IP Interkoms

Konfigurationshandbuch

2N TELEKOMUNIKACE a.s.
Modřanská 621 | Prague 4 | 143 01

2N.com

Inhaltsverzeichnis

Verwendete Ports

Service	Port	Protokoll	Richtung	Standardmäßig eingeschaltet	Einstellbar	Einstellungen
802.1x	–	–	In/Out	×	×	–
DHCP	68	UDP	In/Out	✓	×	–
DNS	53	TCP/UDP	In/Out	✓	×	–
Echo (device discovery)*	8002	UDP	In/Out	✓	×	–
FTP	21	TCP	Out	×	×	–
2N IP Eye	8003	UDP	Out	×	×	–
HTTP	80	TCP	In/Out	✓	✓	**System > Netzwerkverbindung > Registerkarte WEB-SERVER**
HTTPS	443	TCP	In/Out	✓	✓	**System > Netzwerkverbindung > Registerkarte WEB-SERVER**
Multicast audio	22222	UDP	Out	×	✓	**Integration > Audio**
Multicast-Audio für ICU-Protokoll	8006	UDP	Out	×	×	–

Service	Port	Protokoll	Richtung	Standardmäßig eingeschaltet	Einstellbar	Einstellungen
Multicast-Video für ICU-Protokoll	8008	UDP	Out	×	×	–
Multicast Video (wide) für ICU Protokoll	8016	UDP	In/Out	×	×	–
NTP-Klient	123	UDP	In/Out	✓	×	–
ONVIF	80, 443, 3702	TCP/UDP	In/Out	×	×	–
RTP+RTCP Ports (SIP)	4900+ (range of 64 ports)	UDP	In/Out	×	✓	**Anruf > Allgemeine Einstellungen**
RTP+RTCP Ports (externe Kamera)	4800+ (range of 64 ports)	UDP	In/Out	×	✓	**Integration > ONVIF / RTSP**
R5TSP-Klient	554	UDP	In/Out	×	✓	
RTSP server	554	UDP	In/Out	×	×	–
SingleWire Commands	80	TCP	In/Out	×	×	–
SingleWire Communication	8081	TCP	Out	×	×	–
SingleWire Media	20000+	UDP	In	×	×	–
SLP	427	UDP	In/Out	✓	×	–
SIP	5060, 5062	TCP/UDP	In/Out	×	✓	**Anruf > SIP**

Service	Port	Protokoll	Richtung	Standardmäßig eingeschaltet	Einstellbar	Einstellungen
SIPS	5061	TCP	In/Out	×	✓	**Anruf >SIP**
SMTP	25	TCP	Out	×	✓	**Integration > E-Mail-Benachrichtigungen**
Syslog	514	UDP	Out	×	×	–
TFTP	69	UDP	Out	×	×	–
My2N Knocker	443	TCP	Out	✓	×	–
My2N Tribble Tunnel	443	TCP	Out	✓	×	–
SNMP Agent	161	UDP	In/Out	✓	×	–
SNMP Trap	162	UDP	Out	✓	×	–
SSDP	1900	UDP	In/Out	✓	×	–
SDDP	1902	UDP	In/Out	✓	×	–
Multicast receiver (Automation)	4433	UDP	In	×	×	–
WS-Discovery	3702	UDP	In/Out	✓	×	–
CIP Client (Crestron)	41794	UDP	In/Out	×	×	–
Sitechannel (ICU-Protokoll)	8004	UDP	In/Out	×	×	–
Multicast DNS	5353	UDP	In/Out	✓	×	–

Erste Anmeldung

Suche nach Geräten im Netzwerk

Für den Zugriff auf die Schnittstelle müssen Sie die IP-Adresse des Geräts kennen. Das Gerät muss mit dem lokalen IP-Netzwerk verbunden sein und gespeist werden.

Domänename

Für den Zugriff auf die Webkonfigurationsschnittstelle können Sie anstelle der IP-Adresse einen Domänennamen im Browser im Format „hostname.local“ eingeben. Der Hostname eines neuen Geräts besteht aus dem Produktnamen und der Seriennummer des Geräts. Verwenden Sie bei der Eingabe eines Hostnamens nur Buchstaben und Zahlen und keine Leerzeichen, Punkte, Bindestriche oder andere Sonderzeichen.

Der Standarddomänenname : 2NIPIntercom20-{Seriennummer ohne Bindestriche}.local (z.B.: „2NIPIntercom20-0000000001.local“)

Das Format des Namens des jeweiligen Geräts ist im Installationshandbuch des Produkts im Kapitel Domainname angegeben.

TIPP
Sie können den Hostnamen später in der Webkonfigurationsoberfläche unter **System > Netzwerkverbindung > Registerkarte Erweiterte Konfiguration > Hostname** ändern.

Die Anmeldung mit einem Domänennamen hat bei der Verwendung der dynamischen IP-Adresse des Geräts einen Vorteil. Während sich die dynamische IP-Adresse ändert, bleibt der Domänenname derselbe. Sie können von einer vertrauenswürdigen Zertifizierungsstelle signierte Zertifikate für einen Domänennamen erzeugen.

IP-Adresse des Geräts

In der Werkseinstellung verwendet das Gerät eine dynamische IP-Adresse, die vom DHCP-Server zugewiesen wird.

Um die IP-Adresse eines 2N Geräts in Ihrem lokalen Netzwerk zu ermitteln, verwenden Sie das 2N IP Utility. Die Applikation 2N IP Utility kann von der Website 2N.com heruntergeladen werden. Sie müssen Microsoft .NET Framework 4.7.2 installiert haben.

Je nach den Möglichkeiten des Geräts können Sie die IP-Adresse auch auf eine der folgenden Arten herausfinden:

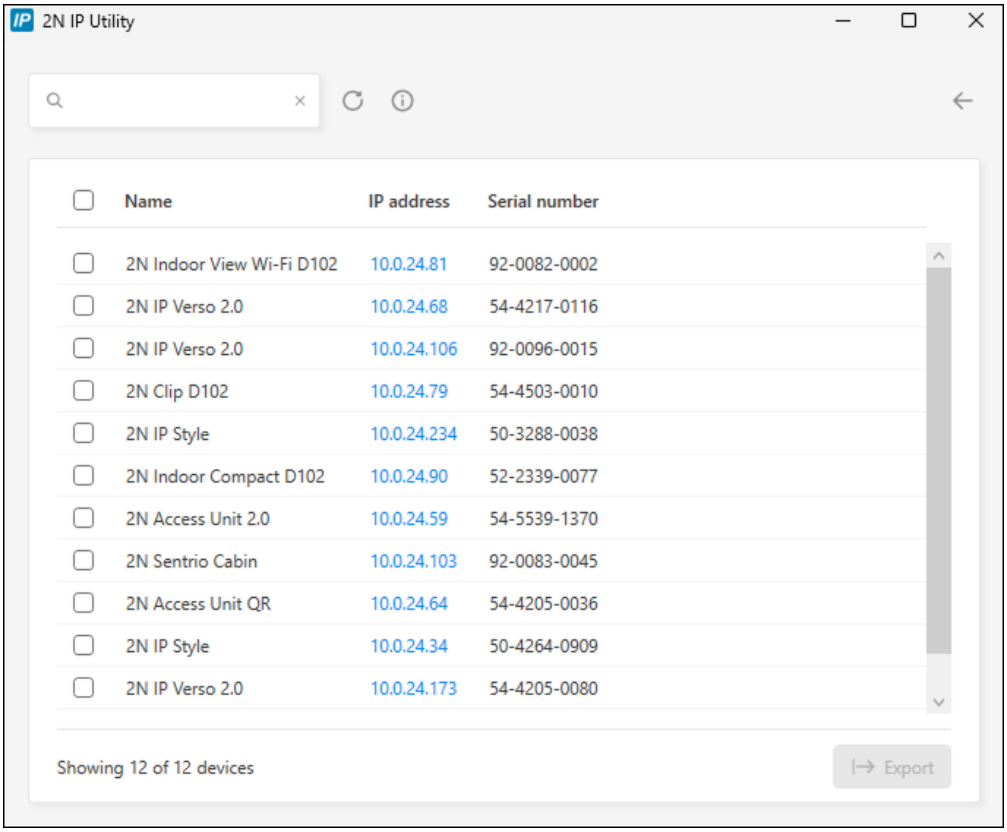
- Schnellwahltaste
- auf dem Display des Geräts (siehe die Installationsanleitung des Produkts für das Verfahren)

Abrufen einer IP-Adresse mit 2N IP Utility

Um die IP-Adresse eines 2N Geräts in Ihrem lokalen Netzwerk zu ermitteln, verwenden Sie das 2N IP Utility. Die Applikation 2N IP Utility kann von der Website 2N.com heruntergeladen werden. Sie müssen Microsoft .NET Framework 4.7.2 installiert haben.

1. Führen Sie das Installationsprogramm 2N IP Utility aus.
2. Der Installationsassistent wird Sie durch die Installation führen.

3. Nach der Installation der Applikation 2N IP Utility starten Sie die Applikation über das Startmenü des Betriebssystems Microsoft Windows.
   Nach dem Start sucht die Applikation automatisch im lokalen Netzwerk nach allen 2N und AXIS Geräten, die eine per DHCP zugewiesene oder statisch eingestellte IP-Adresse haben. Diese Geräte werden dann in der Tabelle angezeigt.



4. Wählen Sie das Gerät, das Sie konfigurieren möchten, aus der Liste aus und klicken Sie es mit der linken Maustaste an. Dadurch wird die rechte Seite des Webkonfigurationsfensters geöffnet.

TIPP

- Die Webkonfigurationsschnittstelle kann auch über die Schaltfläche **Open in external browser** aufgerufen werden, mit der Sie die Schnittstelle in einem separaten Browserfenster öffnen können.
- Klicken Sie auf ein Gerät in der Liste, um detaillierte Informationen zu erhalten. Klicken Sie auf die Schaltfläche **IP settings**, um die IP-Adresse durch Eingabe der gewünschten statischen IP-Adresse oder durch Aktivierung von DHCP zu ändern.
- Die Anwendung ermöglicht es Ihnen auch, ausgewählte Geräte in eine CSV-Datei zu exportieren. Wählen Sie zunächst das Gerät aus, indem Sie die Kästchen für jedes Gerät in der Liste markieren, und verwenden Sie dann die Schaltfläche **Export**, die unten im Fenster erscheint. Die exportierte Datei enthält den Namen, die IP-Adresse und die Seriennummer der ausgewählten Geräte

Die Standard-Anmeldedaten sind:
Benutzername: **Admin**
Passwort: **2n**
Nach der ersten Anmeldung ist unverzüglich das Passwort zu ändern.

TIPP
Es wird empfohlen, ein Passwort zu verwenden, das schwer zu überwinden ist. Es wird nicht empfohlen, Namen, Ortsnamen oder Sachen in Passwörtern zu verwenden, insbesondere solche, die einen direkten Bezug zum Benutzer haben.

Für höhere Sicherheit des Passworts empfehlen wir:

- einen Passwort-Zufallsgenerator verwenden,
- die Passwortlänge mindestens 12 Zeichen,
- eine Kombination verschiedener Zeichen aus unterschiedlichen Zeichensätzen (z. B. Groß-/Kleinschreibung, Ziffern, Sonderzeichen u. ä.).

Ermittlung der IP-Adresse mithilfe der Kurzwahltaste

Für die Feststellung der IP-Adresse gehen Sie wie folgt vor:

1. Schließen Sie das Gerät an die Stromversorgung an (wenn es bereits angeschlossen ist, trennen Sie es ab und schließen Sie es erneut an).
2. Drücken Sie die erste Schnellwahltaste auf dem Hauptgerät 5 Mal.
3. Das Gerät liest seine IP-Adresse.

ANMERKUNG

- Wenn die Adresse 0.0.0.0 ist, bedeutet es, dass das Gerät keine IP-Adresse vom DHCP-Server erhalten hat.
- Aus Sicherheitsgründen kann man die Reihenfolge der Tasten maximal innerhalb von dreißig Sekunden nach dem Tonsignal eingeben. Zwischen den einzelnen Tastenbetätigungen dürfen die Abstände nicht länger als 2 s sein.

Commutation DHCP

In der Werkseinstellung verwendet das Gerät eine dynamische IP-Adresse, die vom DHCP-Server zugewiesen wird.

Dynamische IP-Adresse

DHCP (Dynamic Host Configuration Protocol) ist ein Netzwerkprotokoll, das eine Liste verfügbarer IP-Adressen verwaltet und diese automatisch den Geräten im lokalen Netzwerk zuweist. Die zugewiesene IP-Adresse ist dynamisch, so dass dem Gerät nach einer gewissen Zeit (Lease Time) eine neue IP-Adresse zugewiesen werden kann.

Statische IP-Adresse

Wenn die IP-Adresse des Geräts unverändert bleiben soll, müssen Sie die IP-Adresszuweisung durch den DHCP-Server auf dem Gerät deaktivieren. Sie können den DHCP-Server über die Web-Konfigurationsoberfläche oder über die Hardware des Geräts deaktivieren.

ANMERKUNG
Die spezifischen Werte für die statische IP-Adresse können nur in der Web-Konfigurationsoberfläche des Geräts eingestellt werden.

Einstellen der Netzwerkparameter in der Web-Konfigurationsoberfläche

1. Rufen Sie die Web-Konfigurationsoberfläche auf.
2. Gehen Sie zu **System > Netzwerkverbindung > Registerkarte Grundeinstellungen > IP-Adresseinstellungen**.
3. Stellen Sie die gewünschten Netzwerkparameter ein.
4. Speichern Sie Ihre Änderungen.

Umschalten von DHCP auf Gerätehardware

Je nach den Fähigkeiten des Geräts kann die IP-Adresse wie folgt umgeschaltet werden:

- Schnellwahltaste
- auf dem Display des Geräts (siehe die Installationsanleitung des Produkts für das Verfahren)

TIPP
Wo sich die RESET-Taste befindet, entnehmen Sie bitte dem Installationshandbuch des Produkts.

Ermittlung der IP-Adresse mithilfe der Kurzwahltaste

Für die Feststellung der IP-Adresse gehen Sie wie folgt vor:

1. Schließen Sie das Gerät an die Stromversorgung an (wenn es bereits angeschlossen ist, trennen Sie es ab und schließen Sie es erneut an).
2. Drücken Sie die erste Schnellwahltaste auf dem Hauptgerät 5 Mal.
3. Das Gerät liest seine IP-Adresse.

ANMERKUNG

- Wenn die Adresse 0.0.0.0 ist, bedeutet es, dass das Gerät keine IP-Adresse vom DHCP-Server erhalten hat.
- Aus Sicherheitsgründen kann man die Reihenfolge der Tasten maximal innerhalb von dreißig Sekunden nach dem Tonsignal eingeben. Zwischen den einzelnen Tastenbetätigungen dürfen die Abstände nicht länger als 2 s sein.

Zugang zur webbasierten Gerätekonfiguration

Die Konfiguration des Geräts erfolgt über eine webbasierte Konfigurationsoberfläche, auf die Sie über einen Webbrowser zugreifen können.

Für den Zugriff auf die Schnittstelle müssen Sie die IP-Adresse des Geräts kennen. Das Gerät muss mit dem lokalen IP-Netzwerk verbunden sein und gespeist werden.

Die webbasierte Konfigurationsoberfläche kann auch über das angeschlossene My2N-Portal oder über das Konfigurationstool 2N Access Commander aufgerufen werden.

Einloggen in die Web-Konfigurationsschnittstelle

1. Starten Sie Ihren Internet-Browser.

2. Geben Sie die IP-Adresse des Geräts oder den Domainnamen des Geräts ein (siehe Kapitel Suche nach Geräten im Netzwerk (S. 8)).
3. Wenn Sie kein Zertifikat für die IP-Adresse erzeugt haben, erhalten Sie möglicherweise eine Warnung über ein ungültiges Sicherheitszertifikat. In diesem Fall müssen Sie bestätigen, dass Sie zur Web-Konfigurationsschnittstelle wechseln möchten.
4. Der Anmeldebildschirm wird angezeigt.
5. Geben Sie die Anmeldedaten ein.
   Die Standard-Anmeldedaten sind:
   - Benutzername: **Admin**
   - Passwort: **2n**
6. Ändern Sie das Passwort nach dem ersten Anmelden.

