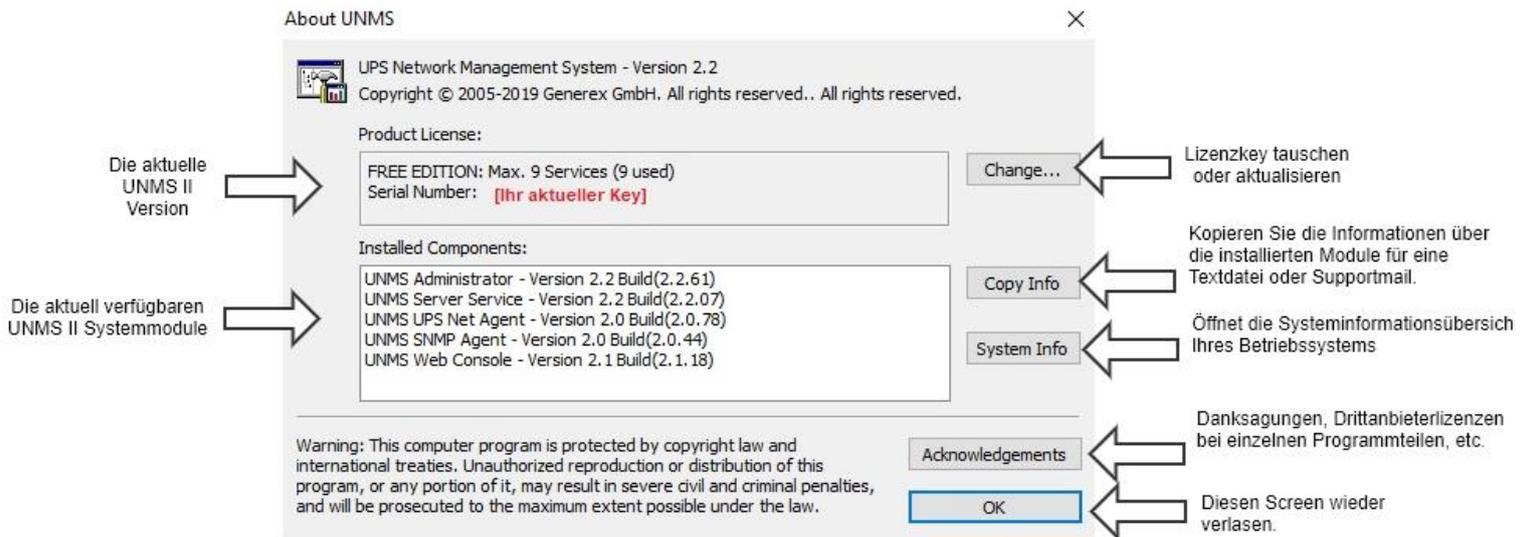
Das es geklappt hat, können Sie daran erkennen, dass der Texteditor die Datei anschließend nicht mehr als Textdatei erkennt und daher auch nicht mehr versucht, diese automatisch mit dem texteditor zu öffnen.

3. About Screen aufrufen:

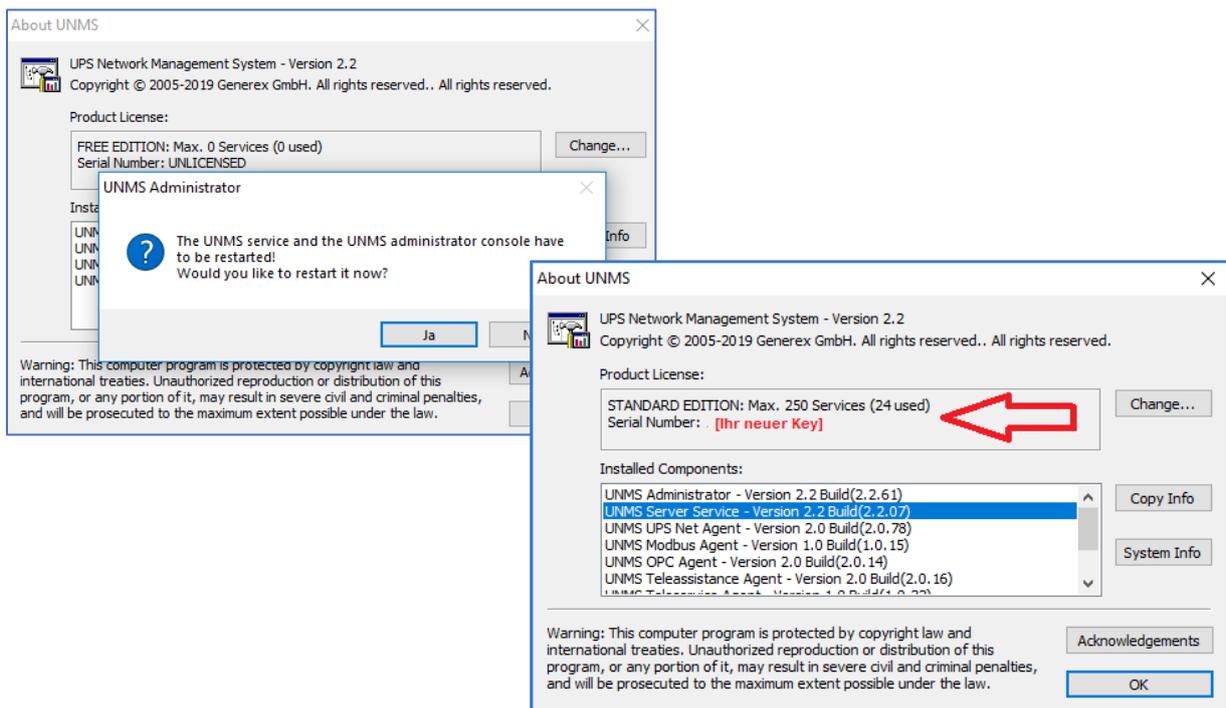
Klicken Sie hierzu einfach in der oberen Leiste auf Help und anschließend auf About UNMS:...



Es öffnet sich ein überichtlicher Hilfebildschirm, welcher Ihnen die aktuelle Installation inklusive aller verfügbaren Module anzeigt



Klicken Sie hier auf Change ... und wählen Sie die eben erstellte Key-Datei aus und bestätigen Sie den Neustart der UNMS II.



Nach dem Neustart der UNMS sind die neuen Module verfügbar.

Tutorial: Einem Ereignis unterschiedliche Mail-Adressen zuweisen

Hier sind Vorbereitungen notwendig, um das entsprechende Konfigurationsmenü freizuschalten:

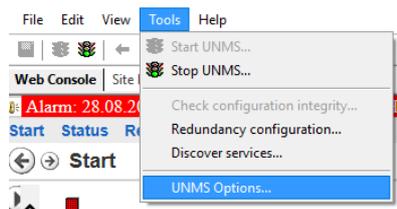
Viele Menüs in der UNMS 2 hängen voneinander ab und werden dann eingeblendet, wenn die Möglichkeit besteht, diese auch nutzen zu können. Dieser spezielle Job kann demnach nur konfiguriert werden, wenn der UNMS 2 vorher ein Mailserver mitgeteilt wurde, über den der Mailverkehr laufen darf. Ist die UNMS Mail-Option nicht entsprechend konfiguriert, ist das Konfigurationsmenü für diesen Job nicht zugänglich. Von daher muss zuerst ein Mailserver eingestellt werden:

Tipp:

die UNMS 2 arbeitet mit einer persistenten Konfiguration, wodurch Sie Änderungen an der UNMS durchführen können, ohne den laufenden Betrieb zu stören. – um die Änderungen jedoch aktiv zu schalten, muss aus diesem Grund die UNMS nach dem Speichern ganz bewusst gestoppt und wieder gestartet werden.

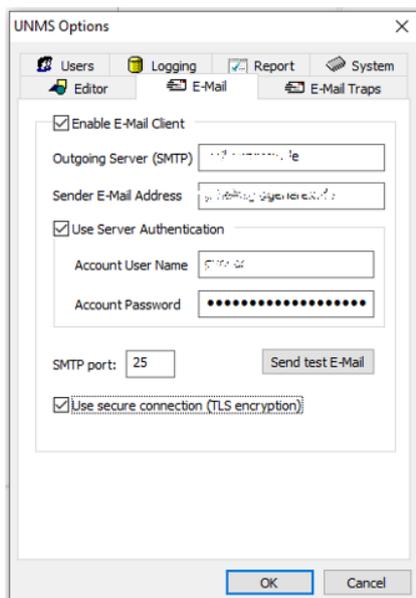
Wenn Ihre UNMS – Version jedoch eine bestimmte Funktion nicht unterstützt, werden Sie das entsprechende Menü auch nicht finden...

