Benutzerhandbuch

icom Connectivity Suite

VPN und M2M SIM

Herausgeber:
INSYS MICROELECTRONICS GmbH
Hermann-Köhl-Str. 22
93049 Regensburg
Telefon: +49 941 58692 0
Telefax: +49 941 58692 45
E-Mail: info@insys-icom.de
Internet: http://www.insys-icom.de

Datum: Feb-23
Artikelnummer: 10001018
Version: 1.18
Sprache: DE

1 Allgemeines 6
2 Hintergrund VPN-Dienst 7
2.1 Vernetzung über die icom Connectivity Suite – VPN 7
2.2 Sichere Kommunikation 8
2.3 Einfache Einrichtung und Verwaltung 8
2.4 China-VPN 8
3 Anmeldung 9
3.1 Registrierung 9
3.2 Anmeldung an der icom Connectivity Suite 10
3.3 Verwalten des eigenen Passworts 10
3.4 Aktivieren von China-VPN 10
4 Konfiguration VPN-Dienst 11
4.1 Geräte 11
4.1.1 Anlegen eines Geräts 11
4.1.2 Verwalten der Geräte 14
4.1.3 Herunterladen der Geräteliste 15
4.1.4 Adressierung über Netmapping 16
4.1.5 Direkte Adressierung 17
4.1.6 Aktivierung des zeitlich begrenzten Zugangs für ein Gerät 18
4.1.7 Konfigurieren der Zwei-Faktor-Authentifizierung (TOTP) 20
4.1.8 Austausch von Zertifikaten 22
4.2 Gruppen 23
4.2.1 Anlegen einer Gruppe 23
4.2.2 Verwalten der Gruppen 24
4.2.3 Kommunikationsregeln 25
4.3 Monitoring 27
4.3.1 Anlegen einer Prüfung 27
4.3.2 Verwalten der Prüfungen 29
4.3.3 Anlegen eines Hosts 30
4.3.4 Verwalten der Hosts 31
4.3.5 Konfigurieren der Prüfungs-Optionen 32
4.4 Lizenzen 33
4.4.1 Bestellen einer Lizenz 34
4.4.2 Verwalten der Lizenzen 35
4.5 Web-Proxies 36
4.5.1 Einrichten eines Web-Proxies 37
4.5.2 Verwalten der Web-Proxies 38
4.6 Mein VPN 39
4.6.1 Ändern des Standard-Codes 39
4.6.2 VPN-Log herunterladen 40
4.6.3 VPN-Instanz neu starten 40
4.6.4 Verbindungs-Log herunterladen 40
4.6.5 Bestellen von Lizenzen 40
4.6.6 Verwalten der Zwei-Faktor-Authentifizierung 40

4.7 VPN-Teilnehmer 43
4.7.1 Konfigurieren eines INSYS-Routers mit icom OS 43
4.7.2 Konfigurieren eines INSYS-Routers mit INSYS OS 44
4.7.3 Konfigurieren eines Fremdgeräts 45
4.8 VPN-Aktivitäten 46

5 SIM-Karten-Management 47

6 Benutzer-Management 49
6.1.1 Anlegen eines Benutzers 49
6.1.2 Verwalten der Benutzer 50
6.1.3 Erzwingen der Zwei-Faktor-Authentifizierung für einen Benutzer 51
6.1.4 Herunterladen der Benutzerliste 51

1 Allgemeines

Dieses Zusatzhandbuch dient als Beschreibung der icom Connectivity Suite und ist nur zusammen mit dem Benutzerhandbuch, der Inline- und Online-Hilfe sowie dem Quick Installation Guide des jeweiligen Routers zu verwenden. Sicherheitshinweise, Technische Daten und Funktionsbeschreibungen sind dem Benutzerhandbuch des jeweiligen Geräts zu entnehmen. Die icom Connectivity Suite besteht aus zwei Produkten,

- dem VPN-Dienst **icom Connectivity Suite – VPN** und
- dem M2M SIM Service **icom Connectivity Suite – M2M SIM**.

Beide Produkte sind unabhängig voneinander, teilen sich jedoch eine Bedienoberfläche. Für Benutzer des M2M SIM Service sind nur die Abschnitte „Anmeldung“ und „SIM-Karten-Management“ in diesem Handbuch interessant.

Die icom Connectivity Suite – VPN wird von den meisten Routern und Störmeldern von INSYS icom unterstützt, unter anderem von:

- den auf icom OS basierenden Serien MRX, MRO, ECR, SCR und MIRO
- den auf INSYS OS basierenden Serien EBW, IMON, MoRoS, RSM und MLR

Kontaktieren Sie uns für andere Geräte von INSYS unter support@insys-icom.de.

Der Technsiche Support von INSYS (https://www.insys-icom.com/support/technischer-support/) empfiehlt, eine aktuelle Version des OpenVPN-Clients auf Geräten von Drittanbietern zu installieren.

Die icom Connectivity Suite – VPN stellt einen sicheren VPN-Dienst zur Verfügung: PCs, Router und lokal angeschlossene Netzwerkgeräte (z.B. Steuerungen, Messgeräte, Webcams) sind in allen Netzen erreichbar und jederzeit ansprechbar.

Ein Vorgehen in folgender Reihenfolge hat sich beim Aufbau eines VPN-Netzwerks mit der icom Connectivity Suite – VPN als vorteilhaft erwiesen:

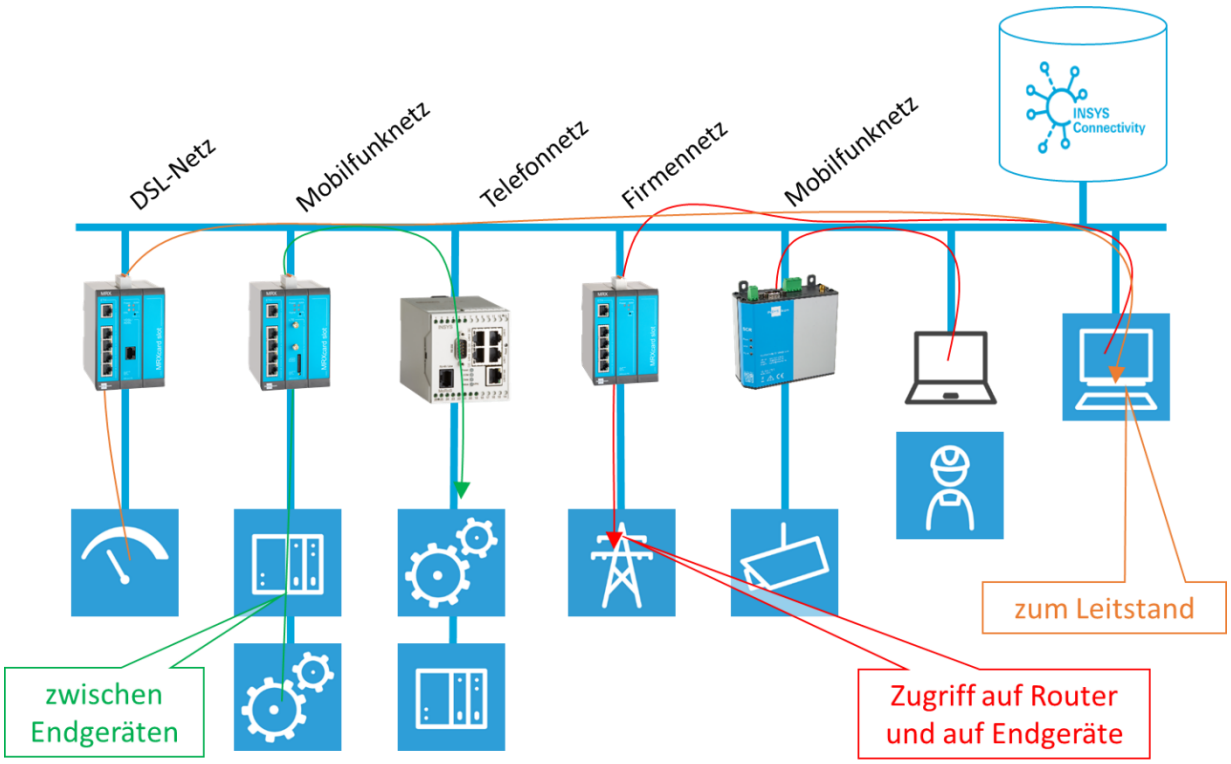
1. Planung der Netz-Topologie
2. Anlegen der Geräte (Clients) in der icom Connectivity Suite – VPN
3. Konfiguration der Geräte; dabei gibt es für Geräte von INSYS icom zwei Möglichkeiten:
   a) Konfiguration über den Schnellstart-Assistenten (vorteilhaft für Geräte, die noch nicht konfiguriert wurden (Werkseinstellungen))
   b) Konfiguration über die Konfigurationsdatei (vorteilhaft für bereits konfigurierte Geräte)

2 Hintergrund VPN-Dienst

Die icom Connectivity Suite – VPN ist ein Dienst von INSYS icom für die einfache und sichere Vernetzung von Standorten, Anlagen, Leitständen und mobilen Geräten über ein VPN-Netzwerk.

2.1 Vernetzung über die icom Connectivity Suite – VPN

Die über die icom Connectivity Suite – VPN vernetzten PCs und Router (VPN-Clients) sowie die lokal angeschlossene Netzwerkgeräte (z.B. Steuerungen, Messgeräte, Webcams) sind in allen Netzen erreichbar und jederzeit ansprechbar. Über einfache Regeln kann festgelegt werden, welcher Teilnehmer sich mit wem verbinden darf und welche Verbindungen nicht möglich sind.



Die icom Connectivity Suite – VPN (VPN-Server) sorgt für den Austausch der Routing-Informationen, indem er dies jedem VPN-Client bei der Anmeldung mitteilt. Bei einer Änderung am VPN-Netzwerk wird der Server neu gestartet, so dass eine erneute automatische Anmeldung jedes Clients erforderlich ist wobei die Routing-Informationen aktualisiert werden.

Wenn es sich bei den Clients um Router oder Störmelder von INSYS icom handelt, können diese so konfiguriert werden, dass sie direkt oder über Netmapping erreichbar sind. Letzteres ist hilfreich, wenn die Adressen im lokalen Netzwerk hinter dem Router nicht umkonfiguriert werden sollen, beispielsweise bei Serienmaschinen. Weitere Informationen dazu finden Sie im Abschnitt Konfiguration – Geräte dieses Handbuchs.

Die icom Connectivity Suite – VPN umfasst nicht nur den VPN-Server, sondern auch einen Web-Server für den Zugriff auf das Management-Portal zur Konfiguration des VPN-Diensts sowie einen Init-Server, der den INSYS-Routern im Rahmen des Schnellstarts die erforderlichen Konfigurationen zur Verfügung stellt.

2.2 Sichere Kommunikation

Der Server dieses VPN-Netzwerks ist sicher in einem deutschen Rechenzentrum gehostet. Das VPN-Netzwerk ist mit Zertifikaten abgesichert. Diese Zertifikate werden vom VPN-Server erstellt, verwaltet und regelmäßig erneuert. Der VPN-Zugriff erfolgt über den auf dem Reiter „Mein VPN“ angezeigten UDP-Port.

2.3 Einfache Einrichtung und Verwaltung

Die Verwaltung des VPN-Diensts erfolgt über ein übersichtliches Management-Portal. Sie müssen sich nicht um die Erzeugung und Verwaltung der Zertifikate kümmern, da dies alles von der icom Connectivity Suite – VPN übernommen wird. Der HTTPS-Zugriff auf das Management-Portal erfolgt über TCP-Port 443.

Sie profitieren von der icom Connectivity Suite – VPN, da Sie keinen eigenen OpenVPN-Server in Ihrem Netz betreiben müssen und somit dessen Betriebs- und Administrationskosten einsparen. Weiterhin ermöglicht er Ihnen eine hochflexible und einfach zu bedienende Rechtevergabe für alle OpenVPN-Clients sowie eine übersichtliche Verwaltung der Geräte im Feld.

Ihre Techniker profitieren von einer automatisierten OpenVPN-Konfiguration der Clients im Feld, die eine Installation ohne weiteres OpenVPN-Know-How ermöglicht. INSYS-Router erhalten mit Hilfe des Schnellstart-Assistenten die vollständige OpenVPN-Konfiguration sicher übermittelt.

2.4 China-VPN

Die icom Connectivity Suite ermöglicht eine sichere und zuverlässige Verbindung zu Geräten auf dem chinesischen Festland. Dazu muss Ihre icom Connectivity Suite dafür konfiguriert werden. Siehe dazu Aktivieren von China-VPN auf Seite 10.

Nach dieser Umstellung ist es möglich, beim Anlegen eines Geräts auszuwählen, ob dieses in China oder dem Rest der Welt installiert ist. Geräte, bei denen China als Gerätestandort ausgewählt sind, werden automatisch so konfiguriert, dass eine sichere und zuverlässige Verbindung vom chinesischen Festland aus mit der icom Connectivity Suite gewährleistet ist. Geräte, die als Rest der Welt konfiguriert sind, werden genauso konfiguriert wie alle anderen Geräte in der icom Connectivity Suite.

3 Anmeldung

3.1 Registrierung

Um die icom Connectivity Suite nutzen zu können, müssen Sie sich zuerst dafür registrieren. Dabei registrieren Sie sich unter anderem für einen 30-tägigen kostenlosen Testzugang in vollem Leistungsumfang, mit dem Sie vier Lizenzen für den Betrieb von Geräten im OpenVPN-Netzwerk erhalten. Der kostenlose Testbetrieb endet nach 30 Tagen automatisch. Anschließend können zwei Lizenzen dauerhaft kostenlos weiter genutzt werden. Informationen zur weiteren Lizenzierung finden Sie im Abschnitt Lizenzen dieses Handbuchs. Nutzern des SIM-Management-Portals entstehen hierdurch auch keine zusätzlichen Kosten.

Registrierung für die icom Connectivity Suite

1. ***Öffnen Sie die Seite*** https://connectivity.insys-icom.de

2. ***Wählen Sie Ihre Sprache und klicken Sie auf*** ***Registrieren***.

✓ Die Seite für die Registrierung des Zugangs öffnet sich.

3. ***Füllen Sie das Registrierungsformular entsprechend aus und klicken Sie auf*** ***Absenden***.

ⓘ Aus dem hier eingegebenen Firmennamen wird durch das System der Kundenname erzeugt, mit dem Sie sich im Schnellstart-Wizard der Geräte von INSYS icom für die icom Connectivity Suite anmelden. Dabei werden Leerzeichen durch Unterstriche ersetzt und Sonderzeichen umgewandelt. Der Benutzername dient zur Anmeldung am Management-Portal der icom Connectivity Suite.
Achten Sie auf die korrekte Schreibweise von Firmenname, E-Mail-Adresse, Benutzername und Passwort sowie die geforderten Pflichtfelder und das Akzeptieren der AGB.

✓ An die angegebene E-Mail-Adresse wird eine E-Mail mit einem Aktivierungslink gesendet.

4. ***Klicken Sie auf den Aktivierungslink in der E-Mail um Ihren Zugang freizuschalten.***

✓ Sie erhalten eine weitere E-Mail mit Ihren Zugangs- und Kundendaten.

✓ Nun können Sie die icom Connectivity Suite nutzen. Sie können den VPN-Dienst im Testbetrieb nutzen oder Lizenzen für den regulären Betrieb bestellen. Haben Sie INSYS M2M SIM-Karten bestellt, werden diese von uns im Rahmen der Bereitstellung Ihrem Zugang (Account) im Management Portal der icom Connectivity Suite zugeordnet.

3.2 Anmeldung an der icom Connectivity Suite

Anmeldung an der icom Connectivity Suite

→ Sie haben sich für die icom Connectivity Suite registriert und die E-Mail mit den Zugangsdaten erhalten

1. ***Gehen Sie auf die Seite*** https://connectivity.insys-icom.de
2. ***Geben Sie Benutzername und Passwort ein, wählen Sie Ihre Sprache und klicken Sie auf*** ***Anmelden***.

