

## AXIS A1601 Network Door Controller

# AXIS A1601 Network Door Controller

## Inhalt

---

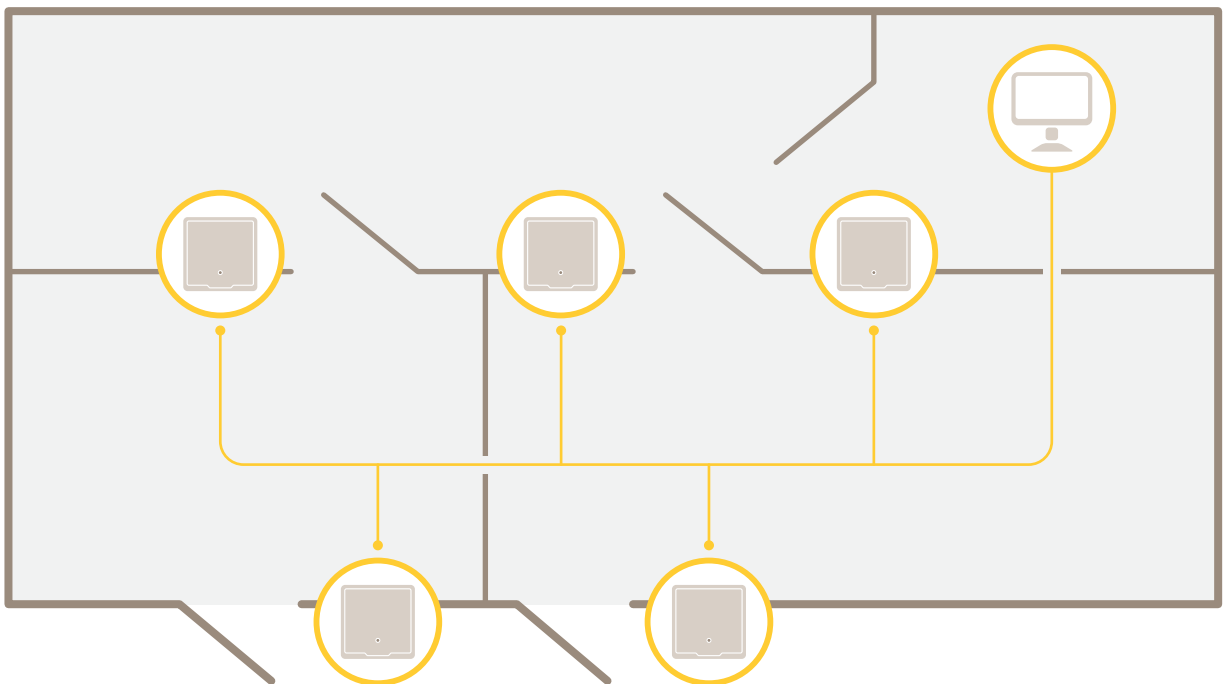
<b>Lösungsübersicht</b> .....	3
<b>Produktübersicht</b> .....	5
<b>Das Gerät im Netzwerk ermitteln</b> .....	7
Auf das Gerät zugreifen .....	7
Über das Internet auf das Produkt zugreifen .....	7
Sichere Kennwörter .....	7
Die Übersichtsseite .....	8
<b>Systemkonfiguration</b> .....	9
Konfigurieren – Schritt für Schritt .....	9
Eine Sprache wählen .....	9
Einstellen von Datum und Uhrzeit .....	9
Konfigurieren der Netzwerkeinstellungen .....	10
Konfigurieren der Hardware .....	11
Überprüfen der Hardwareanschlüsse .....	17
Karten und Formate konfigurieren .....	18
Dienste konfigurieren .....	20
Wartungsanweisungen .....	21
<b>Ereigniskonfiguration</b> .....	23
Anzeigen des Ereignisprotokolls .....	23
Das Ereignisprotokoll konfigurieren .....	23
Aktionsregeln einrichten .....	23
Leser-Feedback .....	26
<b>Systemoptionen</b> .....	27
Sicherheit .....	27
Netzwerk .....	29
Ports und Geräte .....	34
Wartung .....	34
Support .....	35
Erweitert .....	35
<b>Fehlerbehebung</b> .....	37
Zurücksetzen auf die Werkseinstellungen .....	37
Die aktuelle Firmware überprüfen .....	37
Die Firmware aktualisieren .....	37
Symptome, mögliche Ursachen und Maßnahmen zur Behebung .....	38
<b>Technische Daten</b> .....	40
LED-Anzeigen .....	40
Tasten .....	40
Anschlüsse .....	40
<b>Sicherheitsinformationen</b> .....	47
Gefährdungsstufen .....	47
Andere Meldeebenen .....	47
<b>Geräteschnittstelle</b> .....	48
Status .....	48
Zutrittskontrolle .....	49
System .....	49
Wartung .....	59

# AXIS A1601 Network Door Controller

## Lösungsübersicht

---

### Lösungsübersicht

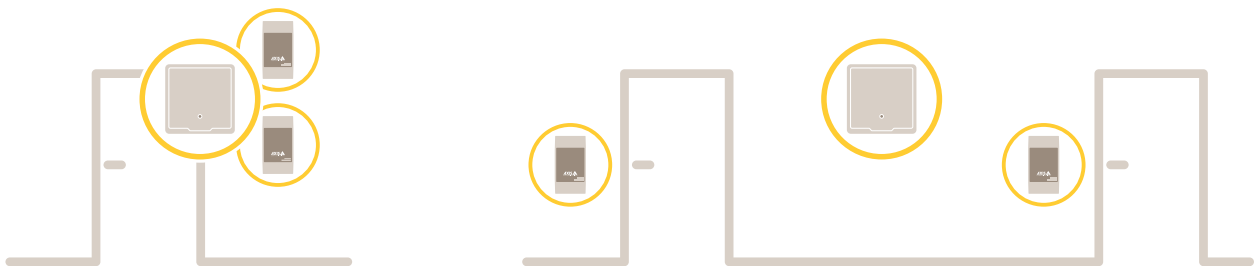


Der Netzwerk-Türcontroller kann einfach an ein bestehendes IP-Netzwerk angeschlossen und darüber mit Strom versorgt werden. Besondere Kabel sind nicht erforderlich.

# AXIS A1601 Network Door Controller

## Lösungsübersicht

---

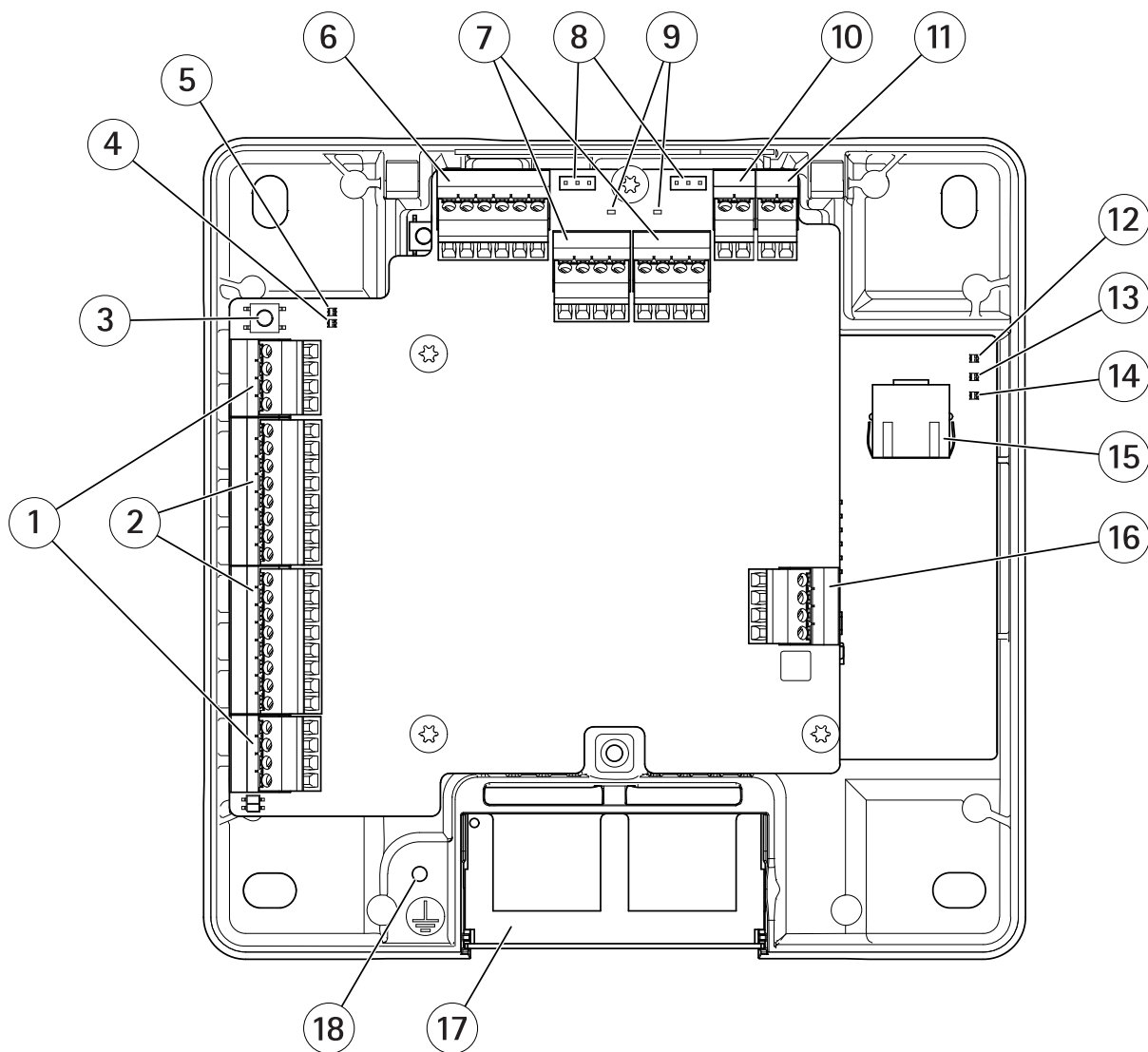


Netzwerk-Türcontroller sind mit intelligenten Funktion ausgestattete Geräte, die einfach in Türnähe angebracht werden können. Sie können bis zu zwei Lesegeräte mit Strom versorgen und steuern.

# AXIS A1601 Network Door Controller

## Produktübersicht

### Produktübersicht



- 1 Türanschluss auf Seite 42 (2 St.)
- 2 Lesegerätanschluss auf Seite 41 (2 St.)
- 3 Steuertaste auf Seite 40
- 4 Überstrom-LED des Lesegerätes
- 5 Überstrom-LED
- 6 Zusatzanschluss auf Seite 44
- 7 Relaisanschluss auf Seite 43 (2 St.)
- 8 Relaisbrücke (2 St.)
- 9 Relay-LED (2 St.)
- 10 Anschlusseingang Sicherungsbatterie auf Seite 45
- 11 Stromanschluss auf Seite 45
- 12 Netz-LED
- 13 Status-LED

# AXIS A1601 Network Door Controller

## Produktübersicht

---

- 14 *Netzwerk-LED*
- 15 *Netzwerk-Anschluss auf Seite 40*
- 16 *Externer Anschluss auf Seite 45*
- 17 *Umkehrbare Kabelabdeckung*
- 18 *Position Erdung*

# AXIS A1601 Network Door Controller

## Das Gerät im Netzwerk ermitteln

---

### Das Gerät im Netzwerk ermitteln

Mit AXIS IP Utility und AXIS Device Manager die Axis Geräte im Netzwerk ermitteln und ihnen unter Windows® IP-Adressen zuweisen. Beide Anwendungen sind kostenlos und können von [axis.com/support](http://axis.com/support) heruntergeladen werden.

Weitere Informationen zum Zuweisen von IP-Adressen finden Sie unter *Zuweisen von IP-Adressen und Zugreifen auf das Gerät*.

### Auf das Gerät zugreifen

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

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

2. Den Benutzernamen und das Kennwort eingeben. Wenn dies der erste Zugriff auf das Gerät ist, muss zuerst das Root-Kennwort konfiguriert werden. Siehe .
3. Im Browser wird die Webseite des Geräts geöffnet. Die Startseite wird als Übersichtsseite bezeichnet.

### Über das Internet auf das Produkt zugreifen

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

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

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

#### Die Funktion NAT-Traversal aktivieren

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

#### Hinweis

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

### Sichere Kennwörter

#### Wichtig

Das voreingestellte Kennwort wird vom Axis Gerät unverschlüsselt über das Netz gesendet. Um das Gerät zu schützen, nach dem ersten Anmelden eine sichere und verschlüsselte HTTPS-Verbindung einrichten und dann das Kennwort ändern.

Das Gerätekenwort ist der Hauptschutz für Ihre Daten und Dienste. Produkte von Axis geben keine Kennwortrichtlinien vor, da die Produkte unter den verschiedensten Bedingungen eingesetzt werden.

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

# AXIS A1601 Network Door Controller

## Das Gerät im Netzwerk ermitteln

---

- Ein Kennwort zu verwenden, das aus mindestens acht Zeichen besteht, und das bevorzugt von einem Kennwortgenerator erzeugt wurde.
- Das Kennwort geheimzuhalten.
- Das Kennwort regelmäßig und mindestens jährlich zu ändern.

### Das Root-Kennwort festlegen

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

Um ein Abhören der Netzwerk-Kommunikation zu verhindern, können Sie das Root-Kennwort über eine verschlüsselte HTTPS-Verbindung festlegen, die ein HTTPS-Zertifikat erfordert. Das Protokoll HTTPS (Hypertext Transfer Protocol over SSL) wird verwendet, um den Datenverkehr zwischen Webbrowsern und Servern zu verschlüsseln. Das HTTPS-Zertifikat gewährleistet den verschlüsselten Informationsaustausch. Siehe *HTTPS auf Seite 27*.

Der standardmäßige Administrator-Benutzername **root** kann nicht geändert bzw. gelöscht werden. Wenn Sie das entsprechende Kennwort vergessen haben, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 37*.

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

### Die Übersichtsseite

Die Webseite des Produkts zeigt Informationen wie den Namen, die MAC-Adresse, die IP-Adresse und die Firmwareversion des Türcontrollers an. Mithilfe dieser Angaben lässt sich der Türcontroller im Netzwerk identifizieren.

Beim ersten Zugriff auf das Axis Produkt werden Sie auf der Übersichtsseite aufgefordert, die Hardware zu konfigurieren, Datum und Uhrzeit festzulegen sowie die Netzwerkeinstellungen zu konfigurieren. Weitere Informationen zum Konfigurieren des Systems, siehe *Konfigurieren – Schritt für Schritt auf Seite 9*.

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



# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

### Systemkonfiguration

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

Dieses Axis Produkt kann von Administratoren konfiguriert werden. Weitere Informationen zu Benutzern und Administratoren, siehe *Seite 27*.

