AXIS A1001 Network Door Controller & AXIS Entry Manager

Benutzerhandbuch

Über dieses Dokument

Dieses Handbuch ist für Administratoren und Benutzer des AXIS A1001bNetzwerk-Tür-Controllers vorgesehen und gilt für AXIS Entry Manager und Firmware 1.25 und höher. Es enthält Anweisungen zum Verwenden und Verwalten des Produkts im Netzwerk. Für die Verwendung dieses Produkts sind Erfahrungen mit Netzwerktechnologie von Vorteil. Kenntnisse zu UNIX- oder Linux-basierten Systemen kann zum Entwickeln von Shellskripts und Anwendungen ebenfalls nützlich sein. Spätere Versionen dieses Dokuments werden bei Bedarf auf der Axis Website veröffentlicht. Beachten Sie auch die über die webbasierte Schnittstelle verfügbare Online-Hilfe.

Der AXIS A1001 Netzwerk-Tür-Controller wird in diesem Handbuch bezeichnet als: das Axis Produkt, Produkt, Netzwerk-Tür-Controller und Tür-Controller.

Haftungsausschluss

Dieses Dokument wurde mit äußerster Sorgfalt erstellt. Informieren Sie bitte Ihre Axis Vertretung vor Ort über Ungenauigkeiten oder Auslassungen. Axis Communications AB übernimmt keinerlei Haftung für technische oder typographische Fehler und behält sich das Recht vor, jederzeit ohne vorherige Ankündigung Änderungen am Produkt und an den Handbüchern vorzunehmen. Axis Communications AB übernimmt keinerlei Garantie für den Inhalt dieses Dokuments. Dies gilt auch für die eingeschlossene Gewähr bezüglich der Handelsfähigkeit und Zweckdienlichkeit, ist aber nicht darauf beschränkt. Axis Communications AB ist nicht für direkte oder indirekte Folgeschäden haftbar oder verantwortlich, die in Verbindung mit der Ausstattung, der Leistung und dem Einsatz dieses Produkts entstehen. Dieses Produkt darf nur für seinen vorgesehenen Zweck verwendet werden.

Rechte zum Schutz des geistigen Eigentums

Axis AB besitzt Rechte zum Schutz des geistigen Eigentums an der Technologie des Produkts, welches in diesem Dokument beschriebenen ist. Insbesondere und ohne jedwede Einschränkung können diese Rechte zum Schutz des geistigen Eigentums eines oder mehrere der Patente enthalten, die unter *www.axis.com/patent.htm* aufgeführt sind, sowie eines oder mehrere weitere Patente oder Anwendungen, die in den USA oder anderen Ländern zum Patent angemeldet sind.

Dieses Produkt enthält den urheberrechtlich geschützten Quellcode von Apple Computer, Inc., unter den Bedingungen der Apple Public Source License 2.0 (siehe *www.opensource.apple.com/apsl*). Dieser Quellcode ist verfügbar unter *https://developer.apple.com/bonjour/*

Geräteänderungen

Dieses Gerät darf nur unter strikter Einhaltung der Anleitungen der Benutzerdokumentation installiert und verwendet werden.Dieses Gerät enthält keine vom Benutzer zu wartenden Komponenten.Nicht genehmigte Geräteänderungen oder Modifikationen setzen alle geltenden gesetzlichen Zertifikate und Zulassungen außer Kraft.

Marken

AXIS COMMUNICATIONS, AXIS, ETRAX, ARTPEC und VAPIX sind eingetragene Marken oder Markenanmeldungen der Axis AB in verschiedenen Rechtsordnungen. Alle weiteren Firmen- und Produktnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

Network Time Protocol Version 4 Distribution ist das urheberrechtliche Eigentum der University of Delaware – © University of Delaware 1992–2011. Der folgende Urheberrechtshinweis gilt für alle Dateien, die zusammengefasst als Network Time Protocol Version 4 Distribution bezeichnet werden. Wenn nicht ausdrücklich anderweitig in einer einzelnen Datei angegeben, gilt dieser Hinweis so, als ob der Text explizit in die Datei eingeschlossen wäre. Die Genehmigung zum Nutzen, Kopieren, Modifizieren und Verteilen dieser Software und der zugehörigen Dokumentation für einen beliebigen Zweck mit oder ohne Gebühr wird hiermit gewährt, vorausgesetzt, dass der oben genannte Urheberrechtshinweis in allen Kopien erscheint und dass sowohl der Urheberrechtshinweis als auch der vorliegende Genehmigungshinweis in der begleitenden Dokumentation erscheinen und dass der Name University of Delaware nicht in Werbung oder in Verbindung mit der Verteilung der Software ohne vorherige ausdrückliche schriftliche Genehmigung verwendet wird. Die University of Delaware gibt keine Zusicherungen bezüglich der Tauglichkeit dieser Software für irgendeinen Zweck. Sie wird entsprechend dem aktuellen Entwicklungsstand ohne ausdrückliche oder konkludente Garantie bereitgestellt.

Zulassungsrelevante Informationen

Europa

CE Dieses Produkt entspricht den anwendbaren CE-Kennzeichnungsrichtlinien und vereinheitlichten Standards:

- Elektromagnetische Verträglichkeit von Elektro- und Elektronikprodukten (EMV) – Richtlinie 2004/108/EG. Siehe *Hinweise zur elektromagnetischen Verträglichkeit (EMV) auf Seite 2*.
- Niedrigspannung (LVD) – Richtlinie 2006/95/EG. Siehe *Sicherheit auf Seite 3*.
- Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten (RoHS) – Richtlinie 2011/65/EU. Siehe *Entsorgung und Recycling auf Seite 3*.

Eine Kopie des Originals der Konformitätserklärung ist bei der Axis Communications AB erhältlich. Siehe *Kontaktinformationen auf Seite 3*.

Hinweise zur elektromagnetischen Verträglichkeit (EMV)

Dieses Gerät wurde konzipiert und getestet für nachstehende Standards:

- Radiofrequenzemission, wenn es entsprechend den Anleitungen installiert und in seiner angedachten Umgebung verwendet wird.
- Immunität gegen elektrische und elektromagnetische Phänomene, wenn es entsprechend den Anleitungen installiert und in seiner angedachten Umgebung verwendet wird.

USA

Dieses Gerät wurde gemäß Teil 15 der FCC-Bestimmungen unter Verwendung eines abgeschirmten Netzwerkkabels (STP) mit den Grenzwerten eines digitalen Geräts der Klasse B geprüft. Diese Grenzwerte bieten einen angemessenen Schutz gegen schädliche Störungen bei der Installation in einem Wohngebiet. Dieses Gerät erzeugt und nutzt hochfrequente Energie und kann diese abstrahlen. Wenn das Gerät nicht anweisungsgemäß installiert und eingesetzt wird, kann es schädliche Störungen im Funkverkehr verursachen. Es kann jedoch nicht garantiert werden, dass bei bestimmten Installationen keine Störungen auftreten. Bei einer Störung des Radio- oder Fernsehempfangs durch dieses Gerät (dies kann durch Aus- und Wiedereinschalten des Geräts festgestellt werden), sollten Sie versuchen, die Störung durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne neu aus oder bringen Sie sie an einem anderen Ort an.
- Vergrößern Sie den Abstand zwischen dem Gerät und dem Empfänger.
- Schließen Sie das Gerät an eine Steckdose eines anderen Stromkreises an, als der, an den der Empfänger angeschlossen ist.
- Ziehen Sie den Händler oder einen qualifizierten Radio- und Fernsehtechniker zu Rate.

Das Produkt muss mit einem abgeschirmten Netzwerkkabel (STP) angeschlossen werden, das vorschriftsmäßig geerdet ist.

Kanada

Dieses Gerät entspricht CAN ICES-3 (Klasse B). Das Produkt muss mit einem abgeschirmten Netzwerkkabel (STP) angeschlossen werden, das vorschriftsmäßig geerdet ist.
Cet appareil numérique est conforme à la norme CAN NMB-3 (classe B). Le produit doit être connecté à l'aide d'un câble réseau blindé (STP) qui est correctement mis à la terre.

Europa

Dieses digitale Gerät erfüllt die Anforderungen der RF-Emission gemäß der Grenzen der Klasse B von EN 55022. Das Produkt muss mit einem abgeschirmten Netzwerkkabel (STP) angeschlossen werden, das vorschriftsmäßig geerdet ist.

Dieses Produkt erfüllt die Anforderungen für Immunität gemäß EN 61000-6-1 der Wohn-, kommerziellen und Leichtindustriegebiete.

Dieses Produkt erfüllt die Anforderungen für Immunität gemäß EN 61000-6-2 der Industriegebiete.

Dieses Produkt erfüllt die Anforderungen für Immunität gemäß EN 55024 für Büro- und Industrieumgebungen.

Dieses Produkt erfüllt die Anforderungen für Immunität gemäß EN 50130-4 der Wohn-, kommerziellen, Leichtindustrie- und Industriegebiete.

Australien/Neuseeland
Dieses digitale Gerät erfüllt die Anforderungen für RF-Emission gemäß der Grenzen der Klasse B der AS/NZS CISPR 22. Das Produkt muss mit einem abgeschirmten Netzwerkkabel (STP) angeschlossen werden, das vorschriftsmäßig geerdet ist.

Japan
この装置は、クラスB 情報技術装置です。この装置は、家庭環境で使用することを目 的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、 受信障害を引き起こすことがあります。 取扱説明書に従って正しい取り扱いをして下さい。 本製品は、シールドネットワークケーブル(STP)を使用して接続してください。また適切に接地してください。

Sicherheit
Dieses Produkt entspricht IEC/EN/UL 60950-1: Einrichtungen der Informationstechnik – Sicherheit. Wenn die Anschlusskabel des Produkts im Außenbereich verlegt werden, muss es entweder über ein geschirmtes Netzwerkkabel (STP) oder durch Anwendung einer anderen geeigneten Methode geerdet werden.

Die für dieses Produkt verwendete Stromversorgung muss die Anforderungen für Schutzkleinspannung (SELV) und für Stromquellen mit begrenzter Leistung (LPS) gemäß IEC/EN/UL 60950-1 erfüllen.

Entsorgung und Recycling
Wenn dieses Produkt ausgedient hat, entsorgen Sie es den geltenden Gesetzen und Bestimmungen entsprechend. Für Informationen zu Ihrem nächstliegendsten Wertstoffhof kontaktieren Sie bitte die örtliche Behörde für Abfallentsorgung. Gemäß den örtlichen gesetzlichen Regelungen können Geldstrafen für die nicht fachgerechte Entsorgung verhängt werden.

Europa

Dieses Symbol bedeutet, dass das Produkt nicht zusammen mit Hausmüll oder Gewerbeabfall entsorgt werden darf. Die Richtlinie 2012/19/EU für elektrischen Müll und elektronische Geräte (WEEE) ist in den Ländern der Europäischen Union anzuwenden. Um potentiellen Schaden für Mensch und Umwelt zu vermeiden, muss das Produkt durch einem geprüften und umweltverträglichen Recycling-Prozess entsorgt werden. Für Informationen zu Ihrem nächstliegendsten Wertstoffhof kontaktieren Sie bitte die örtliche Behörde für Abfallentsorgung. Unternehmen sollten den Produktlieferanten kontaktieren, um zu erfahren wie sie dieses Produkt richtig entsorgen können.

Dieses Produkt entspricht der Richtlinie 2011/65/EU bezüglich der Einschränkung der Verwendung bestimmter gefährdenden Substanzen in Elektro- und Elektronikgeräten (RoHS).

China
Dieses Produkt unterliegt den Anforderungen der zentralen Verwaltungsorgane bezüglich der Kontrolle von Umweltverschmutzungen durch elektronische Produkte.

Kontaktinformationen
Axis Communications AB
Emdalavägen 14
223 69 Lund
Schweden

Tel: +46 46 272 18 00
Fax: +46 46 13 61 30

www.axis.com

Unterstützte Leser
Die Liste der unterstützten Leser kann jederzeit ohne Vorankündigung geändert werden. Wenden Sie ich an Ihren Axis Händler, wenn Sie weitere Informationen zu unterstützten Lesern benötigen.

Dieses Produkt ist kompatibel mit UL-gelisteten Wiegand-Lesern für die Zugangskontrolle.

Dieses Produkt ist kompatibel mit folgenden RS485-Lesern für die Zugangskontrolle:

AXIS A4011-E Reader

HID iCLASS® **RW100**: 6101CG40000, 6101CGM0000, 6101CK40000, 6101CK40002, 6101CK40100, 6101CK403C0, 6101CKM0000, 6101CKM0002, 6101CKM0203; **RW300**: 6111CG40000, 6111CG400C0, 6111CGM0000, 6111CK40000, 6111CK4000Z, 6111CKM0000; **RW400**: 6121CG40000, 6121CGM0000, 6121CK40000, 6121CK40003, 6121CK40007-G3.0, 6121CK4000D-G3.0, 6121CKM0000; **R40**: 6122CKP00P0, 6122CKP05P0, 6122CKP06P0; **RWK400**: 6131CG4020000, 6131CK4000000, 6131CK4000014, 6131CK4000300, 6131CK4020000, 6131CKM000000, 6131CKM000214; **RK40**: 6132BKP00Q709-G3.0, 6132CKP000009, 6132CKP000011, 6132CKP000700-G3.0, 6132CKP000709-G3.0, 6132CKP001009, 6132CKP001011, 6132CKP00P000, 6132CKP00P009, 6132CKP00P709-G3.0, 6132CKP00Q709-G3.0, 6132CKP030014, 6132CKP060514, 6132CKP06P009, 6132CKP06P609, 6132CKP070209; **RW150**: 6141CG40000, 6141CGM0000, 6141CK40000, 6141CKM0000; **R15**: 6142CKP000Z, 6142CKP00P0, 6142CKP0100; **RWKL550**: 6171BK4000000, 6171BK4000009, 6171BK4000014, 6171BK4000214, 6171BK4000500, 6171BK4040Z14, 6171BK4060000, 6171BK4060209, 6171BK4060Z09, 6171BK4061000, 6171BKM000000, 6171BKM000200, 6171BKM000300, 6171BKM040400; **RWKLB575**: 6181BK4000000, 6181BK4000009, 6181BK4000014, 6181BK4000022, 6181BK406C009;

HID Smartid®: 8031DSAP

HID pivClass® **R10-H**: 900LHRNAK00000, 900LHRTAK00000, 900NHRNAK00000, 900NHRTAK00000, 900PHRNAK00000, 900PHRTAK00000, 910LHRNAK00000, 910LHRTAK00000, 910NHRNAK00000, 910NHRTAK00000, 910PHRNAK00000, 910PHRTAK00000, 920LHRNAK00000, 920LHRTAK00000, 920NHRNAK00000, 920NHRTAK00000, 920PHRNAK00000, 920PHRTAK00000, 921LHRNAK00000, 921LHRTAK00000, 921NHRNAK00000, 921NHRTAK00000, 921PHRNAK00000, 921PHRTAK00000; **RPKCL40-P**: 923LPRNAK00000, 923LPRTAK00000, 923NPRTAK00000, 923PPRNAK00000, 923PPRTAK00000

Aptiq™: M11, MTK15, MTMSK15, MT15, MTMS15

UL-geprüfte RS485-Leser für die Zugangskontrolle finden Sie unter *www.axis.com* in der entsprechenden Installationsanleitung.

Support

Wenn Sie technische Unterstützung benötigen, wenden Sie sich bitte an Ihren Axis Händler. Wenn Ihre Fragen nicht sofort beantwortet werden können, leitet Ihr Händler Ihre Anfragen an die zuständigen Stellen weiter, damit Sie umgehend Unterstützung erhalten. Wenn Sie über eine Internetverbindung verfügen, können Sie:

- Benutzerhandbücher und Softwareaktualisierungen herunterladen
- Antworten auf bereits gelöste Probleme in der FAQ-Datenbank finden Eine Suche auf der Grundlage eines Produkts, einer Kategorie oder eines Satzes
- Axis Supportmitarbeiter über Probleme informieren, indem Sie sich in Ihrem persönlichen Supportbereich anmelden
- Chat mit Axis Supportmitarbeitern (nur in bestimmten Ländern möglich)
- Axis Support im Internet: *www.axis.com/techsup/*

Erfahren Sie mehr!

Besuchen Sie das Axis-Schulungszentrum *www.axis.com/academy/* für anregende Schulungen, Webinare, Tutorien und Anleitungen.

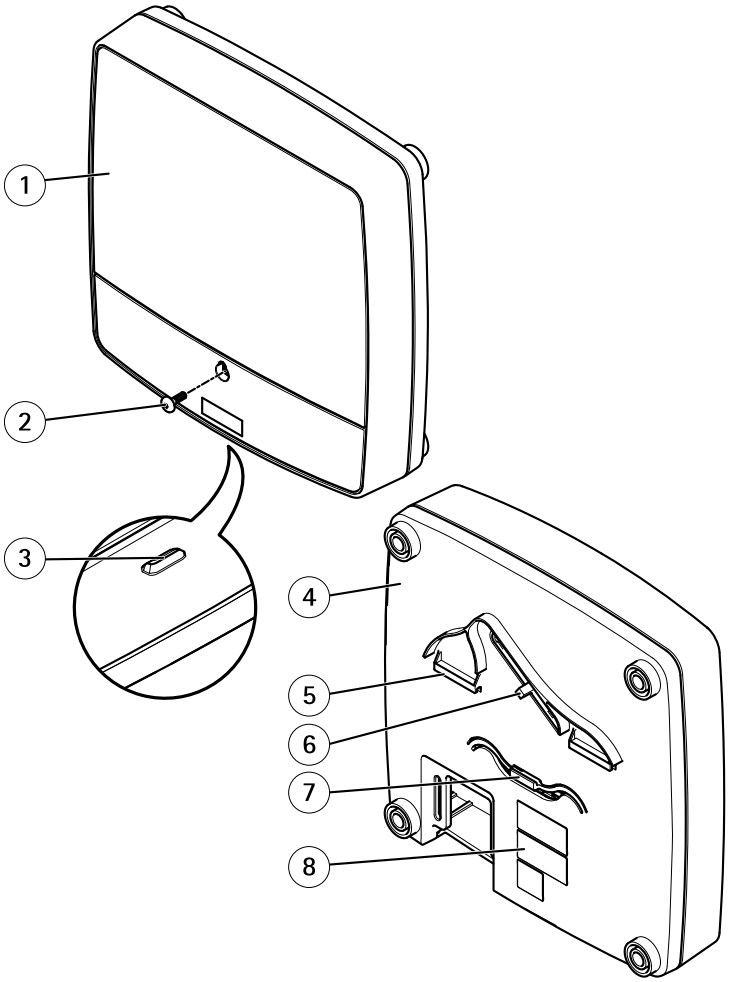
Inhalt

Übersicht über die Hardware

Übersicht über die Hardware

Die Hardwareübersicht ist in folgende Kategorien unterteilt:

- Vorder- und Rückseite. Siehe *Seite 5*.
- E/A-Schnittstelle. Siehe *Seite 6*.
- Externe Stromanschlüsse. Siehe *Seite 6*.
- Stromausgänge. Siehe *Seite 6*.
- LED-Anzeigen, Tasten und andere Hardware. Siehe *Seite 7*.