✓ Damit haben Sie sich erfolgreich am Management Portal der icom Connectivity Suite angemeldet.

3.3 Verwalten des eigenen Passworts

Ein sicheres Passwort für den Zugang zur icom Connectivity Suite ist entscheidend für die Sicherheit des VPN-Netzwerks. Bei der ersten Anmeldung eines vom Administrator angelegten Benutzers wird dringend empfohlen, dass Passwort auf ein nur diesem Benutzer bekanntes Passwort zu ändern. Genauso sollte das Passwort geändert werden, wenn der Verdacht besteht, dass dieses einem unbefugten Dritten bekannt geworden ist.

Ändern des Passworts

→ Sie haben sich an der icom Connectivity Suite angemeldet

1. ***Klicken Sie auf*** ***Einstellungen*** ***in der Titelleiste und wählen Sie „Passwort".***
2. ***Geben Sie Ihr altes Passwort ein, geben Sie Ihr neues Passwort ein, bestätigen Sie Ihr neues Passwort durch eine zweite Eingabe und klicken Sie auf*** ***Passwort ändern***.

ⓘ Mit der Schaltfläche Zurücksetzen werden sämtliche Eingaben in den Feldern gelöscht.

✓ Damit haben Sie Ihr Passwort für den Zugang zur icom Connectivity Suite geändert.

3.4 Aktivieren von China-VPN

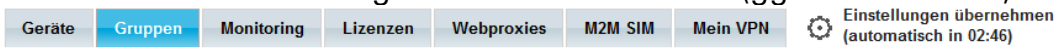
Wenden Sie sich an das Customer Support Center von INSYS icom (support@insys-icom.de), wenn Sie die icom Connectivity Suite für die Verwendung mit Geräten auf dem chinesischen Festland umstellen lassen möchten. Die icom Connectivity Suite wird dann manuell für China-VPN umkonfiguriert.

4 Konfiguration VPN-Dienst

4.1 Geräte

Auf dem Reiter Geräte können die einzelnen VPN-Teilnehmer als Gerät angelegt und verwaltet werden (Device-Management). Dabei wird unterschieden zwischen Routern und Störmeldern von INSYS icom und anderen, fremden Geräten. Dies können PCs, Steuerungen, Kameras, andere Router, etc. sein, die OpenVPN unterstützen und werden in der icom Connectivity Suite – VPN zusammenfassend PC genannt. Außerdem kann eine Liste aller angelegten Geräte heruntergeladen werden.

ⓘ Nach jedem Anlegen eines Geräts bzw. nach jeder Änderung an einem Gerät erscheint in Menüleiste ein Timer, der die Zeit bis zur vollständigen Übernahme der Einstellungen anzeigt. Wenn die Änderungen einen Neustart der OpenVPN-Server-Instanz erfordern, erfolgt mit dem Ablauf des Timers auch ein Neustart. Mit einem Klick auf das Zahnrad-Symbol wird der Timer beendet und es erfolgt eine sofortige Übernahme der Einstellungen (ggf. mit Neustart).
Dadurch verkürzt den Konfigurationsvorgang, indem alle Änderungen zusammengefasst und gleichzeitig ausgeführt werden. Ein aktiver Timer läuft nach dem Verlassen des Management-Portals weiter und übernimmt die Einstellungen nach seinem Ablauf (ggf. mit Neustart).



ⓘ Als zusätzliche Sicherheits- und Nachweisfunktion wird bei jedem Hinzufügen oder Löschen eines Geräts eine E-Mail an die in Ihrem Account hinterlegte E-Mail-Adresse gesendet. Diese Funktion kann nicht deaktiviert werden.

4.1.1 Anlegen eines Geräts

Beim Anlegen eines Geräts wird grundsätzlich unterschieden, ob es sich um einen INSYS-Router mit icom OS, mit INSYS OS oder einen PC handelt. Je nach Auswahl stehen verschiedene Parameter zur Verfügung.

Konfiguration (Reiter „Geräte“, Schaltfläche „Gerät hinzufügen“)

Mit dem **Gerätetyp** wählen Sie, ob es sich bei dem Gerät um einen INSYS-Router der entsprechenden Serien oder einen PC handelt. Je nach Auswahl ändert sich die im Folgenden beschriebene Konfiguration der Geräte-Adresse.

Der **Gerätestandort** muss für Geräte, die auf dem chinesischen Festland installiert sind, angegeben werden.

⚠ Dieses Auswahlfeld ist nur verfügbar, wenn Ihre icom Connectivity Suite für China-VPN konfiguriert ist. Siehe dazu Aktivieren von China-VPN auf Seite 10.

Der **Gerätename** ist ein Name, der das Gerät so eindeutig beschreibt, dass es von anderen Geräten unterschieden werden kann.

Die **Seriennummer** muss nur für INSYS-Router eingegeben werden und befindet sich bei diesen auf dem Aufkleber am Gerät.

Der **Geräte-Code** kann optional für einen INSYS-Router angegeben werden und wird für die Konfiguration des Routers über den Schnellstart-Assistent verwendet. Wird hier kein eigener Geräte-Code angegeben, wird der Standard-Code verwendet (konfigurierbar unter dem Reiter „Mein VPN“). Außerdem wird dieser Code auch als Passwort für den Zugriff auf den Router über einen Web-Proxy verwendet.

⚠ Aus Sicherheitsgründen wird die Vergabe eines individuellen Geräte-Codes empfohlen.

Das **Passwort für Zertifikat** kann bei Fremdgeräten für eine zusätzliche Sicherheit optional angegeben werden. Ist hier ein Passwort angegeben, muss dies auf dem OpenVPN-Client des PCs eingegeben werden.

⚠ INSYS empfiehlt, das Zertifikat durch ein starkes Passwort abzusichern, da dies insbesondere bei PCs und mobilen Geräten für zusätzliche Sicherheit sorgt.

⚠ Wenn ein Passwort für ein Zertifikat nachträglich angegeben wird, ist ein neues Zertifikat zu erzeugen (Schaltfläche "Neues Zertifikat"). Danach muss mit dieser Konfiguration eine neue Verbindung initiiert werden, damit der zusätzliche Passwortschutz wirksam wird.

Unter **Gruppe** kann das Gerät einer Gruppe zugeordnet werden. Sind noch keine Gruppen angelegt, steht hier nur die Standardgruppe zur Verfügung.

Unter **Lizenz** wird dem Gerät eine der verfügbaren Lizenzen zugeordnet.

Mit der Checkbox **Default-Überwachung** kann angegeben werden, ob die Erreichbarkeit des Geräts überwacht werden soll. Weitere Informationen dazu finden Sie im Abschnitt Monitoring dieses Handbuchs.

ⓘ Je nachdem, ob Sie einen INSYS Router mit INSYS OS, icom OS oder ein Gerät von Drittanbietern (PC) konfigurieren, ist nur einer der folgenden Absätze relevant. Hinweise zur Adressierung über Netmapping finden Sie unter Adressierung über Netmapping auf Seite 16; Hinweise zur direkten Adressierung finden Sie unter Direkte Adressierung auf Seite 17.

Für einen INSYS OS-Router kann mit dem Radiobutton **direkt erreichbar** bestimmt werden, ob das Gerät auf eine IP-Adresse durch die icom Connectivity Suite – VPN umkonfiguriert werden soll.
Dann wird mit dem Feld **erreichbare lokale IP-Adresse** die lokale IP-Adresse des Geräts angegeben, unter dem das Gerät (und weitere lokale Geräte) erreichbar sein sollen.

Für einen INSYS OS-Router kann mit dem Radiobutton **über Netmapping erreichbar** bestimmt werden, ob eine (eindeutige) virtuelle IP-Adresse auf die unveränderte lokale Adresse des Geräts umgeleitet werden soll.
Dann wird mit dem Feld **erreichbare Netmapping-Adresse** die virtuelle IP-Adresse des Geräts angegeben, unter dem das Gerät (und weitere lokale Geräte) erreichbar sein sollen.
Mit dem Feld **lokale IP-Adresse** kann die lokale IP-Adresse des Geräts angegeben werden. Die lokale IP-Adresse ist nicht von außen ansprechbar.

Für einen icom OS-Router wird mit dem Feld **Lokale IP-Adresse** die lokale IP-Adresse des Geräts angegeben, unter dem das Gerät (und weitere lokale Geräte) erreichbar sein sollen. Diese Adresse wird dem Router über die Router-Konfiguration zugewiesen.
Wird im Feld **erreichbar nur über Netmapping-IP** eine virtuelle IP-Adresse angegeben, ist das Gerät (und weitere lokale Geräte) nur über diese Adresse erreichbar. Diese Adresse wird dem Router über die Router-Konfiguration zugewiesen. Bei Netmapping muss außerdem die lokale IP-Adresse vorkonfiguriert werden auch wenn der Router darüber im VPN nicht erreichbar ist.

Für einen PC kann im Feld **Erreichbare IP-Adresse** die IP-Adresse des PCs angegeben werden, unter dem der PC (und weitere lokale Geräte) erreichbar sein sollen.

Die **Netzmaske** bestimmt die Größe des Netzes, das um die lokale IP-Adresse herum über Routing bekannt gemacht wird. Die Netzmaske kann in Langform (255.255.255.0) oder im CIDR-Format (/24) eingegeben werden. Wird eine andere Netzmaske als der Standard (255.255.255.0) eingegeben, wird der DHCP-Server im Gerät deaktiviert.

ⓘ Weitere Informationen dazu erhalten Sie unter dem Link „Einstellung der Netzwerke“.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

4.1.2 Verwalten der Geräte

Der Reiter „Geräte“ zeigt eine Liste der angelegten Geräte. Hier können die Geräte verwaltet und angepasst werden.

Konfiguration (Reiter „Geräte“)

Mit der Schaltfläche **Gerät hinzufügen** kann ein weiteres Gerät hinzugefügt werden.

Mit der Schaltfläche **Ersetzen** kann ein im Feld verwendetes Gerät durch ein neues Gerät ersetzt werden, indem die bestehenden Einstellungen bezüglich VPN-Konnektivität innerhalb der icom Connectivity Suite – VPN übernommen werden. Diese Funktion ist nur für Premium-Accounts verfügbar (nähere Informationen zu den Account-Typen finden Sie im Abschnitt „Lizenzen“).

Mit der Schaltfläche **Kopieren** kann ein weiteres Gerät hinzugefügt werden, wobei die Parameter des Fensters bereits mit denen des kopierten Geräts vorbelegt werden. Die Anpassung dieser Parameter ermöglicht ein schnelles Anlegen ähnlicher Geräte.

Mit der Schaltfläche **Löschen** kann dieses Gerät gelöscht werden.

In der Spalte **Gerät** wird der Gerätename dieses Geräts angezeigt.

Mit der Schaltfläche **Verwalten** können die Einstellungen dieses Geräts bearbeitet werden. Weiterhin kann hier ein neues Zertifikat angelegt werden und ältere Zertifikate können entwertet werden. Außerdem ist es möglich, den Router in der icom Connectivity Suite – VPN abzuschalten, d.h. er wird vom VPN-Netzwerk abgewiesen, solange die Checkbox „abgeschaltet“ markiert ist. Dies ist beispielsweise erforderlich, wenn einem Gerät nicht mehr vertraut werden kann (z.B. ein gestohlenes Notebook).
Es werden die Seriennummern für sämtliche für dieses Gerät ausgestellten Zertifikate angezeigt (siehe dazu Austausch von Zertifikaten auf Seite 22).
Optional kann für jedes Gerät ein zeitlich begrenzter Zugang (TR-Zugang) aktiviert und konfiguriert werden. Für PCs kann optional eine Zwei-Faktor-Authentifizierung mittels TOTP aktiviert werden (siehe dazu Konfigurieren der Zwei-Faktor-Authentifizierung (TOTP) auf Seite 20).

ⓘ Werden hier Änderungen vorgenommen, ist dafür zu sorgen, dass diese Änderungen auch im betroffenen Gerät vorgenommen werden. Dies kann für INSYS-Router entweder einmal täglich automatisch (wenn der Router zu diesem Zeitpunkt online ist) oder manuell vorgenommen werden, indem die Funktion für das automatische Update im Web-Interface des Routers manuell angestoßen wird. Bei PCs müssen die Änderungen immer manuell vorgenommen werden.

ⓘ Wird hier der Geräte-Code geändert, muss dieser in den Einstellungen des Update-Servers im Web-Interface des Routers manuell geändert werden, da ansonsten kein automatisches Update mehr möglich ist.

Mit der Schaltfläche **Herunterladen** können eine Konfigurationsdatei für dieses Gerät sowie ein Container mit den Zertifikaten und Schlüsseln heruntergeladen werden.

Mit der Schaltfläche **Mehr Info** können weitere Informationen zu diesem Gerät wie das übertragene Datenvolumen oder die VPN-IP-Adresse angezeigt werden.

In der Spalte **Status** wird der aktuelle Zustand dieses Geräts mit einer Verzögerung von 1-2 Minuten angezeigt. Folgende Zustände sind möglich:

- online: Der Router ist mit der icom Connectivity Suite – VPN verbunden.
- offline: Der Router ist nicht mit der icom Connectivity Suite – VPN verbunden.
- abgeschaltet: Der Router wurde abgeschaltet (siehe Schaltfläche Verwalten oben).
- ohne Lizenz: Dem Router ist keine Lizenz zugeordnet oder die zugeordnete Lizenz ist abgelaufen (wenn die Lizenz abgelaufen ist, wird der Router auch abgeschaltet).

In der Spalte **TR-Zugang** wird angezeigt, ob der zeitlich begrenzte Zugang (auf Anfrage erhältlich) für dieses Gerät aktiviert ist.

In der Spalte **seit** wird angezeigt, seit wann sich dieses Gerät in diesem Zustand befindet.

In der Spalte **Gruppe** wird angezeigt, welcher Gruppe dieses Gerät zugeordnet ist.

In der Spalte **erreichbare IP** wird die IP-Adresse angegeben, unter der dieses Gerät erreichbar ist.

In der Spalte **S/N** wird die Seriennummer dieses Geräts angezeigt (nur für INSYS-Geräte).

In der Spalte **Lizenz** wird der Lizenzumfang angegeben.

4.1.3 Herunterladen der Geräteliste

Der Reiter „Geräte“ zeigt eine Liste der angelegten Geräte. Diese Liste kann als CSV-Datei heruntergeladen werden. Zusätzlich zu den in der Liste dargestellten Informationen enthält die Datei auch Informationen über das verbrauchte Datenvolumen im aktuellen Monat, im Vormonat, und über den gesamten Zeitraum seit Anlegen des Gerätes. Die CSV-Datei enthält die Spalten analog zur Geräteliste getrennt durch ein „=“ (Gleichheitszeichen).

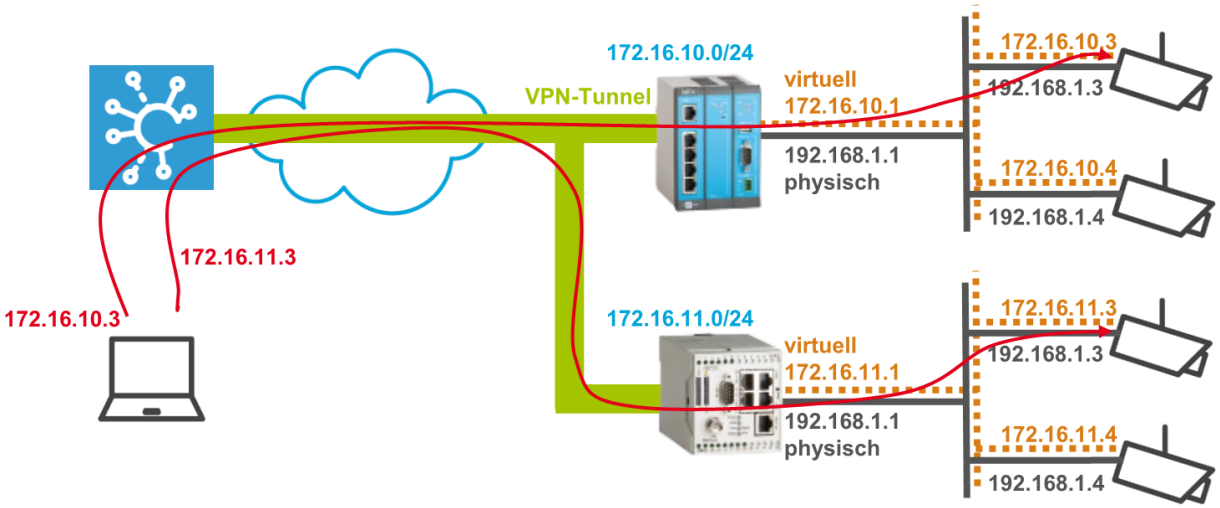
Konfiguration (Reiter „Geräte“, Schaltfläche „Geräteliste herunterladen“)

Mit einem Klick auf **Geräteliste** wird im Download-Fenster die Geräteliste heruntergeladen.

