

AXIS Camera Station S1264 Rack Recording Server

Inhalt

Über das Gerät	4
Funktionsweise.....	5
Das Gerät installieren	6
Vor der Installation.....	6
Ihr Gerät konfigurieren	7
Erstes Setup des Axis Recorders	7
AXIS Camera Station Pro konfigurieren.....	7
Das Video Management System starten	8
Geräte hinzufügen.....	8
Passen Sie die Speicherkapazität an.....	8
Konfigurieren des Aufzeichnungsverfahrens	8
Live-Video ansehen.....	8
Aufzeichnungen anzeigen.....	9
Lesezeichen hinzufügen	9
Aufzeichnungen exportieren	9
Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen	9
Netzwerkconfiguration.....	10
Server-Port-Konfiguration	10
Hinweise zur Systemsicherheit	10
Ein System online lizenzieren.....	10
Ein System offline lizenzieren	10
Lokale Windows®-Benutzerkonten verwalten.....	12
Ein Benutzerkonto erstellen.....	12
Administratorkonto erstellen	12
Eine lokale Benutzergruppe erstellen	12
Ein Benutzerkonto löschen	12
Das Kennwort eines Benutzerkontos ändern	13
Einen Kennworrücksetzdatenträger für ein Benutzerkonto erstellen.....	13
AXIS Camera Station Pro Benutzerkonten verwalten.....	14
Benutzerberechtigungen.....	14
Hinzufügen von Benutzern oder Gruppen.....	14
Benutzer-/Gruppenberechtigungen	15
Ihr Gerät verwalten.....	18
Secure-Boot-Zertifikate aktualisieren.....	18
Den Status Ihres Zertifikats prüfen	18
Empfohlene Aktionen.....	19
Zertifikat über das BIOS aktualisieren	19
Zertifikat über Windows Update aktualisieren.....	19
Aktuelle BIOS-Version überprüfen	19
BIOS aktualisieren	20
Windows® aktualisieren.....	20
Update-Einstellungen für Windows® konfigurieren	20
Festplattenlaufwerk hinzufügen.....	21
Vorgehensweise.....	21
Hot-Swap-Festplatte installieren.....	21
RAID ändern.....	22
.....	22
Neues RAID-Array erstellen	23
Microsoft Windows® konfigurieren.....	24
Konfigurieren von iDRAC.....	25
Cybersicherheit	26
Sicheres Hochfahren	26
Trusted Platform Module (TPM).....	26

Secure Component Verification (SCV)	26
Axis Sicherheitsbenachrichtigungsdienst.....	26
Schwachstellen-Management.....	26
Sicherer Betrieb von Axis Geräten.....	27
Fehlerbehebung	28
Diagnose ausführen.....	28
Eine Systemwiederherstellung durchführen.....	28
Interne Wiederherstellung	28
Externe Wiederherstellung.....	28
Eine SupportAssist Sammlung exportieren	29
Fehlerbehebung beim Netzteil	30
Speicherfehler beheben.....	30
Fehlerbehebung bei AXIS Camera Station Pro.....	30
Produktübersicht	31
Vorder- und Rückseite	31
Technische Daten	31
.....	31
Benötigen Sie Hilfe?.....	36
Nützliche Links	36
Support.....	36

Über das Gerät

Die Serie AXIS Camera Station S12 Recorder besteht aus sofort einsatzbereiten Rack-Servern und Workstations, die für eine zuverlässige HD-Überwachung mit bis zu 4K validiert sind. Für eine schnelle und einfache Installation ist die Recorder-Serie vorkonfiguriert und mit der Video Management Software AXIS Camera Station Pro einschließlich Lizenzen sowie der gesamten erforderlichen Systemsoftware vorinstalliert. Die Systemkonfiguration kann einfach von AXIS Site Designer importiert werden und mit AXIS Camera Station Pro lassen sich die vielen Vorteile des großen Produktangebots an Videosicherheitsgeräten von Axis nutzen. Die Festplatten sind für den professionellen Einsatz ausgelegt und das Betriebssystem ist auf einem Solid-State-Laufwerk installiert. Diese Rekorderserie bietet Ihrem System also sowohl Leistungsstärke als auch Zuverlässigkeit.