Zugriff über 2N Access Commander

1. Melden Sie sich bei der Schnittstelle Access Commander an.
2. Gehen Sie zu Geräte.
3. Drücken Sie für das ausgewählte Gerät .

Passwortänderung

Sie müssen das Standardpasswort ändern, um vollen Zugriff auf die Funktionen der Webkonfigurationsoberfläche zu erhalten. Sie können das Gerät nicht konfigurieren, ohne das Standardpasswort zu ändern.

TIPP

Es wird empfohlen, ein Passwort zu verwenden, das schwer zu überwinden ist. Es wird nicht empfohlen, Namen, Ortsnamen oder Sachen in Passwörtern zu verwenden, insbesondere solche, die einen direkten Bezug zum Benutzer haben.

Für höhere Sicherheit des Passworts empfehlen wir:

- einen Passwort-Zufallsgenerator verwenden,
- die Passwortlänge mindestens 12 Zeichen,
- eine Kombination verschiedener Zeichen aus unterschiedlichen Zeichensätzen (z. B. Groß-/Kleinschreibung, Ziffern, Sonderzeichen u. ä.).

Empfohlene Browser

Die Web-Konfigurationsoberfläche ist für Chrome-basierte Webbrowser (wie Google Chrome, Microsoft Edge oder Opera) optimiert. Bei der Verwendung anderer Browser kann es zu geringfügigen Unterschieden in der Funktionalität und im Erscheinungsbild der Benutzeroberfläche kommen.

Grundlegende Geräteeinstellungen

Aktualisierung der Firmware

Neue Firmware-Versionen sind auf dem Update-Server verfügbar. Wenn die Web-Konfigurationsschnittstelle keinen Zugang zum öffentlichen Internet hat, können Sie die Firmware-Datei auch manuell auf das Gerät hochladen.

ANMERKUNG
Firmware-Updates erfolgen nicht automatisch. Um die Systemintegrität zu gewährleisten und unbeabsichtigte Fehler zu vermeiden, müssen alle Updates manuell bestätigt oder vom Benutzer initiiert werden. Bevor Sie ein Update durchführen, lesen Sie bitte die Versionshinweise für die neue Version und überprüfen Sie die Kompatibilität mit Ihrer bestehenden Infrastruktur.

Abrufen der Firmware vom Update-Server

1. Gehen Sie zu **System > Wartung > Registerkarte Firmware**.
2. Klicken Sie auf Nach Updates suchen.
3. Wenn ein Update verfügbar ist, werden seine Versionshinweise geladen. Um das Upgrade zu starten, klicken Sie in der Kopfzeile des Fensters auf Upgrade.
4. Nach erfolgreichem Firmware-Upload wird das Gerät automatisch neu gestartet. Nach dem Neustart ist das Gerät mit der neuen Firmware verfügbar. Die Firmwareaktualisierung beeinflusst nicht die Konfiguration.

Hochladen neuer Firmware aus dem Speicher

1. Gehen Sie zu **System > Wartung > Registerkarte Firmware**.
2. Klicken Sie auf Firmware hochladen.
3. Wählen Sie in dem sich öffnenden Dialogfenster eine Datei aus Ihrem eigenen Repository.
4. Bestätigen Sie das Hochladen der Datei, indem Sie auf Upload klicken.
   Das Gerät überprüft die Firmware-Datei und kann keine falsche oder beschädigte Datei hochladen.
5. Nach erfolgreichem Firmware-Upload wird das Gerät automatisch neu gestartet. Nach dem Neustart ist das Gerät mit der neuen Firmware verfügbar. Die Firmwareaktualisierung beeinflusst nicht die Konfiguration.

ANMERKUNG
Die Funktionalität, Zuverlässigkeit und Sicherheit des Geräts hängen von der installierten Firmware ab. Das regelmäßige Aktualisieren der Firmware auf die aktuelle Version ist Teil der Nutzungsbedingungen des Produkts. Fehler, die durch die Verwendung einer veralteten Firmware-Version verursacht werden, können nicht reklamiert werden. Die aktuelle Firmware setzt Kundenerfahrungen und Anforderungen im Bereich der Sicherheit von personenbezogenen Daten um.

Telefonbuch

Der Abschnitt Verzeichnis ist ein wichtiger Teil der Gerätekonfiguration. Sie erstellen Benutzer im Verzeichnis und verwalten deren Zugriffsrechte oder Parameter für den Telefonanschluss. Jeder Benutzer kann gleichzeitig als Inhaber von Zugriffsrechten, als anrufender Kontakt oder als beides fungieren.

Manuelles Hinzufügen eines Benutzers zu einem Verzeichnis

1. Klicken Sie auf der Seite Verzeichnis auf Benutzer hinzufügen.
2. Die Benutzerdetails werden geöffnet. Auf der Registerkarte Persönliche Informationen geben Sie dem Benutzer einen Namen.
3. Stellen Sie die Telefonnummer des Kontakts gemäß Erstellen von Anrufkontakten (S. 14) ein.
4. Stellen Sie die Zugriffsoptionen gemäß Ansätze (S. 19) ein.

Massive Benutzerverwaltung in Access Commander oder My2N

Wenn das Gerät über Access Commander oder My2N Bulk-Konfigurations-Tools verwaltet wird, werden alle in der webbasierten Konfigurationsoberfläche vorgenommenen Änderungen durch die Einstellungen im Bulk-Konfigurations-Tool überschrieben. Ein Benutzer, der direkt in der Weboberfläche angelegt wurde, wird gelöscht.

Die Spalte holder in der Verzeichnistabelle listet das Massenkonfigurationsprogramm auf, das den Benutzer erstellt hat. Die Spalte Halter ist standardmäßig ausgeblendet.

Telefon

Das 2N Gerät bietet mehrere Möglichkeiten, Anrufe zu verbinden. Bevor Sie Kontakte erstellen und das Wählverfahren einrichten können, müssen Sie zunächst die Dienste aktivieren und einrichten, die den Anruf vermitteln sollen:

- Anrufe über SIP (S. 17)
- Ortsgespräche zwischen 2N Geräten (S. 19)
- andere spezielle Integrationen

Erstellen von Anrufkontakten

Das Erstellen eines Anrufkontakts besteht darin, dem entsprechenden Benutzer im Geräteverzeichnis eine Telefonnummer hinzuzufügen.

TIPP

Sie können die Funktion für lokale Anrufe verwenden, um eine Verbindung zu einem anderen 2N Gerät in Ihrem lokalen Netzwerk herzustellen, siehe Hinzufügen eines lokalen 2N Geräts (S. 15).

1. Gehen Sie auf **Verzeichnis**.
2. Öffnen Sie die Benutzerdetails, indem Sie auf die Zeile klicken, oder wählen Sie Benutzer hinzufügen, um einen neuen Benutzer anzulegen.
3. Auf der Registerkarte **Telefonnummern von** öffnen Sie die Telefonnummernbearbeitung, indem Sie auf das Symbol klicken.
4. Wählen Sie **Anrufart**, in der der Kontakt verfügbar sein soll (SIP, lokales Netzwerk, MS Teams, VMS, ...).
   - Anrufe über SIP (S. 17) - für VoIP-Dienste und Konten
   - Ortsgespräche zwischen 2N Geräten (S. 19) - für Anrufe an 2N Geräte
   - MS Teams, VMS,... - für spezielle Integrationen

5. Geben Sie die Zielnummer oder -adresse ein, die das Gerät anrufen soll.
   Geben Sie die Durchwahlnummer, die SIP-URI (z. B. „sip:101@192.168.1.50“), den Domänennamen (z. B. „2NIPVerso20-22222222“ oder eine andere für den Anruftyp geeignete Nummer) ein.
6. Stellen Sie im Feld **Optionen** zusätzliche Anruffunktionen ein, die das Verhalten des Anrufs beeinflussen.
   Mit diesen Optionen kann der Administrator die Sicherheit, die Funktionalität und die Wähllogik so konfigurieren, dass sie genau auf die Bedürfnisse der Einrichtung zugeschnitten sind, z. B. um eine verschlüsselte Übertragung zu verwenden, die Verbindung zu beschleunigen oder die Türumkehr zu aktivieren.
7. Geben Sie im Abschnitt **Verfügbarkeit auf** an, wann die Nummer angerufen werden kann. Sie können zum Beispiel die Verfügbarkeit nur für die Arbeitszeiten des Benutzers festlegen.
8. Speichern Sie die Änderung, indem Sie auf Bestätigen klicken.
9. Wenn Sie die Kurzwahltaste zum Anrufen des Kontakts verwenden möchten, weisen Sie dem Kontakt auf der Registerkarte **Schaltflächen eine Schaltfläche zu.**

Einrichten von 2N IP Eye

Anwendung 2N IP Eye ermöglicht es Ihnen, das Video der IP-Sprechanlage auf Ihrem Computerbildschirm zu betrachten. Nachdem Sie die Adresse **des 2N IP Eye** eingegeben haben, zeigt der Kontakt das Video auf diesem Computer an, wenn Sie einen Anruf tätigen.

Die Adresse wird in folgender Form eingegeben: `domain[:port1][:port2]`

- `eye_computer.company.cz`
- `192.168.22.111:8009:8080`

Die Parameter `port1` und `port2` sind optional. Geben Sie sie ein, wenn die Adressübersetzung (NAT) zwischen dem 2N IP-Gerät und dem Computer mit 2N IP Eye im Gange ist. Konfigurieren Sie die Ports entsprechend der Konfiguration des Routers oder eines anderen NAT-Geräts.

- `port1` - Standardwert 8003, Zielport für den Empfang von UDP-Nachrichten von der 2N IP Eye Anwendung.
- `port2` - Standardwert 80, Zielport für die HTTP-Kommunikation zwischen der 2N IP Eye Anwendung und dem 2N IP Gerät.

Hinzufügen eines lokalen 2N Geräts

ACHTUNG
Lokale Anrufe müssen sowohl auf diesem als auch auf dem gesuchten Gerät mit dem identischen **Zugriffsschlüssel** aktiviert sein, siehe Ortsgespräche zwischen 2N Geräten (S. 19).

1. Klicken Sie auf der Seite **Verzeichnis** auf Lokales Gerät hinzufügen.
2. In dem sich öffnenden Dialogfenster markieren Sie das Gerät, mit dem Sie eine Verbindung herstellen möchten.
3. Wählen Sie Zum Verzeichnis hinzufügen.
4. Ein neuer Benutzer erscheint im Verzeichnis mit einer eingestellten Rufnummer.
5. Klicken Sie auf die Benutzerzeile, um sie weiter zu bearbeiten.

TIPP
Um die Zugriffsrechte des Inhabers dieses Geräts festzulegen, folgen Sie Ansätze (S. 19).

Wählen von Anrufen auf dem Gerät

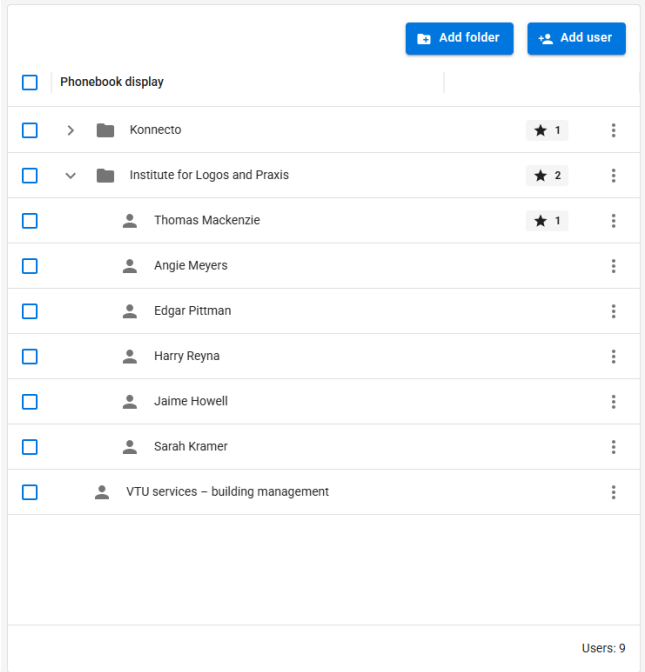
Zuweisen von Kurzwahltasten

Um den Kurzwahltasten Kontakte zuzuweisen, gehen Sie zu **Anrufen > Wählen > Registerkarte Kurzwahltasten**.

Die Schaltflächen für die Schnellauswahl von Modulen, die über VBUS an das Hauptgerät angeschlossen sind, werden ebenfalls hier eingestellt.

So zeigen Sie die Kontakte des Adressbuchs auf dem Display an

Um die Anzeige und Reihenfolge der Kontakte auf dem Gerätedisplay einzustellen, gehen Sie zu **Anrufen > Wählen > Registerkarte Telefonbuchanzeige**.



Alle Kontakte mit einer zugewiesenen Rufnummer werden standardmäßig im Stammordner gespeichert. Die Kontakte können weiter in Ordnern sortiert werden, zum Beispiel nach Abteilung oder Stockwerk.

Kontakte in einen Ordner verschieben

1. Erstellen Sie in der Kopfzeile der Telefonbuchtabelle einen neuen Ordner und benennen Sie ihn.

> **TIPP**
>
> Im Erweiterungsmenü ⋮ für einen Ordner können Sie ein Bild zu dem Ordner hinzufügen, unter dem es dann in der Telefonbuchansicht angezeigt wird.

2. Um Ihre Kontakte in einen anderen Ordner zu verschieben, wählen Sie sie zunächst aus und klicken dann auf ✥.
3. Wählen Sie einen neuen Ort im Telefonbuch.
4. Speichern Sie Ihre Änderungen, indem Sie auf Verschieben klicken.

In jedem Ordner sind die Kontakte normalerweise alphabetisch sortiert. Diese Reihenfolge kann geändert werden, indem Sie die Priorität einstellen (im erweiterten Menü ⋮ für den Kontakt).

Ein neu angelegter Benutzer mit einer Telefonnummer wird automatisch im Stammordner angezeigt.

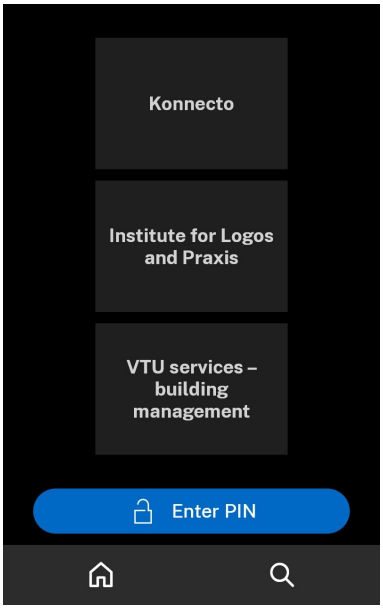
Anrufgruppen

Anrufgruppen ermöglichen es, mehrere Kontakte gleichzeitig anzurufen (z. B. den Empfang und das Lager gleichzeitig anzurufen).

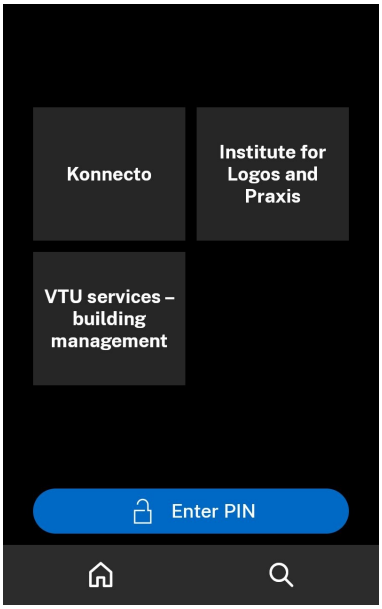
1. Wählen Sie in der Tabelle **Telefonbuchansicht** alle Kontakte aus, die Sie in die Gruppe aufnehmen möchten.
2. Klicken Sie oberhalb der Tabelle auf .
3. Geben Sie den Namen der Anrufergruppe und ihre Position im Telefonbuch ein.
4. Wählen Sie, ob Sie die Kontakte weiterhin als einzelne Kontakte anzeigen möchten oder ob Sie sie nur im Telefonbuch unter der Anrufgruppe anzeigen möchten.
5. Speichern Sie Ihre Änderungen, indem Sie auf Verschieben klicken.