Mail-Einstellungen Konfigurieren / Überprüfen



Öffnen Sie zunächst die UNMS Options, um den grundlegenden Konfigurationsdialog aufzurufen.

Um einen gültigen Mailserver zu hinterlegen, wählen Sie im Konfigurationsdialog den Reiter „E-Mail“ aus:



- Wählen Sie den Reiter "E-Mail" aus
- Aktivieren Sie den E-Mail-Client
- Definieren Sie den Mailserver
- Dies ist in der Mail das „Von“ – Feld
- Wenn der Server Nutzer und Passwort benötigt
- Login-Namen
- Login - Passwort
- Welchen Port benutzt der Mail-Server als Standard?
- Soll die Kommunikation verschlüsselt werden?
- Übernehmen der Einstellungen / Abbrechen

Nachdem der Mail-Test erfolgreich verlief, klicken Sie auf OK, um die Einstellungen zu übernehmen und die entsprechenden Konfigurationsmenüs freizuschalten.

Tipp:

Wenn die Zugangsdaten sich ändern und falsch sind, wird der E-Mail Server den Versand schlicht ablehnen. Die UNMS hingegen benötigt zumindest irgendwelche Server-Eingaben, damit dieser Job für sich überhaupt angezeigt und konfigurierbar ist. Das bedeutet, wenn die UNMS den Mail-Job nach erfolgter Konfiguration nicht wie gewünscht sendet, müssen Sie beide Einstellungen überprüfen – Die Angaben unter Mailserver UND die Bedingungen für den konfigurierten Job.

Denken Sie daran: Diese Jobs werden nur dann auch ausgeführt, wenn Sie Speichern, Beenden und Starten geklickt haben, um die aktive Konfiguration zu schreiben!

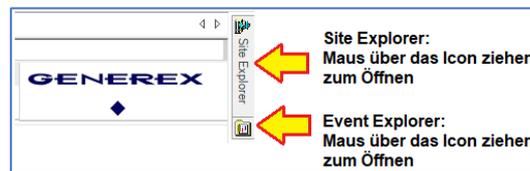
Einrichten der abweichenden Mail-Adresse als Ziel

Nachdem man den Mailserver hinterlegt hat, ist es möglich, die Mail-Jobs entsprechend zu konfigurieren. Dies geschieht im „Event Explorer“. Dieser ist an zwei Stellen auf der Rechten Seite der Administratorkonsole zu finden. Entweder unten rechts, wo man zwischen Site Explorer (Listet alle eingebundenen Geräte auf) oder den Event Explorer, wo die möglichen ausführbaren Jobs stehen, die mit beliebigen Geräteereignissen in Verbindung gebracht werden können:

Wenn die Taskbar unten rechts verankert ist:



Dynamische Sitebar rechts oben:



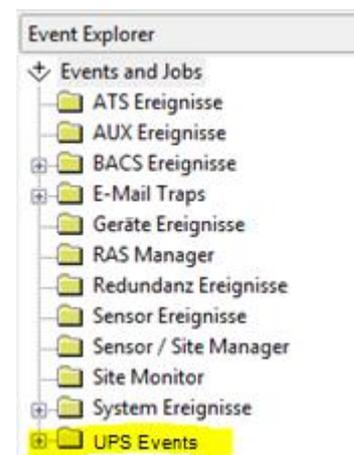
Der Event-Explorer

Der Event-Explorer bietet eine Übersicht über alle verfügbaren Ereignisse sowie vorkonfigurierte Standardaufträge, die entsprechend ausgeführt werden, wenn eins dieser Ereignisse eintritt.

Wenn sich Jobs in Unterordnern befinden, können diese durch einen Klick auf das + direkt ausgeklappt und betrachtet oder editiert werden.

Was dieses Tutorial beschreibt:

Die Aufgabe ist, dass bei einem USV-Ereignis eine E-Mail an eine andere E-Mail-Adresse als die Standard-Mail-Benachrichtigungen gesendet werden. Die USV-Ereignisse befinden sich im entsprechenden Ordner und den Unterordnern, die mit "USV-Ereignisse" (UPS Events) bezeichnet sind.



Diese Aufgabe wurde an die Technikabteilung übertragen:

Es gab in letzter Zeit einfach zu viele Stromausfälle, die zu Problemen geführt haben. Der Vorstand des Unternehmens hat daher in seiner grenzenlosen Weisheit einstimmig beschlossen, sofort Informationen einzuholen, wenn dies wieder geschieht.

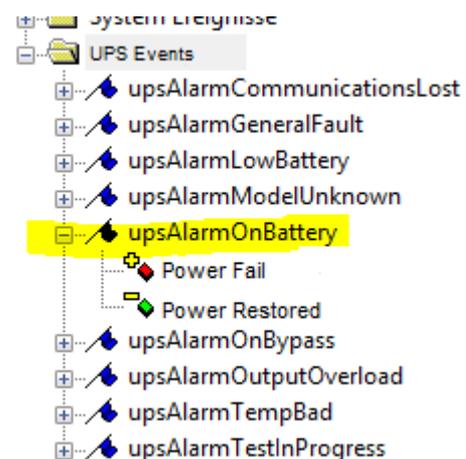
Der schnellste Weg, dies zu tun, ist die Verwendung der UNMS 2, da hier Funktionen wie ein automatischer Mailversand angeboten werden.

Das richtige USV-Ereignis identifizieren

Die vordefinierten Bezeichnungen sind eigentlich sehr selbsterklärend: UPS Alarm On Battery (USV Alarm: Auf Batterie). Klappen Sie mit + den Ordner auf, und betrachten Sie die Alarmer, die dort hinterlegt sind::

- Power Fail
- Power Restored.

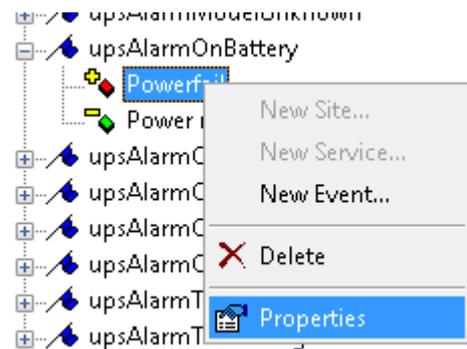
Diese Beiden Ereignisse sind also selbsterklärend die gesuchten Alarmer:



Im nächsten Schritte sollen hier eigene Mailadressen angelegt werden – Denken Sie daran, dass Email-Jobs nur dann eingblendet werden, wenn der E-Mail Server im Vorfeld definiert wurde.

How to add a customized mail job

Öffnen Sie zunächst das Kontextmenü dieses Ereignisses mit der rechten Maustaste und wählen Sie Properties aus.-



in den Event Properties stellen Sie dann ein, was genau geschehen soll, wenn sich dieses Ereignis auftritt. Aktuell wird der Job aus der Job-Liste „DEFAULT“ ausgeführt. Das müssen wir jetzt anpassen:

→ ... beschreibt das Ereignis und den aktuellen Ereignis-Status

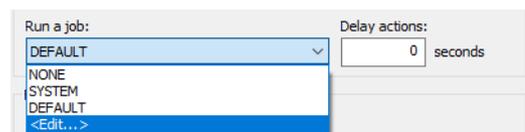
→ ... Name des Ereignisses und die aktuelle Priorität

→ ... Was soll im UNMS Logfile hierzu stehen ?

→ ... Welcher Job soll ausgeführt werden?

→ ... Filter: Sind weitere Gruppenkonditionen für das Auslösen zu erfüllen?

