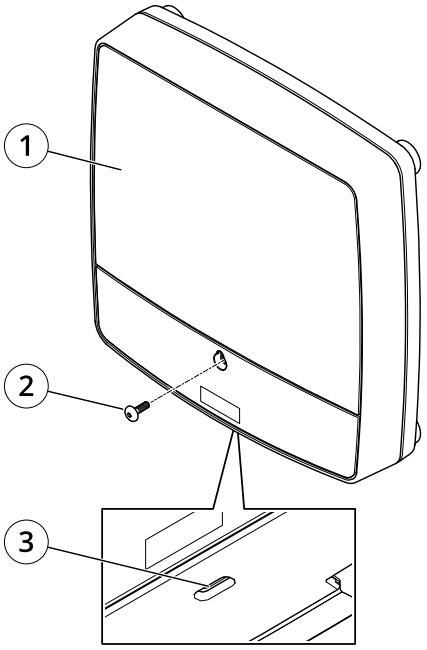
AXIS A1001 & AXIS Entry Manager

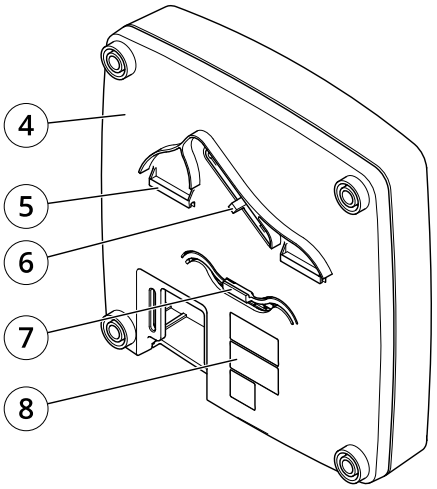
Benutzerhandbuch

Inhalt

Produktübersicht

Produktübersicht

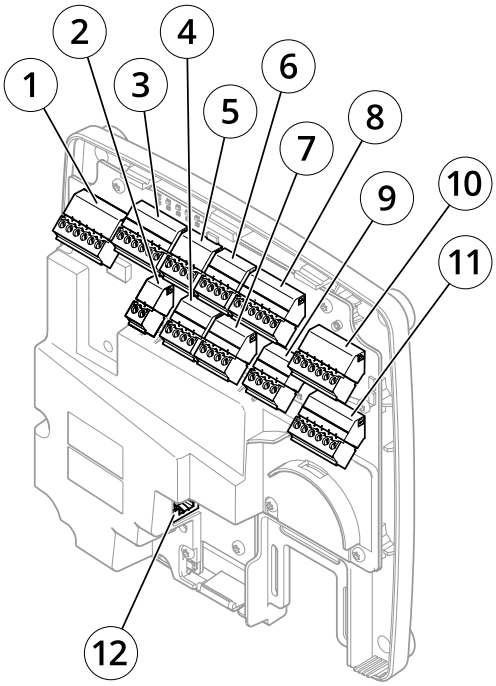




Vorder- und Rückseite:

1 *Abdeckung*
2 *Schraube für Abdeckung*
3 *Schlitz zum Entfernen der Abdeckung*
4 *Grundplatte*
5 *DIN-Halterung – obere*
6 *Manipulationsalarmschalter – Rückseite*
7 *DIN-Halterung – untere*
8 *Teilenummer (P/N) und Seriennummer (S/N)*

Produktübersicht



E/A-Schnittstelle:

1 Leser-Daten-Anschluss (READER DATA 1)
10 Leser-Daten-Anschluss (READER DATA 2)
3 Leser-E/A-Anschluss (READER I/O 1)
8 Leser-E/A-Anschluss (READER I/O 2)
4 Türanschluss (DOOR IN 1)
7 Türanschluss (DOOR IN 2)
6 Zusatzanschluss (AUX)
5 Audioanschluss (AUDIO) (nicht verwendet)

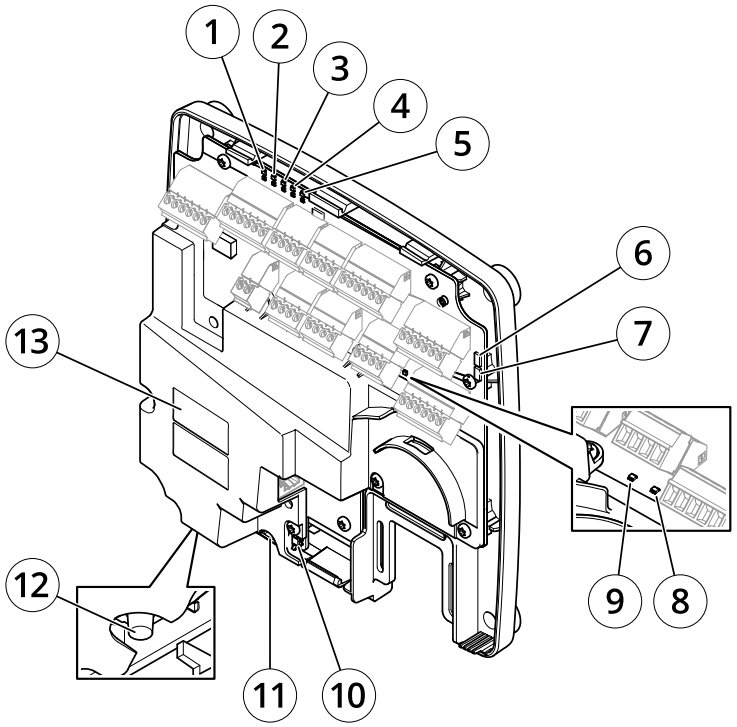
Externe Stromanschlüsse:

2 Netzanschluss (Gleichstrom IN)
12 Netzwerk-Anschluss (PoE)

Stromausgänge:

9 Stromanschluss für Schloss (LOCK)
11 Netz- und Relaisanschluss (PWR, RELAY)

Produktübersicht



LED-Anzeigen, Tasten und andere Hardware:

1 *LED-Betriebsanzeige*
2 *LED-Statusanzeige*
3 *LED-Netzwerk-Anzeige*
4 *LED-Anzeige für Leser 2 (nicht verwendet)*
5 *LED-Anzeige für Leser 1 (nicht verwendet)*
6 *Stiftleiste für Manipulationsalarm – Vorderseite (TF)*
7 *Stiftleiste für Manipulationsalarm – Rückseite (TB)*
8 *LED-Anzeige für Schloss*
9 *LED-Anzeige für Schloss*
10 *Manipulationsalarmsensor – Vorderseite*
11 *SD-Speicherkarteneinschub (microSDHC) (nicht verwendet)*
12 *Steuertaste*
13 *Bestellnummer (P/N) und Seriennummer (S/N)*

LED-Anzeigen

LED	Farbe	Bedeutung
Netzwerk	Grün	Dauerhaft bei Verbindung mit einem Netzwerk mit 100 MBit/s Blinkt bei Netzwerkaktivität.
	Gelb	Leuchtet bei Verbindung mit einem 10 MBit/s-Netzwerk. Blinkt bei Netzwerkaktivität.
	Leuchtet nicht	Keine Netzwerk-Verbindung vorhanden.
Status	Grün	Leuchtet bei Normalbetrieb grün.
	Gelb	Leuchtet beim Start und beim Wiederherstellen der Einstellungen.
	Rot	Blinkt langsam bei einem Aktualisierungsfehler.
Stromversorgung	Grün	Normaler Betrieb.
	Gelb	Blinkt grün/gelb bei der Firmware-Aktualisierung.

Schloss	Grün	Konstant im spannungslosen Zustand.
	Rot	Konstant bei anliegender Spannung.
	Leuchtet nicht	Potentialfrei.

Hinweis

- Die Status-LED kann so eingestellt werden, dass sie blinkt, wenn ein Ereignis aktiv ist.
- Die Status-LED kann so eingestellt werden, dass sie blinkt, wenn die Einheit erkannt wird. Rufen Sie **Setup > Additional Controller Configuration > System Options > Maintenance (Setup > Grundeinstellungen des Controllers > Systemoptionen > Wartung)** auf.

Anschlüsse und Tasten

E/A-Schnittstelle

Leser-Daten-Anschlüsse
Zwei 6-polige Anschlussblöcke mit Unterstützung für RS485- und Wiegand-Protokolle zur Kommunikation mit dem Leser. Technische Daten finden Sie auf *Seite 70*.

Leser-E/A-Anschlüsse
Zwei 6-polige Anschlussblöcke für Lesereingang und -ausgang. Abgesehen vom 0 V Gleichstrom-Bezugspunkt und Strom (Gleichstromausgang) verfügt der Leser-E/A-Anschluss über eine Schnittstelle zum:

- Digitaleingang – z. B. zum Anschließen eines Leser-Manipulationsalarms.
- Digitalausgang – z. B. zum Anschließen von Leser-Signaltongebern und Leser-LEDs.

Technische Daten finden Sie auf *Seite 70*.

Türanschlüsse
Zwei 4-polige Anschlussblöcke zum Anschließen von Türüberwachungsgeräten und REX-Geräten (Request to Exit). Technische Daten finden Sie auf *Seite 71*.

Zusatzanschluss
4-poliger konfigurierbarer E/A-Anschlussblock. Zur Verwendung mit externen Geräten in Verbindung mit Manipulationsalarmen, Ereignisauslösung, Alarmbenachrichtigungen usw. Abgesehen vom 0 V Gleichstrom-Bezugspunkt und Strom (Gleichstromausgang) verfügt der Zusatzanschluss über eine Schnittstelle zum:

- Digitaleingang – Alarmeingang für den Anschluss von Geräten, die zwischen geöffnetem und geschlossenem Schaltkreis wechseln können, z. B. PIR-Sensoren oder Glasbruchmelder.
- Digitalausgang – zum Anschluss externer Geräte wie Einbruchalarme, Sirenen oder Leuchten. Angeschlossene Geräte können über die VAPIX®-API (Application Programming Interface) oder über eine Aktionsregel aktiviert werden.

Technische Daten finden Sie auf *Seite 72*.

Externe Stromanschlüsse

HINWEIS

Das Produkt muss mit einem abgeschirmten Netzwerk-Kabel (STP) angeschlossen werden. Alle Kabel, die das Produkt mit dem Netzwerk-Switch verbinden, müssen hierfür ausgelegt sein. Stellen Sie sicher, dass die Netzwerk-Geräte gemäß den Anweisungen des Herstellers installiert wurden. Informationen zu gesetzlichen Bestimmungen finden Sie unter .

Netzanschluss
2-poliger Anschlussblock für die Gleichstromversorgung. Verwenden Sie eine mit den Anforderungen für Schutzkleinspannung (SELV) kompatible Stromquelle mit begrenzter Leistung (LPS), entweder mit einer Nennausgangsleistung von ≤100 W oder einem dauerhaft auf ≤5 A begrenzten Nennausgangsstrom. Technische Daten finden Sie auf *Seite 72*.

Produktübersicht

Netzwerk-Anschluss
RJ-45-Ethernetanschluss. Unterstützt Power over Ethernet (PoE). Technische Daten finden Sie auf *Seite 73*.

Stromausgänge

Stromanschluss (Schloss)

Vierpoliger Anschlussblock für ein oder zwei Schlösser. Dieser Anschluss kann auch zur Stromversorgung externer Geräte verwendet werden. Technische Daten, siehe *Seite 73*.

Netz- und Relaisanschluss

Sechspoliger Anschlussblock für den Netzanschluss und das Relais des Türcontrollers für externe Geräte wie Schlösser und Sensoren. Technische Daten, siehe *Seite 73*.

Tasten und andere Hardware

Stiftleiste für Manipulationsalarm
Zwei 2-polige Stiftleisten zum Trennen des vorderen und rückseitigen Manipulationsalarms. Technische Daten finden Sie auf *Seite 74*.

Steuertaste
Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen Siehe *Seite 65*.
- Verbinden mit einem AXIS Video Hosting System-Dienst Siehe *Seite 59*. Halten Sie zum Verbinden die Taste für ca. 1 Sekunde gedrückt, bis die Status-LED-Leuchte grün blinkt.
- Verbinden mit dem AXIS Internet Dynamic DNS Service. Siehe *Seite 59*. Halten Sie zum Verbinden die Taste für ca. 3 Sekunden gedrückt.

Installation

Installationsvideo für das Produkt.

Zugriff auf das Produkt

Anweisungen zum Installieren des Axis Produkts finden Sie in der mitgelieferten Installationsanleitung.

Auf das Gerät zugreifen

1. Öffnen Sie einen Browser, und geben Sie die IP-Adresse oder den Hostnamen des Axis Geräts in die Adresszeile des Browsers ein.

   Verwenden Sie bei unbekannter IP-Adresse die AXIS IP Utility oder den AXIS Device Manager, um das Gerät im Netzwerk zu ermitteln.

2. Den Benutzernamen und das Kennwort eingeben. Wenn dies der erste Zugriff auf das Gerät ist, muss zuerst das Root-Kennwort konfiguriert werden. Siehe .

3. Im Browser wird der AXIS Entry Manager geöffnet. Wenn ein Computer verwendet wird, wird die Übersichtsseite angezeigt. Wenn ein mobiles Gerät verwendet wird, wird die mobile Landing Page angezeigt.

Die mobile Landingpage

Die mobile Landingpage zeigt den Status der Türen und Schlösser, die mit dem Türcontroller verbunden sind. Sie können das Sperren und Entsperren testen. Die Seite aktualisieren, um das Ergebnis zu sehen.

Ein Link führt Sie zum AXIS Entry Manager.

Hinweis

- AXIS Entry Manager unterstützt keine mobilen Geräte.
- Wenn Sie mit AXIS Entry Manager fortfahren, gibt es keinen Link, der Sie auf die mobile Landingpage zurückführt.

Über das Internet auf das Produkt zugreifen

Mit einem Netzwerkrouter können Produkte in einem privaten Netzwerk (LAN) eine einzelne Internetverbindung gemeinsam nutzen. Dazu wird der Netzwerk-Verkehr vom privaten Netzwerk zum Internet weitergeleitet.

Die meisten Router sind so vorkonfiguriert, dass sie Zugriffsversuche vom öffentlichen Netzwerk (Internet) auf das private Netzwerk (LAN) verhindern.

NAT-Traversal aktivieren, wenn sich das Axis Produkt in einem Intranet (LAN) befindet und von der anderen (WAN) Seite eines NAT-Routers (Network Address Translator) darauf zugegriffen werden soll. Wenn NAT-Traversal ordnungsgemäß konfiguriert ist, wird sämtlicher HTTP-Datenverkehr zu einem externen HTTP-Port des NAT-Routers zum Produkt weitergeleitet.

Die Funktion NAT-Traversal aktivieren

- Die Aktivierung erfolgt über **Setup > Zusätzliche Controllerkonfiguration > Systemeinstellungen > Netzwerk > TCP/IP > Erweitert**.
- **Aktivieren** anklicken.
- Den NAT-Router für den Zugriff aus dem Internet manuell konfigurieren.

Siehe auch AXIS Internet Dynamic DNS-Service unter *www.axiscam.net*

Hinweis

- In diesem Zusammenhang bezieht sich ein „Router" auf ein Netzwerk-Routinggerät wie z. B. NAT-Router, Netzwerkrouter, Internet Gateway, Breitbandrouter, Breitbandgerät oder Software wie z. B. eine Firewall.
- Damit NAT-Traversal funktioniert, muss NAT-Traversal vom Router unterstützt werden. Der Router muss außerdem UPnP® unterstützen.

Das Root-Kennwort festlegen

Für den Zugriff auf das Produkt muss das Kennwort für den Standardadministrator-Benutzer **root** festgelegt werden. Bei der erstmaligen Verwendung des Produkts wird das Dialogfeld **Configure Root Password (Root-Kennwort konfigurieren)** angezeigt. Dort kann das Kennwort festgelegt werden.

Um ein Abhören der Netzwerk-Kommunikation zu verhindern, können Sie das Root-Kennwort über eine verschlüsselte HTTPS-Verbindung festlegen, die ein HTTPS-Zertifikat erfordert. Das Protokoll HTTPS (Hypertext Transfer Protocol over SSL) wird verwendet, um den Datenverkehr zwischen Webbrowsern und Servern zu verschlüsseln. Das HTTPS-Zertifikat gewährleistet den verschlüsselten Informationsaustausch. Siehe *HTTPS auf Seite 55*.

Der standardmäßige Administrator-Benutzername **root** kann nicht geändert bzw. gelöscht werden. Wenn Sie das entsprechende Kennwort vergessen haben, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 65*.

Zum Festlegen des Kennworts, dieses direkt in das Dialogfeld eingeben.

Die Übersichtsseite

Die Übersichtsseite des AXIS Entry Manager zeigt Informationen wie den Namen, die MAC-Adresse, die IP-Adresse und die Firmwareversion des Türcontrollers an. Mithilfe dieser Angaben lässt sich der Türcontroller im Netzwerk oder im System identifizieren.

Beim ersten Einsatz Zugriff auf das Axis Produkt werden Sie auf der Übersichtsseite aufgefordert, die Hardware zu konfigurieren, Datum und Uhrzeit festzulegen sowie den Türcontroller als Teil eines Systems oder als eigenständiges Gerät zu konfigurieren. Weitere Informationen zum Konfigurieren des Systems, siehe *Konfigurieren – Schritt für Schritt auf Seite 11*.

Um die Übersichtsseite von anderen Webseiten des Produkts aus aufzurufen, in der Menüleiste **Overview (Übersicht)** anklicken.

Systemkonfiguration

Zum Öffnen der Setup-Seiten des Produkts in der oberen rechten Ecke der Übersichtseite **Setup** anklicken.

Dieses Axis Produkt kann von Administratoren konfiguriert werden. Weitere Informationen zu Benutzern und Administratoren, siehe *Seite 31*, *Seite 40* und *Seite 55*.

Konfigurieren – Schritt für Schritt

Vor dem Verwenden des Zutrittskontrollsystems führen Sie bitte folgende Einrichtungsschritte durch:

1. Falls erforderlich, die Spracheinstellung von AXIS Entry Manager ändern (Standardsprache ist Englisch). Siehe *Eine Sprache wählen auf Seite 11*.
2. Datum und Datum einstellen. Siehe *Seite 11*.
3. Die Netzwerkeinstellungen konfigurieren. Siehe *Seite 13*.
4. Den Türcontroller und angeschlossene Geräte konfigurieren (zum Beispiel Lesegeräte, Schlösser und REX-Geräte). Siehe *Konfigurieren der Hardware auf Seite 13*.
5. Die Hardwareanschlüsse überprüfen. Siehe *Seite 20*.
6. Karten und Formate konfigurieren. Siehe *Seite 21*.
7. Das Türcontroller-System konfigurieren. Siehe *Verwalten von Netzwerk-Tür-Controllern auf Seite 26*.

Weitere Informationen zum Konfigurieren und Verwalten der Türen, Zeitpläne, Benutzer und Gruppen des Systems finden Sie unter *Zugangsverwaltung auf Seite 31*.

Empfehlungen zur Wartung finden Sie unter *Wartungsanweisungen auf Seite 29*.

Hinweis

Zum Hinzufügen oder Entfernen von Türcontrollern, Hinzufügen, Entfernen oder Bearbeiten von Benutzern oder zum Konfigurieren der Hardware müssen mehr als die Hälfte aller Türcontroller des Systems **online** sein. Zum Überprüfen des Status von Türcontrollern rufen Sie **Setup > Manage Network Door Controllers in System (Setup > Netzwerk-Türcontroller im System verwalten)** auf.

Eine Sprache wählen

Die Standardsprache von AXIS Entry Manager ist Englisch. Sie kann jedoch in eine beliebigen Sprache geändert werden, die in der Firmware des Produkts enthalten ist. Für weitere Informationen zur aktuell verfügbaren Firmware, siehe *www.axis.com*

Die Sprachen können auf jeder Produktwebseite geändert werden.

Um zwischen Sprachen zu wechseln, die Dropdown-Liste Sprachen  anklicken und eine Sprache wählen. Alle Produktwebseiten und Hilfeseiten des Produkts werden in der gewählten Sprache angezeigt.

Hinweis

- Wenn die Sprache geändert wird, wechselt auch das Datumsformat zu einem in der gewählten Sprache üblichen Format. In den Datenfeldern wird das korrekte Format angezeigt.
- Wenn das Produkt auf die Werkseinstellungen zurückgesetzt wird, wechselt AXIS Entry Manager zurück zu Englisch.
- Wenn das Produkt wiederhergestellt wird, verwendet AXIS Entry Manager weiterhin die gewählte Sprache.
- Wenn das Produkt neugestartet wird, verwendet AXIS Entry Manager weiterhin die gewählte Sprache.
- Wenn Sie die Firmware aktualisieren, verwendet AXIS Entry Manager weiter die ausgewählte Sprache.

Einstellen von Datum und Uhrzeit

Wenn der Tür-Controller Teil eines System ist, werden die Datums- und Uhrzeiteinstellungen von allen Tür-Controllern übernommen. Die Einstellungen werden den anderen Controllern des Systems zugewiesen, egal, ob Sie für die Synchronisierung einen NTP-Server verwenden, die Datums- und Uhrzeiteinstellungen manuell vornehmen oder sie vom Computer abrufen. Aktualisieren Sie die Seite im Browser, wenn die Änderungen nicht angezeigt werden. Weitere Informationen über die Verwaltung von Tür-Controller-Systemen finden Sie unter *Verwalten von Netzwerk-Tür-Controllern auf Seite 26*.

Wechseln Sie zu **Setup > Date & Time (Setup > Datum und Uhrzeit)**, um Datum und Uhrzeit für ein Axis Produkt einzustellen.

Datum und Uhrzeit können auf folgende Arten eingestellt werden:

- Abrufen von Datum und Uhrzeit von einem NTP (Network Time Protocol)-Server. Siehe *Seite 12*.
- Manuelles Einstellen von Datum und Uhrzeit. Siehe *Seite 12*.
- Abrufen von Datum und Uhrzeit vom Computer. Siehe *Seite 13*.

Current controller time (Aktuelle Controller-Zeit) zeigt das aktuelle Datum und die aktuelle Uhrzeit des Tür-Controllers an (24-Stunden-System).

Die gleichen Optionen für Datum und Uhrzeit finden Sie auch auf den Seiten mit Systemoptionen. Rufen Sie **Setup > Additional Controller Configuration > System Options > Date & Time (Setup > Zusätzliche Controller-Konfiguration > Systemoptionen > Datum und Uhrzeit)** auf.

Abrufen von Datum und Uhrzeit von einem NTP (Network Time Protocol)-Server

1. Wechseln Sie zu **Setup > Date & Time (Setup > Datum und Uhrzeit)**.
2. Wählen Sie in der Dropdown-Liste Ihre **Timezone (Zeitzone)** aus.
3. Wählen Sie **Adjust for daylight saving (Automatische Zeitumstellung)** aus, wenn in der jeweiligen Region zwischen Sommer- und Winterzeit umgestellt wird.
4. Wählen Sie **Synchronize with NTP (Mit NTP synchronisieren)** aus.
5. Wählen Sie die Standard-DHCP-Adresse aus, oder geben Sie die Adresse des NTP-Servers ein.
6. Klicken Sie auf **Save (Speichern)**.

Wenn Datum und Uhrzeit mit einem NTP-Server synchronisiert werden, werden diese ständig aktualisiert, da der NTP-Server die Daten mithilfe von Push überträgt. Weitere Informationen zu NTP-Einstellungen finden Sie unter *NTP-Konfiguration auf Seite 60*.

Wenn Sie für den NTP-Server einen Host-Namen verwenden, muss ein DNS-Server konfiguriert werden. Siehe *DNS-Konfiguration auf Seite 60*.

Manuelles Einstellen von Datum und Uhrzeit

1. **Setup > Date & Time (Setup > Datum und Uhrzeit)** aufrufen.
2. Wenn in der jeweiligen Region zwischen Sommer- und Winterzeit umgestellt wird, **Adjust for daylight saving (Automatische Zeitumstellung)** wählen.
3. Wählen Sie **Set date & time manually (Datum und Uhrzeit manuell einstellen)** aus.
4. Geben Sie das Datum und die Uhrzeit ein.
5. Klicken Sie auf **Save (Speichern)**.

Beim manuellen Einstellen von Datum und Uhrzeit werden die Werte einmal eigegeben und nicht automatisch aktualisiert. Da keine Verbindung mit einem externen NTP-Server besteht, müssen Datum und Uhrzeit ggf. manuell aktualisiert werden.

Abrufen von Datum und Uhrzeit vom Computer

1. **Setup > Date & Time (Setup > Datum und Uhrzeit)** aufrufen.
2. Wenn in der jeweiligen Region zwischen Sommer- und Winterzeit umgestellt wird, **Adjust for daylight saving (Automatische Zeitumstellung)** wählen.
3. Wählen Sie **Set date & time manually (Datum und Uhrzeit manuell einstellen)** aus.
4. Klicken Sie auf **Sync now and save (Jetzt synchronisieren und speichern)** aus.

Wenn Sie die Computerzeit verwenden, werden Datum und Uhrzeit einmal mit dem Computer synchronisiert und anschließend nicht mehr automatisch aktualisiert. Daher müssen Sie Datum und Uhrzeit erneut synchronisieren, wenn diese Angaben auf dem Computer geändert wurden.

Konfigurieren der Netzwerkeinstellungen

Um die grundlegenden Netzwerkeinstellungen zu konfigurieren, **Setup > Network Settings (Setup > Netzwerkeinstellungen)** bzw. **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Setup > Zusätzliche Controller-Konfiguration > Systemoptionen > Netzwerk > TCP/IP > Grundeinstellungen)** aufrufen.

Weitere Informationen zu Netzwerkeinstellungen, siehe *Netzwerk auf Seite 58*.

Konfigurieren der Hardware

Um die Türen und Etagen verwalten zu können, muss erst die Hardware auf den Seiten der Hardwarekonfiguration konfiguriert werden.

Türen, Schlösser und andere Geräte können vor Abschluss der Hardwarekonfiguration an das Axis Produkt angeschlossen werden. Das Anschließen von Geräten ist jedoch einfacher, wenn Sie zuerst die Hardwarekonfiguration abschließen, da nach Abschluss der Konfiguration der Kontaktbelegungsplan zur Verfügung steht. Der Kontaktbelegungsplan ist der Leitfaden zum Anschließen der Kontakte sowie die Referenz bei der Wartung. Anweisungen zur Wartung finden Sie auf *Seite 29*.

Führen Sie die erstmalige Konfiguration der Hardware mithilfe einer der folgenden Methoden aus:

- Importieren einer Hardwarekonfigurationsdatei. Siehe *Seite 13*.
- Eine neue Hardwarekonfiguration erstellen. Siehe *Seite 14*.

Hinweis

Falls die Hardware des Produkts noch nicht bereits konfiguriert oder gelöscht wurde, steht dafür die Option **Hardware Configuration (Hardwarekonfiguration)** im Benachrichtigungsbereich der Übersichtsseite zur Verfügung.

Eine Hardwarekonfigurationsdatei konfigurieren

Die Hardwarekonfiguration des Axis Produkts kann schneller abgeschlossen werden, indem eine Hardwarekonfigurationsdatei importiert wird.

Durch das Exportieren der Datei aus einem Produkt und das Importieren in ein anderes können Sie mehrere Kopien der gleichen Hardware-Einrichtung erstellen, ohne die gleichen Schritte wiederholen zu müssen. Sie können exportierte Dateien auch als Sicherungen speichern und diese zum Wiederherstellen vorheriger Hardwarekonfigurationen verwenden. Für weitere Informationen siehe *Eine Hardwarekonfigurationsdatei exportieren auf Seite 14*

So importieren Sie eine Hardwarekonfigurationsdatei:

1. **Setup > Hardware Configuration (Setup > Hardwarekonfiguration)** aufrufen.
2. **Import hardware configuration (Hardwarekonfiguration importieren)** anklicken oder wenn bereits eine Hardwarekonfiguration vorhanden ist **Reset and import hardware configuration (Zurücksetzen und Hardwarekonfiguration importieren)**.
3. Wählen Sie im angezeigten Dateibrowser die Hardwarekonfigurationsdatei (*.json) auf dem Computer aus.

4. Klicken Sie auf **OK**.

Eine Hardwarekonfigurationsdatei exportieren

Die Hardwarekonfiguration des Axis Produkts lässt sich exportieren und so auch für baugleiche Geräte verwenden. Exportierte Dateien können auch als Sicherungskopien gespeichert werden, um diese zum Wiederherstellen vorheriger Hardwarekonfigurationen zu verwenden.

Hinweis

Die Hardwarekonfiguration ganzer Etagen kann nicht exportiert werden.

Die Exportdatei der Hardwarekonfiguration enthält keine Angaben zu drahtlos betriebenen Schlössern.

Die Hardwarekonfigurationsdatei exportieren:

1. **Setup > Hardware Configuration (Setup > Hardwarekonfiguration)** aufrufen.
2. Klicken Sie auf **Export hardware configuration (Hardwarekonfiguration exportieren)**.
3. Je nach verwendetem Browser müssen Sie vor dem Export in einem Dialogfeld weitere Einstellungen vornehmen.

   Wenn nicht anders angegeben, wird die Exportdatei (JSON) im standardmäßigen Downloadordner gespeichert. Den Downloadordner können Sie in den Benutzereinstellungen des Webbrowsers festlegen.

Eine neue Hardwarekonfiguration erstellen

Die Anweisungen gemäß den Installationsvorgaben befolgen:

- *Eine neue Hardwarekonfiguration ohne Peripheriegeräte erstellen. auf Seite 14*
- *Eine neue Hardwarekonfiguration für Funkschlösser erstellen. auf Seite 18*
- *Eine neue Hardwarekonfiguration mit Elevator Control (AXIS A9188) erstellen auf Seite 19*

Eine neue Hardwarekonfiguration ohne Peripheriegeräte erstellen.

1. **Setup > Hardware Configuration (Setup > Hardwarekonfiguration)** aufrufen und **Start new hardware configuration (Neue Hardwarekonfiguration starten)** anklicken.
2. Einen Namen für das Axis Produkt eingeben.
3. Die Anzahl der angeschlossenen Türen wählen und **Next (Weiter)** anklicken.
4. Die Türmonitore (Türpositionssensoren) und Schlösser konfigurieren und **Next (Weiter)** anklicken. Weitere Informationen zu den verfügbaren Optionen, siehe *Schlösser und Türmonitore konfigurieren auf Seite 14*.
5. Die zu verwendenden Lesegeräte und REX-Geräte wählen und **Finish (Beenden)** anklicken. Weitere Informationen zu den verfügbaren Optionen, siehe *Konfigurieren von Lesern und REX-Geräten auf Seite 17*.
6. **Close (Schließen)** oder den Link zur Kontaktbelegungsübersicht anklicken.