Display-Einstellungen 2N IP Style

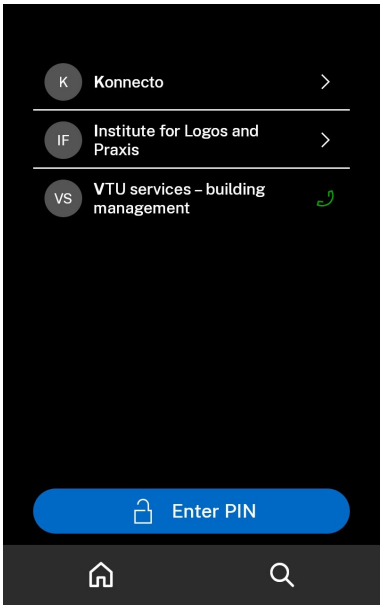
Auf der linken Registerkarte **Display-Einstellungen** können Sie zwischen den folgenden Möglichkeiten wählen, um das Verzeichnis auf dem Gerätedisplay anzuzeigen **2N IP Style**.



Karten (1 Spalte)



Karten (2 Spalte)



Phonebook

Anrufe über SIP

Registrierung des Geräts beim SIP-Server

Die Registrierung beim SIP-Server ist entscheidend für die volle Funktionalität des Geräts in einer SIP-Umgebung.

1. Gehen Sie zu **Calling > SIP** des Kontos, das Sie einrichten möchten.
2. Aktivieren Sie das SIP-Konto im oberen Bereich.
3. Geben Sie auf der Registerkarte **, Geräteidentität** ein:
   - **Anzeigename** - dieser Text wird dem anderen Teilnehmer als Anrufer-ID angezeigt.
   - **Telefonnummer (ID)** - diese Nummer identifiziert zusammen mit der Domain das Gerät bei Anrufen und bei der Registrierung eindeutig.
   - **Domain**- Legt den Domainnamen des Dienstes fest, für den das Gerät registriert ist. Üblicherweise ist dieser identisch mit dem SIP-Proxy oder der SIP-Registrar-Adresse.

   Diese drei Werte zusammen identifizieren das Gerät in der SIP-Umgebung.

4. Geben Sie unter **Authentifizierung** die Anmeldedaten ein, die der Administrator des SIP-Servers zugewiesen hat, um das Gerät beim SIP-Proxy-Server zu authentifizieren. Diese Authentifizierung verhindert unbefugten Zugriff, betrügerische Anrufe oder Identitätsbetrug.
   Wenn die **Authentifizierungs-ID nicht in** eingegeben wird, authentifiziert sich das Gerät mit **Telefonnummer**.
5. Wählen Sie unter **Transportprotokolloptionen** das vom SIP-Server verwendete Protokoll aus.
6. Aktivieren Sie die Funktion **SIP-Registrar** Registerkarte.
7. Geben Sie die Details der SIP-Registrierungsstelle ein, bei der Sie das 2N Gerät registrieren möchten.
   Wenn Sie den Parameter **Port** leer lassen oder der Parameterwert 0 ist, wird der Standardport entsprechend dem gewählten Transportprotokoll verwendet.

Standardportwerte je nach Transportprotokoll

Konto	UDP / TCP	TLS
SIP 1	5060	5061
SIP 2	5062	5063
SIP 3	5064	5065
SIP 4	5066	5067

8. Die Registerkartenüberschrift zeigt den Registrierungsstatus und die Fehlermeldungen der Registrierung an.

ANMERKUNG
Weitere SIP-Kontoeinstellungen sind im Kapitel Erweiterte SIP-Kontoeinstellungen (S. 40) beschrieben.

So legen Sie die öffentliche IP-Adresse eines Geräts fest

Diese Einstellung wird verwendet, wenn sich das Gerät hinter einem Router (NAT) befindet und mit dem Control Panel außerhalb des lokalen Netzwerks kommuniziert (z.B. in der Cloud oder über das Internet). Bei der SIP-Kommunikation muss das Gerät die öffentliche IP-Adresse angeben, unter der es aus dem Internet erreichbar ist. Wenn es seine interne IP-Adresse senden würde, könnte die Telefonanlage den Anruf oder den RTP-Datenstrom nicht korrekt weiterleiten.

Wenn sich das Gerät und die Telefonanlage im selben lokalen Netzwerk befinden, ist die Einstellung einer öffentlichen IP-Adresse nicht erforderlich.

1. Gehen Sie zu **Calling > SIP** des Kontos, das Sie einrichten möchten.
2. Wählen Sie auf der Registerkarte **die öffentliche IP-Adresse** aus den folgenden Optionen aus:
   - STUN (Automatisch)
     Geben Sie die Details zu Ihrem STUN-Server ein.
   - Manuell eingeben
     Geben Sie Ihre eigene externe IP-Adresse für das Gerät ein.

Ortsgespräche zwischen 2N Geräten

Es ist möglich, sogenannte lokale Anrufe zwischen 2N IP-Geräten einzurichten, die eine direkte Kommunikation zwischen 2N Geräten innerhalb eines lokalen Netzwerks ermöglichen, ohne dass eine Verbindung zu einem SIP-Server oder einer externen Infrastruktur erforderlich ist.

So aktivieren Sie Ortsgespräche

1. Gehen Sie zu **Anrufe > Ortsgespräche**.
2. Aktivieren Sie die Funktion in der Kopfzeile der Seite.
3. Legen Sie Zugriffsschlüssel fest, um eine sichere Kommunikation mit anderen Geräten im Netzwerk zu gewährleisten.
   Zugriffsschlüssel stellen sicher, dass nur Geräte mit identischen Schlüsseln miteinander kommunizieren können. Dies trägt zur Sicherheit bei und bietet die Möglichkeit, unabhängige Gerätegruppen zu definieren.

Ansätze

Eine der Grundfunktionen des Geräts ist die Verwaltung des Zugangs und der Entriegelung des elektrischen Türschlosses. Das Gerät verwaltet den Zugriff auf der Grundlage der Auswertung von Zugriffsanfragen gemäß vordefinierter Zugriffsregeln. Wenn das Gerät die Anfrage als legitim erachtet, aktiviert es den Türschalter, der das elektrische Türschloss steuert. Dies wird die Tür entriegeln.

Neben der herkömmlichen Benutzerauthentifizierung (RFID-Karte, Biometrie, Bluetooth usw.) kann der Schalter auch über externe Signale und Schnittstellen aktiviert werden, was flexible Integrations- und Automatisierungsmöglichkeiten bietet. Die verschiedenen Möglichkeiten, den Türschalter zu aktivieren, werden im Folgenden beschrieben:

Benutzer überprüfen

Der Benutzer verwendet seine Authentifizierungsmethode, und wenn seine Benutzerberechtigungen mit den Zugriffsregeln übereinstimmen, wird ihm der Zugriff gewährt. Der erlaubte Zugang aktiviert den Türschalter.

Die Einrichtung wird im Kapitel Benutzerzugriffseinstellungen (S. 20) beschrieben.

Switch-Steuerung in der Web-Konfigurationsoberfläche

1. Gehen Sie zu **Integration > Switches**.
2. Finden Sie die Schalterkarte, die die Tür steuert.

ANMERKUNG
Die Funktion des Türschalters im Gerät wird von **Switch 1** übernommen.

3. Klicken Sie unter **Manual Switch Control** auf Hold.
4. Der Schalter bleibt so lange eingeschaltet, bis Sie das Halten der manuellen Steuerung wieder aufheben.

Ausschalten basierend auf einem Zeitprofil

In der Web-Konfigurationsoberfläche können Sie den Schalter so einstellen, dass die Tür für eine bestimmte Zeit, z.B. über die Mittagszeit, nicht verriegelt wird.

1. Gehen Sie zu **Integration > Switches**.
2. Finden Sie die Schalterkarte, die die Tür steuert.

ANMERKUNG
Die Funktion des Türschalters im Gerät wird von **Switch 1** übernommen.

3. Klicken Sie auf den Pfeil → des ausgewählten Schalters, um zu dessen Details zu gelangen.
4. Auf der Registerkarte **Status** aktivieren Sie die Option **Zeitgesteuerter Hold-Schalter**.
5. Wählen Sie die Zeitprofile aus, in denen der Schalter gehalten werden soll, oder geben Sie eine benutzerdefinierte Zeitspanne ein.

Ausschalten des Schalters bei einem Anruf (DTMF)

DTMF-Code-Einstellungen

1. Gehen Sie zu **Integration > Switches**.
2. Finden Sie die Schalterkarte, die die Tür steuert.

> **ANMERKUNG**
> Die Funktion des Türschalters im Gerät wird von **Switch 1** übernommen.

3. Klicken Sie auf den Pfeil → des ausgewählten Schalters, um zu dessen Details zu gelangen.
4. Auf der Registerkarte **Aktivierungscodes von** können Sie die Codes festlegen, die Sie während eines Anrufs mit dem Gerät per DTMF eingeben können.
   Die Gültigkeit jedes Codes kann zeitlich begrenzt sein.

> **ANMERKUNG**
> Für den ersten Aktivierungscode können Sie festlegen, dass er als eine ältere Form des Codes verarbeitet wird. In dieser Form müssen Sie den Code nicht mit einem Sternchen bestätigen, wenn Sie ihn auf der Telefontastatur eingeben.

Verwenden des DTMF-Codes

1. Wenn Sie mit dem Gerät verbunden sind, geben Sie den Aktivierungscode auf der Tastatur Ihres Telefons ein und bestätigen ihn mit einem Sternchen.

> **ANMERKUNG**
> Der Empfang von DTMF-Signalen ist auf dem Gerät standardmäßig aktiviert. Sie können die Berechtigungen auf der Seite Rufdienst (SIP/Lokalrufe) unter der Registerkarte **Audio**, auf der Registerkarte **DTMF-Empfang** überprüfen.

Schalten des Schalters mithilfe der HTTP API

Die vollständige Verwendung, einschließlich einer Beschreibung der erforderlichen HTTP-API-Autorisierung, ist im HTTP-API-Handbuch für 2N-Geräte beschrieben. Der Türschalter wird über den Endpunkt `api switch ctrl` gesteuert. Für Schalter 1 sieht der Befehl wie folgt aus: `https://ip_adresa/api/switch/ctrl?switch=1&action=on`.

Schalten des Schalters Automatisierung

Die Einrichtung der Automatisierung wird im Handbuch Automatisierung beschrieben. Der Schalter wird durch die Aktion **ActivateSwitch** ausgelöst.

Benutzerzugriffseinstellungen

Um sich erfolgreich an der Zugangskontrolleinheit zu authentifizieren und die Tür zu entriegeln, muss der Benutzer zwei Bedingungen erfüllen: Er muss über die dem Gerät zugewiesenen Zugangsrechte verfügen

und mindestens eine Authentifizierungsmethode eingerichtet haben. Die verfügbaren Authentifizierungsmethoden hängen vom jeweiligen Gerät ab und können RFID-Karten, numerische PINs, QR-Codes zum Scannen mit der Kamera usw. umfassen.

Einstellungen für die Authentifizierung:

1. Gehen Sie auf **Verzeichnis**.
2. Öffnen Sie die Benutzerdetails, indem Sie auf die Zeile klicken, oder wählen Sie Benutzer hinzufügen, um einen neuen Benutzer anzulegen.
3. Auf der Registerkarte **Authentifizierung** legen Sie alle Methoden fest, mit denen sich der Benutzer authentifizieren soll, siehe Methoden zur Authentifizierung (S. 21).
4. Geben Sie auf der Registerkarte **Zugangseinstellungen von** an, wann der Benutzer Zugang zum Betreten und Verlassen erhalten soll.
   - Jederzeit
   - Zeitprofil - bietet eingestellte **Zeitprofile**
   - Benutzerdefiniert - verwenden Sie die Schaltfläche Bearbeiten, um Zeitintervalle festzulegen, die nur für diesen Benutzer gelten.

   Legen Sie ein Ablaufdatum fest, um den Zugriff des Benutzers auf einen bestimmten Kalenderzeitraum zu begrenzen.

   Durch die Gewährung von **Ausnahmen** erhält der Benutzer einen permanenten Zugang, der nicht einmal die vorübergehende Sperrung des durch die Zugangsregeln angegebenen Geräts einschränkt (siehe Zutrittsregeln (S. 23)).

Methoden zur Authentifizierung

ACHTUNG
Die verfügbaren Authentifizierungsmethoden hängen von dem jeweiligen Gerät und den angeschlossenen Modulen ab.

RFID-Karte

Einem Benutzer können bis zu 2 RFID-Karten zugewiesen werden.

Die Kennung kann manuell über die Tastatur eingegeben oder durch Einstecken der Karte in ein an den Computer angeschlossenes USB-Lesegerät gelesen werden.

Anforderungen für RFID-Karten

- Die Kennung muss eine hexadezimale Zahl sein.
- Die Mindestlänge des Identifikators beträgt 6 Zeichen.
- Es können nur Karten verwendet werden, die vom Gerät unterstützt werden - der Kartentyp muss in den Moduleinstellungen aktiviert sein (siehe **Zugriff > Module**).

TIPP
Sie können die Kennung einer vorhandenen Karte aus dem Protokoll unter **System > Ereignisprotokoll** ablesen. Laden Sie die neue/nicht zugewiesene Karte in das Gerät und kopieren Sie dann ihre Kennung (UUID) aus dem Protokoll. Nach dem Einfügen des Identifikators zwischen die RFID-Karten kann der Benutzer die Karte zur Authentifizierung benutzen.

My2N

My2N – Wird für die Verbindung mit der Anwendung verwendet My2N App Aktivieren der Authentifizierung über Bluetooth.

PIN-Code / QR-Code

Die PIN dient als persönlicher numerischer Zugangscode, den der Benutzer über die Tastatur des Geräts eingibt oder der von der Kamera des Geräts in Form eines QR-Codes gescannt werden kann.

ACHTUNG
QR-Codes können nur mit der internen Kamera des Geräts gelesen werden.

PIN-Anforderungen

- Die Mindestlänge beträgt 2 Ziffern.
- Der Code kann nur Ziffern (0-9) enthalten.
- QR-Codes können nur für PINs mit einer Länge zwischen 4 und 15 Ziffern verwendet werden.
- Wenn Sie die Funktion **Stiller Alarm** verwenden, empfehlen wir Ihnen, geradzahlige PINs zu erstellen.

ANMERKUNG
Wenn Sie einen hexadezimalen QR-Code verwenden, muss der Wert vor der Eingabe in ein dezimales Format umgewandelt werden.

Akzeptierter Hexadezimalbereich: 1000 bis FFFFFFFF.

Fingerabdruck

Jeder Benutzer kann bis zu 2 Fingerabdrücke hochladen. Verwenden Sie zum Hochladen einen externen Fingerabdruckleser. Überprüfen Sie, ob Sie den Treiber installiert haben 2N USB Driver. Der Treiber steht zum Download bereit Hier.

Der hochgeladene Fingerabdruck eines Benutzers kann für die folgenden Aktionen verwendet werden:

- Öffne die Tür;
- Einen stillen Alarm starten – kann nur eingestellt werden, wenn die Türöffnungsfunktion aktiv ist;
- Automatisierung F1 und F2 – generiert das FingerEntered-Ereignis in der Automatisierung. F1 und F2 werden verwendet, um den angebrachten Finger in der Automatisierung zu unterscheiden.

Kennzeichen

Einige Geräte unterstützen die Kfz-Kennzeichenerkennung mit externen AXIS Kameras, die mit der Zusatzanwendung **VaxALPR** ausgestattet sind. Erkannte Nummernschilder werden in einer HTTP-Anfrage an den Endpunkt `api/lpr/licenseplate` gesendet (mehr HTTP-API-Handbuch für IP-Sprechanlagen).

TIPP
Die Vorgehensweise zum Hinzufügen einer externen Kamera wird unter ??? beschrieben.

Kennzeichen – legt das Kennzeichen des Fahrzeugs des Benutzers fest, das das Gerät scannen und zur Authentifizierung des Benutzers verwenden kann.

Anforderungen an das Nummernschild:

- Die maximale Länge eines Nummernschildes beträgt 10 Zeichen.
- Einem Benutzer können bis zu 20 Nummernschilder zugewiesen werden.
- Jedes Kennzeichen sollte nur einem Benutzer zugewiesen werden - wenn mehrere Zuweisungen vorgenommen werden, wird der erste gefundene Datensatz verwendet.
- Die Nummernschilder werden in der Erkennungsfunktion aus dem externen Kamerabild verwendet (siehe Handbuch Interoperabilität).

