

AXIS Camera Station S9302 Mk II Workstation

Funktionsweise

Der Standardworkflow zum Konfigurieren eines AXIS Camera Station Pro Recording Servers ist:

1. *Das Gerät installieren.*
2. *Erstes Windows®-Setup:* Nach der Installation Ihres Geräts werden Sie durch einige Schritte geführt, um die Region, die Sprache, das Tastaturlayout, ein Administratorkonto und dessen Passwort einzurichten.
3. *Erstes Setup des AXIS Recorders:* Nach der Ersteinrichtung von Windows wird die AXIS Recorder Toolbox geöffnet, und Sie werden durch einige Schritte geführt, um grundlegende und notwendige Einstellungen vorzunehmen, z. B. Computername, Datum und Uhrzeit sowie Netzwerk. Siehe *Erstes Setup des Axis Recorders, on page 4*.
4. *Windows® konfigurieren. Wir empfehlen:*
 - Windows® auf die neuste Version aktualisieren. Siehe *Windows® aktualisieren, on page 16*.
 - Ein Standardbenutzerkonto erstellen. Siehe *Ein Benutzerkonto erstellen, on page 8*.
5. *AXIS Camera Station Pro auf die neuste Version aktualisieren.*
 - Wenn Ihr System online ist: Die AXIS Recorder Toolbox-App öffnen und auf **Update AXIS Camera Station Pro (AXIS Camera Station Pro aktualisieren)** klicken.
 - Wenn Ihr System offline ist: *axis.com* aufrufen und die neueste Version herunterladen.
6. *Starten Sie den AXIS Camera Station Pro Client.*
7. *Stellen Sie eine Verbindung zum AXIS Camera Station Pro-Server her.*
8. *AXIS Camera Station Pro konfigurieren, on page 4.*

Das Gerät installieren

Vor der Installation

- Bereiten Sie weiteres Zubehör für die Installation vor: Monitor, Maus, Tastatur und Netzkabel.
- Die Verwendung verschiedener Benutzerkonten verstehen.

In der folgenden Tabelle sind die Benutzerkonten aufgeführt, die für die Installation, Konfiguration und den Betrieb Ihres AXIS Systems verwendet werden können.

Benutzerkonto	Beschreibung	Hinweis
MyAxis	Wird verwendet, um die neueste Software herunterzuladen und auf das Lizenzsystem, AXIS Secure Remote Access und System Health Monitoring zuzugreifen.	Registriert von <i>my.axis.com</i> .
Windows®		
Windows®-Administrator	Administratorrechte in Windows®. Wir empfehlen Ihnen, dies nicht als AXIS Camera Station Pro Administrator zu verwenden.	Erstellt während des ersten Windows®-Setups.
Windows®-Benutzer mit AXIS Camera Station Pro Administratorrechten	Ein Windows®-Benutzer mit Administratorrechten in AXIS Camera Station Pro, der von einem Systemintegrator oder Systemadministrator zur Konfiguration oder Fehlerbehebung verwendet werden kann.	In Windows®-Einstellungen erstellt.
Windows®-Benutzer mit Bediener- oder Betrachterrechten in AXIS Camera Station Pro.	Ein Windows®-Benutzer mit Bediener- oder Betrachterrechten in AXIS Camera Station Pro.	In Windows®-Einstellungen erstellt.
Gerät		
Geräteadministrator	Wird vom Administrator für den Zugriff auf die Kamera über das Video Management System oder die Webseite des Geräts verwendet.	Erstellt von der Gerätewebseite oder beim Hinzufügen des Geräts zur AXIS Camera Station Pro.

Installation

Hinweise zur Installation des Produkts finden Sie in der Installationsanleitung in der Verpackung oder auf der Produkt-Supportseite unter *auf axis.com*.

Ihr Gerät konfigurieren

Erstes Setup des Axis Recorders

Nach der Konfiguration von Windows® wird AXIS Recorder Toolbox automatisch geöffnet und Sie werden durch den Assistenten für die Erstkonfiguration geführt. Mit diesem Assistenten können Sie mehrere grundlegende und erforderliche Einstellungen konfigurieren, bevor Sie Ihr Gerät in AXIS Recorder Toolbox verwalten.

1. Wählen Sie **Helles** oder **Dunkles Design** aus und klicken Sie auf **Weiter**.
2. Ändern Sie ggf. den Computernamen und klicken Sie auf **Weiter**.
3. Unter **Energieeinstellungen** ist
 - Den Computer niemals in den Standbymodus versetzen und Das Display niemals ausschalten standardmäßig ausgewählt.
 - Um die Live-Ansicht und Aufzeichnungen immer verfügbar zu machen, empfehlen wir Ihnen, beide Optionen ausgewählt zu lassen. Sie können die Einstellungen jederzeit unter **Start > Einstellungen > System > Betrieb & Ruhezustand** ändern.
4. Konfigurieren Sie unter **Date and time (Datum und Uhrzeit)** die folgenden Einstellungen und klicken Sie auf **Weiter**.
 - Wählen Sie eine Zeitzone.
 - **NTP server (NTP-Server)** auswählen, um einen NTP-Server einzurichten, und die NTP-Server-Adresse eingeben.
 - Wählen Sie zum manuellen Einstellen **Manual (Manuell)** aus und wählen Sie Datum und Uhrzeit aus.
5. Konfigurieren Sie unter **Network settings (Netzwerkeinstellungen)** die folgenden Einstellungen und klicken Sie auf **Weiter**.
 - **Automatische IP-Einstellungen (DHCP)** verwenden und **Automatische DNS-Einstellungen** verwenden sind standardmäßig aktiviert.
 - Wenn Ihr Gerät mit einem Netzwerk mit einem DHCP-Server verbunden ist, werden die zugewiesene IP-Adresse, Subnetzmaske, das Gateway und das bevorzugte DNS automatisch angezeigt.
 - Wenn Ihr Gerät nicht mit einem Netzwerk verbunden ist oder kein DHCP-Server verfügbar ist, geben Sie die IP-Adresse, die Subnetzmaske, das Gateway und das bevorzugte DNS je nach Netzwerkanforderungen ein.
6. Klicken Sie auf **Finish (Fertig)**. Wenn Sie den Computernamen geändert haben, werden Sie von AXIS Recorder Toolbox zum Neustart des Geräts aufgefordert.