Schlösser und Türmonitore konfigurieren

Nach Wählen einer Türoption in der neuen Hardwarekonfiguration können die Türmonitore und Schlösser konfiguriert werden.

1. Wenn ein Türmonitor verwendet wird, **Door monitor (Türmonitor)** und anschließend die den Schaltkreisen des Türmonitors entsprechenden Optionen wählen.
2. Wenn das Türschloss verriegelt werden soll, sobald die Tür geöffnet wurde, wählen Sie **Cancel access time once door is opened (Zugangsdauer nach dem Öffnen der Tür begrenzen)** aus.

Wenn Sie die erneute Verriegelung hinauszögern möchten, setzen Sie die Verzögerungszeit in Millisekunden in **Verriegelungszeit**.

3. Legen Sie die Zeitoptionen für den Türmonitor fest oder, wenn kein Türmonitor verwendet wird, die Zeitoptionen für das Schloss.
4. Wählen Sie die Einstellungen passend zu den Stromkreisen des entsprechenden Schlosses aus.
5. Wenn ein Schlossmonitor verwendet wird, wählen Sie **Lock monitor (Schlossmonitor)** und anschließend die Optionen passend zu den Stromkreisen des entsprechenden Schlossmonitors aus.
6. Wenn Sie die Eingangsanschlüsse von Lesern, REX-Geräten und Türmonitoren überwachen möchten, wählen Sie **Enable supervised inputs (Überwachte Eingänge aktivieren)** aus.

   Weitere Informationen, siehe *Überwachte Eingänge verwenden: auf Seite 17*

Hinweis

- Die meisten Optionen für Schlösser, Türmonitore und Leser können angepasst werden, ohne dass Sie das Gerät zurücksetzen und eine neue Hardwarekonfiguration durchführen müssen. Rufen Sie **Setup > Hardware Reconfiguration (Setup > Hardwareneukonfiguration)** auf.
- Mit jedem Tür-Controller kann nur ein Schlossmonitor verbunden werden. Wenn Sie Türen mit Doppelschlössern verwenden, kann nur eines der Schlösser über einen Schlossmonitor verfügen. Wenn zwei Türen mit dem gleichen Tür-Controller verbunden sind, können keine Schlossmonitore verwendet werden.
- Motorschlösser müssen als sekundäre Schlösser konfiguriert werden.

Informationen zu Türmonitoren und Zeitoptionen

Die folgenden Türmonitor-Optionen sind verfügbar:

- **Türmonitor** – Standardmäßig ausgewählt. Jede Tür verfügt über einen eigenen Türmonitor, der beispielsweise angibt, ob eine Tür aufgebrochen wurde oder zu lange geöffnet bleibt. Diese Option deaktivieren, wenn kein Türmonitor verwendet wird.
  - **Offener Schaltkreis = Tür geschlossen** – Wählen, wenn der Türmonitor-Schaltkreis normalerweise geöffnet ist. Der Türmonitor gibt bei geschlossenem Stromkreis an, dass die Tür geöffnet ist. Die Türmonitor gibt bei offenem Stromkreis an, dass die Tür geschlossen ist.
  - **Offener Stromkreis = Tür geöffnet** – Wählen, wenn der Türmonitor-Schaltkreis normalerweise geschlossen ist. Der Türmonitor gibt bei offenem Stromkreis an, dass die Tür geöffnet ist. Der Türmonitor gibt bei geschlossenem Stromkreis an, dass die Tür geschlossen ist.
- **Zugangsdauer aufheben, wenn die Tür geöffnet ist** – Wählen, um Doppelzutritt zu verhindern. Sobald der Türmonitor anzeigt, dass die Tür geöffnet wurde, schließt sich das Schloss.

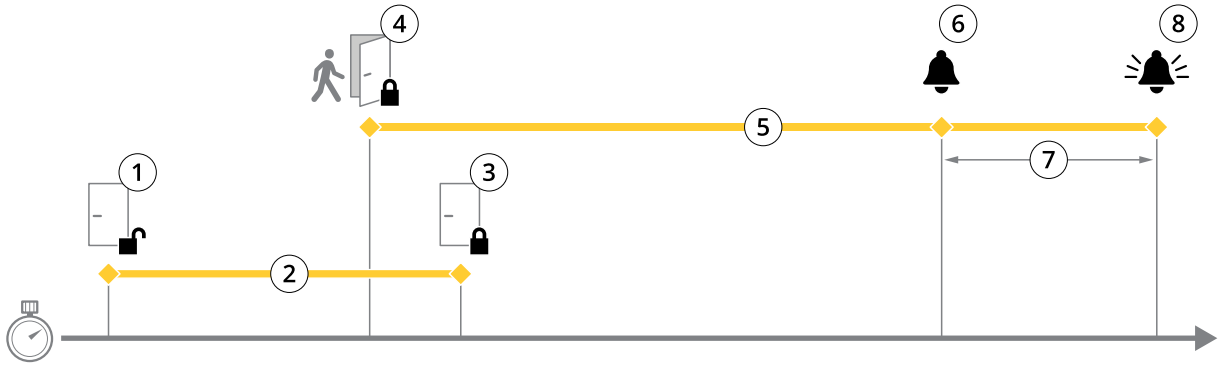
Folgende Zeitoptionen für Türen stehen immer zur Verfügung:

- **Zugangsdauer** – Die Anzahl von Sekunden einstellen, die die Tür geöffnet bleiben soll, nachdem Zugang gewährt wurde. Die Tür bleibt entriegelt, bis die Tür geöffnet oder die festgelegte Dauer erreicht wurde. Die Tür wird verriegelt, wenn sie geschlossen wird. Auch, wenn die Zugangsdauer nicht erreicht wurde.
- **Lange Zugangsdauer** – Die Anzahl von Sekunden einstellen, die die Tür entriegelt bleiben soll, nachdem Zugang gewährt wurde. Die lange Zugangsdauer überschreibt die bereits festgelegte Zugangsdauer. Sie wird für Benutzer aktiviert, für die die lange Zugangsdauer gewählt ist. Siehe *Zugangsdaten für Benutzer auf Seite 41*

Türmonitor wählen, um die folgenden Zeitoptionen für Türen wählbar zu machen:

- **Maximale Öffnungsdauer** – Die Anzahl von Sekunden festlegen, die die Tür maximal geöffnet bleiben darf. Wenn die festgelegte Dauer erreicht wird, wird der Alarm für die maximale Öffnungsdauer ausgelöst. Eine Aktionsregel einrichten, die festlegt, welche Aktion ausgelöst werden soll, wenn die maximale Öffnungsdauer überschritten wird.
- **Voralarmdauer** – Ein Voralarm ist ein Warnsignal, das ausgelöst wird, bevor die maximale Öffnungsdauer der Tür überschritten wird. Die Aktionsregel informiert und warnt den Administrator (und je nach Konfiguration der Aktionsregel

auch die Person an der Tür), dass die Tür geschlossen werden muss oder sonst der Alarm für die maximale Öffnungsdauer ausgelöst wird. Festlegen, wie viele Sekunden vor dem Auslösen eines Alarms aufgrund der Überschreitung der maximalen Öffnungsdauer das System den Voralarm auslösen soll. Legen Sie die Voralarmdauer auf 0 fest, um den Voralarm zu deaktivieren.



1 *Zugang gewährt – Schloss entriegelt*
2 *Zugangsdauer*
3 *Keine Aktion ausgeführt – Schloss verriegelt*
4 *Aktion ausgeführt (Tür geöffnet) – Schloss verriegelt oder bleibt entriegelt, bis die Tür geschlossen wird*
5 *Zu lange geöffnet*
6 *Voralarm wird ausgelöst*
7 *Voralarmdauer*
8 *Zu lange geöffnet – Alarm wird ausgelöst*

Weitere Informationen zum Einrichten einer Aktionsregel finden Sie unter *Aktionsregeln einrichten auf Seite 47*.

Informationen zu Schlossoptionen

Verfügbare Optionen für den Schaltkreis des Schlosses:

- 12 V
  - **Arbeitsstrom** – Für Schlösser wählen, die bei Stromausfällen verriegelt bleiben. Wenn Strom angelegt wird, entriegelt sich das Schloss.
  - **Ruhestrom** – Für Schlösser wählen, die bei Stromausfällen entriegelt werden. Wenn Strom angelegt wird, verriegelt sich das Schloss.
- **Relais** – Kann nur für ein Schloss pro Türcontroller verwendet werden. Sind zwei Türen mit dem Türcontroller verbunden, kann ein Relais nur am Schloss der zweiten Tür verwendet werden.
  - **Relais geöffnet = verriegelt** – Für Schlösser wählen, die bei geöffnetem Relais verriegelt bleiben (Arbeitsstrom). Wenn sich das Relais schließt, wird das Schloss entriegelt.
  - **Relais geöffnet = entriegelt** – Für Schlösser wählen, die bei Stromausfällen entriegelt werden (Ruhestrom). Wenn sich das Relais schließt, wird das Schloss verriegelt.
- **Keine** – Wählen, wenn nur ein Schloss verwendet wird. Nur verfügbar für Schloss 2.

Die folgenden Schlossüberwachungsoptionen sind für Konfigurationen mit einer Tür verfügbar:

- **Lock Monitor** – Wählen, um die Lock Monitor - Steuerelemente zu aktivieren. Dann das zu überwachende Schloss wählen. Eine Schlossüberwachung kann nur bei Doppelschlosstüren verwendet werden. Sie kann nicht verwendet werden, wenn zwei Türen mit dem Türcontroller verbunden sind.

- **Offener Schaltkreis = verriegelt** – Wählen, wenn der Schaltkreis der Schlossüberwachung normalerweise geschlossen ist. Wenn der Schaltkreis geschlossen ist, zeigt die Schlossüberwachung eine unverriegelte Tür an. Wenn der Schaltkreis geöffnet ist, zeigt die Schlossüberwachung eine verriegelte Tür an.
- **Offener Schaltkreis = entriegelt** – Wählen, wenn der Schaltkreis der Schlossüberwachung normalerweise geöffnet ist. Wenn der Schaltkreis geöffnet ist, zeigt die Schlossüberwachung eine unverriegelte Tür an. Wenn der Schaltkreis geschlossen ist, zeigt die Schlossüberwachung eine verriegelte Tür an.

Konfigurieren von Lesern und REX-Geräten

Nach dem Konfigurieren der Türmonitore und Schlösser in der neuen Hardware können die Lesegeräte und Anfragen an Ausgangsgeräte (REX) konfiguriert werden.

1. Wenn ein Reader verwendet wird, aktivieren Sie das Kontrollkästchen und wählen Sie dann die Optionen aus, die dem Kommunikationsprotokoll des Readers entsprechen.
2. Wenn ein REX-Gerät wie ein Taster, ein Sensor oder eine Druckstange verwendet wird, das Wahlfeld aktivieren und anschließend die den Schaltkreisen des REX-Geräts entsprechenden Optionen wählen.

   Wenn das REX-Signal nicht auf das Öffnen der Tür wirkt (zum Beispiel bei Türen mit Klinken oder Druckstangen) **REX does not unlock door (Kein Öffnen der Tür durch REX)** wählen.
3. Zum Anschließen von mehr als einem Leser oder REX-Gerät an den Türcontroller die vorherigen beiden Schritte für alle Lesegeräte und REX-Geräte wiederholen.

Informationen zu Optionen für Lesegräte und REX-Geräte

Für Lesergeräte stehen folgende Optionen zur Verfügung:

- **Wiegand** – Diese Option für Lesegeräte wählen, die Wiegand-Protokolle verwenden. Anschließend die vom Lesegerät unterstützte LED-Steuerung wählen. Leser mit einer einfachen LED-Steuerung wechseln für gewöhnlich zwischen Rot und Grün. Leser mit einer dualen LED-Steuerung verwenden verschiedene Adern für die roten und grünen LEDs. Dadurch werden die LEDs unabhängig voneinander gesteuert. Wenn beide LEDs eingeschaltet sind, leuchtet das Licht gelb. Die vom Lesegerät unterstützten LED-Steuerungen sind in den Herstellerinformationen aufgeführt
- **OSDP, RS-485 Halbduplex** – Diese Option für RS485-Lesegeräte mit Unterstützung für Halbduplex wählen. Die vom Lesegerät unterstützten Protokolle sind in den Herstellerinformationen aufgeführt

Für REX-Geräte stehen folgende Optionen zur Verfügung:

- **Active low (Aktiv niedrig)** – Diese Option wählen, wenn das Aktivieren des REX-Geräts den Schaltkreis schließt.
- **Active high (Aktiv hoch)** – Diese Option wählen, wenn das Aktivieren des REX-Geräts den Schaltkreis öffnet.
- **REX does not unlock door (Kein Öffnen der Tür durch REX)** – Diese Option wählen, wenn das REX-Signal nicht auf das Öffnen der Tür wirkt (zum Beispiel bei Türen mit Klinken oder Druckstangen). Der Zwangsöffnungsalarm wird nicht ausgelöst, solange der Benutzer die Tür innerhalb der Zugangszeit öffnet. Diese Option deaktivieren, wenn die Tür automatisch entriegelt werden soll, sobald der Benutzer das REX-Gerät aktiviert.

Hinweis

Die meisten Optionen für Schlösser, Türmonitore und Lesegeräte können ohne Zurücksetzen des Geräts oder neues Konfigurieren der Hardware geändert werden. Rufen Sie **Setup > Hardware Reconfiguration (Setup > Hardwareneukonfiguration)** auf.

Überwachte Eingänge verwenden:

Bei diesen Eingängen wird der Status der Verbindung zwischen Türcontroller und Lesern, REX-Geräten und Türmonitoren überwacht. Bei Unterbrechung der Verbindung wird ein Ereignis ausgelöst.

Um überwachte Eingänge zu verwenden:

1. Bringen Sie an allen verwendeten Eingängen Abschlusswiderstände an. Siehe Anschlussschaltbild unter *Seite 75*.

2. **Setup > Hardware-Rekonfiguration (Setup > Hardwareneukonfiguration)** aufrufen und **Enable supervised inputs (Überwachte Eingänge aktivieren)** wählen. Die Option Überwachte Eingänge kann auch während der Hardwarekonfiguration aktiviert werden.

Informationen zur Kompatibilität überwachter Eingänge

Die folgenden Anschlüsse unterstützen überwachte Eingänge:

- Anschluss E/A Lesegerät – Manipulationssignal. Siehe *Seite 70*.
- Türanschluss. Siehe *Seite 71*.

Zu den Lesegeräten und Schaltern, die mit überwachten Eingängen verwendet werden können, gehören:

- Leser und Schalter mit internem 1-kΩ-Pullup-Widerstand gegen 5 V.
- Leser und Schalter ohne internen Pullup-Widerstand.

Eine neue Hardwarekonfiguration für Funkschlösser erstellen.

1. **Setup > Hardware Configuration (Setup > Hardwarekonfiguration)** aufrufen und **Start new hardware configuration (Neue Hardwarekonfiguration starten)** anklicken.
2. Einen Namen für das Axis Produkt eingeben.
3. Aus der Liste der Peripheriegeräte einen Hersteller von drahtlosen Gateways wählen.
4. Um eine verdrahtete Tür anzuschließen, das Wahlfeld **1 Door (Tür)** markieren und **Next (Weiter)** anklicken. Wenn keine Tür aufgeführt ist, **Finish (Abschließen)** anklicken.
5. Dem Hersteller des Schlosses entsprechend nach einem der folgenden Gliederungspunkte verfahren:
   - **ASSA Aperio**: Den Link zur Belegungsübersicht der Hardwarepins anklicken oder **Schließen** und **Setup > Hardware Reconfiguration (Setup > Neue Hardwarekonfiguration)** wählen, um die Konfiguration abzuschließen. Siehe dazu *Türen und Geräte des Typs Assa Aperio™ hinzufügen auf Seite 18*.
   - **SmartIntego**: Den Link zur Belegungsübersicht der Hardwarepins anklicken oder **Click here to select wireless gateway and configure doors (Hier klicken, um Funkgateways zu wählen und Türen zu konfigurieren)** wählen, um die Konfiguration abzuschließen. Siehe dazu *SmartIntego konfigurieren auf Seite 26*.

Türen und Geräte des Typs Assa Aperio™ hinzufügen

Vor dem Hinzufügen einer Funktür zum System muss diese mithilfe des Aperio PAP (Aperio-Programmieranwendungstool) mit dem angeschlossenen Assa Aperio-Kommunikationshub verbunden werden.

So fügen Sie eine Funktür hinzu:

1. Rufen Sie **Setup** > **Hardware Reconfiguration (Hardwareneukonfiguration)** auf.
2. Klicken Sie unter Wireless Doors and Devices (Funktüren und -geräte) auf **Add door (Tür hinzufügen)**.
3. Geben Sie im Feld **Door name (Türname)** einen beschreibenden Namen ein.
4. Geben Sie im Feld **ID** unter **Lock (Schloss)** Die aus sechs Zeichen bestehende Adresse des hinzuzufügenden Geräts eingeben. Die Geräteadresse befindet sich auf dem Produktaufkleber.
5. Optional auch unter **Türpositionssensor**: **Built in door position sensor (Integrierter Türpositionssensor)** oder **External door position sensor (Externer Türpositionssensor)** wählen.

Hinweis

Vor dem Konfigurieren eines externen Türpositionssensors (DPS) sicherstellen, dass das Aperio-Schließgerät die Türgriffstatuserkennung unterstützt.

6. Optional auch im**ID**-Feld unter **Türpositionssensor**: Die aus sechs Zeichen bestehende Adresse des Geräts eingeben, das hinzugefügt werden soll. Die Geräteadresse befindet sich auf dem Produktaufkleber.
7. Klicken Sie auf **Add (Hinzufügen)**.

Eine neue Hardwarekonfiguration mit Elevator Control (AXIS A9188) erstellen

Wichtig

Vor dem Erstellen einer Hardwarekonfiguration einen Benutzer zum AXIS A9188 Network I/O Relay Module hinzufügen. Dazu über die Weboberfläche des A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Benutzereinstellungen > Weitere Gerätekonfigurationen > Grundeinstellungen > Benutzer > Hinzufügen> Benutzer einrichten)** aufrufen.

Hinweis

Pro Network Door Controller können maximal zwei AXIS 9188 Network I/O Relay Module konfiguriert werden.

1. Unter A1001 **Setup > Hardware Configuration (Setup > Hardwarekonfiguration)** aufrufen und **Neue Hardwarekonfiguration starten** aufrufen.
2. Einen Namen für das Axis Produkt eingeben.
3. Um ein AXIS A9188 Network I/O Relay Module aufzunehmen, aus der Liste der Netzwerkperipheriegeräte **Elevator Control** wählen, und **Next (weiter)** anklicken.
4. Einen Namen für das angeschlossene Lesegerät eingeben.
5. Das auf das Lesegerät anzuwendende Protokoll wählen und **Finish (Beenden)** wählen.
6. **Networkperipheriegeräte** anklicken, um die Konfiguration abzuschließen, siehe *Netzwerkperipheriegeräte hinzufügen und einrichten auf Seite 19* oder den Link zur Belegungsübersicht der Hardwarekontakte anklicken.

Netzwerkperipheriegeräte hinzufügen und einrichten

Wichtig

- Vor dem Einrichten von Netzwerkperipheriegeräten einen Benutzer im AXIS A9188 Network I/O Relay Module einrichten. Dazu über die Weboberfläche des AXIS A9188 >**Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Benutzereinstellungen > Weitere Gerätekonfigurationen > Grundeinstellungen > Benutzer > Hinzufügen> Benutzer einrichten)** aufrufen.
- Fügen Sie keinen weiteren AXIS A1001 Network Door Controller als Netzwerkperipheriegerät hinzu.

1. Um ein Gerät hinzuzufügen, **Setup > Network Periphals (Netzwerkperipheriegeräte)** aufrufen.
2. Das oder die Geräte über **Discovered devices (Ermittelte Geräte)** ermitteln.
3. **Add this device (Dieses Gerät hinzufügen)** anklicken.
4. Einen Namen für das Gerät angeben.
5. Den Benutzernamen und das Kennwort für das AXIS A9188 eingeben.
6. Auf **Add (Hinzufügen)** klicken.

Hinweis

Netzwerkperipheriegeräte können manuell über das Dialogfeld **Manually add device (Gerät manuell hinzufügen)** durch Eingabe der MAC- oder IP-Adresse hinzugefügt werden.

Wichtig

Wenn Sie einen Zeitplan löschen möchten, stellen Sie zunächst sicher, dass er nicht vom E/A-Relaismodul des Netzwerks verwendet wird.

E/As und Relais in Netzwerkperipheriegeräten einrichten

Wichtig

Vor dem Einrichten von Netzwerkperipheriegeräten einen Benutzer im AXIS A9188 Network I/O Relay Module einrichten. Dazu über die Weboberfläche des AXIS A9188 >**Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Benutzereinstellungen > Weitere Gerätekonfigurationen > Grundeinstellungen > Benutzer > Hinzufügen> Benutzer einrichten)** aufrufen.

1. **Setup > Network Periphals (Netzwerkperipheriegeräte)** aufrufen und **Added devices row (Zeile Hinzugefügte Geräte)** anklicken.
2. Die als Etage zu setzenden E/As und Relais wählen
3. **Set as floor (Als Etage setzen)** anklicken und einen Namen eingeben.
4. Auf **Add (Hinzufügen)** klicken.

Die Etage wird jetzt auf der Registerkarte **Floor (Etage)** unter **Access Management (Zugangsverwaltung)** angezeigt.

Hinweis

Im AXIS Entry Manager können Sie maximal 16 Etagen hinzufügen.

Überprüfen der Hardwareanschlüsse

Die angeschlossenen Türmonitore, Schlösser und Leser können überprüft werden nach Abschluss von Installation und Konfiguration sowie jederzeit während der gesamten Nutzungsdauer des Türcontrollers.

Um die Konfiguration zu prüfen und den entsprechenden Bereich zu öffnen, **Setup > Hardware Connection Verification (Setup > Überprüfen der Hardwareanschlüsse)** aufrufen.

Steuerelemente der Türüberprüfung

- **Door state (Türstatus)** – Den aktuellen Status von Türmonitoren, Türalarmen und Schlössern überprüfen. **Get current state (Aktuellen Status abrufen)** anklicken.
- **Lock (Verriegeln)** – Das Schloss manuell sperren. Betrifft primäre und sekundäre Schlösser (sofern vorhanden). **Lock (Verriegeln)** oder **Unlock (Entriegeln)**.
- **Lock (Verriegeln)** – Schloss manuell zum Gewähren von Zugang auslösen. Betrifft nur primäre Schlösser. **Access (Zugang)** anklicken.
- **Lesegerät: Feedback** – Das Feedback von Lesegeräten zu Befehlen überprüfen, zum Beispiel akustische Meldungen und LED-Signale. Wählen Sie den Befehl aus, und klicken Sie auf **Test (Testen)**. Die Typen des verfügbaren Feedbacks variieren ja nach Leser. Weitere Informationen, siehe*Leser-Feedback auf Seite 52* Siehe dazu auch die Anleitung des Herstellers.
- **Lesegerät: Tampering (Manipulation)** – Informationen zum letzten Manipulationsversuch aufrufen. Der erste Manipulationsversuch wird beim Installieren des Lesegeräts aufgezeichnet. **Get last tampering (Letzte Manipulation aufrufen)** anklicken.
- **Lesegerät: Card swipe (Swipe-Karte)** – Informationen zur letzten angewendeten Swipe-Karte oder anderen vom Lesegerät akzeptierten Berechtigungsnachweisen aufrufen. **Get last credential (Letzten Berechtigungsnachweis aufrufen)** anklicken.
- **REX** – Informationen zur letzten Anfrage zum Verlassen (REX) über eine Drucktaste aufrufen. Klicken Sie auf **Get last REX (Letzte REX-Betätigung abrufen)**.

Steuerelemente der Etagenüberprüfung

- **Floor Status (Etagenstatus)** – Den aktuellen Status des Etagenzugangs überprüfen. **Get current state (Aktuellen Status aufrufen)** anklicken.

- **Floor lock & unlock (Sperren und Freigeben von Etagen)** – Etagenzugang manuell auslösen. Betrifft sowohl primäre als auch sekundäre Schlösser (sofern vorhanden). **Lock (Sperren)** oder **Unlock (Entriegeln)** anklicken.
- **Floor Access (Etagenzugang)** – Manuell zeitweiligen Etagenzugang einräumen. Betrifft nur primäre Schlösser. **Access (Zugang)** anklicken.
- **Fahrstuhllesegerät: Feedback** – Das Feedback von Lesegeräten zu Befehlen überprüfen, zum Beispiel akustische Meldungen und LED-Signale. Wählen Sie den Befehl aus, und klicken Sie auf **Test (Testen)**. Die Typen des verfügbaren Feedbacks variieren ja nach Leser. Weitere Informationen, siehe *Leser-Feedback auf Seite 52*. Siehe dazu auch die Anleitung des Herstellers.
- **Fahrstuhllesegerät: Tampering (Manipulation)** – Informationen zum letzten Manipulationsversuch aufrufen. Der erste Manipulationsversuch wird beim Installieren des Lesegeräts aufgezeichnet. **Get last tampering (Letzten Manipulationsversuch aufrufen)** anklicken.
- **Fahrstuhllesegerät: Card swipe (Swipe-Karte)** – Informationen zur letzten angewendeten Swipe-Karte oder anderen vom Lesegerät akzeptierten Berechtigungsnachweisen aufrufen. **Get last credential (Letzten Berechtigungsnachweis aufrufen)** anklicken.
- **REX** – Informationen zur letzten Anfrage zum Verlassen (REX) über eine Drucktaste aufrufen. Klicken Sie auf **Get last REX (Letzte REX-Betätigung abrufen)**.

Karten und Formate konfigurieren

Der Türcontroller verfügt über einige vordefinierte, häufig verwendete Kartenformate, die direkt verwendet oder je nach Anforderung geändert werden können. Außerdem können Sie benutzerdefinierte Kartenformate erstellen. Jedes Kartenformat verfügt über einen eigenen Satz an Regeln (Feldzuordnungen), die die Organisation der auf der Karte gespeicherten Informationen bestimmen. Durch Definieren des Kartenformats wird festgelegt, wie das System die Informationen interpretiert, die der Controller vom Lesegerät erhält. Für Informationen zu den vom Lesegerät unterstützten Kartenformate, siehe die Anweisungen des Herstellers.

Kartenformate aktivieren:

1. **Setup > Configure cards and formats (Setup >Karten und Formate konfigurieren)** aufrufen.
2. Ein oder mehrere Kartenformate wählen, die von den verbundenen Lesern unterstützt werden.

Ein neues Kartenformat erstellen:

1. **Setup >Karten und Formate konfigurieren** aufrufen.
2. **Add card format (Kartenformat hinzufügen)** aufrufen.
3. Im Dialogfenster **Add card format (Kartenformat hinzufügen)** einen Namen, eine Beschreibung und die Bitlänge des Kartenformats eingeben. Siehe *Beschreibungen der Kartenformate auf Seite 22*.
4. Klicken Sie auf **Add field map (Feldzuordnung hinzufügen)**, und geben Sie die erforderlichen Informationen in die Felder ein. Siehe *Feldzuordnungen auf Seite 22*.
5. Zum Hinzufügen von mehreren Feldzuordnungen wiederholen Sie den letzten Schritt.

Zum Anzeigen zusätzlicher Informationen eines Elements in der Liste **Card formats (Kartenformate)**, etwa der Beschreibung des Kartenformats und der Feldzuordnung, anklicken.

Zum Bearbeiten eines Kartenformats, anklicken und die Beschreibung des Kartenformats und der Feldzuordnung ändern. Klicken Sie anschließend auf **Save (Speichern)**.

Zum Löschen einer Feldzuordnung im Dialogfeld **Kartenformat bearbeiten** oder **Kartenformat hinzufügen**, anklicken.

Zum Löschen eines Kartenformats, anklicken.

Wichtig

- Jede Änderung an den Kartenformaten gilt für das gesamte System von Tür-Controllern.
- Kartenformate können nur aktiviert oder deaktiviert werden, wenn mindestens ein Türcontroller im System mit mindestens einem Leser konfiguriert wurde. Siehe *Konfigurieren der Hardware auf Seite 13* und *Konfigurieren von Lesern und REX-Geräten auf Seite 17*.
- Zwei Kartenformate mit der gleichen Bitlänge können nicht gleichzeitig aktiviert sein. Wenn beispielsweise zwei Kartenformate mit 32 Bit als „Format A" und „Format B" definiert wurden und „Format A" aktiviert ist, kann „Format B" erst dann aktiviert werden, wenn „Format A" zuvor deaktiviert wurde.
- Wenn keine Kartenformate aktiviert wurde, können die Identifikationstypen **Card raw only (Nur Rohdatenkarte)** und **Card raw and PIN (Rohdatenkarte und PIN)** verwendet werden, um eine Karte zu identifizieren und Benutzern Zugang zu gewähren. Dies wird jedoch nicht empfohlen, da Leser von verschiedenen Herstellern oder mit unterschiedlichen Einstellungen, für die Karten verschiedene Rohdaten generieren können.

Beschreibungen der Kartenformate

- **Name** (erforderlich) – Einen aussagekräftigen Namen eingeben.
- **Description (Beschreibung)** – Bei Bedarf weitere Informationen eingeben. Diese Informationen werden nur in den Dialogfenstern **Edit card format (Kartenformat bearbeiten)** und **Add card format (Kartenformat hinzufügen)** angezeigt.
- **Bit length (Bitlänge)** (erforderlich) – Die Bitlänge des Kartenformats eingeben. Dies muss ein numerischer Wert zwischen 1 und 1000000000 sein.

Feldzuordnungen

- **Name** (erforderlich) – Den Namen der Feldzuordnung ohne Leerzeichen eingeben. Zum Beispiel `UngeradeParität`.