Virtuelle Karte

Die virtuelle Karte wird zur Identifizierung des Benutzers in Geräten verwendet, die über die Wiegand-Schnittstelle angeschlossen sind. Nach erfolgreicher Authentifizierung des Benutzers über die My2N-Anwendung oder den Biometrieleser wird die virtuelle Karten-ID an die Wiegand-Schnittstelle gesendet (wenn das Senden von Identifikatoren in der Konfiguration aktiviert ist, siehe **Access > Access Rules > Access/ Egress tab > Advanced**).

Anforderungen für virtuelle Karten:

- Die ID muss eine hexadezimale Zahl sein (Zeichen 0-9, A-F).
- Die Länge der ID beträgt 6 bis 32 Zeichen.
- Einem Benutzer kann gerade eine virtuelle Karte zugeordnet haben.

Schaltercode

Schaltercode – ermöglicht die Einstellung von bis zu 4 Codes zur Aktivierung von Schaltern (z. B. Türschloss). Der Schaltcode dient zum Öffnen des Schlosses über die Tastatur am Gerät sowie ein DTMF-Code.

Zutrittsregeln

Auf der Seite **Zugriff > Zugriffsregeln** werden die Parameter und die Logik für die Entriegelung der Tür festgelegt, die über den Türschalter des Geräts verwaltet wird. Diese Konfiguration legt fest, wie Zugriffsanfragen (Authentifizierung) bewertet werden, welche Bedingungen für eine erfolgreiche Benutzerautorisierung erforderlich sind und welche Regeln für die Verwaltung einzelner Zugriffe gelten.

Während Sie die einzelnen Berechtigungen in den Benutzereinstellungen festlegen, bestimmen die Zugriffsregeln, wann, unter welchen Bedingungen und wie diese Berechtigungen verwendet werden können. Sie können z.B. festlegen, ob der Türdurchgang nur in eine Richtung erlaubt ist, ob die Authentifizierung einen stillen Alarm auslösen kann oder ob sich der Benutzer nur einmal pro definiertem Zeitintervall authentifizieren kann.

Zustand von Tür und Schloss

Die Registerkarte Status zeigt an, ob der Türschalter aktiv ist und ob die Tür geöffnet ist.

Tür

- „Open“ - der Zugang wurde gewährt, der Türschalter ist geschlossen und die Tür kann geöffnet werden.
- „Geschlossen“ - die Tür ist verschlossen und kann nicht geöffnet werden.

Verriegelung

- „Unlocked“ - der Schalter ist aktiv, er kann bedient werden.
- „Gesperrt“ - der Schalter ist deaktiviert und kann nicht durch Zugriffsregeln gesteuert werden.

TIPP
Die Schaltfläche mit dem Schlosssymbol auf dieser Registerkarte dient zum Sperren bzw. Entsperren des Switches über die Weboberfläche.

Türerkennung

Auf der Registerkarte **Türen** können Sie festlegen, dass das unbefugte Öffnen einer Tür oder das Öffnen über einen längeren Zeitraum ein Ereignis auslöst. Dieses Ereignis kann dann durch Automatisierungen weiterverfolgt werden. Ereignisse werden auch in das Logo des Geräts geschrieben.

Ankunft und Abreise

Ein Gerät kann für die Verwaltung von Durchgängen in zwei Richtungen verwendet werden. Sie können einige Module an das Gerät auf der gegenüberliegenden Seite der Tür anbringen und dann diese beiden Seiten getrennt einstellen. So können Sie einschränken, zu welcher Tageszeit die Durchfahrt in der Richtung **Ankunft** und zu welcher Tageszeit die Durchfahrt in der Richtung **Abflug** erlaubt ist, oder welche Authentifizierungsmethoden in einer bestimmten Richtung akzeptiert werden, usw.

Modulzuweisung für Ankunft oder Abreise

1. Gehen Sie zu **Zugriff > Zugriffsregeln**.
2. Klicken Sie auf der Registerkarte **Ankunft** oder **Abreise** unter **Module** auf Verwalten.
3. Es öffnet sich ein Dialogfenster mit einer Liste der verfügbaren Zugangsverwaltungsmodule.
4. Ziehen Sie die Module per Drag & Drop in Gruppen entsprechend der Richtung, die sie bieten sollen.

TIPP
Klicken Sie auf , um ein bestimmtes Modul zu finden. Das Modul löst je nach seinen Fähigkeiten ein optisches oder akustisches Signal aus.

Zutrittsregeln

Zugriffsregeln bestimmen, welche Authentifizierungsmethoden für den Zugriff akzeptiert werden. Es können mehrere Zugriffsregeln für verschiedene Zeitprofile festgelegt werden. Zugriffsregeln können auch verwendet werden, um zu bestimmen, wann ein Zugriff verweigert werden sollte.

Sie können Zugriffsregeln verwenden, um die akzeptierten Authentifizierungsmethoden einzuschränken, z.B. können Sie Benutzer zwingen, von 8:00 bis 9:00 Uhr eine RFID-Karte zu verwenden.

TIPP
Die Authentifizierungsbeschränkung ist nützlich für ein Gerät, das Schlüssel für **2N IP Fortis** verwaltet. Die Benutzer werden daher gezwungen sein, die Schlüssel zu **2N IP Fortis** auf ihrer RFID-Karte regelmäßig zu aktualisieren.

Beim Einrichten der Regeln können Sie wählen, ob Sie einen Zonencode zum Öffnen der Tür verwenden möchten. **Der Zonencode** wird angewendet, wenn das Gerät in einer Massengeräteverwaltung (wie Access Commander) in Zonen eingeteilt wird. **Der Zonencode** kann auch manuell im Abschnitt **Erweiterte** eingestellt werden. Er funktioniert ähnlich wie der **Switch Activation Code**; wenn Sie ihn auf der Tastatur des Moduls eingeben, wird der Türschalter aktiviert.

Stiller Alarm

Der stille Alarm ist ein spezieller Modus zum Öffnen des Schlosses, mit dem Sie unauffällig eine Sicherheitsaktion auslösen können. Der stille Alarm wird vor allem in Räumlichkeiten und Gebäuden eingesetzt, die von Räubern gesucht werden - Kasinos, Finanzzentren, Banken usw. Nach Eingabe des PIN-Codes öffnet sich die Tür, aber gleichzeitig wird der Alarm aktiviert, ohne dass der Angreifer dies bemerkt.

Wenn Sie den stillen Alarm aktivieren, wird das Ereignis **SilentAlarm** ausgelöst. Auf dieses Ereignis kann zum Beispiel eine Automatisierung folgen:

- Senden einer HTTP-Anfrage an das Sicherheitssystem.
- Aufnehmen von Bildern mit der Kamera des Geräts.
- Aufbau eines Anrufs zu einem voreingestellten Ziel.

Aktivieren des stillen Alarms

1. Der Benutzer gibt einen Code ein, der um eins höher ist als seine normale PIN.
   Beispiel: Der Benutzer hat einen PIN-Code festgelegt „1926“. Geben Sie den Code „1927“ ein, um die Tür zu öffnen. Die Tür öffnet sich und das Ereignis SilentAlarm wird gleichzeitig ausgelöst.

ACHTUNG
Um die Tür mit einem PIN-Code öffnen zu können (auch wenn gleichzeitig der Stille Alarm ausgelöst wird), ist es notwendig, die Registerkarte **In/Out unter** zu aktivieren.

Sperrung des Zugriffs nach fehlgeschlagenen Versuchen

Nach fünf aufeinanderfolgenden erfolglosen Zugriffsversuchen wird der Zugriff für 30 Sekunden gesperrt. Während dieses Zeitraums ist der Zugriff nicht möglich, selbst wenn die Benutzerauthentifizierung gültig ist.

Diese Funktion blockiert nur den Zugriff durch eine Benutzerautorisierung. Der Türschalter kann auch durch andere Methoden wie DTMF, HTTP-Befehl usw. geschaltet werden.

Lesen von QR-Codes

Der dem Benutzer zugewiesene Zugangs-PIN-Code oder Schalteraktivierungscode kann von der Kamera in Form eines QR-Codes gelesen werden.

Zum korrekten Laden müssen Sie **QR-Code-Lesemodus** einstellen. Die Codes werden im Gerät immer im Dezimalformat gespeichert. Beim Lesen im Dezimalmodus müssen die gelesenen QR-Codes genau mit den im Gerät gespeicherten PIN-Codes (4 bis 15 Ziffern lang) übereinstimmen. Im Hexadezimalmodus werden QR-Codes nach dem Lesen in das Dezimalzahlenformat umgewandelt und dann mit den gespeicherten Dezimalcodes verglichen. Vorangestellte Nullen werden beim hexadezimalen Lesen ignoriert.

ANMERKUNG
Akzeptierter Hexadezimalbereich: 1000 bis FFFFFFFF.

Für das Lesen von QR-Codes können Sie auch festlegen, dass nur das Ereignis **CodeEntered** ausgelöst wird, anstatt den Türschalter zu steuern. Dieses Ereignis kann dann über Automationen mit weiteren Aktionen verfolgt werden.

Der gescannte QR-Code kann an ein externes Zugangskontrollsystem weitergeleitet werden, das über eine Wiegand-Schnittstelle kommuniziert (siehe ???).

Anti-Passback

Anti-Passback ist eine Erweiterung des Zugangskontrollsystems, die den erneuten Zutritt während eines festgelegten Zeitintervalls verhindert. In diesem Modus erlaubt das Gerät dem Benutzer nur eine einmalige Eingabe innerhalb einer bestimmten Zeit. Nachdem ein Benutzer das System erfolgreich betreten hat, zeichnet das System dieses Ereignis auf und der Benutzer kann erst wieder auf das System zugreifen, wenn die angegebene Zeit verstrichen ist. Diese Zeit wird eingestellt, wenn Anti-Passback aktiviert ist.

Anti-Passback-Modi:

- „Hard“ - Der Benutzer kann das Gerät für die eingestellte Zeitspanne in keiner Richtung passieren. Dem Benutzer wird der Zugriff verweigert, bis das Intervall abläuft oder der Zugriff vom Geräteadministrator wiederhergestellt wird.
- „Soft“ - Regelverstöße werden nur protokolliert und können den Administrator alarmieren, aber dem Benutzer wird der Zugriff gestattet.

Datenübertragung für Wiegand

ACHTUNG
Um Wiegand-Daten weiterzuleiten, muss ein Wiegand-Erweiterungsmodul ordnungsgemäß an das Gerät angeschlossen sein. Das Wiegand-Erweiterungsmodul ist in der Regel nicht im Lieferumfang des Produkts enthalten.

Die Wiegand-Weiterleitungsfunktion ermöglicht es dem Gerät, die Identifikationsdaten des authentifizierten Benutzers an ein externes Zugangskontrollsystem weiterzuleiten, das über die Wiegand-Schnittstelle kommuniziert. Dies ermöglicht die Integration von 2N Geräten in herkömmliche Zugangskontrollsysteme. Mit dieser Einstellung können Sie die entsprechende Gruppe für die Datenweiterleitung auswählen.

Die Datenweiterleitung für Wiegand wird unter **Access > Access Rules > I/O > Advanced** eingerichtet. Das Senden von Berechtigungen an Benutzer, die ihren QR-Code gelesen haben, wird auf der Registerkarte **Access/Exit** für die Aktivierung des QR-Code-Lesens eingestellt.

Einstellung des Türschalters

Der Türschalter ist eine logische Funktion des Geräts, das das elektrische Türschloss steuert. Der Schalter kann auf verschiedene Arten aktiviert werden (z.B. per HTTP-Befehl, RFID-Karte oder DTMF-Signal).

Die Funktion des Türschalters im Gerät wird von **Switch 1** übernommen.

Auf der Seite **Access > Modules** können Sie dann ein bestimmtes Zugangsmodul zur Steuerung eines anderen Switches zuweisen.

Einstellung des Türschalters

1. Verbinden Sie die elektrischen Türschlosskontakte (z.B. Magnetkontakt) mit dem dafür vorgesehenen Eingang an der Gegensprechanlage.
2. Gehen Sie in der Web-Konfigurationsoberfläche zu **Integration > Switches**.
3. Öffnen Sie die Einstellungen von Schalter 1, indem Sie auf den Pfeil in der Registerkartenüberschrift klicken.

4. Auf der Registerkarte **Konfiguration des Schalters** stellen Sie die Parameter des Hardware-Ausgangs ein, den der Türschalter steuern soll.
   - **Gesteuerter Ausgang** - gibt den Ausgang an, der das elektrische Türschloss schaltet.
   - **Modus** - Monostabil / Bistabil.
   - **Einschaltzeit**– hier wird die Einschaltzeit des Schalters im monostabilen Modus eingestellt. Die eingestellte Schaltzeit wird nicht im bistabilen Modus angewendet.
   - **Ausgangstyp** - im Modus „Security“ arbeitet der Ausgang im invertierten Modus, d.h. er ist permanent eingeschaltet und steuert das Security-Relais mit einer bestimmten Impulsfolge. Wenn Sie ein umgekehrtes Türschloss verwenden (d.h. das Schloss ist verriegelt, wenn der Strom eingeschaltet wird), stellen Sie den Ausgangstyp auf „Umgekehrt“ ein.

   TIPP
   Wenn Sie ein Sicherheitsrelais verwenden, stellen Sie den Ausgangstyp auf „Security“ ein.

   Wenn mehrere Schalter mit unterschiedlich eingestelltem Ausgangstyp an einen Ausgang angeschlossen sind, werden sie nach der folgenden Priorität gesteuert:

   1. Sicherheit
   2. Inverted
   3. Normal
5. Auf den Registerkarten **Aktivierung** und **Aktivierungscodes** können Sie zusätzliche Möglichkeiten zur Aktivierung des Schalters festlegen. Wenn Sie keine anderen Methoden festlegen, wird der Schalter nur aktiviert, wenn Sie den Benutzerzugriff erlauben.
6. Speichern Sie die Änderungen.

Module

Die Seite **Access > Modules** bietet eine zentrale Verwaltung aller Zugangshardwaretechnologien auf dem Gerät. Jedes Modul hat eine eigene Registerkarte auf der Seite, die seine Verwaltung ermöglicht. Hier werden sowohl Module verwaltet, die direkt in die Haupteinheit des Geräts integriert sind, als auch solche, die über VBUS angeschlossen sind.

Jedes Modul kann benannt und einem bestimmten Schalter zur Steuerung zugewiesen werden. Andere Parameter hängen von der Art des Moduls ab.

In der Werkseinstellung steuern alle Module den Türschalter.

ANMERKUNG
Wenn die Firmware-Versionen des anzuschließenden Moduls und des Hauptgeräts nicht kompatibel sind, wird das Modul nicht erkannt. Aktualisieren Sie in diesem Fall die Gerätefirmware (Aktualisierung der Firmware (S. 13)), nachdem Sie das Modul angeschlossen haben.

Bluetooth-Zugang einrichten

Die Benutzerauthentifizierung über Bluetooth erfolgt über die My2N app, die der Nutzer auf sein Mobiltelefon heruntergeladen haben muss.

GET IT ON Google Play Download on the App Store

ACHTUNG
Die Einstellung des Pairing-Codes muss derzeit in der alten Konfigurationsoberfläche vorgenommen werden.

Erstellen Sie einen Pairing-Code auf dem Gerät

1. Gehen Sie auf **Verzeichnis** und öffnen Sie das Detail des Benutzers, für den Sie den passenden Code erstellen möchten.
2. Klicken Sie in der Kopfzeile der Webkonfigurationsoberfläche auf . Gehen Sie zur alten Schnittstelle.
   Öffnet das Benutzerdetail in der alten Konfigurationsoberfläche.
3. Klicken Sie im Block **WaveKey** auf  .
   In dem sich öffnenden Dialogfeld wird ein Pairing-Code generiert, den Sie in der Anwendung My2N auf Ihrem Gerät eingeben müssen.
4. Öffnen Sie die App und geben Sie die Kopplungs-PIN ein.

   ANMERKUNG
   Wenn Sie bereits eine App mit einem anderen Gerät verbunden haben, können Sie die Pairing-PIN über das Hinzufügen-Symbol oben auf dem Bildschirm eingeben.

5. Folgen Sie den Anweisungen auf Ihrem Mobiltelefon - nähern Sie sich dem Gerät im Kopplungsmodus und klicken Sie auf Kopplung starten.

WARNUNG
Bei Mobiltelefonen mit älteren Betriebssystemen (Android 9 / iOS 17 und niedriger) müssen Sie zum Koppeln die Anwendung verwenden Mobiler Schlüssel.