AXIS Camera Station Pro konfigurieren

Vorbereitungen:

- Je nach Art Ihrer Installation das Netzwerk konfigurieren. Siehe *Netzwerkkonfiguration*.
- Konfigurieren Sie bei Bedarf die Server-Ports. Siehe *Server-Port-Konfiguration*.
- Berücksichtigen Sie dabei Sicherheitsbelange. Siehe *Hinweise zur Systemsicherheit*.

Nach Abschluss der Konfiguration können Sie mit AXIS Camera Station Pro arbeiten:

1. *Das Video Management System starten*
2. *Geräte hinzufügen*
3. *Konfigurieren des Aufzeichnungsverfahrens, on page 5*
4. *Live-Video ansehen, on page 5*
5. *Aufzeichnungen anzeigen, on page 5*
6. *Lesezeichen hinzufügen, on page 5*

7. *Aufzeichnungen exportieren, on page 6*
8. *Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen, on page 6*

Das Video Management System starten

Um den AXIS Camera Station Pro Client zu starten, klicken Sie mit einem Doppelklick auf das Symbol des Clients. Beim ersten Starten des Clients versucht dieser, sich beim auf demselben Computer installierten AXIS Camera Station Pro Server anzumelden.

Die Verbindung mit mehreren Servern von AXIS Camera Station Pro ist auf verschiedene Weise möglich:

Geräte hinzufügen

Wenn Sie AXIS Camera Station S9302 Mk II Workstation zum ersten Mal aufrufen, wird die Seite **Add devices (Geräte hinzufügen)** geöffnet, auf der das Netzwerk nach Geräten durchsucht wird, die hinzugefügt werden sollen.

1. Wählen Sie hinzuzufügende Geräte aus der Liste aus. Wenn Sie ein Gerät nicht finden können, klicken Sie auf **Manual search (Manuelle Suche)** oder geben Sie einen Suchbegriff ein, um die Ergebnisse einzugrenzen.
2. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Close (Schließen)**, um die Konfiguration zu überspringen und später fortzufahren. So fahren Sie jetzt mit der Konfiguration fort:
 - 3.1. Wählen Sie **Quick configuration (Schnellkonfiguration)** oder **Site Designer configuration (Site Designer Konfiguration)**. Weitere Informationen finden Sie unter .
 - 3.2. Wählen Sie **Add image overlay for date, time, and text (Overlay für Datum, Uhrzeit und Text hinzufügen)**, um Overlays zu allen Axis Kameras hinzuzufügen, die noch keine haben.
 - 3.3. Klicken Sie auf **Next (Weiter)**.
 - 3.4. Wählen Sie Ihre bevorzugte **Aufzeichnungsmethode** aus.
 - 3.5. Klicken Sie auf **Next (Weiter)**.
 - 3.6. Wählen Sie Ihre **Speicherdauer** und den **Aufzeichnungsspeicher** aus und klicken Sie auf **Finish (Fertigstellen)**, um die Konfiguration zu übernehmen.

Konfigurieren des Aufzeichnungsverfahrens

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
2. Eine Kamera wählen
3. Aktivieren Sie **Motion detection (Bewegungserkennung)** oder **Continuous (Kontinuierlich)** oder beides.
4. Klicken Sie auf **Anwenden**.

Live-Video ansehen

1. Öffnen Sie eine Registerkarte **Live view (Live-Ansicht)**.
2. Wählen Sie eine Kamera aus, um ihr Live-Video anzusehen.

Aufzeichnungen anzeigen

1. Öffnen Sie eine Registerkarte **Recordings (Aufzeichnungen)**.
2. Wählen Sie die Kamera aus, von der Sie Aufzeichnungen ansehen möchten.

Lesezeichen hinzufügen

1. Zu Aufzeichnung wechseln.

2. Um die Zeitleistenmarkierung an die gewünschte Position zu setzen, zoomen Sie in die Zeitleiste und ziehen Sie daran.
3. Klicken Sie auf .
4. Einen Namen und eine Beschreibung für das Lesezeichen eingeben. Verwenden Sie Stichwörter, damit das Lesezeichen leicht zu finden ist.
5. Wählen Sie **Löschen von Aufzeichnungen verhindern**, um die Aufzeichnung zu sperren.

Hinweis

Um die Aufzeichnung zu entsperren, deaktivieren Sie **Prevent recording deletion (Löschung der Aufzeichnung verhindern)** oder löschen Sie das Lesezeichen.

6. Klicken Sie auf **OK**, um das Lesezeichen zu speichern.

Aufzeichnungen exportieren

1. Öffnen Sie eine Registerkarte **Recordings (Aufzeichnungen)**.
2. Wählen Sie die Kamera aus, von der Sie Aufzeichnungen exportieren möchten.
3. Um die Auswahlmarkierungen anzuzeigen,  anklicken.
4. Ziehen Sie die Markierungen, um die zu exportierenden Aufzeichnungen einzuschließen.
5. Klicken Sie auf , um die Registerkarte **Export** zu öffnen.
6. Klicken Sie auf **Export... (Exportieren...)**

Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen

1. Wechseln Sie in den Ordner mit den exportierten Aufzeichnungen.
2. AXIS File Player doppelklicken.
3. Klicken Sie auf , um die Aufzeichnungshinweise anzeigen zu können.
4. Die digitale Signatur überprüfen:
 - 4.1. **Tools > Digitale Signatur überprüfen** aufrufen.
 - 4.2. Wählen Sie **Mit Kennwort validieren** und geben Sie Ihr Kennwort ein.
 - 4.3. Klicken Sie auf **Verify (Überprüfen)**, um die Überprüfungsergebnisse anzuzeigen.

Hinweis

- Eine digitale Signatur unterscheidet sich von signiertes Video. Anhand eines signierten Videos können Sie eine Aufzeichnung bis zu der Kamera zurückverfolgen, von der sie stammt, und so sicherstellen, dass sie nicht manipuliert wurde. Weitere Informationen dazu finden Sie unter *Signierte Videos* und in der Bedienungsanleitung der Kamera.
- Wenn gespeicherte Dateien keine Verbindung zu einer Datenbank der AXIS Camera Station haben (nicht indizierte Dateien), müssen Sie sie konvertieren, damit sie im AXIS File Player wiedergegeben werden können. Wenden Sie sich an den technischen Support von Axis, wenn Sie Hilfe bei der Konvertierung Ihrer Dateien benötigen.