4.1.4 Adressierung über Netmapping

Die Verwendung von Netmapping ermöglicht, dass die Geräte im lokalen Netzwerk hinter einem INSYS-Router nicht umkonfiguriert werden müssen. Dabei wird dem lokalen Netzwerk eine virtuelle Netzadresse zugewiesen. Geräte im lokalen Netzwerk können anschließend über die icom Connectivity Suite – VPN mit der virtuellen Adresse angesprochen werden. Der Router tauscht den Netzwerkanteil der virtuellen IP-Adresse gegen den Netzwerkanteil des lokalen Netzwerkes aus und leitet das Paket an das Ziel weiter.

In folgendem Beispiel sind die beiden INSYS-Router so konfiguriert, dass die Geräte im lokalen Netz über Netmapping erreichbar sind, obwohl die Adressen im lokalen Netz unverändert bleiben. Sie müssen nicht umkonfiguriert werden, obwohl sie dieselben lokalen Netzwerkadressen haben.



4.1.4.1 Netmapping in INSYS Routern mit icom OS

Wenn die Konfiguration des Routers über die icom Connectivity Suite – VPN erfolgt, wird Netmapping automatisch eingerichtet. Dazu werden entsprechende NAT-Regeln konfiguriert. Manuell können unten stehende NAT-Regeln im Menü „Netzfilter“ auf der Seite „NAT“ eingerichtet werden. Weitere Hinweise dazu finden Sie in der Inline- und Online-Hilfe des Routers.

In obigem Beispiel werden im oberen Router folgende NAT-Regeln angelegt:

Source-NAT-Regel:

Typ: Netmap

Protokoll: Alle

Ausgehendes Interface: openvpn1 – icom Connectivity Suite – VPN

Absender-IP-Adresse: 192.168.1.0/24

Source-NAT auf Adresse: 172.16.10.0

Destination-NAT-Regel:

Typ: Netmap

Protokoll: Alle

Eingehendes Interface: openvpn1 – icom Connectivity Suite – VPN

Absender-IP-Adresse: 172.16.10.0/24

Source-NAT auf Adresse: 192.168.1.0

Die DNAT-Regel bewirkt, dass Pakete im VPN-Dienst, die an Adressen im Netzwerk 172.16.10.0/24 gerichtet sind, an die entsprechenden Adressen im lokalen Netzwerk 192.168.1.0/24 weitergeleitet werden. Die SNAT-Regel bewirkt, dass Pakete von den Geräten im lokalen Netzwerk 192.168.1.0/24, die in das VPN-Netzwerk gerichtet sind, mit einer Absender-IP-Adresse im Netzwerk 172.16.10.0/24 versehen werden.

Dadurch sind die Geräte im lokalen Netzwerk (192.168.1.0/24) auch über die virtuelle Netzadresse (172.16.10.0/24) erreichbar und müssen nicht umkonfiguriert werden. Die Kamera mit der lokalen Netzwerkadresse 192.168.1.3 kann somit von außen über die Adresse 172.16.10.3 erreicht werden.

4.1.4.2 Netmapping in INSYS-Routern mit INSYS OS

Wenn die Konfiguration des Routers über die icom Connectivity Suite – VPN erfolgt, wird Netmapping automatisch eingerichtet. Manuell kann Netmapping im Menü „Basic Settings“ auf der Seite „IP-Adresse (LAN)“ des INSYS-Routers eingerichtet werden. Weitere Hinweise dazu finden Sie im Benutzerhandbuch des Routers.

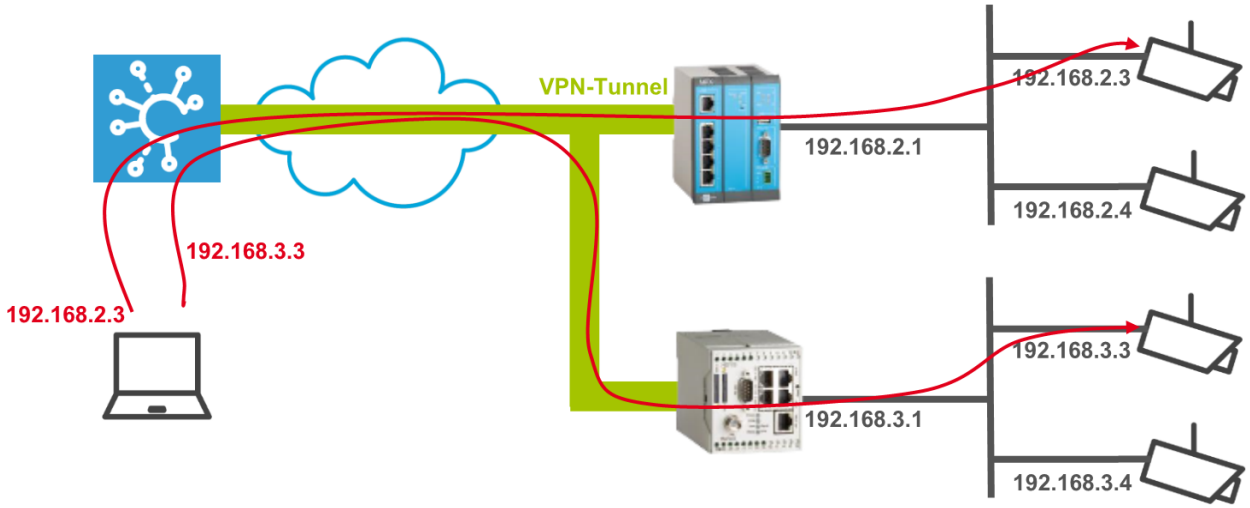
In obigem Beispiel wird im unteren Router Netmapping aktiviert und die virtuellen Netzadresse „172.16.11.0“ im lokalen Netz konfiguriert.

Dadurch sind die Geräte im lokalen Netzwerk (192.168.1.0/24) auch über die virtuelle Netzadresse (172.16.11.0/24 unten) erreichbar und müssen nicht umkonfiguriert werden. Die Kamera mit der lokalen Netzwerkadresse 192.168.1.3 kann somit von außen über die Adresse 172.16.11.3 erreicht werden.

4.1.5 Direkte Adressierung

Bei der direkten Adressierung werden die Geräte im lokalen Netzwerk über die icom Connectivity Suite – VPN mit ihrer Adresse direkt angesprochen.

In folgendem Beispiel ist dies im Gegensatz zur Adressierung über Netmapping dargestellt.



4.1.6 Aktivierung des zeitlich begrenzten Zugangs für ein Gerät

Der zeitlich begrenzte Zugang (time-restricted (TR) access) ist nicht Teil des Standard-Funktionsumfangs und auf Anfrage verfügbar. Für jedes Gerät, insbesondere den Gerätetyp PC, kann ein zeitlich begrenzter Zugang eingerichtet werden. Damit kann einem Gerät der Zugang begrenzt auf eine bestimmte Zeit gewährt werden. Ohne einen zeitlich begrenzten Zugang kann von jedem Gerät aus eine Verbindung zum VPN-Netzwerk aufgebaut werden. Dazu muss nur dessen OpenVPN-Client mit der für ein Gerät vom Typ PC in der icom Connectivity Suite heruntergeladenen Konfigurationsdatei konfiguriert worden sein. Wird der zeitlich begrenzte Zugang für ein Gerät aktiviert, werden Verbindungen von diesem Gerät aus ins VPN-Netzwerk nur dann für eine bestimmte Zeit freigegeben, wenn der Anwender dies mit Hilfe eines per E-Mail versandten Tokens bestätigt.

Dabei sind zwei verschiedene Freigaben möglich:

- Aktivierung der Verbindung für ein bestimmtes Zeitfenster
- Aktivierung der Verbindung für eine bestimmte Dauer

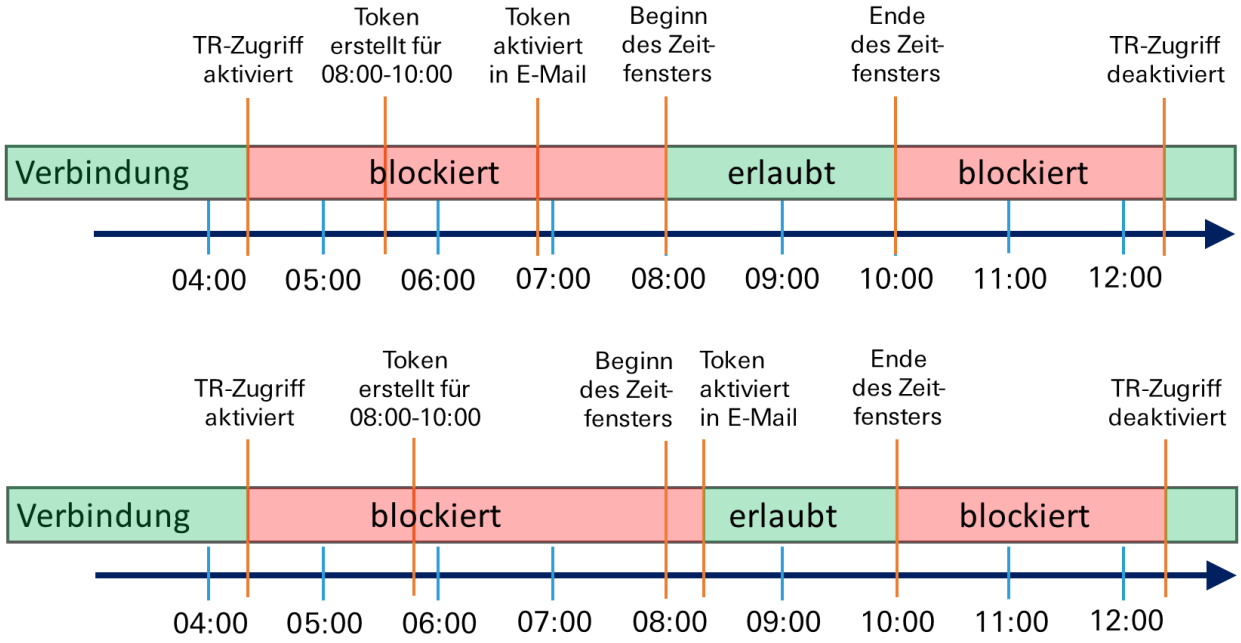
Der zeitlich begrenzte Zugang wird in der Geräteliste (Reiter **Geräte**) in den Geräteeinstellungen (Schaltfläche **Verwalten** (⚙) des jeweiligen Geräts) über die Schaltfläche **TR-Zugang verwalten** konfiguriert.

Hier wird die Funktion mit der Checkbox **Zeitlich begrenzten Zugang aktivieren** aktiviert. Der Token wird an die dort angegebene E-Mail-Adresse versandt.

4.1.6.1 Aktivierung der Verbindung für ein bestimmtes Zeitfenster

Im Modus **Zeitfenster** wird das Zeitfenster angegeben, in welchem Verbindungen von diesem Gerät aus ins VPN-Netzwerk nach der Authentifizierung über den Link in der E-Mail freigegeben sind.

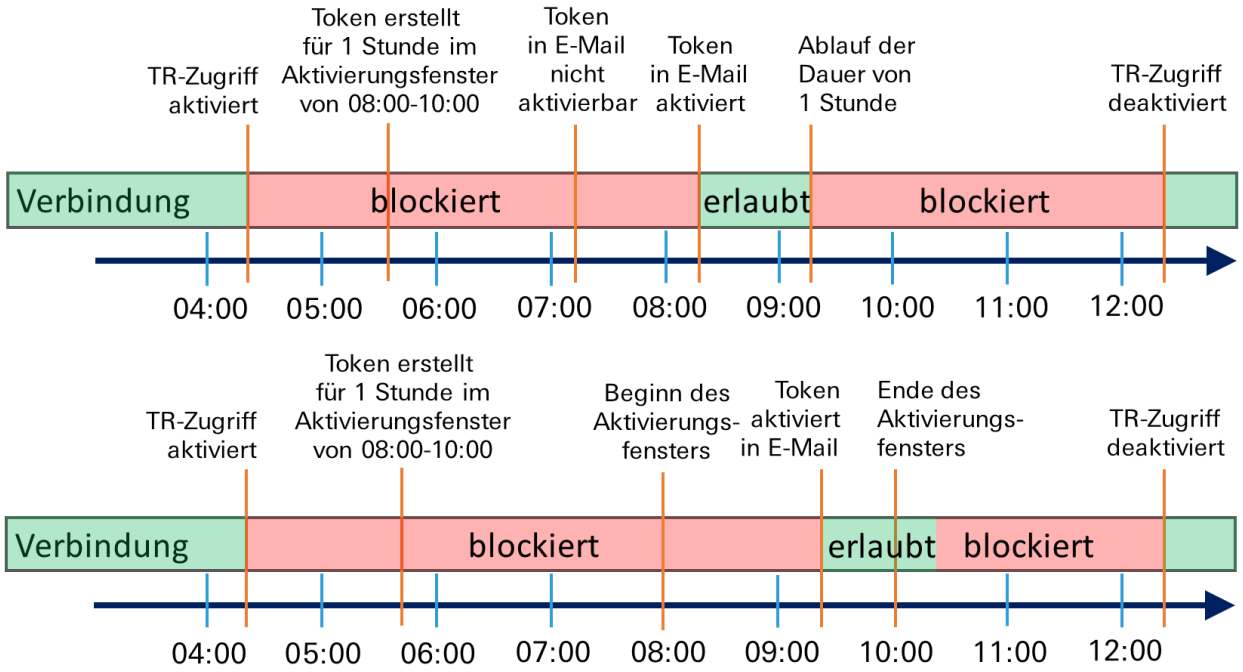
Folgendes Diagramm zeigt verschiedene Beispiele für den Ablauf eines zeitlich begrenzten Zugangs für ein bestimmtes Zeitfenster:



4.1.6.2 Aktivierung der Verbindung für eine bestimmte Dauer

Im Modus **Dauer** wird der Zeitraum angegeben, für den Verbindungen von diesem Gerät aus ins VPN-Netzwerk nach der Authentifizierung über den Link in der E-Mail freigegeben sind. Weiter wird ein Zeitfenster festgelegt, in dem die Authentifizierung über den Link in der E-Mail erfolgen kann (Aktivierungsfenster).

Folgendes Diagramm zeigt verschiedene Beispiele für den Ablauf eines zeitlich begrenzten Zugangs für eine bestimmte Dauer:



4.1.7 Konfigurieren der Zwei-Faktor-Authentifizierung (TOTP)

Zur Erhöhung der Sicherheit kann für Geräte vom Typ PC eine Zwei-Faktor-Authentifizierung mittels TOTP eingerichtet werden.