Kopplung in der mobilen App Mobiler Schlüssel

1. Laden Sie die App herunter Mobile Key auf Ihr Mobiltelefon. Den Antrag gibt es unter App Store Und Google Play.
2. Öffnen Sie die App und aktivieren Sie die App Mobiler Schlüssel Zugriff auf Bluetooth.
3. Je nach Art des mobilen Schlüssels nähern Sie sich dem USB-Leser oder dem Kopplungsgerät mit dem Mobiltelefon.
4. In der App Mobiler Schlüssel Klicken Sie zum Koppeln auf das angebotene Gerät.
5. Die Anwendung fordert Sie zur Eingabe eines PIN-Codes auf. Geben Sie den Pairing-Code ein und bestätigen Sie die Eingabe.

Bluetooth-Authentifizierungsmethoden

In der Web-Konfigurationsoberfläche können verschiedene Bluetooth-Authentifizierungsmethoden eingestellt werden.

- **Direkt in der mobilen App** - der Benutzer wählt die Tür, die er öffnen möchte, direkt in der My2N Mobile App aus. Wenn sich sein mobiles Gerät in Reichweite des 2N Geräts befindet, verbindet es sich mit dem Gerät und wenn die Zugangsregeln erfüllt sind, wird die Tür entriegelt.

- **Indem Sie das Mobiltelefon in die Nähe des Geräts bringen und das Gerät berühren** - ein Benutzer mit einem mobilen Gerät und aktiviertem Bluetooth nähert sich dem 2N Gerät und berührt die Bluetooth-Authentifizierungsstelle auf dem 2N Gerät, die normalerweise mit dem Bluetooth-Symbol gekennzeichnet ist. Sobald die Verbindung hergestellt ist und die Zugriffsrechte überprüft wurden, wird die Tür entriegelt.
- **Bewegungserkennung** - 2N Geräte mit einer Kamera erkennen Bewegungen in der Umgebung und aktivieren automatisch Bluetooth. Wenn ein 2N Gerät das mobile Gerät eines Benutzers mit gültigem Zugang in Reichweite erkennt, wird die Tür entriegelt.

Akzeptierte Bluetooth-Authentifizierungsmethoden einstellen

1. Gehen Sie zu **Zugriff > Module**.
2. Auf der Registerkarte **für das Bluetooth-Modul** wählen Sie die möglichen Methoden im Feld **Start Authentication** aus.
3. Wenn Sie „Bewegungserkennung“ gewählt haben, wählen Sie das Profil aus, mit dem die Bewegung erkannt werden soll.

ANMERKUNG
Bewegungserkennungsprofile werden unter **Anpassung > Kamera > Interne Kamera** eingestellt.

Aufzugsteuerung

Durch den Anschluss des Relaismoduls AXIS A9188 an eine 2N Sprechanlage (2N IP Verso, 2N IP Force, 2N IP Safety, 2N IP Vario) oder an eine Access Unit kann der Zugang zu den einzelnen Etagen eines Gebäudes über den Aufzug gesteuert werden. Maximal 8 dieser Relaismodule können an eine 2N Sprechanlaege oder Access Unit angeschlossen werden, von denen jedes 8 Etagen steuern kann, also insgesamt 64 Etagen. Um diese Funktion nutzen zu können, müssen Sie über eine aktive 2N IP Intercom Lizenz (Best.-Nr. 9137916) und Access Unit Lizenz (Best.-Nr. 9160401) verfügen.

Anschluss an den Aufzug

1. Schließen Sie die Eingänge der Aufzugssteuerungen an das AXIS A9188 Relais an und verbinden Sie das Relais mit dem IP-Netzwerk. Notieren Sie sich die IP-Adresse des Relais.
   Folgen Sie der Dokumentation für das AXIS A9188 E/A-Relaismodul, die Sie unter http://www.axis.com finden.
2. Öffnen Sie die Web-Konfigurationsoberfläche des 2N Geräts, das die Aufzugszugänge verwalten soll.
3. Gehen Sie zu **Integration > Zutrittskontrolle > Registerkarte Aufzug**.
4. Aktivieren Sie auf der Registerkarte **Relaismodule (AXIS A9188)** eines der Module.
5. Klicken Sie auf das Bleistiftsymbol und geben Sie die IP-Adresse des Relaismoduls in das sich öffnende Feld ein.
6. Wenn der Zugriff auf das Relais einer Authentifizierung unterliegt, geben Sie den Benutzernamen und das Passwort auf der Registerkarte **Allgemein** ein.
7. Wenn das Relaismodul aktiviert ist, erscheinen die Etagen, die dieses Modul verwaltet, auf der Registerkarte **Elevator Floors**. Sie können jedes Stockwerk benennen.

Einrichtung eines öffentlichen Zugangs zum Boden

1. Wählen Sie auf der Registerkarte **Elevator Floors** die Etagen aus, die für die Öffentlichkeit zugänglich sein sollen (der Zugang ist nicht genehmigungspflichtig).
2. Klicken Sie auf das Bleistiftsymbol neben der ausgewählten Etage.

3. Aktivieren Sie in den offenen Einstellungen **Public Access.**
4. Optional können Sie die öffentliche Zugriffszeit begrenzen, indem Sie ein Zeitprofil auswählen oder eine eigene Zugriffszeit festlegen.

Einrichtung der Nummernschild-Authentifizierung

Einige Geräte unterstützen die Kfz-Kennzeichenerkennung mit externen AXIS Kameras, die mit der Zusatzanwendung **VaxALPR** ausgestattet sind. Erkannte Nummernschilder werden in einer HTTP-Anfrage an den Endpunkt `api/lpr/licenseplate` gesendet (mehr HTTP-API-Handbuch für IP-Sprechanlagen).

TIPP
Die Vorgehensweise zum Hinzufügen einer externen Kamera wird unter ??? beschrieben.

Aktivieren von HTTP-API-Diensten

Die Authentifizierung des Kennzeichens wird anhand der HTTP-Anfrage ausgewertet. Daher müssen Sie die entsprechenden HTTP-API-Dienste auf dem Gerät aktivieren. Diese Einstellung wird noch in einer älteren Version der Web-Konfigurationsoberfläche vorgenommen. Die detaillierte Vorgehensweise finden Sie unter FAQ.

Einstellungen anzeigen

So laden Sie Ihre eigene Anzeigesprache hoch

Über die webbasierte Konfigurationsschnittstelle können Sie die auf dem Gerätedisplay angezeigten Sprachtexte anpassen. Auf diese Weise können Sie das Gerät an eine andere Sprachumgebung anpassen oder benutzerdefinierte Nachrichten anzeigen.

1. Gehen Sie in der Web-Konfigurationsoberfläche auf **Anpassung > Anzeige**.
2. Auf der Registerkarte **Sprache** können Sie die Vorlage für die Übersetzungsdatei herunterladen. Die Vorlage enthält englische Standardtexte.
3. Öffnen Sie die heruntergeladene Datei in einem Texteditor.
4. Ersetzen Sie die englischen Ausdrücke in der Datei durch Ihre eigenen Texte.

   ACHTUNG
   Ändern Sie nicht die Struktur und das Format der Schlüsselsätze. Wenn die Syntax geändert wird oder einige Elemente fehlen, wird die Übersetzungsdatei möglicherweise nicht korrekt geladen.

5. Speichern Sie die geänderte Datei im Format `.ini`.
6. Kehren Sie zur Registerkarte **Sprache** in der Weboberfläche zurück und wählen Sie „Benutzerdefiniert“ aus dem Dropdown-Menü Sprache.
7. Die Option zum Hochladen von Dateien wird angezeigt - wählen Sie Ihre geänderte `.ini` Datei aus und laden Sie sie hoch.
8. Speichern Sie die Änderungen nach erfolgreichem Upload.

Diashow

ANMERKUNG
Auf dem **2N IP Style** Display können neben der Präsentation auch andere Demonstrationsmodi eingestellt werden (siehe Demo-Modus (**2N IP Style**) (S. 31)).

Präsentation ist ein Demonstrationsmodus, der eine Abfolge von Bildern und Videos auf dem Bildschirm anzeigt. Sie können die Anzeigezeit für jedes Element (Bild oder Video) einstellen.

1. Gehen Sie zu **Anpassung > Anzeige**.
2. Aktivieren Sie die Funktion in der Kopfzeile der Registerkarte **Präsentation**.
3. Legen Sie fest, wie lange der Startbildschirm im Vorschaumodus angezeigt werden soll.
4. Für jedes Element können Sie angeben, ob es nur in einem bestimmten Zeitfenster oder außerhalb davon angezeigt werden soll. Um eine Ansicht nach Zeitfenster zu erhalten, klicken Sie auf Präsentation bearbeiten. Erweitern Sie das erweiterte Menü, indem Sie auf ⋮ für ein bestimmtes Element klicken, um festzulegen, wann das Element in der Präsentation angezeigt werden soll.
5. Speichern Sie die Änderungen.

Demo-Modus (2N IP Style)

Der Demo-Modus auf **2N IP Style** ist der Anzeigezustand, in den das Gerät nach einer bestimmten Zeit der Inaktivität auf dem Startbildschirm übergeht. Das Display des Geräts kann zum Beispiel eine Reihe von Bildern oder Videos, die Adresse eines Gebäudes oder das Datum und die Uhrzeit anzeigen.

ANMERKUNG
Nach 2 Minuten Inaktivität wird der Displayschoner des Geräts ausgelöst, bei dem die Helligkeit des Displays in 20-Sekunden-Intervallen abwechselnd verringert und erhöht wird. Der Schoner wird durch eine Berührung des Displays, einen Zugriffsversuch, einen eingehenden Anruf, eine Benachrichtigung auf dem Display oder eine Bewegungserkennung beendet, auch wenn die Bewegungserkennung nicht aktiviert ist. Wenn der Bildschirmschoner im Hintergrund im Vorschaumodus läuft, schaltet das Gerät beim Beenden des Bildschirmschoners durch Berühren auch auf die Startseite um.

Einstellungen für den Vorschaumodus

1. Gehen Sie zu **Anpassung > Anzeige**.
2. Aktivieren Sie in der Kopfzeile der Registerkarte **die Funktion** Vorschaumodus.
3. Legen Sie fest, wie lange der Startbildschirm im Vorschaumodus angezeigt werden soll.
4. Wählen Sie die gewünschte Art des Probenmodus.
5. Sie können die Anzeige von Informationspiktogrammen über die antibakterielle Oberfläche oder das Berührungssymbol im Bereich **Icon Display auf** aktivieren.
6. Speichern Sie die Änderungen.

Diashow

Präsentation ist ein Demonstrationsmodus, der eine Abfolge von Bildern und Videos auf dem Bildschirm anzeigt. Sie können die Anzeigezeit für jedes Element (Bild oder Video) einstellen.

Für jedes Element können Sie angeben, ob es nur in einem bestimmten Zeitfenster oder außerhalb davon angezeigt werden soll. Um eine Ansicht nach Zeitfenster zu erhalten, klicken Sie auf Präsentation bearbeiten. Erweitern Sie das erweiterte Menü, indem Sie auf ⋮ für ein bestimmtes Element klicken, um festzulegen, wann das Element in der Präsentation angezeigt werden soll.

Logo

Logo-Modus wird verwendet, um ein statisches Firmenlogo auf dem Bildschirm anzuzeigen.

Sie können ein Hintergrundbild für die Anzeige (hinter dem Logo) auf der Registerkarte **Hintergrundbild** hochladen.

Text

Der Modus **Text** zeigt statischen Text auf dem Bildschirm an, z.B. die Adresse der Einrichtung, eine Begrüßungsnachricht oder andere Informationen für Personen, die sich in der Einrichtung bewegen.

Datum und Uhrzeit

Modus **Datum und Uhrzeit** zeigt das Datum, die aktuelle Uhrzeit des Geräts und den Standort des Geräts an.

Informative Berichte (2N IP Style)

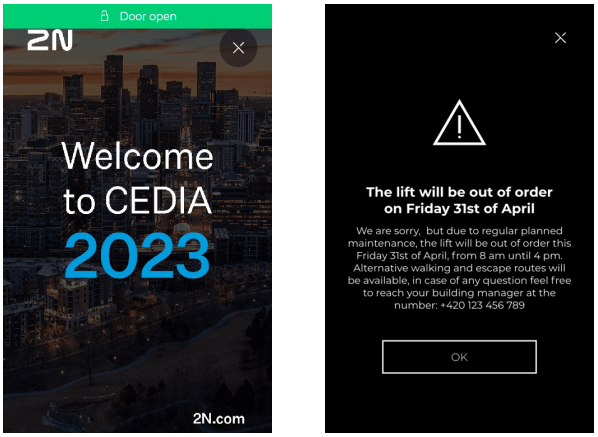
Das Gerät **2N IP Style** kann voreingestellte Informationsmeldungen auf seinem Display anzeigen. Den Benutzern oder Besuchern kann dann nach der Erteilung des Zutritts eine Nachricht angezeigt werden, die sie durch das Gebäude führt, sie über Veranstaltungen im Gebäude informiert usw.

Auf jeder Registerkarte können Sie spezifische Informationsmeldungen für jedes der folgenden Ereignisse einstellen:

- **Autorisierter Benutzer** - Diese Meldung erscheint auf dem Display, nachdem sich ein im Geräteverzeichnis gespeicherter Benutzer am Gerät authentifiziert hat.
- **Besucher** – diese Meldung erscheint, wenn ein Besucher während eines Anrufs Zutritt erhält. Ein Besucher ist eine Person, die einen Anruf vom Gerät zu einem Benutzer im Verzeichnis ausgelöst hat. Die Meldung erscheint, wenn dieser Benutzer dem Besucher während des Anrufs Zugang gewährt.
- **Zugriff verweigert** – diese Meldung wird angezeigt, wenn das Gerät den Zugriff verweigert.

Einstellungen für Informationsnachrichten

1. Gehen Sie zu **Zugang > Newsletter**.
2. Wählen Sie auf den Registerkarten die Art der Informationsmeldung aus, die Sie einrichten möchten.
3. Aktivieren Sie die Informationsmeldung in der Kopfzeile der Registerkarte.
4. Legen Sie auf der Registerkarte **Zeitplanung und Zeiteinstellungen** die Zeit fest, zu der die Zeitnachricht angezeigt werden soll, und auch, wie lange die Informationsnachricht auf dem Display bleiben soll. Sie können auch den Kalenderzeitraum angeben, für den die Nachricht angezeigt werden soll.
5. Auf der Registerkarte **Nachrichteninhalt von** erstellen Sie eine Nachricht. Sie können entweder eine Textnachricht erstellen oder ein Bild einfügen.
6. Speichern Sie die Änderungen.



Beispiel für eine Informationsnachricht mit Bild und Text

Erweiterte Einstellungen

Kamera- und Videoeinstellungen

Die Kamera in 2N Gegensprechanlagen überträgt das Bild während eines Videogesprächs an den Gesprächspartner, erkennt Bewegungen in der Umgebung und liest QR-Codes,

Es ist möglich, externe Kameras an das Gerät anzuschließen, von denen Sie dann das Bild anzeigen lassen können. Während eines Anrufs können Sie zusätzlich zum Video des angerufenen Geräts die Ansicht einer weiteren Kamera sehen.

Es ist möglich, externe Kameras an das Gerät anzuschließen, von denen Sie dann das Bild lesen können.

Interne Kameraeinstellungen

1. Gehen Sie zu **Anpassung > Kamera**.
2. Auf der Registerkarte **Interne Kamera** klicken Sie auf →.
3. Auf der Registerkarte **Einstellungen** können Sie grundlegende Bildparameter der Kamera bearbeiten.
4. Nach dem Speichern werden die Änderungen in der Kameravorschau angezeigt.

Modus

Im Kameramodus können Sie die optimale Kombination aus Belichtungsmodus und Leistungsfrequenz einstellen, um stabile und hochwertige Bilder zu erzielen. Dieser Modus wird verwendet, um unerwünschtes Flackern zu reduzieren, das bei künstlicher Beleuchtung oder bei Schwankungen der Netzfrequenz auftreten kann. Bei der Installation von Kameras in Innenräumen kann eine geeignete Methode zur Unterdrückung von durch Lichtquellen verursachtem Flimmern ausgewählt werden, während bei der Aufstellung im Freien ein Modus zur Unterdrückung von direktem Sonnenlicht aktiviert werden kann, um eine optimale Bildanpassung an die aktuellen Lichtverhältnisse zu gewährleisten.