Netzwerkconfiguration

Konfigurieren Sie die Proxy- oder Firewall-Einstellungen, bevor Sie AXIS Camera Station S9302 Mk II Workstation verwenden, falls sich Client, Server und die angeschlossenen Netzwerkgeräte in unterschiedlichen Netzwerken befinden.

Client-Proxyeinstellungen

Wenn sich ein Proxy-Server zwischen dem Client und dem Server befindet, müssen Sie die Proxy-Einstellungen in Windows auf dem Client-Computer konfigurieren. Weitere Informationen erhalten Sie vom Axis Support.

Proxysteinstellungen des Servers

Wenn sich der Proxy-Server zwischen dem Netzwerkgerät und dem Server befindet, müssen Sie die Proxy-Einstellungen in Windows auf dem Server konfigurieren. Weitere Informationen erhalten Sie vom Axis Support.

NAT und Firewall

Wenn ein NAT oder eine Firewall den Client und den Server voneinander trennt, konfigurieren Sie diese so, dass der in AXIS Camera Station S9302 Mk II Workstation „Service Control“ angegebene HTTP-Port, TCP-Port und Streaming-Port durchgelassen werden. Wenden Sie sich bitte an Ihren Netzwerk-Administrator, um Unterstützung zu erhalten.

Server-Port-Konfiguration

Der AXIS Camera Station S9302 Mk II Workstation-Server verwendet die Ports 55752 (HTTP), 55754 (TCP), 55756 (mobile Kommunikation) und 55757 (mobiles Streaming) für die Kommunikation zwischen dem Server und dem Client. Bei Bedarf können Sie die Ports über AXIS Camera Station Service Control ändern.

Hinweise zur Systemsicherheit

Um unbefugten Zugriff zu Kameras und Aufzeichnungen zu verhindern:

- Verwenden Sie für alle Netzwerk-Geräte (Kameras, Video-Encoder und Zusatzgeräte) starke Kennwörter.
- Installiert AXIS Camera Station S9302 Mk II Workstation-Server, die Kameras, Video-Encoder und Zusatzgeräte in einem sicheren, vom Büronetz separaten Netzwerk. Sie können den AXIS Camera Station S9302 Mk II Workstation Client auf einem Computer eines anderen Netzwerks installieren, zum Beispiel einem Netzwerk mit Internetzugang.
- Sicherstellen, dass alle Benutzer starke Kennwörter verwenden.

Lokale Windows®-Benutzerkonten verwalten

Ein Benutzerkonto erstellen

Um Ihre persönlichen Daten und Informationen besser zu schützen, empfehlen wir Ihnen, für jedes lokale Konto ein Kennwort hinzuzufügen.

Wichtig

Vergessen Sie die Kennwörter nicht, die Sie für die lokalen Konten erstellt haben! Es gibt keine Möglichkeit, verlorene Passwörter für lokale Konten wiederherzustellen.

1. Rufen Sie **Settings > Accounts > Other users > Add other user** (Einstellungen > Konten > Andere Benutzer > Andere Benutzer hinzufügen) auf und klicken Sie auf **Add account** (Konto hinzufügen).
2. Auf **I don't have this person's sign-in information** (Ich habe die Anmeldeinformationen dieser Person nicht) klicken.
3. Auf **Add a user without a Microsoft account** (Einen Benutzer ohne Microsoft-Konto hinzufügen) klicken.
4. Einen Benutzernamen, ein Kennwort und einen Kennworthinweis eingeben.
5. Auf **Next (Weiter)** klicken und den Anweisungen folgen.

Administratorkonto erstellen

1. **Settings > Accounts > Other people** (Einstellungen > Konten > Andere Personen) aufrufen.
2. Zu dem Konto gehen, dessen Kontotyp geändert werden soll, und auf **Change account type** (Kontotypen ändern) klicken.
3. **Account type** (Kontotyp) aufrufen und **Administrator** (Administrator) auswählen.
4. Klicken Sie auf **OK**.
5. Gerät neu starten und mit dem neuen Administratorkonto anmelden.

Eine lokale Benutzergruppe erstellen

1. **Computer Management** (Computerverwaltung) aufrufen.
2. **Local Users and Groups > Group** (Lokale Benutzer und Gruppen > Gruppe) aufrufen.
3. Rechtsklick auf **Group** (Gruppe) und **New Group** (Neue Gruppe) auswählen.
4. Einen Gruppennamen und eine Beschreibung eingeben.
5. Gruppenmitglieder hinzufügen:
 - 5.1. Klicken Sie auf **Hinzufügen**.
 - 5.2. Klicken Sie auf **Erweitert**.
 - 5.3. Suchen Sie die Benutzerkonten, die zur Gruppe hinzugefügt werden sollen, und klicken Sie auf **OK**.
 - 5.4. Klicken Sie noch einmal auf **OK**.
6. Klicken Sie auf **Create** (Erstellen).

Ein Benutzerkonto löschen

Wichtig

Nach Löschen eines Benutzerkontos erscheint dieses nicht mehr auf dem Anmeldebildschirm. Außerdem werden alle Dateien, Einstellungen und Programmdateien gelöscht, die im entsprechenden Benutzerkonto gespeichert sind.

1. **Settings > Accounts > Other people** (Einstellungen > Konten > Andere Personen) aufrufen.
2. Zu dem Konto gehen, das gelöscht werden soll, und **Remove** (Entfernen) klicken.

Das Kennwort eines Benutzerkontos ändern

1. Mit einem Administratorkonto anmelden.
2. **User Accounts > User Accounts > Manage another account in sequence (Benutzerkonten > Benutzerkonten > Anderes Konto verwalten)** aufrufen.
Es wird eine Liste mit allen Benutzerkonten auf dem Gerät angezeigt.
3. Das Benutzerkonto auswählen, dessen Kennwort geändert werden soll.
4. Auf **Change the password (Kennwort ändern)** klicken.
5. Neues Kennwort eingeben und auf **Change password (Kennwort ändern)** klicken.

Einen Kennwortrücksetzdatenträger für ein Benutzerkonto erstellen

Es wird empfohlen, einen Kennwortrücksetzdatenträger zu erstellen. Als Datenträger bietet sich ein USB-Stick an. Mit diesem können Sie das Kennwort zurücksetzen. Ohne Kennwortrücksetzdatenträger kann das Kennwort nicht zurückgesetzt werden.