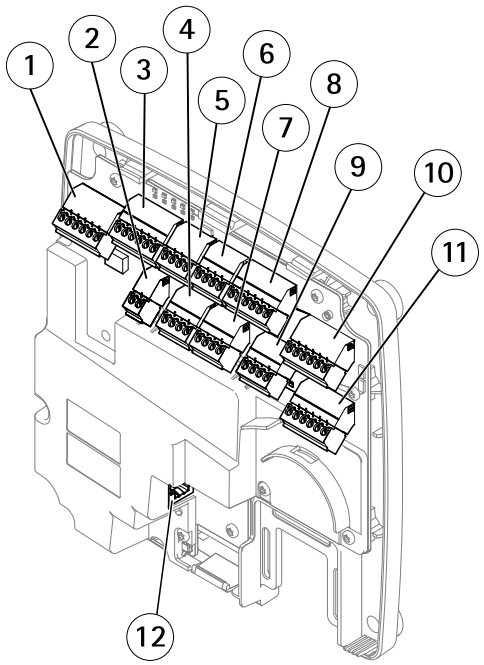


Vorder- und Rückseite:

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

Übersicht über die Hardware

8 Bestellnummer (P/N) und Seriennummer (S/N)



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)

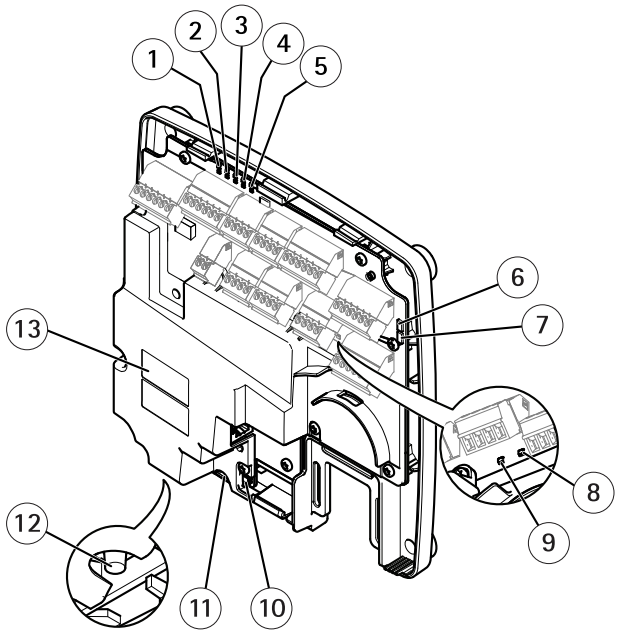
Externe Stromanschlüsse:

2 Netzanschluss (DC IN)
12 Netzwerkanschluss (PoE)

Stromausgänge:

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

Übersicht über die Hardware



LED-Anzeigen, Tasten und andere Hardware:

1 *LED-Betriebsanzeige*
2 *LED-Statusanzeige*
3 *LED-Netzwerkanzeige*
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)*

LEDs

LED	Farbe	Bedeutung
Netzwerk	Grün	Leuchtet bei Verbindung mit einem 100 MBit/s-Netzwerk. Blinkt bei Netzwerkaktivität.
	Gelb	Leuchtet bei Verbindung mit einem 10 MBit/s-Netzwerk. Blinkt bei Netzwerkaktivität.
	Leuchtet nicht	Keine Netzwerkverbindung 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.

Beachten

- 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

Für die technischen Daten siehe *Seite 59*.

E/A-Schnittstelle

Leser-Daten-Anschluss
Zwei 6-polige Anschlussblöcke mit Unterstützung für RS485- und Wiegand-Protokoll zur Kommunikation mit dem Leser. Technische Daten finden Sie auf *Seite 63*.

Leser-E/A-Anschluss
Zwei 6-polige Anschlussblöcke für Lesereingang und -ausgang. Abgesehen vom 0 V DC-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 63*.

Türanschluss
Zwei 4-polige Anschlussblöcke zum Anschließen von Türüberwachungsgeräten und REX-Geräten (Request to Exit). Technische Daten finden Sie auf *Seite 64*.

Zusatzanschluss
4-poliger konfigurierbarer E/A-Anschlussblock. Zur Verwendung mit externen Geräten in Verbindung mit Manipulationsalarmen, Ereignisauslösung, Alarmbenachrichtigungen usw. Abgesehen vom 0 V DC-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 64*.

Externe Stromanschlüsse

HINWEIS

Das Produkt muss mit einem abgeschirmten Netzwerkkabel (STP) angeschlossen werden. Alle Kabel, die das Produkt mit dem Netzwerkswitch verbinden, müssen hierfür ausgelegt sein. Stellen Sie sicher, dass die Netzwerkgeräte 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 64*.

Übersicht über die Hardware

Netzwerkanschluss
RJ-45-Ethernetanschluss. Unterstützt Power over Ethernet (PoE). Technische Daten finden Sie auf *Seite 65*.

Stromausgänge

Stromanschluss
4-poliger Anschlussblock für ein oder zwei Schlösser. Dieser Anschluss kann auch zur Stromversorgung externer Geräte verwendet werden. Technische Daten finden Sie auf *Seite 65*.

Netz- und Relaisanschluss
6-poliger Anschlussblock für den Netzanschluss und das Relais des Tür-Controllers für externe Geräte wie Schlösser und Sensoren. Technische Daten finden Sie auf *Seite 65*.

Tasten und andere Hardware

Stiftleiste für Manipulationsalarm
Zwei 2-polige Stiftleisten zum Trennen des vorderen und rückseitigen Manipulationsalarms. Technische Daten finden Sie auf *Seite 66*.

Steuertaste
Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Seite 54*.
- Anschluss an einen AXIS Video Hosting System-Service. Siehe *Seite 48*. 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 48*. Halten Sie zum Verbinden die Taste für ca. 3 Sekunden gedrückt.

Zugriff auf das Produkt

Anweisungen zur Installation des Axis Produkts finden Sie in der mitgelieferten Installationsanleitung.

Das Produkt ist mit den meisten Standard-Betriebssystemen und Browsern kompatibel. Empfohlen werden die Browser Internet Explorer für Windows, Safari für Macintosh und Firefox für andere Betriebssysteme. Siehe *Spezifikationen auf Seite 59*.

Zugriff über einen Browser

1. Starten Sie einen Browser (Chrome, Internet Explorer, Firefox, Safari).
2. Geben Sie in die Adresszeile des Browsers die IP-Adresse oder den Host-Namen des Axis Produkts ein. Wenn Sie von einem Macintosh-Computer (Mac OS X) auf das Produkt zugreifen möchten, klicken Sie auf die Bonjour-Tab, und wählen Sie ein Produkt aus der Dropdownliste aus.

   Wenn Sie die IP-Adresse nicht kennen, können Sie das Produkt mithilfe von AXIS IP Utility im Netzwerk identifizieren. Weitere Informationen zum Ermitteln und Zuweisen von IP-Adressen finden Sie auf den Support-Seiten unter *www.axis.com/techsup* oder in der Installationsanleitung unter *www.axis.com*.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Wenn dies der erste Zugriff auf das Produkt ist, muss das Root-Kennwort konfiguriert werden. Anweisungen finden Sie unter *Festlegen des Root-Kennworts auf Seite 10*.
4. AXIS Entry Manager wird im Browser geöffnet. Die Startseite wird als Übersichtsseite bezeichnet.

Zugriff über das Internet

Nach dem Anschließen können Sie über Ihr lokales Netzwerk (LAN) auf das Axis Produkt zugreifen. Um über das Internet auf das Produkt zugreifen zu können, muss der Netzwerk-Router so konfiguriert werden, dass eingehender Datenverkehr zum Produkt zugelassen wird. Aktivieren Sie dazu die NAT-Traversal-Funktion, bei der versucht wird, den Router automatisch für den Zugriff auf das Produkt zu konfigurieren. Rufen Sie dazu **Setup > System Options > Network > TCP/IP Advanced (Grundeinstellungen > Systemoptionen > Netzwerk > TCP/IP Erweitert)** auf.

Für weitere Informationen siehe *NAT-Traversal (Port-Mapping) für IPv4 auf Seite 50*. Beachten Sie auch den AXIS Internet Dynamic DNS-Service unter *www.axiscam.net*.

Technische Hinweise zu diesem und anderen Themen finden Sie auf der Axis Support-Website unter *www.axis.com/techsup*.

Festlegen des Root-Kennworts

Für den Zugriff auf das Produkt muss das Kennwort für den standardmäßigen Administrator-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 Netzwerkkommunikation 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 44*.

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 Werkseinstellungen auf Seite 54*.

Zum Festlegen des Kennworts über eine standardmäßige HTTP-Verbindung geben Sie dieses direkt in das Dialogfeld ein.

Um das Kennwort über eine verschlüsselte HTTPS-Verbindung festzulegen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Use HTTPS (HTTPS verwenden)**.

Ein befristetes Zertifikat (gültig für ein Jahr) wird erstellt. Dieses gewährleistet die sichere Datenübertragung zum und vom Produkt. Das Kennwort kann jetzt sicher festgelegt werden.

2. Geben Sie ein Kennwort ein und wiederholen Sie die Eingabe, um die korrekte Schreibweise zu bestätigen.
3. Klicken Sie auf **OK**. Damit ist das Kennwort konfiguriert.

Die Seite „Overview" (Übersicht)

Die Seite „Overview" (Übersicht) von AXIS Entry Manager enthält Informationen wie den Namen, die MAC-Adresse, die IP-Adresse und die Firmwareversion des Tür-Controllers. Mithilfe dieser Angaben lässt sich der Tür-Controller im Netzwerk oder im System identifizieren.

Bei der ersten Verwendung des Axis Produkts werden Sie auf der Seite „Overview" (Übersicht) aufgefordert, die Hardware zu konfigurieren, Datum und Uhrzeit festzulegen sowie den Tür-Controller als Teil eines Systems oder als Standalone-Gerät zu konfigurieren. Weitere Informationen zur Konfiguration des Systems finden Sie unter *Konfiguration – Schritt für Schritt auf Seite 12*.

Klicken Sie in der Menüleiste auf **Overview (Übersicht)**, um von anderen Websites des Produkts aus die Seite „Overview" (Übersicht) aufzurufen.

Systemkonfiguration

Klicken Sie zum Öffnen der Setup-Seiten des Produkts in der oberen rechten Ecke der Seite „Overview" (Übersicht) auf **Setup**.

Dieses Axis Produkt kann von Administratoren konfiguriert werden. Weitere Informationen zu Benutzern und Administratoren finden Sie unter *Seite 25*, *Seite 31* und *Seite 44*.

Konfiguration – Schritt für Schritt

Vor der Verwendung des Zugangskontrollsystems sollten Sie folgende Einrichtungsschritte durchführen:

1. Ändern der Spracheinstellung von AXIS Entry Manager, wenn erforderlich. (Standardsprache ist Englisch.) Siehe .
2. Konfigurieren des Tür-Controllers und verbundener Geräte (z. B. Leser, Schlösser und REX-Geräte). Siehe *Konfigurieren der Hardware auf Seite 13*.
3. Überprüfen der Hardwareanschlüsse. Siehe .
4. Einstellen von Datum und Uhrzeit. Siehe *Seite 18*.
5. Konfigurieren der Netzwerkeinstellungen. Siehe *Seite 19*.
6. Konfigurieren des Kartenformats. Siehe *Seite 20*.
7. Konfigurieren des Tür-Controller-Systems. Siehe *Verwalten von Netzwerk-Tür-Controllern auf Seite 22*.

Weitere Informationen zum Konfigurieren und Verwalten der Türen, Zeitpläne, Benutzer und Gruppen des Systems finden Sie unter *Zugangsverwaltung auf Seite 25*.

Empfehlungen zur Wartung finden Sie unter *Wartungsanweisungen auf Seite 24*.

Beachten

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

Auswählen einer Sprache

Die Standardsprache von AXIS Entry Manager ist Englisch. Sie können jedoch zu einer beliebigen Sprache wechseln, die in der Firmware des Produkts enthalten ist. Unter *www.axis.com* finden Sie Informationen über die aktuell verfügbare Firmware.

Sie können die Sprache auf allen Webseiten des Produkts ändern.

Wenn Sie die Sprache ändern möchten, klicken Sie auf die entsprechende Dropdownliste und wählen eine Sprache aus. Alle Webseiten des Produkts einschließlich der Onlinehilfe werden in der ausgewählten Sprache angezeigt.

Wichtig

- Die Sprachauswahl wird ab Firmware 1.25 unterstützt. Wenn der Tür-Controller eine ältere Version verwendet, müssen Sie die Firmware aktualisieren, bevor Sie eine Sprache auswählen können. Siehe *Aktualisieren der Firmware auf Seite 56*.
- Die Spracheinstellungen werden nicht automatisch für alle Tür-Controller im System übernommen. Wählen Sie die Sprache entweder in allen Tür-Controllern aus, oder öffnen Sie AXIS Entry Manager immer über denselben Tür-Controller.

Beachten

- Wenn Sie die Sprache ändern, wechselt auch das Datumsformat zu einem in der ausgewählten Sprache üblichen Format. In den Datenfeldern wird das korrekte Format angezeigt.
- Wenn Sie das Produkt auf die Werkseinstellungen zurücksetzen, wechselt AXIS Entry Manager zurück zu Englisch.
- Wenn Sie das Produkt wiederherstellen, verwendet AXIS Entry Manager weiter die ausgewählte Sprache.
- Wenn Sie das Produkt neu starten, verwendet AXIS Entry Manager weiter die ausgewählte Sprache.
- Wenn Sie die Firmware aktualisieren, verwendet AXIS Entry Manager weiter die ausgewählte Sprache.

Konfigurieren der Hardware

Um die Türen zu verwalten, muss die Hardware auf den Hardware-Konfigurationsseiten 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 Ihnen somit das Pin Chart zur Verfügung steht. Das Pin Chart dient als Leitfaden für den Anschluss der Kontakte sowie als Referenz bei der Wartung. Anweisungen zur Wartung finden Sie auf *Seite 24*.

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

- Importieren einer Hardwarekonfigurationsdatei. Siehe *Seite 13*.
- Erstellen einer neuen Hardwarekonfiguration. Siehe *Seite 14*.

Importieren einer Hardware-Konfigurationsdatei

Die Hardwarekonfiguration des Axis Produkts kann schneller abgeschlossen werden, indem eine Hardware-Konfigurationsdatei importiert wird.

Durch das Exportieren der Datei aus einem Produkt und das Importieren in ein anderes können Sie mehrere Kopien der 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 Hardware-Konfigurationen verwenden. Für weitere Informationen siehe

So importieren Sie eine Hardware-Konfigurationsdatei:

1. Rufen Sie **Setup > Hardware Configuration (Setup > Hardwarekonfiguration)** auf.
2. Klicken Sie auf **Import hardware configuration (Hardwarekonfiguration importieren)** oder, wenn bereits eine Hardwarekonfiguration vorhanden ist, auf **Reset and import hardware configuration (Zurücksetzen und Hardwarekonfiguration importieren.)**.
3. Wählen Sie im angezeigten Dateibrowser die Hardware-Konfigurationsdatei (*.json) auf dem Computer aus.
4. Klicken Sie auf **OK**.

Exportieren einer Hardwarekonfigurationsdatei

Die Hardwarekonfiguration des Axis Produkts lässt sich exportieren und so auch für baugleiche Geräte verwenden. Sie können exportierte Dateien auch als Sicherungen speichern und diese zum Wiederherstellen vorheriger Hardwarekonfigurationen verwenden.

So exportieren Sie eine Hardwarekonfigurationsdatei:

1. Rufen Sie **Setup > Hardware Configuration (Setup > Hardwarekonfiguration)** auf.
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.

Erstellen einer neuen Hardwarekonfiguration

So erstellen Sie eine komplett neue Hardwarekonfiguration:

1. Rufen Sie **Setup > Hardware Configuration (Setup > Hardwarekonfiguration)** auf und klicken Sie auf **Start new hardware configuration (Neue Hardwarekonfiguration starten)**.

   Wenn die Hardware des Produkts zuvor nicht konfiguriert wurde oder gelöscht wurde, ist die Option **Hardware Configuration (Hardwarekonfiguration)** im Benachrichtigungsbereich der Übersichtsseite verfügbar.

2. Wählen Sie eine Türoption entsprechend der Anzahl von Türen, eine (1) oder zwei (2), die mit dem Axis Produkt verbunden werden.