Die UNMS unterscheidet hier zwischen einer Liste von existierenden Jobs und der Zuweisung zu Systemereignissen. Damit muss der Job nicht jedes Mal neu angelegt werden, sondern kann hinterher beliebig vielen Ereignissen dynamisch zugeordnet werden. Da dieser Job mit den Mail-Adressen noch nicht existiert, wählen Sie bei „Run a job“ den Eingabedialog <Edit...> aus:



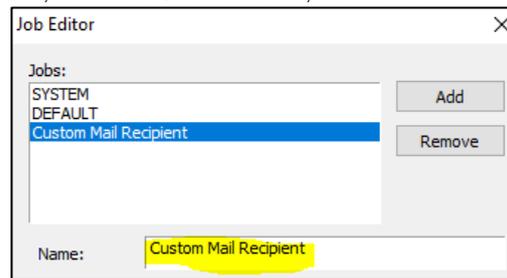
Der Jobeditor

Es öffnet sich der Jobeditor, der Sie dabei unterstützt, neue Jobs zu definieren. Unter Jobs finden Sie alle bisher angelegten Jobs wieder, wobei DEFAULT und SYSTEM die voreingestellten Jobs darstellen.

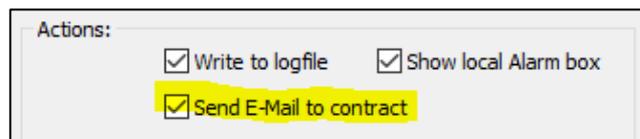
Mit Add fügen Sie entsprechend einen neuen Job hinzu. With edit, a new configuration dialog for the according job will be opened:

E-mail-Job anlegen

Drücken Sie auf "Add", um einen neuen Job hinzuzufügen. Denken Sie daran, dem Job einen eindeutigen Namen zuzuweisen, damit Sie ihn spätestens dann, wenn viele Jobs existieren, auch wiederfinden können.

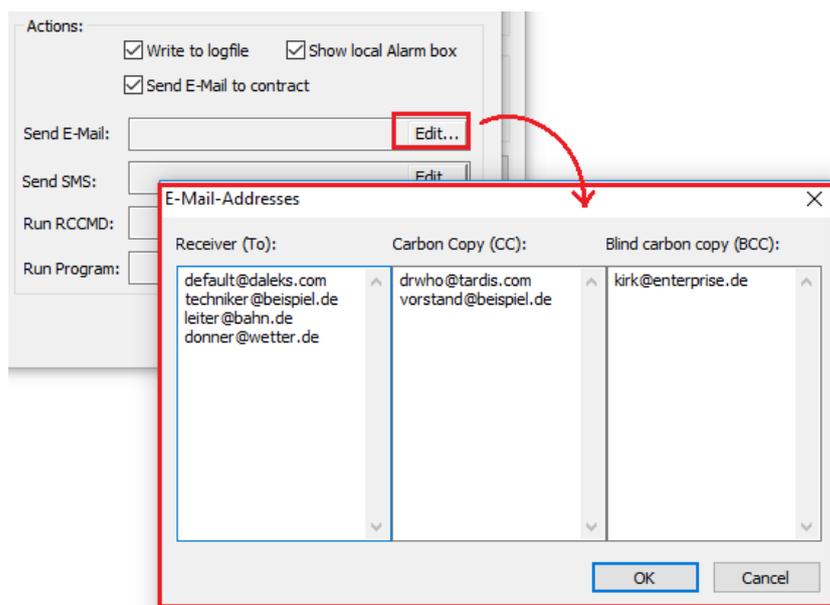


Mit der Funktion "Send E-Mail to contract" aktivieren Sie den Mailversand an eine vordefinierte Mail-Adresse.



Im nächsten Schritt müssen Sie der UNM mitteilen, welche Empfänger alles eine E-Mail erhalten sollen

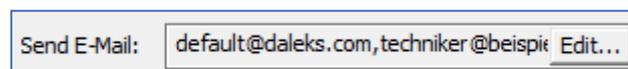
Klicken Sie hierzu bei "Send E-Mail" auf Edit:



Die UNMS 2 bietet drei unterschiedliche Varianten für das Senden von Em-Mails an:

1. Receiver – Der klassische Mail-Empfänger.
2. Carbon Copy (CC) – Dem Empfänger (An) wird sehen dass die UNMS eine Kopie
3. Blind Carbon Copy (BCC) – Die Blindkopie. Der Standard Empfänger sieht nicht, dass die Mail einen weiteren Empfänger hat.

Tragen Sie beliebig viele Mail-Empfänger ein, die UNMS wird der Konfiguration entsprechend hinterlegen:



Den Job aktiv schalten

Zuguterletzt müssen Sie nur noch sicher stellen, dass der Job auch entsprechend ausgewählt wurde – ansonsten hätten Sie zwar den Job an sich korrekt erstellt, aber die UNMS wusste nicht, dass er in diesem Kontext auch ausgeführt werden sollte.

Wie bereits beschrieben, unterscheidet die UNMS zwischen den Job und den Ereignissen, damit man nicht jeden Job einzeln ständig neu anlegen muss. Es lang aus, dass dieses Ereignis einen speziellen Job ausführen soll.

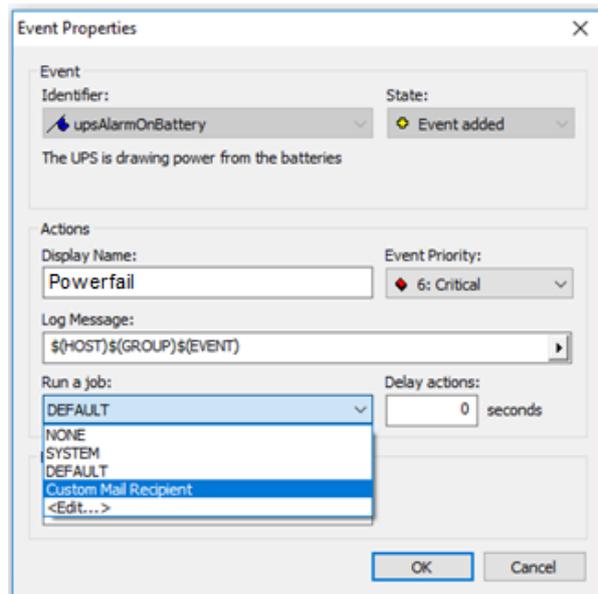
Standardmäßig wird unter „Run a Job“shows der Job „Default“ ausgeführt – der von Ihnen erstellte Job ist konfiguriert und gespeichert, aber Sie müssen diesen jetzt noch auswählen, damit er für das Ereignis Powerfail aktiv geschaltet ist.

Wählen Sie hierzu den Job einfach aus dem Drop-Down-Menü aus und klicken Sie auf OK, um die Einstellung zu speichern.

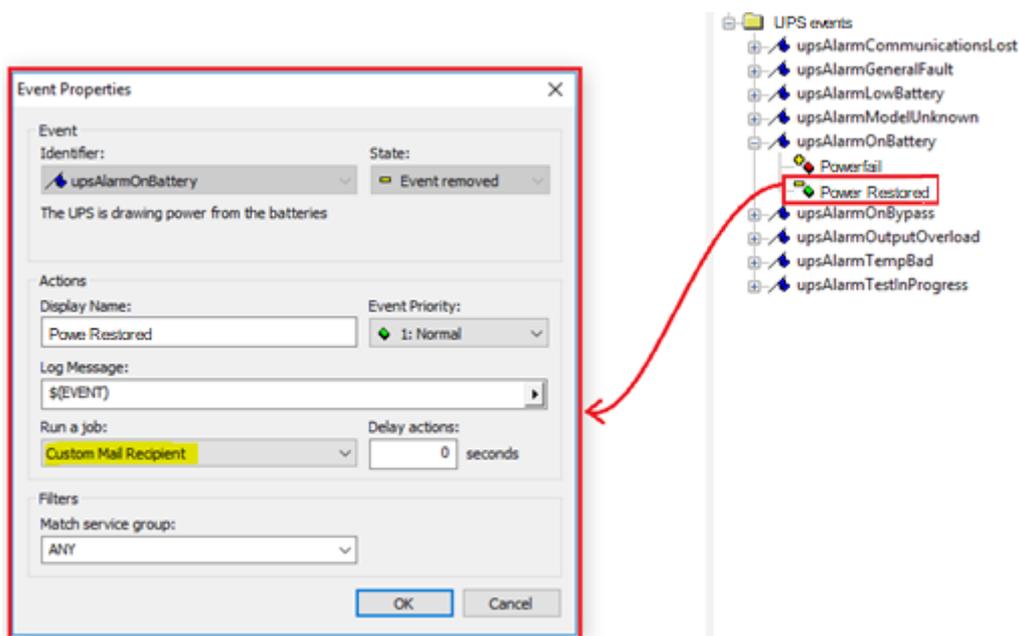
Der Vollständigkeit halber...