  Beispiele gängiger Feldzuordnungen:

  - `Parity` – Paritätsbits werden zum Ermitteln von Fehlern verwendet. Paritätsbits werden in der Regel an den Anfang oder das Ende einer Binärcode-Zeichenfolge gestellt. Sie geben an, ob die Anzahl der Bits gerade oder ungerade ist.
  - `EvenParity` – Gerade Paritätsbits stellen sicher, dass die Zeichenfolge eine gerade Anzahl an Bits enthält. Die Bits mit dem Wert „1" werden gezählt. Wenn die Anzahl bereits gerade ist, wird das Paritätsbit auf den Wert 0 festgelegt. Wenn die Anzahl ungerade ist, wird das Paritätsbit auf den Wert auf 1 festgelegt, sodass die Gesamtanzahl eine gerade Zahl aufweist.
  - `OddParity` – Ungerade Paritätsbits stellen sicher, dass die Zeichenfolge eine ungerade Anzahl an Bits enthält. Die Bits mit dem Wert „1" werden gezählt. Wenn die Anzahl bereits ungerade ist, wird das Paritätsbit auf den Wert 0 festgelegt. Wenn die Anzahl gerade ist, wird das Paritätsbit auf den Wert 1 festgelegt, sodass die Gesamtanzahl eine ungerade Zahl aufweist.
  - `FacilityCode` – Anlagencodes werden gelegentlich verwendet, um sicherzustellen, dass das Token dem angeforderten Zugangsdaten-Batch des Endbenutzers entspricht. In Altsystemen der Zugangskontrolle wurde der Anlagencode für eine eingeschränkte Überprüfung verwendet. Diese gewährte allen Mitarbeitern Zugang, deren Daten mit dem entsprechenden Standortcode codiert wurden. Dieser Feldzuordnungsname berücksichtigt Groß- und Kleinschreibung und wird vom Produkt zum Überprüfen de Anlagencodes benötigt
  - `CardNr` – Die Kartennummer oder Benutzerkennung ist das von Zugangskontrollsystemen am häufigsten überprüfte Kriterium. Dieser Feldzuordnungsname berücksichtigt Groß- und Kleinschreibung und wird vom Produkt zum Überprüfen der Kartennummer benötigt
  - `CardNrHex` – Die binären Kartendaten sind im Produkt in Form von Hexadezimalzahlen in Kleinschreibung codiert. Sie werden hauptsächlich für die Fehlebehebung verwendet, wenn vom Lesegerät nicht die erwartete Kartennummer ausgegeben wird.
- **Range** – (erforderlich) – Der Bereich) der Feldzuordnung, zum Beispiel 1, 2–17, 18–33 und 34.
- **Encoding** (erforderlich) – Gibt den für die jeweilige Feldzuordnung gewählten Codierungstyp an.

- **BinLE2Int**– Die Binärdaten werden als ganze Zahlen in der Bit-Reihenfolge Little-Endian codiert. Ganze Zahlen sind Zahlen ohne Dezimalstellen. Bei der Bit-Reihenfolge Little-Endian ist das erste Bit das kleinste (mit der geringsten Bedeutung).
- **BinBE2Int** – Die Binärdaten werden als ganze Zahlen in der Bit-Reihenfolge Big-Endian codiert. Ganze Zahlen sind Zahlen ohne Dezimalstellen. Bei der Bit-Reihenfolge Big-Endian ist das erste Bit das größte (mit der größten Bedeutung).
- **BinLE2Hex** – Die Binärdaten werden als Hexadezimalzahlen in Kleinschreibung in der Bit-Reihenfolge Little-Endian codiert. Das Hexadezimalsystem ist ein Stellenwertsystem zur Basis 16 und verwendet 16 eindeutige Zeichen: die Ziffern 0 bis 9 und die Buchstaben a bis f. Bei der Bit-Reihenfolge Little-Endian ist das erste Bit das kleinste (mit der geringsten Bedeutung).
- **BinBE2Hex** – Die Binärdaten werden als Hexadezimalzahlen in Kleinschreibung in der der Bit-Reihenfolge Big-Endian codiert. Das Hexadezimalsystem ist ein Stellenwertsystem zur Basis 16 und verwendet 16 eindeutige Zeichen: die Ziffern 0 bis 9 und die Buchstaben a bis f. Bei der Bit-Reihenfolge Big-Endian ist das erste Bit das größte (mit der größten Bedeutung).
- **BinLEIBO2Int** – Die Binärdaten sind wie bei BinLE2Int codiert, aber die Rohkartendaten werden als Abfolge mehrerer Bytes in umgekehrter Reihenfolge ausgelesen, bevor Feldzuordnungen zum Kodieren aufgerufen werden.
- **BinBEIBO2Int** – Die Binärdaten sind wie bei BinLE2Int codiert, aber die Rohkartendaten werden als Abfolge mehrerer Bytes in umgekehrter Reihenfolge ausgelesen, bevor Feldzuordnungen zum Kodieren aufgerufen werden.

Informationen zu den von Ihrem Kartenformat verwendeten Feldzuordnungen finden Sie in der Anleitung des Herstellers.

Voreingestellter Einrichtungscode

Mithilfe von Einrichtungscodes lässt sich überprüfen, ob ein Token mit dem Zugangskontrollsystem einer Einrichtung übereinstimmt. Oft weisen alle Tokens einer bestimmten Einrichtung den gleichen Einrichtungscode auf. Einen voreingestellten Einrichtungscode verwenden, um in der Chargenverarbeitung Karten einfacher manuell zu registrieren. Der voreingestellte Einrichtungscode wird beim Hinzufügen von Benutzern automatisch eingesetzt. Siehe dazu *Zugangsdaten für Benutzer auf Seite 41*.

Einen voreingestellten Einrichtungscode anlegen:

1. **Setup > Configure cards and formats (Karten und Formate konfigurieren)** aufrufen.
2. Unter **Preset facility code (Voreingestellter Einrichtungscode)**: Einen Einrichtungscode eingeben
3. **Set facility code (Einrichtungscode übernehmen)** anklicken.

Dienste konfigurieren

Mit der Option Dienste konfigurieren auf der Seite Setup werden mit dem Türcontroller nutzbare externe Dienste eingerichtet.

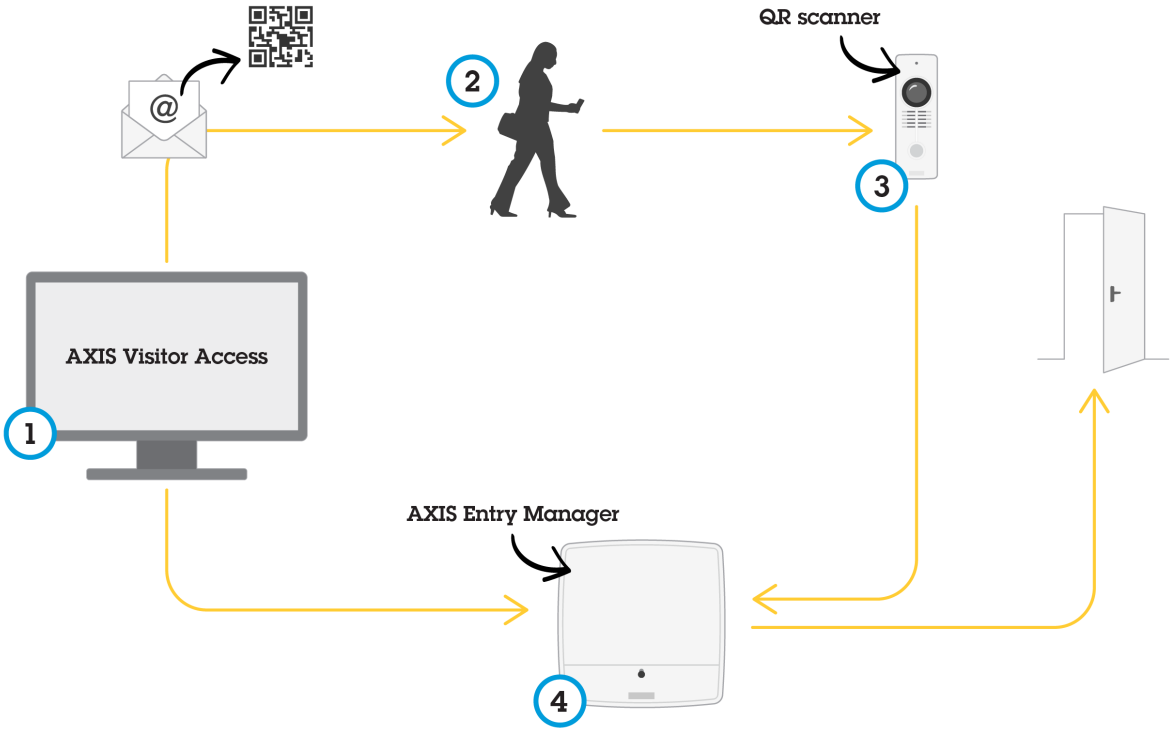
AXIS Visitor Access

Sie können mit dem AXIS Visitor Access temporäre Anmeldedaten in Form eines QR-Codes erstellen. Der QR-Code wird von einer Axis Netzwerk-Kamera oder einer mit dem Zutrittskontrollsystem verbundenen Türstation gescannt.

Dieser Dienst besteht aus:

- einem Axis Tür-Controller mit AXIS Entry Manager und Firmware-Version 1.65.2 oder höher
- einer Axis Netzwerk-Kamera oder Türstation mit der installierten QR-Scanner-Anwendung
- einem Windows® PC mit der installierten AXIS Visitor Access-Anwendung

Systemkonfiguration



Nutzung des AXIS Visitor Access-Dienstes

Der Nutzer erstellt eine Einladung im AXIS Visitor Access (1) und schickt diese an die E-Mail-Adresse des Besuchers. Gleichzeitig werden die Anmeldedaten erstellt, die zum Entsperren der Tür verwendet werden und in den verbundenen Axis Türcontrollern gespeichert (4). Der Besucher hält den QR-Code, der in der Einladung enthalten ist, in die Netzwerk-Kamera oder Türstation (3), die dann einen Befehl an den Tür-Controller (4) sendet, um die Tür für den Besucher zu entsperren.

QR Code ist eine eingetragene Marke von Denso Wave, inc.

Erforderlich für AXIS Visitor Access

Um den AXIS Visitor Access-Dienst nutzen zu können, müssen folgende Voraussetzungen getroffen werden:

- die Türcontroller-Hardware muss konfiguriert werden
- eine Axis Netzwerk-Kamera oder Türstation muss mit dem gleichen Netzwerk verbunden sein wie der Türcontroller und an der Tür platziert werden, wo sie für den Besucher zugänglich ist
- das Installationspaket von AXIS Visitor Access muss bereit stehen. Sie finden es unter *axis.com*
- zwei zusätzliche Nutzerkonten im Türcontroller müssen erstellt werden, die nur für den AXIS Visitor Access-Dienst verwendet werden. Sie benötigen eins für die AXIS Visitor Acess-Anwendung und den anderen für die QR-Scanner-Anwendung. Um Benutzerkonten zu erstellen, siehe *Benutzer auf Seite 55*.

Systemkonfiguration

Wichtig

- Der AXIS Visitor Access-Dienst kann nur mit einem einzigen Türcontroller im gesamten System verbunden werden.
- Mit dem AXIS Visitor Access-Dienst können Sie nur Türen erreichen, die durch den verbundenen Türcontroller gesteuert werden. Sie können keine anderen Türen im System erreichen.
- Verwenden Sie die AXIS Visitor Access-Anwendung, um Besucher zu ändern und zu löschen. Verwenden Sie nicht den AXIS Entry Manager.
- Wenn Sie das Kennwort des Benutzerkontos ändern, das für den AXIS Visitor Access verwendet wird, müssen Sie es auch im AXIS Visitor Access ändern.
- Wenn Sie das Kennwort des Benutzerkontos ändern, das für die QR-Scanner-Anwendung verwendet wird, müssen Sie den QR-Scanner erneut einrichten.

AXIS Visitor Access einrichten

Installieren Sie die QR-Scanneranwendung auf der Axis Netzwerk-Kamera oder der Türstation, wenn Sie den AXIS Visitor Access Dienst einrichten. Eine separate Installation muss nicht vorgenommen werden.

1. Rufen Sie **Setup > Dienste konfigurieren > Einstellungen** auf der Webpage des Türcontrollers auf.
2. Klicken Sie auf **Eine neue Einrichtung starten**.
3. Folgen Sie den Anweisungen, um die Einrichtung abzuschließen.

Wichtig

Wenn Sie HTTPS verwenden möchten, stellen Sie sicher, dass der Türcontroller über HTTPS kommuniziert. Andernfalls kann die Anwendung nicht mit dem Türcontroller kommunizieren.

4. Installieren Sie auf dem Computer, der zur Erstellung der temporären Anmeldedaten verwendet wird, die AXIS Visitor Access Anwendung und richten Sie sie ein.

SmartIntego

SmartIntego ist eine drahtlose Lösung, mit der die Anzahl der von einem Türcontroller verwaltbaren Türen erhöht wird.

Voraussetzungen für SmartIntego

Bevor SmartIntego konfiguriert werden kann, müssen folgende Voraussetzungen erfüllt sein:

- Es muss eine csv-Datei erstellt werden. Die csv-Datei enthält Informationen zum von der SmartIntego-Lösung verwendeten Gateway-Knoten und zu den zugeordneten Türen. Die Datei wird von einer eigenständigen Software erstellt. Die Software wird von einem SimonsVoss-Partner bereitgestellt.
- Die Hardwarekonfiguration von SmartIntego wurde abgeschlossen, siehe *Eine neue Hardwarekonfiguration für Funkschlösser erstellen. auf Seite 18*.

Hinweis

- Das Konfigurationstool für SmartIntego Configuration muss in der Version 2.1.6452.23485, Build 2.1.6452.23485 (8/31/2017 1:02:50 PM) oder später vorliegen.
- Der Verschlüsselungsstandard Advanced Encryption Standard (AES) wird von SmartIntego nicht unterstützt und muss deshalb im Konfigurationstool für SmartIntego deaktiviert werden.

SmartIntego konfigurieren

Hinweis

- Sicherstellen, dass die aufgeführten Anforderungen erfüllt sind.
- Um die Sichtbarkeit des Batteriestatus zu verbessern, **Setup** > **Configure event and alarms logs (Protokolle für Ereignisse konfigurieren)** und entweder **Door – Battery alarm (Tür – Batteriealarm)** oder **IdPoint – Battery alarm (ID-Punkt – Batteriealarm)** als Alarm hinzufügen.
- Die Einstellungen für den Türmonitor werden über die importierte CSV-Datei bereitgestellt. Für eine Standardinstallation müssen diese Einstellungen nicht geändert werden.

1. **Browse... (Durchsuchen...)** anklicken, die CSV-Datei wählen und **Upload file (Datei hochladen)** anklicken.
2. Einen Gateway-Knoten wählen und **Weiter** anklicken.
3. Eine Vorschau der neuen Konfiguration wird angezeigt. Bei Bedarf die Türmonitoren deaktivieren.
4. **Configure (Konfigurieren)** anklicken.
5. Eine Vorschau der in die Konfiguration aufgenommenen Türen wird angezeigt. **Settings (Einstellungen)** anklicken, um jede Tür einzeln zu konfigurieren.

SmartIntego umkonfigurieren

1. Im oberen Menü **Setup** anklicken.
2. **Configure Services (Dienste konfigurieren)** > **Settings (Einstellungen)** anklicken.
3. **Reconfigure (Umkonfigurieren)** anklicken.
4. **Browse... (Durchsuchen...)** anklicken, die CSV-Datei wählen und **Upload file (Datei hochladen)** anklicken.
5. Einen Gateway-Knoten wählen und **Weiter** anklicken.
6. Eine Vorschau der neuen Konfiguration wird angezeigt. Bei Bedarf die Türmonitoren deaktivieren.

Hinweis

Die Einstellungen für den Türmonitor werden über die importierte CSV-Datei bereitgestellt. Für eine Standardinstallation müssen diese Einstellungen in der Regel nicht geändert werden.

7. **Configure (Konfigurieren)** anklicken.
8. Eine Vorschau der in die Konfiguration aufgenommenen Türen wird angezeigt. **Settings (Einstellungen)** anklicken, um jede Tür einzeln zu konfigurieren.

Verwalten von Netzwerk-Tür-Controllern

Auf der Seite „Manage Network Door Controllers in System" (Netzwerk-Tür-Controller im System verwalten) werden Informationen zum Tür-Controller und dessen Systemstatus angezeigt sowie Informationen zu weiteren im System vorhandenen Tür-Controllern. Ein Administrator hat hier auch die Möglichkeit, die Systemkonfiguration anzupassen, indem er Tür-Controller hinzufügt oder entfernt.

Wichtig

Alle Tür-Controller in einem System müssen mit dem selben Netzwerk verbunden und für die Verwendung an einem einzigen Standort eingerichtet sein.

Zum Verwalten von Tür-Controllern rufen Sie **Setup > Manage Network Door Controllers in System (Setup > Netzwerk-Tür-Controller im System verwalten)** auf.

Die Seite Manage Network Door Controllers in System (Netzwerk-Tür-Controller im System verwalten) enthält folgende Bereiche:

- **System status for this controller (Systemstatus dieses Türcontrollers)** – Zeigt den Systemstatus des Türcontrollers an und ermöglicht das Wechseln zwischen Systembetriebsmodus und Einzelbetriebsmodus. Weitere Informationen, siehe *Tür-Controller-Systemstatus auf Seite 27*.
- **Network door controllers in system (Netzwerk-Türcontroller im System)** – Zeigt Informationen zu den Netzwerk-Türcontrollern im System an und bietet Steuerelemente zum Hinzufügen und Entfernen von Computern. Weitere Informationen, siehe *Verbundene Tür-Controller im System auf Seite 27*

Tür-Controller-Systemstatus

Der Systemstatus eines Tür-Controllers legt fest, ob dieser in ein System aus mehreren Tür-Controllern integriert werden kann. Der Systemstatus von Tür-Controllern wird im Bereich **System status for this controller (Systemstatus dieses Tür-Controllers)** angezeigt.

Wenn sich der Tür-Controller nicht im Standalone-Modus befindet und Sie verhindern möchten, dass der Tür-Controller zu einem System hinzugefügt wird, klicken Sie auf **Activate standalone mode (Standalone-Modus aktivieren)**.

Wenn sich der Tür-Controller im Standalone-Modus befindet, Sie diesen jedoch einem System hinzufügen möchten, klicken Sie auf **Deactivate standalone mode (Standalone-Modus deaktivieren)**.

Systemmodi

- **This controller is not part of a system and not in standalone mode (Dieser Controller ist kein Teil eines Systems und nicht im Modus Einzelgerät** – Der Controller ist nicht als Teil eines Systems konfiguriert und befindet sich nicht im Modus Einzelgerät Das heißt, dass der Türcontroller von einem anderen Tür-Controller im selben Netzwerk zu einem System hinzugefügt werden kann. Wenn der Türcontroller nicht zu einem System hinzugefügt werden soll, den Modus Einzelgerät aktiveren.
- **This controller is set to standalone mode (Dieser Controller befindet sich im Modus Einzelgerät)** – Der Türcontroller ist nicht Teil eines Systems. Er kann nicht von anderen Türcontrollern im Netzwerk zu einem System hinzugefügt werden und kann auch selbst keine anderen Controller hinzufügen. Der Standalone-Modus wird in der Regel bei kleineren Anlagen mit einem Tür-Controller und ein bis zwei Türen verwendet. Um den Türcontroller zu einem System hinzuzufügen, den Modus Einzelgerät deaktivieren.
- **This controller part of a system (Dieser Controller ist Teil eines Systems)** – Der Türcontroller ist Teil eines verzweigten Systems. In größeren Systemen werden Benutzer, Gruppen und Zeitpläne von allen verbundenen Controllern gemeinsam verwendet.

Verbundene Tür-Controller im System

Im Bereich **Network door controllers in system (Netzwerk-Tür-Controller im System)** können Sie folgende Änderungen am System vornehmen:

- Hinzufügen eines Tür-Controllers zum System, siehe *Hinzufügen von Tür-Controllern zu einem System auf Seite 28*.
- Entfernen eines Tür-Controllers aus dem System, siehe *Entfernen von Tür-Controllern aus dem System auf Seite 29*.

Liste verbundener Türcontroller

Der Bereich **Network door controllers in system (Netzwerk-Türcontroller im System)** enthält auch eine Liste mit den folgenden Informationen zu ID und Status der Türcontrollern im System:

- **Name** – Der vom Benutzer festgelegte Name des Türcontrollers. Wenn der Administrator während der Hardwarekonfiguration keinen Namen angegeben hat, wird der Standardname angezeigt.
- **IP-Adresse**
- **MAC-Adresse**
- **Status** – Der Türcontroller, über den der Systemzugriff erfolgt, weist den Status **This controller (Dieser Controller)** auf. Die übrigen Türcontroller des Systems weisen den Status **Online** auf.
- **Firmwareversion**

Um die Webseite eines anderen Türcontrollers aufzurufen, die entsprechende IP-Adresse anklicken.

Um die Liste zu aktualisieren, **Refresh the list of controllers (Controller-Liste aktualisieren)** anklicken.

Hinweis

Alle Controller des Systems müssen immer mit Firmware der selben Version versehen sein. Mit Axis Device Manager die Firmware aller Controller des Systems parallel aktualisieren.

Hinzufügen von Tür-Controllern zu einem System

Wichtig

Beim Koppeln von Tür-Controllern werden alle Zugangsverwaltungseinstellungen des hinzugefügten Tür-Controllers gelöscht und mit den Zugangsverwaltungseinstellungen des Systems überschrieben.

So fügen Sie einen Tür-Controller aus der Liste der Tür-Controller zum System hinzu:

1. Rufen Sie **Setup > Manage Network Door Controllers in System (Setup > Netzwerk-Tür-Controller im System verwalten)** auf.
2. Klicken Sie auf **Add controllers to system from list (Controller aus der Liste zum System hinzufügen)**.
3. Wählen Sie den Tür-Controller aus, den Sie hinzufügen möchten.
4. Klicken Sie auf **Add (Hinzufügen)**.
5. Zum Hinzufügen weiterer Tür-Controller wiederholen Sie die vorherigen Schritte.

So fügen Sie einen Tür-Controller anhand der IP- oder MAC-Adresse hinzu:

1. Rufen Sie **Manage Devices (Geräte verwalten)** auf.
2. Klicken Sie auf **Add controller to system by IP or MAC address (Controller anhand von IP- oder MAC-Adresse zum System hinzufügen)**.
3. Geben Sie die IP- oder MAC-Adresse ein.
4. Klicken Sie auf **Add (Hinzufügen)**.
5. Zum Hinzufügen weiterer Tür-Controller wiederholen Sie die vorherigen Schritte.

IM Anschluss an die Koppelung verwenden alle Tür-Controller im System die gleichen Benutzer, Türen, Zeitpläne und Gruppen.

Klicken Sie auf **Refresh list of controllers (Controller-Liste aktualisieren)**, um die Liste zu aktualisieren.

Entfernen von Tür-Controllern aus dem System

Wichtig

- Setzen Sie vor dem Entfernen eines Tür-Controllers aus dem System dessen Hardwarekonfiguration zurück. Wenn Sie diesen Schritt überspringen, verbleiben alle mit dem entfernten Tür-Controller verbundenen Türen im System und können nicht gelöscht werden.
- Wenn Sie einen Tür-Controller aus einem System mit zwei Tür-Controllern entfernen, wechseln beide Tür-Controller automatisch in den Standalone-Modus.

So entfernen Sie einen Tür-Controller aus dem System:

1. Rufen Sie das System über den zu entfernenden Tür-Controller auf, und wechseln Sie zu **Setup > Hardware Configuration (Setup > Hardwarekonfiguration)**.
2. Klicken Sie auf **Reset hardware configuration (Hardwarekonfiguration zurücksetzen)**.
3. Rufen Sie nach dem Zurücksetzen der Hardwarekonfiguration **Setup > Manage Network Door Controllers in System (Setup > Netzwerk-Tür-Controller im System verwalten)** auf.
4. Wählen Sie in der Liste **Network door controllers in system (Netzwerk-Tür-Controller im System)** den zu entfernenden Tür-Controller aus, und klicken Sie auf **Remove from system (Aus System entfernen)**.
5. Sie werden in einem Dialogfeld dazu aufgefordert, die Hardwarekonfiguration des Tür-Controllers zurückzusetzen. Klicken Sie zur Bestätigung auf **Remove controller (Controller entfernen)**.
6. Sie werden in einem Dialogfeld dazu aufgefordert, das Entfernen des Tür-Controllers zu bestätigen. Klicken Sie zur Bestätigung auf **OK**. Der entfernte Tür-Controller befindet sich jetzt im Standalone-Modus.

Hinweis

- Wenn ein Tür-Controller aus einem System entfernt wird, werden alle Einstellungen für die Zugangsverwaltung gelöscht.
- Es können nur Tür-Controller entfernt werden, die online sind.

Konfigurationsmodus

Der Konfigurationsmodus ist beim Erstzugriff auf das Gerät der Standardmodus. Bei deaktiviertem Konfigurationsmodus werden die meisten Konfigurationsoptionen des Geräts nicht angezeigt.

Wichtig

Das Deaktivieren des Konfigurationsmodus ist keine Sicherheitsfunktion. Es soll lediglich Konfigurationsfehler vermeiden, kann aber böswillige Benutzer nicht davon abhalten, wichtige Einstellungen zu verändern.

Den Konfigurationsmodus deaktivieren

1. **Setup** > **Disable Configuration Mode (Konfigurationsmodus deaktivieren)** aufrufen.
2. Die PIN eingeben und **OK** wählen.

Hinweis

Die PIN-Eingabe ist nicht verpflichtend.

Den Konfigurationsmodus aktivieren

1. **Setup** > **Enable Configuration Mode (Konfigurationsmodus aktivieren)** aufrufen.
2. Die PIN eingeben und **OK** wählen.

Hinweis

Bei nicht verfügbarer PIN den Konfigurationsmodus konfigurieren über `http://[IP-address]/webapp/pacs/index.shtml#resetConfigurationMode`.

Wartungsanweisungen

Für einen reibungslosen Betrieb des Zugangskontrollsystems empfiehlt Axis eine regelmäßige Wartung des Systems, einschließlich Tür-Controller und angeschlossener Geräte.

Die Wartung sollte mindestens einmal pro Jahr erfolgen. Die empfohlene Wartungsprozedur umfasst unter anderem die folgenden Schritte:

- Stellen Sie sicher, dass alle Verbindungen zwischen dem Tür-Controller und den externen Geräten sicher sind.
- Überprüfen Sie alle Hardware-Anschlüsse. Siehe *Steuerelemente der Türüberprüfung auf Seite 20*.
- Stellen Sie sicher, dass das System, einschließlich der angeschlossenen externen Geräte, ordnungsgemäß funktioniert.
    - Ziehen Sie eine Karte durch und testen Sie Leser, Türen und Schlösser.
    - Wenn zum System Geräte, Sensoren oder andere Geräte von REX gehören, müssen diese ebenfalls getestet werden.
    - Ebenfalls aktivierte Manipulationsalarme testen.

Falls die Ergebnisse eines der oben genannten Schritte auf Fehler oder unerwartetes Verhalten hindeuten:

- Testen Sie die Signale der Drähte mit entsprechender Ausrüstung und überprüfen Sie, ob die Drähte oder Kabel beschädigt sind.
- Ersetzen Sie alle beschädigten oder fehlerhaften Kabel und Drähte.
- Überprüfen Sie nach dem Austauschen der Kabel und Drähte alle Hardware-Anschlüsse erneut. Siehe *Steuerelemente der Türüberprüfung auf Seite 20*.

- Stellen Sie sicher, dass alle Zutrittszeitpläne, Türen, Gruppen und Benutzer aktuell sind.
- Wenn der Tür-Controller nicht wie erwartet funktioniert, finden Sie im *Fehlerbehebung auf Seite 67* und *Wartung auf Seite 63* weitere Informationen.

Zugangsverwaltung

Benutzer

Personen mit Tokens (z. B. Zugangskarten) werden in AXIS Entry Manager als Benutzer bezeichnet. Jede Person benötigt ein eigenes Benutzerprofil, um Zugang über Türen im Zutrittskontrollsystem zu erhalten. Das Benutzerprofil besteht aus Zugangsdaten, mit denen das System die Benutzer identifiziert, sowie den Informationen, wann und wie die Benutzer an Türen Zutritt erhalten. Weitere Informationen, siehe *Benutzer erstellen und bearbeiten auf Seite 40*

Benutzer sind in diesem Zusammenhang nicht mit Administratoren zu verwechseln. Administratoren haben unbeschränkten Zutritt zu allen Einstellungen. Im Zusammenhang mit der Verwaltung des Zutrittskontrollsystems, den Produktwebseiten (AXIS Entry Manager), werden Administratoren gelegentlich als Benutzer bezeichnet. Weitere Informationen, siehe *Benutzer auf Seite 55*

Die Seite „Access Management" (Zugangsverwaltung)

Auf der Seite „Access Management" (Zugangsverwaltung) können Sie Benutzer, Gruppen, Türen und Zeitpläne des Systems konfigurieren und verwalten. Klicken Sie auf **Access Management (Zugangsverwaltung)**, um die Seite zu öffnen.

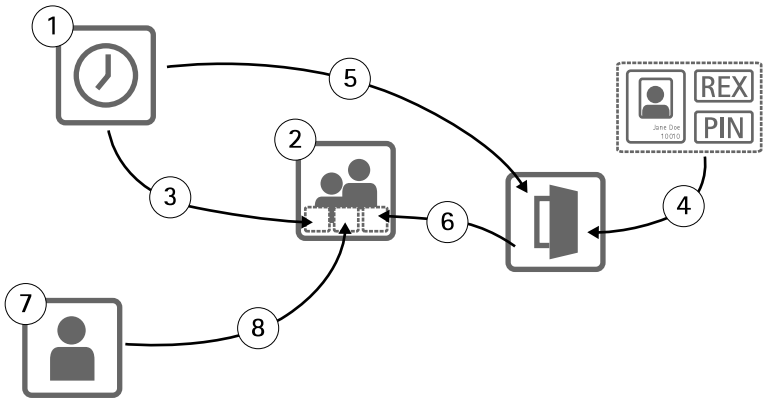
Um Benutzer zu Gruppen und Zutrittszeitpläne zu Türen zuzuweisen, ziehen Sie die Elemente in das jeweilige Ziel in den Listen **Groups (Gruppen)** und **Doors (Türen)**.