IR LED

Die IR-LED-Hintergrundbeleuchtung sorgt auch bei schwachem Umgebungslicht für ein hochwertiges Bild. Dieser Modus wird ausgelöst, wenn die Lichtverhältnisse unter den eingestellten Wert fallen. Der Grenzwert für die Lichtverhältnisse wird erst festgelegt, nachdem die IR-LED-Beleuchtung aktiviert wurde.

ANMERKUNG
Wenn der zulässige Stromverbrauch überschritten werden könnte - zum Beispiel, wenn mehrere PoE-betriebene Erweiterungsmodule gleichzeitig in Betrieb sind - wird der IR-Strompegel automatisch optimiert, um die Stabilität des Geräts zu erhalten.

Erweiterte Einstellung

Tag/Nacht-Modus - ermöglicht es Ihnen, je nach Lichtverhältnissen zwischen Farb- und Schwarzweißbildern zu wechseln. Stellen Sie **Immer Tag** ein, wenn Sie möchten, dass die Kamera einen IR-Unterdrückungsfilter verwendet und die IR-Hintergrundbeleuchtung ausgeschaltet ist. Die Einstellung "Immer Nacht" hingegen schaltet den Filter aus und schaltet die IR-Beleuchtung ein, wodurch das Bild in einen Schwarz-Weiß-Modus umgeschaltet wird, der für die Nachtsicht geeignet ist. Der Auto-Modus schaltet die Kamera je nach Umgebungslicht zwischen diesen beiden Zuständen um.

Lokaler Kontrast - hebt Details und Texturen hervor, indem die Helligkeitsunterschiede zwischen benachbarten Bildbereichen (Kanten) verstärkt werden.

Tone Mapping - erhöht die Helligkeit und Sichtbarkeit des Bildes, kann aber leichte Farbverzerrungen verursachen.

Maximale Belichtungszeit - Legt die maximale Belichtungszeit für das Bild fest. Wenn mehr Licht verfügbar ist, ist der Verschluss möglicherweise nicht immer geöffnet und die Kamera stellt automatisch eine kürzere aktuelle Belichtungszeit ein.

Bewegungserkennung

Die Bewegungserkennung auf 2N Geräten ist eine Funktion, die automatisch Bewegungen im Sichtfeld der internen Kamera erkennt und Ihnen ermöglicht, verschiedene Aktionen auszulösen, wie z.B. die Aktivierung von Bluetooth oder das Senden einer Benachrichtigung.

Für eine optimale Leistung kann die Erkennung auf die Umgebung und die Bedingungen kalibriert werden, z. B. durch Änderung der Empfindlichkeitsparameter und des von der Kamera zu überwachenden Bereichs.

Einstellungen der Bewegungserkennung

1. Gehen Sie zu **Anpassung > Kamera**.
2. Auf der Registerkarte **Interne Kamera** klicken Sie auf .
3. Klicken Sie auf der Registerkarte **Kamera-Vorschau** auf das Stiftsymbol neben dem Parameter **Bewegungserkennung**.
4. Es öffnet sich ein Fenster mit den Einstellungen für das Bewegungserkennungsprofil.
5. Erweitern Sie die Registerkarte des Profils, das Sie einrichten möchten.
6. Indem Sie das Quadrat in der Kameravorschau eines bestimmten Bereichs anpassen, in dem die Kamera Bewegungen aufnehmen soll.

> **ACHTUNG**
> Der Bildbereich ist relativ zum aktuellen Bildausschnitt. Wenn Sie den Ausschnitt des Kamerabildes ändern, bleiben die vorhandenen Bereiche gleich, decken aber effektiv einen anderen Teil des Raums ab. Es ist daher immer empfehlenswert, diese Bereiche nach der Bearbeitung eines Ausschnitts zu überprüfen und anzupassen.

7. Wählen Sie den Motion-Capture-Modus für das Profil, siehe Profil-Modi (S. 34)
8. Passen Sie ggf. weitere Parameter an, je nach Modus.
9. Denken Sie immer daran, das Profil zu aktivieren!
10. Um Ihre Änderungen zu speichern, klicken Sie oben auf der Seite auf die Schaltfläche **Speichern** oder **Speichern und schließen**.

Profil-Modi

Auslösen der Ereignisse

In diesem Modus nimmt die Kamera sofortige, einmalige Bewegungen auf. Ein Anwendungsbeispiel ist die Aufnahme eines Bildes, wenn jemand den Raum betritt oder wenn ein Fahrzeug in der Nähe des Geräts vorbeifährt.

Die Aktivierung des ausgelösten Ereignisses kann mit Hilfe der eingestellten Verzögerung verzögert werden.

Verwenden Sie den Filter, um die Arten von Bewegungen zu definieren, die die Kamera ignorieren soll - zum Beispiel kleine Objekte (kleine Vögel) oder sich wiederholende Bewegungen (Bäume im Wind).

Upload läuft...

Dieses Profil löst ein Ereignis von 30 Sekunden aus, wenn eine Bewegung erkannt wird. Wenn während dieser Zeit eine weitere Bewegung stattfindet, fasst das Profil alles zu einem Ereignis zusammen. Dieser

Modus eignet sich für die kontinuierliche Überwachung und verhindert die Erstellung einer großen Anzahl von kurzen Aufzeichnungen.

Verwenden Sie den Filter, um die Arten von Bewegungen zu definieren, die die Kamera ignorieren soll - zum Beispiel kleine Objekte (kleine Vögel) oder sich wiederholende Bewegungen (Bäume im Wind).

Gesichtserkennung

Das Profil erkennt eine Bewegung, wenn ein Gesicht im überwachten Bereich erscheint. Ein Ereignis kann auch eintreten, wenn ein statisches Bild eines Gesichts (z.B. ein Foto) im Rahmen erscheint.

Erkennung von ankommenden Personen

Das Profil erkennt nur sich bewegende Personen und ignoriert statische Bilder von Gesichtern.

Datenschutzbestimmungen

Die Privatsphärenfunktion maskiert einen Teil des Bildes, so dass dieser nicht sichtbar ist oder im Video aufgezeichnet wird. Diese Option ist ideal für Situationen, in denen Sie z. B. sensible Bereiche des Bildes schützen möchten. Wenn das Gerät beispielsweise an der Rezeption aufgestellt ist und die Kamera auch den Flur erfasst, in dem sich Fremde bewegen, können Sie den Flurbereich ausblenden.

ACHTUNG
Der Schutz der Privatsphäre kann die Aktivität des Lesens von QR-Codes oder die Bewegungserkennung einschränken. Es wird nicht empfohlen, den Schutz der Privatsphäre gleichzeitig mit diesen Funktionen zu verwenden.

Einstellungen der Bewegungserkennung

1. Gehen Sie zu **Anpassung > Kamera**.
2. Auf der Registerkarte **Interne Kamera** klicken Sie auf →.
3. Klicken Sie auf der Registerkarte **Kamera-Vorschau** auf das Stiftsymbol neben dem Parameter **Datenschutz**.
4. Passen Sie in der Kameravorschau das Quadrat so an, dass es den Bereich abdeckt, den Sie maskieren möchten.

   ACHTUNG
   Der Bildbereich ist relativ zum aktuellen Bildausschnitt. Wenn Sie den Ausschnitt des Kamerabildes ändern, bleiben die vorhandenen Bereiche gleich, decken aber effektiv einen anderen Teil des Raums ab. Es ist daher immer empfehlenswert, diese Bereiche nach der Bearbeitung eines Ausschnitts zu überprüfen und anzupassen.
5. Wählen Sie den Tarnmodus:
   - **Farbe** - der ausgewählte Bereich wird mit der Farbe Ihrer Wahl überlagert.
   - **Mosaik** - der ausgewählte Bereich wird verpixelt. Legen Sie die Größe des Mosaiks entsprechend dem erforderlichen Grad der Datenanonymisierung fest.
6. Vergessen Sie nicht, den Schutz der Privatsphäre in der Kopfzeile der Parametereinstellungen zu aktivieren!
7. Um Ihre Änderungen zu speichern, klicken Sie oben auf der Seite auf die Schaltfläche **Speichern** oder **Speichern und schließen**.

Externe Kamera

Die externe Kamera wird dem 2N Gerät als Videostream (RTSP) hinzugefügt. Wenn Sie eine externe Kamera anschließen, können Sie während eines Gesprächs zwischen den Ansichten wechseln. Die Funktion der externen Kamera ist also rein bildgebend.

ACHTUNG
QR-Codes können nur mit der internen Kamera des Geräts gelesen werden.

Hinzufügen einer externen Kamera

1. Gehen Sie zu **Anpassung > Kamera**.
2. Wählen Sie unter der Registerkarte **Externe Kamera** Kamera hinzufügen.
3. In dem sich öffnenden Dialogfenster aktivieren Sie die Kamera.
4. Geben Sie die Stream-Quelladresse der externen IP-Kamera im Format `rtsp://ip_address_camera/parameters` ein.
5. Wenn der externe Kamerastream einer Authentifizierung unterliegt, füllen Sie **mit den Anmeldedaten für den Stream**.
6. Speichern Sie Ihre Änderungen, indem Sie auf Kamera hinzufügen klicken.
7. Wenn die externe Kamera die Hauptkamera des Geräts sein soll, dann klicken Sie nach dem Speichern auf der Registerkarte **Externe Kamera** auf Als Standardquelle festlegen.
   Wenn Sie mit dem Gerät sprechen, wird das Bild der Kamera, die als Standardquelle eingestellt ist, zuerst angezeigt.

Erstellen Sie einen Videostream von der Gerätekamera

Die IP-Video-Streaming-Funktion wird verwendet, um Live-Videos von der Kamera des Geräts über das Netzwerk an ein Empfangsgerät wie eine mobile App, eine Tracking-Software oder auf einem Computer in einem Video-Player zu übertragen. Dieses Verfahren stellt sicher, dass Benutzer Videos in Echtzeit von einer Vielzahl von Geräten aus ansehen können.

Erstellen eines Videostreams

1. Gehen Sie zu **Integration > ONVIF / RTSP**.
2. Aktivieren Sie den **RTSP-Serverdienst**.
3. Stellen Sie die Stream-Parameter ein, siehe Video-Stream-Parameter (S. 36).
4. Auf der Registerkarte **Verbindungseinschränkungen** können Sie die IP-Adressen eingeben, von denen der Stream verfügbar sein soll. Wenn keine IP-Adressen eingetragen sind, können Sie sich von jeder IP-Adresse aus verbinden.
5. Auf der Registerkarte **Vorkonfigurierte Streams** geben Sie an, ob der Stream zugänglich sein soll:
   - Anonym
   - mit Authentifizierung - legen Sie die Authentifizierungsdetails auf der Registerkarte **Authentifizierung** fest.
6. Auf der Registerkarte **Vorkonfigurierte Streams** finden Sie die IP-Adressen der konfigurierten Streams entsprechend dem ausgewählten Videocodec.

Video-Stream-Parameter

Allgemeine Stream-Einstellungen

Jitter Kompensation- Legt die Pufferlänge fest, um ungleichmäßige Intervalle zwischen eingehenden Audiopaketen auszugleichen. Ein längerer Speicher bedeutet höhere Ausfallsicherheit, aber auch mehr Audioverzögerung.

Wert QoS DSCP – stellt die Priorität der RTP-Video-Pakete im Netz ein. Der eingestellte Wert wird im Feld TOS (Type of Service) im Kopf des IP-Pakets abgesendet.

Freigabe des Modus UDP Unicast – erlaubt den Modus des Datenabsendens des Audio-und Videostreams mittels des RTP/UDP-Protokolls. Ist dieser Modus ausgeschalten, werden die Audio/Video-Stream-Daten nur über RTP/RTSP gesendet.

Ausgangs-RTP-Port– Legen Sie den anfänglichen lokalen RTP-Port im 60-Port-Bereich für die Audio- und Videoübertragung fest. Der voreingestellte Wert ist 4800 (d. h. der verwendete Bereich liegt bei 4800-4859).

Zipstream - wählt das voreingestellte Kompressionsniveau des Zipstream (für H.264) aus. AXIS Zipstream bewahrt alle wichtigen forensischen Details, die Sie benötigen, und reduziert gleichzeitig die Datenübertragungs- und Speicheranforderungen um durchschnittlich 50 %.

Einrichten von benutzerdefinierten Format-Streams

1. Klicken Sie auf der Registerkarte **Streams des benutzerdefinierten Formats** auf Stream-URL generieren. Ein Dialogfenster wird geöffnet.
2. Stellen Sie im Dialogfenster ein:
   - **Codec** - wählt aus den verfügbaren Codecs aus
   - **Audio aktivieren** - legt fest, ob nur Video oder Video mit Audio übertragen werden soll
   - **Auflösung** - legt die Auflösung des Bildes fest
   - **Framerate** - legt die Bildrate des aufgenommenen Videos fest
   - **Bitrate** - legt die Bitrate fest
   - **Zipstream** - wählt das voreingestellte Kompressionsniveau des Zipstream (für H.264) aus. AXIS Zipstream bewahrt alle wichtigen forensischen Details, die Sie benötigen, und reduziert gleichzeitig die Datenübertragungs- und Speicheranforderungen um durchschnittlich 50 %.
3. Die Stream-Adresse mit Parametern wird automatisch unten im Dialogfeld geladen.
4. Kopieren Sie die Stream-Adresse und speichern Sie Ihre Änderungen.

Ton-Einstellungen

Einstellen der Gerätelautstärke

Um die Lautstärke Ihres Geräts einzustellen, gehen Sie zu **Anpassung > Audio**.

Die Gesamtlautstärke bestimmt die Grundlautstärke aller anderen Töne des Geräts. Stellen Sie diesen Parameter so ein, dass er den Geräuschpegel der Umgebung widerspiegelt, in der das Gerät installiert ist. Die Einstellung der anderen Sounds ist also immer relativ zu dieser **Gesamtlautstärke**.

Adaptive Lautstärke

Auf der Registerkarte **Adaptive Lautstärke** können Sie die automatische Lautstärkeanpassung auf der Grundlage von Umgebungsgeräuschen aktivieren. Diese Funktion ist besonders für Installationen in Umgebungen geeignet, in denen die Umgebungsgeräusche variabel sind.

Stellen Sie auf der Registerkarte **Empfindlichkeitsschwelle** ein, ab der die Lautstärke des Geräts ansteigt. Das Gerät kann bis zu einem einstellbaren Wert verstärkt werden **Maximale Tonverstärkung**.

Audioübertragung bei Anrufen

Die Audioparameter für den Anruf werden direkt auf der Registerkarte des Dienstes, der den Anruf bereitstellt (Anrufe über SIP (S. 17) oder Ortsgespräche zwischen 2N Geräten (S. 19)), auf der Registerkarte **Video** eingestellt.

1. Öffnen Sie den Bereich **. Rufen Sie** auf.
2. Rufen Sie die Seite des Dienstes auf, der den Anruf tätigt (bestimmtes SIP-Konto, Ortsgespräche).
3. Öffnen Sie die Registerkarte **Audio**.
4. Auf dieser Registerkarte stellen Sie die erforderlichen Klangparameter ein.

Aktivieren der Übertragung von DTMF-Signalen

Mit Hilfe von DTMF-Befehlen, die an dieses Gerät gesendet werden, ist es möglich, das Türschloss zu aktivieren und so die Tür zu öffnen.

1. Öffnen Sie den Bereich **. Rufen Sie** auf.
2. Rufen Sie die Seite des Dienstes auf, der den Anruf tätigt (bestimmtes SIP-Konto, Ortsgespräche).
3. Öffnen Sie die Registerkarte **Audio**.
4. Wählen Sie auf der Registerkarte **Senden von DTMF** die Option **Sendemodus**, um festzulegen, während welcher Anrufe DTMF-Signale gesendet werden können.
5. Wählen Sie die gewünschte DTMF-Sendemethode.

> **TIPP**
> Vergewissern Sie sich, dass Sie die Methoden aktiviert haben, die von dem Gerät, das Sie anrufen möchten, akzeptiert werden.

6. Legen Sie auf der Registerkarte **DTMF-Empfang** die DTMF-Methoden fest, die das Gerät empfangen soll.
7. Speichern Sie die Änderungen.