Aktuell sind alle registrierten Mail-Empfänger darauf ausgelegt, bei einem Power Fail – also einem Stromausfall – informiert zu werden.

Im Umkehrschluss gibt es aber auch das Ereignis, dass das Ende des Stromausfalls – Power Restored – aufzeigt.



Um jetzt nicht alle Mails neu einzugeben, wählen Sie bei Power Restored einfach den von Ihnen erstellten Mail-Job noch einmal aus:



Niemals vergessen: Speichern, Beenden, Starten:



Die UNMS muss die neuen Konfigurationsdaten einlesen und aktiv schalten. Das geschieht, indem Sie auf Speichern, Beenden und dann wieder auf Starten drücken. Die UNMS lädt dann die Änderungen in die aktive Konfiguration.

E- Mail-Tutorial, Teil 2: Mail Ereignisse mit Service-Gruppen kombinieren: Wer kriegt wann eine Mail?

Wenn man unterschiedliche Mailadressen angeben kann, muss es auch zwangsläufig eine Möglichkeit geben, unterschiedliche USV-Anlagen mit abweichenden Mail-Adressen zu belegen - es ist schließlich nicht abwegig, dass ein Kunde an 4 Standorten jeweils eine baugleiche USV stehen hat, es jedoch unterschiedliche Service-Teams gibt, die an jedem Standort vor Ort informiert werden sollen – und natürlich zentral verwaltet.

Wenn man dem Gedankengang folgt, muss man irgendwo einstellen können, dass ein bestimmter Job unter bestimmten Bedingungen ausgelöst werden kann.

Die UNMS bietet hierzu die Möglichkeit, Jobs, Ereignisse und Servicegruppen unabhängig voneinander anzulegen, und diese logisch miteinander zu verknüpfen:

1. Ein unabhängiger Job kann mehreren Ereignissen zugewiesen werden
2. Ein Job kann an eine Service-Gruppe gebunden werden
3. Eine USV kann an eine Service-Gruppe gebunden werden
4. Der Mail Job „Contract“ wird seine Mailadresse unabhängig aus den Kontaktdaten des Kunden ziehen.

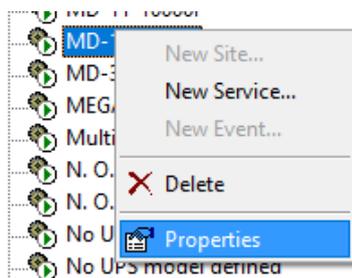
Als Folge können in dem oben genannten Beispiel im Event-Explorer unter dem Ereignis „Stromausfall“ 4 Email-Jobs mit eigenen Listen hinterlegt sein:

- Der Job für die Servicegruppe 1 wird nur dann ausgeführt, wenn sowohl der Job als auch die USV derselben Servicegruppe angehören.
- Die Mail, die in den Kundendaten hinterlegt wurde, wird USV-bezogen unabhängig von der Servicegruppe ausgelöst

Soweit die Theorie.... Konfiguriert wird das Ganze wie folgt:

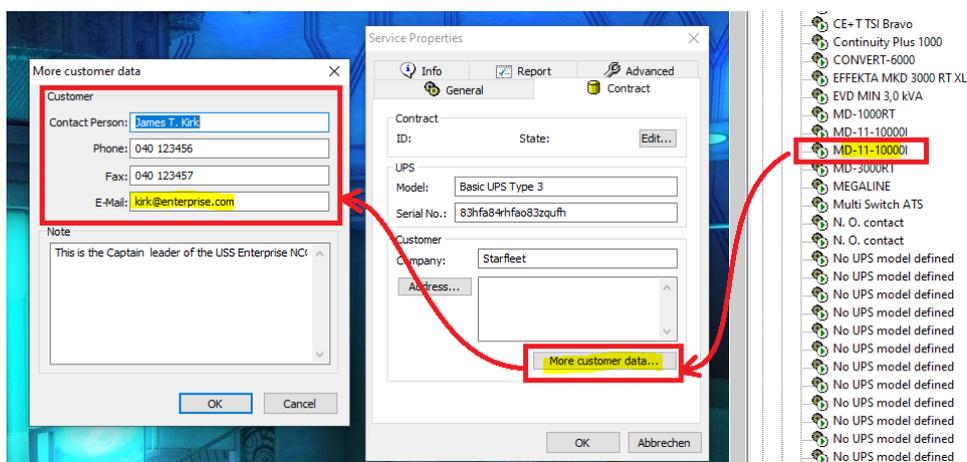
Schritt 1: Kontaktdaten der USV einfügen:

Im SITE EXPLORER öffnen Sie mit der rechten Maustaste die Eigenschaften:



Dort wählen Sie den Reiter Contract aus und hinterlegen grundsätzliche USV-Daten, die eventuell notwendig sind.

Klicken Sie im Anschluss auf „More customer data“:



Dort können Sie einen Ansprechpartner hinterlegen inklusive einer E-Mail Adresse. Diese Mail-Adresse ist an die USV gebunden und wird später bei einem Mail-Job USV-bezogen unabhängig von einer Service-Gruppe ausgelöst.

Schritt 2: Die Service Gruppe

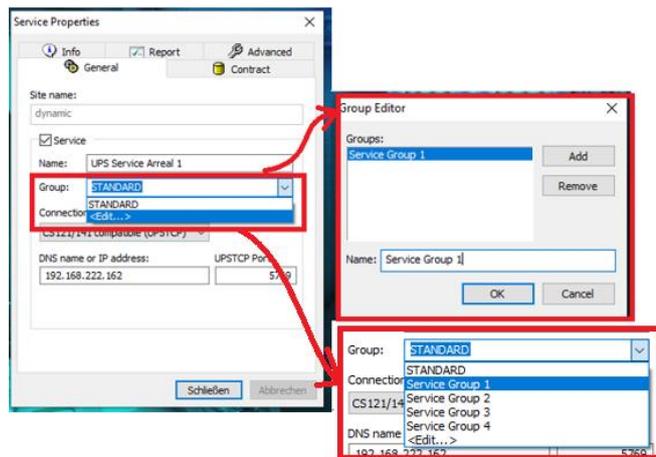
Öffnen Sie in den „Service Properties“ den Hauptreiter „General“:

Unter „Group“ ist die Servicegruppe hinterlegt. Jedes neue Gerät landet dabei automatisch zunächst in der Gruppe „Standard“.

Unter Name können Sie jetzt den Anzeigenamen der USV auf eine für Sie logische Bezeichnung ändern.

Hinter „Group“ versteckt sich der Editor für die Servicegruppen. Dieser Servicegruppeneditor taucht immer wieder auch im Eventexplorer auf, es ist aber immer dasselbe Modul. In unserem Fall benötigen wir hier die Service-Gruppen 1 – 4:

- Service Group 1
- Service Group 2
- Etc.



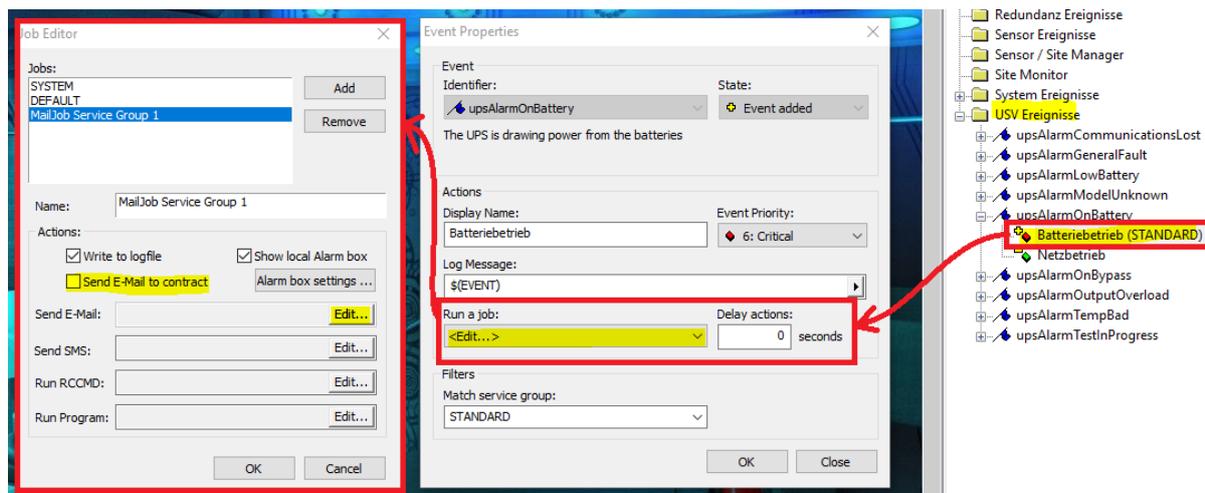
Nachdem Sie die Servicegruppen erfolgreich angelegt haben, können Sie diese auch auswählen.