Hinweis

Unter Windows® 10 oder höher ist ein Kennwortrücksetzdatenträger nicht notwendig. In diesem Fall können Sicherheitsfragen zum lokalen Benutzerkonto hinzugefügt werden. Die Sicherheitsfragen können folgendermaßen hinzugefügt werden: **Start (Start)** auswählen und auf **Settings > Sign-in options > Update your security questions (Einstellungen > Anmeldeoptionen > Sicherheitsfragen aktualisieren)** klicken.

1. Mit einem lokalen Benutzerkonto bei Ihrem Gerät anmelden. Für ein verbundenes Konto kann kein Kennwortrücksetzdatenträger erstellt werden.
2. Einen leeren USB-Stick an Ihr Gerät anschließen.
3. Vom Windows®-Suchfeld zu **Create a password reset disk (Kennwortrücksetzdatenträger erstellen)** wechseln.
4. Klicken Sie im Setup-Assistenten **Forgotten Password (Kennwort vergessen)** auf **Next (Weiter)**.
5. Ihren USB-Stick auswählen und auf **Next (Weiter)** klicken.
6. Ihr aktuelles Kennwort eingeben und auf **Next (Weiter)** klicken.
7. Den Anweisungen auf dem Bildschirm folgen.
8. Entfernen Sie den USB-Stick und bewahren Sie ihn an einem sicheren Ort auf. Wird das Kennwort geändert, muss kein neuer Kennwortrücksetzdatenträger erstellt werden – selbst dann nicht, wenn das Kennwort mehrfach geändert wird.

AXIS Camera Station Pro Benutzerkonten verwalten

Benutzerberechtigungen

Rufen Sie **Configuration (Konfiguration) > Security (Sicherheit) > User permissions (Benutzerrechte)** auf, um die Benutzer und Gruppen in AXIS Camera Station S9302 Mk II Workstation anzuzeigen.

Hinweis

Administratoren von Computern, auf denen AXIS Camera Station S9302 Mk II Workstation Server ausgeführt werden, erhalten automatisch Administratorrechte in AXIS Camera Station S9302 Mk II Workstation. Die Zugriffsrechte der Benutzergruppe „Administratoren“ können nicht geändert oder gelöscht werden.

Bevor Sie einen Benutzer oder eine Gruppe hinzufügen können, stellen Sie bitte sicher, dass diese auf dem lokalen Computer registriert sind oder über ein Windows® Active Directory-Konto verfügen. So fügen Sie Benutzer bzw. Gruppen hinzu: *Hinzufügen von Benutzern oder Gruppen*.

Wenn ein Benutzer einer Gruppe angehört, erhält er die höchste Rollenberechtigung, die ihm persönlich oder der Gruppe zugewiesen wurde. Beispielsweise hat ein Benutzer, der Zugriff auf Kamera X hat und gleichzeitig einer Gruppe angehört, die Zugriff auf die Kameras Y und Z hat, Zugriff auf alle drei Kameras.

	Gibt an, ob es sich um einen Einzelbenutzer handelt.
	Gibt an, ob es sich um eine Benutzergruppe handelt.
Bezeichnung	Der auf dem lokalen Computer oder in Active Directory angezeigte Benutzername.
Domäne	Domain, zu der der Benutzer oder die Benutzergruppe gehört.
Rolle	Die dem Benutzer oder der Benutzergruppe zugewiesene Zugriffsrolle. Mögliche Werte sind: Administrator, Bediener und Betrachter.
Details	Detaillierte Benutzerinformationen wie diese auf dem lokalen Rechner oder in Active Directory erscheinen.
Server	Server, zu der der Benutzer oder die Benutzergruppe gehört.

Hinzufügen von Benutzern oder Gruppen

Benutzer von Microsoft Windows® und Active Directory sowie Benutzergruppen können auf AXIS Camera Station S9302 Mk II Workstation zugreifen. Um einen Benutzer zu AXIS Camera Station S9302 Mk II Workstation hinzufügen zu können, müssen Sie zuerst Benutzer oder eine entsprechende Benutzergruppe in Windows® hinzufügen.

So fügen Sie einen Benutzer in Windows® 10 und 11 hinzu:

- Drücken Sie die Windows-Taste + X und wählen Sie **Computer Management (Computerverwaltung)**.
- Navigieren Sie im Fenster **Computer Management (Computerverwaltung)** zu **Local Users and Groups (Lokale Benutzer und Gruppen) > Users (Benutzer)**.
- Klicken Sie mit der rechten Maustaste auf **Users (Benutzer)** und wählen Sie **New User (Neuer Benutzer)**.
- Geben Sie im Popup-Dialog die Daten des neuen Benutzers ein und deaktivieren Sie **User must change password at next login (Benutzer muss bei der nächsten Anmeldung das Passwort ändern)**.
- Klicken Sie auf **Create (Erstellen)**.

Falls Sie eine Active Directory-Domäne verwenden, halten Sie bitte Rücksprache mit Ihrem Netzwerkadministrator.

Hinzufügen von Benutzern oder Gruppen

1. Gehen Sie zu **Configuration > Security > User permissions (Konfiguration > Sicherheit > Benutzerrechte)**.
2. Klicken Sie auf **Hinzufügen**. Die verfügbaren Benutzer und Gruppen werden in der Liste angezeigt.
3. Wählen Sie unter **Scope (Bereich)** aus, wo nach Benutzern und Benutzergruppen gesucht werden soll.
4. Wählen Sie unter **Show (Anzeigen)** aus, ob Sie Benutzer oder Benutzergruppen anzeigen möchten. Die Suchergebnisse werden möglicherweise nicht angezeigt, wenn zu viele Benutzer oder Gruppen vorhanden sind. Verwenden Sie den Filter, um die Ergebnisse einzugrenzen.
5. Wählen Sie Benutzer bzw. Gruppen und klicken Sie auf **Hinzufügen**.

Bereich	
Server	Wählen Sie diese Option, um auf Ihrem lokalen Rechner nach Benutzern oder Benutzergruppen zu suchen.
Domäne	Wählen Sie diese Option, um nach Active Directory-Benutzern oder -Benutzergruppen zu suchen.
Ausgewählter Server	Wenn eine Verbindung zu mehreren AXIS Camera Station S9302 Mk II Workstation-Servern besteht, wählen Sie einen Server aus, um auf diesem Server nach Benutzern oder Gruppen zu suchen.