Hinweis

Meldungen, die Maßnahmen erfordern, werden in roter Schrift dargestellt.

Vorgehensweise

Die Struktur der Zugangsverwaltung ist flexibel. Gehen Sie anhand der Anforderungen der jeweiligen Anwendung vor. Im Folgenden finden Sie ein Beispiel für eine Vorgehensweise:



1. Erstellen von Zugangszeitplänen. Siehe *Seite 32*.
2. Erstellen von Gruppen. Siehe *Seite 34*.
3. Zuordnen von Zugangszeitplänen zu Gruppen.
4. Hinzufügen von Identifizierungstypen zu Etagen. Siehe *Seite 35* und *Seite 36*.
5. Zuordnen von Zugangszeitplänen zu Identifikationstypen.
6. Türen und Etagen Gruppen zuordnen.
7. Benutzer anlegen. Siehe *Seite 40*.

8. Benutzer zu Gruppen hinzufügen.

Für Anwendungsbeispiele für diese Vorgehensweise, siehe *Beispiele für Kombinationen von Zugangszeitplänen auf Seite 42*.

Erstellen und Bearbeiten von Zugangszeitplänen

Zugangszeitpläne definieren allgemeine Regeln, wann Zugang zu Türen besteht und wann nicht. Sie definieren außerdem Regeln, wann Gruppen Zugang zu Türen innerhalb des Systems erhalten und wann nicht. Weitere Informationen, siehe *Zugangszeitplantypen auf Seite 32*

So erstellen Sie einen neuen Zugangszeitplan:

1. Rufen Sie **Access Management (Zugangsverwaltung)** auf.
2. Klicken Sie auf der Registerkarte **Access Schedules (Zugangszeitpläne)** auf **Add new schedule (Neuen Zeitplan hinzufügen)**.
3. Geben Sie im Dialogfeld **Add access schedule (Zeitplan hinzufügen)** einen Namen für den Zeitplan ein.
4. Wählen Sie zum Erstellen eines normalen Zugangszeitplans **Addition Schedule (Additionszeitplan)** aus.

   Wählen Sie zum Erstellen eines Subtraktionszeitplans **Subtraction Schedule (Subtraktionszeitplan)** aus.

   Weitere Informationen, siehe *Zugangszeitplantypen auf Seite 32*
5. Klicken Sie auf **Save (Speichern)**.

Zum Erweitern eines Elements in der Liste **Access Schedules (Zugangszeitpläne)**  anklicken. Additionszeitpläne werden in Grün angezeigt, Subtraktionszeitpläne in Dunkelrot.

Zum Anzeigen des Kalenders für einen Zugangszeitplan  anklicken.

Um den Namen eines Zutrittssplans oder eines Zeitplanelements zu bearbeiten,  anklicken und Änderungen vornehmen. Klicken Sie anschließend auf **Save (Speichern)**.

Zum Löschen eines Zugangszeitplans  anklicken.

Hinweis

Der Tür-Controller verfügt über einige vordefinierte häufig verwendete Zugangszeitpläne, die als Beispiele verwendet oder modifiziert werden können. Der vordefinierte Zugangszeitplan **Always (Immer)** kann jedoch weder modifiziert noch gelöscht werden.

Zugangszeitplantypen

Es gibt zwei Arten von Zugangszeitplänen:

- **Additionszeitpläne** – Normale Zugangszeitpläne, die festlegen, wann Türen geöffnet werden können. Typische Additionszeitpläne regeln Bürozeiten, Geschäftszeiten, Zeiten nach Geschäftsschluss oder Nachtstunden.
- **Subtraktionszeitpläne** – Ausnahmen von den regulären Zugangszeitplänen. Diese werden überwiegend dazu genutzt, um für eines bestimmten Zeitraum innerhalb des regulären Zeitplans (des Additionszeitplans) den Zugang zu beschränken. Mithilfe eines Subtraktionszeitplans kann beispielsweise festgelegt werden, dass an Feiertagen, die auf Wochentage fallen, Benutzer keinen Zugang zum Gebäude erhalten.

Beide Zugangszeitplantypen können auf zwei Ebenen verwendet werden:

- **Identifizierungstyp-Zeitpläne** – Bestimmen, wann und wie Lesegeräte Benutzern das Öffnen von Türen gestatten. Jeder Identifizierungstyp muss einem Zugangszeitplan zugeordnet werden. Dieser teilt dem System mit, wann Benutzer mit einem bestimmten Identifizierungstyp Zugang zu einem Gebäude erhalten sollen. Jedem Identifizierungstyp können mehrere Additions- und Subtraktionszeitpläne hinzugefügt werden. Informationen zu Identifizierungstypen finden Sie unter *Seite 36*.

- **Gruppenzeitpläne** – Legen fest wann, jedoch nicht wie Mitglieder einer Gruppe Türen öffnen können. Jede Gruppe muss mindestens einem Zugangszeitplan zugeordnet werden. Dieser teilt dem System mit, wann die Mitglieder der Gruppe Zugang zu einem Gebäude erhalten sollen. Jeder Gruppe können mehrere Additions- und Subtraktionszeitpläne hinzugefügt werden. Weitere Informationen über Gruppen finden Sie unter *Seite 34*.

Gruppenzeitpläne können Zugangsrechte einschränken, jedoch nicht über den Zeitplan des Identifizierungstyps hinaus erweitern. Mit anderen Worten: Wenn der Zeitplan eines Identifizierungstyps die Zugangsrechte zu bestimmten Zeiten einschränkt, kann ein Gruppenzeitplan diese Einschränkungen nicht überschreiben. Wenn der Gruppenzeitplan jedoch Einschränkungen vorsieht, die über den Zeitplan des Identifizierungstyps hinausgehen, überschreibt der Gruppenzeitplan den Zeitplan des Identifizierungstyps.

Identifizierungstyp- und Gruppenzeitpläne können für verschiedene Zwecke auf unterschiedliche Art kombiniert werden. Beispiele für Zugangszeitpläne finden Sie unter *Seite 42*.

Hinzufügen von Ereignissen zum Zeitplan

Sowohl Additions- als auch Subtraktionszeitpläne können einmalige und wiederkehrende Ereignisse enthalten.

So fügen Sie ein Ereignis zu einem Zugangszeitplan hinzu:

1. Erweitern Sie den Zugangszeitplan in der Liste **Access Schedules (Zugangszeitpläne)**.
2. Klicken Sie auf **Add schedule item (Zeitplanereignis hinzufügen)**.
3. Geben Sie einen Namen für das Zeitplanereignis ein.
4. Wählen Sie **One time (Einmalig)** oder **Recurrence (Wiederkehrend)** aus.
5. Legen Sie in den Zeitfeldern die Dauer fest. Siehe *Zeitoptionen auf Seite 33*.
6. Wählen Sie für wiederkehrende Zeitplanereignisse die Parameter **Recurrence pattern (Wiederholungsmuster)** und **Range of recurrence (Wiederholungszeitraum)** aus. Siehe *Optionen für Wiederholungsmuster auf Seite 33* und *Optionen für den Wiederholungszeitraum auf Seite 33*.
7. Klicken Sie auf **Save (Speichern)**.

Zeitoptionen

Es stehen folgende Zeitoptionen zur Verfügung:

- **All day (Ganztägig)** – Diese Option für Ereignisse auswählen, die 24 Stunden andauern. Anschließend das gewünschte **Start**datum eingeben.
- **Start** – In das Uhrzeitfeld klicken und die gewünschte Zeit wählen. Bei Bedarf das Datumsfeld anklicken und Monat, Tag und Jahr wählen. Das Datum kann auch direkt in das Feld eingegeben werden.
- **End (Ende)** – Das Uhrzeitfeld anklicken und die gewünschte Uhrzeit wählen. Bei Bedarf das Datumsfeld anklicken und Monat, Tag und Jahr wählen. Sie können das Datum auch direkt in das Feld eingeben.

Optionen für Wiederholungsmuster

Es stehen folgende Optionen für Wiederholungsmuster zur Verfügung:

- **Yearly (Jährlich)** – Für jährliche Wiederholung wählen.
- **Weekly (Wöchentlich)** – Für wöchentliche Wiederholung wählen.
- Wiederholung wöchentlich **Monday (Montag)**, **Tuesday (Dienstag)**, **Wednesday (Mittwoch)**, **Thursday (Donnerstag)**, **Friday (Freitag)**, **Saturday (Samstag)** oder **Sunday (Sonntag)**. Die Wiederholungstage auswählen.

Optionen für den Wiederholungszeitraum

Es stehen folgende Optionen für den Wiederholungszeitraum zur Verfügung:

- **First occurrence (Erstes Auftreten)** – In das Datumsfeld klicken und Monat, Tag und Jahr wählen. Das Datum kann auch direkt in das Feld eingegeben werden.
- **No end date (Kein Enddatum)** – Die Wiederholungen erfolgen zeitlich unbegrenzt.
- **End by (Ende am)** – In das Datumsfeld klicken und Monat, Tag und Jahr wählen. Sie können das Datum auch direkt in das Feld eingeben.

Erstellen und Bearbeiten von Gruppen

Gruppen ermöglichen Ihnen, Benutzer und deren Zugangsrechte gemeinsam und effizient zu verwalten. Eine Gruppe besteht aus den Zugangsdaten, mit denen das System die zu einer Gruppe gehörigen Benutzer identifiziert, sowie den Informationen, wann und wie die Mitglieder der Gruppe an Türen Zugang erhalten.

Jeder Benutzer muss zu einer oder mehreren Gruppen gehören. Zum Hinzufügen eines Benutzers zu einer Gruppe fügen Sie den Benutzer per Drag & Drop zur Liste **Groups (Gruppen)** hinzu. Weitere Informationen, siehe *Benutzer erstellen und bearbeiten auf Seite 40*

So erstellen Sie eine neue Gruppe:

1. Rufen Sie **Access Management (Zugangsverwaltung)** auf.
2. Klicken Sie auf der Registerkarte **Groups (Gruppen)** auf **Add new Group (Neue Gruppe hinzufügen)**.
3. Geben Sie im Dialogfeld **Add Group (Gruppe hinzufügen)** die Zugangsdaten für die Gruppe an. Siehe *Gruppenzugangsdaten auf Seite 34*.
4. Klicken Sie auf **Save (Speichern)**.

Zum Anzeigen zusätzlicher Informationen für ein Element in der Liste **Groups (Gruppen)** wie zum Beispiel Mitglieder der Gruppe, Zugangsrechte für Türen oder Zeitpläne  anklicken.

Um den Namen einer Gruppe oder die Gültigkeit zu bearbeiten,  anklicken. Klicken Sie anschließend auf **Save (Speichern)**.

Zum Verifizieren, wann und wie eine Gruppe Zugang an bestimmten Türen erhält,  anklicken.

Zum Löschen einer Gruppe, von Gruppenmitgliedern, Türen oder Zeitplänen einer Gruppe,  anklicken.

Gruppenzugangsdaten

Für Gruppen stehen folgende Zugangsdaten zur Verfügung:

- **Name** (erforderlich)
- **Gültig von** und **Gültig bis** – Das Start- und Enddatum für die Gültigkeit der Zugangsdaten einer Gruppe eingeben. Das Datumsfeld anklicken und Tag, Monat und Jahr wählen. Das Datum kann auch direkt in das Feld eingegeben werden.
- **Whitelist** – Benutzer einer Whitelist-Gruppe haben immer Zugang zu Türen der Gruppe. Auch bei Netzwerk- oder Stromausfällen. Da die Benutzer in der Gruppe immer Zugang zu den Türen haben, finden Zeitpläne, „Gültig von" und „Gültig bis" keine Anwendung. Die „lange Zugangsdauer" wird nicht für Benutzer unterstützt, die eine Tür in der Whitelist-Gruppe öffnen. Der Gruppe können nur Türen hinzugefügt werden, die über Drahtlosschließung verfügen und Whitelist unterstützen.

Hinweis

- Um die Gruppe zu speichern, muss das Feld **Name** für die Gruppe ausgefüllt sein.
- „Gültig bis" und „Gültig von" für einen Benutzer finden keine Anwendung, wenn der Benutzer der Whitelist-Gruppe hinzugefügt wird.
- Das Synchronisieren von Zugangsdaten auf der Whitelist mit einer Drahtlosschließung nimmt einige Zeit in Anspruch und beeinträchtigt reguläre Türöffnungsvorgänge. Während Stoßzeiten sollte es vermieden werden, große Mengen an Zugangsdaten im System hinzuzufügen oder zu entfernen. Wenn das Synchronisieren von aktualisierten Zugangsdaten an ein Schloss abgeschlossen ist, zeigt das Ereignisprotokoll für dieses Schloss `SyncOngoing: falsch`.

Verwalten von Türen

Die allgemeinen Regeln für alle Türen können auf der Registerkarte **Doors (Türen)** festgelegt werden. Die Regeln beinhalten das Hinzufügen von Identifizierungstypen zur Bestimmung, wie Benutzer Zugang erhalten, und Zugangszeitpläne zur Bestimmung, wann die einzelnen Identifizierungstypen gültig sind. Weitere Informationen finden Sie unter *Identifizierungsmöglichkeiten auf Seite 36* und *Erstellen und Bearbeiten von Zugangszeitplänen auf Seite 32*.

Um eine Tür zu verwalten, müssen Sie diese dem Zugangskontrollsystem hinzufügen, indem Sie die Hardwarekonfiguration durchführen (siehe *Konfigurieren der Hardware auf Seite 13*).

So verwalten Sie Türen:

1. Rufen Sie **Access Management (Zugangsverwaltung)** auf, und wählen Sie die Registerkarte **Doors (Türen)** aus.
2. In der Liste **Türen** neben der zu bearbeitenden Tür anklicken.
3. Ziehen Sie die Tür in mindestens eine Gruppe. Erstellen Sie eine neue Gruppe, wenn die Liste **Groups (Gruppen)** leer ist. Siehe *Erstellen und Bearbeiten von Gruppen auf Seite 34*.
4. Klicken Sie auf **Add identification type (Identifizierungstyp hinzufügen)**, und wählen Sie die Zugangsdaten aus, die ein Benutzer am Leser angeben muss, wenn er Zugang durch eine Tür erhalten möchte. Siehe *Identifizierungsmöglichkeiten auf Seite 36*.

   Fügen Sie für jede Tür mindestens einen Identifizierungstyp hinzu.
5. Zum Hinzufügen von mehreren Identifizierungstypen wiederholen Sie den letzten Schritt.

   Wenn Sie die beiden Identifizierungstypen **Card number only (Nur Kartenummer)** und **PIN only (Nur PIN)** hinzufügen, können Benutzer zum Betreten der Tür entweder ihre Karte durch den Leser ziehen oder ihre PIN eingeben. Wenn Sie stattdessen nur den Identifizierungstyp **Card number and PIN (Kartenummer und PIN)** hinzufügen, müssen Benutzer zum Öffnen der Tür sowohl ihre Karte durch den Leser ziehen als auch ihre PIN eingeben.
6. Ziehen Sie einen Zeitplan auf die einzelnen Identifikationstypen, um festzulegen, wann die Zugangsdaten gültig sind.

Zum manuellen Verriegeln oder Entriegeln von Türen oder zum vorübergehenden Freigeben des Zugangs die entsprechende manuelle Türfunktion anklicken. Siehe *Verwenden der manuellen Türfunktionen auf Seite 37*.

Hinweis

Steuerungen zum manuellen Entriegeln und Entriegeln von Türen oder für vorübergehendes Freigeben sind nicht für drahtlose Türen/Geräte verfügbar.

Um weitere Informationen zu einem Element anzuzeigen, in der Liste **Doors (Türen)** anklicken.

Um eine Türe oder einen Lesernamen zu bearbeiten, anklicken. Klicken Sie anschließend auf **Save (Speichern)**.

Zum Überprüfen des Lesers, des Identifizierungstyps und der Zugangszeitplankombinationen anklicken.

Zum Überprüfen der Funktion von Schlössern, die mit den Türen verbundenen sind, klicken Sie auf die Überprüfungssteuerelemente. Siehe *Steuerelemente der Türüberprüfung auf Seite 20*.

Zum Löschen von Identifizierungstypen oder Zugangszeitplänen anklicken.

Identifizierungsmöglichkeiten

Zur Identifizierung können mobile Speichergeräte mit Zugangsdaten, bestimmte auswendig gelernte Informationen oder Kombinationen aus beidem dienen, die den Zugang von Benutzern regeln. Zu den gebräuchlichen Identifizierungsmöglichkeiten zählen Tokens wie Karten oder Schlüsselanhänger, persönliche Identifikationsnummern (PINs) und REX-Geräte (Request to Exit).

Weitere Informationen zu Zugangsdaten finden Sie unter *Zugangsdaten für Benutzer auf Seite 41*.

Folgende Identifizierungsmöglichkeiten stehen zur Verfügung:

- **Nur Einrichtungscode** – Der Benutzer erhält Zugang mit einer vom Reader akzeptierten Karte oder einem anderen Token mit dem Einrichtungscode.
- **Nur Kartennummer** – Der Benutzer erhält Zugang mit einer vom Reader akzeptierten Karte oder einem anderen Token. Die Kartennummer ist eine eindeutige Nummer, die in der Regel auf die Karte aufgedruckt ist. Informationen über die Position der Kartennummer finden Sie in den Anweisungen des Herstellers. Die Kartennummer kann auch vom System abgerufen werden. Ziehen Sie die Karte durch einen angeschlossenen Reader, wählen Sie den Reader in der Liste aus und klicken Sie auf **Retrieve (Abrufen)**.
- **Nur Karte mit Rohdaten** – Der Benutzer erhält Zugang mit einer vom Reader akzeptierten Karte oder einem anderen Token. Die Informationen sind als Rohdaten auf der Karte gespeichert. Die Rohdaten der Karte können auch vom System abgerufen werden. Ziehen Sie die Karte durch einen angeschlossenen Reader, wählen Sie den Reader in der Liste aus, und klicken Sie auf **Retrieve (Abrufen)**. Verwenden Sie diese Art der Identifizierung nur, wenn keine Kartennummer ermittelt werden kann.
- **Nur PIN** – Der Benutzer erhält Zugang mit einer vierstelligen Identifikationsnummer (PIN).
- **Einrichtungscode und PIN** – Der Benutzer erhält Zugang mit der Kombination aus einer vom Reader akzeptierten Karte bzw. einem anderen Token mit dem Einrichtungscode und einer PIN. Der Benutzer muss die Identifizierung in der angegebenen Reihenfolge durchführen (zuerst die Karte, dann die PIN).
- **Kartennummer und PIN** – Der Benutzer erhält Zugang mit der Kombination aus einer vom Reader akzeptierten Karte bzw. einem anderen Token und einer PIN. Der Benutzer muss die Identifizierung in der angegebenen Reihenfolge durchführen (zuerst die Karte, dann die PIN).
- **Karte mit Rohdaten und PIN** – Der Benutzer erhält Zugang mit der Kombination aus einer vom Reader akzeptierten Karte bzw. einem anderen Token und einer PIN. Verwenden Sie diese Art der Identifizierung nur, wenn keine Kartennummer ermittelt werden kann. Der Benutzer muss die Identifizierung in der angegebenen Reihenfolge durchführen (zuerst die Karte, dann die PIN).
- **REX** – Der Benutzer erhält Zugang durch die Aktivierung eines REX (Request to Exit)-Geräts, beispielsweise eines Tasters, eines Sensors, oder einer Druckstange.
- **Nur Fahrzeugkennzeichen** – Der Benutzer erhält Zugang mit einer Kennzeichen-Nummer für ein Fahrzeug.

Hinzufügen geplanter Entriegelungsstatus

Wenn Sie eine Tür während eines bestimmten Zeitraums automatisch entriegeln möchten, können Sie den Status **Scheduled unlock (Geplante Entriegelung)** hinzufügen und zu diesem einen Zugangszeitplan hinzufügen.

Wenn beispielsweise eine Tür während der Geschäftszeiten entriegelt bleiben soll:

1. Rufen Sie **Access Management (Zugangsverwaltung)** auf, und wählen Sie die Registerkarte **Doors (Türen)** aus.
2. Neben dem zu bearbeitenden Punkt der Liste **Türen** anklicken.
3. Klicken Sie auf **Add scheduled unlock (Geplante Entriegelung hinzufügen)**.
4. Wählen Sie den **Unlock state (Entriegelungsstatus)** aus (**Unlock (Entriegeln)** oder **Unlock both locks (Beide Schlösser entriegeln)**, je nachdem, ob die Tür ein oder zwei Schlösser hat).
5. Klicken Sie auf **OK**.

6. Ziehen Sie den vordefinierten Zugangszeitplan **Office hours (Geschäftszeiten)** auf den Status **Scheduled unlock (Geplante Entriegelung)**.

Zum Bestätigen, wann die Tür entriegelt werden soll,  anklicken.

Zum Löschen einer geplanten Entriegelung oder zum Bearbeiten eines Zeitplans  anklicken.

Verwenden der manuellen Türfunktionen

Über die Registerkarte **Doors (Türen)** können mithilfe der **Manual door actions (Manuellen Türfunktionen)** Türen entriegelt und verriegelt oder der Zugang vorübergehend freigegeben werden. Welche manuellen Türfunktionen für eine bestimmte Tür zur Verfügung stehen hängt davon ab, wie die Tür konfiguriert wurde.

So verwenden Sie die manuellen Türfunktionen:

1. Rufen Sie **Access Management (Zugangsverwaltung)** auf, und wählen Sie die Registerkarte **Doors (Türen)** aus.
2. In der Liste **Doors (Türen)** neben der zu bearbeitenden Tür  anklicken.
3. Klicken Sie auf die erforderliche Türfunktion. Siehe *Manuelle Türfunktionen auf Seite 37*.

Hinweis

Zur Verwendung der manuellen Türfunktionen müssen Sie die Seite „Access Management" (Zugangsverwaltung) über den mit der jeweiligen Tür verbundenen Tür-Controller aufrufen. Wenn Sie die Seite „Access Management" (Zugangsverwaltung) über einen anderen Tür-Controller öffnen, wird statt der manuellen Türfunktionen ein Link zu der Übersichtsseite des Tür-Controllers angezeigt, mit dem die Tür verbunden ist. Klicken Sie auf den Link, rufen Sie **Access Management (Zugangsverwaltung)** auf, und wählen Sie die Registerkarte **Doors (Türen)** aus.

Manuelle Türfunktionen

Folgende manuelle Türfunktionen stehen zur Verfügung:

- **Get door status (Türstatus abrufen)** – Zum Überprüfen des aktuellen Status des Türmonitors, der Türalarme und der Schlösser.
- **Access (Zugang)** – Zum Gewähren von Zugang an einer Tür. Es gilt die entsprechende Zugangsdauer. Siehe *Schlösser und Türmonitore konfigurieren auf Seite 14*.
- **Unlock (Entriegeln eines Schlosses)** oder **Unlock both locks (Entriegeln beider Schlösser)** – Zum Entriegeln der Tür. Die Tür bleibt solange entriegelt bis**Lock (Verriegeln)** oder **Lock both locks (Verriegeln beider Schlösser)** angeklickt wird, ein durch einen Zeitplan festgelegter Status aktiviert wird oder der Türcontroller neu gestartet wird.
- **Lock (Verriegeln eines Schlosses)** oder **Lock both locks (Verriegeln beider Schlösser)** – Zum Verriegeln der Tür.
- **Unlock second lock and lock primary (Sekundäres Schloss entriegeln und primäres Schloss verriegeln)** – Diese Option ist nur verfügbar, wenn für die Tür ein sekundäres Schloss konfiguriert wurde. Zum Entriegeln der Tür. Das sekundäre Schloss bleibt entriegelt, bis Sie auf **Double lock (Doppelschloss)** klicken oder ein durch einen Zeitplan festgelegter Status aktiviert wird.

Stockwerke verwalten

Wenn im System ein AXIS 9188 Network I/O Relay Module installiert wurde, können Stockwerke ähnlich wie Türen verwaltet werden.

Hinweis

Sicherstellen, dass jedes Stockwerk über einen aussagekräftigen Namen verfügt, wenn ein A1001 im Verbundmodus mit aktivierten globalen Ereignissen verwendet wird. Beispielsweise *"Aufzug A, 1. Stock"*.

Hinweis

Pro A1001 Network Door Controller lassen sich maximal zwei AXIS 9188 Network I/O Relay Modules konfigurieren.

Die allgemeinen Regeln für jedes Stockwerk werden auf der Registerkarte **Stockwerke** festgelegt. Die Regeln beinhalten das Hinzufügen von Identifizierungstypen zur Bestimmung, wie Benutzer Zugang zum Stockwerk erhalten, und Zugangszeitpläne zur Bestimmung, wann die einzelnen Identifizierungstypen gültig sind. Für weitere Informationen, siehe *Identifizierungsmöglichkeiten für Stockwerke auf Seite 38* und *Erstellen und Bearbeiten von Zugangszeitplänen auf Seite 32*.

Um ein Stockwerk zu verwalten, muss dieses dem Zugangskontrollsystem hinzugefügt werden, indem die Hardwarekonfiguration durchgeführt wird (siehe *Konfigurieren der Hardware auf Seite 13*).

Ein Stockwerk verwalten:

1. **Access Management (Zutrittsverwaltung)** aufrufen und die Registerkarte **Floors (Stockwerke)** wählen.
2. In der Liste **Stockwerke**, neben dem zu bearbeitenden Stockwerk, anklicken.
3. Mit der Maus das Stockwerk in mindestens eine Gruppe ziehen. Eine neue Gruppe erstellen, wenn die Liste **Groups (Gruppen)** leer ist. Siehe *Erstellen und Bearbeiten von Gruppen auf Seite 34*.
4. **Add identification type (Identifizierungstyp hinzufügen)** anklicken und die Zugangsdaten wählen, die ein Benutzer am Leser angeben muss, um Zugang zu dem Stockwerk zu erhalten. Siehe *Identifizierungsmöglichkeiten für Stockwerke auf Seite 38*.

   Jedem Stockwerk mindestens einen Identifizierungstyp hinzufügen.
5. Zum Hinzufügen von mehreren Identifizierungstypen, den letzten Schritt wiederholen.

   Wenn Sie die beiden Identifizierungstypen **Card number only (Nur Kartenummer)** und **PIN only (Nur PIN)** hinzufügen, können Benutzer zum Betreten der Tür entweder ihre Karte durch den Leser ziehen oder ihre PIN eingeben. Wenn Sie stattdessen nur den Identifizierungstyp **Card number and PIN (Kartenummer und PIN)** hinzufügen, müssen Benutzer zum Öffnen der Tür sowohl ihre Karte durch den Leser ziehen als auch ihre PIN eingeben.
6. Um festzulegen, wann die Zugangsdaten gültig sind, einen Zeitplan auf die einzelnen Identifikationstypen ziehen.

Zum manuellen Verriegeln oder Entriegeln von Stockwerken oder für eine vorübergehende Freigabe des Zugangs, ggf. die manuellen Türfunktionen anklicken. Siehe *Manuelle Etagenaktionen verwenden auf Seite 39*.

Hinweis

Steuerungen zum manuellen Verriegeln oder Entriegeln von Stockwerken oder für eine vorübergehende Freigabe des Zugangs, sind für drahtlose Türen/Geräte nicht verfügbar.

Zum Anzeigen weiterer Informationen für ein Element in der Liste **Stockwerke**, anklicken.

Um ein Stockwerk oder einen Lesernamen zu bearbeiten, anklicken und die Änderungen vornehmen. Anschließend **Speichern** anklicken.

Zum Überprüfen des Lesers, des Identifizierungstyps und der Zugangszeitplankombinationen, anklicken.

Zum Überprüfen der Funktion von Schlössern, die mit den Stockwerken verbundenen sind, die Überprüfungssteuerelemente anklicken. Siehe *Steuerelemente der Etagenüberprüfung auf Seite 20*.

Zum Löschen von Identifizierungstypen oder Zugangszeitplänen, anklicken.

Identifizierungsmöglichkeiten für Stockwerke

Zur Identifizierung können mobile Speichergeräte mit Zugangsdaten, bestimmte eingespeicherte Informationen oder Kombinationen aus beiden dienen, die den Zugang von Benutzern zu Stockwerken regeln. Zu den gebräuchlichen Identifizierungsmöglichkeiten zählen Tokens wie Karten oder Schlüsselanhänger, persönliche Identifikationsnummern (PINs) und REX-Geräte (Request to Exit).

Weitere Informationen zu Zugangsdaten finden Sie unter *Zugangsdaten für Benutzer auf Seite 41*.

Folgende Identifizierungsmöglichkeiten stehen zur Verfügung:

- **Nur Einrichtungscode** – Der Benutzer erhält Zugang zum Stockwerk mit einer vom Leser akzeptierten Karte oder einem anderen Token mit dem Einrichtungscode.
- **Nur Kartennummer** – Der Benutzer erhält Zugang zum Stockwerk mit einer vom Leser akzeptierten Karte oder einem anderen Token. Die Kartennummer ist eine eindeutige Nummer, die in der Regel auf die Karte aufgedruckt ist. Informationen über die Position der Kartennummer finden Sie in den Anweisungen des Herstellers. Die Kartennummer kann auch vom System abgerufen werden. Die Karte durch einen angeschlossenen Leser ziehen, den Leser in der Liste wählen und **Abrufen** anklicken.
- **Nur Rohdatenkarte** – Der Benutzer erhält Zugang zum Stockwerk mit einer vom Leser akzeptierten Karte oder einem anderen Token. Die Informationen sind als Rohdaten auf der Karte gespeichert. Die Rohdaten der Karte können auch vom System abgerufen werden. Ziehen Sie die Karte durch einen angeschlossenen Reader, wählen Sie den Reader in der Liste aus, und klicken Sie auf **Retrieve (Abrufen)**. Diese Art der Identifizierung nur verwenden, wenn keine Kartennummer ermittelt werden kann.
- **Nur PIN** – Der Benutzer erhält Zugang zum Stockwerk mit einer vierstelligen Identifikationsnummer (PIN).
- **Einrichtungscode und PIN** – Der Benutzer erhält Zugang zum Stockwerk mit der Kombination aus einer vom Leser akzeptierten Karte bzw. einem anderen Token mit dem Einrichtungscode und einer PIN. Der Benutzer muss die Identifizierung in der angegebenen Reihenfolge durchführen (zuerst die Karte, dann die PIN).
- **Kartennummer und PIN** – Der Benutzer erhält Zugang zum Stockwerk mit der Kombination aus einer vom Leser akzeptierten Karte bzw. einem anderen Token und einer PIN. Der Benutzer muss die Identifizierung in der angegebenen Reihenfolge durchführen (zuerst die Karte, dann die PIN).
- **Rohdatenkarte und PIN** – Der Benutzer erhält Zugang zum Stockwerk mit der Kombination aus einer vom Leser akzeptierten Karte bzw. einem anderen Token und einer PIN. Diese Art der Identifizierung nur verwenden, wenn keine Kartennummer ermittelt werden kann. Der Benutzer muss die Identifizierung in der angegebenen Reihenfolge durchführen (zuerst die Karte, dann die PIN).
- **REX** – Der Benutzer erhält Zugang zum Stockwerk durch die Aktivierung eines REX (Request to Exit)-Geräts, beispielsweise eines Tasters, eines Sensors, oder einer Druckstange.