3. Verwenden Sie eine deskriptive Namensgebung für jede Tür und klicken Sie auf **Next (Weiter)**. Es wird empfohlen, die Türen mit eindeutigen Namen zu beschreiben, damit diese von allen Personen, die für die Verwaltung des Systems verantwortlich sind, identifiziert werden können.

   Sie können auch den Namen des Axis Produkts bearbeiten. Der Standardname umfasst zur leichteren Identifizierung die Seriennummer.

4. Wählen Sie die Optionen für Türmonitor und -schloss aus, die den Anforderungen und dem Typ der verwendeten Schlossverbindungen entsprechen, und klicken Sie auf **Next (Weiter)**. Weitere Informationen finden Sie unter und .

5. Wählen Sie die Typen der zu verwendenden Leser aus und klicken Sie auf **Finish (Beenden)**. Weitere Informationen finden Sie unter und .

6. Klicken Sie im Dialogfeld, das nach Abschluss der Konfiguration angezeigt wird, auf **OK** oder klicken Sie auf den Link, um das Pin Chart anzuzeigen.

   Klicken Sie zum Ausdrucken des Pin Charts auf **Print Hardware Pin Chart (Pin Chart drucken)**.

Klicken Sie zum Abbrechen der Hardwarekonfiguration auf **Cancel (Abbrechen)**. Dies ist auf jeder der Hardware-Konfigurationsseiten möglich.

Konfigurieren von Schlössern und Türmonitoren

1. Wenn ein Türmonitor verwendet wird, wählen Sie **Door monitor (Türmonitor)** und anschließend die Optionen passend zu den Stromkreisen des entsprechenden Türmonitors aus.

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.

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 finden Sie unter *Verwenden überwachter Eingänge auf Seite 17*.

Beachten

- 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.

Optionen für Türmonitore

Es stehen folgende Optionen für Türmonitore zur Verfügung:

- **Door monitor (Türmonitor)** – Diese Option ist standardmäßig ausgewählt. Jede Tür verfügt über einen eigenen Türmonitor, der beispielsweise angibt, ob eine Tür aufgebrochen wurde oder zu lange geöffnet bleibt. Deaktivieren Sie diese Option, wenn kein Türmonitor verwendet wird.
  - **Open circuit = Closed door (Unterbrochener Stromkreis = Tür geschlossen)** – Wählen Sie diese Option aus, wenn der Türmonitor einen Schliesser-Kontakt verwendet. Der Türmonitor gibt bei geschlossenem Stromkreis an, dass die Tür geöffnet ist. Der Türmonitor gibt bei offenem Stromkreis an, dass die Tür geschlossen ist.
  - **Open circuit = Open door (Offener Stromkreis = Tür geöffnet)** – Wählen Sie diese Option aus, wenn der Türmonitor einen Öffner-Kontakt verwendet. Der Türmonitor gibt bei offenem Stromkreis an, dass die Tür geöffnet ist. Der Türmonitor gibt bei geschlossenem Stromkreis an, dass die Tür geschlossen ist.
- **Cancel access time once door is opened (Zugangsdauer nach dem Öffnen der Tür begrenzen)** – Wählen Sie diese Option aus, um den Zugang mehrerer Personen kurz nacheinander (den Zugang nicht autorisierter Besucher) zu verhindern. Die Tür wird sofort nach dem Öffnen wieder verriegelt, sobald sie sich schließt. Die Tür kann erst nach einer erneuten Authentifizierung wieder geöffnet werden.

Folgende Zeitoptionen stehen für Türmonitore zur Verfügung:

- **Access time (Zugangsdauer)** – Stellen Sie Anzahl von Sekunden ein, die die Tür geöffnet bleiben soll, nachdem Zugang gewährt wurde. Die Tür bleibt unverriegelt, bis sie geöffnet wird, und verriegelt sich beim Schließen automatisch, unabhängig davon, ob die Zugangsdauer bereits abgelaufen ist oder nicht. Wenn die Tür nicht geöffnet wird, verriegelt sie sich automatisch, sobald die festgelegte Zugangsdauer abgelaufen ist.
- **Open too long time (Maximale Öffnungsdauer)** – Legen Sie die Anzahl von Sekunden fest, die die Tür maximal geöffnet bleiben darf. Der entsprechende Alarm wird ausgelöst, wenn die maximale Öffnungsdauer der Tür überschritten wird. Richten Sie eine Aktionsregel ein, die festlegt, welche Aktion ausgelöst werden soll, wenn die maximale Öffnungsdauer überschritten wird.
- **Pre-alarm time (Voralarmdauer)** – Ein Voralarm ist ein Warnsignal, das ausgelöst wird, bevor die maximale Öffnungsdauer der Tür überschritten wird. Die Aktionsregel warnt den Administrator (und je nach Konfiguration auch den Benutzer (die Person an der Tür)), dass die Tür geschlossen werden muss oder sonst der eigentliche Alarm (maximale Öffnungsdauer überschritten) ausgelöst wird. Legen Sie fest, 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.

Weitere Informationen zum Einrichten einer Aktionsregel finden Sie unter *Einrichten von Aktionsregeln auf Seite 37*.

Optionen für Schlösser

Deaktivieren Sie die Option **Door monitor (Türmonitor)**, um die folgenden Schließzeitoptionen nutzen zu können:

- **Door unlocked time (Entriegelungszeit der Tür)** – Legen Sie die Dauer in Sekunden fest, die die Tür entriegelt bleiben soll, nachdem der Zugang gewährt wurde. Die Tür bleibt bis zur Öffnung entriegelt und wird nach dem Schließen automatisch wieder verriegelt, unabhängig davon, ob die Entriegelungszeit bereits abgelaufen ist. Wenn die Tür nicht geöffnet wird, verriegelt sie sich wieder, sobald die festgelegte Entriegelungszeit abgelaufen ist.
- **Pre-lock signal time (Zeit für Vorverriegelungssignal)** – Ein Vorverriegelungssignal ist ein Warnsignal, das vor dem Verriegeln der Tür ausgelöst wird. Dieses Signal informiert den Administrator und je nach Aktionsregel ggf. auch den Benutzer (die Person an der Tür) darüber, dass die Tür in Kürze verriegelt wird. Legen Sie fest, wie viele Sekunden vor dem Verriegeln der Tür das System das Vorverriegelungssignal auslösen soll. Die Zeit für das Vorverriegelungssignal muss kürzer als die Entriegelungszeit sein. Legen Sie die Zeit für das Vorverriegelungssignal auf 0 fest, wenn Sie das Vorverriegelungssignal deaktivieren möchten.

Für den Schaltkreis des Schlosses stehen folgende Optionen zur Verfügung:

- 12 V
  - **Fail-secure (Arbeitsstrom)** – Wählen Sie diese Option für Schlösser aus, die bei Stromausfällen verriegelt bleiben. Wenn Strom angelegt wird, entriegelt sich das Schloss.

- **Fail-safe (Ruhestrom)** – Wählen Sie diese Option für Schlösser aus, die bei Stromausfällen entriegelt werden. Wenn Strom angelegt wird, verriegelt sich das Schloss.

- **Relay (Relais)** – Kann nur für ein Schloss pro Tür-Controller verwendet werden. Sind zwei Türen mit dem Tür-Controller verbunden, kann nur am Schloss der zweiten Tür ein Relais verwendet werden.

  - **Relay open = Locked (Relais geöffnet = verriegelt)** – Wählen Sie diese Option für Schlösser aus, die bei geöffnetem Relais verriegelt bleiben (Fail-secure). Wenn sich das Relais schließt, wird das Schloss entriegelt.

  - **Relay open = Unlocked (Relais geöffnet = entriegelt)** – Wählen Sie diese Option für Schlösser aus, die bei Stromausfällen entriegelt werden (Fail-safe). Wenn sich das Relais schließt, wird das Schloss verriegelt.

- **None (Keine)** – Wählen Sie diese Option aus, wenn nur ein einzelnes Schloss verwendet wird.

Für den Schlossmonitor stehen folgende Optionen zur Verfügung:

- **Lock monitor (Schlossmonitor)** – Wählen Sie diese Option aus, um die Schlossmonitor-Steuerelemente zu nutzen. Wählen Sie dann das Schloss aus, das Sie überwachen möchten. Ein Schlossmonitor kann nur bei Doppelschlosstüren verwendet werden. Er kann nicht verwendet werden, wenn zwei Türen mit dem Tür-Controller verbunden sind.

  - **Open circuit = Locked (Offener Schaltkreis = verriegelt)** – Wählen Sie diese Option aus, wenn es sich beim Schaltkreis des Schlossmonitors um einen Öffner-Kontakt handelt. Wenn der Schaltkreis geschlossen ist, zeigt der Schlossmonitor eine unverriegelte Tür an. Wenn der Schaltkreis geöffnet ist, zeigt der Schlossmonitor eine verriegelte Tür an.

  - **Open circuit = Unlocked (Offener Schaltkreis = unverriegelt)** – Wählen Sie diese Option aus, wenn es sich beim Schaltkreis des Schlossmonitors um einen Schliesser-Kontakt handelt. Wenn der Schaltkreis geöffnet ist, zeigt der Schlossmonitor eine unverriegelte Tür an. Wenn der Schaltkreis geschlossen ist, zeigt der Schlossmonitor eine verriegelte Tür an.

Weitere Informationen zum Einrichten einer Aktionsregel finden Sie unter *Einrichten von Aktionsregeln auf Seite 37*.

Konfigurieren von Lesern und REX-Geräten

1. Wählen Sie **Reader (Leser)** und anschließend die Optionen für das Kommunikationsprotokoll des Lesers aus, wenn ein Leser verwendet werden soll.

2. Wenn ein REX-Gerät (Request to Exit) wie ein Taster, ein Sensor oder eine Druckstange verwendet werden soll, wählen Sie **REX** und anschließend die Optionen passend zu den Schaltkreisen des entsprechenden REX-Geräts aus.

   Wählen Sie **REX does not unlock door (REX entriegelt Tür nicht)** aus, wenn die Tür verriegelt bleiben soll, bis diese manuell aufgeschlossen und geöffnet wird.

3. Wiederholen Sie bei Anschluss von mehr als einem Leser bzw. REX-Gerät an den Tür-Controller die vorherigen Schritte, bis alle Leser und REX-Geräte richtig konfiguriert sind.

Optionen für Leser und REX-Geräte

Für Leser stehen folgende Optionen zur Verfügung:

- **Wiegand** – Wählen Sie diese Option für Leser aus, die Wiegand-Protokolle verwenden. Wählen Sie anschließend die LED-Steuerung aus, die vom Leser unterstützt wird. 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. In den Herstellerinformationen finden Sie Informationen darüber, welche LED-Steuerung der Leser unterstützt.

- **RS485 half duplex (RS485 Halbduplex)** – Wählen Sie diese Option für RS485-Leser mit Halbduplex-Unterstützung aus. Wählen Sie anschließend das RS485-Protokoll aus, das vom Leser unterstützt wird. In den Herstellerinformationen finden Sie Informationen darüber, welches Protokoll der Leser unterstützt.

- **RS485 full duplex (RS485 Vollduplex)** – Wählen Sie diese Option für RS485-Leser mit Vollduplex-Unterstützung aus. Wählen Sie anschließend das RS485-Protokoll aus, das vom Leser unterstützt wird. In den Herstellerinformationen finden Sie Informationen darüber, welches Protokoll der Leser unterstützt.

Für REX-Geräte stehen folgende Optionen zur Verfügung:

- **Active low (Aktiv niedrig)** – Wählen Sie diese Option aus, wenn die Aktivierung des REX-Geräts den Stromkreis schließt.
- **Active high (Aktiv hoch)** – Wählen Sie diese Option aus, wenn die Aktivierung des REX-Geräts den Stromkreis öffnet.
- **REX does not unlock door (REX entriegelt Tür nicht)** – Wählen Sie diese Option aus, wenn die Tür verriegelt bleiben soll, bis diese manuell aufgeschlossen und geöffnet wird. Der Türalarm wird nur dann ausgelöst, wenn die Tür nicht innerhalb der festgelegten Zugangszeit geöffnet wird. Deaktivieren Sie diese Option, wenn die Tür automatisch entriegelt werden soll, sobald der Benutzer das REX-Gerät aktiviert.

Wichtig

Wenn der Tür-Controller vor dem Upgrade von Firmware 1.10 auf Firmware 1.15 oder höher nur für eine Tür konfiguriert wurde, steht die Option **REX does not unlock door (REX entriegelt die Tür nicht)** zunächst nicht zur Verfügung. Wenn Sie die Option **REX does not unlock door (REX entriegelt die Tür nicht)** nutzen möchten, wechseln Sie zu **Setup > Hardware Configuration (Setup > Hardewarekonfiguration** und klicken dann auf **Reset and start a new hardware configuration (Zurücksetzen und neue Hardwarekonfiguration starten)**. Richten Sie anschließend Regeln für die mit dem Tür-Controller verbundenen Türen ein, und fügen Sie diese zu Gruppen hinzu. Informationen hierzu finden Sie unter *Verwalten von Türen*.

Beachten

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.

Verwenden überwachter Eingänge

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

So verwenden Sie überwachte Eingänge:

1. Bringen Sie an allen verwendeten Eingängen Abschlusswiderstände an. Siehe Anschlussschaltbild unter *Seite 67*.
2. Rufen Sie **Setup > Hardware Rekonfiguration (Setup > Hardwareneukonfiguration)** auf, und wählen Sie **Enable supervised inputs (Überwachte Eingänge aktivieren)** aus. Sie können die überwachten Eingänge auch während der Hardwarekonfiguration aktivieren.

Unterstützung überwachter Eingänge

Die folgenden Anschlüsse unterstützen überwachte Eingänge:

- Leser-E/A-Anschluss – Manipulationssignal. Siehe *Seite 63*.
- Türanschluss. Siehe *Seite 64*.

Im Folgenden finden Sie Beispiele für Leser und Schalter, die für überwachte Eingänge geeignet sind:

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

Überprüfen der Hardwareanschlüsse

Sie können die angeschlossenen Türmonitore, Schlösser und Leser nach Abschluss von Installation und Konfiguration sowie jederzeit während der gesamten Lebensdauer des Tür-Controllers überprüfen.

Rufen Sie **Setup > Hardware Connection Verification (Setup > Überprüfen der Hardwareanschlüsse)** auf, um die Konfiguration zu prüfen und den entsprechenden Bereich zu öffnen.

Überprüfungssteuerelemente

- **Door state (Status Tür)** – Überprüfen des aktuellen Türmonitorstatus, der Türalarme und der Schlösser. Klicken Sie auf **Get current state (Aktuellen Status abrufen)**.
- **Lock (Verriegeln)** – Manuelle Steuerung des Schlosses. Gilt für primäre und sekundäre Schlösser (sofern vorhanden). Klicken Sie auf **Lock (Verriegeln)** oder **Unlock (Entriegeln)**.
- **Lock (Verriegeln)** – Manuelle Steuerung des Schlosses, um Zugang zu gewähren. Gilt nur für primäre Schlösser. Klicken Sie auf **Access (Zugang)**.
- **Reader: Feedback (Leser: Feedback)** – Überprüfen des Leser-Feedbacks wie Signaltönen und LED-Anzeigen für verschiedene Befehle. Wählen Sie den Befehl aus, und klicken Sie auf **Test (Testen)**. Die Typen des verfügbaren Feedbacks variieren ja nach Leser. Weitere Informationen finden Sie unter *Leser-Feedback*. Beachten Sie auch die Anweisungen des Herstellers.
- **Reader: Tampering (Leser: Manipulation)** – Informationen zum letzten Manipulationsversuch. Der erste Manipulationsversuch wird während der Installation des Lesers registriert. Klicken Sie auf **Get last tampering (Letzte Manipulation abrufen)**.
- **Reader: Card swipe (Leser: Durchziehen einer Karte)** – Informationen über die letzte durchgezogene Karte oder andere vom Leser akzeptierte Benutzer-Token. Klicken Sie auf **Get last credential (Letzte Zugriffsdaten abrufen)**.
- **REX** – Informationen über den letzten Zeitpunkt, an dem das REX-Gerät betätigt wurde. Klicken Sie auf **Get last REX (Letzte REX-Betätigung abrufen)**.

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 22*.

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 18*.
- Manuelles Einstellen von Datum und Uhrzeit. Siehe *Seite 19*.
- Abrufen von Datum und Uhrzeit vom Computer. Siehe *Seite 19*.

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 49*.

Wenn Sie für den NTP-Server einen Host-Namen verwenden, muss ein DNS-Server konfiguriert werden. Siehe *DNS-Konfiguration auf Seite 49*.

Manuelles Einstellen von Datum und Uhrzeit

1. Wechseln Sie zu **Setup > Date & Time (Setup > Datum und Uhrzeit)**.
2. Wählen Sie **Adjust for daylight saving (Automatische Zeitumstellung)** aus, wenn in der jeweiligen Region zwischen Sommer- und Winterzeit umgestellt wird.
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. Wechseln Sie zu **Setup > Date & Time (Setup > Datum und Uhrzeit)**.
2. Wählen Sie **Adjust for daylight saving (Automatische Zeitumstellung)** aus, wenn in der jeweiligen Region zwischen Sommer- und Winterzeit umgestellt wird.
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

Rufen Sie **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)** auf, um die grundlegenden Netzwerkeinstellungen zu konfigurieren.

Weitere Informationen zu Netzwerkeinstellungen finden Sie unter *Netzwerk auf Seite 47*.

Grundlegende TCP/IP-Einstellungen

Das Axis Produkt unterstützt IPv4.

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

- **Dynamische IP-Adresse – Obtain IP address via DHCP (IP-Adresse über DHCP beziehen)** ist standardmäßig aktiviert. Das Axis Produkt erhält seine IP-Adresse automatischen per DHCP (Dynamic Host Configuration Protocol).

  Mithilfe von DHCP können Netzwerkadministratoren die Zuweisung von IP-Adressen zentral verwalten und automatisieren.