Tip:

Sie können auf diese Weise beliebig viele USV-Anlagen einer Service-Gruppe hinzufügen. Wenn später dann eine dieser USV-Anlagen ein Ereignis melden, wird der entsprechende Job darauf gebunden sein

Schritt 3: Mail Job zuordnen

Wie im Vorangegangenen Tutorial ergänzen Sie jetzt den Job das Ereignis Batteriebetrieb:



Öffnen Sie mit der rechten Maustaste die Eigenschaften, klicken Sie bei Run a Job auf Edit und legen Sie die Mailjobs für die Service-Gruppen an. Diese können Sie im Anschluss wie zuvor die Service-Group bei „Run a Job“ auswählen.

Allerdings gibt es eine Erweiterung:

Setzen Sie bei Bedarf den Haken bei „Send E-Mail to contract“, zum Beispiel wenn dort der Team-Leiter als Ansprechpartner hinterlegt wurde.

Schritt 4: Das Ereignis anpassen

Im nächsten Schritt passen Sie das Ereignis an:

- Display name: Definiert den angezeigten Namen?
- Run a job: Welcher Job soll ausgeführt werden?
- Match service group: Definiert die Gültigkeit.

In diesem Fall wurde das Ereignis Batteriebetrieb so angepasst, dass der Job „Mail Service Group 1“ nur dann ausgeführt wird, wenn eine USV-Anlage aus der Service Group 1 einen Schaden meldet.

Sollte eine andere Service-Gruppe kommen, dann wird der Job entsprechend nicht getriggert.

The screenshot shows the 'Event Properties' dialog box for the event 'upsAlarmOnBattery'. The state is 'Event added'. The display name is 'Batteriebetrieb: Service Group 1', the event priority is '6: Critical', the log message is '\$(EVENT)', the run a job is 'Mail Service Group 1', and the match service group is 'Service Group 1'. The dialog has 'OK' and 'Close' buttons.

Schritt 5: Weitere USV-Ereignisse anlegen

Da Sie mehr als eine Service-Gruppe vorliegen haben, müssen Sie die Anzahl der Ereignisse entsprechend erhöhen. Klicken Sie hierzu mit der rechten Maustaste auf upsAlarmOnBattery und wählen Sie aus dem Kontextmenü „New Event“ (neues Ereignis) aus. Passen Sie das Event an, dass es zu der Servicegruppe 2 gehört:

The screenshot shows the 'New Event' dialog box for the event 'upsAlarmOnBattery'. The state is 'Event added'. The display name is 'Batteriebetrieb: Service Group 2', the event priority is '0: Info', the log message is '\$(EVENT)', the run a job is 'Mail Service Group 2', and the match service group is 'Service Group 2'. The dialog has 'Add' and 'Cancel' buttons. A context menu is open over the event in the background, with 'New Event...' highlighted. Red arrows point from the context menu to the dialog fields.

Verfahren Sie so, bis alle 4 Service-Gruppen entsprechend eingerichtet sind.

Achten Sie jetzt auf die Liste im Event-Explorer:



Sie zeigt in Klammern jetzt an, für welche Service-Gruppe dieses Ereignis gültig ist. Wenn Sie neue USV-Anlagen jetzt in Betrieb nehmen, brauchen sie diese nur noch der entsprechenden Servicegruppe zuzuordnen und müssen nicht mehr individuell neue Jobs anlegen. Umgekehrt können Sie zu jedem Ereignis jetzt Jobs hinzufügen und ganz einfach eine Servicegruppe von USV-Anlagen definieren, um die Gültigkeit zu determinieren.

Aktivieren der Konfiguration:



Denken Sie darauf, dass alles, was Sie bislang konfiguriert haben, nur in einer inaktiven Schattenkonfiguration vorliegt. Um die Konfiguration zu aktivieren, müssen Sie noch einmal Speichern, Beenden und Starten.

Tipp:

Die UNMS 2 ist nicht nur ein sehr mächtiges Werkzeug für die Visualisierung von komplexen Netzwerkstrukturen, es kann auch viele Managementfunktionen zentral übernehmen und viele Prozeduren im Krisenmanagement übernehmen:

Mit einer gut konfigurierten UNMS2 haben Sie einen virtuellen Assistenten an der Seite, der nahezu alle Standardaufgaben und Prozeduren sowohl zeitlich als auch ereignisgesteuert Informationen über Systeme und administrative Zugehörigkeiten zentralisieren und bereitstellen kann, Ansprechpartner und Kontaktpersonen automatisch für Sie informiert, Notfallshut downs vorbereiten oder Migrationen anstoßen kann und vieles mehr.

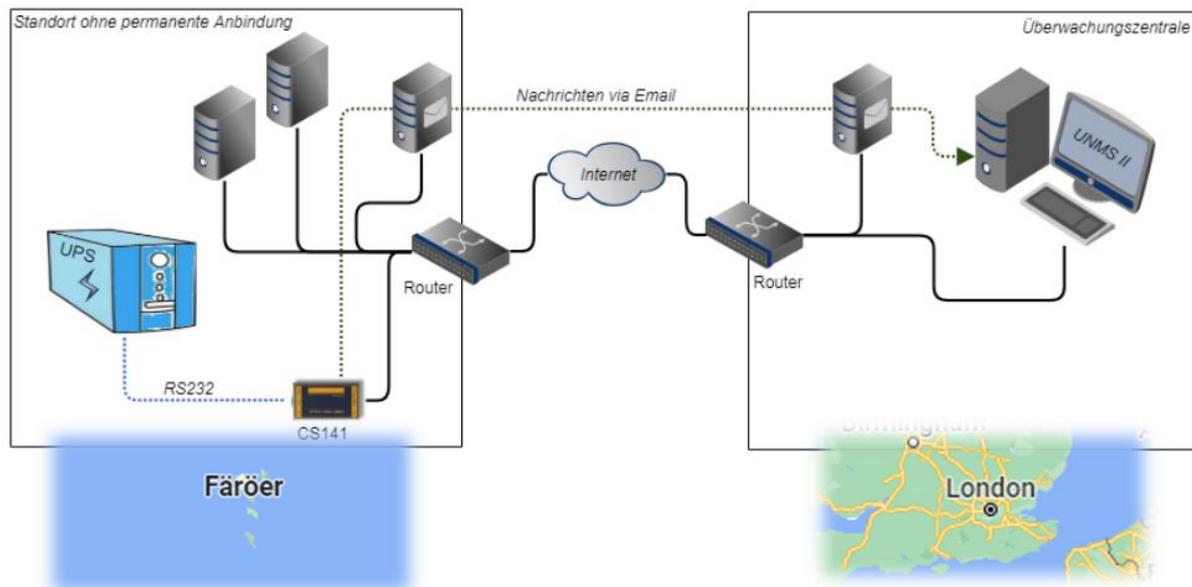
Tutorial: Mail-Traps: Informationen per Mails anzeigen lassen

(Diese Funktion ist in der UNMS free nicht enthalten.)

Diese Funktion dürfte eigentlich jeder Nutzer spannend finden, der mit dem Problem konfrontiert ist, der Statusinformationen von USV-Geräte haben muss, die über keinen direkten Netzwerkzugang verfügen. Ein typisches Beispiel hierfür wäre, wenn die UNMS auf einem Server in London steht, und von in ganz England USV-Anlagen überwacht werden. Die Wahrscheinlichkeit, dass die Insel Färöer eine solide Standleitung hinbekommt, ist ziemlich gering – oder dürfte aus Kostengründen nicht weiter in Betracht kommen.

Eine interessante Lösung bietet hier die Geräte der CS141 Produktfamilie mit der „Mailtrap“ – Funktion.

Über Mailtraps kann ein CS141 relativ einfach regelmäßig Lebenszeichen und Statusinformationen regelmäßig und im Störfall zur UNMS senden:



Mit dieser Funktion kann also ein relatives Monitoring erfolgen, und erhält auch Rückschlüsse über den allgemeinen Systemzustand – Wann die Mails eintreffen, ist dabei von der Qualität des Netzwerkes, der Versand- und Empfangsdurchläufe, etc. abhängig. Die UNMS wird hier automatisch eingehende Emails auswerten und der entsprechend eingerichteten Services zuordnen.