### Konfigurieren – Schritt für Schritt

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


1. Falls Englisch nicht Ihre bevorzugte Sprache ist, können Sie für die die Webseite des Produkts eine andere Sprache wählen. Siehe *Eine Sprache wählen auf Seite 9*.
2. Datum und Datum einstellen. Siehe *Seite 9*.
3. Die Netzwerkeinstellungen konfigurieren. Siehe *Seite 10*.
4. Den Türcontroller und angeschlossene Geräte konfigurieren (zum Beispiel Lesegeräte, Schlösser und REX-Geräte). Siehe *Konfigurieren der Hardware auf Seite 11*.
5. Die Hardwareanschlüsse überprüfen. Siehe *Seite 17*.
6. Karten und Formate konfigurieren. Siehe *Seite 18*.

Empfehlungen zur Wartung finden Sie unter *Wartungsanweisungen auf Seite 21*.

### Eine Sprache wählen

Die Standardsprache der Produktwebseite ist Englisch. Sie kann jedoch in eine beliebigen Sprache geändert werden, die in der Firmware des Produkts enthalten ist. Unter [www.axis.com](http://www.axis.com) finden Sie Informationen über die aktuell verfügbare Firmware.

Die Sprachen können auf jeder Produktwebseite geändert werden.

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

#### Hinweis

- Wenn die Sprache geändert wird, wechselt auch das Datumsformat zu einem in der gewählten Sprache üblichen Format. In den Datenfeldern wird das korrekte Format angezeigt.
- Wenn das Produkt auf die Werkseinstellungen zurückgesetzt wird, wechselt die Produktwebseite zurück zu Englisch.
- Wenn das Produkt wiederhergestellt, neugestartet oder auf eine neue Firmware aktualisiert wird, verwendet die Produktwebseite weiterhin die gewählte Sprache.

### Einstellen von Datum und Uhrzeit

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 10*.
- Manuelles Einstellen von Datum und Uhrzeit. Siehe *Seite 10*.
- Abrufen von Datum und Uhrzeit vom Computer. Siehe *Seite 10*.

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

# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

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 31*.

Wenn Sie für den NTP-Server einen Host-Namen verwenden, muss ein DNS-Server konfiguriert werden. Siehe *DNS-Konfiguration auf Seite 30*.

### Manuelles Einstellen von Datum und Uhrzeit

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

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

### Abrufen von Datum und Uhrzeit vom Computer

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

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

### Konfigurieren der Netzwerkeinstellungen

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

# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

Weitere Informationen zu Netzwerkeinstellungen, siehe *Netzwerk auf Seite 29*.

### Konfigurieren der Hardware

Türen, Schlösser und andere Geräte können vor Abschluss der Hardwarekonfiguration an das Axis Produkt angeschlossen werden. Das Anschließen von Geräten ist jedoch einfacher, wenn Sie zuerst die Hardwarekonfiguration abschließen, da nach Abschluss der Konfiguration der Kontaktbelegungsplan zur Verfügung steht. Der Kontaktbelegungsplan ist der Leitfaden zum Anschließen der Kontakte sowie die Referenz bei der Wartung. Anweisungen zur Wartung finden Sie auf *Seite 21*.

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

- Importieren einer Hardwarekonfigurationsdatei. Siehe *Seite 11*.
- Eine neue Hardwarekonfiguration erstellen. Siehe *Seite 12*.

#### Hinweis

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

### Eine Hardwarekonfigurationsdatei konfigurieren

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

Durch das Exportieren der Datei aus einem Produkt und das Importieren in ein anderes können Sie mehrere Kopien der gleichen Hardware-Einrichtung erstellen, ohne die gleichen Schritte wiederholen zu müssen. Sie können exportierte Dateien auch als Sicherungen speichern und diese zum Wiederherstellen vorheriger Hardwarekonfigurationen verwenden. Für weitere Informationen siehe *Eine Hardwarekonfigurationsdatei exportieren auf Seite 11*

So importieren Sie eine Hardwarekonfigurationsdatei:

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

### Eine Hardwarekonfigurationsdatei exportieren

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

#### Hinweis

Die Hardwarekonfiguration ganzer Etagen kann nicht exportiert werden.

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

Die Hardwarekonfigurationsdatei exportieren:

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

# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

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

### Eine neue Hardwarekonfiguration erstellen

Die Anweisungen gemäß den Installationsvorgaben befolgen:

- *Eine neue Hardwarekonfiguration ohne Peripheriegeräte erstellen. auf Seite 12*
- *Eine neue Hardwarekonfiguration für Funkschlösser erstellen. auf Seite 15*
- *Eine neue Hardwarekonfiguration mit Elevator Control (AXIS A9188) erstellen auf Seite 16*

### Eine neue Hardwarekonfiguration ohne Peripheriegeräte erstellen.

1. Setup > Hardware Configuration (Setup > Hardwarekonfiguration) aufrufen und Start new hardware configuration (Neue Hardwarekonfiguration starten) anklicken.
2. Einen Namen für das Axis Produkt eingeben.
3. Die Anzahl der angeschlossenen Türen wählen und Next (Weiter) anklicken.
4. Die Türmonitore (Türpositionssensoren) und Schlösser konfigurieren und Next (Weiter) anklicken. Weitere Informationen zu den verfügbaren Optionen, siehe *Schlösser und Türmonitore konfigurieren auf Seite 12*.
5. Die zu verwendenden Lesegeräte und REX-Geräte wählen und Finish (Beenden) anklicken. Weitere Informationen zu den verfügbaren Optionen, siehe *Konfigurieren von Lesern und REX-Geräten auf Seite 14*.
6. Close (Schließen) oder den Link zur Kontaktbelegungsübersicht anklicken.

### Schlösser und Türmonitore konfigurieren

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

1. Wenn ein Türmonitor verwendet wird, Door monitor (Türmonitor) und anschließend die den Schaltkreisen des Türmonitors entsprechenden Optionen wählen.
2. Wenn das Türschloss verriegelt werden soll, sobald die Tür geöffnet wurde, wählen Sie Cancel access time once door is opened (Zugangsdauer nach dem Öffnen der Tür begrenzen) aus.  
  
Wenn Sie die erneute Verriegelung hinauszögern möchten, setzen Sie die Verzögerungszeit in Millisekunden in Verriegelungszeit.
3. Legen Sie die Zeitoptionen für den Türmonitor fest oder, wenn kein Türmonitor verwendet wird, die Zeitoptionen für das Schloss.
4. Wählen Sie die Einstellungen passend zu den Stromkreisen des entsprechenden Schlosses aus.
5. Wenn ein Schlossmonitor verwendet wird, wählen Sie Lock monitor (Schlossmonitor) und anschließend die Optionen passend zu den Stromkreisen des entsprechenden Schlossmonitors aus.
6. Wenn Sie die Eingangsanschlüsse von Lesern, REX-Geräten und Türmonitoren überwachen möchten, wählen Sie Enable supervised inputs (Überwachte Eingänge aktivieren) aus.

Weitere Informationen, siehe *Überwachte Eingänge verwenden: auf Seite 15*

# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

### Hinweis

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

### Informationen zu Türmonitoren und Zeitoptionen

Die folgenden Türmonitor-Optionen sind verfügbar:

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

Folgende Zeitoptionen für Türen stehen immer zur Verfügung:

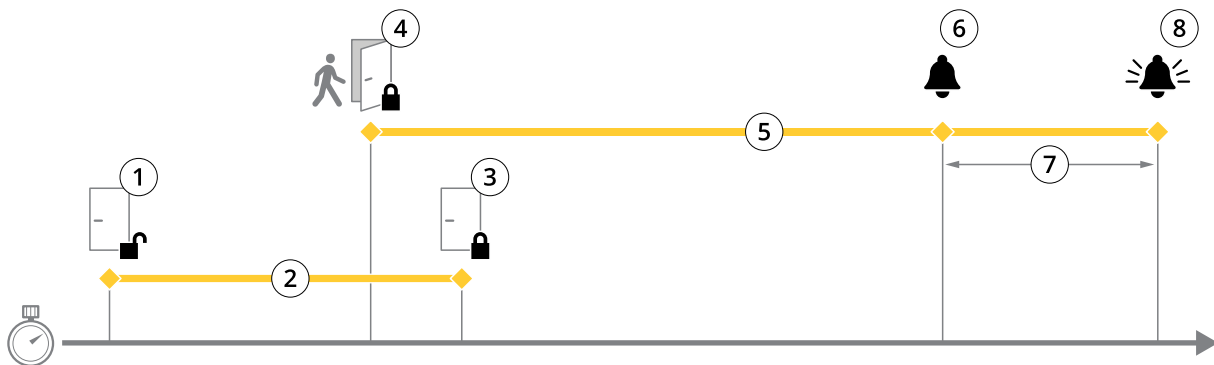
- **Zugangsdauer** – Die Anzahl von Sekunden einstellen, die die Tür geöffnet bleiben soll, nachdem Zugang gewährt wurde. Die Tür bleibt entriegelt, bis die Tür geöffnet oder die festgelegte Dauer erreicht wurde. Die Tür wird verriegelt, wenn sie geschlossen wird. Auch, wenn die Zugangsdauer nicht erreicht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

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

- **Maximale Öffnungsdauer** – Die Anzahl von Sekunden festlegen, die die Tür maximal geöffnet bleiben darf. Wenn die festgelegte Dauer erreicht wird, wird der Alarm für die maximale Öffnungsdauer ausgelöst. Eine Aktionsregel einrichten, die festlegt, welche Aktion ausgelöst werden soll, wenn die maximale Öffnungsdauer überschritten wird.
- **Voralarmdauer** – Ein Voralarm ist ein Warnsignal, das ausgelöst wird, bevor die maximale Öffnungsdauer der Tür überschritten wird. Die Aktionsregel informiert und warnt den Administrator (und je nach Konfiguration der Aktionsregel auch die Person an der Tür), dass die Tür geschlossen werden muss oder sonst der Alarm für die maximale Öffnungsdauer ausgelöst wird. Festlegen, wie viele Sekunden vor dem Auslösen eines Alarms aufgrund der Überschreitung der maximalen Öffnungsdauer das System den Voralarm auslösen soll. Legen Sie die Voralarmdauer auf 0 fest, um den Voralarm zu deaktivieren.

# AXIS A1601 Network Door Controller

## Systemkonfiguration



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

Weitere Informationen zum Einrichten einer Aktionsregel finden Sie unter *Aktionsregeln einrichten auf Seite 23*.

### Informationen zu Schlossoptionen

Verfügbare Optionen für den Schaltkreis des Schlosses:

- **Relais** – Kann nur für ein Schloss pro Türcontroller verwendet werden. Sind zwei Türen mit dem Türcontroller verbunden, kann ein Relais nur am Schloss der zweiten Tür verwendet werden.
- **Keine** – Wählen, wenn nur ein Schloss verwendet wird. Nur verfügbar für Schloss 2.

Die folgenden Schlossüberwachungsoptionen sind für Konfigurationen mit einer Tür verfügbar:

- **Lock Monitor** – Wählen, um die Lock Monitor - Steuerelemente zu aktivieren. Dann das zu überwachende Schloss wählen. Eine Schlossüberwachung kann nur bei Doppelschlossstüren verwendet werden. Sie kann nicht verwendet werden, wenn zwei Türen mit dem Türcontroller verbunden sind.
  - **Offener Schaltkreis = verriegelt** – Wählen, wenn der Schaltkreis der Schlossüberwachung normalerweise geschlossen ist. Wenn der Schaltkreis geschlossen ist, zeigt die Schlossüberwachung eine unverriegelte Tür an. Wenn der Schaltkreis geöffnet ist, zeigt die Schlossüberwachung eine verriegelte Tür an.
  - **Offener Schaltkreis = entriegelt** – Wählen, wenn der Schaltkreis der Schlossüberwachung normalerweise geöffnet ist. Wenn der Schaltkreis geöffnet ist, zeigt die Schlossüberwachung eine unverriegelte Tür an. Wenn der Schaltkreis geschlossen ist, zeigt die Schlossüberwachung eine verriegelte Tür an.

### Konfigurieren von Lesern und REX-Geräten

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

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

Wenn das REX-Signal nicht auf das Öffnen der Tür wirkt (zum Beispiel bei Türen mit Kliniken oder Druckstangen) **REX does not unlock door (Kein Öffnen der Tür durch REX)** wählen.

# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

3. Zum Anschließen von mehr als einem Leser oder REX-Gerät an den Türcontroller die vorherigen beiden Schritte für alle Lesegeräte und REX-Geräte wiederholen.

### Informationen zu Optionen für Lesegeräte und REX-Geräte

Für Lesegeräte stehen folgende Optionen zur Verfügung:

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

Für REX-Geräte stehen folgende Optionen zur Verfügung:

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

### Hinweis

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

### Überwachte Eingänge verwenden:

Diese Eingänge melden den Status der Verbindung zwischen dem Türcontroller und den Türmonitoren. Bei Unterbrechung der Verbindung wird ein Ereignis ausgelöst.

Um überwachte Eingänge zu verwenden:

1. Bringen Sie an allen verwendeten Eingängen Abschlusswiderstände an. Siehe Anschlussschaltbild unter *Seite 42*.
2. **Setup > Hardware-Rekonfiguration (Setup > Hardwareneukonfiguration)** aufrufen und **Enable supervised inputs (Überwachte Eingänge aktivieren)** wählen. Die Option Überwachte Eingänge kann auch während der Hardwarekonfiguration aktiviert werden.

### Informationen zur Kompatibilität überwachter Eingänge

Die folgenden Funktionen unterstützen überwachte Eingänge:

- Türmonitor Siehe *Türanschluss auf Seite 42*.

### Eine neue Hardwarekonfiguration für Funkschlösser erstellen.

1. **Setup > Hardware Configuration (Setup > Hardwarekonfiguration)** aufrufen und **Start new hardware configuration (Neue Hardwarekonfiguration starten)** anklicken.
2. Einen Namen für das Axis Produkt eingeben.
3. Aus der Liste der Peripheriegeräte einen Hersteller von drahtlosen Gateways wählen.
4. Um eine verdrahtete Tür anzuschließen, das Wahlfeld **1 Door (Tür)** markieren und **Next (Weiter)** anklicken. Wenn keine Tür aufgeführt ist, **Finish (Abschließen)** anklicken.

# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

5. Dem Hersteller des Schlosses entsprechend nach einem der folgenden Gliederungspunkte verfahren:
  - **ASSA Aperio:** Den Link zur Belegungsübersicht der Hardwarepins anklicken oder **Schließen und Setup > Hardware Reconfiguration (Setup > Neue Hardwarekonfiguration)** wählen, um die Konfiguration abzuschließen. Siehe dazu *Türen und Geräte des Typs Assa Aperio™ hinzufügen auf Seite 16*.
  - **SmartIntego:** Den Link zur Belegungsübersicht der Hardwarepins anklicken oder **Click here to select wireless gateway and configure doors (Hier klicken, um Funkgateways zu wählen und Türen zu konfigurieren)** wählen, um die Konfiguration abzuschließen. Siehe dazu *SmartIntego konfigurieren auf Seite 21*.