- **Statische IP-Adresse** – Um eine statische IP-Adresse zu verwenden, aktivieren Sie das Kontrollkästchen **Use the following IP address (Folgende IP-Adresse verwenden)**, und geben Sie die IP-Adresse, die Subnetzmaske und den Standardrouter an. 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 .

Konfigurieren des Kartenformats

Der Tür-Controller 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. Indem Sie das Kartenformat definieren, legen Sie fest, wie das System die Informationen interpretiert, die der Leser von den Karten und anderen Tokens erhält. Informationen darüber, welche Kartenformate der Leser unterstützt, finden Sie in den Anweisungen des Herstellers.

So aktivieren Sie Kartenformate:

1. Rufen Sie **Setup > Configure Card Formats (Setup > Kartenformate konfigurieren)** auf.
2. Wählen Sie eines oder mehrere Kartenformate aus, die die verbundenen Leser unterstützen.

So erstellen Sie ein neues Kartenformat:

1. Rufen Sie **Setup > Configure Card Formats (Setup > Kartenformate konfigurieren)** auf.
2. Klicken Sie auf **Add card format (Kartenformat hinzufügen)**.
3. Geben Sie im Dialogfenster **Add card format (Kartenformat hinzufügen)** einen Namen, eine Beschreibung und die Bitlänge des Kartenformats ein. Siehe *Beschreibungen der Kartenformate auf Seite 21*.
4. Klicken Sie auf **Add field map (Feldzuordnung hinzufügen)**, und geben Sie die erforderlichen Informationen in die Felder ein. Siehe *Feldzuordnungen auf Seite 21*.
5. Zum Hinzufügen von mehreren Feldzuordnungen wiederholen Sie den letzten Schritt.

Zum Anzeigen zusätzlicher Informationen für ein Element in der Liste **Card formats (Kartenformate)**, wie zum Beispiel der Beschreibung des Kartenformats und der Feldzuordnung, klicken Sie auf .

Zum Bearbeiten eines Kartenformats klicken Sie auf und bearbeiten Sie die Beschreibung des Kartenformats und die Feldzuordnung wie gewünscht. Klicken Sie anschließend auf **Save (Speichern)**.

Zum Löschen einer Feldzuordnung im Dialogfeld **Edit card format (Kartenformat bearbeiten)** oder **Add card format (Kartenformat hinzufügen)** klicken Sie auf

Zum Löschen eines Kartenformats klicken Sie auf .

Wichtig

- Jede Änderung an den Kartenformaten gilt für das gesamte System von Tür-Controllern.
- Kartenformate können nur aktiviert oder deaktiviert werden, wenn mindestens ein Tür-Controller im System mit mindestens einem Leser konfiguriert wurde. Siehe *Konfigurieren der Hardware auf Seite 13* und *Konfigurieren von Lesern und REX-Geräten auf Seite 16*.
- Zwei Kartenformate mit der gleichen Bitlänge können nicht gleichzeitig aktiviert sein. Wenn beispielsweise zwei Kartenformate mit 32 Bit definiert wurden, "Format A" und "Format B", und "Format A" aktiviert ist, können Sie "Format B" erst dann aktivieren, wenn Sie zuvor "Format A" deaktivieren.
- Wenn kein Kartenformat aktiviert wurde, können Sie die Identifikationstypen **Card raw only (Nur Karte mit Rohdaten)** und **Card raw and PIN (Karte mit Rohdaten und PIN)** verwenden, um eine Karte zu identifizieren und Benutzern Zugang zu gewähren.

Beschreibungen der Kartenformate

- **Name** (erforderlich) – Geben Sie einen beschreibenden Namen ein.
- **Description (Beschreibung)** – Geben Sie zusätzliche Informationen ein, sofern gewünscht. Diese Informationen werden nur in den Dialogfenstern **Edit card format (Kartenformat bearbeiten)** und **Add card format (Kartenformat hinzufügen)** angezeigt.
- **Bit length (Bitlänge)** (erforderlich) – Geben Sie die Bitlänge des Kartenformats ein. Es muss sich um einen nummerischen Wert zwischen 1 und 1000000000 handeln.

Feldzuordnungen

- **Name** (erforderlich) – Geben Sie den Namen der Feldzuordnung ohne Leerzeichen ein, z. B. `OddParity (UngeradeParität)`.

  Beispiele häufiger Feldzuordnungen:

  - `Parity (Parität)` – Paritätsbits werden zur Fehlererfassung verwendet. Paritätsbits werden in der Regel am Anfang oder Ende einer Binärcode-Zeichenfolge angefügt. Sie geben an, ob die Anzahl der Bits gerade oder ungerade ist.
  - `EvenParity (Gerade Parität)` – Gerade Paritätbits stellen sicher, dass die Zeichenfolge eine gerade Anzahl an Bits enthält. Die Bits mit dem Wert „1" werden gezählt. Ist die Anzahl bereits gerade, wird der Wert des Paritätsbits auf „0" festgelegt. Ist die Anzahl ungerade, wird der Wert auf „1" festgelegt, sodass die Gesamtanzahl eine gerade Zahl aufweist.
  - `OddParity (Ungerade Parität)` – Ungerade Paritätbits stellen sicher, dass die Zeichenfolge eine ungerade Anzahl an Bits enthält. Die Bits mit dem Wert „1" werden gezählt. Ist die Anzahl bereits ungerade, wird der Wert des ungeraden Paritätsbits auf „0" festgelegt. Ist die Anzahl gerade, wird der Wert auf „1" festgelegt, sodass die Gesamtanzahl eine ungerade Zahl aufweist.
  - `FacilityCode (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.
  - `CardNr (Kartennummer)` – Die Binärdaten der Kartennummer werden als ganze Zahlen entweder in der Byte-Reihenfolge „Little-Endian" (BinLE2Int) oder der Byte-Reihenfolge „Big-Endian" (BinBE2Int) codiert. Siehe unten.
  - `CardNrHex` – Die Binärdaten der Kartennummer werden als „hex-lowercase numbers" (Hexadezimalzahlen) entweder in der Byte-Reihenfolge „Little-Endian" (BinLE2hex) oder der Byte-Reihenfolge „Big-Endian" (BinBE2hex) codiert. Siehe unten.
- **Range (Bereich)** (erforderlich) – Geben Sie den Bit-Bereich der Feldzuordnung ein, z. B. 1, 2–17, 18–33 und 34.
- **Encoding (Codierung)** (erforderlich) – Wählen Sie den Codierungstyp jeder Feldzuordnung aus.
  - **BinLE2Int** – Die Binärdaten werden als ganze Zahlen in der Byte-Reihenfolge „Little-Endian" codiert. Eine ganze Zahl weist keine Dezimalstellen auf. Bei der Byte-Reihenfolge „Little-Endian" ist in einer Sequenz mehrerer Bytes das erste Byte das kleinste.
  - **BinBE2Int** – Die Binärdaten werden als ganze Zahlen in der Byte-Reihenfolge „Big-Endian" codiert. Eine ganze Zahl weist keine Dezimalstellen auf. Bei der Byte-Reihenfolge „Big-Endian" ist in einer Sequenz mehrerer Bytes das erste Byte das größte.
  - **BinLE2Hex** – Die Binärdaten werden als „hex-lowercase numbers" (Hexadezimalzahlen) in der Byte-Reihenfolge „Little-Endian" codiert. Das Hexadezimalsystem, ein Stellenwertsystem zur Basis 16, umfasst 16 eindeutige Zeichen: die Zahlen 0–9 und die Buchstaben a–f. Bei der Byte-Reihenfolge „Little-Endian" ist in einer Sequenz mehrerer Bytes das erste Byte das kleinste.
  - **BinBE2Hex** – Die Binärdaten werden als „hex-lowercase numbers" (Hexadezimalzahlen) in der Byte-Reihenfolge „Big-Endian" codiert. Das Hexadezimalsystem, ein Stellenwertsystem zur Basis 16, umfasst 16 eindeutige

Zeichen: die Zahlen 0–9 und die Buchstaben a–f. Bei der Byte-Reihenfolge „Big-Endian" ist in einer Sequenz mehrerer Bytes das erste Byte das größte.

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

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.

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

Auf der Seite „Manage Network Door Controllers in System" (Netzwerk-Tür-Controller im System verwalten) finden Sie folgende Bereiche:

- **System status for this controller (Systemstatus dieses Tür-Controllers)** – Zeigt den Systemstatus des Tür-Controllers an und ermöglicht es, zwischen System- und Standalone-Modus zu wechseln. Weitere Informationen finden Sie unter *Tür-Controller-Systemstatus auf Seite 22*.
- **Network door controllers in system (Netzwerk-Tür-Controller im System)** – Enthält Informationen über die Tür-Controller des Systems und Steuerelemente zum Hinzufügen oder Entfernen eines Controllers aus dem System. Weitere Informationen finden Sie unter *Verbundene Tür-Controller im System auf Seite 22*.

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 nicht Teil eines Systems und befindet sich nicht im Standalone-Modus)** – Der Controller wurde nicht als Teil eines Systems konfiguriert und befindet sich nicht im Standalone-Modus. Das heißt, dass der Tür-Controller von einem anderen Tür-Controller im selben Netzwerk zu einem System hinzugefügt werden kann. Aktivieren Sie den Standalone-Modus, wenn der Tür-Controller nicht zu einem System hinzugefügt werden soll.
- **This controller is set to standalone mode (Dieser Controller befindet sich im Standalone-Modus)** – Der Tür-Controller ist nicht Teil eines Systems. Er kann nicht von anderen Tür-Controllern 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. Deaktivieren Sie den Standalone-Modus, damit der Tür-Controller zum System hinzugefügt werden kann.
- **This controller part of a system (Dieser Controller ist Teil eines Systems)** – Der Tür-Controller ist Teil eines größeren Systems. In größeren Systemen werden Benutzer, Gruppen und Zeitpläne für alle verbundenen Controller 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 23*.
- Entfernen eines Tür-Controllers aus dem System, siehe *Entfernen von Tür-Controllern aus dem System auf Seite 23*.

Liste verbundener Tür-Controller

Der Bereich **Network door controllers in system (Netzwerk-Tür-Controller im System)** enthält auch eine Liste mit den folgenden ID- und Statusinformationen zu den Tür-Controllern im System:

- **Name** – Der vom Benutzer festgelegte Name des Tür-Controllers. Wenn der Administrator während der Hardwarekonfiguration keinen Namen angegeben hat, wird der Standardname angezeigt.
- **IP-Adresse**
- **MAC-Adresse**
- **Status** – Der Tür-Controller, über den Sie auf das System zugreifen, erhält den Status **This controller (Dieser Controller)**. Die anderen Tür-Controller im System erhalten den Status **Online**.

Klicken Sie auf die entsprechende IP-Adresse, um die Webseite für einen anderen Tür-Controller aufzurufen.

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

Beachten

- 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.

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 .
- 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 das System REX-Geräte, Sensoren oder andere Geräte umfasst, müssen diese ebenfalls getestet werden.
  - Testen Sie ggf. Manipulationsalarme.

Wenn die Ergebnisse von einem 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 .

- 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 56* und *Wartung auf Seite 52* 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 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. Weitere Informationen finden Sie unter *Erstellen und Bearbeiten von Benutzern auf Seite 31*.

Benutzer sind in diesem Zusammenhang nicht mit Administratoren zu verwechseln. Administratoren haben unbeschränkten Zugang zu allen Einstellungen. Im Zusammenhang mit der Verwaltung des Zugangskontrollsystems, den Produktwebseiten (AXIS Entry Manager), werden Administratoren gelegentlich als Benutzer bezeichnet. Weitere Informationen finden Sie unter *Benutzer auf Seite 44*.

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.

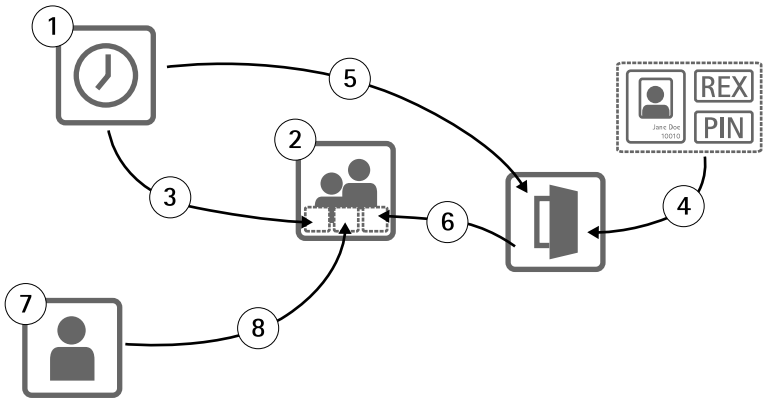
Um Benutzer zu Gruppen und Zutrittszeitpläne zu Türen zuzuweisen, ziehen Sie die Elemente in das jeweilige Ziel in den Listen **Groups (Gruppen)** und **Doors (Türen)**.

Beachten

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 26*.
2. Erstellen von Gruppen. Siehe *Seite 28*.
3. Zuordnen von Zugangszeitplänen zu Gruppen.
4. Hinzufügen von Identifizierungstypen zu Türen. Siehe *Seite 28* und *Seite 29*.
5. Zuordnen von Zugangszeitplänen zu Identifikationstypen.
6. Zuordnen von Türen zu Gruppen.
7. Erstellen von Benutzern. Siehe *Seite 31*.

8. Hinzufügen von Benutzern zu Gruppen.

Anwendungsbeispiele für diese Vorgehensweise finden Sie unter *Beispiele für Kombinationen von Zugangszeitplänen auf Seite 33*.

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 finden Sie unter *Zugangszeitplantypen auf Seite 26*.

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 finden Sie unter *Zugangszeitplantypen*.
5. Klicken Sie auf **Save (Speichern)**.

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

Zum Anzeigen des Kalenders für einen Zugangszeitplan klicken Sie auf .

Zum Bearbeiten des Namens eines Zugangszeitplans oder eines Ereignisses im Zeitplan klicken Sie auf und nehmen Sie die Änderungen vor. Klicken Sie anschließend auf **Save (Speichern)**.

Zum Löschen eines Zugangszeitplans klicken Sie auf .

Beachten

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 Zugang zu Türen besteht. Typische Additionszeitpläne sind Geschäftszeiten, Sprechstunden, Zeiten nach Geschäftsschluss oder Nachtstunden.
- **Subtraktionszeitpläne** – Ausnahmen zu den regulären Zugangszeitplänen. Diese werden überwiegend dazu genutzt, während eines bestimmten Zeitraums 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 Leser Benutzern Zugang zu 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 29*.

- **Gruppenzeitpläne** – Legen fest wann, jedoch nicht wie Mitglieder einer Gruppe Zugang zu einer Tür erhalten. 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 28*.

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 33*.

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*.
6. Wählen Sie für wiederkehrende Zeitplanereignisse die Parameter **Recurrence pattern (Wiederholungsmuster)** und **Range of recurrence (Wiederholungszeitraum)** aus. Siehe *Optionen für Wiederholungsmuster* und *Optionen für den Wiederholungszeitraum*.
7. Klicken Sie auf **Save (Speichern)**.

Zeitoptionen

Es stehen folgende Zeitoptionen zur Verfügung:

- **All day (Ganztägig)** – Wählen Sie diese Option für Ereignisse, die alle 24 Stunden eines Tages belegen sollen. Geben Sie anschließend das gewünschte **Start**datum ein.
- **Start** – Klicken Sie in das Zeitfeld, und wählen Sie die Uhrzeit aus. Klicken Sie ggf. in das Datumsfeld, und wählen Sie Monat, Tag und Jahr aus. Sie können das Datum auch direkt in das Feld eingeben.
- **End (Ende)** – Klicken Sie in das Zeitfeld, und wählen Sie die Uhrzeit aus. Klicken Sie ggf. in das Datumsfeld, und wählen Sie Monat, Tag und Jahr aus. Sie können das Datum auch direkt in das Feld eingeben.

Optionen für Wiederholungsmuster

Es stehen folgende Optionen für Wiederholungsmuster zur Verfügung:

- **Yearly (Jährlich)** – Die Wiederholung erfolgt jährlich.
- **Weekly (Wöchentlich)** – Die Wiederholung erfolgt wöchentlich.
- Wiederholung wöchentlich am **Monday (Montag)**, **Tuesday (Dienstag)**, **Wednesday (Mittwoch)**, **Thursday (Donnerstag)**, **Friday (Freitag)**, **Saturday (Samstag)** oder **Sunday (Sonntag)** – Wählen Sie den Tag für die Wiederholung aus.

Optionen für den Wiederholungszeitraum

Es stehen folgende Optionen für den Wiederholungszeitraum zur Verfügung:

- **First occurrence (Erstes Auftreten)** – Klicken Sie in das Datumsfeld, und wählen Sie Monat, Tag und Jahr aus. Sie können das Datum auch direkt in das Feld eingeben.
- **No end date (Kein Enddatum)** – Die Wiederholungen erfolgen zeitlich unbegrenzt.
- **End by (Ende am)** – Klicken Sie in das Datumsfeld, und wählen Sie Monat, Tag und Jahr aus. 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 finden Sie unter *Erstellen und Bearbeiten von Benutzern auf Seite 31*.

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 28*.
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, klicken Sie auf  .

Zum Bearbeiten eines Gruppennamens oder Gültigkeitsdatums klicken Sie auf  , und nehmen Sie die Änderungen vor. Klicken Sie anschließend auf **Save (Speichern)**.

Zum Verifizieren, wann und wie eine Gruppe Zugang an bestimmten Türen erhält, klicken Sie auf  .

Zum Löschen einer Gruppe, von Gruppenmitgliedern, Türen oder Zeitplänen einer Gruppe klicken Sie auf  .

Gruppenzugangsdaten

Es stehen folgende Zugangsdaten für Gruppen zur Verfügung:

- **Name** (erforderlich)
- **Valid from (Gültig ab)** und **Valid to (Gültig bis)** – Geben Sie hier das Start- und Enddatum für die Gültigkeit der Zugangsdaten einer Gruppe ein. Klicken Sie in das Datumsfeld, und wählen Sie Monat, Tag und Jahr aus. Sie können das Datum auch direkt in das Feld eingeben.