Die Einrichtung erfolgt dabei in mehreren Schritten:

1. Der CS141 benötigt einen Mailserver, über den er Mails versenden darf
2. Mailtrap-Funktion muss aktiviert und konfiguriert sein
3. In der UNMS muss diese Funktion aktiviert sein, und sie benötigt ein Mailpostfach für eingehende Mails

Einrichtung in der UNMS

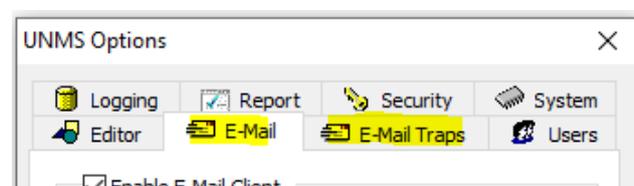
Die UNMS unterscheidet zwischen E-Mail und E-Mail Traps:

E-Mail

Hier werden die Zugangsdaten zum SENDEN hinterlegt, also wenn die UNMS von sich aus basierend auf den Ereignissen eine Mail versenden soll.

E-Mail Trap

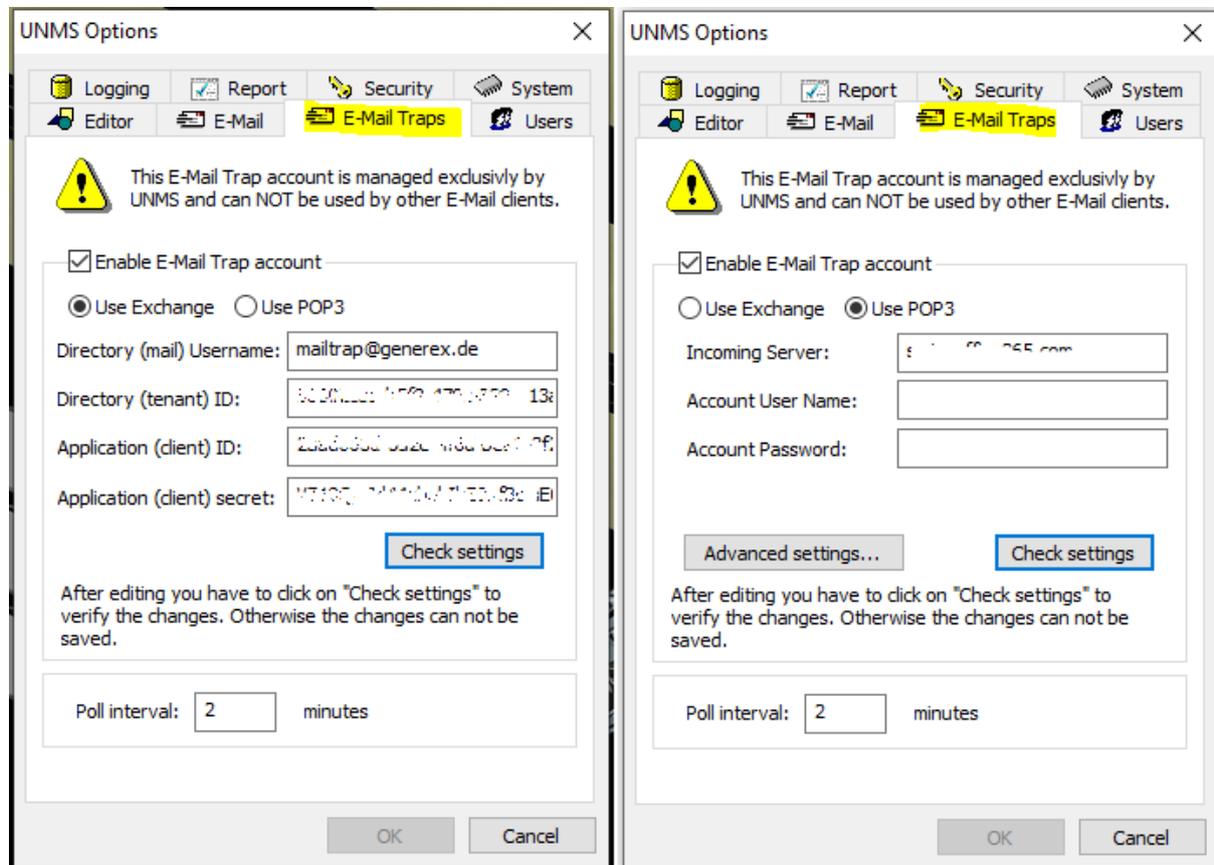
In diesem Konto wird das eingehende Mailpostfach eingestellt: Die UNMS wird dort im Posteingang selbstständig nach eingehenden Mail-Trap – Nachrichten (Speziell konfigurierte E-Mails mit einem Datenpaket) suchen, diese abholen und anschließend aus dem Postfach löschen.



Teil 1: Email-Trap Konto definieren

Dieser Schritt ist notwendig, weil ohne eingehendes Postfach kein sinnvoller Service für Mailtraps eingerichtet werden kann. Um mit der Konfiguration zu beginnen, öffnen Sie die UNMS Options, und klicken auf den Reiter „E-Mail Traps“.

Im nächsten Schritt wählen Sie zwischen zwei unterschiedlichen Servervarianten:

**Wenn Sie POP3 wählen:**

POP3 ist die Abkürzung für Post Office Protocol 3. Es ist ein Kommunikationsprotokoll, das es einem E-Mail-Client ermöglicht, E-Mails von einem Server über ein IP-Netz abzurufen. Dabei werden die E-Mails vom Server auf das lokale Gerät des Nutzers heruntergeladen und können offline bearbeitet werden. POP3 wurde 1988 im RFC 1081 spezifiziert und ist die dritte Version des Post Office Protocols. POP3 ist ein einfaches und wenig komplexes Protokoll, das nur das Abholen, Auflisten und Löschen von E-Mails erlaubt. Bitte beachten Sie, dass Anbieter wie z.B. Gmail zusätzliche Freigaben und Konfigurationen erfordern, ohne die die Mailfunktion der UNMS nicht berechtigt ist, auf das jeweilige Konto zuzugreifen.

Enable E-Mail Trap account

Use Exchange Use POP3

Incoming Server:

Account User Name:

Account Password:

Advanced settings...

After editing you have to click on "Check settings" to verify the changes. Otherwise the changes can not be saved.

→ Geben Sie den eingehenden Mailserver an

→ Benutzernahme

→ Passwort

→ Advanced Settings: Definieren Sie den Port und SSL-Methode

→ Check Settings: Überprüfen Sie Ihre Einstellungen

Wenn die Daten mit Check settings bestätigt wurden, können Sie mit OK das Dialogfeld beenden. Drücken Sie auf Speichern, Beenden und Neustart, um die Einstellungen zu aktivieren.

Teil 2 Einrichten von Geräten, die über Mail-Traps überwacht werden sollen

In Teil 2 dieses Tutorials haben wir der UNMS mitgeteilt, wie sie an die Email-Daten kommt. Jetzt müssen wir der UNMS mitteilen, dass sie auch eingehende Mail-Trap Services erwartet und aktiv danach Ausschau hält. Damit dieser Dienst loslaufen kann, benötigt er zur Grundkonfiguration einmalig einen Service, der angelegt wurde.

Wählen Sie hierzu im Site Explorer eine Site aus, und legen Sie über das Kontextmenü mit „New Service“ ein neues Gerät an.

- Als Connection Type wählen Sie Email-Traps aus
- Wenn bekannt, können Sie die MAC-Adresse des zu erwartenden Geräts mit angeben. Die MAC-Adresse finden Sie im CS141 unter System>About (Über).

Wenn Sie die MAC-Adresse des Zielgeräts nicht zur Hand haben, dann lassen Sie einfach die voreingestellte Dummy-Adresse stehen, und beenden den Dialog mit OK:

Sobald der Service läuft, wird jedes Gerät, das sich per Mail-Trap bei der UNMS auf diesem Weg meldet, automatisch unter „Lost & Found“ abgelegt, von wo aus sie im Site Explorer eine Verteilung auf die jeweiligen Sites durchführen können.