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 7*.
4. *Windows® konfigurieren. Wir empfehlen:*
 - Windows® auf die neuste Version aktualisieren. Siehe *Windows® aktualisieren, on page 20*.
 - Ein Standardbenutzerkonto erstellen. Siehe *Ein Benutzerkonto erstellen, on page 12*.
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 7.*

Das Gerät installieren

Vor der Installation

- Bereiten Sie weiteres Zubehör für die Installation vor: Monitor, Maus, Tastatur und Netzkabel.
- Beachten Sie, dass das Netzkabel nicht im Lieferumfang enthalten ist.
- 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.
Hardware-Verwaltung		
iDRAC	Wird für den Zugriff auf das Tool iDRAC (Integrated Dell Remote Access Controller) verwendet.	Benutzername: root Kennwort: Auf der Rückseite der Beschriftung aufgedruckt.
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.

Ihr Gerät konfigurieren

Erstes Setup des Axis Recorders

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

1. Wählen Sie als Erscheinungsbild **Light (Hell)** oder **Dark (Dunkel)**, und klicken Sie auf **Next (Weiter)**,, sofern Ihr Produkt diese Möglichkeit bietet.
2. Ändern Sie ggf. den Computernamen und klicken Sie auf **Weiter**.
3. 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.
4. 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.
5. 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 8*
4. *Live-Video ansehen, on page 8*
5. *Aufzeichnungen anzeigen, on page 9*
6. *Lesezeichen hinzufügen, on page 9*
7. *Aufzeichnungen exportieren, on page 9*
8. *Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen, on page 9*

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 S1264 Rack Recording Server 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.

Passen Sie die Speicherkapazität an

Hinweis

Bei Systemen mit über 80 Videokanälen oder einer Aufzeichnungsbitrate von über 750 Mbit/s empfehlen wir eine Speicherplatzzuweisung von 95 %. Auf allen Geräten mit AXIS Camera Station 5.56 oder höher sind standardmäßig 95 % eingestellt.

1. Gehen Sie zu **Configuration > Storage > Management (Konfiguration > Speicher > Verwaltung)** und wählen Sie einen lokalen Speicher oder ein freigegebenes Netzwerklaufwerk aus der Speicherliste.
2. Legen Sie den maximalen, von AXIS Camera Station Video Management Software zu verwendenden Speicherplatz mithilfe des Schiebereglers in dem Bereich „Overview“ (Übersicht) fest.
3. Klicken Sie auf **Anwenden**.

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 S1264 Rack Recording Server 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.

Proxyeinstellungen 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 S1264 Rack Recording Server „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 S1264 Rack Recording Server-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 S1264 Rack Recording Server-Server, die Kameras, Video-Encoder und Zusatzgeräte in einem sicheren, vom Büronetz separaten Netzwerk. Sie können den AXIS Camera Station S1264 Rack Recording Server Client auf einem Computer eines anderen Netzwerks installieren, zum Beispiel einem Netzwerk mit Internetzugang.
- Sicherstellen, dass alle Benutzer starke Kennwörter verwenden.

Ein System online lizenzieren.

Um die automatische Lizenzierung zu verwenden, müssen Sie Ihr System registrieren und mit einer Organisation verbinden.

1. Rufen Sie **Configuration (Konfiguration) > Licenses (Lizenzen) > Management (Verwaltung)** auf.
2. Stellen Sie sicher, dass **Automatic licensing (Automatische Lizenzierung)** eingeschaltet ist.
3. Klicken Sie auf **Register... (Registrieren...)**.
4. Melden Sie sich mit Ihrem MyAxis Konto an und befolgen Sie die Anweisungen auf dem Bildschirm.
5. Klicken Sie auf **Go to AXIS License Manager (AXIS License Manager aufrufen)**, um Ihre Lizenzen zu verwalten. Weitere Informationen finden Sie unter *My Systems - Benutzerhandbuch auf help.axis.com*.

Ein System offline lizenzieren

So lizenzieren Sie Ihr System manuell:

1. Rufen Sie **Configuration (Konfiguration) > Licenses (Lizenzen) > Management (Verwaltung)** auf.
2. **Automatic licensing (Automatische Lizenzierung)** deaktivieren.