Geplante Entriegelungsstatus hinzufügen

Um automatisch allen für eine bestimmte Zeit Zugang zu einer Etage zu gewähren, der betreffenden Etage den Status **Scheduled unlock (Geplante Entriegelung)** hinzufügen und einen Zugangszeitplan hinzufügen.

Zum Beispiel ist die Etage während den Geschäftszeiten allen zugänglich:

1. **Access Management (Zugangsverwaltung)** aufrufen und die Registerkarte **Floors (Etagen)** wählen.
2. Neben dem zu bearbeitenden Punkt der Liste **Etagen**  anklicken.
3. **Add scheduled unlock (Geplante Entriegelung hinzufügen) anklicken.**
4. Für Etagen mit einem Schloss **Unlock state (Entriegelungsstatus)unlocked (entriegelt)** wählen. Für Türen mit zwei Schlössern **Unlock both locks (Beide Schlösser entriegeln)** wählen.
5. Klicken Sie auf **OK**.
6. Den Zugangszeitplan **Office hours (Geschäftszeiten)** auf den Status **Scheduled unlock (Geplante Entriegelung)** ziehen.

Zum Bestätigen der Entriegelungszeit  anklicken.

Zum Löschen einer geplanten Entriegelung oder zum Bearbeiten eines Zeitplans  anklicken.

Manuelle Etagenaktionen verwenden

Etagen können verschiedene Zugangsberechtigungen haben, eingeschränkt oder für jedermann zugänglich. Zeitweiliger Zugang kann auf der Registerkarte **Floors (Etagen)** über die Option **Manuelle Etagenaktionen** gewährt werden. Welche manuellen Etagenaktionen für eine bestimmte Etage zur Verfügung stehen hängt davon ab, wie die Etage konfiguriert wurde.

Manuelle Etagenaktionen verwenden:

1. **Access Management (Zugangsverwaltung)** aufrufen und die Registerkarte **Floors (Etagen)** wählen.
2. In der Liste **Floors (Etagen)** neben der zu bearbeitenden Etage anklicken.
3. Die erforderliche Etagenaktion anklicken. Siehe *Manuelle Etagenaktionen auf Seite 40*.

Hinweis

Um manuelle die Etagenaktionen zu nutzen, die Seite Access Management (Zugangsverwaltung) über den an die spezifische Tür angeschlossenen Etagencontroller öffnen. Wird die Seite Access Management (Zugangsverwaltung) über einen anderen Etagencontroller geöffnet, wird statt der manuellen Etagenaktionen ein Link zu der Übersichtsseite des Etagencontrollers angezeigt, mit dem die spezifische Etage verbunden ist. Den Link anklicken, **Access Management (Zugangsverwaltung)** aufrufen und die Registerkarte **Floors (Etagen)** wählen.

Manuelle Etagenaktionen

Folgende manuelle Etagenaktionen stehen zur Verfügung:

- **Get floor status (Etagenstatus aufrufen)** – Den aktuellen Status des an eine Etage angeschlossenen Relais überprüfen.
- **Access (Zutritt)** – Gewährt Benutzern Zutritt zu einer Etage. Es gilt die entsprechende Zutrittsdauer. Siehe *Schlösser und Türmonitore konfigurieren auf Seite 14*.
- **Unlock (Entriegeln)** – Es wird uneingeschränkt Zutritt zur Etage gewährt, bis **Lock (Verriegeln)** betätigt, ein zeitplanbasierter Etagenstatus aktiviert oder der Türcontroller neu gestartet wird.
- **Lock (Verriegeln)** – Es wird uneingeschränkt Zutritt zur Etage verwehrt, bis **Unlock (Entriegeln)** betätigt, ein zeitplanbasierter Etagenstatus aktiviert oder der Türcontroller neu gestartet wird.

Benutzer erstellen und bearbeiten

Jede Person benötigt ein eigenes Benutzerprofil, um Zugang über Türen im Zugangskontrollsystem zu erhalten. Das Benutzerprofil besteht aus Zugangsdaten, mit denen das System die Benutzer identifiziert, sowie den Informationen, wann und wie die Benutzer an Türen Zugang erhalten.

Damit die Benutzerzugangsrechte effizient verwaltet werden können, muss jeder Benutzer einer oder mehreren Gruppen zugeordnet sein. Weitere Informationen, siehe *Erstellen und Bearbeiten von Gruppen*.

So erstellen Sie ein neues Benutzerprofil:

1. Rufen Sie **Access Management (Zugangsverwaltung)** auf.
2. Klicken Sie auf der Registerkarte **Users (Benutzer)** auf **Add new user (Neuen Benutzer hinzufügen)**.
3. Geben Sie im Dialogfeld **Add User (Benutzer hinzufügen)** die Zugangsdaten für den Benutzer ein. Siehe *Zugangsdaten für Benutzer auf Seite 41*.
4. Klicken Sie auf **Save (Speichern)**.
5. Ziehen Sie den Benutzer in der Liste **Groups (Gruppen)** in eine oder mehrere Gruppen. Erstellen Sie eine neue Gruppe, wenn die Liste **Groups (Gruppen)** leer ist. Siehe *Erstellen und Bearbeiten von Gruppen auf Seite 34*.

Zum Erweitern eines Eintrags in der Liste **Users (Benutzer)** und zum Anzeigen der Zugangsdaten eines Benutzers anklicken.

Wenn Sie nach einem bestimmten Benutzer suchen möchten, geben Sie im Feld zum Filtern von Benutzern einen Filter ein. Wenn genauere Übereinstimmungen gefunden werden sollen, den Filtertext in doppelte Anführungszeichen setzen. Zum Beispiel: "John","potter" oder "virginia".

Um die Zugangsdaten von Benutzern zu bearbeiten, anklicken. Anschließend **Speichern** anklicken.

Um einen Benutzer zu löschen, anklicken.

Wichtig

Wenn ein Benutzer durch AXIS Visitor Manager erstellt wurde, sollte er nicht in AXIS Entry Manager bearbeitet oder gelöscht werden. Weitere Informationen über AXIS Visitor Manager und den QR-Code-Reader-Dienst finden Sie unter *AXIS Visitor Access auf Seite 23*.

Zugangsdaten für Benutzer

Es stehen folgende Zugangsdaten für Benutzer zur Verfügung:

- **First name (Vorname)** (erforderlich)
- **Last Name (Nachname)**
- **Valid from (Gültig von)** und **Valid until (Gültig bis)** – Das Start- und Enddatum für die Gültigkeit der Zugangsdaten eines Benutzers eingeben. Das Datumsfeld anklicken und Tag, Monat und Jahr wählen. Das Datum kann auch direkt in das Feld eingegeben werden.
- **Suspend credential (Zugangsdaten sperren)** – Wählen, um die Zugangsdaten zu sperren. Wenn ein Benutzer gesperrt ist, wird diesem der Zugang bei sämtlichen Türen des Systems verweigert. Die Option deaktivieren, um dem Benutzer den Zugang wieder zu ermöglichen. Die Sperrung ist als vorübergehende Einstellung gedacht. Wenn einem Benutzer der Zugang dauerhaft verweigert werden soll, sollte das Benutzerprofil gelöscht werden.
- **PIN** (erforderlich anstelle einer Kartennummer oder Rohdaten-Karte) – Den vierstelligen persönlichen Identifizierungscode (PIN) eingeben, der vom Benutzer gewählt oder diesem zugewiesen wurde.
- **Facility code (Einrichtungscode)** – Einen Code eingeben, um das Zugangskontrollsystem der Einrichtung zu verifizieren. Wenn ein voreingestellter Einrichtungscode eingegeben wird, wird dieses Feld automatisch ausgefüllt. Siehe *Voreingestellter Einrichtungscode auf Seite 23*
- **Card number (Kartennummer)** (erforderlich anstelle einer PIN oder Rohdaten-Karte) – Die Kartennummer eingeben. Informationen zur Position der Kartennummer finden Sie in den Anweisungen des Herstellers. Die Kartennummer kann auch vom System abgerufen werden. Die Karte durch ein angeschlossenes Lesegerät ziehen, das Lesegerät aus der Liste wählen und **Retrieve (Abrufen)** anklicken.
- **Rohdaten-Karte** (erforderlich anstelle einer PIN oder Kartennummer) – Die Daten der Rohdaten-Karte eingeben. Die Daten können vom System abgerufen werden. Ziehen Sie die Karte durch einen angeschlossenen Leser, wählen Sie den Leser in der Liste aus, und klicken Sie auf **Retrieve (Abrufen)**. Verwenden Sie diese Art der Identifizierung nur, wenn keine Kartennummer ermittelt werden kann.
- **Long access time (Lange Zugangszeit)** – Diese Option wählen, um eine vorhandene Zugangsdauer außer Kraft zu setzen und dem Benutzer die lange Zugangszeit für die Tür zu gewähren. Siehe *Informationen zu Türmonitoren und Zeitoptionen auf Seite 15*
- **License plate (Fahrzeugkennzeichen)** (in einer Standard-Türcontrollerinstallation ist diese Zugangsberechtigung nicht verfügbar) – Wenn diese Zugangsberechtigung von einer Partner-Software aktiviert wird, das Fahrzeugkennzeichen des Benutzers eingeben.
  Diese Zugangsberechtigung kann nur gepaart mit Software von Axis Partnern und einer Kamera mit Software zur Erkennung von Nummernschildern verwendet werden. Für weitere Informationen bitte den Axis Partner oder örtlichen Axis Handelsvertreter kontaktieren.

Hinweis

Die Schaltfläche **Retrieve (Abrufen)** ist nur verfügbar, wenn die Konfiguration der Hardware abgeschlossen wurde und ein oder mehrere Lesegeräte mit dem Controller verbunden sind.

Importieren von Benutzern

Sie können dem System Benutzer hinzufügen, indem Sie eine Textdatei im kommagetrennten Format (CSV) importieren. Das Importieren von Benutzern empfiehlt sich, wenn viele Benutzer gleichzeitig hinzugefügt werden sollen.

Um Benutzer zu importieren, müssen Sie zunächst eine Datei (CSV oder TXT) mit kommagetrennten Werten erstellen und speichern. Werte mit Kommas und nicht mit Leerzeichen trennen. Benutzer durch Zeilenumbruch trennen.

Beispiel

```
jane,doe,1234,12345678,abc123
john,doe,5435,87654321,cde321
```

Benutzer importieren:

1. **Setup > Import Users (Setup > Benutzer importieren)** aufrufen.
2. Die CSV- oder TXT-Datei mit der Benutzerliste ermitteln und auswählen.
3. Wählen Sie für jede Spalte die richtige Option für die Zugangsdaten aus.
4. Klicken Sie zum Importieren der Benutzer auf **Import users (Benutzer importieren)**.
5. Überprüfen Sie, ob jede Spalte den richten Typ von Zugangsdaten enthält.
6. Wenn die Spalten die richtigen Informationen enthalten, klicken Sie auf **Start importing users (Importieren von Benutzern starten)**. Wenn die Spalten nicht die richtigen Informationen enthalten, klicken Sie auf **Cancel (Abbrechen)**, und beginnen Sie von vorne.
7. Wenn der Import abgeschlossen ist, klicken Sie auf **OK**.

Für Zugangsdaten stehen folgende Optionen zur Verfügung:

- **First name (Vorname)**
- **Last name (Nachname)**
- **PIN code (PIN-Code)**
- **Card number (Kartennummer)**
- **License plate (Fahrzeugkennzeichen)**
- **Unassigned (nicht zugeordnet)** – Werte, die nicht importiert werden. Diese Option wählen, um eine bestimmte Spalte zu überspringen.

Weitere Informationen zu Zugangsdaten finden Sie unter *Benutzer erstellen und bearbeiten*.

Exportieren von Benutzern

Die Seite „Export" (Exportieren) zeigt eine kommagetrennte (CSV-)Liste aller Benutzer im System an. Mithilfe dieser Liste können Benutzer in ein anderes System importiert werden.

So exportieren Sie die Benutzerliste:

1. Öffnen Sie einen Text-Editor, und erstellen Sie ein neues Dokument.
2. Wechseln Sie zu **Setup > Export Users (Setup > Benutzer exportieren)**.
3. Wählen Sie alle Werte auf der Seite aus, und kopieren Sie diese.
4. Fügen Sie die Werte in das Textdokument ein.
5. Speichern Sie das Dokument als kommagetrennte Datei (CSV) oder als Textdatei (TXT).

Beispiele für Kombinationen von Zugangszeitplänen

Identifizierungstyp- und Gruppenzeitpläne können für verschiedene Zwecke auf unterschiedliche Art kombiniert werden. Die folgenden Beispiele folgen der unter *Seite 31* beschriebenen Vorgehensweise.

Beispiel

So erstellen Sie eine Kombination von Zeitplänen, mit der

- Sicherheitspersonal jederzeit Zugang an einer Tür gewährt wird,
  - bei Verwendung der persönlichen Karte während der Tagschicht (Montag bis Freitag, von 6 bis 16 Uhr), wobei
  - außerhalb der Tagschicht Karte und PIN zur Identifizierung erforderlich sind, und welche
- weiterem Personal der Tagschicht ausschließlich zu den Zeiten der Tagschicht Zugang zu der Tür gewährt
  - und zur Identifizierung die Karte einsetzen muss:

1. Erstellen Sie einen **Addition schedule (Additionszeitplan)** mit dem Namen **Tagschicht**. Siehe *Seite 32*.
2. Erstellen Sie ein **Zeitplanereignis** das von Montag bis Freitag und zwischen 06:00 und 16:00 eintritt.
3. Erstellen Sie zwei Gruppen, eine **Gruppe** mit der Bezeichnung **Sicherheitspersonal** und eine **Gruppe** mit der Bezeichnung **Personal Tagschicht**. Siehe *Seite 34*.
4. Ziehen Sie den vordefinierten Zugangszeitplan **Always (Immer)** auf die Gruppe **Wachpersonal**.
5. Ziehen Sie den Zugangszeitplan **Tagschicht** auf die Gruppe **Personal Tagschicht**.
6. Fügen Sie dem Leser der Tür die Identifizierungstypen **Card number and PIN (Kartennummer und PIN)** und **Card number only (Nur Kartennummer)** hinzu.
7. Ziehen Sie den vordefinierten Zugangszeitplan **Always (Immer)** auf den Identifizierungstyp **Card number and PIN (Kartennummer und PIN)**.
8. Ziehen Sie den Zugangszeitplan **Day shift hours (Tagschicht)** auf den Identifizierungstyp **Card number only (Nur Kartennummer)**.
9. Ziehen Sie die Tür auf beide Gruppen. Fügen Sie dann Benutzer zu den Gruppen hinzu. Siehe *Seite 40*.

Beispiel

Um eine Zeitplankombination zu erstellen, die

- die dem Sicherheitspersonal jederzeit Zugang an einer Tür gewährt,
  - bei Verwendung der persönlichen Karte während der Tagschicht (Montag bis Freitag, von 6 bis 16 Uhr), wobei
  - außerhalb der Tagschicht Karte und PIN zur Identifizierung erforderlich sind, und dass
- weiteres Personal der Tagschicht jeden Tag zwischen 6 und 16 Uhr,
  - durch Identifizierung mit der Karte Zugang zu der Tür erhält und
  - außerhalb der Tagschicht und an Wochenenden durch Identifizierung mit Karte und PIN:

1. Erstellen Sie einen **Addition schedule (Additionszeitplan)** mit dem Namen **Tagschicht**. Siehe *Seite 32*.
2. Erstellen Sie ein **Zeitplanereignis** das von Montag bis Freitag und zwischen 06:00 und 16:00 eintritt.
3. Erstellen Sie einen **Subtraktionszeitplan)** mit dem Namen **Nächte und Wochenenden**.
4. Erstellen Sie ein **Zeitplanereignis** für Nächte und Wochenenden, das Samstags und Sonntags sowie zwischen 16:00 und 6:00 Uhr eintritt.
5. Ziehen Sie den vordefinierten Zugangszeitplan **Immer** und den Zugangszeitplan **Nächte und Wochenenden** auf die Gruppe **Personal Tagschicht**.
6. Erstellen Sie zwei Gruppen, eine **Gruppe** mit der Bezeichnung **Wachpersonal** und eine **Gruppe** mit der Bezeichnung **Personal Tagschicht**. Siehe *Seite 34*.

7. Ziehen Sie den vordefinierten Zugangszeitplan **Always (Immer)** auf die Gruppe **Wachpersonal** und auf die Gruppe **Personal Tagschicht**.
8. Ziehen Sie den Zugangszeitplan **Nächte und Wochenenden** auf die Gruppe **Personal Tagschicht**.
9. Fügen Sie dem Leser der Tür die Identifizierungstypen **Card number and PIN (Kartennummer und PIN)** und **Card number only (Nur Kartennummer)** hinzu.
10. Ziehen Sie den vordefinierten Zugangszeitplan **Always (Immer)** auf den Identifizierungstyp **Card number and PIN (Kartennummer und PIN)**.
11. Ziehen Sie den Zugangszeitplan **Day shift hours (Tagschicht)** auf den Identifizierungstyp **Card number only (Nur Kartennummer)**.
12. Ziehen Sie die Tür auf beide Gruppen. Fügen Sie dann Benutzer zu den Gruppen hinzu. Siehe *Seite 40*.

Konfigurieren von Alarmen und Ereignissen

Systemereignisse, z. B. wenn ein Benutzer eine Karte durchzieht oder ein REX-Gerät aktiviert wird, werden im Ereignisprotokoll gespeichert. Protokollierte Ereignisse lassen sich so konfigurieren, dass diese Alarme auslösen, die wiederum im Alarmprotokoll gespeichert werden.

- Anzeigen des Ereignisprotokolls. Siehe *Seite 45*.
- Ereignisprotokoll exportieren Siehe *Seite 45*
- Anzeigen des Alarmprotokolls. Siehe *Seite 46*.
- Konfigurieren der Ereignis- und Alarmprotokolle. Siehe *Seite 46*.

Außerdem können Alarme so konfiguriert werden, dass sie Aktionen wie E-Mail-Benachrichtigungen auslösen. Weitere Informationen, siehe *Aktionsregeln einrichten auf Seite 47*.

Anzeigen des Ereignisprotokolls

Um protokollierte Ereignisse anzuzeigen, **Event Log (Ereignisprotokoll)** aufrufen.

Wenn Global events (Globale Ereignisse) aktiviert ist, können die Ereignisprotokolle aller Türcontroller des Systems geöffnet werden. Weitere Informationen zu globalen Ereignissen, siehe *Konfigurieren der Ereignis- und Alarmprotokolle auf Seite 46*.

Um ein Element im Ereignisprotokoll aufzuklappen und Ereignisdetails aufzurufen,  anklicken.

Mithilfe von Filtern können Sie im Ereignisprotokoll einfacher bestimmte Ereignisse finden. Um die Liste zu filtern, einen oder mehrere Ereignisprotokollfilter wählen, und **Apply filters (Filter anwenden)** anklicken. Weitere Informationen, siehe *Ereignisprotokollfilter auf Seite 45*

Als Administrator sind Sie möglicherweise an bestimmten Ereignissen besonders interessiert. Daher können Sie auswählen, welche Ereignisse für welchen Controller protokolliert werden. Weitere Informationen, siehe *Optionen für Ereignisprotokolle auf Seite 46*

Ereignisprotokollfilter

Der Inhalt von Ereignisprotokollen kann mithilfe der folgenden Filter eingegrenzt werden:

- Benutzer – Filter für Ereignisse mit Bezug auf den ausgewählten Benutzer.
- Tür und Etage – Filter für Ereignisse mit Bezug auf eine bestimmte Tür oder Etage.
- Typ – Filter für den Ereignistyp.
- Quelle – Filter für Ereignisse eines gewählten Controllers Verfügbar nur in Controllerclustern und bei aktivierten globalen Ereignissen.
- Datum und Uhrzeit – Filtern des Ereignisprotokolls nach Datum und Uhrzeit

Ereignisprotokoll exportieren

Um protokollierte Ereignisse anzuzeigen, **Event Log (Ereignisprotokoll)** aufrufen.

1.  anklicken.
2. Um den Export zu starten, aus dem Aufklappmenü das Exportformat wählen.

Hinweis

Das Format CSV wird von allen Browsern unterstützt, das Format XLSX von Chrome™ und Internet Explorer®.

Hinweis

Mit Abschluss des Exports wechselt die Exportschaltfläche von  auf  . Für einen weiteren Export die Webseite aktualisieren. Die Exportschaltfläche wechselt zurück zu  .

Anzeigen des Alarmprotokolls

Zum Anzeigen der ausgelösten Alarme rufen Sie **Alarm Log (Alarmprotokoll)** auf. Wenn „Global events (Globale Ereignisse)" aktiviert ist, können Sie das Alarmprotokoll jedes Tür-Controllers im System öffnen. Weitere Informationen zu globalen Ereignissen finden Sie unter *Konfigurieren der Ereignis- und Alarmprotokolle auf Seite 46*.

Um weitere Informationen zu einem Punkt im Alarmprotokoll wie zum Beispiel die Bezeichnung und den Türstatus anzuzeigen,  anklicken

Zum Entfernen eines Alarms aus der Liste nach dem Überprüfen der Alarmursache **Acknowledge (Quittieren)** anklicken. Um alle Alarme zu entfernen, **Acknowledge all alarms (Alle Alarme quittieren** anklicken.

Als Administrator müssen Ereignisse für das Auslösen von Alarmen festlegt werden. Daher können Sie wählen, welche Ereignisse Alarme auslösen sollen und für welche Regler. Weitere Informationen, siehe *Optionen für Alarmprotokolle auf Seite 47*

Konfigurieren der Ereignis- und Alarmprotokolle

Auf der Seite „Configure Event and Alarm Logs" (Ereignis- und Alarmprotokolle konfigurieren) können Sie festlegen, welche Ereignisse protokolliert werden und Alarme auslösen.

Um Ereignisse und Alarme auf allen verbundenen Controllern zu teilen, aktivieren Sie **Global Events (Globale Ereignisse)**. Wenn „Global Events" (Globale Ereignisse) aktiviert ist, müssen für die Verwaltung der Ereignisse und Alarme sämtlicher Tür-Controller des Systems nur eine Ereignis- und eine Alarmprotokollseite geöffnet werden. „Globale Events" (Globale Ereignisse) ist standardmäßig aktiviert.

Wenn Sie „Global Events" (Globale Ereignisse) deaktivieren, müssen für die Verwaltung der Ereignisse und Alarme der Tür-Controller des Systems für jeden einzelnen jeweils eine Ereignis- und eine Alarmprotokollseite geöffnet werden.

Wichtig

Jedes Mal, wenn Sie „Global Events" (Globale Ereignisse) aktivieren oder deaktivieren, wird das Ereignisprotokoll zurückgesetzt. Das heißt, alle vorherigen Ereignisse werden gelöscht, und ein neues Ereignisprotokoll wird angelegt.

Außerdem können Alarme so konfiguriert werden, dass sie Aktionen wie E-Mail-Benachrichtigungen auslösen. Weitere Informationen, siehe *Aktionsregeln einrichten auf Seite 47*.

Optionen für Ereignisprotokolle

Um festzulegen, welche Ereignisse in das Ereignisprotokoll aufgenommen werden sollen, **Setup > Configure Event and Alarm Logs (Setup > Ereignis- und Alarmprotokolle konfigurieren)** aufrufen.

Für das Protokollieren von Ereignissen stehen folgende Optionen zur Verfügung:

- **No logging (Keine Protokollierung)** – Das Protokollieren von Ereignissen ist deaktiviert. Das Ereignis wird nicht registriert oder in das Ereignisprotokoll aufgenommen.
- **Log for all controllers (Alle Controller protokollieren)** – Das Protokollieren von Ereignissen für alle Türcontroller ist aktiviert. Das Ereignis wird für alle Controller registriert und in das Ereignisprotokoll aufgenommen.
- **Log for selected controllers (Ausgewählte Controller protokollieren)** – Das Protokollieren von Ereignissen bestimmter Türcontroller ist aktiviert. Das Ereignis wird für alle ausgewählten Controller registriert und in das Ereignisprotokoll aufgenommen. Wählen Sie diese Option für Ereignisse aus, die entweder mit der Alarmprotokolloption **No alarms (Kein Alarm)** oder **Log alarm for selected controllers (Alarm für ausgewählte Controller protokollieren)** kombiniert werden.

Klicken Sie in der Liste **Configure event logging (Protokollierung von Ereignissen konfigurieren)** unter dem zu aktivierenden Ereignisprotokollelement auf **Select controllers (Controller auswählen)**. Das Dialogfeld **Device Specific Event Logging (Protokollierung gerätspezifischer Ereignisse)** wird geöffnet. Wählen Sie unter **Log event (Ereignis protokollieren)** die Controller aus, deren Alarmprotokoll aktiviert werden soll, und klicken Sie auf **Save (Speichern)**.

Optionen für Alarmprotokolle

Zum Festlegen der Ereignisse, die einen Alarm auslösen sollen, **Setup > Configure Event and Alarm Logs (Setup > Ereignis- und Alarmprotokolle konfigurieren)** aufrufen.

Es stehen folgende Optionen zum Auslösen und Protokollieren von Alarmen zur Verfügung:

- **No alarms (Keine Alarme)** – Alarmprotokoll deaktiviert. Das Ereignis löst keine Alarme aus und wird nicht in das Alarmprotokoll aufgenommen.
- **Log for all controllers (Alarm für alle Quellen protokollieren)** – Alarmprotokoll für alle Türcontroller aktiviert. Das Ereignis löst einen Alarm aus und wird in das Alarmprotokoll aufgenommen.
- **Log alarm for selected controllers (Alarm für ausgewählte Controller protokollieren)** – Alarmprotokoll für ausgewählte Türcontroller aktivieren. Das Ereignis löst einen Alarm aus und wird in das Alarmprotokoll aufgenommen.

  In der Liste **Configure alarm logging (Alarmprotokoll konfigurieren)** unter dem zu aktivierenden Alarmprotokollelement **Select controllers (Controller auswählen)** wählen. Das Dialogfeld **Device Specific Alarm Logging (Gerätspezifische Alarmauslösung)** wird geöffnet. Wählen Sie unter **Trigger alarm (Alarm auslösen)** die Türcontroller, deren Alarme protokolliert werden sollen, und klicken Sie auf **Save (Speichern)**.

Aktionsregeln einrichten

Auf den Ereignisseiten können Sie das Axis Produkt so konfigurieren, dass Aktionen bei unterschiedlichen Ereignissen ausgeführt werden. Beispielsweise kann das Produkt eine E-Mail-Benachrichtigung senden oder einen Ausgangs-Port aktivieren, wenn ein Alarm ausgelöst wird. Der Satz von Bedingungen, mit denen Art und Zeitpunkt der Auslösung der Aktion definiert werden, wird als Aktionsregel bezeichnet. Wenn mehrere Bedingungen definiert werden, müssen zum Auslösen der Aktion alle Bedingungen erfüllt sein.

Für weitere Informationen zu den verfügbaren Auslösern und Aktionen, siehe *Auslöser auf Seite 48* und *Aktionen auf Seite 50*.

Dieses Beispiel beschreibt das Einrichten einer Aktionsregel zum Senden einer E-Mail-Benachrichtigung, wenn ein Alarm ausgelöst wird.

1. Die Alarme konfigurieren. Siehe *Konfigurieren der Ereignis- und Alarmprotokolle auf Seite 46*.
2. **Setup > Zusätzliche Controllerkonfiguration > Ereignisse > Aktionsregeln** aufrufen und **Hinzufügen** anklicken.
3. Wählen Sie **Enable rule (Regel aktivieren)** aus und geben Sie einen beschreibenden Namen für die Regel ein.
4. Wählen Sie in der Dropdown-Liste **Trigger (Auslöser)** die Option **Event Logger (Ereignisaufzeichnung)** aus.
5. Wählen Sie bei Bedarf einen **Schedule (Zeitplan)** und **Additional conditions (Weitere Bedingungen)** aus. Siehe unten.
6. Aus der Dropdown-Liste **Typ** unter **Aktionen** die Option **Benachrichtigung senden** wählen.
7. Aus der Dropdown-Liste einen E-Mail-Empfänger wählen. Siehe *Empfänger hinzufügen auf Seite 51*.

Dieses Beispiel beschreibt das Einrichten einer Aktionsregel, um einen Ausgangsport zu aktivieren, wenn die Tür aufgebrochen wird.

1. Wechseln Sie zu **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Setup > Zusätzliche Controller-Konfiguration > Systemoptionen > Anschlüsse und Geräte > E/A-Ports)**.
2. Wählen Sie in der gewünschten Dropdown-Liste **I/O Port Type (Typ des E/A-Ports)** die Option **Output (Ausgabe)** aus und geben Sie einen **Name** ein.
3. Wählen Sie den **Normal state (Normalzustand)** des E/A-Ports aus und klicken Sie auf **Save (Speichern)**.
4. Wechseln Sie zu **Events > Action Rules (Ereignisse > Aktionsregeln)** und klicken Sie auf **Add (Hinzufügen)**.