### Türen und Geräte des Typs Assa Aperio™ hinzufügen

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

So fügen Sie eine Funktür hinzu:

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

#### Hinweis

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

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

### Eine neue Hardwarekonfiguration mit Elevator Control (AXIS A9188) erstellen

#### Wichtig

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

#### Hinweis

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

1. Über die Webseite des Türcontrollers **Setup > Hardware Configuration (Hardwarekonfiguration)** aufrufen und **Start new hardware configuration (Neue Hardwarekonfiguration starten)** anklicken.
2. Einen Namen für das Axis Produkt eingeben.
3. Um ein AXIS A9188 Network I/O Relay Module aufzunehmen, aus der Liste der Netzwerkperipheriegeräte **Elevator Control** wählen, und **Next (weiter)** anklicken.
4. Einen Namen für das angeschlossene Lesegerät eingeben.
5. Das auf das Lesegerät anzuwendende Protokoll wählen und **Finish (Beenden)** wählen.



# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

6. Netzwerkperipheriegeräte anklicken, um die Konfiguration abzuschließen, siehe *Netzwerkperipheriegeräte hinzufügen und einrichten auf Seite 17* oder den Link zur Belegungsübersicht der Hardwarekontakte anklicken.

### Netzwerkperipheriegeräte hinzufügen und einrichten

#### Wichtig

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

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

#### Hinweis

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

#### Wichtig

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

### E/As und Relais in Netzwerkperipheriegeräten einrichten

#### Wichtig

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

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

## Überprüfen der Hardwareanschlüsse

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

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

# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

### Steuerelemente der Türüberprüfung

- **Door state (Türstatus)** – Den aktuellen Status von Türmonitoren, Türalarmen und Schlössern überprüfen. **Get current state (Aktuellen Status abrufen)** anklicken.
- **Lock (Verriegeln)** – Das Schloss manuell sperren. Betrifft primäre und sekundäre Schlösser (sofern vorhanden). **Lock (Verriegeln)** oder **Unlock (Entriegeln)**.
- **Lock (Verriegeln)** – Schloss manuell zum Gewähren von Zugang auslösen. Betrifft nur primäre Schlösser. **Access (Zugang)** anklicken.
- **Lesegerät: Feedback** – Das Feedback von Lesegeräten zu Befehlen überprüfen, zum Beispiel akustische Meldungen und LED-Signale. Wählen Sie den Befehl aus, und klicken Sie auf **Test (Testen)**. Die Typen des verfügbaren Feedbacks variieren je nach Leser. Weitere Informationen, siehe *Leser-Feedback auf Seite 26*. Siehe dazu auch die Anleitung des Herstellers.
- **Lesegerät: Tampering (Manipulation)** – Informationen zum letzten Manipulationsversuch aufrufen. Der erste Manipulationsversuch wird beim Installieren des Lesegeräts aufgezeichnet. **Get last tampering (Letzte Manipulation aufrufen)** anklicken.
- **Lesegerät: Card swipe (Swipe-Karte)** – Informationen zur letzten angewendeten Swipe-Karte oder anderen vom Lesegerät akzeptierten Berechtigungsnachweisen aufrufen. **Get last credential (Letzten Berechtigungsnachweis aufrufen)** anklicken.
- **REX** – Informationen zur letzten Anfrage zum Verlassen (REX) über eine Drucktaste aufrufen. Klicken Sie auf **Get last REX (Letzte REX-Betätigung abrufen)**.

### Steuerelemente der Etagenüberprüfung

- **Floor Status (Etagenstatus)** – Den aktuellen Status des Etagenzugangs überprüfen. **Get current state (Aktuellen Status aufrufen)** anklicken.
- **Floor lock & unlock (Sperren und Freigeben von Etagen)** – Etagenzugang manuell auslösen. Betrifft sowohl primäre als auch sekundäre Schlösser (sofern vorhanden). **Lock (Sperren)** oder **Unlock (Entriegeln)** anklicken.
- **Floor Access (Etagenzugang)** – Manuell zeitweiligen Etagenzugang einräumen. Betrifft nur primäre Schlösser. **Access (Zugang)** anklicken.
- **Fahrstuhllesegerät: Feedback** – Das Feedback von Lesegeräten zu Befehlen überprüfen, zum Beispiel akustische Meldungen und LED-Signale. Wählen Sie den Befehl aus, und klicken Sie auf **Test (Testen)**. Die Typen des verfügbaren Feedbacks variieren je nach Leser. Weitere Informationen, siehe *Leser-Feedback auf Seite 26*. Siehe dazu auch die Anleitung des Herstellers.
- **Fahrstuhllesegerät: Tampering (Manipulation)** – Informationen zum letzten Manipulationsversuch aufrufen. Der erste Manipulationsversuch wird beim Installieren des Lesegeräts aufgezeichnet. **Get last tampering (Letzten Manipulationsversuch aufrufen)** anklicken.
- **Fahrstuhllesegerät: Card swipe (Swipe-Karte)** – Informationen zur letzten angewendeten Swipe-Karte oder anderen vom Lesegerät akzeptierten Berechtigungsnachweisen aufrufen. **Get last credential (Letzten Berechtigungsnachweis aufrufen)** anklicken.
- **REX** – Informationen zur letzten Anfrage zum Verlassen (REX) über eine Drucktaste aufrufen. Klicken Sie auf **Get last REX (Letzte REX-Betätigung abrufen)**.

### Karten und Formate konfigurieren

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

Kartenformate aktivieren:

1. **Setup > Configure cards and formats (Setup >Karten und Formate konfigurieren)** aufrufen.

# AXIS A1601 Network Door Controller


## Systemkonfiguration


---

2. Ein oder mehrere Kartenformate wählen, die von den verbundenen Lesern unterstützt werden.

Ein neues Kartenformat erstellen:

1. **Setup >Karten und Formate konfigurieren** aufrufen.
2. **Add card format (Kartenformat hinzufügen)** aufrufen.
3. Im Dialogfenster **Add card format (Kartenformat hinzufügen)** einen Namen, eine Beschreibung und die Bitlänge des Kartenformats eingeben. Siehe *Beschreibungen der Kartenformate auf Seite 19*.
4. Klicken Sie auf **Add field map (Feldzuordnung hinzufügen)**, und geben Sie die erforderlichen Informationen in die Felder ein. Siehe *Feldzuordnungen auf Seite 19*.
5. Zum Hinzufügen von mehreren Feldzuordnungen wiederholen Sie den letzten Schritt.

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

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

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

Zum Löschen eines Kartenformats,  anklicken.

### Wichtig

- Kartenformate können nur aktiviert oder deaktiviert werden, wenn der Türcontroller im System mit mindestens einem Leser konfiguriert wurde. Siehe *Konfigurieren der Hardware auf Seite 11* und *Konfigurieren von Lesern und REX-Geräten auf Seite 14*.
- Zwei Kartenformate mit der gleichen Bitlänge können nicht gleichzeitig aktiviert sein. Wenn beispielsweise zwei Kartenformate mit 32 Bit als „Format A“ und „Format B“ definiert wurden und „Format A“ aktiviert ist, kann „Format B“ erst dann aktiviert werden, wenn „Format A“ zuvor deaktiviert wurde.
- Wenn keine Kartenformate aktiviert wurde, können die Identifikationstypen **Card raw only (Nur Rohdatenkarte)** und **Card raw and PIN (Rohdatenkarte und PIN)** verwendet werden, um eine Karte zu identifizieren und Benutzern Zugang zu gewähren. Dies wird jedoch nicht empfohlen, da Leser von verschiedenen Herstellern oder mit unterschiedlichen Einstellungen, für die Karten verschiedene Rohdaten generieren können.

### Beschreibungen der Kartenformate

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

### Feldzuordnungen

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

Beispiele gängiger Feldzuordnungen:

- `Parity` – Paritätsbits werden zum Ermitteln von Fehlern verwendet. Paritätsbits werden in der Regel an den Anfang oder das Ende einer Binärcode-Zeichenfolge gestellt. Sie geben an, ob die Anzahl der Bits gerade oder ungerade ist.
- `EvenParity` – Gerade Paritätsbits stellen sicher, dass die Zeichenfolge eine gerade Anzahl an Bits enthält. Die Bits mit dem Wert „1“ werden gezählt. Wenn die Anzahl bereits gerade ist, wird das Paritätsbit auf den

# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

Wert 0 festgelegt. Wenn die Anzahl ungerade ist, wird das Paritätsbit auf den Wert auf 1 festgelegt, sodass die Gesamtanzahl eine gerade Zahl aufweist.

- **OddParity** – Ungerade Paritätsbits stellen sicher, dass die Zeichenfolge eine ungerade Anzahl an Bits enthält. Die Bits mit dem Wert „1“ werden gezählt. Wenn die Anzahl bereits ungerade ist, wird das Paritätsbit auf den Wert 0 festgelegt. Wenn die Anzahl gerade ist, wird das Paritätsbit auf den Wert 1 festgelegt, sodass die Gesamtanzahl eine ungerade Zahl aufweist.
  - **FacilityCode** – Anlagencodes werden gelegentlich verwendet, um sicherzustellen, dass das Token dem angeforderten Zugangsdaten-Batch des Endbenutzers entspricht. In Altsystemen der Zugangskontrolle wurde der Anlagencode für eine eingeschränkte Überprüfung verwendet. Diese gewährte allen Mitarbeitern Zugang, deren Daten mit dem entsprechenden Standortcode codiert wurden. Dieser Feldzuordnungsname berücksichtigt Groß- und Kleinschreibung und wird vom Produkt zum Überprüfen der Anlagencodes benötigt
  - **CardNr** – Die Kartenummer oder Benutzerkennung ist das von Zugangskontrollsystemen am häufigsten überprüfte Kriterium. Dieser Feldzuordnungsname berücksichtigt Groß- und Kleinschreibung und wird vom Produkt zum Überprüfen der Kartenummer benötigt
  - **CardNrHex** – Die binären Kartendaten sind im Produkt in Form von Hexadezimalzahlen in Kleinschreibung codiert. Sie werden hauptsächlich für die Fehlebehebung verwendet, wenn vom Lesegerät nicht die erwartete Kartenummer ausgegeben wird.
- **Range** – (erforderlich) – Der Bereich der Feldzuordnung, zum Beispiel 1, 2–17, 18–33 und 34.
  - **Encoding** (erforderlich) – Gibt den für die jeweilige Feldzuordnung gewählten Codierungstyp an.
    - **BinLE2Int** – Die Binärdaten werden als ganze Zahlen in der Bit-Reihenfolge Little-Endian codiert. Ganze Zahlen sind Zahlen ohne Dezimalstellen. Bei der Bit-Reihenfolge Little-Endian ist das erste Bit das kleinste (mit der geringsten Bedeutung).
    - **BinBE2Int** – Die Binärdaten werden als ganze Zahlen in der Bit-Reihenfolge Big-Endian codiert. Ganze Zahlen sind Zahlen ohne Dezimalstellen. Bei der Bit-Reihenfolge Big-Endian ist das erste Bit das größte (mit der größten Bedeutung).
    - **BinLE2Hex** – Die Binärdaten werden als Hexadezimalzahlen in Kleinschreibung in der Bit-Reihenfolge Little-Endian codiert. Das Hexadezimalsystem ist ein Stellenwertsystem zur Basis 16 und verwendet 16 eindeutige Zeichen: die Ziffern 0 bis 9 und die Buchstaben a bis f. Bei der Bit-Reihenfolge Little-Endian ist das erste Bit das kleinste (mit der geringsten Bedeutung).
    - **BinBE2Hex** – Die Binärdaten werden als Hexadezimalzahlen in Kleinschreibung in der der Bit-Reihenfolge Big-Endian codiert. Das Hexadezimalsystem ist ein Stellenwertsystem zur Basis 16 und verwendet 16 eindeutige Zeichen: die Ziffern 0 bis 9 und die Buchstaben a bis f. Bei der Bit-Reihenfolge Big-Endian ist das erste Bit das größte (mit der größten Bedeutung).
    - **BinLEIBO2Int** – Die Binärdaten sind wie bei BinLE2Int codiert, aber die Rohkartendaten werden als Abfolge mehrerer Bytes in umgekehrter Reihenfolge ausgelesen, bevor Feldzuordnungen zum Kodieren aufgerufen werden.
    - **BinBEIBO2Int** – Die Binärdaten sind wie bei BinLE2Int codiert, aber die Rohkartendaten werden als Abfolge mehrerer Bytes in umgekehrter Reihenfolge ausgelesen, bevor Feldzuordnungen zum Kodieren aufgerufen werden.

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

## Dienste konfigurieren

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

### SmartIntego

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

# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

### Voraussetzungen für SmartIntego

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

- Es muss eine csv-Datei erstellt werden. Die csv-Datei enthält Informationen zum von der SmartIntego-Lösung verwendeten Gateway-Knoten und zu den zugeordneten Türen. Die Datei wird von einer eigenständigen Software erstellt. Die Software wird von einem SimonsVoss-Partner bereitgestellt.
- Die Hardwarekonfiguration von SmartIntego wurde abgeschlossen, siehe *Eine neue Hardwarekonfiguration für Funkschlösser erstellen. auf Seite 15.*

#### Hinweis

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

### SmartIntego konfigurieren

#### Hinweis

- Sicherstellen, dass die aufgeführten Anforderungen erfüllt sind.
  - Um die Sichtbarkeit des Batteriestatus zu verbessern, **Setup > Configure event and alarms logs (Protokolle für Ereignisse konfigurieren)** und entweder **Door – Battery alarm (Tür – Batteriealarm)** oder **IdPoint – Battery alarm (ID-Punkt – Batteriealarm)** als Alarm hinzufügen.
  - Die Einstellungen für den Türmonitor werden über die importierte CSV-Datei bereitgestellt. Für eine Standardinstallation müssen diese Einstellungen nicht geändert werden.
1. **Browse... (Durchsuchen...)** anklicken, die CSV-Datei wählen und **Upload file (Datei hochladen)** anklicken.
  2. Einen Gateway-Knoten wählen und **Weiter** anklicken.
  3. Eine Vorschau der neuen Konfiguration wird angezeigt. Bei Bedarf die Türmonitore deaktivieren.
  4. **Configure (Konfigurieren)** anklicken.
  5. Eine Vorschau der in die Konfiguration aufgenommenen Türen wird angezeigt. **Settings (Einstellungen)** anklicken, um jede Tür einzeln zu konfigurieren.

### SmartIntego umkonfigurieren

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

#### Hinweis

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

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

# AXIS A1601 Network Door Controller

## Systemkonfiguration

---

### Wartungsanweisungen

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

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

- Stellen Sie sicher, dass alle Verbindungen zwischen dem Tür-Controller und den externen Geräten sicher sind.
- Überprüfen Sie alle Hardware-Anschlüsse. Siehe *Steuerelemente der Türüberprüfung auf Seite 18*.
- Stellen Sie sicher, dass das System, einschließlich der angeschlossenen externen Geräte, ordnungsgemäß funktioniert.
  - Ziehen Sie eine Karte durch und testen Sie Leser, Türen und Schlösser.
  - Wenn zum System Geräte, Sensoren oder andere Geräte von REX gehören, müssen diese ebenfalls getestet werden.
  - Ebenfalls aktivierte Manipulationsalarme testen.

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

- Testen Sie die Signale der Drähte mit entsprechender Ausrüstung und überprüfen Sie, ob die Drähte oder Kabel beschädigt sind.
- Ersetzen Sie alle beschädigten oder fehlerhaften Kabel und Drähte.
- Überprüfen Sie nach dem Austauschen der Kabel und Drähte alle Hardware-Anschlüsse erneut. Siehe *Steuerelemente der Türüberprüfung auf Seite 18*.
- Wenn der Tür-Controller nicht wie erwartet funktioniert, finden Sie im *Fehlerbehebung auf Seite 37* und *Wartung auf Seite 34* weitere Informationen.