Beachten

Sie müssen das Feld **Name** für die Gruppe ausfüllen, um das Profil zu speichern.

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 29* und *Erstellen und Bearbeiten von Zugangszeitplänen auf Seite 26*.

Zugangsverwaltung

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. Klicken Sie in der Liste **Doors (Türen)** neben der entsprechenden Tür auf .
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 28*.
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 29*.

   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 für eine vorübergehende Freigabe des Zugangs klicken Sie ggf. auf die manuellen Türfunktionen. Siehe *Verwenden der manuellen Türfunktionen auf Seite 30*.

Zum Anzeigen weiterer Informationen für ein Element in der Liste **Doors (Türen)**, klicken Sie auf .

Zum Bearbeiten eines Tür- oder Lesernamens klicken Sie auf , und nehmen Sie die Änderungen vor. Klicken Sie anschließend auf **Save (Speichern)**.

Zum Überprüfen des Lesers, des Identifizierungstyps und der Zugangszeitplankombinationen klicken Sie auf .

Zum Überprüfen der Funktion von Schlössern, die mit den Türen verbundenen sind, klicken Sie auf die Überprüfungssteuerelemente. Siehe *Überprüfungssteuerelemente auf Seite 18*.

Zum Löschen von Identifizierungstypen oder Zugangszeitplänen klicken Sie auf .

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 31*.

Folgende Identifizierungsmöglichkeiten stehen zur Verfügung:

- **Nur Kartenummer** – Der Benutzer erhält Zugang 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. Ziehen Sie die Karte durch einen angeschlossenen Leser, wählen Sie den Leser in der Liste aus, und klicken Sie auf **Retrieve (Abrufen)**.
- **Nur Karte mit Rohdaten** – Der Benutzer erhält Zugang 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 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.

- **Nur PIN** – Der Benutzer erhält Zugang mit einer vierstelligen Identifikationsnummer (PIN).
- **Kartenummer und PIN** – Der Benutzer erhält Zugang 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).
- **Karte mit Rohdaten und PIN** – Der Benutzer erhält Zugang mit der Kombination aus einer vom Leser 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.

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. Klicken Sie auf  . Diese Schaltfläche befindet sich neben dem zu bearbeitenden Element in der Liste **Doors (Türen)**.
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, klicken Sie auf  .

Zum Löschen einer geplanten Entriegelung oder zum Bearbeiten des Zeitplans klicken Sie auf  .

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. Klicken Sie in der Liste **Doors (Türen)** neben der entsprechenden Tür auf  .
3. Klicken Sie auf die erforderliche Türfunktion. Siehe *Manuelle Türfunktionen auf Seite 31*.

Beachten

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)** – Zur Überprüfung des aktuellen Status des Türmonitors, der Türalarme und der Schlösser.
- **Access (Zugang)** – Zur Gewährung von Zugang an einer Tür. Es gilt die entsprechende Zugangsdauer. Siehe *Konfigurieren von Schlössern und Türmonitoren auf Seite 14*.
- **Unlock (Entriegeln)** (bei einem Schloss) oder **Unlock both locks (Beide Schlösser entriegeln)** (bei zwei Schlössern) – Zum Entriegeln der Tür. Die Tür wird entriegelt, bis Sie auf **Lock (Verriegeln)** bzw. **Lock both locks (Beide Schlösser verriegeln)** klicken, ein durch einen Zeitplan festgelegter Status aktiviert oder der Tür-Controller neu gestartet wird.
- **Lock (Verriegeln)** (bei einem Schloss) oder **Lock both locks (Beide Schlösser verriegeln)** (bei zwei Schlössern) – 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.

Erstellen und Bearbeiten von Benutzern

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 finden Sie unter *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 31*.
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 28*.

Klicken Sie zum Erweitern eines Eintrags in der Liste **Users (Benutzer)** und zum Anzeigen der Zugangsdaten eines Benutzers auf  .

Wenn Sie nach einem bestimmten Benutzer suchen möchten, geben Sie im Feld zum Filtern von Benutzern einen Filter ein. Wenn Sie nach genauen Übereinstimmungen suchen möchten, setzen Sie um den Filtertext doppelte Anführungszeichen, z. B. "John" oder "potter, virginia".

Zum Bearbeiten der Zugangsdaten eines Benutzers klicken Sie auf  und nehmen die gewünschten Änderungen vor. Klicken Sie anschließend auf **Save (Speichern)**.

Zum Löschen eines Benutzers klicken Sie auf  .

Zugangsdaten für Benutzer

Es stehen folgende Zugangsdaten für Benutzer zur Verfügung:

- **First name (Vorname)** (erforderlich)
- **Last name (Nachname)**

- **Valid from (Gültig ab)** und **Valid until (Gültig bis)** – Geben Sie hier das Start- und Enddatum für die Gültigkeit der Zugangsdaten eines Benutzers ein. Klicken Sie in das Datumsfeld, und wählen Sie Monat, Tag und Jahr aus. Sie können das Datum auch direkt in das Feld eingeben.
- **Suspend User (Benutzer sperren)** – Wählen Sie diese Option zum Sperren eines Benutzers aus. Wenn Sie einen Benutzer sperren, wird diesem bei sämtlichen Türen des Systems der Zugang verweigert. Deaktivieren Sie diese Option, um dem Benutzer den Zugang wieder zu ermöglichen. Die Sperrung ist als vorübergehende Einstellung gedacht. Wenn Sie einem Benutzer dauerhaft den Zugang verweigern möchten, sollten Sie das Benutzerprofil löschen.
- **PIN** (erforderlich anstelle einer Kartennummer oder einer Karte mit Rohdaten) – Geben Sie den vierstelligen persönlichen Identifizierungscode (PIN) ein, der von dem Benutzer ausgewählt oder diesem zugewiesen wurde.
- **Card number (Kartennummer)** (erforderlich anstelle einer PIN oder Karte mit Rohdaten) – Geben Sie die Kartennummer ein. 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 Leser, wählen Sie den Leser in der Liste aus, und klicken Sie auf **Retrieve (Abrufen)**.
- **Card raw (Karte mit Rohdaten)** (erforderlich anstelle von PIN oder Kartennummer) – Geben Sie die Daten der Karte mit Rohdaten ein. 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.

Beachten

- Zum Speichern des Profils eines Benutzers müssen Sie seinen **Vornamen** oder **Nachnamen** angeben und entweder die **PIN**, die **Kartennummer** oder die Daten der **Karte mit Rohdaten**.
- Die Schaltfläche **Retrieve (Abrufen)** ist nur verfügbar, wenn die Konfiguration der Hardware abgeschlossen wurde und einer oder mehrere Leser 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. Trennen Sie Werte durch Kommas, nicht durch Leerzeichen, und trennen Sie die einzelnen Benutzer durch Zeilenumbrüche.

Beispiel

```
virginia,potter,1212,56781234
jane,doe,1234,12345678
leia,garfunkel,8545,45673258
ororo,wolf,3548,78542654
john,doe,5435,87654321
```

So importieren Sie Benutzer:

1. Wechseln Sie zu **Setup > Import Users (Setup > Benutzer importieren)**.
2. Suchen Sie die CSV- oder TXT-Datei mit der Benutzerliste, und wählen Sie diese aus.
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)**
- **Unassigned (nicht zugeordnet)** – Werte, die nicht importiert werden. Wählen Sie diese Option aus, wenn Sie eine bestimmte Spalte überspringen möchten.

Weitere Informationen zu Zugangsdaten finden Sie unter *Erstellen und Bearbeiten von Benutzern*.

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 25* beschriebenen Vorgehensweise.

Beispiel
So erstellen Sie eine Kombination von Zeitplänen, bei der

- Wachpersonal jederzeit Zugang an einer Tür erhält,
  - wobei während der Tagschicht (Montag–Freitag, 6 bis 16 Uhr) die Karte,
  - außerhalb der Tagschicht Karte und PIN zur Identifizierung erforderlich sind, während
- weiteres Personal der Tagschicht ausschließlich zu den Zeiten der Tagschicht Zugang zu der Tür hat
  - und zur Identifizierung die Karte erforderlich ist:

1. Erstellen Sie einen **Addition schedule (Additionszeitplan)** mit dem Namen **Tagschicht**. Siehe *Seite 26*.
2. Erstellen Sie ein **Schedule item (Zeitplanereignis)** mit den Zeitangaben Montag–Freitag, 06:00–16:00.
3. Erstellen Sie zwei Gruppen, eine **Gruppe** mit der Bezeichnung **Wachpersonal** und eine **Gruppe** mit der Bezeichnung **Personal Tagschicht**. Siehe *Seite 28*.
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 31*.

Beispiel

So erstellen Sie eine Kombination von Zeitplänen, bei der

- Wachpersonal jederzeit Zugang an einer Tür erhält,
  - wobei während der Tagschicht (Montag–Freitag, 6 bis 16 Uhr) die Karte,
  - außerhalb der Tagschicht Karte und PIN zur Identifizierung erforderlich sind, während
- 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 26*.
2. Erstellen Sie ein **Schedule item (Zeitplanereignis)** mit den Zeitangaben Montag–Freitag, 06:00–16:00.
3. Erstellen Sie einen **Subtraction schedule (Subtraktionszeitplan)** mit dem Namen **Nächte und Wochenenden**.
4. Erstellen Sie ein **Schedule item (Zeitplanereignis)** für Nächte und Wochenenden mit den Zeitangaben Sonntag–Samstag, 16:00–06:00.
5. Ziehen Sie den vordefinierten Zugangszeitplan **Always (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 28*.
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 31*.

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 35*.
- Anzeigen des Alarmprotokolls. Siehe *Seite 35*.
- Konfigurieren der Ereignis- und Alarmprotokolle. Siehe *Seite 36*.

Außerdem können Alarme so konfiguriert werden, dass sie Aktionen wie E-Mail-Benachrichtigungen auslösen. Weitere Informationen finden Sie unter *Einrichten von Aktionsregeln auf Seite 37*.

Anzeigen des Ereignisprotokolls

Rufen Sie **Event Log (Ereignisprotokoll)** auf, um protokollierte Ereignisse anzuzeigen. Wenn „Global events" (Globale Ereignisse) aktiviert ist, können Sie das Ereignisprotokoll jedes Tür-Controllers im System öffnen. Weitere Informationen zu globalen Ereignissen finden Sie unter *Konfigurieren der Ereignis- und Alarmprotokolle auf Seite 36*.

Klicken Sie zum Erweitern eines Elements im Ereignisprotokoll und Anzeigen der Ereignisdetails auf ▶.

Mithilfe von Filtern können Sie im Ereignisprotokoll einfacher bestimmte Ereignisse finden. Wählen Sie zum Filtern der Liste einen oder mehrere Ereignisprotokollfilter aus, und klicken Sie auf **Refresh list (Liste aktualisieren)**. Weitere Informationen finden Sie unter *Ereignisprotokollfilter auf Seite 35*

Als Administrator sind Sie möglicherweise an bestimmten Ereignissen besonders interessiert. Daher können Sie auswählen, welche Ereignisse für welchen Controller protokolliert werden. Weitere Informationen finden Sie unter *Optionen für Ereignisprotokolle auf Seite 36*

Ereignisprotokollfilter

Sie können die Inhalte von Ereignisprotokollen mithilfe der folgenden Filter eingrenzen:

- Thema – Wählen Sie das Ereignis in der Liste **Filter by topics (Nach Thema filtern)** aus.
- Tür-Controller – Wählen Sie den Controller in der Liste **Filter by controller (Nach Controller filtern)** aus.
- Datum und Uhrzeit – Wählen Sie unter **Filter by date and time (Nach Datum und Uhrzeit filtern)** die Option **Based on date and time interval (Nach Datum und Zeitraum)** aus, und geben Sie den gewünschten Zeitraum ein.

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 36*.

Zum Erweitern eines Ereignisses im Alarmprotokoll und Anzeigen der Alarmdetails, wie beispielsweise der Bezeichnung und des Status der Tür, klicken Sie auf ▶.

Zum Entfernen eines Alarms aus der Liste nach dem Überprüfen der Alarmursache klicken Sie auf **Acknowledge (Bestätigen)**.

Administrator müssen festlegen können, welche Ereignisse einen Alarm auslösen sollen und für welche Controller. Weitere Informationen finden Sie unter *Optionen für Alarmprotokolle*.

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 finden Sie unter *Einrichten von Aktionsregeln auf Seite 37*.

Optionen für Ereignisprotokolle

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

Für das Protokollieren von Ereignissen stehen folgende Optionen zur Verfügung:

- **No logging (Keine Protokollierung)** – Mit dieser Option wird die Protokollierung von Ereignissen deaktiviert. Das Ereignis wird nicht registriert oder in das Ereignisprotokoll aufgenommen.
- **Log for all controllers (Alle Controller protokollieren)** – Mit dieser Option wird die Protokollierung von Ereignissen für alle Tür-Controller aktiviert. Das Ereignis wird für alle Controller registriert und in das Ereignisprotokoll aufgenommen.
- **Log for selected controllers (Ausgewählte Controller protokollieren)** – Mit dieser Option wird die Protokollierung von Ereignissen für bestimmte Tür-Controller 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

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

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 nicht in das Alarmprotokoll aufgenommen.
- **Log for all controllers (Alarm für alle Controller protokollieren)** – Alarmprotokoll für alle Tür-Controller 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 Tür-Controller aktivieren. Das Ereignis löst einen Alarm aus und wird in das Alarmprotokoll aufgenommen.

  Klicken Sie in der Liste **Configure alarm logging (Alarmprotokoll konfigurieren)** unter dem Alarmprotokollelement, das Sie aktivieren möchten, auf **Select controllers (Controller auswählen)**. Das Dialogfeld **Device Specific Alarm Logging**

(Gerätspezifisches Alarmauslösung) wird geöffnet. Wählen Sie unter **Trigger alarm (Alarm auslösen)** die Tür-Controller aus, deren Alarme protokolliert werden sollen, und klicken Sie auf **Save (Speichern)**.

Einrichten von Aktionsregeln

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.

Weitere Informationen zu den verfügbaren Auslösern und Aktionen finden Sie unter *Auslöser auf Seite 38* und *Aktionen auf Seite 40*.

Im folgenden Beispiel wird die Einrichtung einer Aktionsregel zum Senden einer E-Mail-Benachrichtigung beschrieben, wenn ein Alarm ausgelöst wird.

1. Konfigurieren Sie die Alarme. Siehe .
2. Wechseln Sie zu **Setup > Additional Controller Configuration > Events > Action Rules (Setup > Zusätzliche Controller-Konfiguration > Ereignisse > Aktionsregeln)**, und klicken Sie auf **Add (Hinzufügen)**.
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. Wählen Sie in der Dropdown-Liste **Type (Typ)** unter **Actions (Aktionen)** die Option **Send Notification (Benachrichtigung senden)** aus.
7. Wählen Sie in der Dropdown-Liste einen E-Mail-Empfänger aus. Siehe *Hinzufügen von Empfängern auf Seite 40*.

Im folgenden Beispiel wird die Einrichtung einer Aktionsregel zum Aktivieren eines Ausgangs-Ports beschrieben, 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.

Weitere Informationen finden Sie in der Online-Hilfe .

Auslöser

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

- **Access Point**
  - **Access Point Enabled (Access Point aktiviert)** – Löst die Aktionsregel aus, wenn ein Access Point-Gerät wie ein Reader oder REX-Gerät konfiguriert wird, z. B. wenn die Hardwarekonfiguration abgeschlossen oder ein Identifizierungstyp hinzugefügt wird.
- **Konfiguration**
  - **Access Point Changed (Access Point geändert)** – Löst die Aktionsregel aus, wenn die Konfiguration eines Access Point-Geräts wie eines Readers oder REX-Geräts geändert wird, z. B. wenn Hardware konfiguriert oder ein Identifizierungstyp bearbeitet wird und dabei die Art des Zugangs zu einer Tür geändert wird.
  - **Access Point Removed (Access Point entfernt)** – Löst die Aktionsregel aus, wenn die Hardwarekonfiguration eines Access Point-Geräts wie eines Readers 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 vom System entfernt wird.
  - **Door Changed (Tür geändert)** – Löst die Aktionsregel aus, wenn die Konfigurationseinstellungen der Tür, beispielsweise der Türname, geändert werden oder eine Tür zum System hinzugefügt wird. Dies kann beispielsweise zum Senden einer Benachrichtigung verwendet werden, wenn eine Tür installiert und konfiguriert wird.
  - **Door Removed (Tür entfernt)** – Löst die Aktionsregel aus, wenn eine Tür vom System entfernt wird. Dies kann beispielsweise zum Senden einer Benachrichtigung verwendet werden, wenn eine Tür vom System entfernt wird.
- **Tür**
  - **Door Alarm (Türalarm)** – Löst die Aktionsregel aus, wenn der Türmonitor anzeigt, dass die Tür aufgebrochen wurde, zu lange geöffnet ist oder einen anderen Fehler aufweist. Dies kann beispielsweise zum Senden einer Benachrichtigung verwendet werden, wenn die Tür aufgebrochen wird.
  - **Door Double-Lock Monitor (Türdoppelschloss-Monitor)** – Löst die Aktionsregel aus, wenn der Zustand des sekundären Schlosses zu verriegelt oder entriegelt wechselt.
  - **Door Lock Monitor (Türschloss-Monitor)** – Löst die Aktionsregel aus, wenn der Zustand des normalen Schlosses zu verriegelt oder entriegelt wechselt. Beispielsweise wird ein Fehler ausgelöst, wenn der Türmonitor erkennt, dass die Tür geöffnet ist, obwohl das Schloss verriegelt ist.
  - **Door Mode (Türmodus)** – Löst die Aktionsregel aus, wenn der Zustand der Tür geändert wird, beispielsweise, wenn auf die Tür zugegriffen wurde, die Tür blockiert wurde oder sich die Tür im abgesperrten Modus befindet. Ausführlichere Beschreibungen dieser Modi finden Sie in der Online-Hilfe.