- ➔ Starten Sie den UNMS Service neu, um den MailTrap-Service zu triggern.

Teil 3: Einrichten auf dem CS141 / BACS

Im letzten Schritt müssen Sie noch den CS141 / BACS mitteilen, dass er sich per Mail bei der UNMS melden soll. Dies geschieht auf dem Webmanager.

Mailtraps aktivieren:

Aktivieren Sie hierzu zunächst unter Services>Email-Traps die Mailtrap-Funktion, und hinterlegen ein gültiges Mailkonto.

Ziel und Zeitfenster einrichten:

Unter Advanced definieren Sie, wohin der CS141 / BACS seine Mails senden soll.

In diesem Beispiel würde jetzt ein CS141/ BACS alle 6 Stunden eine Statusmail senden, in der die wichtigsten USV-Daten enthalten sind. Sollte es einen Störfall geben, wird alle 5 Minuten eine Statusmail mit USV-Daten versendet. Passen Sie die Zeitfenster nach Ihren Vorstellungen an.

Events kontrollieren

Wenn Sie jetzt unter UPS>Events schauen, werden Sie feststellen, dass in der Grundkonfiguration bereits Jobs zu den wichtigsten USV-Ereignissen hinterlegt sind. Sobald die Mailtraps eingerichtet haben, werden diese Jobs automatisch ausgeführt, und zwar unabhängig vom eingerichteten Zeitfenster: Sie erhalten zu jedem Ereignis, wo ein Email Trap hinterlegt ist, eine Nachricht mit Zeitstempel.

Passen Sie die Ereignisse an Ihre Vorstellungen an, indem Sie den Job Email Trap und entfernen bzw. fügen.

Event	Jobs...	Log	E-Mail	E-Mail Trap
contains...	conf			
Powerfail	3	1	0	1
Job Type	When	Parameter		
Log	Periodic all 100s, immediately	{ "text": "Powe		
RCCMD Trap	Once, immediately	{ "text": "Powe		
E-Mail Trap	Once, immediately	{ }		

Tutorial: APC PDU Outlets schalten, wenn eine APC USV einen Powerfail meldet.

Batteriegestützter Notstrom stellt eine hochkritische und begrenzte Ressource dar – je nach Netzwerk und Funktion kann es unter Umständen also ratsam sein, unwichtige Netzwerkgeräte von der Stromversorgung zu trennen – das kann unter Umständen die wertvollen Zeitfenster für eine angemessene Reaktion enorm verlängern. APC setzt hier zum Beispiel unter anderem auch auf eine über das Netzwerk schaltbare PDU:

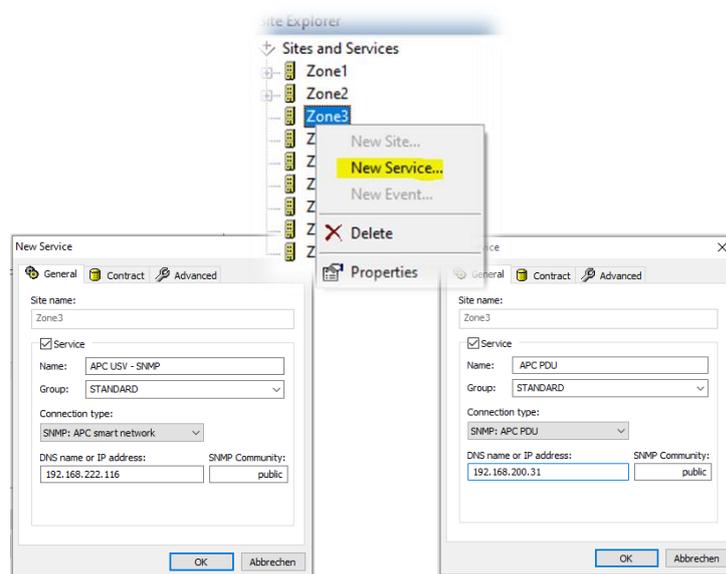
Outlets können über das Netzwerk direkt an- und abgeschaltet werden. Im einfachen Fall kann hierdurch z.B. unwichtige WLAN-Hotspots und dazugehörige Switches automatisch abgeschaltet werden. *Die Aufgabe für die UNMS 2 ist also klar: Sie soll also je nach Betriebszustand einer bestimmten USV die Outlets an der PDU schalten, damit die Fachkräfte vor Ort sich nicht um so etwas kümmern müssen.*

Das Grundproblem ist, dass die UNMS 2 zuerst das eine Gerät abfragt und dann auf einem anderen Gerät eine Aktion auslösen soll. In diesem Fall ist es eine APC USV und eine dazugehörige PDU, die über LAN zwar abgefragt werden können, aber ansonsten nichts miteinander zu tun haben.

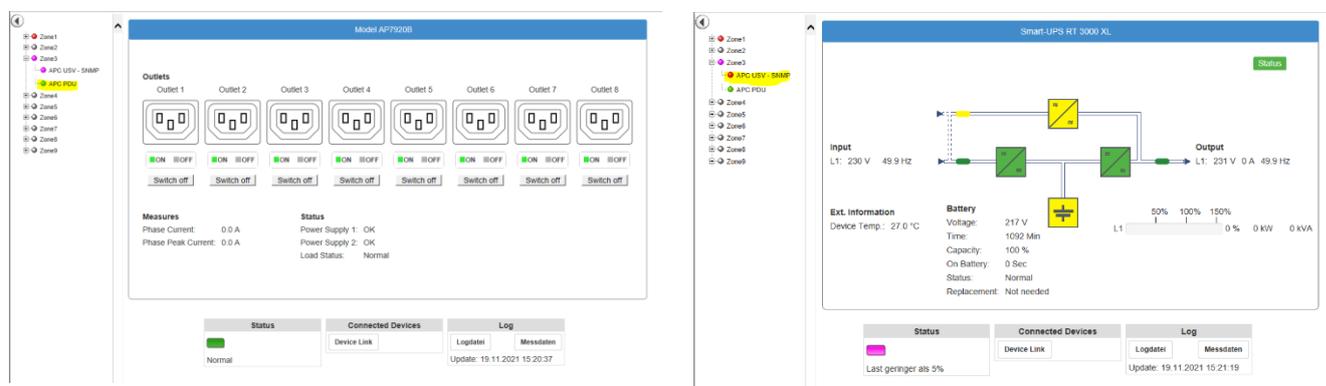
Schritt 1: Geräte anlegen

Zuerst müssen beide Geräte in der UNMS eingerichtet werden, so dass man sie direkt ansprechen kann.

Im Site Explorer bei der entsprechenden Zone mit der rechten Maustaste über das Kontextmenü „New Service“ auswählen:



Nach dem Neustart sind beide Geräte in der UNMS ein geschlüsselt und können über SNMP abgefragt werden. Speichern, beenden und neustarten bringt dann auch die beiden Geräte in die aktive Überwachung:



Die PDU zeigt die schaltbaren Steckerports,

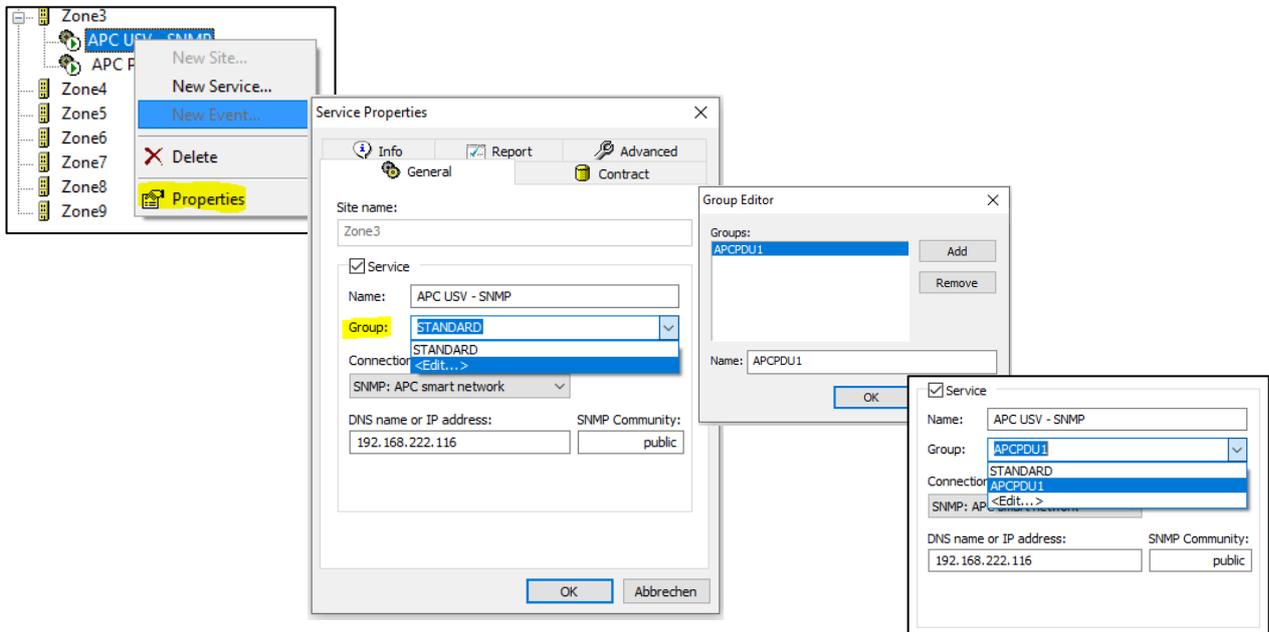
Die USV mit Blockschaubild und Messdaten