# AXIS A1601 Network Door Controller

## Ereigniskonfiguration

---


### Ereigniskonfiguration

Systemereignisse wie das Durchziehen einer Karte oder das Aktivieren eines REX-Geräts werden im Ereignisprotokoll gespeichert.

- Anzeigen des Ereignisprotokolls. Siehe *Seite 23*.
- Ereignisprotokoll exportieren Siehe .
- Ereignisprotokoll konfigurieren Siehe *Das Ereignisprotokoll konfigurieren auf Seite 23*.

### Anzeigen des Ereignisprotokolls

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

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

Mithilfe von Filtern können Sie im Ereignisprotokoll einfacher bestimmte Ereignisse finden. Um die Liste zu filtern, einen oder mehrere Ereignisprotokollfilter wählen, und **Apply filters (Filter anwenden)** anklicken. Weitere Informationen, siehe *Ereignisprotokollfilter auf Seite 23*

Als Administrator sind Sie möglicherweise an bestimmten Ereignissen besonders interessiert. Daher können Sie auswählen, welche Ereignisse protokolliert werden. Weitere Informationen, siehe *Optionen für Ereignisprotokolle auf Seite 23*

### Ereignisprotokollfilter

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

- Benutzer – Filter für Ereignisse mit Bezug auf den ausgewählten Benutzer.
- Tür und Etage – Filter für Ereignisse mit Bezug auf eine bestimmte Tür oder Etage.
- Typ – Filter für den Ereignistyp.
- Datum und Uhrzeit – Filtern des Ereignisprotokolls nach Datum und Uhrzeit

### Das Ereignisprotokoll konfigurieren

Auf der Seite Ereignisprotokoll konfigurieren werden die zu protokollierenden Ereignisse definiert.

### Optionen für Ereignisprotokolle

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

Für das Protokollieren von Ereignissen stehen folgende Optionen zur Verfügung:

- **No logging (Keine Protokollierung)** – Das Protokollieren von Ereignissen ist deaktiviert. Das Ereignis wird nicht registriert oder in das Ereignisprotokoll aufgenommen.
- **Log for all sources (Protokollieren aller Quellen)** – Ereignisaufzeichnung aktiviert. Das Ereignis wird registriert oder in das Ereignisprotokoll aufgenommen.

### Aktionsregeln einrichten

Auf den Ereignisseiten können Sie das Axis Produkt so konfigurieren, dass Aktionen bei unterschiedlichen Ereignissen ausgeführt werden. 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.

# AXIS A1601 Network Door Controller

## Ereigniskonfiguration

---

Für weitere Informationen zu den verfügbaren Auslösern und Aktionen, siehe die Hilfeseiten des Produkts.

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

1. Wechseln Sie zu **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Setup > Zusätzliche Controller-Konfiguration > Systemoptionen > Anschlüsse und Geräte > E/A-Ports)**.
2. Wählen Sie in der gewünschten Dropdown-Liste **I/O Port Type (Typ des E/A-Ports)** die Option **Output (Ausgabe)** aus und geben Sie einen **Name** ein.
3. Wählen Sie den **Normal state (Normalzustand)** des E/A-Ports aus und klicken Sie auf **Save (Speichern)**.
4. Wechseln Sie zu **Events > Action Rules (Ereignisse > Aktionsregeln)** und klicken Sie auf **Add (Hinzufügen)**.
5. Wählen Sie in der Dropdown-Liste **Trigger (Auslöser)** die Option **Door (Tür)** aus.
6. Wählen Sie in der Dropdown-Liste die Option **Door Alarm (Türalarm)** aus.
7. Wählen Sie in der Dropdown-Liste die gewünschte Tür aus.
8. Wählen Sie in der Dropdown-Liste die Option **DoorForcedOpen (Tür aufgebrochen)** aus.
9. Wählen Sie bei Bedarf einen **Schedule (Zeitplan)** und **Additional conditions (Weitere Bedingungen)** aus. Siehe unten.
10. Wählen Sie in der Dropdown-Liste **Type (Typ)** unter **Actions (Aktionen)** die Option **Output Port (Ausgangs-Port)** aus.
11. Wählen Sie in der Dropdown-Liste **Port** den gewünschten Ausgangs-Port aus.
12. Legen Sie den Zustand auf **Active (Aktiv)** fest.
13. Wählen Sie **Duration (Dauer)** und **Go to opposite state after (Danach zum Gegenzustand wechseln)** aus. Geben Sie dann die gewünschte Dauer der Aktion ein.
14. Klicken Sie auf **OK**.

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

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

Für weitere Informationen, siehe die Hilfeseiten des Produkts.

### Empfänger hinzufügen

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

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**.



# AXIS A1601 Network Door Controller

## Ereigniskonfiguration

---

### E-Mail-Empfänger einrichten

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

#### Hinweis

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

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

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

Um z. B. mithilfe eines Firmen-E-Mail-Servers einen E-Mail-Empfänger einzurichten, führen Sie die oben angeführten Schritte durch, wählen jedoch als **Provider (Anbieter)** **User defined (Benutzerdefiniert)** aus. Geben Sie im Feld **From (Von)** die als Absender anzuzeigende E-Mail-Adresse ein. Wählen Sie **Advanced settings (Erweiterte Einstellungen)** aus, und geben Sie die SMTP-Server-Adresse, den Port und die Authentifizierungsmethode an. Wählen Sie optional **Use encryption (Verschlüsselung verwenden)** aus, um E-Mails über eine verschlüsselte Verbindung zu senden. Das Server-Zertifikat kann mit dem für das Axis Produkt verfügbaren Zertifikaten validiert werden. Weitere Informationen zum Hochladen von Zertifikaten finden Sie unter *Zertifikate auf Seite 28*.

### Zeitpläne einrichten

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

So erstellen Sie einen neuen Zeitplan:

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

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

### Wiederholungen einrichten

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

So richten Sie eine Wiederholung ein:

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

# AXIS A1601 Network Door Controller

## Ereigniskonfiguration

---

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 Signaltongebnern 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-Signaltongebnern verschiedene Sequenzen an kurzen und langen Signalen als Feedback übermitteln.

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

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

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

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

# AXIS A1601 Network Door Controller

## Systemoptionen

---

### Systemoptionen

#### Sicherheit

##### Benutzer

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

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

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

##### Hinweis

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

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

##### ONVIF

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

Beim Erstellen eines Benutzers wird automatisch ONVIF-Kommunikation aktiviert. Verwenden Sie den Benutzernamen und das Kennwort für sämtliche ONVIF-Kommunikation mit dem Produkt. Weitere Informationen finden Sie unter [www.onvif.org](http://www.onvif.org).

##### IP-Adressfilter

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

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

##### HTTPS

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

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

Um HTTPS verwenden zu können, muss zunächst ein HTTPS-Zertifikat installiert werden. Um Zertifikate zu installieren und zu verwalten, diesen Optionspfad aufrufen: **Setup > Additional Controller Configuration > System Options > Security > Certificates (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Sicherheit > Sicherheitszertifikate)** Siehe *Zertifikate auf Seite 28*.

So aktivieren Sie HTTPS auf dem Axis Produkt:

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

# AXIS A1601 Network Door Controller

## Systemoptionen

---

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

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

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

### IEEE 802.1X

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

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

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

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

Um Zertifikate zu installieren und zu verwalten, diesen Optionspfad aufrufen: **Setup > Additional Controller Configuration > System Options > Security > Certificates (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Sicherheit > Sicherheitszertifikate** Siehe *Zertifikate auf Seite 28*.

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

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

#### Hinweis

Damit die Authentifizierung ordnungsgemäß funktioniert, sollten die Datums- und Uhrzeiteinstellungen des Axis Produkts mit einem NTP-Server synchronisiert werden. Siehe .

### Zertifikate

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

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

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

# AXIS A1601 Network Door Controller

## Systemoptionen

---

### Hinweis

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

### Selbstsignierte Zertifikate erstellen

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

### Ein CA-signiertes Zertifikat erstellen

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

### Weitere CA-Zertifikate installieren

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

## Netzwerk

### Grundlegende TCP/IP-Einstellungen

Das Axis Produkt unterstützt IP-Version 4 (IPv4) und IP-Version 6 (IPv6).

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

- **Dynamic IP address (Dynamische IP-Adresse) – Obtain IP address via DHCP (IP-Adresse über DHCP beziehen)**. Dies ist die Standardeinstellung. Das Axis Produkt erhält seine IP-Adresse automatisch per DHCP (Dynamic Host Configuration Protocol).  
Mithilfe von DHCP können Netzwerkadministratoren das Zuweisen von IP-Adressen zentral verwalten und automatisieren.
- **Static IP address (Statische IP-Adresse) – Um eine statische IP-Adresse zu verwenden, Use the following IP address (Folgende IP-Adresse verwenden)** wählen und die IP-Adresse, die Subnetzmaske und den Standardrouter angeben. Klicken Sie anschließend auf **Save (Speichern)**.

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

# AXIS A1601 Network Door Controller

## Systemoptionen

---

Wenn DHCP aktiviert ist, auf das Produkt jedoch nicht zugegriffen werden kann, führen Sie AXIS IP Utility aus, um im Netzwerk nach verbundenen Axis Produkten zu suchen, oder setzen Sie das Produkt auf die werksseitigen Standardeinstellungen zurück, und führen Sie die Installation anschließend erneut durch. Informationen zum Wiederherstellen der werksseitigen Standardeinstellung finden Sie unter *Seite 37*.

### 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-Diensteanbieters finden Sie unter „[www.axis.com/hosting](http://www.axis.com/hosting)“.

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

**One-click enabled (One-Click aktiviert)** – Halten Sie die Steuertaste des Produkts (siehe *Produktübersicht auf Seite 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 wird ständig versuchen, über das Internet eine Verbindung mit dem AVHS-Dienst herzustellen. Nach der Registrierung bleibt das Produkt mit dem Dienst verbunden. Diese Option kann verwendet werden, wenn das Produkt bereits installiert und die One-Click-Installation unpraktisch oder nicht möglich ist.

#### Hinweis

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

### AXIS Internet Dynamic DNS Service

Mit dem AXIS Internet Dynamic DNS Service wird ein Host-Name für den einfachen Zugriff auf das Produkt zugewiesen. Weitere Informationen finden Sie unter [www.axiscam.net](http://www.axiscam.net).

Das Axis Produkt bei AXIS Internet Dynamic DNS Service wie folgt registrieren unter: **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic Setup > Zusätzliche Controllereinstellungen > Systemoptionen > Netzwerk > TCP/IP > Einfach**. Unter **Services (Dienste)** die Schaltfläche **Settings (Einstellungen)** für AXIS Internet Dynamic DNS Service (erfordert Internetzugang) anklicken. Der aktuell bei AXIS Internet Dynamic DNS-Service für das Produkt registrierte Domänenname kann jederzeit entfernt werden.

#### Hinweis

AXIS Internet Dynamic DNS Service erfordert IPv4.

## Erweiterte TCP/IP-Einstellungen

### DNS-Konfiguration

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

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

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

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

# AXIS A1601 Network Door Controller

## Systemoptionen

---

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

### NTP-Konfiguration

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

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

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

### Host-Namen-Konfiguration

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

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

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

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

### Verknüpfen einer lokalen IPv4-Adresse

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

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

### HTTP

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

### HTTPS

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

Zum Aktivieren von HTTPS aufrufen: **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Sicherheit > HTTPS)**. Weitere Informationen, siehe *HTTPS auf Seite 27*

### NAT-Traversal (Port-Mapping) für IPv4

Mit einem Netzwerkrouter können Geräte in einem privaten Netzwerk (LAN) eine einzelne Internetverbindung gemeinsam nutzen. Dazu wird der Netzwerk-Verkehr vom privaten Netzwerk zur Außenwelt, also zum Internet, weitergeleitet. Die Sicherheit im privaten

# AXIS A1601 Network Door Controller

## Systemoptionen

---

Netzwerk (LAN) wird dadurch erhöht, da die meisten Router so vorkonfiguriert sind, dass Zugriffsversuche auf das private Netzwerk (LAN) aus dem öffentlichen Netzwerk (Internet) unterbunden werden.

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

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

### Hinweis

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

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

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

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

### Hinweis

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

## FTP

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

## RTSP

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

### Hinweis

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

## SOCKS

SOCKS ist ein Netzwerk-Proxy-Protokoll. Das Axis Produkt kann zum Verwenden eines SOCKS-Servers konfiguriert werden, um Netzwerke auf der anderen Seite einer Firewall oder eines Proxy-Servers zu erreichen. Diese Funktion ist nützlich, wenn sich das Axis



# AXIS A1601 Network Door Controller

## Systemoptionen

---

Produkt in einem lokalen Netzwerk hinter einer Firewall befindet und Benachrichtigungen, Hochladevorgänge, Alarmer usw. an ein Ziel außerhalb des lokalen Netzwerks (beispielsweise das Internet) gesendet werden müssen.

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

### QoS (Quality of Service)

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

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

### SNMP

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

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

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

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

#### Hinweis

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

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

Es stehen folgende Traps zur Verfügung:

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

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

Zur Verwendung von SNMP v3 muss HTTPS aktiviert werden, siehe *HTTPS auf Seite 27*. Um SNMP v3 zu aktivieren, aktivieren Sie das Kontrollkästchen und geben Sie das anfängliche Benutzerkennwort an.

#### Hinweis

Das anfängliche Kennwort kann nur einmal festgelegt werden. Wenn das Kennwort verloren ist, muss das Axis Produkt auf die werksseitige Standardeinstellung zurückgesetzt werden, siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 37*.

# AXIS A1601 Network Door Controller

## Systemoptionen

---

### UPnP

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

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

### Bonjour

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

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

## Ports und Geräte

### E/A-Ports

Der Zusatzanschluss bietet vier konfigurierbare Eingangs- und Ausgangsports zum Anschließen von externen Geräten.

Der externe Anschluss Produkt bietet zwei konfigurierbare Eingangs- und Ausgangsports zum Anschließen von externen Geräten.

Die E/A-Ports werden unter **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports** (**Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Ports und Geräte > E/A-Ports**) konfiguriert. Die Portrichtung (**Input** (Eingang) oder **Output** (Ausgang)) wählen. Den Ports aussagekräftige Namen geben. Den **Normal states** (Normalstatus) als **Open circuit** (Offen) oder **Grounded circuit** (Geerdet) angeben.

### Port-Status

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

## Wartung

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

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

#### Hinweis

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

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

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

# AXIS A1601 Network Door Controller

## Systemoptionen

---

**Default (Standard)** anklicken, um alle Einstellungen einschließlich der IP-Adresse auf die Werkseinstellungen zurückzusetzen. Diese Schaltfläche sollte mit Vorsicht verwendet werden. Das Axis Produkt kann auch mit der Steuertaste auf die werksseitige Standardeinstellung zurückgesetzt werden, siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 37*.

Informationen zur Firmware-Aktualisierung finden Sie unter *Die Firmware aktualisieren auf Seite 37*.