Die Zwei-Faktor-Authentifizierung fügt der Anmeldung über das Zertifikat (mit oder ohne Passwortschutz) ein weiteres Sicherheitsniveau hinzu, indem es die zusätzliche Eingabe eines Einmal-Passworts erfordert. Dass Passwort wird über das TOTP (Time-based One-time Password)-Verfahren mit Hilfe einer App auf einem separatem Gerät (z.B. Smartphone) erzeugt. Während der Einrichtung muss die App, die das Einmal-Passwort (TOTP) zur Verfügung stellt, (einmalig) mit dem gerät vom Typ PC in der icom Connectivity Suite synchronisiert werden. TOTP ist ein offener Standard und es sind eine Vielzahl von Apps für verscheidene Plattformen wie die Open Source-Software FreeOTP (https://freeotp.github.io/) verfügbar. Da die Einmal-Passwörter zeitbasiert erzeugt werden und nur eine begrenzte Zeit gültig sind, ist es erforderlich, dass die Uhrzeit auf dem separatem Gerät genau ist und regelmäßig synchronisiert wird.

Gehen Sie wie folgt vor, um die Zwei-Faktor-Authentifizierung für das Gerät vom Typ PC zu aktivieren.

Einrichten der Zwei-Faktor-Authentifizierung für einen PC

- ⇢ Sie haben sich an der icom Connectivity Suite angemeldet
- ⇢ Das Gerät, für das die Zwei-Faktor-Authentifizierung aktiviert werden soll, ist bereits angelegt (siehe Anlegen eines Geräts auf Seite 11)
- ⇢ Sie haben den Reiter „Geräte“ geöffnet

1. ***Klicken Sie auf die Schaltfläche „verwalten“ (⚙) in der Zeile des Geräts.***
2. ***Klicken Sie auf die Schaltfläche „TOTP für dieses Gerät einrichten“.***
3. ***Scannen Sie den angezeigten QR-Code mit der TOTP-App.***
4. ***Erzeugen Sie in der App das Einmal-Passwort und geben Sie es in der icom Connectivity Suite ein.***
5. ***Klicken Sie auf „Einmal-Passwort konfigurieren“.***

   ✓ Damit haben Sie die Zwei-Faktor-Authentifizierung für dieses Gerät eingerichtet.

6. ***Klicken Sie auf die Schaltfläche „Herunterladen“ (⤓) in der Zeile des Geräts.***
7. ***Importieren Sie diese Konfigurationsdatei in den OpenVPN-Client Ihres PCs und initiieren Sie eine Verbindung.***

8. Geben Sie zur Authentifizierung der Verbindung folgendes ein:

- Benutzername: insys
- Passwort: ein Einmalpasswort aus Ihrer TOTP-App
- Private Key-Passwort: das Passwort für das Zertifikat, das beim Anlgegen des Geräts vom Typ PC angegeben wurde – wurde hier kein Passwort konfiguriert, ist das Zertifikat nicht passwortgeschützt und es wird kein Schlüssel angefordert

✓ Der OpenVPN-Client verbindet sich mit der icom Connectivity Suite.

Gehen Sie wie folgt vor, um die Zwei-Faktor-Authentifizierung für ein Gerät vom Typ PC zu deaktivieren.

Deaktivieren der Zwei-Faktor-Authentifizierung für einen PC

⇢ Sie haben sich an der icom Connectivity Suite angemeldet

⇢ Die Zwei-Faktor-Authentifizierung ist für das fragliche Gerät aktiv

⇢ Sie haben den Reiter „Geräte“ geöffnet

1. Klicken Sie auf die Schaltfläche „verwalten“ (⚙) in der Zeile des Geräts.

2. Klicken Sie auf die Schaltfläche „TOTP für dieses Gerät deaktivieren“.

✓ Damit haben Sie die Zwei-Faktor-Authentifizierung für dieses Gerät wieder deaktiviert.

ⓘ Nach dem Deaktivieren der Zwei-Faktor-Authentifizierung müssen Sie die Konfigurationsdatei erneut herunterladen und wieder in den OpenVPN-Client Ihres PCs importieren. Wenn auch kein Passwort zur Verschlüsselung des Zertifikats vorhanden ist, erfolgt keine Authentifizierung bei einer erneuten Verbindung.

ⓘ Wird eine Zwei-Faktor-Authentifizierung für ein Gerät deaktiviert, sollte sie auch aus der App gelöscht werden. Wenn Sie wieder aktiviert wird, muss sie in der App neu eingerichtet werden.

4.1.8 Austausch von Zertifikaten

Zusätzlich zur regelmäßigen Rotation der Zertifikate alle 90 Tage läuft das CA-Zertifikat nach 10 Jahren auch aus und muss dann ersetzt werden. Der Benutzer wird mit 120 Tagen Vorlauf darüber (per E-Mail und Benachrichtigung bei Anmeldung) informiert. Mit dieser CA erstellte Client-Zertifikate müssen dann ausgetauscht werden, damit sich das Gerät weiterhin mit der icom Connectivity Suite verbinden kann.

Im Dialogfeld „Gerät verwalten“ werden die Seriennummern für die für dieses Gerät ausgestellten Zertifikate angezeigt. Wird die Seriennummer fett und schwarz dargestellt, ist das Zertifikat aktuell. Eine gelbe Nummer bedeutet, dass das Zertifikat von der alten CA ausgestellt wurde und nur noch 30-120 Tage funktioniert (so lange das alte CA-Zertifikat gültig ist). Unter 30 Tagen Gültigkeit wird die Seriennummer rot dargestellt. Ist mehr als eine Seriennummer angezeigt, handelt es sich dabei um Zertifikate, die ausgestellt aber noch nicht angewendet wurden, oder um Zertifikate, die abgelaufen, aber noch nicht gelöscht sind. Normalerweise werden abgelaufene Zertifikate nach 15-30 Minuten gelöscht. Wenn mehrere Seriennummern angezeigt werden, wird ein Austausch des Zertifikats und die Aktualisierung der Konfiguration für die icom Connectivity Suite auf dem Router empfohlen.

Je nach Gerät und Zustand sind folgende Maßnahmen erforderlich, um das Zertifikat auszutauschen und die Konfiguration zu aktualisieren:

4.1.8.1 INSYS-Router, der noch in der icom Connectivity Suite erreichbar ist

Stellen Sie sicher, dass der Update-Server der icom Connectivity Suite im Router aktiviert ist. Dies erfolgt im Router-Menü “Administration” auf der Seite “Update”. Wenn dieser aktiviert ist, erfolgt eine automatische Aktualisierung des Zertifikats im Betrieb.

4.1.8.2 INSYS-Router, der nicht mehr in der icom Connectivity Suite erreichbar ist

In diesem Fall muss das Zertifikat über einen lokalen Zugriff am Router ausgetauscht werden. Siehe dazu Manuelle Konfiguration (für einen icom OS-Router) auf Seite 44 bzw. Manuelle Konfiguration (für einen INSYS OS-Router) auf Seite 45.

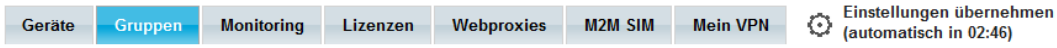
4.1.8.3 Fremdgerät (PC, Steuerung, Tablet, etc.)

Bei einem Fremdgerät muss die OpenVPN-Konfiguration manuell am Fremdgerät ausgetauscht werden. Siehe dazu Konfigurieren eines Fremdgeräts auf Seite 45.

4.2 Gruppen

Auf dem Reiter Gruppen können die Gruppen, denen die Geräte zugeordnet sind, angelegt und verwaltet werden (Gruppen-Management). Gruppen dienen dazu, Geräte mit ähnlicher Funktion zusammenzufassen, um ihnen gemeinsame Kommunikationsregeln zuzuordnen.

ⓘ Nach jeder Änderung an einer Gruppe erscheint in der Menüleiste ein Timer, der die Zeit bis zum Übernehmen der Einstellungen anzeigt. Mit einem Klick auf das Zahnrad-Symbol erfolgt ein sofortiger Neustart. Da sämtliche Änderungen der Gruppen-Konfiguration einen Neustart der OpenVPN-Server-Instanz erfordern, verkürzt dies den Konfigurationsvorgang, indem alle Änderungen, die einen Neustart erfordern, zusammengefasst und gleichzeitig ausgeführt werden. Ein aktiver Timer läuft nach dem Verlassen des Management-Portals weiter und startet die OpenVPN-Server-Instanz nach seinem Ablauf neu.



4.2.1 Anlegen einer Gruppe

Vor dem Anlegen von Gruppen empfiehlt es sich, eine sinnvolle Einteilung der Geräte in Gruppen zu überlegen.

Konfiguration (Reiter „Gruppen“, Schaltfläche „Gruppe hinzufügen“)

Der **Gruppenname** ist ein Name, der die Gruppe so eindeutig beschreibt, dass sie von anderen Gruppen unterschieden werden kann.

Mit der Checkbox **Verbindungen unter Gruppenmitgliedern erlauben** kann angegeben werden, ob sich die Geräte innerhalb dieser Gruppe untereinander verbinden können.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

4.2.2 Verwalten der Gruppen

Der Reiter „Gruppen“ zeigt eine Liste der angelegten Gruppen. Hier können die Gruppen verwaltet werden. Außerdem wird hier die Kommunikation innerhalb einer Gruppe und zwischen verschiedenen Gruppen festgelegt.

Konfiguration (Reiter „Gruppen“)

Mit der Schaltfläche **Gruppe hinzufügen** kann eine weitere Gruppe hinzugefügt werden.

Mit der Schaltfläche **Kopieren** kann eine weitere Gruppe hinzugefügt werden, wobei die Parameter des Fensters bereits mit denen der kopierten Gruppe vorbelegt werden. Die Anpassung dieser Parameter ermöglicht ein schnelles Anlegen ähnlicher Gruppen.

Mit der Schaltfläche **Löschen** kann diese Gruppe gelöscht werden.

In der Spalte **Gruppenname** wird der Name dieser Gruppe angezeigt.

Mit der Schaltfläche in der Spalte **Interne Verbindungen** kann festgelegt werden, ob Verbindungen zwischen den Geräten in dieser Gruppe erlaubt oder verboten sind.

Mit der Schaltfläche in der Spalte **Verbindung von** kann festgelegt werden, von welchen Gruppen eingehende Verbindungen akzeptiert werden, d.h. Geräte in den markierten Gruppen können Verbindungen zu den Geräten in dieser Gruppe aufbauen. Weiterhin können diese Verbindungen auf bestimmte Protokolle, Ziel-Stationen und Ziel-Ports eingeschränkt werden (Gruppen-Management advanced). Die Namen der für diese Verbindungen zugelassenen Gruppen werden auf der Schaltfläche angezeigt. Der Zusatz [LIMITED] zeigt an, dass zusätzliche Beschränkungen für diese Verbindungen festgelegt wurden.

Mit der Schaltfläche in der Spalte **Verbindung nach** kann festgelegt werden, zu welchen Gruppen ausgehende Verbindungen aufgebaut werden können, d.h. Geräte in dieser Gruppe können Verbindungen zu den Geräten in den markierten Gruppen aufbauen. Weiterhin können diese Verbindungen auf bestimmte Protokolle, Ziel-Stationen und Ziel-Ports eingeschränkt werden (Gruppen-Management advanced). Die Namen der für diese Verbindungen zugelassenen Gruppen werden auf der Schaltfläche angezeigt. Der Zusatz [LIMITED] zeigt an, dass zusätzliche Beschränkungen für diese Verbindungen festgelegt wurden.

Wenn eine Verbindung mit einer der Schaltflächen „Verbindung von“ oder „Verbindung nach“ festgelegt wird, wird diese automatisch auch für die andere Richtung festgelegt.

4.2.3 Kommunikationsregeln

Die Kommunikationsregeln legen fest, ob sich PCs, INSYS-Router und daran lokal angeschlossene Geräte miteinander verbinden dürfen.

4.2.3.1 Kommunikation innerhalb einer Gruppe

Die icom Connectivity Suite – VPN ermöglicht es, allen Geräten, die sich in einer Gruppe befinden, die Kommunikation untereinander zu erlauben oder zu verbieten. Ein Verbot von internen Verbindungen ist beispielsweise sinnvoll, wenn sich Geräte unterschiedlicher Kunden in einer Gruppe befinden. Die Festlegung der Regel für die interne Kommunikation erfolgt beim Anlegen der Gruppe und kann auf dem Reiter „Gruppen“ in der Spalte „Interne Verbindungen“ jederzeit geändert werden.

4.2.3.2 Kommunikation zwischen Gruppen

Die icom Connectivity Suite – VPN ermöglicht es, Regeln für die Kommunikation zwischen Geräten, die sich in einer Gruppe befinden, und Geräten, die sich in einer anderen Gruppe befinden, festzulegen. Die Festlegung der Regeln für die Kommunikation zwischen den Gruppen erfolgt auf dem Reiter „Gruppen“ in den Spalten „Verbindung von“ (eingehend) bzw. „Verbindung nach“ (ausgehend) für die jeweilige Gruppe. Wenn für eine Gruppe (A) beispielsweise eingehende Verbindungen von einer anderen Gruppe (B) erlaubt werden, werden automatisch für die Gruppe (B) ausgehende Verbindungen zu Gruppe (A) erlaubt.

4.2.3.3 Einschränkungen bei der Kommunikation zwischen Gruppen

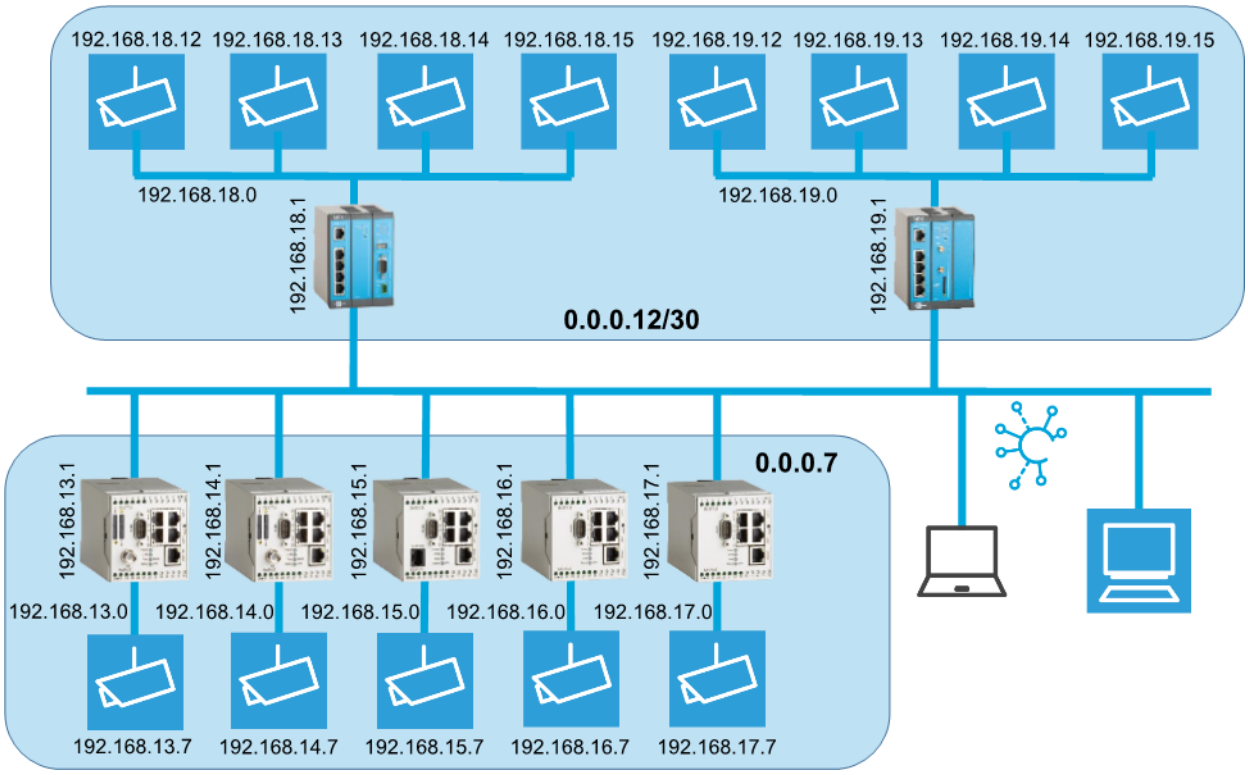
Wenn Verbindungen zwischen den Geräten einzelner Gruppen erlaubt sind, ist bei Verbindungen zu einem Router der Zugriff auf das gesamte Netz hinter diesem Router freigegeben. Daher ist es möglich, diese Verbindungen auf bestimmte Protokolle, Ziel-Stationen und Ziel-Ports einzuschränken. Dies erfolgt beim Festlegen der erlaubten Verbindungen durch Markieren der Checkbox „zusätzliche Beschränkungen für die Verbindungs-Ziele“.