Konfigurieren eines Benutzers oder einer Gruppe

1. Wählen Sie einen Benutzer oder eine Gruppe aus der Liste aus.
2. Wählen Sie unter **Role (Rolle)** eine der Optionen **Administrator**, **Operator (Bediener)** oder **Viewer (Betrachter)** aus.
3. Bei Auswahl von **Operator (Bediener)** oder **Viewer (Betrachter)** können Sie die entsprechenden Benutzer- oder Benutzergruppenberechtigungen konfigurieren. Siehe *Benutzer-/Gruppenberechtigungen*.
4. Klicken Sie auf **Save**.

Benutzer oder Benutzergruppe entfernen

1. Wählen Sie einen Benutzer oder eine Benutzergruppe aus.
2. Klicken Sie auf **Remove (Entfernen)**.
3. Wählen Sie **OK** in dem Dialogfenster, um den Benutzer oder die Gruppe zu löschen.

Benutzer-/Gruppenberechtigungen

Einem Benutzer oder einer Benutzergruppe können drei verschiedene Rollen zugewiesen werden. Weitere Informationen dazu, wie Sie die Rolle eines Benutzers oder einer Benutzergruppe definieren, finden Sie unter *Hinzufügen von Benutzern oder Gruppen*.

Administrator – Vollständiger Zugriff auf das gesamte System, einschließlich Zugriff auf Live-Videos und Video-Aufzeichnungen sämtlicher Kameras, alle I/O-Ports und Ansichten. Diese Rolle ist erforderlich, um Zutritt zur Systemkonfiguration zu haben.

Bediener – Auswahl von Kameras, Ansichten und I/O-Ports für den Zugriff auf Live-Videos und Video-Aufzeichnungen. Ein Bediener hat vollen Zugriff auf alle Funktionen der AXIS Camera Station S9302 Mk II Workstation mit Ausnahme der Systemkonfiguration.

Betrachter – Zugriff auf Live-Videos bestimmter Kameras, I/O-Ports und Ansichten. Betrachter haben keinen Zugriff auf Video-Aufzeichnungen oder die Systemkonfiguration.

Kameras

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** oder **Viewer (Betrachter)** können die folgenden Zugriffsrechte erteilt werden.

Zugriff	Gewährt dem Benutzer Zugriff auf die Kamera und alle Kamerafunktionen.
Video	Gewährt dem Benutzer Zugriff auf das Live-Video der Kamera.
Audio – Wiedergeben	Gewährt dem Benutzer Zugriff auf das Abhören der Kamera.
Audio – Sprechen	Gewährt dem Benutzer Zugriff auf das Sprechen über die Kamera.
Manuelle Aufzeichnung	Erlaubt das manuelle Starten und Beenden von Aufzeichnungen.
Mechanisches PTZ	Zugriff auf mechanische PTZ-Steuerungen gewähren. Nur für Kameras mit mechanischer PTZ-Steuerung verfügbar.
PZT-Priorität	Legen Sie die PTZ-Priorität fest. Eine niedrigere Zahl steht für eine höhere Priorität. Ist keine Priorität zugewiesen, beträgt die Einstellung 0. Ein Administrator hat die höchste Priorität. Wenn ein Rolle mit höherer Priorität eine PTZ-Kamera ansteuert, können andere Rollen dieselbe Kamera 10 Sekunden lang (Standardkonfiguration) nicht ansteuern. Nur für Kameras mit mechanischem PTZ-Antrieb und Auswahl von Mechanical PTZ (Mechanischer PTZ) verfügbar.

Ansichten

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** oder **Viewer (Betrachter)** können die folgenden Zugriffsrechte erteilt werden. Sie können mehrere Ansichten auswählen und die Zugriffsberechtigungen festlegen.

Zugriff	Gewährt Zugriff auf die Ansichten in AXIS Camera Station S9302 Mk II Workstation.
Bearbeiten	Ermöglicht die Bearbeitung von Ansichten unter AXIS Camera Station S9302 Mk II Workstation.

I/O

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** oder **Viewer (Betrachter)** können die folgenden Zugriffsrechte erteilt werden.

Zugriff	Gewährt dem Benutzer uneingeschränkten Zugriff auf den E/A-Port.
Lesen	Ermöglicht die Ansicht des Zustands des I/O-Ports, ohne diesen zu ändern.
Schreiben	Ermöglicht die Änderung des Zustands des I/O-Ports.

System

Ausgegraute Zugriffsrechte in der Liste können nicht konfiguriert werden. Mit einem Häkchen markiert bedeutet, dass die jeweiligen Benutzer oder Benutzergruppe standardmäßig über dieses Privileg verfügt.

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** können die folgenden Zugriffsrechte erteilt werden. Die Option **Take snapshots (Momentaufnahmen erstellen)** ist ebenfalls für die Rolle **Viewer (Betrachter)** möglich.

Schnappschuss aufnehmen	Ermöglicht das Aufnehmen von Schnappschüssen in der Live-Ansicht und im Aufzeichnungsmodus.
Aufzeichnungen exportieren	Das Exportieren von Aufzeichnungen zulassen.
Vorfallsberichte erstellen	Das Erstellen von Vorfallsberichten zulassen.
Prevent access to recordings older than (Zugriff auf Aufzeichnungen verhindern, wenn älter als)	Verhindert den Zugriff auf Aufzeichnungen, die älter sind als die angegebene Minutenzahl. Benutzer können diese Aufzeichnungen bei der Suche nicht finden.
Zugriff auf Alarmer, Aufgaben und Protokolle	Erlaubt den Erhalt von Alarmbenachrichtigungen und den Zugriff auf die Funktionsleiste Alarms and tasks (Alarme und Aufgaben) sowie die Registerkarte Logs (Protokolle) .
Access data search (Zugriff auf die Datensuche)	Ermöglicht die Suche nach Daten, um nachzuverfolgen, was zum Zeitpunkt eines Ereignisses passiert ist.
Ereignisse zu Kategorien hinzufügen	Ermöglicht das Hinzufügen von Kategorien zu Ereignissen auf der Registerkarte Recordings (Aufzeichnungen) .
Kategorien von Ereignissen entfernen	Ermöglicht das Entfernen von Kategorien aus Ereignissen auf der Registerkarte Recordings (Aufzeichnungen) .