## Support

### Support-Übersicht

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

Siehe auch *Fehlerbehebung auf Seite 37*.

### Systemübersicht

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

### Protokolle und Berichte

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

**Systemprotokoll** – Enthält Informationen zu Systemereignissen.

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

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

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

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

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

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

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

## Erweitert

### Skripterstellung

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

# AXIS A1601 Network Door Controller

## Systemoptionen

---

### **HINWEIS**

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

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

Den Scripteditor öffnen über **Setup > Additional Controller Configuration > System Options > Advanced > Scripting (Setup > Zusätzliche Controllerkonfiguration > Systemoptionen > Erweitert > Skripterstellung)**. Wenn ein Skript Probleme verursacht, das Produkt auf die Werkseinstellungen zurücksetzen, siehe *Seite 37*.

Weitere Informationen finden Sie unter [www.axis.com/developer](http://www.axis.com/developer).

### **Datei-Upload**

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

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

# AXIS A1601 Network Door Controller

## Fehlerbehebung

---

### Fehlerbehebung

#### Zurücksetzen auf die Werkseinstellungen

##### Wichtig

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

So wird das Produkt auf die werksseitigen Standardeinstellungen zurückgesetzt:

1. Trennen Sie das Produkt von der Stromversorgung.
2. Drücken und halten Sie die Steuertaste, um das Gerät wieder einzuschalten. Siehe *Produktübersicht auf Seite 5*.
3. Halten Sie die Steuertaste 25 Sekunden gedrückt, bis die Status-LED zum zweiten Mal gelb leuchtet.
4. Lassen Sie die Steuertaste wieder los. Der Vorgang ist abgeschlossen, sobald die Status-LED grün aufleuchtet. Das Produkt wurde auf die Werkseinstellungen zurückgesetzt. Wenn im Netzwerk kein DHCP-Server verfügbar ist, lautet die Standard-IP-Adresse 192 . 168 . 0 . 90.
5. Mithilfe der Softwaretools für das Installieren und Verwalten, IP-Adressen zuweisen, das Kennwort festlegen und auf das Produkt zugreifen.

Außerdem besteht die Möglichkeit, bestimmte Parameter über die Webschnittstelle auf die Werkseinstellungen zurückzusetzen. Den folgenden Optionspfad aufrufen: **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Setup > Zusätzliche Controllerkonfiguration > Setup > Systemoptionen > Wartung)** und dann die Option **Default (Standardeinstellung)** anklicken.

#### Die aktuelle Firmware überprüfen

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

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

#### Die Firmware aktualisieren

##### Wichtig

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

##### Hinweis

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

# AXIS A1601 Network Door Controller

## Fehlerbehebung

---

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

## Symptome, mögliche Ursachen und Maßnahmen zur Behebung

### Probleme beim Aktualisieren der Firmware

---

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

### Probleme beim Einstellen der IP-Adresse

---

Beim Verwenden von ARP/Ping	Die Installation erneut durchführen. Die IP-Adresse muss innerhalb von zwei Minuten nach Einschalten des Produkts eingestellt werden. Sicherstellen, dass die Ping-Länge auf 408 eingestellt ist. Die Anleitung dazu befindet sich auf der Produktseite auf <a href="http://www.axis.com">www.axis.com</a> .
-----------------------------	--

Das Produkt befindet sich in einem anderen Subnetz	Wenn sich die IP-Adresse des Produkts und die IP-Adresse des zum Zugriff auf das Produkt verwendeten Computers in unterschiedlichen Subnetzen befinden, kann die IP-Adresse nicht eingestellt werden. Wenden Sie sich an Ihren Netzwerkadministrator, um eine IP-Adresse zu erhalten.
--	---

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 <code>ping</code> und die IP-Adresse des Produkts ein): <ul style="list-style-type: none"><li>• Wenn Folgendes angezeigt wird: <code>Reply from &lt;IP-Adresse&gt;: bytes=32; time=10...</code> 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.</li><li>• Wenn Folgendes angezeigt wird: <code>Request timed out</code> bedeutet dies, dass die IP-Adresse mit dem Axis Produkt verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Produkt erneut.</li></ul>
---	---

Möglicher IP-Adressenkonflikt mit einem anderen Gerät im selben Subnetz.	Die statische IP-Adresse des Axis Produkts wird verwendet, bevor der DHCP-Server eine dynamische Adresse festlegt. Wenn daher ein anderes Gerät standardmäßig dieselbe statische IP-Adresse verwendet, treten beim Zugreifen auf das Produkt möglicherweise Probleme auf.
--	---

### Vom Browser kein Zugriff auf das Produkt möglich

---

Anmelden nicht möglich	Bei aktiviertem HTTPS sicherstellen, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise muss <code>http</code> oder <code>https</code> manuell in die Adressleiste des Browsers eingegeben werden.
------------------------	--

Wenn das Kennwort für den Benutzer „root“ vergessen wurde, muss das Produkt auf die werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 37*.

# AXIS A1601 Network Door Controller

## Fehlerbehebung

---

Die IP-Adresse wurde von DHCP geändert	<p>Von einem DHCP-Server zugeteilte IP-Adressen sind dynamisch und können sich ändern. Wenn die IP-Adresse geändert wurde, das Produkt mit AXIS IP Utility oder AXIS Camera Management im Netzwerk zu ermitteln. Das Produkt anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde) ermitteln.</p> <p>Bei Bedarf kann eine statische IP-Adresse manuell zugewiesen werden. Für die Anleitung dazu, siehe das Dokument <i>Zuweisen einer IP-Adresse und Zugriff auf das Gerät</i> auf der Produktseite auf <a href="http://axis.com">axis.com</a></p>
Zertifikatfehler beim Verwenden von IEEE 802.1X	<p>Damit die Authentifizierung durchgeführt werden kann, müssen die Einstellungen des Axis Produkts für Datum und Uhrzeit mit einem NTP-Server synchronisiert sein. Siehe .</p>

### Auf das Produkt kann lokal, nicht jedoch extern zugegriffen werden

---

Routerkonfiguration	<p>Um den Router für das Zulassen eingehenden Datenverkehrs zum Axis Produkt zu konfigurieren, die Funktion NAT-Traversal aktivieren. Diese versucht, den Router automatisch für den Zugriff auf das Axis Produkt zu konfigurieren. Siehe <i>NAT-Traversal (Port-Mapping) für IPv4 auf Seite 31</i>. Der Router muss UPnP® unterstützen.</p>
Schutz durch Firewall	<p>Die Firewall zum Internet gemeinsam mit dem Netzwerkadministrator überprüfen.</p>
Standardrouter erforderlich	<p>Überprüfen, ob die Routereinstellungen unter <b>Setup &gt; Network Settings (Setup &gt; Netzwerkeinstellungen)</b> oder <b>Setup &gt; Additional Controller Configuration &gt; System Options &gt; Network &gt; TCP/IP &gt; Basic (Setup &gt; Zusätzliche Controllerkonfiguration &gt; Systemoptionen &gt; Netzwerk &gt; TCP/IP &gt; Basis)</b> konfiguriert werden müssen.</p>

# AXIS A1601 Network Door Controller

## Technische Daten

---

### Technische Daten

Der mit UL gekennzeichnete Text ist nur für Installationen gemäß UL 293 oder UL 294 gültig.

### LED-Anzeigen

LED	Farbe	Bedeutung
Netzwerk	Grün	Dauerhaft bei Verbindung mit einem 100 MBit/s-Netzwerk Blinkt bei Netzwerkaktivität.
	Gelb	Leuchtet bei Verbindung mit einem 10 MBit/s-Netzwerk. Blinkt bei Netzwerkaktivität.
	Ausgeschaltet	Keine Netzwerk-Verbindung vorhanden.
Status	Grün	Leuchtet bei Normalbetrieb grün.
	Gelb	Leuchtet beim Start und beim Wiederherstellen der Einstellungen.
	Rot	Blinkt langsam bei einem Aktualisierungsfehler.
Stromversorgung	Grün	Normalbetrieb.
	Gelb	Blinkt während einer Firmwareaktualisierung grün/gelb.
Überspannungs-Relais	Rot	Dauerhaft bei Kurzschluss oder Überspannung.
	Ausgeschaltet	Normalbetrieb.
Überspannung Lesegerät	Rot	Dauerhaft bei Kurzschluss oder Überspannung.
	Ausgeschaltet	Normalbetrieb.
Relais	Grün	Relais aktiv. <sup>1</sup>
	Ausgeschaltet	Relais nicht aktiv.

1. Aktives Relais wenn COM an NO angeschlossen.

#### Hinweis

- Die Status-LED kann so eingestellt werden, dass sie bei einem aktiven Ereignis blinkt.
- 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.

## Tasten

### Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 37*.

## Anschlüsse

### Netzwerk-Anschluss

RJ45-Ethernetanschluss mit Power over Ethernet Plus (PoE+).

UL: Power over Ethernet (PoE) wird von einem UL 294 gelisteten Power over Ethernet IEEE 802.3 AF/802.3at Typ 1 Klasse 3 oder Power over Ethernet Plus (PoE+) IEEE 802.3at Typ 2 Klasse 4 Power Limited Injector geliefert, der 44 bis 57 V Gleichstrom, 15,4 W/30 W liefert. Power over Ethernet (PoE) wurde durch UL mit AXIS T8133 Midspan 30 W 1-Port bewertet.



# AXIS A1601 Network Door Controller

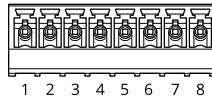
## Technische Daten

### Lesegerätanschluss

Zwei achtpolige Anschlussblöcke für die Kommunikation mit dem Lesegerät (unterstützt die Protokolle RS-485 und Wiegand).

Die angegebene Ausgangsleistung wird von den Ports beider Lesegeräte gemeinsam genutzt. Eine Ausgangsleistung von 486 mA mit 12 V ist somit für alle an den Türcontroller angeschlossenen Lesegeräte reserviert.

Auf der Webseite des Produkts das zu verwendende Protokoll wählen.



#### Konfiguriert für RS-485

Funktion	Kontakt	Hinweis	Technische Daten
Erdung (GND) Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang (+12 V)	2	Versorgt das Lesegerät mit Strom.	12 V Gleichstrom, max. 486 mA kombiniert für beide Lesegeräte
RX/TX	3-4	Vollduplex: RX. Halbduplex: RX/TX.	
TX	5-6	Vollduplex: TX	
Konfigurierbar (Ein- oder Ausgang)	7-8	Digitaleingang – Zum Aktivieren mit Kontakt 1 verbinden; zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom
		Digitaler Ausgang – Bei Verwendung mit einer induktiven Last, wie etwa einem Relais, muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA

#### Wichtig

- Bei Stromversorgung des Lesers über den Controller beträgt die zulässige Kabellänge maximal 200 m.
- Erfolgt die Stromversorgung des Lesers nicht über den Controller, beträgt die zulässige Datenkabellänge maximal 1000 m, sofern die folgenden Kabelanforderungen erfüllt sind: 1 Twisted Pair geschirmt, AWG 24, Impedanz 120 Ohm.

#### Für Wiegand konfiguriert

Funktion	Kontakt	Hinweis	Technische Daten
Erdung (GND) Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang (+12 V)	2	Versorgt das Lesegerät mit Strom.	12 V Gleichstrom, max. 486 mA kombiniert für beide Lesegeräte
D0	3		
D1	4		
0	5-6	Digitalausgang, Open Drain	

# AXIS A1601 Network Door Controller

## Technische Daten

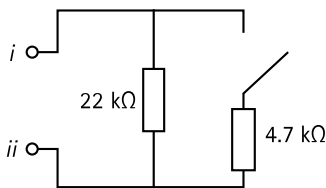
Konfigurierbar (Ein- oder Ausgang)	7-8	Digitaleingang – Zum Aktivieren mit Kontakt 1 verbinden; zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom
		Digitaler Ausgang – Bei Verwendung mit einer induktiven Last, wie etwa einem Relais, muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA

### Wichtig

- Bei Stromversorgung des Lesers über den Controller beträgt die zulässige Kabellänge maximal 150 m.
- Erfolgt die Stromversorgung des Lesers nicht über den Controller, beträgt die zulässige Datenkabellänge maximal 150 m, sofern die folgenden Kabelanforderungen erfüllt sind: AWG 22.

### Überwachte Eingänge

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



*i* Eingang

*ii* 0 V Gleichstrom (-)

UL: Überwachte Eingänge wurden von UL nicht für die Verwendung bei Einbruch evaluiert. Nur Türmonitor und REX unterstützen das Überwachen mit Abschlusswiderständen.

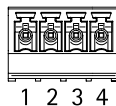
### Hinweis

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

### Türanschluss

Zwei vierpolige Anschlussblöcke für Türüberwachungsgeräte (Digitaleingang).

Nur der Türmonitor unterstützt das Überwachen mit Abschlusswiderständen. Bei Unterbrechen der Verbindung wird ein Alarm ausgelöst. Um überwachte Eingänge zu verwenden, Abschlusswiderstände anbringen. Das Anschlussschaltbild für überwachte Eingänge beachten. Siehe Seite 42.



# AXIS A1601 Network Door Controller

## Technische Daten

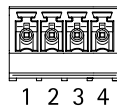
Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1, 3		0 V Gleichstrom
Eingang	2, 4	Zum Kommunizieren mit der Türüberwachung. Digitaleingang oder überwachter Eingang – Zum Aktivieren mit Kontakt 1 oder 3 verbinden. Zum Türanlage nicht anschließen.	0 bis max. 30 V Gleichstrom

### Wichtig

Das Kabel darf bis zu 30 m lang sein, wenn es folgende Anforderungen erfüllt: AWG 24.

### Relaisanschluss

Zwei vierpolige Anschlussblocks für Relais Typ C, die zum Beispiel ein Schloss oder eine Schnittstelle zu einem Tor steuern.



Funktion	Kontakt	Hinweise	Technische Daten
Erdung (GND) Gleichstrom	1		0 V Gleichstrom
NO	2	Normal offen Zum Anschließen von Relaisgeräten. Ein ausfallsicheres Schloss an NO und Erdung Gleichstrom anschließen. Sofern die Brücken nicht verwendet werden, sind die beiden Relaiskontakte galvanisch von der übrigen Schaltung getrennt.	Maimalstrom = 2 A pro Relais Maximalspannung = 30 V Gleichstrom
COM	3	Gemeinsam	
NC	4	Normal geschlossen Zum Anschließen von Relaisgeräten. Ein ausfallsicheres Schloss an NC und Erdung Gleichstrom anschließen. Sofern die Brücken nicht verwendet werden, sind die beiden Relaiskontakte galvanisch von der übrigen Schaltung getrennt.	

### Relaisstrombrücke

Die Relaisstrombrücke überbrückt 12 V Gleichstrom oder 24 V Gleichstrom und den Relaiskontakt COM.

Mit ihr kann ein Schloss an die Kontakte GND und NO oder GND und NC geschaltet werden.

Stromquelle	Maximale Leistung bei 12 V Gleichstrom <sup>1</sup>	Maximale Leistung bei 24 V Gleichstrom <sup>1</sup>
Gleichstrom IN	1600 mA	800 mA
PoE	800 mA	400 mA

1. . Die Leistung wird von beiden Relais und AUX E/A 12 V Gleichstrom genutzt.