5. Wählen Sie in der Dropdown-Liste **Trigger (Auslöser)** die Option **Door (Tür)** aus.
6. Wählen Sie in der Dropdown-Liste die Option **Door Alarm (Türalarm)** aus.
7. Wählen Sie in der Dropdown-Liste die gewünschte Tür aus.
8. Wählen Sie in der Dropdown-Liste die Option **DoorForcedOpen (Tür aufgebrochen)** aus.
9. Wählen Sie bei Bedarf einen **Schedule (Zeitplan)** und **Additional conditions (Weitere Bedingungen)** aus. Siehe unten.
10. Wählen Sie in der Dropdown-Liste **Type (Typ)** unter **Actions (Aktionen)** die Option **Output Port (Ausgangs-Port)** aus.
11. Wählen Sie in der Dropdown-Liste **Port** den gewünschten Ausgangs-Port aus.
12. Legen Sie den Zustand auf **Active (Aktiv)** fest.
13. Wählen Sie **Duration (Dauer)** und **Go to opposite state after (Danach zum Gegenzustand wechseln)** aus. Geben Sie dann die gewünschte Dauer der Aktion ein.
14. Klicken Sie auf **OK**.

Um mehrere Auslöser für die Aktionsregel zu verwenden, wählen Sie **Additional conditions (Weitere Bedingungen)** aus und fügen Sie durch Klicken auf **Add (Hinzufügen)** weitere Auslöser hinzu. Bei Verwendung zusätzlicher Bedingungen müssen zum Auslösen der Aktion alle Bedingungen erfüllt sein.

Damit eine Aktion nicht wiederholt ausgelöst wird, kann eine Zeitdauer für **Wait at least (Mindestens warten)** festgelegt werden. Geben Sie die Zeit in Stunden, Minuten und Sekunden ein, während der Auslöser ignoriert werden soll und bevor die Aktionsregel erneut aktiviert werden kann.

Für weitere Informationen, siehe die Hilfeseiten des Produkts.

Auslöser

Zu den verfügbaren **Auslösern** und **Bedingungen** einer Aktionsregel gehören:

- **Zugangspunkt**
  - **Access Point Enabled (Zugangspunkt aktiviert)** – Löst die Aktionsregel aus, wenn ein Zugangspunktgerät wie etwa ein Lesegerät oder REX-Gerät konfiguriert ist. Dies kann zum Beispiel nach Abschluss der Hardwarekonfiguration oder nachdem ein Identifizierungstyp hinzugefügt wurde der Fall sein.
- **Konfiguration**
  - **Access Point Changed (Zugangspunkt geändert)** – Löst die Aktionsregel aus, wenn die Konfiguration eines Zugangspunktgeräts wie etwa eines Lesegeräts oder REX-Geräts geändert wird. Dies kann der Fall sein, wenn Hardware konfiguriert oder ein Identifizierungstyp bearbeitet wird und dabei die Art des Öffnens einer Tür geändert wird.
  - **Access Point Removed (Zugangspunkt entfernt)** – Löst die Aktionsregel aus, wenn die Hardwarekonfiguration eines Zugangspunktgeräts wie etwa eines Lesegeräts oder REX-Geräts zurückgesetzt wird.
  - **Area Changed (Bereich geändert)** – Wird von dieser Version des AXIS Entry Manager nicht unterstützt. Dies muss von einem Client wie einem Zugangsverwaltungssystem über die VAPIX®-API (Application Programming Interface), die diese Funktion unterstützt, konfiguriert und mit Geräten verwendet werden, die die erforderlichen Signale bereitstellen können. Löst die Aktionsregel aus, wenn ein Zugangsbereich geändert wird.
  - **Area Removed (Bereich entfernt)** – Wird von dieser Version des AXIS Entry Manager nicht unterstützt. Dies muss von einem Client wie einem Zugangsverwaltungssystem über die VAPIX®-API (Application Programming Interface), die diese Funktion unterstützt, konfiguriert und mit Geräten verwendet werden, die die erforderlichen Signale bereitstellen können. Löst die Aktionsregel aus, wenn ein Zugangsbereich aus dem System entfernt wird.
  - **Door Changed (Tür geändert)** – Löst die Aktionsregel aus, wenn die Konfigurationseinstellungen der Tür, zum Beispiel der Türname, geändert werden oder eine Tür zum System hinzugefügt wird. Dies kann zum Beispiel zum Senden einer Benachrichtigung verwendet werden, wenn eine Tür installiert und konfiguriert wird.

  - **Door Removed (Tür entfernt)** – Löst die Aktionsregel aus, wenn eine Tür aus dem System entfernt wird. Dies kann zum Beispiel zum Senden einer Benachrichtigung verwendet werden, wenn eine Tür aus dem System entfernt wird.

- **Tür**

  - **Battery Alarm (Batteriealarm)** – Löst die Aktionsregel aus, wenn die Batterie schwach oder entladen ist.

  - **Door Alarm (Türalarm)** – Löst die Aktionsregel aus, wenn der Türmonitor anzeigt, dass die Tür aufgebrochen wurde, zu lange geöffnet oder anderweitig fehlerhaft ist. Dies kann zum Beispiel zum Senden einer Benachrichtigung verwendet werden, wenn die Tür aufgebrochen wird.

  - **Door Double-Lock Monitor(Doppelschlosstür-Monitor)** – Löst die Aktionsregel aus, wenn der Status des sekundären Schlosses auf verriegelt oder entriegelt wechselt.

  - **Door Lock Monitor (Türschlossmonitor)** – Löst die Aktionsregel aus, wenn der Zustand des Standardschlosses auf verriegelt oder entriegelt wechselt. Zum Beispiel wird ein Fehler ausgelöst, wenn der Türmonitor erkennt, dass die Tür geöffnet ist, obwohl sich das Schloss in Verriegelungsposition befindet.

  - **Door Mode (Türmodus)** – Löst eine Aktionsregel aus, wenn der Status der Tür geändert wird, wenn zum Beispiel auf die Tür zugegriffen wurde, die Tür blockiert wurde oder sich die Tür im Verriegelungsmodus befindet. Ausführlichere Beschreibungen dieser Modi finden Sie in der Onlinehilfe.

  - **Door Monitor (Türmonitor)** – Löst eine Aktionsregel aus, wenn sich der Status des Türmonitors ändert. Dies kann zum Beispiel zum Senden einer Benachrichtigung verwendet werden, wenn ein Türmonitor erkennt, dass die Tür geöffnet oder geschlossen wurde.

  - **Door Tamper (Türmanipulation)** – Löst eine Aktionsregel aus, wenn der Türmonitor eine Unterbrechung der Verbindung erkennt, zum Beispiel wenn zum Türmonitor führende Kabel durchtrennt werden. Bei Verwenden dieses Auslösers sicherstellen, dass **Enable supervised inputs (Überwachte Eingänge aktivieren)** ausgewählt ist und dass Abschlusswiderstände an den entsprechenden Eingangsports der Türanschlüsse angebracht sind. Weitere Informationen, siehe *Überwachte Eingänge verwenden: auf Seite 17*.

  - **Door Warning (Türwarnung)** – Löst eine Aktionsregel aus, bevor der Alarm zu einer zu lange geöffneten Tür ausgelöst wird. Dies kann zum Beispiel zum Senden eines Warnsignals verwendet werden, dass der Türcontroller den eigentlichen Alarm (Alarm zu einer zu lange geöffneten Tür) sendet, wenn die Tür nicht in der festgelegten Zeit für eine zu lange geöffnete Tür geschlossen wird. Weitere Informationen zur Zeit von zu lange geöffneten Türen, siehe *Schlösser und Türmonitore konfigurieren auf Seite 14*.

  - **Lock Jammed (Schloss blockiert)** – Löst eine Aktionsregel aus, wenn das Schloss einer Funktür physisch blockiert ist.

- **Event Logger (Ereignisaufzeichnung)** – Zeichnet alle Ereignisse des Tür-Controllers auf, z. B. wenn ein Benutzer eine Karte durchzieht oder eine Tür öffnet. Wenn **Global events (Globale Ereignisse)** aktiviert ist, werden von der Ereignisaufzeichnung alle Ereignisse in jedem Controller des Systems aufgezeichnet. Unter **Setup > Configure Event and Alarm Logs (Setup > Ereignis- und Alarmprotokolle konfigurieren)** können Sie festlegen, bei welchen Alarmen und Ereignissen eine Aktionsregel ausgelöst wird. Die Ereignisaufzeichnung gilt für das gesamte System und kann bis zu 30.000 Ereignisse speichern. Bei Erreichen des Höchstwerts gilt das FIFO-Verfahren („first in first out"). Dabei wird das erste Ereignis zuerst überschrieben.

  - **Alarm** – Löst eine Aktionsregel aus, wenn einer der angegebenen Alarme ausgelöst wurde. Der Systemadministrator kann konfigurieren, welche Ereignisse wichtiger als andere sind, und auswählen, ob ein bestimmtes Ereignis einen Alarm auslösen soll.

  - **Dropped Alarms (Verworfene Alarme)** – Löst eine Aktionsregel aus, wenn neue Alarmaufzeichnungen nicht in die Alarmprotokolle geschrieben werden können. Dies kann der Fall sein, wenn so viele gleichzeitige Alarme vorliegen, dass die Ereignisaufzeichnung nicht mithalten kann. Wenn ein Alarm verworfen wird, kann eine Benachrichtigung an den Bediener gesendet werden.

  - **Dropped Events (Verworfene Ereignisse)** – Löst eine Aktionsregel aus, wenn neue Ereignisaufzeichnungen nicht in die Ereignisprotokolle geschrieben werden können. Dies kann der Fall sein, wenn so viele gleichzeitige Ereignisse vorliegen, dass die Ereignisaufzeichnung nicht mithalten kann. Wenn ein Ereignis verworfen wird, kann eine Benachrichtigung an den Bediener gesendet werden.

- **Hardware**
  - **Network (Netzwerk)** – Löst eine Aktionsregel bei Verlust der Netzwerk-Verbindung aus. **Yes (Ja)** wählen, um die Aktionsregel bei Verlust der Netzwerk-Verbindung auszulösen. **No (Nein)** wählen, um die Aktionsregel bei wiederhergestellter Netzwerk-Verbindung auszulösen. **IPv4/v6 address removed (IPv4/v6-Adresse entfernt)** oder **New IPv4/v6 address (Neue IPv4/v6-Adresse)** auswählen, um eine Aktion auszulösen, wenn die IP-Adresse sich ändert.
  - **Peer Connection (Gleichrangige Verbindung)** – Löst eine Aktionsregel aus, wenn das Axis Produkt eine Verbindung mit einem anderen Türcontroller hergestellt hat, die Netzwerk-Verbindung zwischen den Geräten unterbrochen ist oder das Koppeln der Türcontroller fehlgeschlagen ist. Dies kann beispielsweise zum Senden einer Benachrichtigung verwendet werden, wenn die Netzwerk-Verbindung eines Türcontrollers unterbrochen wurde.
- **Eingangssignal**
  - **Digital Input Port (Digitaler Eingangs-Port)** – Löst eine Regel aus, wenn ein E/A-Port ein Signal von einem verbundenen Gerät empfängt. Siehe *E/A-Ports auf Seite 63*.
  - **Manual Trigger (Manuelle Auslösung)** – Löst eine Aktionsregel aus, wenn die manuelle Auslösung aktiviert ist. Dies kann von einem Client wie einem Zugangsverwaltungssystem über die VAPIX®-API (Application Programming Interface) verwendet werden, um eine Aktionsregel manuell zu starten oder zu stoppen.
  - **Virtual Inputs (Virtuelle Eingänge)** – Löst eine Aktionsregel aus, wenn sich der Status eines der virtuellen Eingänge ändert. Dies kann von einem Client wie einem Zugangsverwaltungssystem über die VAPIX®-API (Application Programming Interface) verwendet werden, um Aktionen auszulösen. Virtuelle Eingänge können beispielsweise mit Schaltflächen der Benutzeroberfläche des Verwaltungssystems verbunden werden.
- **Zeitplan**
  - **Interval (Intervall)** – Löst eine Aktionsregel zur Startzeit des Zeitplans aus und bleibt so lange aktiv, bis die Endzeit des Zeitplans erreicht ist.
  - **Pulse (Impuls)** – Löst eine Aktionsregel aus, wenn ein einmaliges Ereignis auftritt, also ein zu einem bestimmten Zeitpunkt auftretendes Ereignis ohne Dauer.
- **System**
  - **System Ready (System bereit)** – Löst die Aktionsregel bei Systembereitschaft aus. Das Axis Produkt kann beispielsweise bei Systemstart den Systemstatus erfassen und eine Benachrichtigung senden.

    Wählen Sie **Yes (Ja)** aus, um die Aktionsregel auszulösen, wenn sich das Produkt im Status „Bereit" befindet. Hinweis: Die Regel wird nur ausgelöst wird, nachdem alle erforderlichen Dienste, wie etwa das Ereignissystem, gestartet wurden.
- **Zeit**
  - **Recurrence (Wiederholung)** – Löst eine Aktionsregel durch Überwachen der erstellten Wiederholungen aus. Dieser Auslöser kann zum Initiieren von sich wiederholenden Aktionen wie dem stündlichen Senden von Benachrichtigungen verwendet werden. Wählen Sie ein Wiederholungsmuster aus, oder erstellen Sie ein neues Wiederholungsmuster. Weitere Informationen zum Einrichten eines Wiederholungsmusters, siehe *Wiederholungen einrichten auf Seite 52*.
  - **Use Schedule (Zeitplan verwenden)** – Löst eine Aktionsregel gemäß dem ausgewählten Zeitplan aus. Siehe *Zeitpläne einrichten auf Seite 52*.

Aktionen

Es können mehrere Aktionen konfiguriert werden:

- **Ausgangsport** – Aktivieren eines E/A-Ports zum Steuern eines externen Geräts.
- **Benachrichtigung senden** – Senden einer Benachrichtigung an einen Empfänger.

- **Status LED (Status-LED)** – Die Status-LED kann so eingestellt werden, dass sie während der Dauer der Aktionsregel oder eine bestimmte Anzahl von Sekunden blinkt. Die Status-LED kann bei Installation und Konfiguration verwendet werden, um visuell zu prüfen, ob die Auslösereinstellungen beispielsweise des Auslösers zu einer zu lange geöffneten Tür ordnungsgemäß funktionieren. Wählen Sie zum Festlegen der Blinkfarbe der Status-LED aus der Dropdown-Liste eine **LED Color (LED-Farbe)** aus.

Empfänger hinzufügen

Das Produkt kann Benachrichtigungen zu Ereignissen und Alarmen an Empfänger senden. Es muss mindestens ein Empfänger definiert werden, damit das Produkt Benachrichtigungen senden kann. Informationen zu den verfügbaren Optionen finden Sie unter *Empfängertypen auf Seite 51*.

So fügen Sie einen Empfänger hinzu:

1. Wechseln Sie zu **Setup > Additional Controller Configuration > Events > Recipients (Setup > Zusatzkontrollenkonfiguration > Ereignisse > Empfänger)** und klicken Sie auf **Add (Hinzufügen)**.
2. Geben Sie einen beschreibenden Namen ein.
3. Wählen Sie einen **Type (Typ)** für den Empfänger aus.
4. Geben Sie die für den Empfängertyp erforderlichen Informationen ein.
5. Klicken Sie auf **Test (Prüfen)**, um die Verbindung mit dem Empfänger zu prüfen.
6. Klicken Sie auf **OK**.

Empfängertypen

Es stehen folgende Empfängertypen zur Verfügung:

HTTP

HTTPS

E-Mail

TCP

E-Mail-Empfänger einrichten

Die E-Mail-Empfänger können mittels eines der aufgeführten E-Mail-Anbieter oder durch Angeben des SMTP-Servers, des Ports und der zum Beispiel von einem Firmen-E-Mail-Server verwendeten Authentifizierung konfiguriert werden.

Hinweis

Einige E-Mail-Dienste verwenden Sicherheitsfilter, die verhindern, dass Benutzer eine große Anzahl von Anhängen erhalten oder anzeigen, zeitgeplante E-Mails erhalten und anderes. Prüfen Sie die Sicherheitsrichtlinien des E-Mail-Anbieters, um Sendeprobleme und gesperrte E-Mail-Konten zu vermeiden.

So richten Sie mit einem der aufgeführten Anbieter einen E-Mail-Empfänger ein:

1. Wechseln Sie zu **Events > Recipients (Ereignisse > Empfänger)**, und klicken Sie auf **Add (Hinzufügen)**.
2. Geben Sie einen **Namen** ein, und wählen Sie aus der Liste **Type (Typ)** die Option **Email** aus.
3. Geben Sie im Feld **To (An)** die E-Mail-Adressen ein, an die E-Mails gesendet werden sollen. Trennen Sie mehrere Adressen mit Kommas.
4. Wählen Sie aus der Liste **Provider (Anbieter)** den E-Mail-Anbieter aus.
5. Die Benutzer-ID und das Kennwort für das E-Mail-Konto eingeben.
6. Klicken Sie auf **Test**, um eine Test-E-Mail zu senden.

Um z. B. mithilfe eines Firmen-E-Mail-Servers einen E-Mail-Empfänger einzurichten, führen Sie die oben angeführten Schritte durch, wählen jedoch als **Provider (Anbieter)User defined (Benutzerdefiniert)** aus. Geben Sie im Feld **From (Von)** die als Absender anzuzeigende E-Mail-Adresse ein. Wählen Sie **Advanced settings (Erweiterte Einstellungen)** aus, und geben Sie die SMTP-Server-Adresse, den Port und die Authentifizierungsmethode an. Wählen Sie optional **Use encryption (Verschlüsselung verwenden)** aus, um E-Mails über eine verschlüsselte Verbindung zu senden. Das Server-Zertifikat kann mit dem für das Axis Produkt verfügbaren Zertifikaten validiert werden. Weitere Informationen zum Hochladen von Zertifikaten finden Sie unter *Zertifikate auf Seite 56*.

Zeitpläne einrichten

Zeitpläne können als Auslöser oder als zusätzliche Bedingungen für Aktionsregeln verwendet werden. Verwenden Sie einen der vordefinierten Zeitpläne, oder erstellen Sie wie unten beschrieben einen neuen Zeitplan.

So erstellen Sie einen neuen Zeitplan:

1. Wechseln Sie zu **Setup > Additional Controller Configuration > Events > Schedules (Setup > Zusatzkontrollenkonfiguration > Ereignisse > Zeitpläne)**, und klicken Sie auf **Add (Hinzufügen)**.
2. Geben Sie einen beschreibenden Namen und die für einen täglichen, wöchentlichen, monatlichen oder jährlichen Zeitplan erforderlichen Informationen ein.
3. Klicken Sie auf **OK**.

Um den Zeitplan in einer Aktionsregel zu verwenden, wählen Sie den Zeitplan auf der Seite „Action Rule Setup (Aktionsregel-Setup)" in der Dropdown-Liste **Schedule (Zeitplan)** aus.

Wiederholungen einrichten

Mit Wiederholungen werden Aktionsregeln wiederholt ausgelöst, zum Beispiel alle 5 Minuten oder stündlich.

So richten Sie eine Wiederholung ein:

1. Wechseln Sie zu **Setup > Additional Controller Configuration (Zusatzkontrollenkonfiguration) > Events (Ereignisse) > Recurrences (Wiederholungen)** und klicken Sie auf **Add (Hinzufügen)**.
2. Einen aussagekräftigen Namen und das Wiederholungsmuster eingeben.
3. Klicken Sie auf **OK**.

Um die Wiederholung in einer Aktionsregel zu verwenden, wählen Sie zunächst auf der Seite „Action Rule Setup (Aktionsregel-Setup)" in der Dropdown-Liste **Trigger (Auslöser)** die Option **Time (Zeit)** aus.

Zum Ändern oder Entfernen von Wiederholungen wählen Sie die Wiederholung in der **Recurrences List (Wiederholungsliste)** aus und klicken Sie auf **Modify (Ändern)** oder **Remove (Entfernen)**.

Leser-Feedback

Mithilfe von LEDs und Signaltongebern senden Leser Feedback an den Benutzer (die Person, die an der Tür Zugang erhält oder dieses versucht). Der Tür-Controller kann eine Reihe von Feedbacksignalen auslösen. Einige sind im Tür-Controller vorkonfiguriert und werden von den meisten Lesern unterstützt.

Auch wenn sich Leser beim LED-Verhalten unterscheiden, verwenden sie doch in der Regel verschiedene Sequenzen von Dauer- und Blinklicht in Rot, Grün und Gelb.

Leser können auch mithilfe von Eintonhöhen-Signaltongebern verschiedene Sequenzen an kurzen und langen Signalen als Feedback übermitteln.

In der folgenden Tabelle sind die Ereignisse aufgeführt, die im Türcontroller vorkonfiguriert sind und bei denen Lesegerätfeedback und typische Feedbacksignale ausgelöst werden. Die Feedbacksignale für AXIS Reader sind in der mit dem AXIS Reader mitgelieferten Installationsanleitung aufgeführt.

Konfigurieren von Alarmen und Ereignissen

Ereignis	Wiegand Doppel-LED	Wiegand Einzel-LED	OSDP	Muster Signaltongeber	Status
Leerbetrieb[1]	Aus	Rot	Rot	Stumm	Normal
RequirePIN (PIN erforderlich)	Rot-grün blinkend	Rot-grün blinkend	Rot-grün blinkend	Zwei kurze Signaltöne	PIN erforderlich
AccessGranted (Zugang gewährt)	Grün	Grün	Grün	Signalton	Zugang gewährt
AccessDenied (Zugang verweigert)	Rot	Rot	Rot	Signalton	Zugang verweigert

1. Der Leerbetrieb setzt bei geschlossener Tür und verriegeltem Schloss ein.

Andere Feedbacksignale als die oben aufgeführten müssen von einem Client wie einem Zugangsverwaltungssystem über die VAPIX®-API (Application Programming Interface), die diese Funktion unterstützt, konfiguriert und mit Geräten verwendet werden, die die erforderlichen Signale bereitstellen können. Weitere Informationen finden Sie in den Benutzerinformationen, die vom Entwickler des Zugangsverwaltungssystems und dem Hersteller des Lesers zur Verfügung gestellt werden.

Berichte

Auf der Seite „Reports" (Berichte) können Sie Berichte mit unterschiedlichen Informationen über das System anzeigen, drucken und exportieren. Weitere Informationen zu den verfügbaren Berichten finden Sie unter *Berichtstypen auf Seite 54*.

Anzeigen, Drucken und Exportieren von Berichten

Klicken Sie zum Öffnen der Seite „Reports" (Berichte) auf **Reports (Berichte)**.

Klicken Sie zum Anzeigen eines Berichts auf **View and print (Anzeigen und drucken)**.

So drucken Sie einen Bericht:

1. Klicken Sie auf **View and print (Anzeigen und drucken)**.
2. Wählen Sie die Spalten aus, die Sie in den Bericht einschließen möchten. Standardmäßig sind alle Spalten ausgewählt.
3. Wenn Sie den Bereich des Berichts eingrenzen möchten, geben Sie im entsprechenden Filterfeld einen Filter ein. Sie können z. B. Benutzer nach Gruppenzugehörigkeit, Türen nach Zeitplan oder Gruppen nach Türen, zu denen sie Zugang haben, filtern.

   Um exakte Übereinstimmungen zu ermitteln, den Filtertext in doppelte Anführungszeichen setzen. Beispiel: "John".
4. Wenn die Berichtselemente in anderer Reihenfolge angezeigt werden sollen, in der entsprechenden Spalte anklicken. Wechseln Sie mithilfe der Sortierschaltflächen zwischen Standard- und umgekehrter Reihenfolge.

   Zeigt die Elemente in der Standardreihenfolge (aufsteigend) an.

   Zeigt die Elemente in umgekehrter Reihenfolge (absteigend) an.
5. **Print selected columns (Ausgewählte Spalten drucken)** anklicken.

Zum Exportieren eines Berichts **Export CSV file (CSV-Datei exportieren)** anklicken.

Der Bericht wird als Datei mit trennzeichengetrennten Werten (CSV) exportiert und enthält alle Spalten und Elemente des jeweiligen Berichttyps. Wenn nicht anders angegeben, wird die Exportdatei (CSV) in den Standardordner für heruntergeladene Dateien heruntergeladen. Alternativ kann in den Benutzereinstellungen des Webbrowsers ein anderer Ordner festgelegt werden.

Hinweis

In Berichten werden nur Benutzer mit Zugangsdaten ausgewiesen.

Berichtstypen

Es stehen folgende Berichtstypen zur Verfügung:

- Zugangszeitpläne. Weitere Informationen zu Arten von Zugangszeitplänen und zugehörigen Optionen finden Sie unter *Seite 32* und *Seite 33*.
- Gruppen. Weitere Informationen zu Gruppen finden Sie unter *Seite 34*.
- Türen. Weitere Informationen zu Türen und Identifikationstypen finden Sie unter *Seite 35* und *Seite 36*.
- Benutzer. Weitere Informationen zu Benutzerzugangsdaten finden Sie unter *Seite 41*.
- Tür-Controller. Weitere Informationen über verbundene Controller und deren ID-Typen finden Sie unter *Seite 27*. Weitere Informationen über Zeitoptionen für Türmonitore finden Sie unter *Seite 16*.

Systemoptionen

Sicherheit

Benutzer

Die Benutzerzugangskontrolle ist in der Standardeinstellung aktiviert und kann unter **Setup > Additional Controller Configuration > System Options > Security > Users (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Sicherheit > Benutzer)** konfiguriert werden. Administratoren können weitere Benutzer einrichten, indem sie diesen Benutzernamen und Kennwörter zuweisen.

In der Benutzerliste werden autorisierte Benutzer und Benutzergruppen (Zugangsstufen) angezeigt:

- **Administratoren** haben unbeschränkten Zugang zu allen Einstellungen. Administratoren können Benutzer hinzufügen, bearbeiten und entfernen.

Hinweis

Bei Wahl der Option **Encrypted & unencrypted (Verschlüsselt und unverschlüsselt** verschlüsselt der Webserver das Kennwort. Die Option Verschlüsselt ist die Standardeinstellung für neue und für auf die Werkseinstellungen zurückgesetzte Einheiten.

Unter **HTTP/RTSP Password Settings (HTTP/RTSP-Kennworteinstellungen)** den zulässigen Kennworttyp wählen. Möglicherweise müssen nicht verschlüsselte Kennwörter zugelassen werden, wenn Anzeigeclients Verschlüsselung nicht unterstützen oder wenn die Firmware aktualisiert wurde und vorhandene Clients zwar Verschlüsselung unterstützen, sich jedoch neu anmelden und zur Verwendung dieser Funktion konfiguriert werden müssen.

ONVIF

ONVIF ist ein offenes Branchenforum, das standardisierte Schnittstellen für effektive Kompatibilität von IP-basierten physischen Sicherheitsprodukten anbietet und fördert.

Beim Erstellen eines Benutzers wird automatisch ONVIF-Kommunikation aktiviert. Verwenden Sie den Benutzernamen und das Kennwort für sämtliche ONVIF-Kommunikation mit dem Produkt. Weitere Informationen finden Sie unter *www.onvif.org*.

IP-Adressfilter

Das Filtern von IP-Adressen wird aktiviert über**Setup > Additional Controller Configuration > System Options > Security > IP Address Filter (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Sicherheit > Filter IP-Adresse)**. Nach der Aktivierung wird den aufgeführten IP-Adressen der Zugriff auf das Axis Produkt gewährt oder verweigert. Wählen Sie in der Liste **Allow (Zulassen)** oder **Deny (Verweigern)** aus, und klicken Sie auf **Apply (Übernehmen)**, um den IP-Adressfilter zu aktivieren.

Der Administrator kann der Liste bis zu 256 IP-Adresseinträge hinzufügen (ein einzelner Eintrag kann mehrere IP-Adressen enthalten).

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer oder HTTP over SSL) ist ein Internetprotokoll, das ein verschlüsseltes Browsen ermöglicht. Mit HTTPS können Benutzer und Clients zudem prüfen, ob auf das richtige Gerät zugegriffen wird. Die von HTTPS gebotene Sicherheitsstufe wird für den Großteil des gewerblichen Datenaustauschs als angemessen betrachtet.

Das Axis Produkt kann so konfiguriert werden, dass für die Anmeldung von Administratoren HTTPS vorausgesetzt wird.

Um HTTPS verwenden zu können, muss zunächst ein HTTPS-Zertifikat installiert werden. Um Zertifikate zu installieren und zu verwalten, diesen Optionspfad aufrufen: **Setup > Additional Controller Configuration > System Options > Security > Certificates (Setup> Zusätzliche Controllerkonfiguration > Systemoptionen > Sicherheit > Sicherheitszertifikate** Siehe *Zertifikate auf Seite 56*.

So aktivieren Sie HTTPS auf dem Axis Produkt:

1. Wechseln Sie zu **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Setup > Zusätzliche Controller-Konfiguration > Systemoptionen > Sicherheit > HTTPS)**
2. Wählen Sie aus der Liste der installierten Zertifikate ein HTTPS-Zertifikat aus.

3. Klicken Sie optional auf **Ciphers (Verschlüsselungen)** und wählen Sie die Verschlüsselungsalgorithmen für SSL aus.
4. Die **HTTPS Connection Policy (HTTPS-Verbindungsrichtlinie)** erläutert die einzelnen Benutzergruppen.
5. Um die Einstellungen zu aktivieren, **Speichern** anklicken

Um über das gewünschte Protokoll auf das Axis Produkt zuzugreifen, geben Sie im Adressfeld des Browsers `https://` für das HTTPS-Protokoll und `http://` für das HTTP-Protokoll ein.

Der HTTPS-Port kann auf der Seite **System Options > Network > TCP/IP > Advanced (Systemoptionen > Netzwerk > TCP/IP > Erweitert)** geändert werden.

IEEE 802.1X

IEEE 802.1X ist ein Standard für portbasierte Netzwerk-Zugriffskontrolle, die eine sichere Authentifizierung für drahtgebundene und drahtlose Netzwerk-Geräte bietet. IEEE 802.1X basiert auf EAP (Extensible Authentication Protocol).

Zum Zugriff auf ein mit IEEE 802.1X geschütztes Netzwerk müssen die Geräte authentifiziert sein. Die Authentifizierung erfolgt durch einen Authentifizierungsserver, üblicherweise ein **RADIUS-Server** wie z. B. FreeRADIUS mit Microsoft-Internetauthentifizierungsdienst.