Zutrittskontrolle

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** können die folgenden Zugriffsrechte erteilt werden. Die Option **Access management (Zugriffsverwaltung)** ist ebenfalls für die Rolle **Viewer (Betrachter)** möglich.

Konfiguration der Zutrittskontrolle	Erlaubt die Konfiguration von Türen und Zonen, Identifikationsprofilen, Kartenformaten und PIN, verschlüsselter Kommunikation und Multi-Server.
Zutrittsverwaltung	Erlaubt die Zugriffsverwaltung und Zugriff auf die Einstellungen von Active Directory.

Die folgenden Zugriffsberechtigungen sind für Benutzer oder Gruppen mit der Rolle **Betrachter** verfügbar.

Systemzustand überwachen

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** können die folgenden Zugriffsrechte erteilt werden. Die Option **Access to system health monitoring (Zugriff auf Systemzustandsüberwachung)** ist ebenfalls für die Rolle **Viewer (Betrachter)** möglich.

Konfigurieren der Überwachung des Systemzustands	Erlaubt das Konfigurieren der Systemzustandsüberwachung.
Auf Systemzustandsüberwachung zugreifen	Erlaubt den Zugriff auf die Systemzustandsüberwachung.

Ihr Gerät verwalten

Secure-Boot-Zertifikate aktualisieren

Microsoft wird die Secure-Boot-Zertifikate aus dem Jahr 2011 im Juni 2026 außer Kraft setzen und durch neue Zertifikate aus dem Jahr 2023 ersetzen. Um die Sicherheit Ihres Geräts für die Aufzeichnung zu gewährleisten, führen Sie bitte die Installation der Zertifikate für das Jahr 2023 noch vor diesem Zeitpunkt durch.

Für die Installation der Zertifikate für das Jahr 2023 ist Windows 10 LTSC (Long-Term Servicing Channel) oder Windows 11 LTSC erforderlich. Falls Ihr Gerät noch unter die Garantie fällt, jedoch mit Windows 10 SAC (Semi-Annual Channel) statt einer LTSC-Version betrieben wird, wenden Sie sich bitte an den technischen Support von Axis. Dort kann man Ihnen mitteilen, ob eine Aktualisierung auf eine LTSC-Version möglich ist, bevor Sie das BIOS aktualisieren oder Zertifikate ändern.

Hinweis

Nach Juni 2026 funktionieren Geräte ohne die Zertifikate aus dem Jahr 2023 zwar weiterhin wie gewohnt, erhalten jedoch keine neuen Sicherheitsmaßnahmen für den frühen Startvorgang mehr, darunter Updates für den Windows-Boot-Manager und Sperrlisten für neue Sicherheitslücken.

Den Status Ihres Zertifikats prüfen

Um zu überprüfen, ob die Zertifikate für 2023 installiert sind und der Windows-Bootloader aktualisiert wurde, wenden Sie eine der folgenden Methoden an:

Methode 1:

1. Öffnen Sie den Registrierungseditor.
2. Wechseln Sie zu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing`.
3. Prüfen Sie den Wert `UEFICA2023Status`. Wenn der Wert **Updated (Aktualisiert)** lautet, ist das Zertifikat für 2023 installiert.

 (Default)	REG_SZ	(value not set)
 BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
 ConfidenceLevel	REG_SZ	No Data Observed - Action Required
 ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
 LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
 UEFICA2023Status	REG_SZ	Updated
 WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

Methode 2:

1. Öffnen Sie Windows Security (Windows-Sicherheit).
2. Rufen Sie Device security (Gerätesicherheit) auf.
3. Prüfen Sie unter Secure Boot (Sicheres Hochfahren) die Statusmeldung. Ist das Zertifikat auf dem neuesten Stand, wird auf der Karte Folgendes angezeigt: „Secure Boot is on and all required certificate updates have been applied (Secure Boot ist aktiviert und alle erforderlichen Aktualisierungen des Zertifikats wurden vorgenommen).“ No further certificate changes are needed (Es müssen keine weiteren Zertifikate geändert werden).“



Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

Hinweis

„Windows-Sicherheit“ zeigt den Zertifikatsstatus nur an, wenn auf Ihrem Gerät das kumulative Update vom 14. April 2026 oder ein neueres Update installiert ist. Sollte keine Meldung zum Zertifikatsstatus angezeigt werden, führen Sie bitte die Installation des neuesten Windows-Updates durch oder wenden Sie stattdessen Methode 1 an.

Empfohlene Aktionen

Durch eine Aktualisierung des BIOS werden die Zertifikate für das Jahr 2023 dauerhaft in der Firmware gespeichert. Dies ist die zuverlässigste Methode, und wir empfehlen sie auch dann, wenn Sie die Zertifikate bereits über Windows Update installiert haben.

Wichtig

Wenn Sie die Zertifikate ausschließlich über Windows Update installieren und anschließend die BIOS-Secure-Boot-Schlüssel auf die werksseitigen Standardeinstellungen zurücksetzen, gehen die Zertifikate verloren, und das Gerät lässt sich bei eingeschaltetem Secure Boot nicht mehr starten. Aktualisieren Sie das BIOS, um die Zertifikate dauerhaft zu speichern, bevor Sie die Secure-Boot-Schlüssel zurücksetzen.

Zertifikat über das BIOS aktualisieren

Für die Serien AXIS S12 und S93 aktualisieren Sie das BIOS bitte von Dell statt von Axis.com. Siehe *BIOS aktualisieren, on page 16*.

Weitere Informationen:

- *Dell: Auslaufen des Microsoft-Secure-Boot-Zertifikats 2011.*
- *Dell: Richtlinien zur Aktualisierung des BIOS für PowerEdge-Server im Hinblick auf Secure Boot.*

Zertifikat über Windows Update aktualisieren

Sollte für Ihr Modell noch keine Aktualisierung des BIOS verfügbar sein, können Sie stattdessen die Zertifikate für 2023 über Windows Update beziehen.