### HINWEIS

Wir empfehlen, nichtpolare Schlösser mit einer externen Schutzdiode auszustatten.

# AXIS A1601 Network Door Controller

## Technische Daten

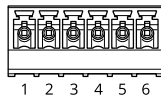
### Zusatzanschluss

Über den Zusatzanschluss werden externe Geräte für Funktionen wie Manipulationsalarm, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigung und andere angeschlossen. Abgesehen vom Bezugspunkt 0 V Gleichstrom und Strom (Gleichstromausgang) verfügt der Zusatzanschluss über eine Schnittstelle zum:

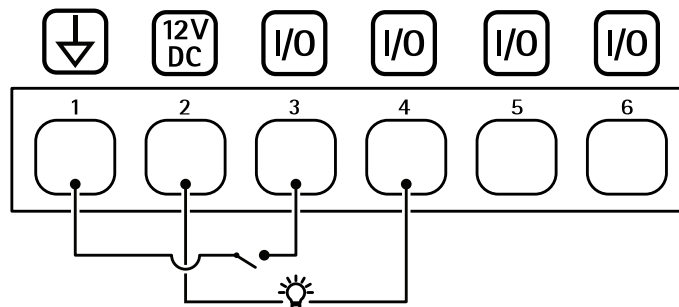
**Digitaleingang** – Zum Anschließen von Geräten, die zwischen geöffnetem und geschlossenem Schaltkreis wechseln können wie etwa PIR-Sensoren, Tür- und Fensterkontakte sowie Glasbruchmelder.

**Digitalausgang** – Zum Anschluss externer Geräte wie Relais und LEDs. Die angeschlossenen Geräte können über das VAPIX® Application Programming Interface oder über die Produktwebsite aktiviert werden.

Sechspoliger Anschlussblock



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	Darf für die Stromversorgung von Zusatzgeräten verwendet werden. Hinweis: Dieser Kontakt darf nur für den Stromausgang verwendet werden.	12 V Gleichstrom max. Last = 50 mA für jeden E/A
Konfigurierbar (Ein- oder Ausgang)	3-6	Digitaleingang – zum Aktivieren an Kontakt 1 anschließen; zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom
		Digitaler Ausgang – Interne Verbindung mit Kontakt 1 (Gleichstrom Erdschluss), wenn aktiviert; unverbunden, wenn deaktiviert. Bei Verwendung mit einer induktiven Last wie etwa einem Relais muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden. Jeder E/A kann eine 12-V-Gleichstrom-, 50 mA (max.) externe Last antreiben, wenn ein interner 12-V-Gleichstromausgang (Pin 2) verwendet wird. Bei Verwendung von Open-Drain-Verbindungen in Kombination mit einem externen Netzteil kann der E/A die Gleichstromversorgung von 0 bis 30 V Gleichstrom, 100 mA, verwalten.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA



- 1 Erdung Gleichstrom
- 2 Gleichstromausgang 12 V
- 3 E/A als Eingang konfiguriert
- 4 E/A als Ausgang konfiguriert
- 5 Konfigurierbarer E/A
- 6 Konfigurierbarer E/A

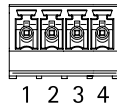
# AXIS A1601 Network Door Controller

## Technische Daten

### Externer Anschluss

Vierpoliger Anschlussblock für externe Geräte wie Glasbruchmelder oder Feuermelder.

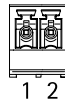
UL: Der Anschluss wurde nicht für die Verwendung als Einbruch- und Feueralarm von UL bewertet.



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1, 3		0 V Gleichstrom
Konfigurierbar (Ein- oder Ausgang)	2, 4	Digitaleingang – zum Aktivieren an Kontakt 1 oder 3 anschließen; zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom
		Digitalausgang – zum Aktivieren an Kontakt 1 oder 3 anschließen; zum Deaktivieren nicht anschließen. Bei Verwendung mit einer induktiven Last, wie etwa einem Relais, muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA

### Stromanschluss

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



Funktion	Kontakt	Hinweise	Technische Daten
0 V Gleichstrom (-)	1		0 V Gleichstrom
Gleichstromeingang	2	Stromversorgung des Controllers ohne Power over Ethernet. Hinweis: Dieser Kontakt kann nur für den Stromeingang verwendet werden.	10,5–28 V Gleichstrom, max. 36 W

UL: Die Gleichstromleistung muss je nach Anwendung über ein UL 294-, UL 293- oder UL 603-gelistetes Netzteil mit entsprechenden Nennleistungen bereitgestellt werden.

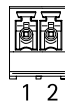
### Anschlusseingang Sicherungsbatterie

Für eine Backup-Lösung unter Verwendung einer Batterie mit integriertem Ladegerät. Gleichstromeingang 12 V.

UL: Der Anschluss wurde nicht von UL bewertet.

#### Wichtig

Wenn der Batterieeingang verwendet wird, muss eine externe, träge Sicherung mit 3 A in Reihe geschaltet werden.



# AXIS A1601 Network Door Controller

## Technische Daten

---

Funktion	Kontakt	Hinweise	Technische Daten
0 V Gleichstrom (-)	1		0 V Gleichstrom
Batterieingang	2	Für die Stromversorgung des Türmonitors bei Ausfall anderer Stromquellen. Hinweis: Dieser Kontakt kann nur als Batteriestrom verwendet werden. Nur für den Anschluss an USV.	11– 13.7 V Gleichstrom, max 36 W

# AXIS A1601 Network Door Controller

## Sicherheitsinformationen

---

### Sicherheitsinformationen

#### Gefährdungsstufen

**▲GEFAHR**

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

**▲WARNUNG**

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

**▲VORSICHT**

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

**HINWEIS**

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

#### Andere Meldeebenen

**Wichtig**

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

**Hinweis**

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

# AXIS A1601 Network Door Controller

## Geräteschnittstelle









---

### Geräteschnittstelle

Um die Geräteschnittstelle zu erreichen, müssen Sie die IP-Adresse des Geräts in einen Web-Browser eingeben.

#### Hinweis

Dieser Abschnitt betrifft nur AXIS A1601 Network Door Controller mit AXIS Camera Station Secure Entry Firmware.

-  Hauptmenü anzeigen oder ausblenden.
-  Auf die Hilfe zum Produkt zugreifen.
-  Die Sprache ändern.
-  Helles oder dunkles Design einstellen.
-  Das Benutzermenü enthält:
  - Informationen zum angemeldeten Benutzer.
  -  Benutzer ändern: Darüber können Sie den aktuellen Benutzer ab- und einen neuen Benutzer anmelden.
  -  Abmelden: Darüber melden Sie den aktuellen Benutzer ab.
-  Das Kontextmenü enthält:
  - **Analysedaten:** Stimmen Sie der Teilung nicht personenbezogener Browserdaten zu.
  - **Feedback:** Teilen Sie Feedback, um Ihr Benutzererlebnis zu verbessern.
  - **Rechtliches:** Lassen Sie sich Informationen zu Cookies und Lizenzen anzeigen.
  - **Info:** Lassen Sie sich Geräteinformationen, einschließlich Firmwareversion und Seriennummer anzeigen.
  - **Frühere Benutzeroberfläche:** Wechseln Sie zur früheren Benutzeroberfläche.

### Status

#### NTP-Synchronisierung

Zeigt Informationen zur NTP-Synchronisierung an, z. B. ob das Gerät mit einem NTP-Server synchronisiert ist und wie lange es noch bis zur nächsten Synchronisierung dauert.

**NTP-Einstellungen:** Klicken Sie darauf, um zur Seite Datum und Uhrzeit zu wechseln, auf der Sie die NTP-Einstellungen ändern können.

#### Geräteinformationen

Zeigt die Geräteinformationen an, einschließlich Firmwareversion und Seriennummer.

**Firmwareaktualisierung:** Klicken Sie darauf, um zur Wartungsseite zu gehen, auf der Sie eine Firmwareaktualisierung durchführen können.



# AXIS A1601 Network Door Controller

## Geräteschnittstelle

---

### Zutrittskontrolle

#### Alarme

**Gerätebewegung:** Diese Option ist standardmäßig aktiviert, um einen Alarm in Ihrem System auszulösen, wenn eine Gerätebewegung des Zugangscontrollers erkannt wird.

**Gehäuse geöffnet:** Diese Option ist standardmäßig aktiviert, um einen Alarm in Ihrem System auszulösen, wenn ein geöffnetes Gehäuse des Zugangscontrollers erkannt wird.

**Externe Manipulation:** Sie ist an E/A 13 angeschlossen. Aktivieren Sie diese Option, um bei erkannter externer Manipulation einen Alarm in Ihrem System auszulösen. Zum Beispiel, wenn der externe Schrank geöffnet oder geschlossen wird.

**Überwachter Eingang:** Aktivieren Sie den Eingangsstatus des Monitors und konfigurieren Sie die Abschlusswiderstände.

- Um die parallele erste Verbindung zu verwenden, wählen Sie **Parallele erste Verbindung mit parallelem Widerstand (22 22 KΩ) und seriellen Widerstand (4,7 22 KΩ)**.
- Wählen Sie für eine Serienschaltung Sie **Serienschaltung** und in der Auswahlliste **Widerstandswerte** einen Widerstandswert.

#### Peripheriegeräte

**Upgrade readers (Leser aktualisieren):** Klicken Sie hier, um Leser auf eine neue Firmware-Version zu aktualisieren. Nur der AXIS A4020-E Reader kann aktualisiert werden, wenn er online ist.

### System

#### Datum und Uhrzeit

Das Zeitformat hängt von den Spracheinstellungen des Webbrowsers ab.

##### Hinweis

Wir empfehlen Ihnen, Datum und Uhrzeit des Geräts mit einem NTP-Server zu synchronisieren.

**Synchronisierung:** Wählen Sie eine Option zur Synchronisierung von Datum und Uhrzeit des Geräts aus.

- **Automatic date and time (manual NTS KE servers) (Datum und Uhrzeit automatisch (manuelle NTS-KE-Server)):** Diese Option führt eine Synchronisierung mit den sicheren NTP-Schlüssel-Servern durch, die mit dem DHCP-Server verbunden sind.
  - **Manual NTS KE servers (Manuelle NTS-KE-Server):** Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
- **Automatic date and time (NTP servers using DHCP) (Datum und Uhrzeit automatisch (NTP-Server mit DHCP)):** Synchronisieren Sie das Gerät mit den NTP-Servern, die mit dem DHCP-Server verbunden sind.
  - **Fallback NTP servers (NTP-Reserve-Server):** Geben Sie die IP-Adresse eines oder zweier Reserve-Server ein.
- **Automatic date and time (manual NTP servers) (Datum und Uhrzeit automatisch (manuelle NTP-Server)):** Führen Sie eine Synchronisierung mit NTP-Servern Ihrer Wahl durch.
  - **Manual NTP servers (Manuelle NTP-Server):** Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
- **Benutzerdefinierte Datum und Uhrzeit:** Stellen Sie Datum und Uhrzeit manuell ein. Klicken Sie auf **Vom System abrufen**, um die Datums- und Uhrzeiteinstellungen einmalig von Ihrem Computer oder Mobilgerät zu abrufen.

**Zeitzone:** Wählen Sie die zu verwendende Zeitzone aus. Die Zeit wird automatisch bei Sommer- und Standardzeit angepasst.

##### Hinweis

Die Einstellungen für Datum und Uhrzeit werden vom System für alle Aufzeichnungen, Protokolle und Systemeinstellungen verwendet.

# AXIS A1601 Network Door Controller

## Geräteschnittstelle

---

### Netzwerk

#### IPv4

**Assign IPv4 automatically (IPv4 automatisch zuweisen):** Wählen Sie diese Option, damit der Netzwerkrouter dem Gerät automatisch eine IP-Adresse zuweisen kann. Für die meisten Netzwerke empfehlen wir eine automatische Zuweisung der IP-Adresse (DHCP).

**IP address (IP-Adresse):** Geben Sie für das Gerät eine eindeutige IP-Adresse ein. Statische IP-Adressen können innerhalb von isolierten Netzwerken zufällig zugewiesen werden, sofern jede Adresse eindeutig ist. Zur Vermeidung von Konflikten empfehlen wir Ihnen, sich vor dem Zuweisen einer statischen IP-Adresse an den Netzwerkadministrator zu wenden.

**Subnet mask (Subnetzmaske):** Geben Sie die Subnetzmaske ein, um festzulegen, welche Adressen sich im lokalen Netzwerk befinden. Jede Adresse außerhalb des lokalen Netzwerks wird über den Router geleitet.

**Router:** Geben Sie die IP-Adresse des Standardrouters (Gateway) ein, um Geräten zu verbinden, die in verschiedenen Netzwerken und Netzwerk-Segmenten verwendet werden.

#### IPv6

**Assign IPv6 automatically (IPv6 automatisch zuweisen):** Wählen Sie diese Option aus, um IPv6 einzuschalten und damit der Netzwerkrouter dem Gerät automatisch eine IP-Adresse zuweisen kann.

#### Host-Name

**Assign hostname automatically (Host-Namen automatisch zuweisen):** Wählen Sie diese Option aus, damit der Netzwerkrouter dem Gerät automatisch einen Host-Namen zuweisen kann.

**Host-Name:** Geben Sie den Host-Namen manuell ein, um ihn als alternative Möglichkeit für den Zugriff auf das Gerät zu verwenden. Der Host-Name wird im Server-Bericht und im Systemprotokoll verwendet. Zugelassene Zeichen sind A-Z, a-z, 0-9 und -).

#### DNS servers (DNS-Server)

**Assign DNS automatically (DNS automatisch zuweisen):** Wählen Sie diese Option aus, damit der Netzwerkrouter dem Gerät automatisch Domains für die Suche und DNS-Server-Adressen zuweisen kann. Für die meisten Netzwerke empfehlen wir eine automatische Zuweisung der DNS-Server-Adresse (DHCP).

**Search domains (Suchdomains):** Wenn Sie einen Host-Namen verwenden, der nicht vollständig qualifiziert ist, klicken Sie auf **Add search domain (Suchdomain hinzufügen)** und geben Sie eine Domain ein, in der nach dem vom Gerät verwendeten Host-Namen gesucht werden soll.

**DNS servers (DNS-Server):** Klicken Sie auf **Add DNS server (DNS-Server hinzufügen)** und geben Sie die IP-Adresse des DNS-Servers ein. Dadurch werden in Ihrem Netzwerk Host-Namen in IP-Adressen übersetzt.

#### HTTP und HTTPS

**Zugriff zulassen über:** Wählen Sie aus, ob Sie einem Benutzer erlauben wollen, eine Verbindung mit dem Gerät über die Protokolle HTTP, HTTPS oder HTTP und HTTPS herzustellen.

HTTPS ist ein Protokoll, das Verschlüsselung für Seitenanforderungen von Benutzern und für die vom Webserver zurückgegebenen Seiten bereitstellt. Der verschlüsselte Austausch von Informationen wird durch die Verwendung eines HTTPS-Zertifikats geregelt, das die Authentizität des Servers gewährleistet.