3. Klicken Sie auf **Export system file... (Systemdatei exportieren...)** und speichern Sie die Datei auf dem Computer.

Hinweis

Sie müssen über eine Internetverbindung verfügen, um auf AXIS License Manager zugreifen zu können. Falls Ihr Client-Computer nicht mit dem Internet verbunden ist, kopieren Sie die Systemdatei auf einen Computer mit Internetverbindung.

4. Öffnen Sie *AXIS License Manager*.
5. Im AXIS License Manager:
 - 5.1. Wählen Sie die richtige Organisation aus oder erstellen Sie eine, falls noch keine vorhanden ist. Weitere Informationen finden Sie unter *My Systems - Benutzerhandbuch auf help.axis.com*.
 - 5.2. Rufen Sie **System setup (Systemsetup)** auf.
 - 5.3. **Upload system file (Systemdatei hochladen)** anklicken.
 - 5.4. Klicken Sie auf **Upload system file (Systemdatei hochladen)** und wählen Sie die Systemdatei aus.
 - 5.5. **Upload system file (Systemdatei hochladen)** anklicken.
 - 5.6. Klicken Sie auf **Download license file (Lizenzdatei herunterladen)**.
6. Zurück zum AXIS Camera Station S1264 Rack Recording Server Client.
7. Klicken Sie auf **Import license file... (Lizenzdatei importieren...)** und wählen Sie Ihre Lizenzdatei aus.
8. Klicken Sie auf **Go to AXIS License Manager (AXIS License Manager aufrufen)**, um Ihre Lizenzen zu verwalten.

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 S1264 Rack Recording Server anzuzeigen.

Hinweis

Administratoren von Computern, auf denen AXIS Camera Station S1264 Rack Recording Server ausgeführt werden, erhalten automatisch Administratorrechte in AXIS Camera Station S1264 Rack Recording Server. 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 S1264 Rack Recording Server zugreifen. Um einen Benutzer zu AXIS Camera Station S1264 Rack Recording Server 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 S1264 Rack Recording Server-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 S1264 Rack Recording Server 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 S1264 Rack Recording Server.
Bearbeiten	Ermöglicht die Bearbeitung von Ansichten unter AXIS Camera Station S1264 Rack Recording Server.

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

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 20*.

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**.

Festplattenlaufwerk hinzufügen

Der Speicherplatzbedarf kann variieren. Die Vorhaltezeit der gespeicherten Daten oder die Speicherung hochauflösender Aufzeichnungen erfordert häufig die Installation von mehr Speicher. In diesem Abschnitt ist beschrieben, wie Sie Ihre AXIS S12-Serie mit zusätzlichen Festplatten erweitern und diese zu Ihrer RAID-5-Konfiguration hinzufügen.

Hinweis

Für die Erweiterung bestimmter AXIS S12-Serien mit zusätzlichen Datenspeichern sind die nachstehenden Anweisungen zu befolgen. Die Anweisungen gelten ohne Gewähr. Axis Communications AB übernimmt keine Haftung für dabei entstehende Datenverluste und/oder eine fehlerhafte Konfiguration. Zur Sicherung geschäftskritischer Daten sollten die üblichen Vorsichtsmaßnahmen getroffen werden. Das folgende Verfahren zum Erweitern des Speichers wird vom technischen Support von Axis nicht unterstützt.

Hinweis

Zur Vermeidung elektrostatischer Entladungen sollte bei Arbeiten an innenliegenden Systemkomponenten stets eine Antistatikmatte und ein Antistatikband verwendet werden.

Gewährleistung

Ausführliche Informationen zur Gewährleistung finden Sie unter: www.axis.com/support/warranty.

Vorgehensweise

1. *Hot-Swap-Festplatte installieren, on page 21*
 - 1.1. *Blende entfernen, on page 21*
 - 1.2. *Blindeinschub entfernen, on page 22*
 - 1.3. *Festplatte installieren, on page 22*
2. *Neues RAID-Array erstellen, on page 23*
 - 2.1. *Rufen Sie das Konfigurationsdienstprogramm Dell PERC 11 auf., on page 23*
 - 2.2. *RAID-Storage-Array erstellen, on page 23*
 - 2.3. *RAID-Storage-Array rekonfigurieren, on page 23*
- 3.