- **Door Monitor (Türmonitor)** – Löst die Aktionsregel aus, wenn der Zustand des Türmonitors geändert wird. Dies kann beispielsweise zum Senden einer Benachrichtigung verwendet werden, wenn ein Türmonitor erkennt, dass die Tür geöffnet oder geschlossen wurde.

- **Door Tamper (Türmanipulation)** – Löst die Aktionsregel aus, wenn der Türmonitor eine Unterbrechung der Verbindung erkennt, z. B. wenn die Drähte zum Türmonitor durchgeschnitten werden. Stellen Sie bei Verwendung dieses Auslösers sicher, dass **Enable supervised inputs (Überwachte Eingänge aktivieren)** ausgewählt ist und dass Abschlusswiderstände an den entsprechenden Eingangs-Ports der Türanschlüsse angebracht sind. Weitere Informationen finden Sie unter

- **Door Warning (Türwarnung)** – Löst die Aktionsregel aus, bevor der Alarm zu einer zu lange geöffneten Tür ausgelöst wird. Dies kann beispielsweise zum Senden eines Warnsignals verwendet werden, dass der Tür-Controller 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 zu der Zeit für eine zu lange geöffnete Tür finden Sie unter .

- **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 die 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 die 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 die 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**

  - **Casing Open (Gehäuse geöffnet)** – Löst die Aktionsregel aus, wenn die Abdeckung des Tür-Controllers geöffnet bzw. wenn der Tür-Controller von der Wand oder der Decke entfernt wird. Dies kann beispielsweise zum Senden einer Benachrichtigung verwendet werden, wenn das Gehäuse zur Wartung geöffnet oder das Gehäuse manipuliert wurde.

  - **Network (Netzwerk)** – Löst die Aktionsregel aus, wenn die Netzwerkverbindung abgebrochen ist. Wählen Sie **Yes (Ja)** aus, um die Aktionsregel auszulösen, wenn die Netzwerkverbindung abgebrochen ist. Wählen Sie **No (Nein)** aus, um die Aktionsregel auszulösen, wenn die Netzwerkverbindung wiederhergestellt wurde.

  - **Peer Connection (Peer-Verbindung)** – Löst die Aktionsregel aus, wenn das Axis Produkt eine Verbindung mit einem anderen Tür-Controller hergestellt hat, die Netzwerkverbindung zwischen den Geräten abgebrochen ist oder die Koppelung der Tür-Controller fehlgeschlagen ist. Dies kann beispielsweise zum Senden einer Benachrichtigung verwendet werden, wenn die Netzwerkverbindung eines Tür-Controllers abgebrochen ist.

- **Eingangssignal**

  - **Digital Input Port (Digitaler Eingangsport)** – Löst die Regel aus, wenn ein E/A-Port ein Signal von einem verbundenen Gerät empfängt. Siehe *E/A-Ports auf Seite 52*.

  - **Manual Trigger (Manuelle Auslösung)** – Löst die Aktionsregel aus, wenn die manuelle Auslösung aktiviert wird. Dies kann von einem Client wie einem Zugangsverwaltungssystem über die VAPIX®-API (Application Programming Interface) verwendet werden, um die Aktionsregel manuell zu starten oder anzuhalten.

  - **Virtual Inputs (Virtuelle Eingänge)** – Löst die Aktionsregel aus, wenn der Zustand eines virtuellen Eingangs geändert wird. 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 in der Benutzeroberfläche des Verwaltungssystems verbunden werden.

- **Zeitplan**
  - **Interval (Intervall)** – Löst die Aktionsregel zur Startzeit des Zeitplans aus und bleibt aktiv, bis die Endzeit des Zeitplans erreicht wird.
  - **Pulse (Takt)** – Löst die Aktionsregel aus, wenn ein einmaliges Ereignis auftritt, also ein Ereignis, das zu einem bestimmten Zeitpunkt auftritt und nicht andauert.
- **System**
  - **System Ready (System bereit)** – Löst die Aktionsregel aus, wenn das System bereit ist. Das Axis Produkt kann beispielsweise den Systemstatus erkennen und eine Benachrichtigung senden, wenn das System gestartet wurde.

    Wählen Sie **Yes (Ja)** aus, um die Aktionsregel auszulösen, wenn sich das Produkt im Status „Bereit" befindet. Beachten Sie, dass die Regel nur ausgelöst wird, wenn alle erforderlichen Dienste, wie das Ereignissystem, gestartet wurden.
- **Uhrzeit**
  - **Recurrence (Wiederholung)** – Löst die Aktionsregel durch Überwachen der von Ihnen 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 finden Sie unter *Einrichten von Wiederholungen auf Seite 42*.
  - **Use Schedule (Zeitplan verwenden)** – Löst die Regel gemäß dem ausgewählten Zeitplan aus. Siehe *Erstellen von Zeitplänen auf Seite 41*.

Aktionen

Zu den verfügbaren **Aktionen** gehören:

- **Output Port (Ausgangs-Port)** – Aktivieren eines E/A-Ports zum Steuern eines externen Geräts.
- **Send Notifications (Benachrichtigungen 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 in der Dropdown-Liste eine **LED Color (LED-Farbe)** aus.

Hinzufügen von Empfängern

Das Produkt kann Nachrichten senden, um Administratoren über Ereignisse und Alarme zu benachrichtigen. Damit das Produkt Benachrichtigungen senden kann, muss mindestens ein Empfänger definiert werden. Informationen zu den verfügbaren Optionen finden Sie unter .

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 Empfänger zur Verfügung:

- HTTP
- HTTPS
- E-Mail
- TCP

Einrichten der E-Mail-Empfänger

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

Beachten

Einige E-Mail-Anbieter verwenden Sicherheitsfilter, mit denen verhindert wird, dass Benutzer eine große Anzahl von Anhängen erhalten oder anzeigen, geplante E-Mails erhalten usw. 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. Geben Sie die Benutzer-ID und das Kennwort für das E-Mail-Konto ein.
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-Serveradresse, den Port und die Authentifizierungsmethode an. Wählen Sie optional **Use encryption (Verschlüsselung verwenden)** aus, um E-Mails über eine verschlüsselte Verbindung zu senden. Das Serverzertifikat kann mit dem für das Axis Produkt verfügbaren Zertifikaten validiert werden. Weitere Informationen zum Hochladen von Zertifikaten finden Sie unter *Certificates (Zertifikate) auf Seite 45*.

Erstellen von Zeitplänen

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.

Einrichten von Wiederholungen

Mit Wiederholungen werden Aktionsregeln wiederholt ausgelöst, beispielsweise alle 5 Minuten oder jede Stunde.

So richten Sie eine Wiederholung ein:

1. Wechseln Sie zu **Setup > Additional Controller Configuration > Events > Recurrences (Setup > Zusatzkontrollenkonfiguration > Ereignisse > Wiederholungen)**, und klicken Sie auf **Add (Hinzufügen)**.
2. Geben Sie einen beschreibenden Namen und das Wiederholungsmuster ein.
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.

Table 5.1. In der folgenden Tabelle sind die Ereignisse aufgeführt, die im Tür-Controller vorkonfiguriert sind und bei denen Leserfeedback und typische Feedbacksignale ausgelöst werden.

Ereignis	Doppelte Wiegand-LED	Einfache Wiegand-LED	OSDP	Signaltongeber-Muster	Status
Idle (Leerlauf)	Aus	Rot	Rot	Still	Normal
RequirePIN (PIN erforderlich)	Rot-grün blinkend	Rot-grün blinkend	Rot-grün blinkend	Zwei kurze Signaltöne	PIN erforderlich
AccessGranted (Zugang gewährt)	Grün	Grün	Grün	Ein kurzer Signalton	Zugang gewährt
AccessDenied (Zugang verweigert)	Rot	Rot	Rot	Ein langer Signalton	Zugang verweigert

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 43*.

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.

   Setzen Sie zum Suchen nach exakten Übereinstimmungen um den Filtertext doppelte Anführungszeichen, z. B. "John".
4. Wenn Sie die Berichtselemente in einer anderen Reihenfolge anzeigen möchten, klicken Sie in der entsprechenden Spalte auf ⬍. Wechseln Sie mithilfe der Sortierschaltflächen zwischen Standard- und umgekehrter Reihenfolge.

   ▲ Zeigt die Elemente in der Standardreihenfolge (aufsteigend) an.

   ▼ Zeigt die Elemente in der umgekehrten Reihenfolge (absteigend) an.
5. Klicken Sie auf **Print selected columns (Ausgewählte Spalten drucken)**.

Klicken Sie zum Exportieren eines Berichts auf **Export CSV file (CSV-Datei exportieren)**.

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) im standardmäßigen Downloadordner gespeichert. Den Downloadordner können Sie in den Benutzereinstellungen des Webbrowsers festlegen.

Berichtstypen

Es stehen folgende Berichtstypen zur Verfügung:

- Zugangszeitpläne. Weitere Informationen zu Arten von Zugangszeitplänen und zugehörigen Optionen finden Sie unter *Seite 26* und *Seite 27*.
- Gruppen. Weitere Informationen zu Gruppen finden Sie unter *Seite 28*.
- Türen. Weitere Informationen zu Türen und Identifikationstypen finden Sie unter *Seite 28* und *Seite 29*.
- Benutzer. Weitere Informationen zu Benutzerzugangsdaten finden Sie unter *Seite 31*.
- Tür-Controller. Weitere Informationen über verbundene Controller und deren ID-Typen finden Sie unter *Seite 23*. Weitere Informationen über Zeitoptionen für Türmonitore finden Sie unter *Seite 15*.

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. Ein Administrator kann weitere Benutzer einrichten, indem er Benutzernamen und Kennwörter ausgibt.

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

Administrator – Unbeschränkter Zugang zu allen Einstellungen; kann andere Benutzer hinzufügen, ändern und entfernen.

Wählen Sie unter **HTTP/RTSP Password Settings (HTTP/RTSP-Kennworteinstellungen)** den zulässigen Kennworttyp aus. 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.

Heben Sie die Auswahl der Option **Enable Basic Setup (Basiskonfiguration aktivieren)** auf, damit das Menü „Basic Setup (Basiskonfiguration)" ausgeblendet wird. Die Basiskonfiguration bietet schnellen Zugriff auf Einstellungen, die vor der Verwendung des Axis Produkts vorgenommen werden sollten.

ONVIF

ONVIF (Open Network Video Interface Forum) ist ein globaler Schnittstellenstandard, der Endbenutzern, Integratoren, Beratern und Herstellern die Nutzung der Vorteile von Netzwerkvideotechnologie erleichtert. ONVIF bietet Kompatibilität zwischen Produkten unterschiedlicher Hersteller, erhöhte Flexibilität, verringerte Kosten und zukunftssichere Systeme.

Beim Erstellen eines Benutzers wird ONVIF-Kommunikation automatisch 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

Der IP-Adressfilter wird auf der Seite **Setup > Additional Controller Configuration > System Options > Security > IP Address Filter (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Sicherheit > IP-Adressfilter)** aktiviert. 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 erstellen und zu installieren, wechseln Sie zu **Setup > Additional Controller Configuration(Zusätzliche Controller-Konfiguration) > System Options (Systemoptionen) > Security (Sicherheit) > Certificates (Zertifikat)**. Siehe *Certificates (Zertifikate) auf Seite 45*.

So aktivieren Sie HTTPS auf dem Axis Produkt:

1. Wechseln Sie zu **Setup > Additional Controller Configuration (Zusätzliche Controller-Konfiguration) > System Options (Systemoptionen) > Security (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 verschiedenen Benutzergruppen finden Sie in der **HTTPS Connection Policy (HTTPS-Verbindungsrichtlinie.**
5. Klicken Sie auf **Save (Speichern)**, um die Einstellungen zu aktivieren.

Um über das gewünschte Protokoll auf das Axis Produkt zuzugreifen, geben Sie in das Adressfeld des Browsers `https://` bzw. `http://` ein.

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

IEEE 802.1X

IEEE 802.1X ist ein Standard für portbasierte Netzwerk-Zugangskontrolle, die eine sichere Authentifizierung für drahtgebundene und drahtlose Netzwerkgeräte 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 erstellen und zu installieren, wechseln Sie zu **Setup > Additional Controller Configuration(Zusätzliche Controller-Konfiguration) > System Options (Systemoptionen) > Security (Sicherheit) > Certificates (Zertifikat)**. Siehe *Certificates (Zertifikate) auf Seite 45*. Viele CA-Zertifikate sind vorinstalliert.

So ermöglichen Sie den Zugriff des Produkts auf ein mit IEEE 802.1X geschütztes Netzwerk

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. Wählen Sie unter **Settings (Einstellungen)** die EAPOL-Version aus, und geben Sie die EAP-Identität des Clientzertifikats an.
4. Markieren Sie das Kontrollkästchen zum Aktivieren von IEEE 802.1X, und klicken Sie auf **Save (Speichern)**.

Beachten

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 46*.

Certificates (Zertifikate)

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

Server-/Clientzertifikate – So zertifizieren Sie das Axis Produkt

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.

Beachten

Beim Zurücksetzen des Produkts auf die Werkseinstellungen werden die installierten Zertifikate mit Ausnahme der vorinstallierten CA-Zertifikate gelöscht. Gelöschte vorinstallierte CA-Zertifikate werden erneut installiert.

Ein **Server-/Clientzertifikat** kann selbstsigniert oder von einer Zertifizierungsstelle (Certificate Authority, CA) ausgegeben worden sein. Ein selbstsigniertes Zertifikat bietet begrenzten Schutz und kann verwendet werden, bevor Sie Ihr CA-Zertifikat erhalten haben.

So installieren Sie ein selbstsigniertes Zertifikat

1. Wechseln Sie zu **Setup > Additional Controller Configuration (Zusätzliche Controller-Konfiguration) > System Options (Systemoptionen) > Security (Sicherheit) > Certificates (Zertifikat)**.
2. Klicken Sie auf die Schaltfläche **Create self-signed certificate (Selbstsigniertes Zertifikat erstellen)**, um die erforderlichen Informationen anzugeben.

So erstellen und installieren Sie ein CA-signiertes Zertifikat

1. Erstellen Sie wie oben beschrieben ein selbstsigniertes Zertifikat.
2. Wechseln Sie zu **Setup > Additional Controller Configuration(Zusätzliche Controller-Konfiguration) > System Options (Systemoptionen) > Security (Sicherheit) > Certificates (Zertifikat)**.
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. Wenn Sie das signierte Zertifikat zurückerhalten, klicken Sie auf **Install certificate (Zertifikat installieren)**, und laden Sie das Zertifikat hoch.

Server-/Clientzertifikate können als **Certificate from signing request (Zertifikat aus Signieranforderung)** oder **Certificate and private key (Zertifikat und privater Schlüssel)** installiert werden. Wählen Sie **Certificate and private key (Zertifikat und privater Schlüssel)** aus, wenn der private Schlüssel als separate Datei hochgeladen werden muss, oder wenn das Zertifikat das PKCS#12-Format aufweist.

Das Axis Produkt wird mit einigen vorinstallierten **CA-Zertifikaten** geliefert: Gegebenenfalls können zusätzliche CA-Zertifikate installiert werden:

1. Wechseln Sie zu **Setup > Additional Controller Configuration (Zusätzliche Controller-Konfiguration) > System Options (Systemoptionen) > Security (Sicherheit) > Certificates (Zertifikat)**.
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 Serverzeit) 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 Serverzeit)** den gewünschten **Time mode (Zeitmodus)** aus:

- **Synchronize with computer time (Mit Computerzeit synchronisieren)** – Das Datum und die 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 49*.

  Wenn für den NTP-Server ein Host-Name verwendet wird, muss ein DNS-Server konfiguriert werden. Siehe *DNS-Konfiguration auf Seite 49*.
- **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 auf folgende Arten eine IPv4-Adresse beziehen:

- **Dynamische IP-Adresse – Obtain IP address via DHCP (IP-Adresse über DHCP beziehen)** ist standardmäßig aktiviert. Das Axis Produkt erhält seine IP-Adresse automatischen per DHCP (Dynamic Host Configuration Protocol).

  Mithilfe von DHCP können Netzwerkadministratoren die Zuweisung von IP-Adressen zentral verwalten und automatisieren.

- **Statische IP-Adresse** – Um eine statische IP-Adresse zu verwenden, aktivieren Sie das Kontrollkästchen **Use the following IP address (Folgende IP-Adresse verwenden)**, und geben Sie die IP-Adresse, die Subnetzmaske und den Standardrouter an. 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 .

ARP/Ping

Die IP-Adresse des Produkts kann mit ARP und Ping zugewiesen werden. Anweisungen finden Sie unter *Zuweisen der IP-Adresse mit ARP/Ping auf Seite 47*.

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, wechseln Sie zu **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Basis)**.

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

Zuweisen der IP-Adresse mit ARP/Ping

Die IP-Adresse des Produkts kann mit ARP/Ping zugewiesen werden. Der Befehl muss innerhalb von 2 Minuten nach dem Anschließen der Stromversorgung erfolgen.

1. Wählen Sie eine nicht zugewiesene statische IP-Adresse im selben Netzwerksegment, in dem sich der Computer befindet.
2. Suchen Sie nach der Seriennummer (S/N) auf dem Produktaufkleber.
3. Öffnen Sie eine Eingabeaufforderung, und geben Sie die folgenden Befehle ein:

   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. Stellen Sie sicher, dass das Netzwerkkabel angeschlossen ist, und starten Sie das Produkt neu, indem Sie die Stromversorgung unterbrechen und wiederherstellen.
5. Schließen Sie die Eingabeaufforderung, wenn das Produkt mit `Reply from 192.168.0.125:...` oder einer ähnlichen Meldung antwortet.
6. Öffnen Sie einen Browser, und geben Sie `http://<IP-Adresse>` im Adressfeld ein.