Um HTTPS auf dem Gerät verwenden zu können, muss ein HTTPS-Zertifikat installiert werden. Gehen Sie auf **Erstellung und Installation von Zertifikaten zu System > Sicherheit**.

#### Hinweis

Wenn Sie auf verschlüsselte Internetseiten über HTTPS gehen, kann es zu Beeinträchtigungen der Leistung kommen, insbesondere wenn Sie eine Seite zum ersten Mal aufrufen.

# AXIS A1601 Network Door Controller

## Geräteschnittstelle

---

**HTTP-Port:** Geben Sie den zu verwendenden HTTP-Port ein. Port 80 oder ein beliebiger Port im Bereich 1024–65535 sind zulässig. Wenn Sie als Administrator angemeldet sind, können Sie auch einen beliebigen Port im Bereich 1–1023 eingeben. Wenn Sie einen Port in diesem Bereich verwenden, erhalten Sie eine Warnung.

**HTTPS-Port:** Geben Sie den zu verwendenden HTTPS-Port ein. Port 443 oder ein beliebiger Port im Bereich 1024–65535 sind zulässig. Wenn Sie als Administrator angemeldet sind, können Sie auch einen beliebigen Port im Bereich 1–1023 eingeben. Wenn Sie einen Port in diesem Bereich verwenden, erhalten Sie eine Warnung.

**Zertifikat:** Wählen Sie ein Zertifikat, um HTTPS für das Gerät zu aktivieren.

### Anzeigename

**Bonjour®:** Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

**Bonjour-Name:** Geben Sie den im Netzwerk anzuzeigenden Namen an. Der Standardname setzt sich aus dem Namen des Geräts und seiner MAC-Adresse zusammen.

**UPnP® verwenden:** Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

**UPnP-Name:** Geben Sie den im Netzwerk anzuzeigenden Namen an. Der Standardname setzt sich aus dem Namen des Geräts und seiner MAC-Adresse zusammen.

### Cloud-Anbindung mit einem Mausklick

One-Click Cloud Connect (O3C) stellt in Verbindung mit einem O3C-Dienst einen einfachen und sicheren Internetzugang zu Live-Video und aufgezeichneten Videos von jedem Standort aus bereit. Weitere Informationen finden Sie unter [axis.com/end-to-end-solutions/hosted-services](http://axis.com/end-to-end-solutions/hosted-services).

#### O3C zulassen:

- **One-click:** Die Standardeinstellung. Halten Sie die Steuertaste am Gerät gedrückt, um über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Sie müssen das Gerät innerhalb von 24 Stunden nach dem Drücken der Steuertaste beim O3C-Dienst registrieren. Andernfalls wird sich das Gerät vom O3C-Dienst getrennt. Nach der Registrierung des Geräts ist **Immer** aktiviert und das Gerät bleibt mit dem O3C-Dienst verbunden.
- **Immer:** Das Gerät versucht ständig, über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Nach der Registrierung bleibt das Gerät mit dem O3C-Dienst verbunden. Verwenden Sie diese Option, wenn die Steuertaste am Gerät außer Reichweite ist.
- **No (Nein):** Deaktiviert den O3C-Dienst.

**Proxyeinstellungen:** Geben Sie falls erforderlich die Proxyeinstellungen ein, um eine Verbindung zum HTTP-Server herzustellen.

**Host:** Geben Sie die Adresse des SIP-Proxyservers ein.

**Port:** Geben Sie die Nummer der für den Zugriff verwendeten Ports an.

**Anmeldung und Kennwort:** Geben Sie falls erforderlich einen Benutzernamen und ein Kennwort für den Proxyserver ein.

#### Authentication method (Authentifizierungsmethode):

- **Basic (Einfach):** Diese Methode ist das am besten geeignete Authentifizierungsschema für HTTP. Sie ist nicht so sicher wie die **Digest**-Methode, da sie den Benutzernamen und das Kennwort unverschlüsselt an den Server sendet.
- **Digest:** Diese Methode ist sicherer, da das Kennwort hier stets verschlüsselt im Netzwerk übermittelt wird.
- **Auto:** Bei dieser Option kann das Gerät die Authentifizierungsmethode automatisch je nach unterstützten Methoden auswählen. Die Methode **Digest** wird gegenüber der Methode **Einfach** bevorzugt.

**Besitzerauthentifizierungsschlüssel (OAK):** Klicken Sie auf **Schlüssel abrufen**, um den Besitzerauthentifizierungsschlüssel abzurufen. Dies ist nur dann möglich, wenn das Gerät ohne Firewall oder Proxy mit dem Internet verbunden ist.

### SNMP

# AXIS A1601 Network Door Controller

## Geräteschnittstelle

Simple Network Management Protocol (SNMP) ermöglicht die Remoteverwaltung von Netzwerk-Geräten.

SNMP: Wählen Sie die zu verwendende SNMP-Version.

- **v1 und v2c:**
  - **Lese-Community:** Geben Sie den Namen der Community mit ausschließlich Lesezugriff auf alle unterstützten SNMP-Objekte an. Der Standardwert ist **öffentlich**.
  - **Schreib-Community:** Geben Sie den Namen der Community mit Lese- und Schreibzugriff auf alle unterstützten SNMP-Objekte (außer Objekte mit Nur-Lesezugriff) an. Der Standardwert ist **schreiben**.
  - **Traps aktivieren:** Aktivieren Sie die Option, um Trap-Berichte zu erhalten. Traps werden vom Gerät bei wichtigen Ereignissen und Statusänderungen zum Versenden von Meldungen verwendet. In der Geräteschnittstelle können Sie Traps für SNMP v1 und v2c einrichten. Traps werden automatisch deaktiviert, wenn Sie zu SNMP v3 wechseln oder SNMP deaktivieren. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.
  - **Trap-Adresse:** Geben Sie die IP-Adresse oder den Host-Namen des Verwaltungsservers ein.
  - **Trap-Community:** Geben Sie die Trap-Community ein, die das Gerät zum Versenden einer Trap-Meldung an das Verwaltungssystem verwenden soll.
  - **Traps:**
    - **Kaltstart:** Versendet eine Trap-Nachricht, wenn das Gerät hochgefahren wird.
    - **Warmstart:** Versendet eine Trap-Nachricht, wenn Sie eine SNMP-Einstellung ändern.
    - **Verbindungsaufbau:** Versendet eine Trap-Meldung, wenn der Status eines Links von Down zu Up wechselt.
    - **Authentifizierung fehlgeschlagen:** Versendet eine Trap-Meldung, wenn ein Authentifizierungsversuch fehlschlägt.

### Hinweis

Alle Axis Video MIB-Traps sind aktiviert, wenn Sie SNMP v1- und v2c-Traps aktivieren. Weitere Informationen finden Sie unter *AXIS OS Portal > SNMP*.

- **v3:** SNMP v3 ist eine Version mit höherer Sicherheit, die Verschlüsselung und sichere Kennwörter bereitstellt. Beim Verwenden von SNMP v3 empfehlen wir Ihnen, HTTPS zu aktivieren, da Kennwörter dann über HTTPS gesendet werden. Dadurch wird auch verhindert, dass Unbefugte auf unverschlüsselte Traps des Typs SNMP v1 und v2c zugreifen können. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.
  - **Kennwort für das Konto "initial":** Geben Sie das SNMP-Kennwort für das Konto mit dem Namen "initial" ein. Obwohl das Kennwort ohne Aktivierung von HTTPS gesendet werden kann, empfehlen wir es nicht. Das Kennwort für SNMP v3 kann nur einmal und vorzugsweise dann bei aktiviertem HTTPS festgelegt werden. Nach dem Einrichten des Kennworts wird das Kennwortfeld nicht mehr angezeigt. Wenn ein neues Kennwort eingerichtet werden soll, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden.

### Verbundene Clients

In der Liste werden alle Clients angezeigt, die mit dem Gerät verbunden sind.

**Aktualisieren:** Klicken Sie darauf, um die Liste zu aktualisieren.

### Sicherheit

#### Zertifikate

# AXIS A1601 Network Door Controller

## Geräteschnittstelle

Zertifikate werden in Netzwerken zum Authentifizieren von Geräten verwendet. Das Gerät unterstützt zwei Zertifikattypen:

- **Client-/Serverzertifikate**  
Ein Client-/Serverzertifikat identifiziert das Axis Produkt und kann selbstsigniert oder von einer Zertifizierungsstelle (Certificate Authority, CA) ausgegeben worden sein. Ein selbstsigniertes Zertifikat bietet begrenzten Schutz und kann vor Erhalt eines CA-Zertifikats verwendet werden.
- **CA-Zertifikate**  
CA-Zertifikate werden zum Authentifizieren von Peer-Zertifikaten verwendet, um zum Beispiel die Identität eines Authentifizierungsservers zu überprüfen, wenn das Gerät mit einem durch IEEE 802.1X geschützten Netzwerk verbunden ist. Auf dem Gerät sind mehrere CA-Zertifikate vorinstalliert.

Folgende Formate werden unterstützt:

- Zertifikatsformate: .PEM, .CER und .PFX
- Formate von privaten Schlüssel: PKCS#1 und PKCS#12

### Wichtig

Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen, werden alle Zertifikate gelöscht. Vorinstallierte CA-Zertifikate werden neu installiert.



Die Zertifikate in der Liste filtern.



Zertifikat hinzufügen : Klicken Sie, um ein Zertifikat hinzuzufügen.



Das Kontextmenü enthält:

- **Informationen zum Zertifikat:** Lassen Sie sich die Eigenschaften eines installierten Zertifikats anzeigen.
- **Zertifikat löschen:** Löschen Sie das Zertifikat.
- **Signierungsanforderung erstellen:** Erstellen Sie eine Anforderung zur Zertifikatsignierung, um sie an eine Registrierungsstelle zu senden und ein digitales Zertifikat zu erhalten.

## IEEE 802.1x

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

Zum Zugriff auf ein mit IEEE 802.1x geschütztes Netzwerk müssen sich die Netzwerk-Geräte authentifizieren. Die Authentifizierung erfolgt durch einen Authentifizierungsserver, üblicherweise ein RADIUS-Server (zum Beispiel FreeRADIUS und Microsoft Internet Authentication Server).

### Zertifikate

Wenn die Konfiguration ohne CA-Zertifikat erfolgt, ist die Validierung des Serverzertifikats deaktiviert und das Gerät versucht, sich selbst zu authentifizieren, unabhängig vom aktuellen Netzwerk.

Bei Verwendung eines Zertifikats bei der Implementierung von Axis authentifizieren sich das Gerät und der Authentifizierungsserver mithilfe von digitalen Zertifikaten über EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).

Damit das Gerät auf ein netzwerkgeschütztes Netzwerk zugreifen darf, muss ein signiertes Clientzertifikat auf dem Gerät installiert sein.

**Clientzertifikat:** Wählen Sie ein Clientzertifikat aus, um IEEE 802,1x zu verwenden. Der Authentifizierungsserver verwendet das Zertifikat zur Validierung der Identität des Clients.

**CA-Zertifikat:** Wählen Sie ein CA-Zertifikat zur Validierung der Identität des Authentifizierungsservers. Wenn kein Zertifikat ausgewählt sind, versucht das Gerät, sich selbst zu authentifizieren, unabhängig vom Netzwerk, mit dem es verbunden ist.

**EAP-Identität:** Geben Sie die mit dem Clientzertifikat verknüpfte Identität des Benutzers ein.

**EAPOL-Version:** Wählen Sie die in dem Netzwerk-Switch verwendete EAPOL-Version.

# AXIS A1601 Network Door Controller

## Geräteschnittstelle

---

**IEEE 802.1x verwenden:** Wählen Sie diese Option aus, um das IEEE 802.1x-Protokoll zu verwenden.

### Brute-Force-Angriffe verhindern

**Blocken:** Aktivieren Sie diese Option, um Brute-Force-Angriffe zu blockieren. Ein Brute-Force-Angriff versucht über Trial-and-Error, Zugangsdaten oder Verschlüsselungsschlüssel zu erraten.

**Blockierdauer:** Geben Sie ein, wie viele Sekunden ein Brute-Force-Angriff blockiert werden soll.

**Blockierbedingungen:** Geben Sie die Anzahl der pro Sekunde zulässigen Authentifizierungsfehler ein, bevor blockiert wird. Sie können die Anzahl der zulässigen Fehler sowohl auf Seiten- als auch auf Geräteebene festlegen.

### IP-Adressfilter

**Filter verwenden:** Wählen Sie diese Option, um zu filtern, welche IP-Adressen auf das Gerät zugreifen dürfen.

**Richtlinie:** Wählen Sie, ob Sie den Zugriff für bestimmte IP-Adressen **Zulassen** oder **Verweigern** möchten.

**Adressen:** Geben Sie die IP-Nummern ein, denen der Zugriff auf das Gerät erlaubt oder verweigert wird. Sie können auch das CIDR-Format verwenden.

### Spezifisch signiertes Firmwarezertifikat

Zum Installieren von Test-Firmware oder anderer benutzerdefinierter Firmware von Axis auf dem Gerät benötigen Sie ein individuell signiertes Firmwarezertifikat. Das Zertifikat prüft, ob die Firmware sowohl vom Geräteeigentümer als auch von Axis genehmigt wurde. Die Firmware kann nur auf einem bestimmten Gerät ausgeführt werden, das anhand seiner eindeutigen Seriennummer und Chip-ID identifiziert wird. Benutzersignierte Firmwarezertifikate können nur von Axis erstellt werden, da Axis den Schlüssel zum Signieren besitzt.

Klicken Sie auf **Installieren**, um das Zertifikat zu installieren. Sie müssen das Zertifikat installieren, bevor Sie die Firmware installieren.

## Benutzer



**Benutzer hinzufügen:** Klicken Sie darauf, um einen neuen Benutzer hinzuzufügen. Es können bis zu 100 Benutzer hinzugefügt werden.

**Benutzername:** Geben Sie einen eindeutigen Benutzernamen ein.

**Neues Kennwort:** Geben Sie ein Benutzerkennwort ein. Kennwörter müssen aus 1 bis 64 Zeichen bestehen. Für das Kennwort sind nur die druckbaren Zeichen des ASCII-Codes (Code 32 bis 126), also Buchstaben, Ziffern, Satzzeichen sowie einige Sonderzeichen zulässig.

**Kennwort wiederholen:** Geben Sie das gleiche Kennwort erneut eingeben.

**Rolle:**

- **Administrator:** Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Benutzer hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Bediener:** Hat Zugriff auf alle Einstellungen, außer:
  - Alle **System**-Einstellungen.
  - Apps werden hinzugefügt.
- **Betrachter:** Darf keine Änderungen an den Einstellungen vornehmen.



Das Kontextmenü enthält:

**Benutzer aktualisieren:** Bearbeiten Sie die Eigenschaften des Benutzers.

# AXIS A1601 Network Door Controller

## Geräteschnittstelle

---

**Benutzer löschen:** Löschen Sie einen Benutzer. Der Root-Benutzer kann nicht gelöscht werden.

### MQTT

MQTT (Message Queuing Telemetry Transport) ist ein Standardprotokoll für das Internet der Dinge (IoT). Es wurde für eine vereinfachte IoT-Integration entwickelt und wird in einer Vielzahl von Branchen zum Anschließen von Remote-Geräten mit kleinem Code-Footprint und minimaler Netzwerkbandbreite verwendet. Der MQTT-Client in der Axis Geräte-Firmware kann die Integration der im Gerät erzeugten Daten und Ereignisse in Systeme vereinfachen, bei denen es sich nicht um Video Management Systeme (VMS) handelt.