Bei der Implementierung von Axis identifizieren sich das Axis Produkt und der Authentifizierungsserver mithilfe von digitalen Zertifikaten über EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). Die Zertifikate werden von einer **Zertifizierungsstelle** (CA, Certification Authority) bereitgestellt. Sie benötigen:

- ein CA-Zertifikat zur Authentifizierung der Identität des Authentifizierungsservers.
- ein CA-signiertes Clientzertifikat zum Authentifizieren des Axis Produkts.

Um Zertifikate zu installieren und zu verwalten, diesen Optionspfad aufrufen: **Setup > Additional Controller Configuration > System Options > Security > Certificates (Setup> Zusätzliche Controllerkonfiguration > Systemoptionen > Sicherheit > Sicherheitszertifikate** Siehe *Zertifikate auf Seite 56*.

Um den Zugriff des Produkts auf ein mit IEEE 802.1X geschütztes Netzwerk zu ermöglichen:

1. Wechseln Sie zu **Setup > Additional Controller Configuration (Zusätzliche Controller-Konfiguration) > System Options (Systemoptionen) > Security (Sicherheit) > IEEE 802.1X**.
2. Wählen Sie aus der Liste der installierten Zertifikate ein **CA-Zertifikat** und ein **Clientzertifikat** aus.
3. Unter **Settings (Einstellungen)** die EAPOL-Version aus und die EAP-Identität des Clientzertifikats angeben.
4. Das Wahlfeld von IEEE 802.1X aktivieren und **Save (Speichern)** anklicken.

Hinweis

Damit die Authentifizierung ordnungsgemäß funktioniert, sollten die Datums- und Uhrzeiteinstellungen des Axis Produkts mit einem NTP-Server synchronisiert werden. Siehe *Datum und Uhrzeit auf Seite 57*.

Zertifikate

Zertifikate werden in Netzwerken zum Authentifizieren von Geräten verwendet. Zu den typischen Anwendungen zählen das verschlüsselte Browsen im Internet (HTTPS), der Netzwerk-Schutz mit IEEE 802.1X sowie das Verschlüsseln von Benachrichtigungen z. B. per E-Mail. Für das Axis Produkt können zwei Zertifikattypen verwendet werden:

Server-/Clientzertifikate - Das Axis Produkt zertifizieren. Ein **Server/Client-Zertifikat** kann selbstsigniert oder von einer Zertifizierungsstelle (Certificate Authority, CA) ausgegeben worden sein. Ein selbstsigniertes Zertifikat bietet begrenzten Schutz und kann vor Erhalt eines CA-Zertifikats verwendet werden.

CA-Zertifikate - Zum Authentifizieren von Peer-Zertifikaten, z. B. des Zertifikats eines Authentifizierungsservers, wenn das Axis Produkt mit einem über IEEE 802.1X geschützten Netzwerk verbunden ist. Das Axis Produkt wird mit einigen vorinstallierten CA-Zertifikaten geliefert:

Hinweis

- Beim Zurücksetzen des Produkts auf die Werkseinstellungen werden alle Zertifikate mit Ausnahme der vorinstallierten CA-Zertifikate gelöscht.
- Beim Zurücksetzen des Produkts auf die Werkseinstellungen werden alle vorinstallierten CA-Zertifikate, die gelöscht wurden, neu installiert.

Selbstsignierte Zertifikate erstellen

1. Um selbstsignierte Zertifikate zu installieren und zu verwalten, diesen Optionspfad aufrufen: **Setup > Additional Controller Configuration > System Options > Security > Certificates (Setup> Zusätzliche Controllerkonfiguration > Systemoptionen > Sicherheit > Sicherheitszertifikate**
2. Um die erforderlichen Informationen anzugeben, **Create self-signed certificate (Selbstsigniertes Zertifikat erstellen)** anklicken.

Ein CA-signiertes Zertifikat erstellen

1. Zum Erstellen selbstsignierter Zertifikate, siehe .
2. Um weitere Zertifikate zu installieren und zu verwalten, diesen Optionspfad aufrufen: **Setup > Additional Controller Configuration > System Options > Security > Certificates (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Sicherheit > Sicherheitszertifikate)**.
3. Klicken Sie auf die Schaltfläche **Create certificate signing request (Anforderung für Zertifikatsignierung erstellen)**, um die erforderlichen Informationen anzugeben.
4. Kopieren Sie die PEM-formatierte Anforderung und senden Sie sie an die Zertifizierungsstelle Ihrer Wahl.
5. Nachdem das signierte Zertifikat zugestellt ist, **Install certificate (Zertifikat installieren)** anklicken und das Zertifikat hochladen.

Weitere CA-Zertifikate installieren

1. Um weitere Zertifikate zu installieren und zu verwalten, diesen Optionspfad aufrufen: **Setup > Additional Controller Configuration > System Options > Security > Certificates (Setup> Zusätzliche Controllerkonfiguration > Systemoptionen > Sicherheit > Sicherheitszertifikate**
2. Klicken Sie auf **Install certificate (Zertifikat installieren)** und laden Sie das Zertifikat hoch.

Datum und Uhrzeit

Die Datums- und Uhrzeiteinstellungen des Axis Produkts werden unter **Setup > Additional Controller Configuration > System Options > Date & Time (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Datum und Uhrzeit)** konfiguriert.

Current Server Time (Aktuelle Server-Zeit) zeigt das aktuelle Datum und die aktuelle Uhrzeit an (24-Stunden-Uhr).

Um die Datums- und Uhrzeiteinstellungen zu ändern, wählen Sie unter **New Server Time (Neue Server-Zeit)** den gewünschten **Time mode (Zeitmodus)** aus:

- **Synchronize with computer time (Mit Computerzeit synchronisieren)** – Datum und Uhrzeit werden anhand der Uhr des Computers eingestellt. Mit dieser Option werden Datum und Uhrzeit einmal eingestellt und nicht automatisch aktualisiert.
- **Synchronize with NTP Server (Mit NTP-Server synchronisieren)** – Datum und Uhrzeit werden von einem NTP-Server abgerufen. Mit dieser Option werden Datum und Uhrzeit regelmäßig aktualisiert. Weitere Informationen zu NTP-Einstellungen finden Sie unter *NTP-Konfiguration auf Seite 60*.

  Wenn für den NTP-Server ein Host-Name verwendet wird, muss ein DNS-Server konfiguriert werden. Siehe *DNS-Konfiguration auf Seite 60*.
- **Set manually (Manuell einstellen)** – Ermöglicht die manuelle Einstellung von Datum und Uhrzeit.

Wenn ein NTP-Server verwendet wird, wählen Sie in der Dropdown-Liste Ihre **Time zone (Zeitzone)** aus. Aktivieren Sie bei Bedarf das Kontrollkästchen **Automatically adjust for daylight saving time changes (Bei Zeitumstellung automatisch anpassen)**.

Netzwerk

Grundlegende TCP/IP-Einstellungen

Das Axis Produkt unterstützt IPv4.

Das Axis Produkt kann eine IPv4-Adresse auf folgende Arten beziehen:

- **Dynamic IP address (Dynamische IP-Adresse) – Obtain IP address via DHCP (IP-Adresse über DHCP beziehen)**. Dies ist die Standardeinstellung. Das Axis Produkt erhält seine IP-Adresse automatisch per DHCP (Dynamic Host Configuration Protocol).

  Mithilfe von DHCP können Netzwerkadministratoren das Zuweisen von IP-Adressen zentral verwalten und automatisieren.

- **Static IP address (Statische IP-Adresse)** – Um eine statische IP-Adresse zu verwenden, **Use the following IP address (Folgende IP-Adresse verwenden)** wählen und die IP-Adresse, die Subnetzmaske und den Standardrouter angeben. Klicken Sie anschließend auf **Save (Speichern)**.

DHCP sollte nur aktiviert werden, wenn dynamische IP-Adressbenachrichtigungen verwendet werden oder DHCP einen DNS-Server aktualisieren kann und es so möglich ist, anhand des Namens (Host-Namens) auf das Axis Produkt zuzugreifen.

Wenn DHCP aktiviert ist, auf das Produkt jedoch nicht zugegriffen werden kann, führen Sie AXIS IP Utility aus, um im Netzwerk nach verbundenen Axis Produkten zu suchen, oder setzen Sie das Produkt auf die werksseitigen Standardeinstellungen zurück, und führen Sie die Installation anschließend erneut durch. Informationen zum Wiederherstellen der werksseitigen Standardeinstellung finden Sie unter *Seite 65*.

ARP/Ping

Die IP-Adresse des Produkts kann mit ARP und Ping zugewiesen werden. Anweisungen finden Sie unter *Zuweisen einer IP-Adresse mit ARP/Ping auf Seite 58*.

Der ARP/Ping-Dienst ist in der Standardeinstellung aktiviert, wird jedoch zwei Minuten nach dem Start des Produkts oder unmittelbar nach dem Zuweisen einer IP-Adresse automatisch deaktiviert. Um erneut eine IP-Adresse mit ARP/Ping zuzuweisen, muss das Produkt neu gestartet werden, damit ARP/Ping weitere zwei Minuten lang aktiviert wird.

Um den Dienst zu deaktivieren, diesen Optionspfad aufrufen: **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Setup Zusätzliche Controllerkonfiguration > Systemoptionen > Netzwerk >TCP/IP > Grundlegend)**. Anschließend die Option **Enable ARP/Ping setting of IP address (Einstellen der IP-Adresse mit ARP/Ping) löschen**.

Das Produkt kann auch gepingt werden, wenn der Dienst deaktiviert ist.

Zuweisen einer IP-Adresse mit ARP/Ping

Die IP-Adresse des Geräts kann mit ARP/Ping zugewiesen werden. Der Befehl muss innerhalb von zwei Minuten nach Anschließen an die Stromversorgung erteilt werden.

1. Eine nicht zugewiesene statische IP-Adresse im selben Netzwerk-Segment wählen, in dem sich der Computer befindet.
2. Die Seriennummer (S/N) auf dem Produktaufkleber ermitteln.
3. Die Eingabeaufforderung öffnen und die folgenden Befehle eingeben:

   Linux/Unix-Syntax

   ```
   arp -s <IP-Adresse> <Seriennummer> temp
   ping -s 408 <IP-Adresse>
   ```

   Linux/Unix-Beispiel

```
arp -s 192.168.0.125 00:40:8c:18:10:00 temp
ping -s 408 192.168.0.125
```

Windows-Syntax (Dazu müssen Sie die Eingabeaufforderung möglicherweise als Administrator ausführen.)

```
arp -s <IP-Adresse> <Seriennummer>
ping -l 408 -t <IP-Adresse>
```

Windows-Beispiel (Dazu müssen Sie die Eingabeaufforderung möglicherweise als Administrator ausführen.)

```
arp -s 192.168.0.125 00-40-8c-18-10-00
ping -l 408 -t 192.168.0.125
```

4. Das Produkt neu starten. Dazu die Stromversorgung der Netzwerk-Verbindung (PoE) unterbrechen und wiederherstellen.
5. Die Eingabeaufforderung schließen, wenn das Gerät mit `Reply from 192.168.0.125:...` oder einer ähnlichen Meldung antwortet.
6. Einen Browser öffnen und `http://<IP-Adresse>` in die Adresszeile eingeben.

Weitere Methoden zum Zuweisen der IP-Adresse, siehe das Dokument *Zuweisen einer IP-Adresse und Zugreifen auf das Gerät* unter *www.axis.com/support*

Hinweis

- Um eine Eingabeaufforderung in Windows zu öffnen, das **Start**-Menü öffnen und nach `cmd` suchen.
- Zum Verwenden des Befehls ARP unter Windows 8/Windows 7/Windows Vista mit der rechten Maustaste das Befehlszeilensymbol anklicken und **Als Administrator ausführen** wählen.
- Um eine Eingabeaufforderung in Mac OS X zu öffnen, rufen Sie das **Dienstprogramm „Terminal"** unter **Application > Utilities (Programme > Dienstprogramme)** auf.

AXIS Video Hosting System (AVHS)

AVHS bietet in Verbindung mit einem AVHS-Dienst einfachen und sicheren Internetzugang zu Controller-Verwaltung und Protokollen von jedem Standort aus. Weitere Informationen und Unterstützung beim Suchen eines lokalen AVHS-Dienstanbieters finden Sie unter „www.axis.com/hosting".

Die AVHS-Einstellungen werden konfiguriert unter: **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Weitere Controllerkonfigurierung > Systemoptionen > Netzwerk > TCP/IP > Grundlegende Einstellungen)** . Die Möglichkeit, eine Verbindung mit einem AVHS-Dienst herzustellen, ist in der Standardeinstellung aktiviert. Deaktivieren Sie das Kontrollkästchen **Enable AVHS (AVHS aktivieren)**, um die Funktion zu deaktivieren.

One-click enabled (One-Click aktiviert) – Halten Sie die Steuertaste des Produkts (siehe *Produktübersicht auf Seite 3*) ca. 3 Sekunden lang gedrückt, um über das Internet eine Verbindung mit einem AVHS-Dienst herzustellen. Nach der Registrierung wird **Always (Immer)** aktiviert und das Axis Produkt bleibt mit dem AVHS-Dienst verbunden. Wenn das Produkt nicht innerhalb von 24 Stunden nach Drücken der Steuertaste registriert wird, trennt das Produkt die Verbindung mit dem AVHS-Dienst.

Always (Immer) – Das Axis Produkt wird ständig versuchen, über das Internet eine Verbindung mit dem AVHS-Dienst herzustellen. Nach der Registrierung bleibt das Produkt mit dem Dienst verbunden. Diese Option kann verwendet werden, wenn das Produkt bereits installiert und die One-Click-Installation unpraktisch oder nicht möglich ist.

Hinweis

Der AVHS-Support hängt von der Verfügbarkeit von Abonnements von Diensteanbietern ab.

AXIS Internet Dynamic DNS Service

Mit dem AXIS Internet Dynamic DNS Service wird ein Host-Name für den einfachen Zugriff auf das Produkt zugewiesen. Weitere Informationen finden Sie unter *www.axiscam.net*.

Das Axis Produkt bei AXIS Internet Dynamic DNS Service wie folgt registrieren unter: **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic Setup > Zusätzliche Controllereinstellungen >Systemoptionen > Netzwerk > TCP/IP > Einfach)**. Unter**Services (Dienste)** die Schaltfläche **Settings (Einstellungen)** für AXIS Internet Dynamic DNS Service

(erfordert Internetzugang) anklicken. Der aktuell bei AXIS Internet Dynamic DNS-Service für das Produkt registrierte Domänenname kann jederzeit entfernt werden.

Hinweis

AXIS Internet Dynamic DNS Service erfordert IPv4.

Erweiterte TCP/IP-Einstellungen

DNS-Konfiguration

DNS (Domain Name Service) übersetzt Host-Namen in IP-Adressen. Die DNS-Einstellungen werden konfiguriert unter: **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Weitere Controller-Konfigurierung > Systemoptionen > Netzwerk > TCP/IP > Erweiterte Einstellungen)** .

Wählen Sie **Obtain DNS server address via DHCP (DNS-Server-Adresse über DHCP abrufen)** aus, um die vom DHCP-Server bereitgestellten DNS-Einstellungen zu verwenden.

Zum Vornehmen manueller Einstellungen wählen Sie **Use the following DNS server address (Folgende DNS-Server-Adresse verwenden)** aus und geben Sie Folgendes an:

Domain name (Domänenname) - Geben Sie die Domäne(n) an, in der nach dem vom Axis Produkt verwendeten Host-Namen gesucht wird. Mehrere Domänen können durch Strichpunkte getrennt angegeben werden. Der Host-Name ist stets der erste Teil eines vollständig angegebenen Domänennamens (FQDN, Fully Qualified Domain Name). `myserver` ist beispielsweise der Host-Name im vollständig angegebenen Domänennamen `myserver.mycompany.com`, wobei `mycompany.com` der Domänenname ist.

Primary/Secondary DNS server (Primärer/sekundärer DNS-Server) - Geben Sie die IP-Adressen des primären/sekundären DNS-Servers an. Der sekundäre DNS-Server ist optional und wird verwendet, wenn der primäre DNS-Server nicht verfügbar ist.

NTP-Konfiguration

NTP (Network Time Protocol) wird zum Synchronisieren der Uhrzeiten von Geräten in einem Netzwerk verwendet. Die NTP-Einstellungen werden konfiguriert unter: **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Weitere Controller-Konfigurierung > Systemoptionen > Netzwerk > TCP/IP > Erweiterte Einstellungen)** .

Wählen Sie **Obtain NTP server address via DHCP (NTP-Server-Adresse über DHCP abrufen)** aus, um die vom DHCP-Server bereitgestellten DNS-Einstellungen zu verwenden.

Zum Vornehmen manueller Einstellungen wählen Sie **Use the following NTP server address (Folgende NTP-Server-Adresse verwenden)** aus und geben Sie den Host-Namen oder die IP-Adresse des NTP-Servers ein.

Host-Namen-Konfiguration

Auf das Axis Produkt kann mithilfe eines Host-Namens anstelle einer IP-Adresse zugegriffen werden. Der Hostname entspricht in der Regel dem zugewiesenen DNS-Namen. Der Hostname wird unter **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Weitere Controller-Konfigurierung > Systemoptionen > Netzwerk > TCP/IP > Erweiterte Einstellungen)** konfiguriert.

Wählen Sie **Obtain host name via IPv4 DHCP (Host-Namen über IPv4 DHCP abrufen)** aus, um den vom DHCP-Server mit IPv4 bereitgestellten Host-Namen zu verwenden.

Wählen Sie **Use the host name (Host-Namen verwenden)** aus, um den Host-Namen manuell festzulegen.

Wählen Sie **Enable dynamic DNS updates (Dynamische DNS-Aktualisierungen aktivieren)** aus, um lokale DNS-Server dynamisch zu aktualisieren, wenn die IP-Adresse des Axis Produkts geändert wird. Weitere Informationen finden Sie in der Onlinehilfe.

Verknüpfen einer lokalen IPv4-Adresse

Link-Local Address (Verknüpfen einer lokalen Adresse) ist in der Standardeinstellung aktiviert und weist dem Axis Produkt eine zusätzliche IP-Adresse zu, über die von anderen Hosts im selben Segment des lokalen Netzwerks auf das Produkt zugegriffen werden kann. Dem Produkt kann eine verknüpfte lokale IP-Adresse und eine statische oder von DHCP zugewiesene IP-Adresse gleichzeitig zugewiesen sein.

Systemoptionen

Die Funktion kann deaktiviert werden über: **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Weitere Controller-Konfigurierung > Systemoptionen > Netzwerk > TCP/IP > Erweiterte Einstellungen)** .

HTTP

Der vom Axis Produkt verwendete HTTP-Port kann geändert werden über: **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Weitere Controller-Konfigurierung > Systemoptionen > Netzwerk > TCP/IP > Erweiterte Einstellungen)** . Neben der Standardeinstellung (80) kann jeder Port im Bereich von 1024 bis 65535 verwendet werden.

HTTPS

Der vom Axis Produkt verwendete HTTPS-Port kann unter **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Erweitert)** geändert werden. Neben der Standardeinstellung (443) kann jeder Port im Bereich zwischen 1024 und 65535 verwendet werden.

Zum Aktivieren von HTTPS aufrufen: **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Sicherheit > HTTPS)**. Weitere Informationen, siehe *HTTPS auf Seite 55*

NAT-Traversal (Port-Mapping) für IPv4

Mit einem Netzwerkrouter können Geräte in einem privaten Netzwerk (LAN) eine einzelne Internetverbindung gemeinsam nutzen. Dazu wird der Netzwerk-Verkehr vom privaten Netzwerk zur Außenwelt, also zum Internet, weitergeleitet. Die Sicherheit im privaten Netzwerk (LAN) wird dadurch erhöht, da die meisten Router so vorkonfiguriert sind, dass Zugriffsversuche auf das private Netzwerk (LAN) aus dem öffentlichen Netzwerk (Internet) unterbunden werden.

NAT-Traversal verwenden, wenn sich das Axis Produkt in einem Intranet (LAN) befindet und von der anderen Seite (WAN) eines NAT-Routers aus darauf zugegriffen werden soll. Wenn NAT-Traversal ordnungsgemäß konfiguriert ist, wird sämtlicher HTTP-Datenverkehr zu einem externen HTTP-Port des NAT-Routers zum Produkt weitergeleitet.

NAT Traversal Aktivierung wird konfiguriert über: **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Weitere Controller-Konfigurierung > Systemoptionen > Netzwerk > TCP/IP > Erweiterte Einstellungen)** .

Hinweis

- Damit NAT-Traversal funktioniert, muss es vom Router unterstützt werden. Der Router muss außerdem UPnP® unterstützen.
- In diesem Zusammenhang bezieht sich der Router auf ein Netzwerk-Routinggerät wie zum Beispiel NAT-Router, Netzwerkrouter, Internet Gateway, Breitbandrouter, Breitbandgerät oder Software wie zum Beispiel eine Firewall.

Enable/Disable (Aktivieren/Deaktivieren) – Wenn dies aktiviert ist, versucht das Axis Produkt Port-Mapping in einem NAT-Router des Netzwerks mithilfe von UPnPTM zu konfigurieren. Hinweis: UPnP must auf dem Produkt aktiviert sein (siehe **Setup > Additional Controller Configuration > System Options > Network > UPnP (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Netzwerk > UPnP)**).

Den manuell ausgewählten NAT-Router verwenden – Wählen Sie diese Option aus, um manuell einen NAT-Router auszuwählen, und geben Sie die IP-Adresse des Routers in das Feld ein. Wenn kein Router angegeben wird, sucht das Produkt automatisch nach NAT-Routern in Ihrem Netzwerk. Wenn mehr als ein Router gefunden wird, wird der Standardrouter ausgewählt.

Alternative HTTP port (Alternativer HTTP-Port) – Wählen Sie diese Option aus, um manuell einen externen HTTP-Port zu definieren. Geben Sie einen Port im Bereich von 1024 bis 65535. Wenn das Feld für den Port leer ist oder die Standardeinstellung (nämlich 0) enthält, wird bei Aktivierung von NAT-Traversal automatisch eine Portnummer ausgewählt.

Hinweis

- Ein alternativer HTTP-Port kann auch dann verwendet werden oder aktiv sein, wenn NAT-Traversal deaktiviert ist. Dies ist nützlich, wenn Ihr NAT-Router UPnP nicht unterstützt und Sie die Portweiterleitung manuell im NAT-Router konfigurieren müssen.
- Wenn Sie manuell einen Port eingeben, der bereits verwendet wird, wird automatisch ein freier Port ausgewählt.
- Wenn der Port automatisch ausgewählt wird, wird er in diesem Feld angezeigt. Um dies zu ändern, geben Sie eine andere Portnummer ein, und klicken Sie auf **Save (Speichern)**.

FTP

Der im Axis Produkt laufende FTP-Server ermöglicht das Hochladen von neuer Firmware, Benutzeranwendungen und anderem. Der FTP-Server kann deaktiviert werden über: **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Erweitert)..**

RTSP

Mithilfe des im Axis Produkt ausgeführten RTSP-Servers kann ein verbindender Client einen Ereignis-Videostream starten. Die RTSP-Portnummer kann unter **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Erweitert)** geändert werden. Der Standardport ist 554.

Hinweis

Ereignis-Videostreams sind nicht verfügbar, wenn der RTSP-Server deaktiviert ist.

SOCKS

SOCKS ist ein Netzwerk-Proxy-Protokoll. Das Axis Produkt kann zum Verwenden eines SOCKS-Servers konfiguriert werden, um Netzwerke auf der anderen Seite einer Firewall oder eines Proxy-Servers zu erreichen. Diese Funktion ist nützlich, wenn sich das Axis Produkt in einem lokalen Netzwerk hinter einer Firewall befindet und Benachrichtigungen, Hochladevorgänge, Alarme usw. an ein Ziel außerhalb des lokalen Netzwerks (beispielsweise das Internet) gesendet werden müssen.

SOCKS wird konfiguriert unter **Setup > Additional Controller Configuration > System Options > Network > SOCKS (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Netzwerk > SOCKS)**). Weitere Informationen finden Sie in der Onlinehilfe.

QoS (Quality of Service)

QoS (Quality of Service) garantiert eine bestimmte Stufe einer Ressource für ausgewählten Datenverkehr im Netzwerk. In einem Netzwerk mit QoS wird Netzwerkdatenverkehr priorisiert und eine bessere Verlässlichkeit des Netzwerks bereitgestellt, indem die Bandbreite kontrolliert wird, die von einer Anwendung genutzt werden kann.

Die QoS-Einstellungen werden unter **Setup > Additional Controller Configuration > System Options > Network > QoS (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > QoS)** konfiguriert. Mit DSCP-Werten (Differentiated Services Codepoint) kann das Axis Produkt Ereignis-/Alarm- sowie Verwaltungsdatenverkehr markieren.

SNMP

Simple Network Management Protocol (SNMP) ermöglicht die Remoteverwaltung von Netzwerk-Geräten. Eine SNMP-Community besteht aus einer Gruppe von Geräten und der Verwaltungsstation, die SNMP ausführt. Community-Namen werden zur Identifizierung von Gruppen verwendet.

Um SNMP für Axis Produkte zu konfigurieren, muss UPnP muss auf dem Produkt aktiviert sein (siehe die Seite **Setup > Additional Controller Configuration > System Options > Network > UPnP (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Netzwerk > UPnP)**).

Die zu verwendende SNMP-Version entsprechend der erforderlichen Sicherheitsstufe wählen.

Traps werden vom Axis Produkt zum Senden von Meldungen an ein Verwaltungssystem bei wichtigen Ereignissen und Statusänderungen verwendet. Aktivieren Sie das Kontrollkästchen **Enable traps (Traps aktivieren)** und geben Sie die IP-Adresse, an die die Trap-Meldung gesendet werden soll, sowie die **Trap community (Trap-Community)** an, die die Meldung erhalten soll.

Hinweis

Wenn HTTPS aktiviert ist, sollten SNMP v1 und SNMP v2c deaktiviert werden.

Traps for SNMP v1/v2 (Traps für SNMP v1/v2) werden vom Axis Produkt zum Senden von Meldungen an ein Verwaltungssystem bei wichtigen Ereignissen und Statusänderungen verwendet. Aktivieren Sie das Kontrollkästchen **Enable traps (Traps aktivieren)** und geben Sie die IP-Adresse, an die die Trap-Meldung gesendet werden soll, sowie die **Trap community (Trap-Community)** an, die die Meldung erhalten soll.

Es stehen folgende Traps zur Verfügung:

- Cold start (Kaltstart)
- Warm start (Warmstart)
- Link up (Verbindung hergestellt)
- Authentication failed (Authentifizierung fehlgeschlagen)

SNMP v3 bietet Verschlüsselung und sichere Kennwörter. Zur Verwendung von Traps mit SNMP v3 ist eine SNMP v3-Verwaltungsanwendung erforderlich.

Zur Verwendung von SNMP v3 muss HTTPS aktiviert werden, siehe *HTTPS auf Seite 55*. Um SNMP v3 zu aktivieren, aktivieren Sie das Kontrollkästchen und geben Sie das anfängliche Benutzerkennwort an.

Hinweis

Das anfängliche Kennwort kann nur einmal festgelegt werden. Wenn das Kennwort verloren ist, muss das Axis Produkt auf die werksseitige Standardeinstellung zurückgesetzt werden, siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 65*.

UPnP

Das Axis Produkt unterstützt UPnP™®. UPnP ist in der Standardeinstellung aktiviert und das Produkt wird automatisch von Betriebssystemen und Clients erkannt, die dieses Protokoll unterstützen.

Hinweis: UPnP kann auf dem Produkt deaktiviert werden (siehe **Setup > Additional Controller Configuration > System Options > Network > UPnP (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Netzwerk > UPnP)**).

Bonjour

Das Axis Produkt unterstützt Bonjour. Bonjour ist in der Standardeinstellung aktiviert und das Produkt wird automatisch von Betriebssystemen und Clients erkannt, die dieses Protokoll unterstützen.

Bonjour kann deaktiviert werden unter **Setup > Additional Controller Configuration > System Options > Network > Bonjour (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Netzwerk > Bonjour)**.

Ports und Geräte

E/A-Ports

Der Zusatzanschluss des Axis Produkts bietet zwei konfigurierbare Ein- und Ausgangs-Ports für den Anschluss von externen Geräten. Informationen zum Anschließen von externen Geräten finden Sie in der Installationsanleitung auf *www.axis.com*

Die E/A-Ports werden konfiguriert unter **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Setup > Zusätzliche Controllerkonfiguration > Systemeinstellungen > Ports und Geräte > E/A-Ports)**. Wählen Sie die Richtung des Ports (**Eingang** oder **Ausgang**) aus. Die Ports können mit beschreibenden Namen versehen werden, und ihre **Normal states (Normalzustände)** können als **Open circuit (Offener Kreis)** oder **Grounded circuit (Geerdeter Kreis)** konfiguriert werden.

Port-Status

In der Liste auf der Seite **System Options > Ports & Devices > Port Status (Systemoptionen > Ports und Geräte > Portstatus)** wird der Status der Eingangsports und Ausgangsports des Produkts angezeigt.

Wartung

Das Axis Produkt bietet verschiedene Wartungsfunktionen. Diese stehen bereit unter **Setup > Additional Controller Configuration > System Options > Maintenance (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Wartung)**.

Wenn das Axis Produkt nicht erwartungsgemäß funktioniert, **Restart (Neu starten)** anklicken, um einen korrekten Neustart durchzuführen. Dies beeinträchtigt die aktuellen Einstellungen nicht.

Hinweis

Bei einem Neustart werden alle Einträge im Server-Bericht gelöscht.

Klicken Sie auf **Restore (Wiederherstellen)**, um die meisten Einstellungen auf die werksseitigen Standardwerte zurückzusetzen. Die folgenden Einstellungen werden nicht geändert:

- Boot-Protokoll (DHCP oder statisch)
- statische IP-Adresse
- Standardrouter
- Subnetzmaske
- Systemzeit
- Einstellungen für IEEE 802.1X

Default (Standard) anklicken, um alle Einstellungen einschließlich der IP-Adresse auf die Werkseinstellungen zurückzusetzen. Diese Schaltfläche sollte mit Vorsicht verwendet werden. Das Axis Produkt kann auch mit der Steuertaste auf die werksseitige Standardeinstellung zurückgesetzt werden, siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 65*.