Weitere Methoden zum Zuweisen der IP-Adresse finden Sie im Dokument *Assign an IP Address and Access the Video Stream* auf der Axis Support-Website unter *www.axis.com/techsup*.

Beachten

- Um eine Eingabeaufforderung in Windows zu öffnen, rufen Sie das **Startmenü** auf, und geben Sie `cmd` im Feld **Ausführen/Suchen** ein.
- Klicken Sie zum Verwenden des Befehls „ARP" unter Windows 8/Windows 7/Windows Vista mit der rechten Maustaste auf das Befehlszeilensymbol, und wählen Sie **Als Administrator ausführen** aus.
- Um eine Eingabeaufforderung in Mac OS X zu öffnen, rufen Sie das **Dienstprogramm „Terminal"** unter **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 unter **Setup > Additional Controller Configuration > System Options > Network > TCP IP > Basic (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP IP > Basis)** konfiguriert. 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 *Übersicht über die Hardware auf Seite 5*) 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 versucht ständig, 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 Verwendung der One-Click-Installation unpraktisch ist.

Beachten

Der AVHS-Support hängt von der Verfügbarkeit von Abonnements von Dienstanbietern 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 hierzu finden Sie unter *www.axiscam.net*.

Um das Axis Produkt mit AXIS Internet Dynamic DNS-Service zu registrieren, wechseln Sie zu **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Basis)**. Klicken Sie unter **Services (Dienste)** auf die Schaltfläche **Settings (Einstellungen)** für AXIS Internet Dynamic DNS-Service (erfordert Internetzugang). Der aktuell bei AXIS Internet Dynamic DNS-Service für das Produkt registrierte Domänenname kann jederzeit entfernt werden.

Beachten

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 unter **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Erweitert)** konfiguriert.

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 unter **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Erweitert)** konfiguriert.

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 Host-Name entspricht üblicherweise dem zugewiesenen DNS-Namen. Der Host-Name wird unter **Setup > Additional Controller Configuration> System Options > Network > TCP/IP > Advanced (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Erweitert)** 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 Online-Hilfe.

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

Diese Funktion kann unter **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Erweitert)** deaktiviert werden.

HTTP

Der vom Axis Produkt verwendete HTTP-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 (80) kann jeder Port im Bereich 1024–65535 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 1024–65535 verwendet werden.

Wechseln Sie zum Aktivieren von HTTPS zu **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Sicherheit > HTTPS)** Weitere Informationen finden Sie unter *HTTPS auf Seite 44*

NAT-Traversal (Port-Mapping) für IPv4

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

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

NAT-Traversal wird unter **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Erweitert)** konfiguriert.

Beachten

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

Enable/Disable (Aktivieren/Deaktivieren) – Wenn dies aktiviert ist, versucht das Axis Produkt Port-Mapping in einem NAT-Router in Ihrem Netzwerk mithilfe von UPnP™ zu konfigurieren. Beachten Sie, dass UPnP™ im Produkt aktiviert werden muss (siehe **Setup > Additional Controller Configuration > System Options > Network > UPnP (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > UPnP)**).

Use manually selected NAT router (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 ein. Wenn das Feld für den Port leer ist oder die Standardeinstellung (nämlich 0) enthält, wird bei Aktivierung von NAT-Traversal automatisch eine Portnummer ausgewählt.

Beachten

- 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 vom Axis Produkt ausgeführte FTP-Server ermöglicht das Hochladen von neuer Firmware, Benutzeranwendungen usw. Der FTP-Server kann unter **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > TCP/IP > Erweitert)** deaktiviert werden.

RTSP

Mithilfe des im Axis Produkt ausgeführten RTSP-Servers kann ein verbindender Client einen Ereignis-Videostrom 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.

Beachten

Ereignis-Videoströme 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 unter **Setup > Additional Controller Configuration > System Options > Network > SOCKS (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > SOCKS)** konfiguriert. Weitere Informationen finden Sie in der Online-Hilfe .

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 Fernverwaltung von Netzwerkgeräten. Eine SNMP-Community besteht aus einer Gruppe von Geräten und der Verwaltungsstation, die SNMP ausführt. Community-Namen werden zur Identifizierung von Gruppen verwendet.

Auf der Seite **Setup > Additional Controller Configuration > System Options > Network > SNMP (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > SNMP)** können Sie SNMP im Axis Produkt aktivieren und konfigurieren.

Wählen Sie je nach erforderlicher Sicherheitsstufe die zu verwendende SNMP-Version aus.

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.

Beachten

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 44*. Aktivieren Sie zum Aktivieren von SNMP v3 das Kontrollkästchen, und geben Sie das anfängliche Benutzerkennwort ein.

Beachten

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 Werkseinstellungen auf Seite 54*.

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.

UPnP™ kann unter **Setup > Additional Controller Configuration > System Options > Network > UPnP (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Netzwerk > UPnP)**™ deaktiviert werden.

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

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 unter **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Ports und Geräte > E/A-Ports)** konfiguriert. 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 > Port-Status)** wird der Status der Eingangs- und Ausgangs-Ports des Produkts angezeigt.

Wartung

Das Axis Produkt bietet verschiedene Wartungsfunktionen. Diese sind unter **Setup > Additional Controller Configuration > System Options > Maintenance (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Wartung)** verfügbar.

Klicken Sie auf **Restart (Neu starten)**, um einen korrekten Neustart durchzuführen, wenn das Axis Produkt nicht erwartungsgemäß funktioniert. Die beeinträchtigt die aktuellen Einstellungen nicht.

Beachten

Bei einem Neustart werden alle Einträge im Serverbericht 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
- IEEE 802.1X-Einstellungen

Klicken Sie auf **Default (Standard)**, um alle Einstellungen einschließlich der IP-Adresse auf die werksseitigen Standardwerte 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 Werkseinstellungen auf Seite 54*.

Informationen zur Firmware-Aktualisierung finden Sie unter *Aktualisieren der Firmware auf Seite 56*.

Support

Support-Übersicht

Auf der Seite **Setup > Additional Controller Configuration > System Options > Support > Support Overview (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Support > Support-Übersicht)** finden Sie Informationen zur Fehlersuche und Kontaktinformationen, wenn technische Unterstützung erforderlich ist.

Siehe auch *Fehlerbehebung auf Seite 56*.

Systemübersicht

Wechseln Sie zu **Setup > Additional Controller Configuration > System Options > Support > System Overview (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Support > Systemübersicht)**, um eine Übersicht über den Status und die Einstellungen des Axis Produkts zu erhalten. Hier finden Sie u. a. Informationen zur Firmware-Version, zur IP-Adresse, zu Netzwerk- und Sicherheitseinstellungen, zu Ereigniseinstellungen und zu aktuellen Protokolleinträgen. Viele der Angaben sind Links zur entsprechenden Setup-Seite.

Protokolle und Berichte

Auf der Seite **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Unterstützung > Protokolle und Berichte)** werden Protokolle und Berichte zur Systemanalyse und Fehlersuche generiert. Stellen Sie bei der Kontaktaufnahme mit Axis Support einen gültigen Serverbericht mit Ihrer Anfrage bereit.

System Log (Systemprotokoll) – Enthält Informationen zu Systemereignissen.

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

Server Report (Serverbericht) – Stellt Informationen zum Produktstatus in einem Popup-Fenster bereit. Das Zugangsprotokoll wird dem Serverbericht automatisch angefügt.

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. Die Generierung des Berichts nimmt einige Minuten in Anspruch.

Die Protokollstufen für das System- und das Zugangsprotokoll werden unter **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Unterstützung > Protokolle und Berichte > Konfiguration)** eingestellt. Das Zugangsprotokoll kann zum Auflisten aller Verbindungen mit dem Produkt konfiguriert werden (wählen Sie „Critical, Warnings & Info (Kritisch, Warnungen und Informationen)" aus).

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.

Wechseln Sie zum Öffnen des Script Editors zu **Setup > Additional Controller Configuration > System Options > Advanced > Scripting (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Erweitert > Skripterstellung)**. Wenn ein Skript Probleme verursacht, setzen Sie das Produkt auf die werksseitigen Standardeinstellungen zurück, siehe *Seite 54*.

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. Wechseln Sie zum Hochladen einer Datei zu **Setup > Additional Controller Configuration > System Options > Advanced > File Upload (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Erweitert > Datei-Upload)**.

Auf hochgeladene Dateien wird über `http://<IP-Adresse>/local/<Benutzer>/<Dateiname>` zugegriffen, wobei `<Benutzer>` die ausgewählte Benutzergruppe (Anzeige, Bediener oder Administrator) für die hochgeladene Datei ist.

Zurücksetzen auf Werkseinstellungen

Wichtig

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

Beachten

Die Software-Tools für Installation und Verwaltung sind über die Supportseiten unter *www.axis.com/techsup* verfügbar.

So wird das Produkt auf die Werkseinstellungen zurückgesetzt:

1. Trennen Sie das Produkt von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stecken Sie den Netzstecker wieder ein. Siehe *Übersicht über die Hardware auf Seite 5*.
3. Halten Sie die Steuertaste etwa 25 Sekunden gedrückt, bis die LED-Statusanzeige zum zweiten Mal gelb leuchtet.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die LED-Statusanzeige grün leuchtet. Das Produkt wurde auf die Werkseinstellungen zurückgesetzt. Wenn kein DHCP-Server im Netzwerk verfügbar ist, lautet die Standard-IP-Adresse `192.168.0.90`.

5. Mithilfe der Software-Tools für Installation und Verwaltung können Sie eine IP-Adresse zuweisen, das Kennwort festlegen und auf das Produkt zugreifen.

Die Parameter können auch über die Weboberfläche auf die Werkseinstellungen zurückgesetzt werden. Rufen Sie **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Setup > Zusatzkontrollenkonfiguration > Setup > Systemoptionen > Wartung)** auf.

Fehlerbehebung

Prüfen der Firmware

Bei Firmware handelt es sich um Software, die die Funktionalität von Netzwerkgeräten 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 Firmware-Version des Axis Produkts wird auf der Seite **Setup > Additional Controller Configuration > Basic Setup (Setup > Zusatzkontrollenkonfiguration > Basiseinrichtung)** und unter **Setup > Additional Controller Configuration > About (Setup > Zusatzkontrollenkonfiguration > Über)** angezeigt.

Aktualisieren der Firmware

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.

Beachten

- Nach Abschluss des Aktualisierungsvorgangs wird das Produkt automatisch neu gestartet. Bei manuellem Neustart des Produkts nach der Aktualisierung stets 5 Minuten lang warten, auch wenn Sie vermuten, dass die Aktualisierung fehlgeschlagen ist.
- Da nach einer Firmware-Aktualisierung die Datenbank mit Benutzern, Gruppen, Anmeldeinformationen und anderen Daten aktualisiert wird, kann der erste Start einige Minuten lang dauern. Die erforderliche Zeit hängt von der Datenmenge ab.
- Wenn Sie das Axis Produkt mit der aktuellen Firmware von der Axis Website aktualisieren, erhält das Produkt die neueste verfügbare Funktionalität. Lesen Sie vor der Aktualisierung der Firmware stets die Aktualisierungsanweisungen und die Release-Notes.

So aktualisieren Sie die Firmware des Produkts:

1. Speichern Sie die Firmware-Datei auf dem Computer. Die aktuelle Version der Firmware ist kostenlos auf der Axis Website unter *www.axis.com/techsup* verfügbar.
2. Wechseln Sie zu **Setup > Additional Controller Configuration > System Options > Maintenance (Setup > Zusatzkontrollenkonfiguration > Systemoptionen > Wartung)**.
3. Klicken Sie unter **Upgrade Server (Server aktualisieren)** auf **Browse (Durchsuchen)**, und suchen Sie die Datei auf dem Computer. Klicken Sie auf **Upgrade (Aktualisieren)**.
4. Warten Sie etwa 5 Minuten lang, während das Produkt aktualisiert und neu gestartet wird. Löschen Sie anschließend den Cache des Webbrowsers.
5. Greifen Sie auf das Produkt zu.

Notfall-Wiederherstellungsverfahren

Wenn die Stromversorgung oder die Netzwerkverbindung während der Aktualisierung unterbrochen wird, schlägt der Prozess fehl und das Produkt reagiert nicht mehr. Mit der rot blinkenden Statusanzeige wird die fehlgeschlagene Aktualisierung 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. Klicken Sie dann auf **Load (Laden)**, um den Aktualisierungsprozess neu zu starten.
4. Nach Abschluss der Aktualisierung (1–10 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 an den Axis Support unter www.axis.com/techsup/.

Symptome, mögliche Ursachen und Maßnahmen zur Behebung

Probleme mit dem Einstellen der IP-Adresse	
Bei Verwendung von ARP/Ping	Führen Sie die Installation erneut durch. Die IP-Adresse muss innerhalb von zwei Minuten nach dem Einschalten des Produkts eingestellt werden. Stellen Sie sicher, dass die Ping-Länge auf 408 eingestellt ist. Anweisungen finden sich in der Installationsanleitung 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, können Sie die IP-Adresse nicht einstellen. Wenden Sie sich an Ihren Netzwerkadministrator, um eine IP-Adresse zu erhalten.
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-Adresskonflikt 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.

Mit einem Browser kann nicht auf das Produkt zugegriffen werden	
Anmeldung nicht möglich	Wenn HTTPS aktiviert ist, stellen Sie sicher, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise müssen Sie manuell `http` oder `https` in die Adressleiste des Browsers eingeben. Wenn das Kennwort für den Benutzer „root" vergessen wurde, muss das Produkt auf die werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe *Zurücksetzen auf Werkseinstellungen auf Seite 54*.

Fehlerbehebung

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, können Sie das Produkt mithilfe von AXIS IP Utility im Netzwerk finden. Identifizieren Sie das Produkt anhand seiner Modell- oder Seriennummer bzw. anhand des DNS-Namens (wenn der Name konfiguriert wurde). Bei Bedarf kann eine statische IP-Adresse manuell zugewiesen werden. Anweisungen finden Sie in der Installationsanleitung auf *www.axis.com/techsup*.
Zertifikatfehler bei Verwendung von IEEE 802.1X	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 46*.

Auf das Produkt kann lokal, nicht jedoch extern zugegriffen werden

Routerkonfiguration	Um Ihren Router zum Zulassen eingehenden Datenverkehrs zum Axis Produkt zu konfigurieren, aktivieren Sie die NAT-Traversal-Funktion, die versucht, den Router automatisch für den Zugriff auf das Axis Produkt zu konfigurieren. Siehe *NAT-Traversal (Port-Mapping) für IPv4 auf Seite 50*. Der Router muss UPnP™ unterstützen.
Firewallschutz	Prüfen Sie die Internet-Firewall mit Ihrem Netzwerkadministrator.
Standardrouter erforderlich	Überprüfen Sie, ob die Routereinstellungen unter **Setup > Network Settings (Setup > Netzwerkeinstellungen)** bzw. **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Setup > Zusätzliche Controller-Konfiguration > Systemoptionen > Netzwerk > TCP/IP > Basis)** konfiguriert werden müssen.

Anzeige-LEDs zu Status und Netzwerk blinken mit hoher Frequenz rot

Hardwarefehler	Wenden Sie sich an Ihren Axis Händler.