Richten Sie das Gerät als MQTT-Client ein. Die MQTT-Kommunikation basiert auf zwei Entitäten, den Clients und dem Broker. Die Clients können Nachrichten senden und empfangen. Der Broker ist für das Routing von Nachrichten zwischen den Clients zuständig.

Weitere Informationen zu AXIS OS Portal finden Sie unter *AXIS OS*.

### MQTT-Client

**Verbinden:** Aktivieren oder deaktivieren Sie den MQTT-Client.

**Status:** Zeigt den aktuellen Status des MQTT-Clients an.

#### Broker

**Host:** Geben Sie den Host-Namen oder die Adresse des MQTT-Servers ein.

**Protokoll:** Wählen Sie das zu verwendende Protokoll aus.

**Port:** Geben Sie die Portnummer ein.

- 1883 ist der Standardwert für MQTT über TCP
- 8883 ist der Standardwert für MQTT über SSL
- 80 ist der Standardwert für MQTT über WebSocket
- 443 ist der Standardwert für MQTT über WebSocket Secure

**Benutzername:** Geben Sie den Benutzernamen ein, den der Client für den Zugriff auf den Server verwenden soll.

**Kennwort:** Geben Sie ein Kennwort für den Benutzernamen ein.

**Client-ID:** Geben Sie eine Client-ID ein. Die Client-ID wird an den Server gesendet, wenn der Client eine Verbindung herstellt.

**Sitzung bereinigen:** Steuert das Verhalten bei Verbindung und Trennungszeit. Wenn diese Option ausgewählt ist, werden die Statusinformationen beim Verbinden und Trennen verworfen.

**Keep-Alive-Intervall:** Mit dem Keep-Alive-Intervall kann der Client erkennen, wann der Server nicht mehr verfügbar ist, ohne auf das lange TCP/IP-Timeout warten zu müssen.

**Timeout (Zeitüberschreitung):** Das Zeitintervall in Sekunden, in dem eine Verbindung hergestellt werden kann. Standardwert: 60

**Device topic prefix (Themenpräfix des Geräts):** Wird in den Standardwerten für das Thema in der Verbindungsnachricht und der LWT-Nachricht auf der Registrierkarte MQTT Client und in den Veröffentlichungsbedingungen auf der Registrierkarte MQTT-Veröffentlichung verwendet.

**Reconnect automatically (Automatisch wiederverbinden):** Gibt an, ob der Client nach einer Trennung der Verbindung die Verbindung automatisch wiederherstellen soll.

#### Nachricht zum Verbindungsaufbau

Gibt an, ob eine Nachricht gesendet werden soll, wenn eine Verbindung hergestellt wird.

**Nachricht senden:** Aktivieren Sie diese Option, damit Nachrichten versendet werden.

**Standardeinstellung verwenden:** Deaktivieren Sie diese Option, um Ihre eigene Standardnachricht eingeben zu können.

# AXIS A1601 Network Door Controller

## Geräteschnittstelle

---

**Thema:** Geben Sie das Thema der Standardnachricht ein.

**Nutzlast:** Geben Sie den Inhalt der Standardnachricht ein.

**Beibehalten:** Wählen Sie diese Option, um den Status des Clients bei diesem Thema beizubehalten.

**QoS:** Ändern Sie die QoS-Ebene für den Paketfluss.

### Nachricht zum letzten Willen und Testament

Mit Letzter Wille und Testament (LWT) kann ein Client bei der Verbindung mit dem Broker ein Testament zusammen mit seinen Zugangsdaten bereitstellen. Wenn der Kunde die Verbindung irgendwann später auf nicht ordnungsgemäße Weise abbricht (vielleicht weil seine Stromquelle deaktiviert ist), kann er den Broker eine Nachricht an andere Kunden übermitteln lassen. Diese LWT-Nachricht hat dieselbe Form wie eine normale Nachricht und wird über die gleiche Mechanik geroutet.

**Nachricht senden:** Aktivieren Sie diese Option, damit Nachrichten versendet werden.

**Standardeinstellung verwenden:** Deaktivieren Sie diese Option, um Ihre eigene Standardnachricht eingeben zu können.

**Thema:** Geben Sie das Thema der Standardnachricht ein.

**Nutzlast:** Geben Sie den Inhalt der Standardnachricht ein.

**Beibehalten:** Wählen Sie diese Option, um den Status des Clients bei diesem Thema beizubehalten.

**QoS:** Ändern Sie die QoS-Ebene für den Paketfluss.

### MQTT publication (MQTT-Veröffentlichung)

**Use default topic prefix (Standard-Themenpräfix verwenden):** Wählen Sie diese Option aus, um das Standard-Themenpräfix zu verwenden, das im Gerätethemenpräfix auf der Registerkarte **MQTT client (MQTT-Client)** definiert ist.

**Include topic name (Themanamen einschließen):** Wählen Sie diese Option aus, um das Thema einzufügen, das die Bedingung des MQTT-Themas beschreibt.

**Include topic namespaces (Themen-Namespaces einschließen):** Wählen Sie diese Option aus, um Namespaces des ONVIF-Themas im MQTT-Thema einzuschließen.

**Include serial number (Seriennummer hinzufügen):** Wählen Sie diese Option, um die Seriennummer des Geräts in die MQTT-Nutzlast einzuschließen.



**Bedingung hinzufügen:** Klicken Sie darauf, um eine Bedingung hinzuzufügen.

**Retain (Beibehalten):** Definiert, welche MQTT-Meldungen als beibehalten gesendet werden.

- **None (Keine):** Alle Melden werden als nicht beibehalten gesendet.
- **Property (Eigenschaft):** Es werden nur statusbehaftete Meldungen als beibehalten gesendet.
- **Alle:** Es werden nur statuslose Meldungen als beibehalten gesendet.

**QoS:** Wählen Sie die gewünschte Stufe für die MQTT-Veröffentlichung.

### MQTT-Abonnements



# AXIS A1601 Network Door Controller

## Geräteschnittstelle



**Abonnement hinzufügen:** Klicken Sie darauf, um ein neues MQTT-Abonnement hinzuzufügen.

**Abonnementfilter:** Geben Sie das MQTT-Thema ein, das Sie abonnieren möchten.

**Themenpräfix des Geräts verwenden:** Fügen Sie den Abonnementfilter als Präfix zum MQTT-Thema hinzu.

**Abonnementart:**

- **Statuslos:** Wählen Sie diese Option, um MQTT-Meldungen in statuslose Meldungen zu konvertieren.
- **Statusbehaftet:** Wählen Sie diese Option, um MQTT-Meldungen in Bedingungen zu konvertieren. Als Status wird der Nutzlast verwendet.

**QoS:** Wählen Sie die gewünschte Stufe für das MQTT-Abonnement.

## Zubehör



### E/A-Ports



Schließen Sie externe Geräte über digitale Eingänge an, die zwischen geöffnetem und geschlossenem Schaltkreis wechseln können, wie etwa PIR-Sensoren, Tür- oder Fensterkontakte und Glasbruchmelder.

Schließen Sie externe Geräte wie Relais und LEDs über digitale Ausgänge an. Sie können verbundene Geräte über die VAPIX® Application Programming Interface oder über die Geräteschnittstelle aktivieren.

#### Port

**Name:** Bearbeiten Sie den Text, um den Port umzubenennen.


**Richtung:**  gibt an, dass es sich bei dem Port um einen Eingangsport handelt.  gibt an, dass es sich um einen Ausgangsport handelt. Wenn der Port konfigurierbar ist, können Sie auf die Symbole klicken, um zwischen Eingang und Ausgang zu wechseln.

**Normal state (Normalzustand):** Klicken Sie auf  für einen geöffneten Schaltkreis" und auf  für einen geschlossenen Schaltkreis.

**Current state (Aktueller Status):** Zeigt den aktuellen Status der Ports an. Der Ein- oder Ausgang wird aktiviert, wenn der aktuelle Zustand vom Normalzustand abweicht. Ein Eingang am Gerät ist offen, wenn er getrennt ist oder eine Spannung von mehr als 1 V Gleichstrom anliegt.

#### Hinweis

Der Schaltkreis des Ausganges ist während eines Neustarts offen. Nach abgeschlossenem Neustart nimmt der Schaltkreis wieder die normale Position an. Wenn die Einstellungen auf dieser Seite geändert werden, nehmen die Schaltkreise der Ausgänge wieder ihre jeweiligen normalen Positionen an, wobei es unerheblich ist, ob aktive Auslöser vorliegen.

**Supervised (Überwacht)**  : Aktivieren Sie diese Option, um Aktionen zu erkennen und auszulösen, wenn jemand die Verbindung zu digitalen E/A-Geräten manipuliert. Sie können nicht nur erkennen, ob ein Eingang geöffnet oder geschlossen ist, sondern auch, ob jemand diesen manipuliert hat (d. h. abgeschnitten oder gekürzt). Zur Überwachung der Verbindung ist im externen E/A-Kreis zusätzliche Hardware (Abschlusswiderstände) erforderlich.

## Protokolle

### Protokolle und Berichte

# AXIS A1601 Network Door Controller

## Geräteschnittstelle

---

### Berichte

- **Geräteserver-Bericht anzeigen:** Klicken Sie darauf, um Informationen zum Produktstatus in einem Popup-Fenster zu sehen. Das Zugangsprotokoll wird automatisch dem Server-Bericht angefügt.
- **Bericht zum Geräteserver herunterladen:** Klicken Sie, um den Server-Bericht herunterzuladen. Dabei wird eine .zip-Datei mit dem vollständigen Server-Bericht als Textdatei im Format UTF-8 sowie einem Schnappschuss der aktuellen Live-Ansicht erstellt. Schließen Sie beim Kontakt mit dem Support stets die ZIP-Datei des Server-Berichts ein.
- **Absturzbericht herunterladen:** Klicken Sie, um ein Archiv mit ausführlichen Informationen zum Produktstatus herunterzuladen. Der Absturzbericht enthält die im Server-Bericht enthaltenen Informationen sowie ausführliche Debug-Informationen. Dieser Bericht enthält möglicherweise vertrauliche Daten wie z. B. Netzwerk-Traces. Es kann einige Minuten dauern, bis der Bericht generiert wird.

### Protokolle

- **Systemprotokoll sehen:** Klicken Sie, um Informationen zu Systemereignissen, wie z. B. Gerätestart, Warnungen und wichtige Meldungen, zu sehen.
- **Zugangsprotokoll anzeigen:** Klicken Sie darauf, um alle fehlgeschlagenen Zugriffsversuche auf das Gerät zu sehen, bei denen z. B. ein falsches Anmeldekennwort verwendet wurde.

### Netzwerk-Trace

#### Wichtig

Eine Datei zum Netzwerk-Trace enthält möglicherweise vertrauliche Informationen wie Zertifikate oder Kennwörter.

Ein Netzwerk-Trace hilft durch die Aufzeichnung von Aktivitäten im Netzwerk beim Beheben von Problemen. Geben Sie die Dauer des Trace in Sekunden oder Minuten an und klicken Sie auf **Herunterladen**.

### Remote-Systemprotokoll

Syslog ist ein Standard für die Nachrichtenprotokollierung. Dadurch können die Software, die Nachrichten generiert, das System, in dem sie gespeichert sind, und die Software, die sie meldet und analysiert voneinander getrennt werden. Jede Nachricht ist mit einem Einrichtungscode versehen, der den Softwaretyp, der die Nachricht generiert, angibt, und einem Schweregrad zugewiesen.



**Server:** Klicken Sie, um einen neuen Server hinzuzufügen.

**Host:** Geben Sie den Host-Namen oder die Adresse des Servers ein.

**Formatieren:** Wählen Sie das zu verwendende syslog-Nachrichtenformat aus.

- RFC 3164
- RFC 5424

**Protocol (Protokoll):** Wählen Sie das zu verwendende Protokoll und den zu verwendenden Port aus:

- UDP (Standardport ist 514)
- TCP (Standardport ist 601)
- TLS (Standardport ist 6514)

**Schweregrad:** Wählen Sie aus, welche Nachrichten gesendet werden sollen, wenn diese ausgelöst werden.

**CA-Zertifikat einrichten:** Sehen Sie sich die aktuellen Einstellungen an oder fügen Sie ein Zertifikat hinzu.

# AXIS A1601 Network Door Controller

## Geräteschnittstelle

---

### Wartung

**Neustart:** Starten Sie das Gerät neu. Dies hat keine Auswirkungen auf aktuelle Einstellungen. Aktive Anwendungen werden automatisch neu gestartet.

**Wiederherstellen:** Setzen Sie die *meisten Einstellungen* auf die Werkseinstellungen zurück. Anschließend müssen Sie Gerät und Apps neu konfigurieren, nicht vorinstallierte Apps neu installieren sowie Ereignisse und PTZ-Voreinstellungen neu erstellen.

#### Wichtig

Die einzigen nach der Wiederherstellung weiterhin gespeicherten Einstellungen sind:

- Boot-Protokoll (DHCP oder statisch)
- Statische IP-Adresse
- Standardrouter
- Subnetzmaske
- Einstellungen für 802.1X
- Einstellungen für O3C

**Werkseinstellungen:** Setzen Sie *alle* Einstellungen werden auf die Werkseinstellungen zurück. Anschließend müssen Sie die IP-Adresse zurücksetzen, um auf das Gerät zugreifen zu können.

#### Hinweis

Sämtliche Firmware des Axis Geräts ist digital signiert, um sicherzustellen, dass Sie nur die verifizierte Firmware auf Ihrem Gerät installieren. Diese Maßnahme erhöht das allgemeine Mindestniveau der Cybersicherheit für die Geräte von Axis. Weitere Informationen finden Sie im Whitepaper "Signierte Firmware, sicherer Start und Sicherheit von Privatschlüsseln" auf [axis.com](http://axis.com).

**Firmwareaktualisierung:** Aktualisieren Sie auf eine neue Firmwareversion. Neue Firmwareversionen können verbesserte Funktionen, Fehlerkorrekturen und vollständig neue Merkmale beinhalten. Wir empfehlen Ihnen, stets die aktuellste Version zu verwenden. Um die neueste Version herunterzuladen, gehen Sie zu [axis.com/support](http://axis.com/support).

Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

- **Standardaktualisierung:** Aktualisieren Sie auf die neue Firmwareversion.
- **Werkseinstellungen:** Aktualisieren und alle Einstellungen werden auf die Werkseinstellungen zurückgesetzt. Wenn Sie diese Option wählen, können Sie nach der Aktualisierung nicht mehr zur vorherigen Firmwareversion zurückkehren.
- **Automatisches Zurücksetzen:** Aktualisieren Sie und bestätigen Sie die Aktualisierung innerhalb der festgelegten Zeit. Wenn Sie diese nicht bestätigen, wird das Gerät auf die vorherige Firmwareversion zurückgesetzt.

**Firmware zurücksetzen:** Gehen Sie auf die vorherige Firmwareversion zurück.