Protokoll

Es ist möglich, das für die Verbindung verwendete Protokoll auf „TCP+UDP“, „TCP“, „UDP“ oder „ICMP“ zu beschränken. Wenn hier ein bestimmtes Protokoll ausgewählt ist, können nur Verbindungen über dieses Protokoll zwischen den Geräten der betreffenden Gruppen aufgebaut werden. Nutzverbindungen verwenden in der Regel TCP oder UDP; der Ping-Befehl zur Prüfung der Erreichbarkeit verwendet ICMP.

Ziel-Station

Durch die Angabe einer Ziel-Station ist es möglich, die Verbindungen auf bestimmte Geräte im Netzwerk hinter dem Router zu beschränken. Bei der Ziel-Station wird nur der Teil der Adresse angegeben, der die Bezeichnung innerhalb des jeweiligen Netzwerks angibt. Diese Angabe wird zur Netzadresse „addiert“, um die IP-Adresse des Ziel-Geräts zu erhalten. Mit Hilfe einer Netzmaske in CIDR-Notation kann auch eine Ziel-Station angegeben werden, die einen ganzen IP-Adressbereich definiert. Folgendes Beispiel illustriert die Wirkungsweise der Angabe einer Ziel-Station:



In diesem Beispiel ist für Verbindungen zu den Geräten in der unteren Gruppe die Ziel-Station 0.0.0.7 konfiguriert. Das bedeutet, dass beispielsweise im Netzwerk mit der Adresse 192.168.13.0 Verbindungen zum Gerät (Kamera) mit der IP-Adresse 192.168.13.7 über den Router mit der IP-Adresse 192.168.13.1 aufgebaut werden können. Dies gilt entsprechend auch für die anderen Geräte in dieser Gruppe.

Für Verbindungen zu den Geräten in der oberen Gruppe ist die Ziel-Station 0.0.0.12/30 konfiguriert. Das bedeutet, dass beispielsweise im Netzwerk mit der Adresse 192.168.18.0 Verbindungen zu den Geräten mit den IP-Adressen 192.168.18.12 bis 192.168.18.15 über den Router mit der IP-Adresse 192.168.18.1 aufgebaut werden können. Dies gilt entsprechend auch für die anderen Geräte in dieser Gruppe.

Ziel-Port

Durch die Angabe eines Ziel-Ports ist es möglich, TCP- und UDP-Verbindungen auf bestimmte Ports zu beschränken. Es können mehrere Ports, getrennt durch Kommas oder ganze Port-Bereiche angegeben werden. Die Ziel-Port-Angabe „80, 443, 1194-1199“ erlaubt beispielsweise Verbindungen über die Ports 80, 443, 1194, 1195, 1196, 1197, 1198 und 1199.

4.3 Monitoring

Die Monitoring-Funktion dient zum Überwachen und Sicherstellen der Erreichbarkeit aller Teilnehmer im VPN-Netzwerk (Netzwerk-Monitoring). Dafür stehen verschieden Möglichkeiten zur Überprüfung der Verbindung zur Verfügung. Auf dem Reiter Monitoring können die Prüfungen und Hosts angelegt und verwaltet werden. Hosts sind alle Netzwerkgeräte, die über eine IP-Adresse im VPN-Netzwerk angesprochen werden können. Das sind die VPN-Teilnehmer (Router, PCs, Tablets, etc.) selbst und die Geräte im Netzwerk (Control Network, OT) hinter den Routern (Steuerungen, Panel-PCs, HMIs, Datenlogger, Messgeräte, Condition-Monitoring- oder Edge-Computing-Geräte, etc.).

Wenn die Überprüfung einer Verbindung fehlschlägt, wird ein Fehlerbericht an eine hinterlegte E-Mail-Adresse versendet. Sobald diese Überprüfung wieder erfolgreich ist, wird eine weitere E-Mail versandt, die über die Wiederherstellung der Verbindung informiert.

Prüfungen werden durch etwaige Kommunikationsregeln nicht beeinflusst.

Pro gültiger VPN-Lizenz können fünf Prüfungen angelegt werden, wobei diese Prüfungen über alle Geräte verteilt werden können und nicht auf das der jeweiligen Lizenz zugeordnete Gerät beschränkt sind. Die Zahl der Hosts ist nicht beschränkt.

Die Prüfungen der Typen PING, HTTP und HTTPS verursachen Datenverkehr über die VPN-Verbindung. Die Prüfung vom Typ VPN verursacht kein zusätzliches Datenaufkommen, da auf dem VPN-Server die fortlaufende Tunnelüberwachung ausgewertet wird.

Siehe dazu auch die FAQ zum Netzwerk-Monitoring.

4.3.1 Anlegen einer Prüfung

Beim Anlegen eines Geräts wird eine Prüfung angelegt, wenn die Checkbox „Default-Überwachung“ markiert ist. Dann wird automatisch dieses Gerät als Host angelegt sowie eine Ping-Prüfung mit einem Intervall von 60 Minuten. Weitere Prüfungen können auf dem Reiter Monitoring/Prüfungen hinzugefügt werden.

Konfiguration (Reiter „Monitoring/Prüfungen“, Schaltfläche „Prüfung hinzufügen“)

Der **Name** ist ein Name, der die Prüfung so eindeutig beschreibt, dass sie von anderen Prüfungen unterschieden werden kann. Der vorgeschlagene Name setzt sich aus dem Typ der Prüfung und dem angegebenen Host zusammen.

Das Feld **Beschreibung** kann für eine detaillierte Beschreibung der Prüfung verwendet werden. Der Inhalt dieses Felds wird auch im Fehlerbericht mit übermittelt. Es kann somit zum Übermitteln weiterer Informationen im Fehlerbericht verwendet werden.

Der **Host**, für den die Prüfung erfolgen soll, wird aus der entsprechenden Dropdown-Liste ausgewählt. Hier sind alle bereits angelegten Hosts aufgelistet. Wenn die Prüfung für einen Host erfolgen soll, der noch nicht angelegt wurde, kann dieser über die Schaltfläche „neuen Host hinzufügen“ angelegt werden.

Der **Typ** der Prüfung wird aus der entsprechenden Dropdown-Liste ausgewählt. Dabei stehen folgende Typen zur Verfügung:

HTTP: Dabei erfolgt eine HTTP-Anfrage an den Web-Server des angegebenen Hosts. Antwortet der Web-Server mit OK gilt die Prüfung als erfolgreich.

HTTPS: Dabei erfolgt eine HTTPS-Anfrage an den Web-Server des angegebenen Hosts. Antwortet der Web-Server mit OK gilt die Prüfung als erfolgreich.

PING: Dabei erfolgt eine Ping-Anfrage an den angegebenen Host. Die Prüfung gilt als erfolgreich, wenn der Host 3 von 5 Ping-Anfragen innerhalb von 5 Sekunden positiv beantwortet.

VPN: Hier wird der OpenVPN Client-Status im VPN-Server verwendet. Ist er noch angemeldet, gilt die Prüfung als erfolgreich.

Das **Überprüfungs-Intervall** gibt an, in welchen Zeitabständen die Prüfung erfolgt.

Das **Wiederholungs-Intervall** gibt an, in welchen Zeitabständen die Prüfung erfolgt, nachdem eine Prüfung fehlgeschlagen ist. Dieses Intervall ist in der Regel kürzer als das Überprüfungs-Intervall.

Die Angabe der **max. Überprüfungs-Versuche** gibt an, nach wie vielen Prüfungen wieder das normale Überprüfungs-Intervall verwendet wird.

An die unter **Alarm-E-Mail** angegebene Adresse werden die Fehlerberichte der Prüfungen gesendet. Mehrere Empfänger-Adressen können durch Komma oder Leerzeichen getrennt eingegeben werden. Wird keine Adresse eingegeben, wird kein Fehlerbericht versendet.

Der **Http(s)-Port** gibt den Port an, über den HTTP(S)-Anfragen an den Web-Server des Hosts eingehen (nur für Typ HTTP(S)).

Der **Http(s)-Benutzername** wird bei HTTP(S)-Anfragen an den Web-Server verwendet, falls dieser eine Authentifizierung erfordert (nur für Typ HTTP(S)).

Das **Http(s)-Passwort** wird bei HTTP(S)-Anfragen an den Web-Server verwendet, falls dieser eine Authentifizierung erfordert (nur für Typ HTTP(S)).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

4.3.2 Verwalten der Prüfungen

Der Reiter „Monitoring/Prüfungen“ zeigt eine Liste der angelegten Prüfungen. Hier können die Prüfungen verwaltet werden. Außerdem wird hier der Status der Prüfungen angezeigt. Die Prüfungen werden nach Hosts gruppiert aufgeführt. Die Prüfungen unter den jeweiligen Hosts können mit der Schaltfläche „+“ bzw. „–“ vor dem Namen des Hosts aus- bzw. eingeklappt werden. Wenn die Checkbox „Gruppen ohne Störung einklappen“ markiert ist, sind nur die Gruppen ausgeklappt, die Störungen aufweisen.

Konfiguration (Reiter „Monitoring/Prüfungen“)

Mit der Schaltfläche **Prüfung hinzufügen** kann eine weitere Prüfung hinzugefügt werden.

Mit der Schaltfläche **Kopieren** kann eine weitere Prüfung hinzugefügt werden, wobei die Parameter des Fensters bereits mit denen der kopierten Prüfung vorbelegt werden. Die Anpassung dieser Parameter ermöglicht ein schnelles Anlegen ähnlicher Prüfungen.

Mit der Schaltfläche **Löschen** kann diese Prüfung gelöscht werden.

Mit der Schaltfläche **Verwalten** können die Einstellungen dieser Prüfung bearbeitet werden.

In der Spalte **Name** wird der Name dieser Prüfung angezeigt.

In der Spalte **Status** wird der letzte Zustand dieser Prüfung angezeigt. Folgende Zustände sind möglich:

OK: Die letzte Prüfung war erfolgreich.

warning: Die letzte Prüfung war erfolgreich, aber die Anfragen wurden nur verzögert (Paketumlaufzeit ≥ 2500 ms) oder nicht vollständig beantwortet.
unstable: Es wurden häufige Zustandsänderungen festgestellt, wenn die Erkennung von Stabilitätsproblemen aktiviert ist (siehe Konfigurieren der Prüfungs-Optionen auf Seite 32).

pending: Bislang wurde noch keine Prüfung durchgeführt.

error: Die letzte Prüfung war nicht erfolgreich.

In der Spalte **seit** wird angezeigt, seit wann sich die Prüfung in diesem Status befindet.

In der Spalte **Typ** wird der konfigurierte Typ dieser Prüfung angezeigt.

In der Spalte **Intervall** wird das konfigurierte Überprüfungs-Intervall dieser Prüfung angezeigt.

In der Spalte **E-Mail** wird die E-Mail-Adresse angezeigt, an welche die Fehlerberichte dieser Prüfung gesendet werden.

4.3.3 Anlegen eines Hosts

Zum Anlegen einer Prüfung muss ein Host angelegt sein. Dies kann beim Anlegen einer Prüfung oder separat auf dem Reiter Monitoring/Hosts erfolgen. Beim Anlegen eines Hosts wird automatisch eine Ping-Prüfung mit einem Intervall von 60 Minuten für diesen Host angelegt. Wird ein Host angelegt, der nicht VPN-Client ist, wird der zugehörige VPN-Client als Host mit angelegt, falls er noch nicht angelegt ist.

Konfiguration (Reiter „Monitoring/Hosts“, Schaltfläche „Host hinzufügen“)

Der **Name** ist ein Name, der den Host so eindeutig beschreibt, dass er von anderen Hosts unterschieden werden kann.

Die **erreichbare IP-Adresse** ist die IP-Adresse unter der das Gerät im VPN-Netzwerk zu erreichen ist, das als Host angelegt werden soll. Die erreichbare IP-Adresse eines Geräts kann auch der entsprechenden Spalte auf dem Reiter Geräte entnommen werden. Wurde für ein Gerät keine erreichbare IP-Adresse hinterlegt, kann auch die feste VPN-IP-Adresse verwendet werden. Diese wird angezeigt, wenn Sie auf dem Reiter Geräte die Schaltfläche „Mehr Info“ des jeweiligen Geräts anwählen.

4.3.4 Verwalten der Hosts

Der Reiter „Monitoring/Hosts“ zeigt eine Liste der angelegten Hosts. Hier können die Hosts verwaltet werden. Außerdem wird hier der Status der Hosts angezeigt. Die Hosts werden nach Geräten gruppiert aufgeführt. Die Hosts unter den jeweiligen Geräten können mit der Schaltfläche „+“ bzw. „–“ vor dem Namen des Geräts aus- bzw. eingeklappt werden. Dabei beginnt die Gruppe mit dem VPN-Host gefolgt von den weiteren Hosts im lokalen Netz des VPN-Clients. Die Netzwerkstruktur wird durch die Einrückung visualisiert. Wenn die Checkbox „Gruppen ohne Störung einklappen“ markiert ist, sind nur die Gruppen ausgeklappt, die Störungen aufweisen.

Konfiguration (Reiter „Monitoring/Hosts“)

Mit der Schaltfläche **Host hinzufügen** kann ein weiterer Host hinzugefügt werden.

Mit der Schaltfläche **Kopieren** kann ein weiterer Host hinzugefügt werden, wobei die Parameter des Fensters bereits mit denen des kopierten Hosts vorbelegt werden. Die Anpassung dieser Parameter ermöglicht ein schnelles Anlegen ähnlicher Hosts.

Mit der Schaltfläche **Löschen** kann dieser Host gelöscht werden.

Mit der Schaltfläche **Verwalten** können die Einstellungen dieses Hosts bearbeitet werden.

In der Spalte **Name** wird der Name dieses Hosts angezeigt.

In der Spalte **erreichbare IP** wird die IP-Adresse angezeigt, unter der dieser Host erreichbar ist.

In der Spalte **Status** wird der letzte Zustand dieses Hosts angezeigt. Folgende Zustände sind möglich:

- up: Die letzte Prüfung dieses Hosts war erfolgreich.
- warning: Die letzte Prüfung dieses Hosts war erfolgreich, aber die Anfragen wurden nur verzögert (Paketumlaufzeit ≥ 2500 ms) oder nicht vollständig beantwortet.
  unstable: Es wurden häufige Zustandsänderungen festgestellt, wenn die Erkennung von Stabilitätsproblemen aktiviert ist (siehe Konfigurieren der Prüfungs-Optionen auf Seite 32).
- unknown: Der Host ist unbekannt.
  unreachable: Der Host konnte nicht erreicht werden.
- down: Die letzte Prüfung dieses Hosts war nicht erfolgreich.

In der Spalte **seit** wird angezeigt, seit wann sich der Host in diesem Status befindet.

4.3.5 Konfigurieren der Prüfungs-Optionen

Der Reiter „Optionen“ verfügt über eine Reihe von Einstellungen für die Darstellung und Benachrichtigung im Zusammenhamg mit den Prüfungen.

Konfiguration (Reiter „Monitoring/Optionen“)

Wenn die Option **Gruppen ohne Störungen einklappen** aktiviert ist, werden nur die Gruppen mit Fehlern auf den Reitern „Prüfungen“ und „Hosts“ angezeigt. Die Gruppen können jederzeit manuell über das Symbol „+“ vor dem Gerätenamen aufgeklappt werden.