Spezifikationen

AXIS A1001 Netzwerk-Tür-Controller

Funk-tion/Gruppe	Artikel	Technische Daten
	Modelle	AXIS A1001 Netzwerk-Tür-Controller
Tür-Controller	**Leser**	Bis zu zwei Leser pro Controller (Wiegand, RS485 (OSDP)) mit den unterstützten Kartenformaten
	Türen	Ein bis zwei Türen pro Controller[1]
	Zugangsdaten	Bis zu 15.000 Zugangsverwaltungssoftware von Drittanbietern, abhängig von der Server-Kapazität
	Ereignisverlauf	30000 FIFO (First In, First Out) pro Controller
	Zugangszeitpläne	Unbegrenzt oder abhängig von Drittanbieter-Software
Digital-E/A	**E/A-Schnittstelle**	**Leser-E/A:** Gleichstromausgang: 2x 12 V DC Ausgabe max. 300 mA; 2x 4 konfigurierbare Eingänge/Ausgänge, (Digitaleingang: 0 bis max. 40 V DC, Digitalausgang: 0 bis max. 40 V DC, Open Drain, max. 100 mA) **Leser-Daten:** RS485 für Vollduplex, RS485 für Halbduplex, Wiegand **Zusatzanschlüsse:** 1x 3,3 V DC Ausgabe max. 100 mA; 2x konfigurierbare Eingänge/Ausgänge, (Digitaleingang: 0 bis max. 40 V DC, Digitalausgang: 0 bis max. 40 V DC, Open Drain, max. 100 mA) **Türanschlüsse:** 2x 2 Eingänge für Türmonitore und REX (Digitaleingang: 0 bis max. 40 V DC)
	E/A-Funktion	Vorkonfiguriert für Leser und Türmonitore, Eingang: Auslöser, Ausgang: Umschalter, Impuls
Netzwerk	**Sicherheit**	Kennwortschutz, IP-Adressfilter, HTTPS[2] Verschlüsselung, Netzwerk-Zugriffskontrolle nach IEEE 802.1X, Digest-Authentifizierung, Benutzer-Zugriffsprotokoll
	Unterstützte Protokolle	IPv4, HTTP, HTTPS[2], TLS[2], QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS
Systemintegra-tion	**API (Application Programming Interface)**	Offene API zur Softwareintegration, darunter VAPIX®; Spezifikationen unter *www.axis.com* ONVIF Profile C, Spezifikationen unter *www.onvif.org* Unterstützung für Zugangskontrolle als Dienst mit One-Click Connection
Ereignisse und Alarme	**Manipulationserken-nung**	Entfernen der Geräteabdeckung/manipulationsgesicherten Vorderseite Entfernen des Geräts von der Wand/manipulationsgesicherten Rückseite Leser-Manipulation
	Ereignisprotokoll	Konfigurierbar nach Zeit und Thema, Alarmbestätigung
	Ereignisaktionen	Benachrichtigung per E-Mail, HTTP und TCP, Externer Ausgangs-Port, Status-LED
	Ereignisauslöser	**Access Point:** Access Point aktiviert **Konfiguration:** Access Point geändert, Access Point entfernt, Bereich geändert, Bereich entfernt, Tür geändert, Tür entfernt **Tür:** Türalarm, Türdoppelschloss-Monitor, Türschlossmonitor, Türmodus, Türmonitor, Türwarnung **Ereignisaufzeichnung:** Alarm **Hardware:** Gehäuse geöffnet, Netzwerk, Peer-Verbindung **Eingangssignal** Digitaler Eingangs-Port, manueller Auslöser, virtuelle Eingänge **Zeitplan:** Intervall, Impuls **System:** Systembereitschaft **Zeit:** Wiederholung, Zeitplan

Spezifikationen

Funk-tion/Gruppe	Artikel	Technische Daten
Allgemeines	Gehäuse	Kunststoff
	Software	Konfiguration und grundlegende Verwaltung der Zugangskontrolle über Internet Explorer, Firefox, Chrome oder Safari
	Arbeitsspeicher	256 MB RAM, 4 GBit Flash
	Stromversorgung	**Netzanschluss:** 10–30 V DC, max. 26 W oder Power over Ethernet IEEE 802.3af/802.3at Typ 1 Klasse 3 **Stromausgang und Relais:** 1x 12 V DC, max. 500 mA 1x elektronisches Lastrelais 30 V DC, max. 700 mA **Stromausgang:** 2x 12 V DC, max. 500 mA[1]
	Anschlüsse	RJ45 10BASE-T/100BASE-TX **Anschlussblöcke:** Gleichstrom, 10 Eingänge/Ausgänge, RS485/Wiegand, Relais **Kabelgröße für die Anschlüsse:** CSA: AWG 28–16, CUL/UL: AWG 30–14
	Betriebsbedingungen	0 °C bis 50 °C, Relative Luftfeuchtigkeit 20 bis 85 % (nicht kondensierend)
	Zulassungen	EN 55022 Klasse B, EN 50130-4, EN 61000-3-2, EN 61000-3-3, EN 55024, EN 61000-6-1, EN 61000-6-2FCC Teil 15 Abschnitt B Klasse B ICES-003 Klasse B C-tick AS/NZS CISPR22 Klasse B VCCI Klasse B IEC/EN/UL 60950-1, UL 294, UL 2043, EN 50581
	Abmessungen (HxBxT)	45,5 x 180 x 180 mm
	Gewicht	500 g
	Im Lieferumfang enthaltenes Zubehör	Anschluss-Kit, Kabelbinder, Installationsanleitung
	Sprachen	Englisch, Deutsch, Französisch, Spanisch, Italienisch
	Garantie	Informationen zur 3-Jahres-Axis-Garantie mit der Option auf Verlängerung auf 5 Jahre finden Sie unter *www.axis.com/warranty*
	Optionales Zubehör	AXIS T8120 Midspan 15 W AXIS T8128 PoE Splitter 24 V (benötigt 30 W Midspan) AXIS T8129 PoE Extender-Netzteil 24 V DC AXIS T98A15-VE Überwachungsschrank[3]

1. Stromverbrauch variiert, max. Last für Leser und andere Ausrüstung beträgt 7,5 W mit PoE und 14 W mit 10–30 V DC.
2. Dieses Produkt enthält Software, die vom OpenSSL Project zur Verwendung im OpenSSL Toolkit entwickelt (http://www.openssl.org/), sowie kryptografische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.
3. In Außenrauminstallationen, die AXIS A1001 und AXIS T98A15-VE kombinieren, beträgt die zulässige maximale Spannung 30 V DC.

Spezifikationen

AXIS Entry Manager

Funk-tion/Gruppe	Artikel	Technische Daten
	Modelle	AXIS A1001 mit integrierter web-basierter Software
Tür-Controller	Leser	Bis zu 2 Leser pro Controller[1] (Wiegand, RS485 (OSDP) mit den unterstützten Kartenformaten
	Controller	1–33
	Zugangsdaten	Bis zu 400
	Ereignisverlauf	30 000 FIFO (First In, First Out) pro System
Digital-E/A	E/A-Schnittstelle	**Leser-E/A:** Gleichstromausgang: 2x 12 V DC Ausgabe max. 300 mA; 2x 4 konfigurierbare Eingänge/Ausgänge, (Digitaleingang: 0 bis max. 40 V DC, Digitalausgang: 0 bis max. 40 V DC, Open Drain, max. 100 mA) **Leser-Daten:** RS485 für Vollduplex, RS485 für Halbduplex, Wiegand **Zusatzanschlüsse:** 1x 3,3 V DC Ausgabe max. 100 mA; 2x konfigurierbare Eingänge/Ausgänge, (Digitaleingang: 0 bis max. 40 V DC, Digitalausgang: 0 bis max. 40 V DC, Open Drain, max. 100 mA) **Türanschlüsse:** 2x 2 Eingänge für Türmonitore und REX (Digitaleingang: 0 bis max. 40 V DC)
	E/A-Funktion	Vorkonfiguriert für Leser und Türmonitore, Eingang: Auslöser, Ausgang: Umschalter, Impuls
Netzwerk	Sicherheit	Kennwortschutz, IP-Adressfilter, HTTPS[2] Verschlüsselung, Netzwerk-Zugriffskontrolle nach IEEE 802.1X, Digest-Authentifizierung, Benutzer-Zugriffsprotokoll
	Unterstützte Protokolle	IPv4, HTTP, HTTPS[2], TLS[2], QoS layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS
Ereignisse und Alarme	Manipulationserken-nung	Entfernen der Geräteabdeckung/manipulationsgesicherten Vorderseite Entfernen des Geräts von der Wand/manipulationsgesicherten Rückseite Leser-Manipulation
	Ereignisprotokoll	Konfigurierbar nach Zeit und Thema; Alarmbestätigung
	Ereignisaktionen	Benachrichtigung per E-Mail, HTTP und TCP, Externer Ausgangs-Port, Status-LED
	Ereignisauslöser	**Access Point:** Access Point aktiviert **Konfiguration:** Access Point geändert, Access Point entfernt, Tür geändert, Tür entfernt **Tür:** Türalarm, Türdoppelschloss-Monitor, Türschloss-Monitor, Türmodus, Türmonitor, Türwarnung **Ereignisaufzeichnung:** Alarm **Hardware:** Gehäuse geöffnet, Netzwerk, Peer-Verbindung **Eingangssignal** Digitaler Eingangs-Port, Manueller Auslöser, Virtuelle Eingänge **Zeitplan:** Intervall, Impuls **System:** Systembereitschaft **Zeit:** Wiederholung, Zeitplan
Systemmerk-male	Zugangszeitpläne	Unbegrenzt
	Installation und Konfiguration	Konfigurationsassistent, Konfigurationsüberprüfung, Farbcodierte Anschlüsse, Ausdruck der E/A-Zuweisung, Automatische Controller-Erkennung, Unmittelbares Feedback bei fehlenden Konfigurationsdaten
	Verwaltung	Drag&Drop-Bedienung mit flexibler Zuweisung von Türen und Benutzergruppen, Laden der Zugriffsrechte vom Leser, Manueller Zugriff/Verriegeln/Entriegeln, Importieren von Benutzern
	Sprachen	Englisch, Deutsch, Französisch, Spanisch, Italienisch

Spezifikationen

Funk-tion/Gruppe	Artikel	Technische Daten
Allgemeines	Gehäuse	Kunststoff
	Software	Konfiguration und grundlegende Verwaltung der Zugangskontrolle über Internet Explorer, Firefox, Chrome oder Safari
	Arbeitsspeicher	256 MB RAM, 4 GBit Flash
	Stromversorgung	**Netzanschluss:** 10–30 V DC, max. 26 W oder Power over Ethernet IEEE 802.3af/802.3at Typ 1 Klasse 3 **Stromausgang und Relais:** 1x 12 V DC, max. 500 mA 1x elektronisches Lastrelais 30 V DC, max. 700 mA **Stromausgang:** 2x 12 V DC, max. 500 mA[1]
	Anschlüsse	RJ45 10BASE-T/100BASE-TX **Anschlussblöcke:** Gleichstrom, 10 Eingänge/Ausgänge, RS485/Wiegand, Relais **, Kabelgröße für die Anschlüsse:** CSA: AWG 28-16, CUL/UL: AWG 30-14
	Betriebsbedingungen	0 °C bis 50 °C, Relative Luftfeuchtigkeit 20 bis 85 % (nicht kondensierend)
	Zulassungen	EN 55022 Klasse B, EN 50130-4, EN 61000-3-2, EN 61000-3-3, EN 55024, EN 61000-6-1, EN 61000-6-2FCC Teil 15 Abschnitt B Klasse B ICES-003 Klasse B C-tick AS/NZS CISPR22 Klasse B VCCI Klasse B IEC/EN/UL 60950-1, UL 294, UL 2043, EN 50581
	Abmessungen (HxBxT)	45,5 x 180 x 180 mm
	Gewicht	500 g
	Im Lieferumfang enthaltenes Zubehör	Anschluss-Kit, Kabelbinder, Installationsanleitung
	Garantie	Informationen zur 3-Jahres-Axis-Garantie mit der Option auf Verlängerung auf 5 Jahre finden Sie unter *www.axis.com/warranty*
	Optionales Zubehör	AXIS T8120 Midspan 15 W AXIS T8128 PoE Splitter 24 V (benötigt 30 W Midspan) AXIS T8129 PoE Extender-Netzteil 24 V DC AXIS T98A15-VE Überwachungsschrank[3]

1. Stromverbrauch abhängig, max. Last für Leser und andere Ausrüstung beträgt 7,5 W mit PoE und 14 W mit 10–30 V DC.
2. Dieses Produkt enthält Software, die vom OpenSSL Project zur Verwendung im OpenSSL Toolkit entwickelt (http://www.openssl.org/), sowie kryptografische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.
3. In Außenrauminstallationen, die AXIS A1001 und AXIS T98A15-VE kombinieren, beträgt die zulässige maximale Spannung 30 V DC.

Anschlüsse

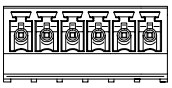
Für Informationen zur Lage der Anschlüsse siehe *Übersicht über die Hardware auf Seite 5*.

Für Anschlussschaltbilder und Informationen zu dem bei der Hardwarekonfiguration erstellten Pin Chart siehe *Anschlussschaltbilder auf Seite 66* und *Konfigurieren der Hardware auf Seite 13*.

Im folgenden Abschnitt finden Sie die technischen Daten der Anschlüsse.

Spezifikationen

Leser-Daten-Anschluss



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

Die RS485-Ports unterstützen:

- Zweiadrig RS485 Halbduplex
- Vieradrig RS485 Vollduplex

Die Wiegand-Ports unterstützen:

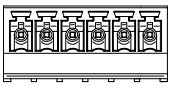
- Zweiadrig Wiegand

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

Wichtig

Die empfohlene maximale Kabellänge beträgt 30 m.

Leser-E/A-Anschluss



6-poliger Anschlussblock für:

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

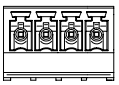
Kontakt 3 an den Leser-E/A-Anschlüssen kann überwacht werden. Bei Unterbrechung der Verbindung wird ein Ereignis ausgelöst. Bringen Sie zur Verwendung überwachter Eingänge Abschlusswiderstände an. Beachten Sie das Anschlussschaltbild für überwachte Eingänge. Siehe *Seite 67*.

Funktion	Kontakt	Hinweise	Technische Daten
0 V DC (-)	1		0 V DC
Gleichstrom-ausgang	2	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt kann nur für den Stromausgang verwendet werden.	12 V DC 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 DC
		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 DC, Open Drain, 100 mA

Spezifikationen

Türanschluss

Zwei 4-polige Anschlussblöcke für Türüberwachungsgeräte (Digitaleingang).

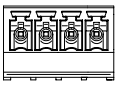


Alle Türeingangskontakte können überwacht werden. Bei Unterbrechung der Verbindung wird ein Alarm ausgelöst. Bringen Sie zur Verwendung überwachter Eingänge Abschlusswiderstände an. Beachten Sie das Anschlussschaltbild für überwachte Eingänge. Siehe *Seite 67*.

Funktion	Kontakt	Hinweise	Technische Daten
0 V DC (-)	1, 3		0 V DC
Eingang	2, 4	Zur Kommunikation mit dem Türmonitor. 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 DC

Zusatzanschluss

4-poliger konfigurierbarer E/A-Anschlussblock für:



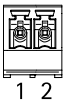
- Zusatzstromversorgung (Gleichstromausgang)
- Digitaleingang
- Digitalausgang
- 0 V DC (-)

Ein Anschlussschaltbild als Beispiel finden Sie unter *Anschlussschaltbilder auf Seite 66*.

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

Stromanschluss

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.



Funktion	Kontakt	Hinweise	Technische Daten
0 V DC (-)	1		0 V DC
Gleichstromeingang	2	Stromversorgung des Controllers ohne Power over Ethernet. Hinweis: Dieser Kontakt kann nur für den Stromeingang verwendet werden.	10–30 V DC, max. 26 W Max. Last an Ausgängen = 14 W

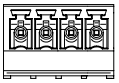
Netzwerkanschluss

RJ45-Ethernetanschluss. Unterstützt Power over Ethernet (PoE). Verwenden Sie Kabel der Kategorie 5e oder höher.

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

Stromanschluss (Schloss)

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

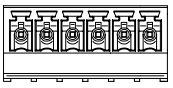


Schließen Sie Schlösser und andere Geräte gemäß dem während der Hardwarekonfiguration erstellten Pin Chart an.

Funktion	Kontakt	Hinweise	Technische Daten
0 V DC (-)	1, 3		0 V DC
0 V DC, frei oder 12 V DC	2, 4	Zur Steuerung von bis zu zwei 12-V-Schlössern. Verwenden Sie das Pin Chart. Siehe *Konfigurieren der Hardware auf Seite 13*.	12 V DC Max. Gesamtlast = 500 mA

Netz- und Relaisanschluss

6-poliger Anschlussblock mit integriertem Relais für:



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

Schließen Sie Schlösser und andere Geräte gemäß dem während der Hardwarekonfiguration erstellten Pin Chart an.

Funktion	Kontakt	Hinweise	Technische Daten
0 V DC (-)	1, 4		0 V DC
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 DC

12 V DC	5	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt kann nur für den Stromausgang verwendet werden.	Max. Spannung = +12 V DC Max. Last = 500 mA
24 V DC	6	Nicht verwendet	

Manipulationsalarm-Stiftleiste

Zwei 2-polige Leisten zur Überbrückung des:

- Hinteren Manipulationsalarms (TB)
- Vorderen Manipulationsalarms (TF)

Funktion	Kontakt	Hinweise
Hinterer Manipulationsalarm	1–2	Setzen Sie die Drahtbrücken zwischen TB 1, TB 2 bzw. TF 1, TF 2, um den vorderen bzw. hinteren Manipulationsalarm zu überbrücken. Bei einer Überbrückung des Manipulationsalarms erkennt das System keine Manipulationsversuche.
Vorderer Manipulationsalarm	1–2	

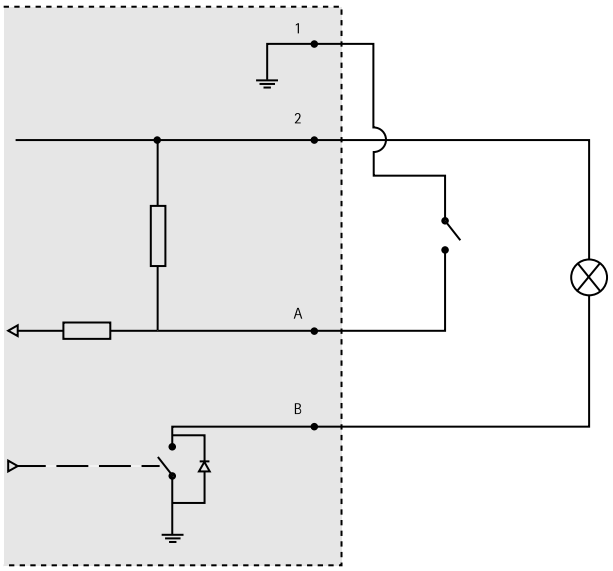
Beachten

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 .

Anschlussschaltbilder

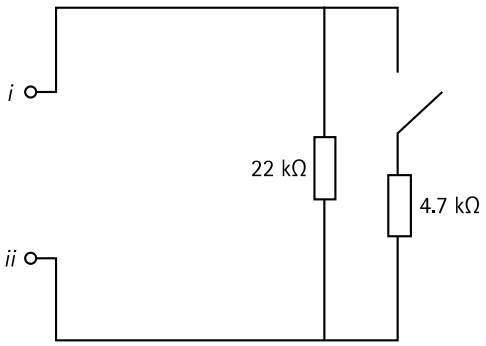
Schließen Sie Geräte gemäß dem während der Hardwarekonfiguration erstellten Pin Chart an. Weitere Informationen zu Hardwarekonfiguration und Pin Chart finden Sie unter *Konfigurieren der Hardware auf Seite 13*.

Zusatzanschluss



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

Überwachte Eingänge



Bringen Sie zur Verwendung überwachter Eingänge Abschlusswiderstände an. Dies gilt für alle überwachten Eingänge. Informationen zu Einschränkungen und Aktualisierungen sind in den Release-Notes des Produkts enthalten.

i Eingang
ii 0 V DC (-)

Benutzerhandbuch
AXIS A1001 Network Door Controller & AXIS Entry Manager

Ver. M5.2
Datum: November 2014
Artikel-Nr. 65603