Informationen zur Firmware-Aktualisierung finden Sie unter *Die Firmware aktualisieren auf Seite 67*.

Anwendungsdaten sichern

Setup > Create a backup (Setup > Sicherung erstellen) aufrufen, um eine Sicherung der Anwendungsdaten zu erstellen. Die gesicherten Daten umfassen Benutzer, Zugangsdaten, Gruppen und Zeitpläne. Wenn Sie eine Sicherung erstellen, wird eine Datei mit den Daten lokal auf Ihrem Computer gespeichert.

Setup > Upload a backup (Setup > Sicherung hochladen) aufrufen, um anhand einer zuvor erstellten Sicherungsdatei die Anwendungsdaten wiederherzustellen. Bevor Sie die Sicherungsdatei hochladen können, müssen Sie das Gerät auf die werksseitigen Standardeinstellungen zurücksetzen. Anweisungen finden Sie unter *Zurücksetzen auf die Werkseinstellungen auf Seite 65*.

Support

Support-Übersicht

Informationen zur Fehlersuche und Kontaktinformationen als technische Unterstützung aufrufen auf der Seite: **Setup > Additional Controller Configuration > System Options > Support > Support Overview (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Support > Support-Übersicht)**

Siehe auch *Fehlerbehebung auf Seite 67*.

Systemübersicht

Setup > Additional Controller Configuration > System Options > Support > System Overview (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Support > Systemübersicht) aufrufen, um eine Übersicht über den Status und die Einstellungen des Axis Produkts zu erhalten. Hier finden Sie Informationen zur Firmwareversion, zur IP-Adresse, zu Netzwerk- und Sicherheitseinstellungen, zu Ereigniseinstellungen und zu aktuellen Protokolleinträgen.

Protokolle und Berichte

Über die Seiten **Setup > Zusätzliche Controllerkonfiguration > Systemeinstellungen > Unterstützung > Protokolle und Berichte** werden Protokolle und Berichte zur Systemanalyse und Problembehandlung erstellt. Bei Anfragen an den Axis Support, stets den Server-Bericht beifügen.

Systemprotokoll – Enthält Informationen zu Systemereignissen.

Zugriffsprotokoll – Enthält alle fehlgeschlagenen Versuche, auf das Produkt zuzugreifen. Das Zugriffsprotokoll kann auch zum Auflisten aller Verbindungen mit dem Produkt konfiguriert werden (siehe unten).

Server-Bericht anzeigen – Stellt Informationen zum Produktstatus in einem Popup-Fenster bereit. Das Zugriffsprotokoll wird dem Server-Bericht automatisch angefügt.

Server-Bericht herunterladen – Erstellt eine .zip-Datei, die einen vollständigen Server-Bericht als Textdatei im UTF-8-Format enthält. Die Option **Schnappschuss aus Live-Ansicht anfügen** wählen, um einen Schnappschuss aus der Live-Ansicht des Produkts anzufügen. Die .zip-Datei bei Supportanfragen immer beifügen.

Parameter List (Parameterliste) – Zeigt die Parameter des Produkts und deren aktuelle Einstellungen an. Dies kann bei der Fehlersuche oder der Kontaktaufnahme mit Axis Support nützlich sein.

Connection List (Verbindungsliste) – Führt alle Clients auf, die aktuell auf Medienströme zugreifen.

Crash Report (Absturzbericht) – Generiert ein Archiv mit Debugging-Informationen. Das Erstellen des Berichts nimmt einige Minuten in Anspruch.

Die Protokollstufen für die System- und Zugriffsprotokolle werden unter **Setup > Zusätzliche Controllerkonfiguration > Systemeinstellungen > Unterstützung > Protokolle und Berichte > Konfiguration** eingestellt. Das Zugriffsprotokoll kann zum Auflisten aller Verbindungen mit dem Produkt konfiguriert werden („Wichtiges, Warnungen und Informationen" wählen).

Erweitert

Skripterstellung

Mithilfe von Skripterstellung können erfahrene Benutzer eigene Skripte anpassen und verwenden.

HINWEIS

Eine unsachgemäße Verwendung kann zu unerwartetem Verhalten und zum Verlust des Kontakts mit dem Axis Produkt führen.

Axis empfiehlt, diese Funktion nur dann zu nutzen, wenn Sie die Konsequenzen abschätzen können. Axis Support bietet keine Unterstützung bei Problemen mit benutzerdefinierten Skripten.

Den Scripteditor öffnen über **Setup > Additional Controller Configuration > System Options > Advanced > Scripting (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Erweitert > Scripterstellung)**. Wenn ein Skript Probleme verursacht, das Produkt auf die Werkseinstellungen zurücksetzen, siehe *Seite 65*.

Weitere Informationen finden Sie unter *www.axis.com/developer*.

Datei-Upload

Dateien wie Webseiten und Bilder können zum Axis Produkt hochgeladen und als benutzerdefinierte Einstellungen verwendet werden. Zum Hochladen von Dateien diesen Optionspfad aufrufen: **Setup > Additional Controller Configuration > System Options > Advanced > File Upload (Setup > Zusätzliche Gerätekonfiguration >Systemoptionen > Erweitert > Hochladen von Dateien)**.

Auf hochgeladene Dateien wird über `http://<IP-Adresse>/local/<Benutzer>/<Dateiname>` zugegriffen, wobei `<Benutzer>` für die gewählte Benutzergruppe (Administrator) der hochgeladene Datei steht.

Zurücksetzen auf die Werkseinstellungen

Wichtig

Das Zurücksetzen auf die Werkseinstellungen sollte mit Vorsicht erfolgen. Beim Zurücksetzen auf die Werkseinstellungen werden alle Einstellungen einschließlich der IP-Adresse zurückgesetzt.

So wird das Produkt auf die werksseitigen Standardeinstellungen zurückgesetzt:

1. Trennen Sie das Produkt von der Stromversorgung.

2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht auf Seite 3*.
3. Halten Sie die Steuertaste 25 Sekunden gedrückt, bis die Status-LED zum zweiten Mal gelb leuchtet.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die Status-LED grün leuchtet. Das Produkt wurde auf die Werkseinstellungen zurückgesetzt. Wenn im Netzwerk kein DHCP-Server verfügbar ist, lautet die Standard-IP-Adresse `192.168.0.90`.
5. Mithilfe der Softwaretools für das Installieren und Verwalten, IP-Adressen zuweisen, das Kennwort festlegen und auf das Produkt zugreifen.

Die Parameter können auch über die Weboberfläche auf die Werkseinstellungen zurückgesetzt werden. Den folgenden Optionspfad aufrufen: **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Setup > Zusätzliche Controllerkonfiguration > Setup > Systemoptionen > Wartung)** und dann die Option **Default (Standardeinstellung)** anklicken.

Fehlerbehebung

Die aktuelle Firmware überprüfen

Bei Firmware handelt es sich um Software, die die Funktionalität von Netzwerk-Geräten bereitstellt. Eine der ersten Maßnahmen bei der Fehlersuche sollte das Prüfen der aktuellen Firmware-Version sein. Die aktuelle Version enthält möglicherweise eine Verbesserung, die das Problem behebt.

Die aktuelle Firmwareversion des Axis Produkts wird auf der Übersichtsseite angezeigt.

Die Firmware aktualisieren

Wichtig

- Ihr Händler behält sich das Recht vor, die Kosten für Reparaturen aufgrund von fehlerhafter Aktualisierung durch den Benutzer in Rechnung zu stellen.
- Vorkonfigurierte und angepasste Einstellungen werden gespeichert, wenn die Firmware aktualisiert wird (vorausgesetzt die Funktionen sind mit der neuen Firmware verfügbar). Dies wird von Axis Communications AB jedoch nicht garantiert.
- Wird eine Vorgängerversion der Firmware installiert, muss das Produkt danach auf die Werkseinstellungen zurückgesetzt werden.

Hinweis

- Nach Abschluss des Aktualisierungsvorgangs wird das Produkt automatisch neu gestartet. Bei manuellem Neustart des Produkts nach der Aktualisierung stets 5 Minuten lang warten, selbst wenn anzunehmen ist, dass die Aktualisierung fehlgeschlagen ist.
- Im Zuge einer Firmwareaktualisierung wird die Datenbank mit den Daten der Benutzer, Gruppen, Anmeldedetails und anderen Informationen aktualisiert. Der erste Start danach kann deshalb einige Minuten dauern. Die erforderliche Zeit hängt von der Datenmenge ab.
- Beim Aktualisieren des Axis Produkts mit der aktuellen Firmware erhält dieses die neuesten verfügbaren Funktionen. Vor dem Aktualisieren der Firmware stets die entsprechenden Aktualisierungsanweisungen und Versionshinweise lesen.

Eigenständige Türcontroller:

1. Die aktuelle Version der Firmware steht unter *www.axis.com/support* zum kostenlosen Herunterladen bereit.
2. Auf den Webseiten des Produkts **Setup > Additional Controller Configuration > System Options > Maintenance (Setup > Zusätzliche Controllerkonfiguration > Systemeinstellungen > Wartung)** aufrufen.
3. Unter **Upgrade Server (Server aktualisieren)Choose file (Datei wählen)** anklicken und die Datei auf dem Computer ermitteln.
4. Wenn das Produkt nach der Aktualisierung automatisch auf Werkseinstellungen zurückgesetzt werden soll, das Kontrollkästchen **Standard** aktivieren.
5. **Aktualisieren** anklicken.
6. Das Aktualisieren und Neustarten des Produkts dauert etwa 5 Minuten. Anschließend den Cache des Browsers leeren.
7. Auf das Produkt zugreifen.

Türcontroller in einem System:

Um alle Türcontroller in einem System zu aktualisieren, können AXIS Device Manager oder AXIS Camera Station verwendet werden. Für weitere Informationen, siehe *www.axis.com*.

Wichtig

- Nicht die Option Sequenzielles Aktualisieren wählen.

Hinweis

- Alle Controller eines Systems müssen stets mit der selben Firmwareversion versehen sein.
- Mit der Option Parallel in AXIS Device Manager oder AXIS Camera Station alle Controller eines System gleichzeitig aktualisieren.

Notfall-Wiederherstellungsverfahren

Wenn die Stromversorgung oder die Netzwerk-Verbindung während der Aktualisierung unterbrochen wird, schlägt der Prozess fehl und das Produkt reagiert eventuell nicht mehr. Die fehlgeschlagene Aktualisierung wird mittels der rot blinkenden Statusanzeige angezeigt Befolgen Sie die unten angegebenen Schritte, um das Produkt wiederherzustellen. Die Seriennummer findet sich auf dem Produktaufkleber.

1. Geben Sie unter **UNIX/Linux** Folgendes in die Befehlszeile ein:

   ```
   arp -s <IP-Adresse> <Seriennummer> temp
   ping -l 408 <IP-Adresse>
   ```

   Geben Sie unter **Windows** Folgendes in die Befehlszeile/DOS-Eingabeaufforderung ein (dazu muss die Eingabeaufforderung möglicherweise als Administrator ausgeführt werden):

   ```
   arp -s <IP-Adresse> <Seriennummer>
   ping -l 408 -t <IP-Adresse>
   ```

2. Wenn das Produkt nicht innerhalb von 30 Sekunden reagiert, starten Sie das Gerät neu, und warten Sie auf eine Reaktion. Drücken Sie STRG+C, um den Ping zu beenden.
3. Öffnen Sie einen Browser, und geben Sie die IP-Adresse des Produkts ein. Wählen Sie auf der geöffneten Seite mit der Schaltfläche **Browse (Durchsuchen)** die zu verwendende Aktualisierungsdatei aus. **Load (Laden)** anklicken, um den Aktualisierungsprozess neu zu starten.
4. Nach Abschluss der Aktualisierung (1 bis 10 Minuten) wird das Produkt automatisch neu gestartet. Die Statusanzeige leuchtet dauerhaft grün.
5. Installieren Sie das Produkt mithilfe der Installationsanleitung neu.

Wenn das Produkt nach dem Notfall-Wiederherstellungsverfahren weiterhin nicht funktioniert, wenden Sie sich bitte unter *www.axis.com/support* an den Axis Support.

Symptome, mögliche Ursachen und Maßnahmen zur Behebung

Probleme beim Aktualisieren der Firmware	
Aktualisierung der Firmware fehlgeschlagen	Nach fehlgeschlagener Aktualisierung der Firmware lädt das Produkt erneut die Vorversion. Die Firmwaredatei überprüfen und erneut versuchen.

Probleme beim Einstellen der IP-Adresse	
Beim Verwenden von ARP/Ping	Die Installation erneut durchführen. Die IP-Adresse muss innerhalb von zwei Minuten nach Einschalten des Produkts eingestellt werden. Sicherstellen, dass die Ping-Länge auf 408 eingestellt ist. Die Anleitung dazu befindet sich auf der Produktseite auf *www.axis.com*.
Das Produkt befindet sich in einem anderen Subnetz	Wenn sich die IP-Adresse des Produkts und die IP-Adresse des zum Zugriff auf das Produkt verwendeten Computers in unterschiedlichen Subnetzen befinden, kann die IP-Adresse nicht eingestellt werden. Wenden Sie sich an Ihren Netzwerkadministrator, um eine IP-Adresse zu erhalten.

Fehlerbehebung

Die IP-Adresse wird von einem anderen Gerät verwendet	Trennen Sie das Axis Produkt vom Netzwerk. Führen Sie einen Ping-Befehl aus (geben Sie in einem Befehls-/DOS-Fenster `ping` und die IP-Adresse des Produkts ein): • Wenn Folgendes angezeigt wird: `Reply from <IP-Adresse>: bytes=32; time=10...` bedeutet dies, dass die IP-Adresse möglicherweise bereits von einem anderen Gerät im Netzwerk verwendet wird. Bitten Sie den Netzwerkadministrator um eine neue IP-Adresse, und installieren Sie das Produkt erneut. • Wenn Folgendes angezeigt wird: `Request timed out` bedeutet dies, dass die IP-Adresse mit dem Axis Produkt verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Produkt erneut.
Möglicher IP-Adressenkonflikt mit einem anderen Gerät im selben Subnetz.	Die statische IP-Adresse des Axis Produkts wird verwendet, bevor der DHCP-Server eine dynamische Adresse festlegt. Wenn daher ein anderes Gerät standardmäßig dieselbe statische IP-Adresse verwendet, treten beim Zugreifen auf das Produkt möglicherweise Probleme auf.

Vom Browser kein Zugriff auf das Produkt möglich

Anmelden nicht möglich	Bei aktiviertem HTTPS sicherstellen, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise muss `http` oder `https` manuell in die Adressleiste des Browsers eingegeben werden. Wenn das Kennwort für den Benutzer „root" vergessen wurde, muss das Produkt auf die werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 65*.
Die IP-Adresse wurde von DHCP geändert	Von einem DHCP-Server zugeteilte IP-Adressen sind dynamisch und können sich ändern. Wenn die IP-Adresse geändert wurde, das Produkt mit AXIS IP Utility oder AXIS Camera Management im Netzwerk zu ermitteln. Das Produkt anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde) ermitteln. Bei Bedarf kann eine statische IP-Adresse manuell zugewiesen werden. Für die Anleitung dazu, siehe das Dokument *Zuweisen einer IP-Adresse und Zugriff auf das Gerät* auf der Produktseite auf *axis.com*
Zertifikatfehler beim Verwenden von IEEE 802.1X	Damit die Authentifizierung durchgeführt werden kann, müssen die Einstellungen des Axis Produkts für Datum und Uhrzeit mit einem NTP-Server synchronisiert sein. Siehe *Datum und Uhrzeit auf Seite 57*.

Auf das Produkt kann lokal, nicht jedoch extern zugegriffen werden

Routerkonfiguration	Um den Router für das Zulassen eingehenden Datenverkehrs zum Axis Produkt zu konfigurieren, die Funktion NAT-Traversal aktivieren. Diese versucht, den Router automatisch für den Zugriff auf das Axis Produkt zu konfigurieren. Siehe *NAT-Traversal (Port-Mapping) für IPv4 auf Seite 61*. Der Router muss UPnP® unterstützen.
Schutz durch Firewall	Die Firewall zum Internet gemeinsam mit dem Netzwerkadministrator überprüfen.
Standardrouter erforderlich	Überprüfen, ob die Routereinstellungen unter **Setup > Network Settings (Setup > Netzwerkeinstellungen)** oder **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Basis)** konfiguriert werden müssen.

Die Anzeige-LEDs für Status und Netzwerk blinken mit hoher Frequenz rot

Hardwarefehler	Wenden Sie sich bitte an Ihren Axis Händler.

Das Produkt kann nicht gestartet werden

Das Produkt kann nicht gestartet werden	Wenn das Produkt nicht gestartet werden kann, das Netzwerk-Kabel angeschlossen halten und das Stromkabel erneut am Midspan anschließen.

Technische Daten

Anschlüsse

Für Informationen zur Lage der Anschlüsse siehe .

Für Anschlussschaltbilder und Informationen zur bei der Hardwarekonfiguration erstellten Belegungsübersicht der Pins, siehe *Anschlussschaltbilder auf Seite 74* und *Konfigurieren der Hardware auf Seite 13*.

Der folgende Abschnitt dokumentiert die technischen Daten der Anschlüsse.

Leser-Daten-Anschluss

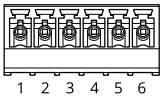
6-poliger Anschlussblock für die Kommunikation mit dem Leser (unterstützt RS485- und Wiegand-Protokoll).

Die RS485-Ports unterstützen:

- Zweiadrig RS485 Halbduplex
- RS-485 Vollduplex, vieradrig

Die Wiegand-Ports unterstützen:

- Wiegand, zweiadrig



Funktion		Kontakt	Hinweise
RS-485	A-	1	RS-485 für Vollduplex RS-485 für Halbduplex
	B+	2	
RS485	A-	3	RS-485 für Vollduplex RS-485 für Halbduplex
	B+	4	
Wiegand	D0 (Daten 0)	5	Für Wiegand
	D1 (Daten 1)	6	

Wichtig

Die RS-485-Ports besitzen eine feste Baudrate von 9600 Bit/s.

Wichtig

Die empfohlene maximale Kabellänge beträgt 30 m.

Wichtig

Die Ausgangsstromkreise dieses Abschnitts sind nach Klasse 2 leistungsbegrenzt.

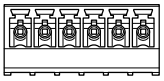
Leser-E/A-Anschluss

6-poliger Anschlussblock für:

- Zusatzstromversorgung (Gleichstromausgang)
- Digitaleingang

- Digitalausgang
- 0 V Gleichstrom (-)

Kontakt 3 an den Leser-E/A-Anschlüssen kann überwacht werden. Bei Unterbrechung der Verbindung wird ein Ereignis ausgelöst. Bringen Sie zur Verwendung überwachter Eingänge Abschlusswiderstände an. Beachten Sie das Anschlussschaltbild für überwachte Eingänge. Siehe *Seite 75*.



Funktion	Kontakt	Hinweise	Technische Daten
0 V Gleichstrom (-)	1		0 V Gleichstrom
Gleichstromausgang	2	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt darf nur für den Stromausgang verwendet werden.	12 V Gleichstrom Max. Stromstärke = 300 mA
Konfigurierbar (Ein- oder Ausgang)	3–6	Digitaleingang – Zum Aktivieren mit Kontakt 1 verbinden; zum Deaktivieren nicht anschließen.	0 bis max. 40 V Gleichstrom
		Digitalausgang – Zum Aktivieren mit Kontakt 1 verbinden; zum Deaktivieren nicht anschließen. Bei Verwendung mit einer induktiven Last, z. B. einem Relais, muss parallel zur Last zum Schutz vor Spannungsspitzen eine Diode zwischengeschaltet werden.	0 bis max. 40 V Gleichstrom, Open Drain, 100 mA

Wichtig

Die empfohlene maximale Kabellänge beträgt 30 m.

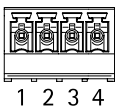
Wichtig

Bei den Ausgangsstromkreisen in diesem Abschnitt handelt es sich um Geräte der Klasse 2 mit begrenzter Leistung.

Türanschluss

Zwei 4-polige Anschlussblöcke für Türüberwachungsgeräte (Digitaleingang).

Alle Türeingangskontakte können überwacht werden. Bei Unterbrechung der Verbindung wird ein Alarm ausgelöst. Bringen Sie zur Verwendung überwachter Eingänge Abschlusswiderstände an. Das Anschlussschaltdiagramm für überwachte Eingänge beachten. Siehe *Seite 75*.



Funktion	Kontakt	Hinweise	Technische Daten
0 V Gleichstrom (-)	1, 3		0 V Gleichstrom
Eingang	2, 4	Zur Kommunikation der Türüberwachung. Digitaleingang – Zum Aktivieren mit Kontakt 1 bzw. 3 verbinden; zum Deaktivieren nicht anschließen. Hinweis: Dieser Kontakt kann nur für den Eingang verwendet werden.	0 bis max 40 V Gleichstrom

Wichtig

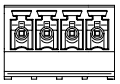
Die empfohlene maximale Kabellänge beträgt 30 m.

Zusatzanschluss

4-poliger konfigurierbarer E/A-Anschlussblock für:

- Zusatzstromversorgung (Gleichstromausgang)
- Digitaleingang
- Digitalausgang
- 0 V Gleichstrom (-)

Für einen Anschlussschaltplan, siehe *Anschlussschaltbilder auf Seite 74*.



Funktion	Kontakt	Hinweise	Technische Daten
0 V Gleichstrom (-)	1		0 V Gleichstrom
Gleichstromausgang	2	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt darf nur für den Stromausgang verwendet werden.	3,3 V Gleichstrom Max. Stromstärke = 100 mA
Konfigurierbar (Ein- oder Ausgang)	3–4	Digitaleingang – Zum Aktivieren mit Kontakt 1 verbinden; zum Deaktivieren nicht anschließen.	0 bis max. 40 V Gleichstrom
		Digitalausgang – Zum Aktivieren mit Kontakt 1 verbinden; zum Deaktivieren nicht anschließen. Bei Verwendung mit einer induktiven Last, z. B. einem Relais, muss parallel zur Last zum Schutz vor Spannungsspitzen eine Diode zwischengeschaltet werden.	0 bis max. 40 V Gleichstrom, Open Drain, 100 mA

Wichtig

Die empfohlene maximale Kabellänge beträgt 30 m.

Wichtig

Bei den Ausgangsstromkreisen in diesem Abschnitt handelt es sich um Geräte der Klasse 2 mit begrenzter Leistung.

Stromanschluss

2-poliger Anschlussblock für die Gleichstromversorgung. Eine mit den Anforderungen für Schutzkleinspannung (SELV) kompatible Stromquelle mit begrenzter Leistung (LPS) verwenden. Entweder mit einer Nennausgangsleistung von ≤100 W oder einem dauerhaft auf ≤5 A begrenzten Nennausgangsstrom.

Funktion	Kontakt	Hinweise	Technische Daten
0 V Gleichstrom (-)	1		0 V Gleichstrom
Gleichstromein-gang	2	Stromversorgung des Controllers ohne Power over Ethernet. Hinweis: Dieser Kontakt kann nur für den Stromeingang verwendet werden.	10–28 V Gleichstrom, max. 36 W Max. Stromstärke an Ausgängen = 14 W

Netzwerk-Anschluss

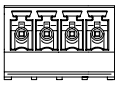
Ethernet-Anschluss RJ-45 Kabel der Kategorie 5e oder höher verwenden.

Funktion	Technische Daten
Stromversorgung und Ethernet	Power over Ethernet IEEE 802.3af/802.3at Typ 1 Klasse 3, 44 bis 57 V Gleichstrom Max. Last an Ausgängen = 7,5 W

Stromanschluss (Schloss)

Vierpoliger Anschlussblock für ein oder zwei Schlösser (Gleichstromausgang). Dieser Anschluss kann auch zur Stromversorgung externer Geräte verwendet werden.

Die Schlösser und andere Geräte gemäß dem während der Hardwarekonfiguration erstellten Kontaktbelegungsplan anschließen.



Funktion	Kontakt	Hinweise	Technische Daten
0 V Gleichstrom (-)	1, 3		0 V Gleichstrom
0 V Gleichstrom, frei oder 12 V Gleichstrom	2, 4	Zur Steuerung von bis zu zwei 12-V-Schlössern. Den Kontaktbelegungsplan der Hardware verwenden. Siehe *Konfigurieren der Hardware auf Seite 13*.	12 V Gleichstrom Max. Gesamtlast = 500 mA

HINWEIS

Wir empfehlen, nichtpolare Schlösser mit einer externen Schutzdiode auszustatten.

Wichtig

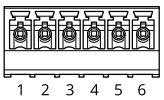
Bei den Ausgangsstromkreisen dieses Abschnitts handelt es sich um Geräte der Klasse 2 mit begrenzter Leistung.

Netz- und Relaisanschluss

Sechspoliger Anschlussblock mit integriertem Relais für:

- Externe Geräte
- Zusatzstromversorgung (Gleichstromausgang)
- 0 V Gleichstrom (-)

Die Schlösser und andere Geräte gemäß dem während der Hardwarekonfiguration erstellten Kontaktbelegungsplan anschließen.



Funktion	Kontakt	Hinweise	Technische Daten
0 V Gleichstrom (-)	1, 4		0 V Gleichstrom
Relais	2–3	Zum Anschluss von Relaisgeräten. Verwenden Sie das Pin Chart. Siehe *Konfigurieren der Hardware auf Seite 13*. Die beiden Relaisanschlüsse sind galvanisch von den anderen Schaltkreisen getrennt.	Max. Stromstärke = 700 mA Max. Spannung = +30 V Gleichstrom
12 V Gleichstrom	5	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt darf für den Stromausgang verwendet werden.	Max. Spannung = +12 V Gleichstrom Max. Stromstärke = 500 mA
24 V Gleichstrom	6	Nicht belegt	

HINWEIS

Wir empfehlen, nichtpolare Schlösser mit einer externen Schutzdiode auszustatten.

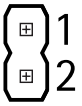
Wichtig

Bei den Ausgangsstromkreisen dieses Abschnitts handelt es sich um Geräte der Klasse 2 mit begrenzter Leistung.

Manipulationsalarm-Stiftleiste

Zwei 2-polige Leisten zur Überbrückung des:

- Hinteren Manipulationsalarms (TB)
- Manipulationsalarm (TF) vorn



Funktion	Kontakt	Hinweise
Hinterer Manipulationsalarm	1–2	Um den vorderen oder hinteren Manipulationsalarm zu überbrücken, Die Drahtbrücken zwischen TB 1, TB 2 beziehungsweise TF 1, TF 2 installieren. Bei einer Überbrückung des Manipulationsalarms erkennt das System keine Manipulationsversuche.
Vorderer Manipulationsalarm	1–2	

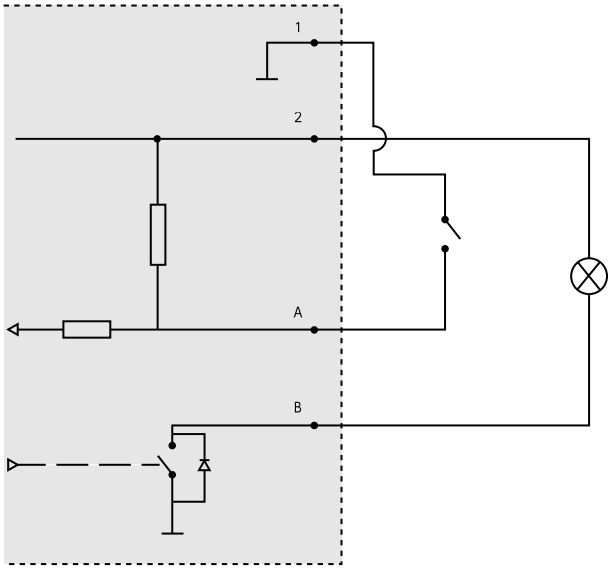
Hinweis

Der vordere und der hintere Manipulationsalarm sind standardmäßig aktiviert. Der Auslöser für die Öffnung des Gehäuses kann so konfiguriert werden, dass eine Aktion ausgeführt wird, wenn der Tür-Controller geöffnet bzw. von der Wand oder der Decke entfernt wird. Weitere Informationen zur Konfiguration von Alarmen und Ereignissen finden Sie im *Konfigurieren von Alarmen und Ereignissen auf Seite 45*.

Anschlussschaltbilder

Schließen Sie Geräte gemäß dem während der Hardwarekonfiguration erstellten Pin Chart an. Weitere Informationen zu Hardwarekonfiguration und Pin Chart finden Sie unter *Konfigurieren der Hardware auf Seite 13*.

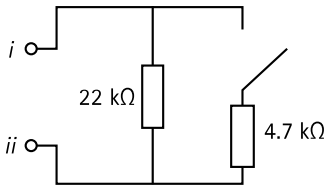
Zusatzanschluss



1 *0 V (-) Gleichstrom*
2 *Gleichstromausgang: 3,3 V, max. 100 mA*
A *E/A als Eingang konfiguriert*
B *E/A als Ausgang konfiguriert*

Überwachte Eingänge

Um überwachte Eingänge zu verwenden, die Abschlusswiderstände wie im Schaltbild unten dargestellt anschließen.



i *Eingang*
ii *0 V Gleichstrom (-)*

Hinweis

Es wird empfohlen, verdrillte und geschirmte Kabel zu verwenden. Die Abschirmung an 0 V Gleichstrom anschließen.

Sicherheitsinformationen

Gefährdungsstufen

⚠GEFAHR

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu Tod oder schweren Verletzungen führen kann.

⚠WARNUNG

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu Tod oder schweren Verletzungen führen kann.

⚠VORSICHT

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu geringfügiger oder mäßiger Verletzung führen kann.

HINWEIS

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu Sachschäden führen kann.

Andere Meldeebenen

Wichtig

Weist auf wichtige Informationen hin, die den richtigen Betrieb des Produkts gewährleisten.

Hinweis

Weist auf nützliche Informationen hin, die die optimale Verwendung des Produkts unterstützen.

Benutzerhandbuch
AXIS A1001 & AXIS Entry Manager

Vers. M25.2
Datum: Dezember 2023
Teil-Nr. T10010336