Unter **Benachrichtigungen bei Instanzneustart unterdrücken** wird festgelegt, wie lange die Überwachung bei einem Neustart ausgesetzt wird. Damit kann der Versand der E-Mails bei Verlust und Wiederherstellung der Verbindung nach einem Neustart vermieden werden.

Wenn die Option **Instabile VPN-Verbindungen erkennen und melden** aktiviert ist, wird zusätzlich zur Prüfung des Verbindungszustands die Stabilität der Verbindung ermittelt. Eine Verbindung wird dann als „instabil“ eingestuft, wenn mehr als 4 Zustandsänderungen bei den letzten 21 Prüfungen aufgetreten sind. Die Verbindung wird wieder als „stabil“ eingestuft, wenn maximal eine Zustandsänderung bei den letzten 21 Prüfungen auftritt. Als Zustandsänderung gilt, wenn die Geräteverbindung von „verbunden“ auf „getrennt“ wechselt oder die Verbindungsqualität zu schlecht wird (Paketumlaufzeit ≥ 2500 ms) und umgekehrt.

Wenn die Option **Benachrichtigungen bei Stabilitätsproblemen** aktiviert ist, werden Benachrichtigungen auch dann versendet, wenn die Verbindung als „instabil“ erkannt wird.

Wenn die Option **Monitoring-Benachrichtigungen deaktivieren** aktiviert ist, werden keine Benachrichtigungen im Zusammenhamg mit den Prüfungen versendet. Eine vorübergehende Deaktivierung der Benachrichtigungen kann hilfreich sein, um bei umfangreichen Konfigurationsänderungen den wiederholten Versand von Benachrichtigungen zu verhindern.

4.4 Lizenzen

Die Benutzung der icom Connectivity Suite – VPN ist an den Kauf von Lizenzen gekoppelt. Direkt nach der Registrierung stehen für 30 Tage vier Flex-Lizenzen kostenlos für Testzwecke zur Verfügung. Nach Ablauf dieser 30 Tage stehen noch zwei Flex-Lizenzen unbegrenzt zur Verfügung. Wenden Sie sich zur Umwandlung einer Teststellung in einen Vertrag an Ihren vertrieblichen Ansprechpartner.

Je nach Art des Accounts stehen unterschiedliche Lizenzen zur Verfügung. Die Art des Accounts wird im Reiter „Mein VPN“ hinter der Instanznummer angezeigt. In dieser Übersicht befinden sich auch die derzeit verwendeten Lizenzen. Detaillierte Informationen dazu finden Sie in der aktuellen Preisliste, die über den Reiter „Lizenzen“ und die Schaltfläche „Lizenzen bestellen“ verfügbar ist.

Derzeit existieren folgende Account-Typen:

- Premium-Account: Jeder neu registrierte Account ist immer ein Premium-Account. Ein Premium-Account verfügt über sämtliche Funktionalitäten.
- Default-Account: Jeder Default-Account kann in einen Premium-Account umgewandelt werden. Wenden Sie sich dazu an Ihren vertrieblichen Ansprechpartner. Ein Default-Account verfügt über eingeschränkte Funktionalitäten (wie keine Funktion zum Ersetzen von Geräten oder Benutzer-Management).

Folgende Lizenzmodelle stehen derzeit zur Verfügung:

- Flex-Lizenzen: Diese Lizenzen werden nachträglich abgerechnet (post-paid mit Stichtag 15. jedes Monats), haben eine unbegrenzte Laufzeit und können monatlich gekündigt werden.
- Service-Lizenzen: Diese Lizenzen werden im Voraus abgerechnet (pre-paid) und haben eine Laufzeit von ein oder zwei Jahren (bis zum Ablauf des 12. oder 24. Monats). Die Lizenzen werden nicht automatisch verlängert. Der Benutzer wird sechs Wochen vor Ablauf einer Lizenz per E-Mail benachrichtigt. Die ehemaligen Lizenzmodelle ‘Classic’ und ‘Unbegrenzt’ fallen unter Service-Lizenzen.

4.4.1 Bestellen einer Lizenz

Im kostenlosen Testbetrieb stehen vier zeitlich begrenzte Lizenzen zur Verfügung. Weitere Lizenzen können auf dem Reiter Lizenzen bestellt werden.

Konfiguration (Reiter „Lizenzen“, Schaltfläche „Lizenzen bestellen“)

Oben im Fenster ist noch einmal der Status aller Lizenzen aufgeführt. Außerdem kann die aktuell gültige Preisliste aufgerufen werden. Für eine Bestellung müssen auch die **AGB** hier akzeptiert werden.

Die Anzahl der **Lizenzen** gibt an, wie viele Lizenzen des jeweiligen Lizenzmodells Sie mit dieser Bestellung bestellen möchten. Für Service-Lizenzen kann die Laufzeit angegeben werden.

In das Feld **Bestell-Referenznummer** sollte die INSYS Bestell-Referenznummer eingetragen werden. Diese Angabe erleichtert die Bearbeitung und kann Verzögerungen dabei verhindern.

ⓘ Kunden, die den Dienst bereits über einen sogenannten CS-Vertrag gebucht haben, müssen hier die Vertragsnummer angeben (z.B. "CS-10002345").

Die **Firmendaten** des Kunden werden von den in der icom Connectivity Suite – VPN hinterlegten Daten übernommen und können nicht bearbeitet werden. Umsatzsteuer-ID und Kundennummer sind noch anzugeben.

Der **Ansprechpartner** wird von den in der icom Connectivity Suite – VPN hinterlegten Daten übernommen und kann noch bearbeitet werden.

Der **Kundenname** für die Eingabe in den Schnellstart-Assistenten von INSYS-Routern wird hier noch einmal angegeben, kann aber nicht bearbeitet werden.

Lösen Sie die Bestellung aus, indem Sie auf „Bestellen“ klicken.

✓ An die in Ihrem Account hinterlegte E-Mail-Adresse wird eine E-Mail mit einer Bestätigung der Bestellung gesendet.

4.4.2 Verwalten der Lizenzen

Der Reiter „Lizenzen“ zeigt eine Liste der vorhandenen Lizenzen. Hier können die Lizenzen verwaltet werden. Außerdem wird hier der Umfang und die Gültigkeitsdauer der Lizenzen angezeigt sowie das Gerät, dem sie zugeordnet sind.

Konfiguration (Reiter „Lizenzen“)

Mit der Schaltfläche **Lizenzen bestellen** können weitere Lizenzen bestellt werden.

Mit der Schaltfläche **Verwalten** kann die Lizenz einem anderen Gerät zugewiesen oder freigegeben werden. Bei Flex-Lizenzen kann eine Lizenz zum Ende des laufenden Monats gekündigt werden. Bei Service-Lizenzen kann eine Lizenz zum Ende der Gültigkeit als Flex-Lizenz fortgesetzt werden.

Mit der Schaltfläche **Mehr Info** kann ein Lizenz-Protokoll für diese Lizenz angezeigt werden. Das Protokoll enthält alle Ereignisse im Zusammenhang mit dieser Lizenz.

In der Spalte **Name** wird der Name dieser Lizenz angezeigt. Der von der icom Connectivity Suite – VPN zugewiesene Name kann hier auch bearbeitet werden.

In der Spalte **Umfang** wird der Umfang dieser Lizenz angezeigt.

In der Spalte **Gültig bis** wird angezeigt, wie lange diese Lizenz noch gültig ist.

In der Spalte **Gerät** wird angezeigt, welchem Gerät diese Lizenz zugeordnet ist.

In der Spalte **Erneuerung** wird angezeigt, um wie viele Jahre diese Lizenz nach Ablauf erneuert wird.

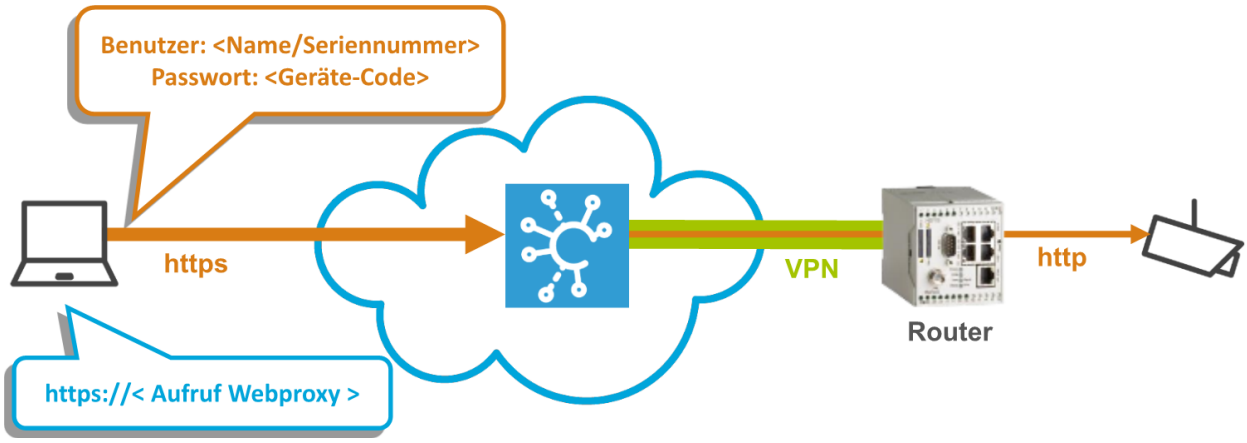
In der Spalte **Beleg** wird angezeigt, mit welcher Bestellung diese Lizenz bestellt wurde.

In der Spalte **Kostenlos** wird angezeigt, ob diese Lizenz kostenlos zur Verfügung gestellt wurde.

Bei jeder Änderung wird eine E-Mail an die in Ihrem Account hinterlegte E-Mail-Adresse gesendet.

4.5 Web-Proxies

Die icom Connectivity Suite – VPN ermöglicht das Einrichten von Web-Proxies. Web-Proxies vermitteln den Zugriff auf einen Web-Dienst, der im VPN erreichbar ist, über das HTTP- oder HTTPS-Protokoll. Damit kann von nahezu jedem PC oder Smartphone mit Internet-Zugang aus auf viele HTTP(S)-fähige Geräte (z.B. IP-Kameras) zugegriffen werden. Die Übertragung der Daten erfolgt verschlüsselt über HTTPS. Auf das Gerät kann über die in der Spalte „Aufruf Webproxy“ angezeigte Adresse zugegriffen werden. Die Authentifizierung erfolgt über eine Kombination aus Benutzernamen und Passwort. Der Benutzername ist entweder der Name des Web-Proxies oder die Seriennummer des INSYS-Routers, an den das Gerät angeschlossen ist, auf das zugegriffen werden soll. Das Passwort ist der Geräte-Code des INSYS-Routers. Wenn kein Geräte-Code konfiguriert ist, gilt der Standard-Code (konfigurierbar im Reiter „Mein VPN“).



Die Authentifizierung per Passwort kann optional deaktiviert werden. Dies ist beispielsweise erforderlich, wenn eine Kamera eine HTTP-Authentifizierung verlangt, da eine zweistufige Authentifizierung in einer Browser-Session nicht möglich ist.

Es ist auch möglich, eine dauerhafte Verbindung für eine Vollduplex-Kommunikation über einen WebSocket unter Verwendung des angegebenen Ports aufzubauen.

Hinweis

Sicherheitsgefahr!

Bei Verwendung eines Web-Proxy ist die betreffende Anwendung über das Internet erreichbar.

Die verschlüsselte Verbindung ist nur noch durch ein Passwort gegen Zugriffe aus dem Internet geschützt. Dies ist entweder der Geräte-Code des INSYS-Routers oder bei Deaktivierung des Passworts im Web-Proxy das Passwort Ihrer Anwendung. Befolgen Sie die Regeln für sichere Passwörter. Wir empfehlen diese Funktion nicht für sicherheitskritische Anwendungen.

4.5.1 Einrichten eines Web-Proxies

Gehen Sie wie folgt vor, um einen Web-Proxy hinzuzufügen.

Konfiguration (Reiter „Webproxies“, Schaltfläche „Webproxy hinzufügen“)

Das **Gerät** für das der Web-Proxy eingerichtet wird, kann aus allen an der icom Connectivity Suite – VPN angemeldeten INSYS-Routern ausgewählt werden.

Der **Name** ist ein Name, der den Web-Proxy so eindeutig beschreibt, dass er von anderen Web-Proxies unterschieden werden kann.

Die **IP-Adresse im VPN** ist die IP-Adresse, unter der das Gerät im VPN erreicht wird.

Ist die Checkbox **Das Ziel benutzt das HTTPS-Protokoll** markiert, unterstützt der Web-Proxy TLS-fähige Verbindungen zwischen dem VPN-Dienst und dem Edge-Gerät bzw. der Anwendung, falls unterstützt.

Der **Port** ist der Port, über den auf das Gerät zugegriffen werden kann.

Ist die Checkbox **Keine Authentifizierung durch Webproxy** markiert, erfolgt der Zugriff auf das Gerät ohne Passwort.

ⓘ Bei seit längerem bestehenden Accounts ist diese Option aus Sicherheitsgründen gesperrt. Kontaktieren Sie bitte unseren Support, um diese Option für Ihren Account freizuschalten.

Folgende **Erweiterte Einstellungen** sind für spezielle Anwendungsfälle verfügbar. Wir empfehlen, die Standardeinstellungen zu verwenden, wenn Sie sich nicht über die Auswirkungen von Änderungen im Klaren sind:

Ist die Checkbox **Zusätzliche eigenständige Authentifizierung auf Zielgerät (nur "Form-based-Auth")** markiert, kann zusätzlich zur Authentifizierung durch den Web-Proxy eine „Form-based authentication“ auf dem Zielgerät erfolgen.

Ist die Checkbox **Proxy WebSocket-Protokoll** aktiviert, wird eine WebSocket-Verbindung (ws: oder wss:) zwischen dem VPN-Dienst und der Anwendung ermöglicht. Wir empfehlen zum Beispiel, eine WebSocket-Verbindung zu erlauben, wenn ein Web-Proxy für den Zugriff auf INSYS-Router mit icom OS 5.5 oder höher verwendet wird.

Unter **Protokollversion auswählen** kann das HTTP-Protokoll für den Web-Proxy festgelegt werden. Für neue Web-Proxies wird HTTP/1.1 empfohlen. Bei Bedarf kann HTTP/1.0 verwendet werden, um die Kommunikation mit älteren Web-Proxies zu unterstützen.

Ist die Checkbox **CORS aktiviert** aktiviert, wird Cross-Origin Resource Sharing erlaubt, d.h. der Client darf auch Script-Anfragen an einen Server einer abweichenden Domain stellen, was normalerweise durch die Same-Origin-Policy (SOP) untersagt ist.

Ist die Checkbox **Accept-Encoding: ohne Komprimierung** aktiviert, erfolgt keine weitere Komprimierung der übertragenen Inhalte.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Hinweis

Sicherheitsgefahr!

Nach Deaktivierung der Authentifizierung ist die betreffende Anwendung ohne Schutz durch die icom Connectivity Suite – VPN über das Internet erreichbar.

Eine Sicherheit kann nur noch durch die Applikation selbst hergestellt werden. Die regelmäßige Prüfung der Applikation auf Sicherheitslücken ist daher unbedingt erforderlich. Wir empfehlen diese Funktion nicht für sicherheitskritische Anwendungen.

4.5.2 Verwalten der Web-Proxies

Der Reiter „Webproxies“ zeigt eine Liste der vorhandenen Web-Proxies. Hier können die Web-Proxies verwaltet werden. Außerdem wird hier der Umfang und die Gültigkeitsdauer der Lizenzen angezeigt sowie das Gerät, dem sie zugeordnet sind.

Konfiguration (Reiter „Webproxies“)

Mit der Schaltfläche **Webproxy hinzufügen** kann ein weiterer Web-Proxy hinzugefügt werden.