Hot-Swap-Festplatte installieren

Blende entfernen

1. Suchen Sie den Blendenschlüssel.
2. Entriegeln Sie die Blende mithilfe des Blendenschlüssels.
3. Schieben Sie die Entriegelungslasche nach oben, und ziehen Sie die Blende nach links ab.
4. Das rechte Ende aushaken und die Blende entfernen.

Blindeinschub entfernen

- Drücken Sie die Entriegelungstaste an der Vorderseite des Blindeinschubs, und ziehen Sie diesen aus dem Festplattenschacht.

Festplatte installieren

▲ VORSICHT

- Verwenden Sie nur für den Betrieb mit der AXIS S12-Serie getestete und zugelassene Festplatten.
 - Bei der Installation einer Festplatte sicherstellen, dass die angrenzenden Laufwerke vollständig installiert sind. Der Versuch, einen Festplattenträger beim Einsetzen neben einem nicht vollständig installierten Carrier zu verriegeln, kann die Schutzfeder des unvollständig installierten Festplattenträgers beschädigen und diesen unbrauchbar machen.
 - Die Kombination von SAS- und SATA-Festplatten im gleichen RAID-Volume wird nicht unterstützt.
1. Falls ein Blindeinschub im Festplattenschacht installiert ist, entfernen Sie diesen.
 2. Eine Festplatte im Festplattenträger installieren.
 3. Die Entriegelungstaste auf der Vorderseite des Festplattenträgers drücken und den Festplattenträgergriff öffnen.
 4. Schieben Sie den Festplattenträger in den Festplattenschacht, bis der Träger an der Rückwand einrastet.
 5. Den Festplattenträgergriff schließen, um die Festplatte an ihrem Platz zu verriegeln.

RAID ändern

▲ VORSICHT

Durch Ändern des RAID werden alle Daten von Ihren Datenträgern gelöscht.

1. Lifecycle Controller starten:
 - 1.1. Gerät einschalten.
 - 1.2. Wenn der AXIS Startbildschirm angezeigt wird, die Taste F10 drücken.
2. Im Lifecycle Controller **Hardware Configuration > Configuration Wizards (Hardwarekonfiguration > Konfigurationsassistenten)** aufrufen und **RAID Configuration (RAID-Konfiguration)** auswählen.
3. Den **RAID Controller (RAID-Controller)** auswählen, auf dem das RAID erstellt werden soll. Details zu allen virtuellen Laufwerken, die auf dem ausgewählten Controller verfügbar sind, werden in der Tabelle angezeigt, die auf der Seite unter der Controllerliste zu sehen ist. **Foreign Configuration (Fremdkonfiguration)** wird angezeigt, wenn auf dem Server fremde oder nicht initialisierte HDDs verfügbar sind.

Hinweis

- Durch das Löschen der Fremdkonfiguration werden alle fremden HDDs, die auf dem ausgewählten RAID-Controller verfügbar sind, gelöscht.
 - Durch das Ignorieren der Fremdkonfiguration werden die fremden HDDs, die auf dem RAID-Controller verfügbar sind, bei der RAID-Erstellung ignoriert.
4. Fremde HDDs und nicht initialisierte HDDs löschen oder ignorieren.

Wenn Sie möchten, können Sie die nicht initialisierten Festplatten initialisieren:

 - 4.1. In der Liste aller (nicht initialisierten) Nicht-RAID-HDDs die HDDs auswählen, die in RAID-fähig konvertiert (d. h. initialisiert) werden sollen, und auf **Next (Weiter)** klicken, um sie zu initialisieren.
 - 4.2. Die entsprechende Option auf der Seite Konfigurations-Assistenten: RAID-Konfiguration auswählen.
 5. RAID-Ebene auswählen.
 6. Die physischen Festplatten aus der Tabelle auswählen und auf **Next (Weiter)** klicken.

Bei Auswahl von **Ignore foreign configuration (Fremdkonfiguration ignorieren)** werden die fremden HDDs nicht in der Tabelle angezeigt.

7. Die Attribute des virtuellen Laufwerks eingeben.
8. Klicken Sie auf **Next (Weiter)**.
9. Prüfen Sie die Einstellungen und klicken Sie auf **Fertigstellen**.
10. Lifecycle Controller zeigt eine Meldung an, die besagt, dass alle aktuellen Daten über die auf dem Controller verfügbaren virtuellen Festplatten verloren gehen. Zum Fortfahren auf **OK** klicken.
11. Auf **OK** und **Finish (Fertigstellen)** klicken.
12. Den Assistenten beenden und das System neu starten.