Wichtig

Während der Installation werden auf diese Weise installierte Zertifikate in der aktuellen Secure-Boot-Datenbank gespeichert, nicht in der Firmware. Wenn Sie die BIOS-Secure-Boot-Schlüssel auf die werksseitigen Standardeinstellungen zurücksetzen, gehen die Zertifikate verloren, und das Gerät kann möglicherweise nicht mehr gestartet werden, wenn Secure Boot eingeschaltet ist. Installieren Sie ein BIOS-Update, sobald eines für Ihr Modell verfügbar ist, auch wenn Sie diese Methode bereits angewendet haben.

So verwenden Sie diesen Pfad:

1. Stellen Sie sicher, dass auf Ihrem Gerät Windows 10 LTSC oder Windows 11 LTSC installiert ist.
2. Installieren Sie alle Windows-Updates, die am 14. April 2026 oder später veröffentlicht wurden.
3. Rufen Sie **Windows Security (Windows-Sicherheit) > Device security (Gerätesicherheit) > Secure Boot (Sicheres Hochfahren)** auf, um den Status Ihres Zertifikats zu prüfen.
4. Falls das Zertifikat nach der Installation der neuesten Updates nicht aktualisiert wird, prüfen Sie den Registrierungswert **UEFICA2023Status**. Sollte Ihr Gerät weiterhin nicht für das automatische Update geeignet sein, aktualisieren Sie das BIOS oder wenden Sie sich an den technischen Support von Axis.

Wichtig

Widerrufen Sie das Zertifikat von 2011 nicht manuell, bevor Sie sich vergewissert haben, dass alle Wiederherstellungsmedien, Startumgebungen und Treiber in Ihrer Umgebung mit dem Zertifikat von 2023 signiert sind. Wenn Sie das Zertifikat aus dem Jahr 2011 zu früh widerrufen, kann Ihr Gerät bei eingeschaltetem Secure Boot nicht mehr gestartet werden.

Aktuelle BIOS-Version überprüfen

So überprüfen Sie das aktuelle BIOS:

1. Schalten Sie das Gerät ein und drücken Sie mehrmals F2, bis das Axis Logo angezeigt wird.

2. Die Versionsnummer wird unter **Übersicht** als erster Eintrag angezeigt.

BIOS aktualisieren

1. Rufen Sie *Dell Support* auf.
2. Geben Sie im Feld **Service Tag** die letzten 7 Zeichen der Seriennummer Ihres Geräts ein. Beispielsweise: HW030ABC1234.
3. Rufen Sie **Drivers & Downloads (Treiber & Downloads)** auf und suchen Sie nach „BIOS“.
4. Sollte für Ihren OEM-Produktnamen (z. B. „OEMR XL R760xs“) keine neuere Version angezeigt werden, führen Sie die Suche erneut durch und verwenden Sie dabei anstelle der Seriennummer den generischen Dell-Plattformnamen (z. B. „R760xs“).
5. Laden Sie die neueste BIOS-Version herunter, die nach April 2026 veröffentlicht wurde, und führen Sie die Installation durch.

Windows® aktualisieren

Windows® sucht regelmäßig nach Updates. Wenn ein Update verfügbar ist, lädt Ihr Gerät das Update automatisch herunter – Sie müssen es jedoch manuell installieren.

Hinweis

Die Aufzeichnung wird während eines geplanten Systemneustarts unterbrochen.

So erfolgt die manuelle Suche nach Updates:

1. Rufen Sie **Settings > Windows Update** (Einstellungen > Windows-Update) auf.
2. Auf **Check for updates (Auf Updates überprüfen)** klicken.

Update-Einstellungen für Windows® konfigurieren

Sie können Ihrem Bedarf entsprechend ändern, wie und wann Windows® Updates durchführt.

Hinweis

Während eines geplanten Systemneustarts werden alle laufenden Aufzeichnungen angehalten.

1. Die Run-App öffnen.
 - **Windows System > Run (Windows-System > Ausführen)** aufrufen oder
2. Geben Sie `gpedit.msc` ein und klicken Sie auf **OK**. Der Editor für lokale Gruppenrichtlinien wird geöffnet.
3. **Computer Configuration > Administrative Templates > Windows Components > Windows Update (Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Windows-Update)** aufrufen.
4. Einstellungen nach Bedarf konfigurieren; siehe Beispiel.

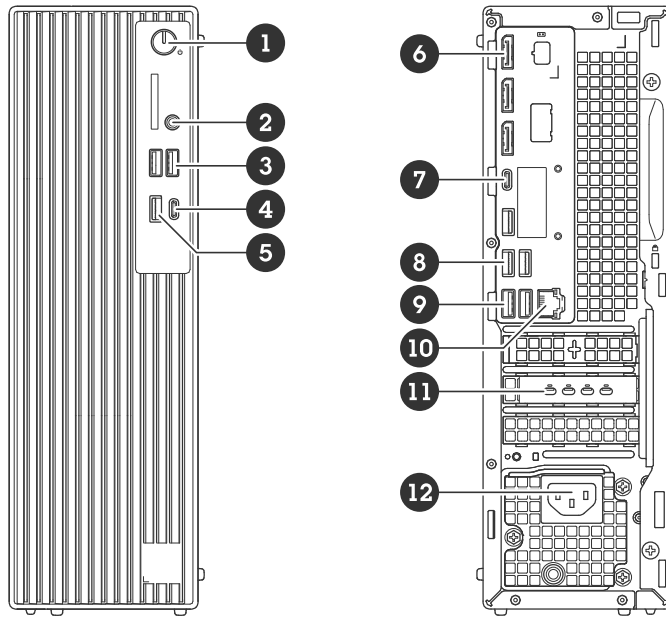
Beispiel:

Um Updates ohne Benutzerinteraktion automatisch herunterzuladen und zu installieren und das Gerät bei Bedarf außerhalb der Geschäftszeiten neu zu starten, muss die folgende Konfiguration vorgenommen werden:

1. **Always automatically restart at the scheduled time (Immer automatisch zum geplanten Zeitpunkt neu starten)** öffnen und folgende Option auswählen:
 - 1.1. **Aktiviert**
 - 1.2. **The restart timer will give users this much time to save their work (minutes) (Der Neustart-Timer gibt Benutzer die angegebene Zeit (Minuten), um ihre Arbeit zu speichern): 15.**
 - 1.3. Klicken Sie auf **OK**.
2. **Configure Automatic Updates (Automatische Updates konfigurieren)** und folgende Option auswählen:
 - 2.1. **Aktiviert**

- 2.2. **Configure Automatic updates (Automatische Updates konfigurieren):** Automatisch herunterladen und Installation planen
 - 2.3. **Schedule Install day (Installationstag planen):** Jeden Sonntag
 - 2.4. **Schedule Install time (Installationszeit planen):** 00:00
 - 2.5. Klicken Sie auf **OK**.
3. Auf **Allow Automatic Updates immediate installation (Automatische Updates sofort installieren)** klicken und folgende Option auswählen:
 - 3.1. **Aktiviert**
 - 3.2. Klicken Sie auf **OK**.