Mit der Schaltfläche **Kopieren** kann ein weiterer Web-Proxy hinzugefügt werden, wobei die Parameter des Fensters bereits mit denen des kopierten Web-Proxies vorbelegt werden. Die Anpassung dieser Parameter ermöglicht ein schnelles Anlegen ähnlicher Web-Proxies.

Mit der Schaltfläche **Löschen** kann dieser Web-Proxy gelöscht werden.

Mit der Schaltfläche **Verwalten** können die Einstellungen dieses Web-Proxies bearbeitet werden.

In der Spalte **Name** wird der Name dieses Web-Proxies angezeigt.

In der Spalte **Aufruf Webproxy** wird die Adresse angezeigt, mit der ohne einen VPN-Zugang auf die Anwendung hinter dem Gerät zugegriffen werden kann.

In der Spalte **IP im VPN** wird die IP-Adresse angezeigt, unter der das Gerät im VPN erreicht wird.

In der Spalte **Port** wird der Port angezeigt, über den auf das Gerät zugegriffen werden kann.

In der Spalte **Gerät** wird das Gerät im VPN angezeigt, über das auf die Anwendung zugegriffen werden kann.

In der letzten Spalte erscheint ein offenes Schloss, wenn dieser Web-Proxy für einen Zugriff ohne Passwort konfiguriert ist.

4.6 Mein VPN

Der Reiter „Mein VPN“ zeigt wichtige Informationen zu diesem Account an. Diese Daten können beispielsweise auch für die manuelle Konfiguration von Fremdgeräten wichtig sein.

Die Instanznummer ist eine eindeutige Nummer zur Identifizierung eines Accounts. Hinter der Instanznummer ist der Account-Typ angegeben, der den Leistungsumfang dieses Accounts festlegt.

Der Kundenname ist für den Schnellstart-Assistenten von INSYS-Routern erforderlich.

Der Standard-Code wird immer dann als Geräte-Code verwendet, wenn für ein Gerät kein eigener Geräte-Code angegeben wird. Der Geräte-Code ist für den Schnellstart-Assistenten von INSYS-Routern und den Zugang über einen Web-Proxy erforderlich.

Die Angaben für VPN-Server, VPN-Port und VPN-Bereich sind für die manuelle VPN-Konfiguration von Fremdgeräten (PCs) wichtig. Der VPN-Port gibt an, auf welchem UDP-Port die icom Connectivity Suite – VPN OpenVPN-Tunnel entgegennimmt. Der Benutzer muss gewährleisten, dass ausgehender UDP-Verkehr für den Router auf diesem Port erlaubt ist und Antworten zugelassen werden (z.B. diesen Port in der Firewall öffnen).

Im Abschnitt Lizenzen finden Sie einen Überblick über die Anzahl und Art der verfügbaren Lizenzen und deren Verwendung.

Neben der Anzeige von Benutzername und Benutzerrolle des angemeldeten Benutzers wird angezeigt, ob die Zwei-Faktor-Authentifizierung auf Grund der Einstellung in der Benutzerverwaltung erforderlich ist (Reiter Benutzer) und wie der Status der Zwei-Faktor-Authentifitzierung für den aktuell angemeldeten Benutzer (Reiter Mein VPN) im Moment ist.

Weiterhin können hier der Standard-Code geändert, weitere Lizenzen bestellt (siehe Abschnitt Lizenzen), das VPN-Log heruntergeladen und die Zwei-Faktor-Authentifizierung für diesen Benutzer aktiviert, deaktiviert und erneuert werden.

4.6.1 Ändern des Standard-Codes

Gehen Sie wie folgt vor, um den Standard-Code zu ändern.

Konfiguration (Reiter „Mein VPN“, Schaltfläche „Standard-Code ändern“)

Der **Standard-Code** wird angezeigt und kann entsprechend geändert werden.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

4.6.2 VPN-Log herunterladen

Im VPN-Log werden alle Ereignisse des VPN-Servers aufgezeichnet.

Konfiguration (Reiter „Mein VPN“, Schaltfläche „VPN-Log“)

Mit der Dropdown-Liste **Tage** wird festgelegt, wie viele Tage das Log umfassen soll.

Laden Sie das Log herunter, indem Sie auf „OK“ klicken.

4.6.3 VPN-Instanz neu starten

Bei Bedarf kann die VPN-Instanz manuell neu gestartet werden.

Konfiguration (Reiter „Mein VPN“, Schaltfläche „VPN-Instanz neu starten“)

Starten Sie die VPN-Instanz neu, indem Sie auf „VPN-Instanz neu starten“ klicken.

4.6.4 Verbindungs-Log herunterladen

Das Verbindungs-Log ist nicht Teil des Standard-Funktionsumfangs und auf Anfrage verfügbar. Es zeichnet sämtliche TCP-Verbindungen im VPN-Netzwerk auf.

Konfiguration (Reiter „Mein VPN“, Schaltfläche „Verbindungs-Log“)

Laden Sie das Verbindungs-Log herunter, indem Sie auf die gewünschte Log-Datei klicken.

4.6.5 Bestellen von Lizenzen

Siehe den Abshnitt Bestellen einer Lizenz auf Seite 34.

4.6.6 Verwalten der Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung fügt der Anmeldung über Benutzername und Passwort ein weiteres Sicherheitsniveau hinzu, indem es die zusätzliche Eingabe eines Einmal-Passworts erfordert. Dass Passwort wird über das TOTP (Time-based One-time Password)-Verfahren mit Hilfe einer App auf einem separatem Gerät (z.B. Smartphone) erzeugt. Dazu muss der Benutzer-Account der icom Connectivity Suite einmalig in der App registriert werden. TOTP ist ein offener Standard und es sind eine Vielzahl von Apps für verscheidene Plattformen wie die Open Source-Software FreeOTP (https://freeotp.github.io/) verfügbar. Da die Einmal-Passwörter zeitbasiert erzeugt werden und nur eine begrenzte Zeit gültig sind, ist es erforderlich, dass die Uhrzeit auf dem separatem Gerät genau ist und regelmäßig synchronisiert wird.

ⓘ Wenn eine Zwei-Faktor-Authentifizierung in der Benutzerverwaltung (siehe Abschnitt Benutzer-Management ab Seite 49) erzwungen wird, kann sie der angemeldete Benutzer hier nicht deaktivieren. Sie kann hier nur aktiviert und deaktiviert werden, wenn sie nicht in der Benutzerverwaltung aktiviert ist.

Gehen Sie wie folgt vor, um die Zwei-Faktor-Authentifizierung für den angemeldeten Benutzer zu aktivieren.

Einrichten der Zwei-Faktor-Authentifizierung für den angemeldeten Benutzer

- ⇢ Sie haben sich an der icom Connectivity Suite angemeldet
- ⇢ Sie haben den Reiter „Mein VPN“ geöffnet

1. ***Klicken Sie auf die Schaltfläche „Zwei-Faktor-Authentifizierung für diesen Benutzer einrichten“.***
2. ***Scannen Sie den angezeigten QR-Code mit der TOTP-App.***
3. ***Erzeugen Sie in der App das Einmal-Passwort und geben Sie es in der icom Connectivity Suite ein.***
4. ***Klicken Sie auf „Einmal-Passwort konfigurieren“.***

✓ Damit haben Sie die Zwei-Faktor-Authentifizierung für diesen Benutzer eingerichtet und Sie werden bei jeder erneuten Anmeldung nach einem Einmal-Passwort gefragt.

Gehen Sie wie folgt vor, um die Zwei-Faktor-Authentifizierung für den angemeldeten Benutzer zu deaktivieren.

Deaktivierender Zwei-Faktor-Authentifizierung für den angemeldeten Benutzer

- ⇢ Sie haben sich an der icom Connectivity Suite angemeldet
- ⇢ Die Zwei-Faktor-Authentifizierung ist für den angemeldeten Benutzer aktiv
- ⇢ Sie haben den Reiter „Mein VPN“ geöffnet

1. ***Klicken Sie auf die Schaltfläche „Zwei-Faktor-Authentifizierung für diesen Benutzer deaktivieren“.***

✓ Damit haben Sie die Zwei-Faktor-Authentifizierung für diesen Benutzer wieder deaktiviert und werden bei der nächsten Anmeldung nicht mehr nach einem Einmal-Passwort gefragt.

ⓘ Wird eine Zwei-Faktor-Authentifizierung für einen Benutzer deaktiviert, sollte sie auch aus der App gelöscht werden. Wenn Sie wieder aktiviert wird, muss sie in der App neu eingerichtet werden.

Gehen Sie wie folgt vor, um die Zwei-Faktor-Authentifizierung für den angemeldeten Benutzer zu erneuern. Dies ist beispielsweise erforderlich, wenn Sie für die Zwei-Faktor-Authentifizierung ein anderes Mobiltelefon verwenden möchten, als das, mit dem die Zwei-Faktor-Authentifizierung ursprünglich eingerichtet wurde.

Erneuern der Zwei-Faktor-Authentifizierung für den angemeldeten Benutzer

- ⇢ Sie haben sich an der icom Connectivity Suite angemeldet
- ⇢ Die Zwei-Faktor-Authentifizierung ist für den angemeldeten Benutzer aktiv
- ⇢ Sie haben den Reiter „Mein VPN“ geöffnet

1. ***Klicken Sie auf die Schaltfläche „Zwei-Faktor-Authentifizierungskonfiguration erneuern“.***
2. ***Scannen Sie den angezeigten QR-Code mit der TOTP-App.***
3. ***Erzeugen Sie in der App das Einmal-Passwort und geben Sie es in der icom Connectivity Suite ein.***
4. ***Klicken Sie auf „Einmal-Passwort konfigurieren“.***

✓ Damit haben Sie die Zwei-Faktor-Authentifizierung für diesen Benutzer erneuert.

ⓘ Wird eine Zwei-Faktor-Authentifizierung für einen Benutzer erneuert, ist es nicht mehr möglich, mit der ursprünglich eingerichteten App einen gültigen Code zu erzeugen.

4.7 VPN-Teilnehmer

Die Konfiguration der VPN-Teilnehmer ist abhängig vom jeweiligen Gerät.

Router und Störmelder von INSYS icom können mit Hilfe ihres Schnellstart-Assistenten schnell und einfach für die icom Connectivity Suite – VPN konfiguriert werden. Alternativ ist es möglich, diese manuell zu konfigurieren. Dazu können eine Konfigurationsdatei und ein Container mit allen erforderlichen Zertifikaten und Schlüsseln von der icom Connectivity Suite – VPN heruntergeladen werden.

Drittgeräte wie PCs, Tablets oder Steuerungen werden manuell konfiguriert. Dazu können eine OpenVPN-Konfigurationsdatei und ein Container mit allen erforderlichen Zertifikaten und Schlüsseln von der icom Connectivity Suite – VPN heruntergeladen werden.

ⓘ Verschiedene Configuration Guides für die Konfiguration der VPN-Teilnehmer finden Sie unter https://docs.insys-icom.de/de_icom_connectivity_suite.html

4.7.1 Konfigurieren eines INSYS-Routers mit icom OS

Die Konfiguration eines INSYS-Routers mit icom OS kann entweder über den Schnellstart-Assistenten oder manuell erfolgen.

4.7.1.1 Schnellstart-Assistent

Der Schnellstart-Assistent im Web-Interface dient zur schnellen Inbetriebnahme des Routers für die icom Connectivity Suite – VPN.

Dabei holt sich der Router die gesamte VPN-Konfiguration von der icom Connectivity Suite – VPN. Dazu muss der Router vorher als Gerät in der icom Connectivity Suite – VPN angelegt worden sein.

Um einen Router mit dem Schnellstart Assistenten für die icom Connectivity Suite – VPN in Betrieb zunehmen, wird empfohlen, ihn zunächst auf die Grundeinstellungen zurückzusetzen. Hinweise dazu finden sich im Quick Installation Guide sowie in der Inline- und Online-Hilfe des Routers. Klicken Sie auf das Fragezeichen in der Kopfzeile, um die Inline-Hilfe einzublenden.

Kundenname und Geräte-Code, die hier erforderlich sind, finden Sie auf dem Reiter „Mein VPN“.

Der Schnellstart-Assistent konfiguriert den Router. Dieser stellt dann eine WAN-Verbindung her und baut eine sichere Verbindung zum Init-Server des VPN-Diensts auf (der Zugriff auf den Init-Server erfolgt über UDP-Port 1194). Dann holt sich der Router die VPN-Konfiguration vom Server und wendet sie an. Dabei wird das lokale Netz des Routers entsprechend den Angaben konfiguriert, die beim Anlegen des Geräts in der icom Connectivity Suite – VPN eingestellt wurden. Nach Abschluss des Schnellstart-Assistenten erscheint der Router mit etwas Verzögerung in der icom Connectivity Suite – VPN mit dem Status online.

4.7.1.2 Manuelle Konfiguration

Die manuelle Konfiguration bietet sich dann an, wenn ein Router bereits konfiguriert und in Betrieb genommen ist und zusätzlich am VPN-Service teilnehmen soll.

Die Konfigurationsdatei, die in der icom Connectivity Suite – VPN auf dem Reiter „Geräte“ beim jeweiligen Gerät über die Schaltfläche „Herunterladen“ (Pfeil nach unten) heruntergeladen werden kann (Link „INSYS Router Konfiguration“), enthält alle dazu erforderlichen Konfigurationseinstellungen. Diese können im Web-Interface des Routers im Menü „Administration“ auf der Seite „Profile“ in das geöffnete Profil geladen werden. Eine sichere Konfiguration für die icom Connectivity Suite – VPN ist damit allerdings noch nicht gewährleistet, da dies von den bereits erfolgten Einstellungen des Routers abhängt. Wurden beispielsweise schon mehr als eine WAN-Kette oder ein VPN-Tunnel definiert, kann dies zu Konflikten mit der Konfigurationsdatei führen. Dann ist eine weitere manuelle Nachbearbeitung der Konfiguration erforderlich. Hinweise dazu finden sich in der Inline- und Online-Hilfe des Routers. Klicken Sie auf das Fragezeichen in der Kopfzeile, um die Inline-Hilfe einzublenden.

4.7.2 Konfigurieren eines INSYS-Routers mit INSYS OS

Dieser Abschnitt gilt für Router mit INSYS OS. Auch hier kann die Konfiguration über den Schnellstart-Assistenten oder manuell erfolgen.

4.7.2.1 Schnellstart-Assistent

Der Schnellstart-Assistent im Web-Interface dient zur schnellen Inbetriebnahme des Routers oder Störmelders für die icom Connectivity Suite – VPN. Der Router muss dazu über eine Firmware ab 2.8.0 verfügen.

Dabei holt sich der Router die gesamte VPN-Konfiguration von der icom Connectivity Suite – VPN. Dazu muss der Router vorher als Gerät in der icom Connectivity Suite – VPN angelegt worden sein.

Um einen Router mit dem Schnellstart Assistenten für die icom Connectivity Suite – VPN in Betrieb zunehmen, muss sich dieser zuerst auf die Grundeinstellungen zurückgesetzt werden. Hinweise dazu finden sich im Quick Installation Guide und im Benutzerhandbuch des Routers. Der Schnellstart-Assistent wird nur beim ersten Start des Routers im Web-Interface angezeigt.

Kundenname und Geräte-Code, die hier erforderlich sind, finden Sie auf dem Reiter „Mein VPN“.

Der Schnellstart-Assistent konfiguriert den Router. Dieser stellt dann eine WAN-Verbindung her und baut eine sichere Verbindung zum Init-Server des VPN-Diensts auf (der Zugriff auf den Init-Server erfolgt über UDP-Port 1194). Dann holt sich der Router die VPN-Konfiguration vom Server und wendet sie an. Nach Abschluss des Schnellstart-Assistenten erscheint der Router mit etwas Verzögerung in der icom Connectivity Suite – VPN mit dem Status online.