Neues RAID-Array erstellen

Das Konfigurationsprogramm „Human Interface Infrastructure“ (HII) ist eine in das System-BIOS integrierte Speicherverwaltungsanwendung. Es dient zur Konfiguration und Verwaltung von Controllern, virtuellen Festplatten und physischen Festplatten. Das Dienstprogramm ist eine vom Betriebssystem unabhängige Anwendung.

Rufen Sie das Konfigurationsdienstprogramm Dell PERC 11 auf.

1. Schalten Sie das System ein.
2. Drücken Sie während des Systemstarts die Taste F2, um das System-Setup aufzurufen.
3. Klicken Sie auf **Device Settings (Geräteeinstellungen)**, um alle RAID-Controller im System anzuzeigen.

RAID-Storage-Array erstellen

1. *Rufen Sie das Konfigurationsdienstprogramm Dell PERC 11 auf, on page 23.*
2. Klicken Sie auf **Main Menu > Configuration Management > Create Virtual Disk (Hauptmenü > Konfiguration verwalten > Virtuelles Laufwerk erstellen)**, und legen Sie die folgenden Parameter für das virtuelle Laufwerk fest.
 - **Select RAID Level (RAID-Level auswählen):** Wählen Sie den gewünschten RAID-Level aus.
 - **Select Physical Disks (Physische Laufwerke auswählen):** Wählen Sie das physische Laufwerk aus, von dem aus die virtuellen Laufwerke erstellt werden sollen. Diese Option wird nur bei Auswahl von **Unconfigured Capacity (Unkonfigurierte Speicherkapazität)** als physische Laufwerkskapazität angezeigt.
 - **Configure Virtual Disk (Virtuelles Laufwerk konfigurieren):** Konfigurieren Sie das virtuelle Laufwerk mithilfe der folgenden Parameter.
 - **Virtual Disk Name (Name des virtuellen Laufwerks):** Geben Sie den Namen des virtuellen Laufwerks ein.
Zulässig sind die Zeichen A-Z, a-z, 0-9, Unterstrich (_) und Bindestrich (-).
 - **Virtual Disk Size (Größe des virtuellen Laufwerks):** Legen Sie die Speicherkapazität des virtuellen Laufwerks fest.
3. Klicken Sie auf **Create Virtual Disk (Virtuelles Laufwerk erstellen)**.

▲ VORSICHT

Es stehen außerdem noch weitere Parameter zur Verfügung, die Sie ändern können. Axis Communications AB übernimmt in diesem Fall jedoch keine Haftung für eine etwaige fehlerhafte Konfiguration durch die Änderung dieser Parameter. Gehen Sie bei der Änderung von Parametern stets vorsichtig vor.

RAID-Storage-Array rekonfigurieren

Die Speicherkapazität und der RAID-Level virtueller Online-Laufwerke können auf verschiedene Weise erweitert oder geändert werden.

▲ VORSICHT

- Übergreifende virtuelle Laufwerke wie RAID 50 und 60 können nicht rekonfiguriert werden.
 - Die Rekonfiguration virtueller Laufwerke wirkt sich normalerweise auf die Speicherleistung aus, bis der Rekonfigurationsvorgang abgeschlossen ist. Die Bearbeitungszeit kann stark variieren und bis zu mehrere Tage in Anspruch nehmen. Dieser Vorgang sollte daher unbedingt während eines geeigneten Wartungsintervalls durchgeführt werden.
 - Erstellen Sie stets eine geprüfte Sicherungskopie Ihrer Daten, bevor Sie eine Aktion ausführen.
1. Rufen Sie das Konfigurationsdienstprogramm Dell PERC 11 auf, on page 23.
 2. Klicken Sie auf **Main Menu > Virtual Disk Management (Hauptmenü > Virtuelle Datenträgerverwaltung)**. Es werden alle mit dem RAID-Controller verknüpften virtuellen Laufwerke angezeigt.
 3. Um die entsprechenden Eigenschaften anzuzeigen, klicken Sie auf das virtuelle Laufwerk.
 4. Wählen Sie im Dropdown-Feld **Operations (Aktionen)** die Option **Reconfigure Virtual Disks (Virtuelle Laufwerke rekonfigurieren)** aus, und klicken Sie auf **GO (Starten)**.
 5. Wählen Sie den gewünschten **RAID Level** aus, und klicken Sie auf **Choose the Operation (Aktion wählen)**.
 6. Wählen Sie die Laufwerke aus, die dem virtuellen Laufwerk hinzugefügt werden sollen, und klicken Sie auf **Apply Changes (Änderungen übernehmen)**.
 7. Bestätigen Sie den Vorgang mit **YES (JA)**.
 8. Klicken Sie auf **Start Operation (Vorgang starten)**.
 9. Klicken Sie auf **OK**.