Benutzertöne

Das Gerät führt mehrere Aktionen aus, die von einem Ton begleitet werden (Klingeln, Schalten usw.). Sie können die abgespielten Töne unter **Anpassung > Benutzertöne** ändern.

Außerdem können bis zu 10 benutzerdefinierte Sounds auf das Gerät hochgeladen werden.

Andere Audiofunktionen des Geräts

Multicast

Das Gerät ist in der Lage, Audio vom Mikrofon mit Hilfe von RTP-Paketen zu übertragen, die an eine Multicast-Adresse gesendet werden, und gleichzeitig einen Audiostrom im gleichen Format zu empfangen, den das Gerät dann über den eingebauten Lautsprecher (oder einen anderen konfigurierten Audioausgang) wiedergibt.

Rauscherkennung

Das Gerät kann den vom Mikrofon empfangenen Ton überwachen, und wenn der Mikrofonsignalpegel einen festgelegten Schwellenwert überschreitet, kann das Gerät ein Ereignis auslösen `Event.NoiseDetected`. Auf dieses Ereignis können weitere Ereignisse in der Automatisierung folgen (siehe Automatisierung (S. 54)).

Aktivieren Sie die Geräuscherkennung

1. Gehen Sie zu **Integration > Audio**.
2. Aktivieren Sie in der Kopfzeile der Registerkarte **Noise Detection** die Funktion.
3. Geben Sie im Parameter **Noise threshold level** den Wert [dB] an, bei dessen Überschreitung das Ereignis **Event.NoiseDetected** ausgelöst wird.
4. Im Parameter **Alarmstartverzögerung** können Sie die Zeitspanne festlegen, die das Geräusch über einem Schwellenwert liegen muss, damit das Ereignis ausgelöst wird.
5. Im Parameter **Alarm End Delay** können Sie dagegen die Zeitspanne angeben, die das Signal unterhalb des Schwellenwerts liegen muss, damit das Ereignis endet.

Audiotest

Das Ergebnis des letzten Tests finden Sie unter **Integration > Audio > Registerkarte Allgemein > Registerkarte Audiotest**.

2N Geräte können eine regelmäßige Überprüfung des eingebauten Lautsprechers und Mikrofons durchführen. Der Lautsprecher generiert im Verlauf des Tests einen oder mehrere kurze Töne. Der generierte Ton

wird mittels des eingebauten Mikrophons aufgenommen und, wenn er richtig erkannt wird, wird der Test für erfolgreich erklärt. Die Testdauer beträgt ungefähr 4 s. Falls der Test nicht erfolgreich ist (was z.B. durch extremen umgebenden Lärm verursacht werden kann), wird der Test in zehn Minuten noch einmal wiederholt. Das Ergebnis des letzten Tests kann in der webbasierten Konfigurationsoberfläche des Geräts angezeigt oder mit Automation verarbeitet werden.

ANMERKUNG
Wenn während des Audiotests ein Anruf läuft, wird der Audiotest aufgeschoben, bis der Anruf beendet ist. Der Audiotest wird gleich nach dem Ende des Anrufes durchgeführt.

Informacast

Wenn Ihr Gerät das InformaCast-Protokoll für das Streaming von Audio unterstützt, finden Sie die entsprechenden Einstellungen unter **Integration > Audio > Informacast-Register**. Mit dem InformaCast-Protokoll kann man einen Audio-Stream (Unicast/Multicast RTP/UDP - codiert mit dem Codec G.711 U-law) zwischen dem 2N Gerät und dem InformaCast-Server oder einem anderen InformaCast-Klienten erstellen.

Nachdem Sie den Dienst unter **Integration > Audio > InformaCast** aktiviert haben, werden die InformaCast Server im lokalen Netzwerk automatisch über das SLP-Protokoll gefunden und das 2N Gerät wird automatisch bei ihnen registriert.

Zeitprofile

Einige der Funktionen, die das Gerät ausführt, sind zeitabhängig. Im Bereich **Zeitprofile von** können Sie Zeitintervalle voreinstellen, aus denen Sie dann für diese Funktionen auswählen können. Das bedeutet, dass Sie die Zeit nicht jedes Mal manuell eingeben müssen, wenn Sie sie einstellen. Sie können das Zeitprofil zur besseren Übersichtlichkeit benennen.

Erstellung des Zeitprofils:

1. Gehen Sie zu **Anpassung > Zeitprofile**.
2. Klicken Sie auf leer, um ein neues Profil zu erstellen.
3. Geben Sie einen Profilnamen ein.
4. Klicken Sie auf Speichern. Die Profildetails werden geöffnet.
5. Legen Sie die Intervalle fest, in denen das Zeitprofil aktiv sein soll.
   1. Klicken Sie auf das gewünschte Intervall.
   2. Sie können den Start und das Ende im geöffneten Menü festlegen.

   ANMERKUNG
   Die Zeile **Feiertage** wird verwendet, um verschiedene Zeitintervalle an ausgewählten Tagen einzustellen, siehe Feiertage (S. 39).
6. Speichern Sie die Änderungen.

Feiertage

In der Gerätekonfiguration können Sie mehrere Tage festlegen, die als Feiertage markiert werden. Für diese Tage werden dann in den Zeitprofilen spezielle Intervalle festgelegt. In der Regel sind dies Tage wie Feiertage, Betriebsferien und andere besondere Tage.

Für jeden Feiertag geben Sie an, ob er nur für ein bestimmtes Jahr gilt oder ob er sich jedes Jahr am selben Tag wiederholt. Urlaube können mehrere Jahre im Voraus geplant werden.

Feiertagseinstellungen:

1. Gehen Sie zu **Anpassung > Zeitprofile > Registerkarte Feiertage**.
2. Wählen Sie das Jahr, für das Sie den Feiertag festlegen möchten.
3. Klicken Sie auf den Tag im Kalender:
   - Der erste Klick markiert den Feiertag, der jedes Jahr an dem angegebenen Tag und Monat wiederholt wird.
   - Mit einem zweiten Klick wird der Feiertag zu einem einmaligen Feiertag für das ausgewählte Jahr.
4. Speichern Sie die Änderungen.

Erweiterte SIP-Kontoeinstellungen

In diesem Abschnitt werden die optionalen Funktionen und SIP-Kontoparameter beschrieben, die im Abschnitt **Anrufe > SIP** eingestellt werden.

Erweiterte SIP-Kontoeinstellungen ermöglichen es Ihnen, die Sicherheit zu erhöhen, die Anrufqualität zu optimieren und die Kompatibilität mit verschiedenen Telefonanlagen zu gewährleisten. Wir empfehlen, dass nur erfahrene Administratoren die Einstellungen ändern.

1. Gehen Sie zu **Calling > SIP** des Kontos, das Sie einrichten möchten.

SIP-Funktionen

Die REFER-Methode ermöglicht die dynamische Weiterleitung aktiver Anrufe zwischen verschiedenen SIP-Identitäten und bietet damit eine flexiblere Steuerung der Kommunikationsflüsse.

Die PRACK-Methode bietet eine zuverlässige Bestätigung von kontinuierlichen Gesprächszuständen zwischen Geräten, was die Qualität und Stabilität der Kommunikation in SIP-Systemen verbessert.

Medien

Nur verschlüsselte Anrufe empfangen (SRTP) - ermöglicht es Ihnen, nur SRTP-verschlüsselte Anrufe zu empfangen. Unverschlüsselte Anrufe werden automatisch abgewiesen. Gleichzeitig wird für höhere Sicherheit TLS als Transportprotokoll für SIP empfohlen.

Verschlüsselte ausgehende Anrufe (SRTP) – stellt ausgehende Anrufe auf diesem Konto ein, die mittels des SRTP-Protokolls verschlüsselt werden. Gleichzeitig wird für höhere Sicherheit TLS als Transportprotokoll für SIP empfohlen.

Adaptive Steuerung der Videoqualität – aktiviert die Verwendung des erweiterten RTP-Profils für Rückkopplung mit RTCP-Protokoll (RTP/AVPF). Diese Wahl ermöglicht eine interaktive Steuerung der Videoqualität nach RFC-4585 und dadurch eine Anpassung des Videodatenstroms an die momentan vorhandene Qualität der Netzverbindung.

Kompatibilität mit Broadsoft-Geräten- Legt den Broadsoft-Kompatibilitätsmodus fest. Wenn in diesem Modus die Sprechanlage ein Re-invite von der Zentrale empfängt, antwortet sie statt komplettes Menü mit einer Wiederholung des zuletzt gesandten SDP mit aktuell genutzten Codecs.

MKI in SRTP-Paketen verwenden – erlaubt die Verwendung der MKI (Master Key Indentifier), die von der Gegenseite zur Identifikation des Hauptschlüssels bei der Rotation mehrerer Schlüssel in den SRTP Paketen verlangt wird.

Keine Übertragung von eingehenden Early-Medien – verhindert die Übertragung eines eingehenden Ton-Streams vor der Annahme des Gesprächs, der von manchen Zentralen oder anderen Geräten versandt wird. Stattdessen soll der übliche Klingelton ertönen.

Erweiterte Konfiguration

KeepAlive-Pakete senden - stellt ein, ob das Gerät regelmäßig STUN/CRLF-Pakete an den Registrator und auch SIP OPTIONS während Anrufen senden soll, um eine bereits bestehende Verbindung aktiv zu halten.

SRV-Eintragsrotation – aktiviert das Rotieren der SRV für SIP-proxy und Registrar. Es handelt sich um eine alternative Methode für Übergang zu Reserve-Server beim Ausfall oder bei Nichterreichbarkeit der Hauptserver.

IP-Adressen-Filters – ermöglicht die Sperrfunktion des SIP-Pakete-Empfangs von anderen Adressen, als die SIP-Proxy- und die SIP-Registrar-Adresse sind. Der primäre Zweck der Funktion ist die Erweiterung der Kommunikationssicherheit und die Beseitigung von nicht autorisierten Anrufen.

Auswertung des Status älterer Backups -

QoS DSCP Wert – Stellt die Priorität der SIP-Pakete im Netz ein. Der eingestellte Wert wird im Feld TOS (Type of Service) im Kopf des IP-Pakets abgesendet. Der Wert wird als Dezimalstelle eingegeben.

Einstellung des Schutzschalters

Der Sicherheitsschalter erkennt das Öffnen der Geräteabdeckung, was von der Software als logisches Schließen des Schalters ausgewertet wird. Auf diese Weise zeigt der Schalter mögliche physische Manipulationen am Gerät an.

Wenn Sie einen Schutzschalter aktivieren, können Sie alle anderen Schalter deaktivieren oder die Automatisierung so einrichten, dass eine Folgeaktion ausgelöst wird, z. B. das Senden einer E-Mail, das Erstellen einer HTTP-Anfrage oder das Aktivieren eines stillen Alarms.

ANMERKUNG
Je nach Gerätetyp kann der Schutzschalter entweder in das Hauptgerät integriert sein oder Sie müssen ihn als zusätzliches Modul installieren. Die Installationsverfahren entnehmen Sie bitte dem Installationshandbuch des jeweiligen Geräts.

Blockierung anderer Schalter, wenn die Abdeckung geöffnet wird

Die Vorrichtung ermöglicht es, sicherzustellen, dass die anderen Schalter während des Öffnens des Deckels (d.h. wenn der Schutzschalter aktiviert ist) blockiert sind. Dadurch wird auch verhindert, dass der Türschalter aktiviert wird und der Zugang durch die Tür, die das Gerät steuert, verhindert.

Verfahren zur Einstellung der Schalterblockierung

1. Gehen Sie zu **Integration > I/O**.
2. Auf der Registerkarte **Schutzschalter** weisen Sie dem Eingang einen Schutzschalter zu.
3. Aktivieren Sie die Option **Automatische Blockierung der Schalter**.

Ereignisse mit Schutzschalter

Durch die Aktivierung des Schutzschalters werden Ereignisse ausgelöst. Diese Ereignisse können mit Automatisierung (S. 54) verknüpft werden.

- Das Öffnen des Deckels löst das Ereignis `TamperSwitchActivated (state: in)` aus.
  Wenn der Schalter als Eingang in **dem E/A-Bereich** zugewiesen ist, wird ein zusätzliches Ereignis `InputChange (port: tamper, state: false)` erzeugt.
- Das Schließen des Deckels löst das Ereignis `TamperSwitchActivated (state: out)` aus.
  Wenn der Schalter als Eingang **dem E/A-Bereich** zugewiesen ist, wird ein zusätzliches Ereignis `InputChange (port: tamper, state: true)` erzeugt.

System

Einstellungen für Datum und Uhrzeit

ACHTUNG
Wenn das Gerät über ein Massenverwaltungsprogramm (2N Access Commander / 2N My2N) verwaltet wird, kann die Gerätezeit über dieses Programm verwaltet werden. Manuelle Änderungen in der Weboberfläche des Geräts haben keinen Einfluss auf die Zeiteinstellung.

Synchronisierung mit NTP

Wenn das Gerät mit dem Internet verbunden ist, können die Uhrzeit und das Datum mit NTP synchronisiert werden.

1. Gehen Sie zu **System > Datum und Uhrzeit**.
2. Aktivieren Sie auf der Registerkarte **der Zeitsynchronisationseinstellungen** die Option **Automatische Zeit von NTP oder Internet**.
3. Geben Sie die Adresse des NTP-Servers Ihrer Wahl ein.

Zeitaktualisierung im Falle eines Ausfalls

1. Gehen Sie zu **System > Datum und Uhrzeit**.
2. Klicken Sie auf der Registerkarte **der Zeitsynchronisationseinstellungen** auf Mit Browser synchronisieren.
   Dadurch wird die Gerätezeit mit der Zeit auf Ihrem Computer synchronisiert.

ANMERKUNG
Die 2N Geräte sind mit einer Echtzeit-Backup-Uhr ausgestattet, mit der Sie einen Stromausfall für mehrere Tage überbrücken können.

Netzwerkeinstellungen

In der Werkseinstellung verwendet das Gerät eine dynamische IP-Adresse, die vom DHCP-Server zugewiesen wird.

Die richtige IP-Adressenkonfiguration ist der Schlüssel, um sicherzustellen, dass Ihre Geräte stabil und zuverlässig mit Ihrem Netzwerk verbunden sind.

1. Um die Netzwerkparameter des Geräts einzustellen, gehen Sie zu **System > Netzwerkverbindung**.

2. Unter Grundeinstellungen > IP-Adresseinstellungen können Sie den DHCP-Server aktivieren oder deaktivieren.

Einstellungen der statischen IP-Adresse:

a. Deaktivieren Sie die Option **DHCP-Server**.
b. Geben Sie die gewünschte IP-Adresse, Subnetzmaske, Standard-Gateway und DNS-Server ein.
c. Speichern Sie Ihre Änderungen. Gerät wird neu gestartet.

DHCP-Einstellungen

a. Aktivieren Sie die Option **DHCP-Server**.
b. Geben Sie die gewünschte IP-Adresse, Netzmaske, Standard-Gateway und DNS-Server ein.
c. Speichern Sie Ihre Änderungen. Gerät wird neu gestartet.

ANMERKUNG
Wenn Sie in Ihrem Netz den RADIUS-Server und den Mechanismus der Überprüfung der angeschlossenen Geräte, der von den Protokollen 802.1x ausgeht, nutzen, können Sie das Gerät so konfigurieren, dass es die Authentifizierung EAP-MD5 oder EAP-TLS anwendet. Der Einstellung dieser Funktion dient die Registerkarte 802.1x.

Lizenz

Einige Funktionen sind nur unter der entsprechenden Lizenz verfügbar. Einen Überblick über die Lizenzen und ob sie aktiv sind, finden Sie unter **System > Lizenzen > Registerkarte Allgemeine Informationen.** Auf der Registerkarte **Lizenzierte Funktionen** finden Sie eine Übersicht der verfügbaren Funktionen, die einer Lizenz unterliegen.

ANMERKUNG
Nachdem Sie die entsprechende Lizenz ausgewählt haben, wenden Sie sich an Ihren 2N Händler. Wenn Sie ein 2N Partner sind, können Sie unseren Kundendienst unter customercare@2n.com kontaktieren. Bitte geben Sie in Ihrer Anfrage die Seriennummer des Geräts an.

Aktualisieren des Lizenzschlüssels

Der aktuelle Lizenzschlüssel ist auf dem Update-Server verfügbar. Wenn die Web-Konfigurationsoberfläche keinen Zugang zum öffentlichen Internet hat, können Sie die Schlüsseldatei manuell auf das Gerät hochladen.