ⓘ Beachten Sie, dass der Router nach dem Neustart bereits über die neue IP-Adresse zu erreichen ist, falls eine solche beim Anlegen des Geräts in der icom Connectivity Suite – VPN unter „erreichbare lokale IP-Adresse“ eingetragen wurde.

4.7.2.2 Manuelle Konfiguration

Die manuelle Konfiguration bietet sich dann an, wenn ein Router bereits konfiguriert und in Betrieb genommen ist und zusätzlich am VPN-Service teilnehmen soll. Der Router muss dazu über eine Firmware ab 2.4.0 verfügen.

Die Konfigurationsdatei, die in der icom Connectivity Suite – VPN auf dem Reiter „Geräte“ beim jeweiligen Gerät über die Schaltfläche „Herunterladen“ (Pfeil nach unten) heruntergeladen werden kann, enthält alle dazu erforderlichen Konfigurationseinstellungen. Diese können im Web-Interface des Routers im Menü „System“ auf der Seite „Update“ auf den Router geladen werden. Eine sichere Konfiguration für die icom Connectivity Suite – VPN ist damit allerdings noch nicht sicher gewährleistet, da dies von den bereits erfolgten Einstellungen des Routers abhängt. Wurde er beispielsweise zuvor als VPN-Server konfiguriert, kann dies zu Konflikten mit der Konfigurationsdatei führen. Dann ist eine weitere manuelle Nachbearbeitung der Konfiguration erforderlich. Hinweise dazu finden sich im Benutzerhandbuch des Routers.

ⓘ Beachten Sie, dass der Router nach dem Neustart bereits über die neue IP-Adresse zu erreichen ist, falls eine solche beim Anlegen des Geräts in der icom Connectivity Suite – VPN unter „erreichbare lokale IP-Adresse“ eingetragen wurde.

4.7.3 Konfigurieren eines Fremdgeräts

Wenn Sie ein Fremdgerät (PC, Steuerung, etc.) in der icom Connectivity Suite – VPN angelegt haben, können Sie die Konfiguration für das VPN-Netzwerk aus der icom Connectivity Suite – VPN herunterladen. Auf dem Fremdgerät sollte nach Möglichkeit die letzte von INSYS verifizierte OpenVPN-Version installiert sein (https://www.insys-icom.com/de-de/support/technischer-support/).

Die Konfigurationsdatei, die in der icom Connectivity Suite – VPN auf dem Reiter „Geräte“ beim jeweiligen Gerät über die Schaltfläche „Herunterladen“ (Pfeil nach unten) heruntergeladen kann enthält die OpenVPN-Konfigurationseinstellungen.

Die OpenVPN-Konfigurationsdatei muss im Verzeichnis „Config“ der OpenVPN-Installation abgelegt werden (z.B. Windows: C:\Programme\OpenVPN\config). Hinweise zur Installation eines OpenVPN-Clients auf einem Windows PC sowie einem Android- oder iOS-Tablet finden Sie unter
https://docs.insys-icom.de/de_icom_connectivity_suite.html

Damit können Sie die OpenVPN GUI starten und sich mit dem VPN verbinden.

ⓘ Unter Windows und älteren OpenVPN-Versionen muss die GUI als Administrator gestartet werden, da ansonsten die Routen nicht gesetzt werden. Der PC erscheint zwar als „online“ in der icom Connectivity Suite – VPN, kann aber nicht kommunizieren.

Die VPN-Verbindung kann überprüft werden, indem Sie beispielsweise vom Fremdgerät aus die IP-Adresse eines VPN-Teilnehmers „anpingen“ oder in einen Browser eingeben (um beispielsweise auf sein Web-Interface zuzugreifen).

4.8 VPN-Aktivitäten

Die icom Connectivity Suite protokolliert verschiedene Aktivitäten im Portal, wie zum Beispiel das An- und Abmelden von Benutzern oder Hinzufügen und Löschen von Geräten.

Ein Klick auf den Reiter „Aktivitäten“ öffnet das neue Portal der icom Connectivity Suite. Dort werden im Menü „Aktivitäten“ sämtliche Vorgänge im Zusammenhang mit der icom Connectivity Suite - VPN und, falls verwendet, icom Connectivity Suite – M2M SIM angezeigt. Ein Klick auf das Fragezeichen in der Titelleiste des neuen Portals öffnet die zugehörige Hilfe.

5 SIM-Karten-Management

ⓘ Sobald Ihr Account auf das neue SIM-Karten-Portal umgestellt wurde, öffnet sich das neue Portal, wenn Sie auf den Link auf dem Reiter „M2M SIM“ klicken. Ein Klick auf das Fragezeichen in der Titelleiste des neuen Portals öffnet die zugehörige Hilfe.

Das Portal der icom Connectivity Suite dient ebenfalls zum Verwalten der industriellen Premium-SIM-Karten mit Multi-Roaming, Pooling und weiteren Funktionen.

Der Reiter „M2M SIM“ zeigt alle diesem Account zugeordneten M2M SIM-Karten an. Die Zuordnung erfolgt durch unsere Bereitstellung. Sollten Sie Ihre bereits von INSYS erworbenen SIM-Karten hier nicht sehen, wenden Sie sich für eine manuelle Zuordnung an unseren Support unter support@insys-icom.de.

Konfiguration (Reiter „M2M SIM“)

In der Spalte **Geräte** wird angezeigt, welchem in der icom Connectivity Suite – VPN angelegten Gerät diese SIM-Karte zugeordnet ist.

Mit der Schaltfläche **Verwalten** können die Einstellungen dieser SIM-Karte bearbeitet werden.
Hier kann die SIM-Karte einem **Gerät** in der icom Connectivity Suite – VPN zugeordnet werden.
Die **Gerätebeschreibung** kann verwendet werden, um das Gerät, dem die SIM-Karte zugeordnet ist, näher zu beschreiben.
Unter **SIM-Karten Status editieren** kann die SIM-Karte aktiviert und deaktiviert werden.
Unter **Kommunikationsplan** kann ausgewählt werden, wo diese SIM-Karte verwendet werden kann.
Unter **Tarifplan** kann das derzeit verwendete Inklusivvolumen für diese SIM-Karte geändert werden.
Mit dem **Änderungsdatum** wird angegeben, ab wann hier erfolgte Änderungen von Kommunikationsplan und Tarifplan wirksam werden.

ⓘ Änderungen von Kommunikationsplan und Tarifplan verändern Ihre monatlichen Kosten. Passen Sie das Abrechnungsmodell für jede SIM-Karte an die Anforderungen der Applikation, in der die SIM-Karte verwendet wird, an. Detaillierte Informationen dazu finden Sie in der aktuellen Preisliste, die über den Reiter „Lizenzen“ und die Schaltfläche „Lizenzen bestellen“ verfügbar ist.

ⓘ Wenn die Option "Smart Cost Control" gebucht wurde, darf der Kommunikations- oder Tarifplan nicht manuell geändert werden.

Mit der Schaltfläche **SIM-Karten-Informationen** können weitere Informationen zu dieser SIM-Karte wie Abrechnungszeitraum, zugeordnetes Gerät, das übertragene Daten- und SMS-Volumen oder die Überschreitung der Abrechnungsgrenze angezeigt werden.

Mit der Schaltfläche **SIM-Karte sperren** kann diese SIM-Karte dauerhaft gesperrt werden. Eine Reaktivierung ist danach nicht mehr möglich. Dies empfiehlt sich beispielsweise bei Verlust der SIM-Karte.

In der Spalte **in Session** wird der Einbuchungszustand dieser SIM-Karte mit einer Verzögerung von 1-2 Minuten angezeigt. Folgende Zustände sind möglich:

- Ja: Die SIM-Karte ist eingebucht.
- Nein: Die SIM-Karte ist nicht eingebucht.

In der Spalte **Rufnummer** wird die Telefonnummer dieser SIM-Karte angezeigt.

In der Spalte **ICCID** wird der Integrated Circuit Card Identifier, also die SIM-Karten-Nummer, dieser SIM-Karte angezeigt.

In der Spalte **S/N** wird die Seriennummer des Geräts angezeigt, dem diese SIM-Karte zugeordnet ist (nur für INSYS-Geräte).

In der Spalte **Tarifplan** wird der derzeit verwendete Tarifplan angezeigt.

In der Spalte **Akt. Verbrauch MB** wird die seit dem letzten Abrechnungszeitraum verbrauchte Menge an übertragenen Daten dieser SIM-Karte angezeigt.

In der Spalte **Akt. Verbrauch SMS** wird die seit dem letzten Abrechnungszeitraum verbrauchte Menge an SMS dieser SIM-Karte angezeigt.

In der Spalte **IMEI** wird der International Mobile Equipment Identity, also die Seriennummer des Mobilfunkgeräts in dem diese SIM-Karte eingesetzt ist, angezeigt. Je nach Provider können hier bis zu 16 Stellen angezeigt werden, wobei aber nur die ersten 14 Stellen relevant sind. Die 15. und eine mögliche 16. Stelle sind lediglich Prüfziffern, die auch oft nur maskiert als 0 oder 1 angezeigt werden.

In der Spalte **SIM-Status** wird angezeigt, ob diese SIM-Karte im Moment aktiviert oder deaktiviert (abgeschaltet) ist.

In der Spalte **seit** wird angezeigt, seit wann sich diese SIM-Karte in dem in der Spalte **SIM-Status** angezeigten Zustand befindet.

6 Benutzer-Management

Für das Portal der icom Connectivity Suite steht auch eine Benutzerverwaltung zur Verfügung.

Der Reiter „Benutzer“ zeigt alle diesem Account zugeordneten Benutzer an. Es können weitere Benutzer mit unterschiedlichen Rechten angelegt werden.

6.1.1 Anlegen eines Benutzers

Beim Anlegen eines Benutzers stehen verschiedene Benutzerrollen mit unterschiedlichen Rechten zur Verfügung:

- Account-Admin: Verfügt über sämtliche Rechte inklusive Benutzerverwaltung. Ein Account-Administrator kann als Ansprechpartner festgelegt werden. Er erhält dann die Systemmeldungen per E-Mail. Bereits bestehend Nutzer werden als Account-Administratoren eingestuft. Der Nutzer, auf den der Account registriert wurde, wird als Ansprechpartner übernommen.
- Nur lesend: Kann in den Menüs sämtliche Listen-Ansichten einsehen sowie die Geräteliste und VPN-Logdateien herunterladen, jedoch keine Einstellungen vornehmen oder Zertifikate bzw. Konfigurationen herunterladen.

Konfiguration (Reiter „Benutzer“, Schaltfläche „Benutzer hinzufügen“)

Mit der **Rolle** wählen Sie, welche Rechte der neu angelegte Benutzer erhalten soll.

Die **Anrede** legt fest, ob der Benutzer in automatisch erzeugten E-Mails als Herr oder Frau angesprochen wird.

Name und **Vorname** dienen ebenso einer Ansprache in der Korrespondenz.

Mit **E-Mail** wird die für die Korrespondenz mit dem Benutzer verwendete E-Mail-Adresse festgelegt.

Mit dem **Benutzernamen** und dem **Passwort** kann sich der neu angelegte Benutzer an der icom Connectivity Suite anmelden. Es wird empfohlen, dass ein neuer Benutzer sein Passwort nach der ersten Anmeldung auf ein nur ihm bekanntes Passwort ändert.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

6.1.2 Verwalten der Benutzer

Der Reiter „Benutzer“ zeigt eine Liste der angelegten Benutzer. Hier können die Benutzer verwaltet und angepasst werden.

Konfiguration (Reiter „Geräte“)

Mit der Schaltfläche **Benutzer hinzufügen** kann ein weiterer Benutzer hinzugefügt werden.

Mit der Schaltfläche **Kundenliste herunterladen** kann eine Liste der angelegten Benutzer heruntergeladen werden.

Mit der Schaltfläche **Verwalten** können die Daten dieses Benutzers bearbeitet werden.
Hier kann auch die Zwei-Faktor-Authentifizierung für diesen Benutzer erzwungen werden.

Mit der Schaltfläche **Löschen** kann dieser Benutzer gelöscht werden.

In der Spalte **Ansprechpartner** kann der Ansprechpartner für diesen Account festgelegt werden. Benutzer, die lediglich Leserechte haben, können nicht als Ansprechpartner festgelegt werden. Benutzer, die als Ansprechpartner festgelegt sind, können nicht gelöscht werden.

In der Spalte **Rolle** wird die diesem Benutzer zugewiesene Benutzerrolle angezeigt.

In der Spalte **Anrede** wird die für diesen Benutzer konfigurierte Anrede angezeigt.

In der Spalte **Nachname** wird der für diesen Benutzer konfigurierte Nachname angezeigt.

In der Spalte **Vorname** wird der für diesen Benutzer konfigurierte Vorname angezeigt.

In der Spalte **Kontakt E-Mail** wird die für diesen Benutzer konfigurierte E-Mail-Adresse angezeigt. Die gesamte Korrespondenz mit diesem Benutzer erfolgt über diese Adresse.

In der Spalte **Benutzername** wird der für diesen Benutzer konfigurierte Benutzername angezeigt.

In der Spalte **Erstellt von** wird angezeigt, welcher Benutzer diesen Benutzer angelegt hat.

In der Spalte **Erstellt am** wird angezeigt, wann dieser Benutzer angelegt wurde.

In der Spalte **Letzte Passwortänderung** wird angezeigt, wann das Passwort dieses Benutzers zuletzt geändert wurde.

In der Spalte **2FA erforderlich** wird angezeigt, ob für diesen Benutzer die Zwei-Faktor-Authentifizierung erzwungen ist.

6.1.3 Erzwingen der Zwei-Faktor-Authentifizierung für einen Benutzer

Die Zwei-Faktor-Authentifizierung fügt der Anmeldung über Benutzername und Passwort ein weiteres Sicherheitsniveau hinzu, indem es die zusätzliche Eingabe eines Einmal-Passworts erfordert. Dass Passwort wird über das TOTP (Time-based One-time Password)-Verfahren mit Hilfe einer App auf einem separatem Gerät (z.B. Smartphone) erzeugt. Dazu muss der Benutzer-Account der icom Connectivity Suite einmalig in der App registriert werden. TOTP ist ein offener Standard und es sind eine Vielzahl von Apps für verscheidene Plattformen wie die Open Source-Software FreeOTP (https://freeotp.github.io/) verfügbar. Da die Einmal- Passwörter zeitbasiert erzeugt werden und nur eine begrenzte Zeit gültig sind, ist es erforderlich, dass die Uhrzeit auf dem separatem Gerät genau ist und regelmäßig synchronisiert wird.

Ein Benutzer mit Administrator-Rechten kann die Zwei-Faktor-Authentifizierung für jeden eingerichteten Benutzer erzwingen. Diese Einstellung hat Vorrang gegenüber der Einrichtung einer Zwei-Faktor-Authentifizierung eines angmeldeten Benutzers auf dem Reiter "Mein VPN" (siehe Verwalten der Zwei-Faktor-Authentifizierung auf Seite 40).

Konfiguration (Reiter „Benutzer", Schaltfläche „Verwalten")

Mit dem Aktivieren von **Zwei-Faktor-Authentifizierung wird benötigt** wird die Zwei-Faktor-Authentifizierung für diesen Benutzer erzwungen.

Bei der nächsten Anmeldung dieses Benutzers wird ein QR-Code angezeigt, den der Benutzer mit der TOTP-App scannen muss, um diese für die Zwei-Faktor-Authentifizierung einzurichten.

6.1.4 Herunterladen der Benutzerliste

Der Reiter „Benutzer" zeigt eine Liste der angelegten Benutzer. Diese Liste kann als CSV-Datei heruntergeladen werden. Die CSV-Datei enthält die Spalten analog zur Benutzerliste getrennt durch ein „=" (Gleichheitszeichen).

Konfiguration (Reiter „Benutzer", Schaltfläche „Kundenliste herunterladen")

Mit einem Klick auf **Kundenliste herunterladen** wird im Download-Fenster die Benutzerliste heruntergeladen.