Produktübersicht



- 1 Netzschalter/Netz-LED
- 2 Universalstecker Audio
- 3 USB-2.0-Ports
- 4 USB 3.2 Gen 2x2 USB-C Port
- 5 USB 3.2 gen 2x1 Port
- 6 DisplayPorts™
- 7 USB 3.2 Gen 2x1 USB-C Port
- 8 USB 3.2 gen 1x1 Ports
- 9 USB-2.0-Ports
- 10 1 GbE Ethernet-Port
- 11 Mini DisplayPorts™
- 12 Stromanschluss

Fehlerbehebung

Eine Systemwiederherstellung durchführen

Interne Wiederherstellung

Wenn das Gerät einen Systemfehler aufwies, führen Sie eine interne Wiederherstellung durch, um das System wiederherzustellen.

1. Öffnen Sie **Windows-Einstellungen**.
2. Gehen Sie zu **System**.
3. Wählen Sie im Menü die Option **Recovery**.
4. Wählen Sie unter **Recovery options (Wiederherstellungsoptionen)** **Reset this PC (Diesen PC zurücksetzen)** aus.
5. **Keep my files (Eigene Dateien beibehalten)** oder **Remove everything (Alles entfernen)** auswählen.
 - Die Option „Keep my files (Eigene Dateien beibehalten)“ ermöglicht die Erhaltung aller persönlichen Dateien und Benutzerdaten sowie der gesamten von Axis installierten Software.
 - Bei Auswahl der Option „Remove everything (Alles entfernen)“ werden alle Ihre persönlichen Dateien und Benutzerdaten gelöscht, während die gesamte von Axis installierte Software (werksseitige Standardeinstellung) erhalten bleibt.
6. Den Anweisungen auf dem Bildschirm folgen.

Hinweis

Vor der Auswahl von **Reset (Zurücksetzen)** wird eine Liste mit Apps angezeigt, die während des Vorgangs entfernt werden. Apps von Axis werden nach der Wiederherstellung wiederhergestellt, andere zuvor von Ihnen installierte Apps jedoch nicht.

Wichtig

Nach einer erfolgreichen Wiederherstellung müssen Sie sich mit einem Administratorkonto bei Windows anmelden, um den Wiederherstellungsprozess zu schließen.

Externe Wiederherstellung

Nach einem kompletten Systemfehler muss das Windows®-System mit einem Wiederherstellungsabbild wiederhergestellt werden. Wenden Sie sich unter Angabe der Seriennummer Ihres Geräts an den *technischen Support von AXIS*, um das AXIS Network Video Recovery Kit herunterzuladen.

Hinweis

Das AXIS Network Video Recorder Recovery Kit ist in zwei Varianten erhältlich:

- **sb11** – für Geräte, die noch das Zertifikat aus dem Jahr 2011 verwenden.
- **sb23** – für Geräte, die auf das Zertifikat für 2023 umgestellt wurden.

Bitte überprüfen Sie den Status Ihres Zertifikats, bevor Sie das Recovery Kit herunterladen, und wählen Sie die entsprechende Variante aus. Sollten Sie die falsche Variante auswählen, führt die Installation nicht zu einem bootfähigen Ergebnis, und Sie müssen mit dem richtigen Image von vorne beginnen. Dies wird Ihrem Gerät keinen Schaden zufügen.

Falls auf Ihrem Gerät bereits das Zertifikat von 2023 installiert ist, kann die Variante „sb11“ weiterhin sicher verwendet werden, solange das Zertifikat von 2011 nicht manuell widerrufen wurde. Sobald die Berechtigung widerrufen wurde, funktioniert nur noch sb23.

1. Laden Sie das AXIS Network Video Recovery Kit und ein ISO-zu-USB-Schreibtool Ihrer Wahl herunter.
2. USB-Stick an Computer anschließen.
 - Der USB-Stick sollte mindestens 16 GB haben.
 - Der USB-Stick wird formatiert und alle vorhandenen Daten werden gelöscht.
3. Führen Sie das ISO-zu-USB-Schreibtool aus und befolgen Sie die Anweisungen auf dem Bildschirm.

- Das Schreiben der Daten auf den USB-Stick dauert etwa 10 bis 15 Minuten. Entfernen Sie den USB-Stick nicht vor Abschluss des Vorgangs.
- 4. Wenn das ISO-zu-USB-Schreibtool den Schreibvorgang abgeschlossen hat, ziehen Sie den USB-Stick von Ihrem Computer ab und schließen ihn an Ihrem Gerät an.
- 5. Gerät starten. Wenn der Axis Begrüßungsbildschirm angezeigt wird, drücken Sie F12, um zum Boot-Menü zu gelangen.
- 6. Wählen Sie Ihren USB-Stick aus und bestätigen Sie mit **Enter**. Das System startet mit dem AXIS Netzwerk-Videorekorder Recovery Kit.
- 7. Klicken Sie auf **Start (Starten)** und befolgen Sie die Anweisungen auf dem Bildschirm.
 - Die Wiederherstellung dauert etwa 10 bis 15 Minuten.

Fehlerbehebung bei AXIS Camera Station Pro

Informationen zur Behebung von Problemen bei AXIS Camera Station Pro finden Sie im *Benutzerhandbuch zu AXIS Camera Station Pro*.

Benötigen Sie Hilfe?

Nützliche Links

- *Benutzerhandbuch zu AXIS Camera Station Pro*
- *Bei AXIS Secure Remote Access anmelden*
- *Bei AXIS Secure Remote Access v2 anmelden*
- *Was in eine Antiviren-Freigabeliste für AXIS Camera Station aufgenommen werden sollte*

Support

Weitere Hilfe erhalten Sie hier: axis.com/support.

T10231344_de

2026-07 (M2.2)

© 2025 – 2026 Axis Communications AB