Bei jedem Neustart des Geräts wird der letzte verfügbare Lizenzschlüssel neu geladen.

Probelizenz

Mit der Testlizenz können Sie vorübergehend alle Funktionen der Gold-Lizenz und der Microsoft Teams-Lizenz für maximal 800 Stunden nach der Aktivierung nutzen. Eine aktivierte Testlizenz kann nicht ausgesetzt werden.

Um eine Testlizenz zu aktivieren, gehen Sie zu **System > Lizenzen > Registerkarte Testlizenz**.

ACHTUNG
Bei jedem Neustart des Geräts wird eine Stunde der Testlizenz entfernt.

Übersicht der lizenzierten Funktionen

Funktion	Lizenzen
Ton • Benutzertöne • Automatischer Klangtest • Geräuscherkennung	Kostenlos
Sicherheit • HTTP-API • Unterstützung 802.1x • SIPS -(TLS)-Unterstützung. • SRTP-Unterstützung • Stiller Alarm • Erfolglose Zugriffsversuche begrenzen • Blockierung der Schalter • Codiertes Tastenfeld • Anti-Passback	Kostenlos
HTTP-API-Unterstützung	Kostenlos
NFC-Unterstützung	Kostenlos
Video • Audio-/Video-Streaming (RTSP-Server) • Unterstützung einer externen IP-Kamera • ONVIF-Unterstützung • Unterstützung der PTZ-Funktion • Unterstützung der Bewegungserkennung	Gold

Funktion	Lizenzen
Integrationen • Erweiterte Schaltereinstellungsoptionen • Automatisierungsfunktionen • E-Mails-Absenden (SMTP-Client) • Automatische Aktualisierung (TFTP/HTTP-Client) • FTP-Klient • SNMP-Client • TR-069 • Genetec Synergis	Gold
Aufzugskontrolle	Gold
Paging und Notfallkommunikation über die Cisco-Plattform	InformaCast
Kommunikation mit dem C-CURE 9000 Server	Plugin für CCUR
Kommunikation mit dem OnGuard Server (LenelS2)	Plugin pro OnGuar
Kommunikation mit dem Symmetry-Server	Plugin für Symmetrie
Kommunikation mit MS Teams	Licence Microsoft Teams

Ereignisprotokoll

Die folgende Übersicht listet die Ereignisse auf, die das Gerät während des Betriebs erzeugen kann, und beschreibt kurz die Bedingungen, unter denen sie auftreten. Die Verfügbarkeit von Ereignissen hängt von der Art und der spezifischen Konfiguration des Geräts ab.

Ereignis	Beschreibung
AccessBlocked	Tritt auf, wenn Zugriffsrechte blockiert sind.
AccessLimited	Tritt nach fünf erfolglosen Authentifizierungsversuchen auf. Der Zugang wird dann für 30 Sekunden gesperrt.
AccessTaken	Tritt auf, wenn die Karte in den Anti-Passback-Bereich eingelegt wird.
ApiAccessRequested	Tritt nach einem erfolgreichen HTTP-API-Aufruf `/api/accesspoint/grantaccess` auf.

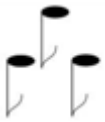
Ereignis	Beschreibung
AudioLoopTest	Erscheint, nachdem der Mikrofon- und Lautsprechertest des Geräts abgeschlossen ist.
CallSessionStateChanged	Tritt auf, wenn sich der Status des Anrufs ändert (Aufbauen, Verbinden, Klingeln, Verbinden, Beenden). Ein einzelner Anruf kann mehrere einzelne Anrufe umfassen. Wenn Sie z. B. eine Telefonnummer in einer Gruppe mit einem Kontaktvertreter anrufen, werden zwei gleichzeitige Anrufe an zwei verschiedene Ziele getätigt. Die Ereignisbeschreibung enthält Informationen über die Art der Änderung, die Kennung des Anrufs, die Adresse des aktuellen Anrufs und die Reihenfolge des aktuell erzeugten Anrufs.
CallStateChanged	Tritt auf, wenn sich der Status des Anrufs ändert (Klingeln, Verbunden, Beendet). Die Ereignisbeschreibung enthält Informationen über die Art der Änderung, die Richtung des Anrufs (eingehend, ausgehend) und die Identifikation der Gegenpartei oder des SIP-Kontos.
CapabilitiesChanged	Erscheint, wenn Sie die verfügbaren Funktionen des Geräts ändern.
CardEntered	Tritt auf, wenn die Karte in das Lesegerät eingeführt wird.
CardHeld	Tritt auf, wenn die Karte für mehr als 4 Sekunden an das Lesegerät gehalten wird.
CodeEntered	Dies geschieht nach der Eingabe des Codes auf dem Ziffernblock und dem Abschluss mit dem Zeichen *.
ConfigurationChanged	Tritt auf, wenn Sie die Gerätekonfiguration ändern.
DeviceState	Tritt auf, wenn das Gerät seinen Zustand ändert (z.B. hochfährt).
DisplayTouched	Tritt auf, wenn das Display berührt wird (am Hauptgerät oder an einem über VBUS angeschlossenen Zusatzmodul).
DoorOpenTooLong	Tritt auf, wenn eine lange offene Tür erkannt wird.
DoorStateChanged	Tritt auf, wenn die Tür ihren Zustand ändert (Öffnen/Schließen).

Ereignis	Beschreibung
DtmfEntered	Tritt auf, wenn ein DTMF-Code während eines Anrufs oder lokal außerhalb eines Anrufs empfangen wird.
ExternalCameraStateChanged	Tritt auf, wenn der Status der externen Kamera geändert wird.
FingerEntered	Tritt während der Authentifizierung per Fingerabdruck auf.
InputChanged	Tritt auf, wenn der Logikeingang (einschließlich des Schutzschalters) geändert wird.
KeyPressed	Sie tritt auf, wenn die Taste gedrückt wird. Die Ziffern sind als 0, 1, 2 ..., 9 gekennzeichnet. Die Reihenfolge der Kurzwahltasten ist %1, %2,.... Die Zifferntasten sind beschriftet mit `0-9`. Die Reihenfolge der Kurzwahltasten ist gekennzeichnet als `%1, %2` usw.
KeyReleased	Er tritt auf, wenn die Taste losgelassen wird. Die Zifferntasten sind beschriftet mit `0-9`. Die Reihenfolge der Kurzwahltasten ist gekennzeichnet als `%1, %2` usw.
LicensePlateRecognized	Dies geschieht, wenn ein Fahrzeugkennzeichen mit gültigen Zugangsrechten erkannt wird, siehe Einrichtung der Nummernschild-Authentifizierung (S. 30).
LiftConfigChanged	Tritt auf, wenn Sie die Einstellungen von Aufzugsteuerung (S. 29) ändern.
LiftFloorsEnabled	Tritt auf, wenn der Zugang zum Aufzugsstockwerk gewährt wird.
LiftStatusChanged	Tritt auf, wenn das Liftkontrollmodul angeschlossen oder getrennt wird.
LoginBlocked	Tritt nach 3 erfolglosen Anmeldeversuchen auf. Die Ereignisbeschreibung enthält die IP-Adressinformationen für diese Zugriffe.
MobKeyEntered	Tritt während der Bluetooth-Authentifizierung auf.
MotionDetected	Wird ausgelöst, wenn eine Bewegung in der Kameraaufzeichnung erkannt wird, siehe Bewegungserkennung (S. 34)

Ereignis	Beschreibung
NoiseDetected	Tritt auf, wenn ein erhöhter Geräuschpegel festgestellt wird, siehe Andere Audiofunktionen des Geräts (S. 38).
OutputChanged	Tritt ein, wenn sich der Zustand des logischen Ausgangs ändert.
PairingStateChanged	
RegistrationState-Changed	Tritt auf, wenn die Registrierung des SIP-Proxys geändert wird.
RexActivated	Tritt auf, wenn ein als REX-Taste konfigurierter Eingang aktiviert wird.
SilentAlarm	Tritt ein, wenn ein stiller Alarm ausgelöst wird, siehe Stiller Alarm (S. 25).
SwitchesBlocked	Tritt auf, wenn der Switch durch einen ungültigen Zugriffsversuch blockiert wird.
SwitchOperation-Changed	Tritt auf, wenn die Funktion des Schalters geändert wird. Das Ereignis zeigt den Zustand der Sperrung oder des Haltens des Schalters, den Übergang zum permanenten Halten des Schalters oder den Wechsel des Schalters (Start, Neustart, Beenden) an.
SwitchStateChanged	Tritt auf, wenn sich der Zustand des Schalters ändert.
TamperSwitchActiva-ted	Tritt auf, wenn sich der Zustand des Sabotageschalters ändert, der auf das Öffnen oder Aufdecken der Geräteabdeckung reagiert.
UnauthorizedDoorO-pen	Tritt auf, wenn eine unbefugte Türöffnung erkannt wird.
UserActionActivated	Signalisiert eine Benutzeraktion, die durch den zugehörigen Benutzeraktions-auslöser ausgelöst wurde.
UserAuthenticated	Tritt bei erfolgreicher Benutzerauthentifizierung und -autorisierung ein.
UserRejected	Tritt auf, wenn die Berechtigung des Benutzers ungültig ist.
WaveKeyActivated	Tritt auf, wenn die Bluetooth-Authentifizierung aktiviert ist.

Signalisierung der Betriebsstatus

Das Gerät signalisiert mittels akustischer Meldungen Änderungen und Übergänge zwischen den verschiedenen Betriebszuständen. Für jede Art der Statusänderung existiert eine andere Meldungsart. Die Liste der einzelnen Meldungen ist in der folgenden Tabelle angeführt:

Akustisches Signal	Status
	**Interne Anwendung läuft** Wenn das Gerät eingeschaltet oder neu gestartet wird, wird die interne Anwendung gestartet.
	**An das lokale Netzwerk angeschlossen, IP-Adresse erhalten** Nach dem Start der internen Anwendung meldet sich das Gerät beim lokalen Netzwerk an.
	**Vom lokalen Netzwerk abgemeldet, IP-Adresse verloren** Vom lokalen Netzwerk abgemeldet, IP-Adresse verloren
	**Ungültige Telefonnummer oder ungültiger Code für die Schaltung des Schalters** Das Gerät ermöglicht die Eingabe eines Codes, um die Tür zu öffnen. Bei der Eingabe von ungültigen Werten ertönt dieses Signal.
	**Zurücksetzen der Netzwerkparameter auf den Standardzustand** Nach dem Einschalten der Stromversorgung können die Netzwerkparameter über die Hardware geändert werden, siehe Kurzanleitung.
	Signalisierung des nahen Anrufendes Das Gerät ermöglicht , ein Zeitlimit einzustellen, nach dessen Ablauf der Anruf beendet wird, siehe **Anruf > ALLGEMEINE EINSTELLUNGEN > Zeitlimit für Anrufe**.
	**Signalisierung der Anrufverlängerung** Der Anruf kann durch Drücken einer Taste auf dem VoIP-Telefon verlängert werden.

Akustisches Signal	Status
	**Verbundener Anruf bei Anrufen von einem VoIP-Telefon an das Gerät** Bei einem Anruf von einem VoIP-Telefon an das Gerät wird ein kurzer Ton abgespielt, um die Verbindung zu signalisieren.

Verwendete Ports

Service	Port	Protokoll	Richtung	Standardmäßig eingeschaltet	Einstellbar	Einstellungen
802.1x	–	–	In/Out	×	×	–
DHCP	68	UDP	In/Out	✓	×	–
DNS	53	TCP/UDP	In/Out	✓	×	–
Echo (device discovery)*	8002	UDP	In/Out	✓	×	–
FTP	21	TCP	Out	×	×	–
2N IP Eye	8003	UDP	Out	×	×	–
HTTP	80	TCP	In/Out	✓	✓	**System > Netzwerkverbindung > Registerkarte WEBSERVER**
HTTPS	443	TCP	In/Out	✓	✓	**System > Netzwerkverbindung > Registerkarte WEBSERVER**

Service	Port	Protokoll	Richtung	Standardmäßig eingeschaltet	Einstellbar	Einstellungen
Multicast audio	22222	UDP	Out	×	✓	**Integration > Audio**
Multicast-Audio für ICU-Protokoll	8006	UDP	Out	×	×	–
Multicast-Video für ICU-Protokoll	8008	UDP	Out	×	×	–
Multicast Video (wide) für ICU Protokoll	8016	UDP	In/Out	×	×	–
NTP-Klient	123	UDP	In/Out	✓	×	–
ONVIF	80, 443, 3702	TCP/UDP	In/Out	×	×	–
RTP+RTCP Ports (SIP)	4900+ (range of 64 ports)	UDP	In/Out	×	✓	**Anruf > Allgemeine Einstellungen**
RTP+RTCP Ports (externe Kamera)	4800+ (range of 64 ports)	UDP	In/Out	×	✓	**Integration > ONVIF / RTSP**
R5TSP-Klient	554	UDP	In/Out	×	✓	
RTSP server	554	UDP	In/Out	×	×	–
SingleWire Commands	80	TCP	In/Out	×	×	–
SingleWire Communication	8081	TCP	Out	×	×	–
SingleWire Media	20000+	UDP	In	×	×	–

Service	Port	Protokoll	Richtung	Standardmäßig eingeschaltet	Einstellbar	Einstellungen
SLP	427	UDP	In/Out	✓	×	–
SIP	5060, 5062	TCP/UDP	In/Out	×	✓	**Anruf > SIP**
SIPS	5061	TCP	In/Out	×	✓	**Anruf >SIP**
SMTP	25	TCP	Out	×	✓	**Integration > E-Mail-Benachrichtigungen**
Syslog	514	UDP	Out	×	×	–
TFTP	69	UDP	Out	×	×	–
My2N Knocker	443	TCP	Out	✓	×	–
My2N Tribble Tunnel	443	TCP	Out	✓	×	–
SNMP Agent	161	UDP	In/Out	✓	×	–
SNMP Trap	162	UDP	Out	✓	×	–
SSDP	1900	UDP	In/Out	✓	×	–
SDDP	1902	UDP	In/Out	✓	×	–
Multicast receiver (Automation)	4433	UDP	In	×	×	–
WS-Discovery	3702	UDP	In/Out	✓	×	–
CIP Client (Crestron)	41794	UDP	In/Out	×	×	–

Service	Port	Protokoll	Richtung	Standardmäßig eingeschaltet	Einstellbar	Einstellungen
Sitechannel (ICU-Protokoll)	8004	UDP	In/Out	×	×	–
Multicast DNS	5353	UDP	In/Out	✓	×	–

Automatisierung

ANMERKUNG
Die Funktion ist nur mit der Gold-Lizenz verfügbar.

Die standardmäßige 2N-Gerätekonfiguration deckt die meisten gängigen Szenarien ab. Für fortgeschrittene Fälle, wie z.B. die Notwendigkeit, das Gerät an bestimmte Anforderungen anzupassen oder es in Systeme von Drittanbietern zu integrieren, kann die Funktion Automatisierung verwendet werden. Mit der Automatisierung können Sie eine benutzerdefinierte Logik für das Geräteverhalten definieren, die auf verschiedene Ereignisse, Signale oder Kombinationen von Bedingungen reagiert. Bestimmte Aktionen können beispielsweise durch das Drücken einer bestimmten Kurzwahltaste, das Aktivieren eines Stillen Alarms, das Erkennen einer offenen Tür, das Aktivieren eines Eingangs oder das Erkennen von Bewegungen in der Nähe des Geräts ausgelöst werden.

Automatisierungseinstellungen:

1. Gehen Sie in der Weboberfläche des Geräts auf **Integration > Automation**.
2. Aktivieren Sie in der Funktionsübersicht die Anzahl der Funktionen nach Bedarf.
3. Klicken Sie auf , um die Konfigurationsoberfläche für die Automatisierung zu öffnen.
4. Geben Sie in der Kopfzeile der Automationsschnittstelle den Namen der Funktion ein, unter dem die Funktion gespeichert werden soll.
5. Erstellen Sie einen Automatisierungsablauf.
   Eine detaillierte Beschreibung der Automatisierungsfunktion und -konfiguration finden Sie in Manuelle Automatisierung.
6. Wenn die Funktion abgeschlossen ist, klicken Sie auf SAVE und verlassen die Automatisierungsschnittstelle.

IP Interkoms – Konfigurationshandbuch

2N.com