Schritt 2: Geräte in der UNMS gruppieren

Über das Gruppieren können beide Geräte über eine zusammengefasst werden, der dann entsprechend Ereignisse und Jobs zugeordnet werden können. Für beide Geräte müssen Sie daher Site Explorer über die jeweiligen Properties die Geräteeigenschaften aufrufen:

Im Reiter „General“ finden Sie den Eintrag „Group“:

Um einen neuen Eintrag hinzuzufügen, wählen Sie hier über das Drop-Down – Menü „Edit“ aus.



Drücken sie auf Add, um eine neue Gruppe anzulegen, passen den Namen an und bestätigen Sie mit OK. Im Anschluss können Sie die neu angelegte Gruppe entsprechend unter Group auswählen. Nachdem beide Geräte in einer Gruppe zusammengefasst wurden, drücken Sie auf Speichern.

Wozu ist dieser Schritt notwendig?

Wenn man genau eine USV und eine PDU hat, ist dieser Schritt schwer nachzuvollziehen. Bei einem sehr großen Gebäude mit 6 USV / PDU -

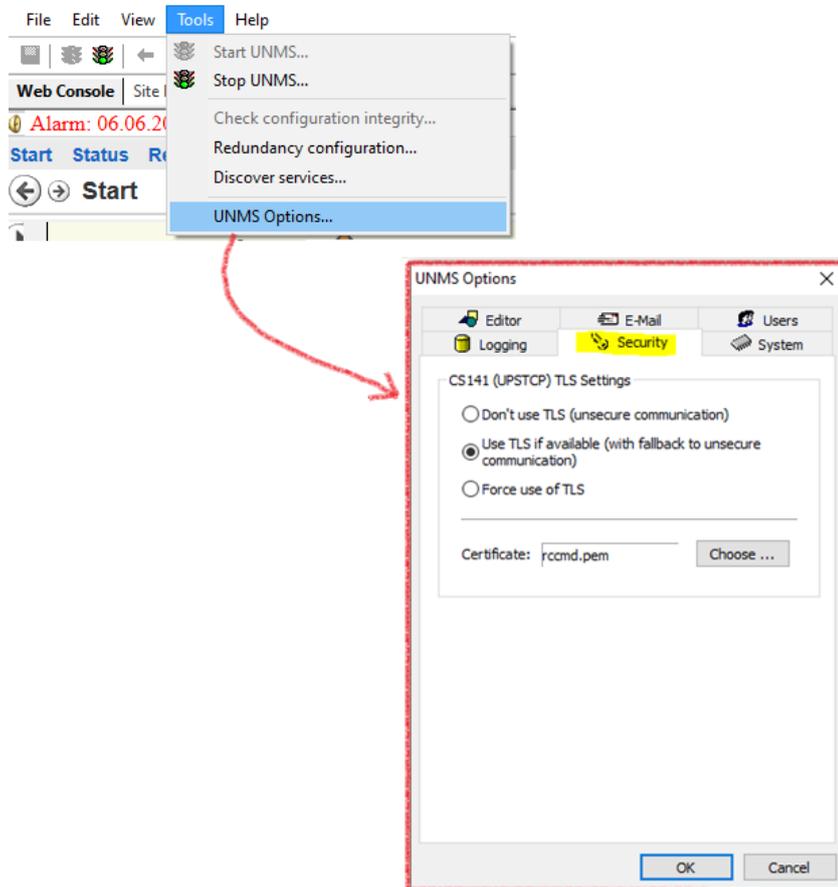
Schritt 3: Jobdefinition

Von jetzt an sind alle Ereignisse, die für die USV gültig sind, auch für die PDU gültig. Die Jobs können entsprechend wie bereits beschrieben definiert werden.

Tutorial: Verschlüsselte Kommunikation nutzen

Das stetig steigende Sicherheitsbedürfnis hat seit 2020 schleichend auch für gesicherte Infrastrukturnetzwerk die vollständig Verschlüsselte Kommunikation zwischen einzelnen Netzwerkgeräten zum Standard gemacht.

Die UNMS 2 kann vollständig verschlüsselt kommunizieren, bietet gerade für Bestandssysteme einen automatischen Fallback-Modus für nicht verschlüsselte Geräte an. Zur Aktivierung dieser Funktion öffnen Sie zunächst unter Tools die UNMS – Optionen und wählen den „Security“-Reiter aus.



Voraussetzung:

1. Das Zielgerät muss mit PEM-Files kompatibel sein

Ob Sie einen PEM-File direkt laden können oder das Zertifikat in unterschiedliche Dateien aufgesplittet ist (dies ist z.B. bei Huawei der Fall), erfahren Sie im jeweiligen Benutzerhandbuch des Zielgeräts.

Tipp: PEM File Tutorial

Für alle Geräte der CS141 Produktfamilie finden Sie im CS141 Benutzerhandbuch eine ausführliche Anleitung, wie man einen PEM-File erstellt.

Diesen PEM-File können Sie selbstverständlich auch für die Kommunikation UNMS 2 <-> CS141 / BACS / SITEMANAGER / SITEMONITOR verwenden.

2. UNMS und Zielgerät benutzen das gleiche Zertifikat (den gleichen PEM-File)

Achten Sie unbedingt darauf, dass derselbe PEM-File beim CS141 bzw. das selbe Zertifikat auf dem jeweiligen Endgerät hinterlegt ist, da ansonsten die Kommunikation nicht funktionieren wird.

3. Wichtig: Verwenden Sie wenn möglich eigene Zertifikate und nicht die Default Zertifikate

Die Default-Zertifikate funktionieren, und können ab Werk auch verwendet werden. Sie können die Funktionen mit diesen Zertifikaten ausgiebig testen und Ihre Konfiguration optimieren. Für den produktiven Einsatz empfehlen wir jedoch, dass Sie eigene Zertifikate erstellen und verwenden.

Auswahlmöglichkeiten

Keep in mind, this is a GLOBAL stting: It is not possible to enable Force TLS on one device and configure another with "Don't use TLS". The UNMS offers you the following options:

Don't use TLS (unsecure communication)

Bei dieser Option wird vollständig auf TLS verzichtet. Dies erfordert jedoch, dass das Zielgerät dem entsprechend TLS-Optionen explizit ausgeschaltet hat, oder zumindest eine Kommunikation ohne TLS ermöglicht.

Use TLS if available

Wenn Sie eine heterogene Systemlandschaft betreiben, bei der sowohl ver- als auch unverschlüsselte Geräte kommunizieren müssen, ist diese Option die beste Wahl:

Die UNMS wird zunächst versuchen, eine verschlüsselte Verbindung aufzubauen. Ist dieses nicht möglich, wird jedoch automatisch für dieses eine Geräte auf die Verschlüsselung verzichtet.

Force use of TLS

Die UNMS 2 wird ausschließlich verschlüsselte Kommunikation versuchen, und sollte dies nicht möglich sein, einen Verbindungsfehler generieren. Gleichzeitig wird die UNMS eingehende Verbindungen ablehnen, sofern diese nicht verschlüsselt sind.

Das Quickstart Tutorial endet hier, im offiziellen Nutzerhandbuch der UNMS 2 erfahren Sie, wie Sie das volle Potential Ihrer UNMS 2 einrichten und nutzen können.