Den Status der Rekonstruktion des geänderten virtuellen Laufwerks können Sie in der virtuellen Datenträgerverwaltung einsehen.

Nach Starten der Rekonstruktion kann das System bis zum Abschluss des Vorgangs im Konfigurationsdienstprogramm Dell PERC 11 bleiben oder neu in das Betriebssystem geladen werden.

Beim Neuladen des Systems in das Betriebssystem ist die Systemleistung bis zum Abschluss des Neuaufbaus beeinträchtigt.

Solange der Neuaufbau nicht abgeschlossen ist, kann das Laufwerk außerdem NICHT unter Windows® erweitert werden.

▲ VORSICHT

Die für den Wiederaufbau benötigte Zeit ist von System zu System unterschiedlich und kann bis zu mehreren Tagen in Anspruch nehmen.

Microsoft Windows® konfigurieren

Neues Volume konfigurieren:

1. Klicken Sie mit der rechten Maustaste auf das Startmenü, und wählen Sie **Datenträgerverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf einen nicht zugeordneten Datenträgerbereich, und wählen Sie **Neues einfaches Volumen**.
3. Klicken Sie im **Assistent zum Erstellen neuer einfacher Volumes** auf **Weiter**.
4. Geben Sie die Größe des zu erstellenden Volumes in Megabyte (MB) ein oder übernehmen Sie die maximale Standardgröße, und klicken Sie auf **Weiter**.
5. Übernehmen Sie den Standard-Laufwerksbuchstaben, oder wählen Sie einen anderen Laufwerksbuchstaben für die Partition aus und klicken Sie auf **Weiter**.
6. Im Dialogfenster „Partition formatieren“:
 - Wenn Sie das Volume nicht sofort formatieren möchten, wählen Sie die Option **Dieses Volume nicht formatieren** aus und klicken anschließend auf **Weiter**.

- Um das Volume mit den Standardeinstellungen zu formatieren, klicken Sie auf **Weiter**.
- 7. Überprüfen Sie Ihre Auswahl, und klicken Sie auf **Fertig stellen**.
In der Datenträgerverwaltung wird nun das neue Volume angezeigt. Sie können die Datenträgerverwaltung nun schließen, und das Volume kann jetzt von Ihrem System verwendet werden.

Vorhandenes Volume konfigurieren:

1. Klicken Sie mit der rechten Maustaste auf das Startmenü, und wählen Sie **Datenträgerverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf das Volume, und wählen Sie **Volume erweitern**.
3. Klicken Sie im **Assistenten zur Datenträgererweiterung** auf **Weiter**.
4. Wählen Sie den Datenträger mit dem ungenutzten Speicherplatz aus, und klicken Sie auf **Weiter**. Diese Einstellung ist in der Regel standardmäßig aktiviert.
5. Überprüfen Sie Ihre Auswahl, und klicken Sie auf **Fertig stellen**.
In der Datenträgerverwaltung wird nun das erweiterte Volume angezeigt. Sie können die Datenträgerverwaltung nun schließen, und das Volume kann jetzt von Ihrem System verwendet werden.

Konfigurieren von iDRAC

Der Integrated Dell Remote Access Controller 9 (iDRAC9) mit Lifecycle Controller wurde entwickelt, um die Produktivität von Systemadministratoren zu steigern und die Gesamtverfügbarkeit von Dell-Systemen zu verbessern. iDRAC macht Administratoren auf Systemprobleme aufmerksam, unterstützt sie bei der Remote-Systemverwaltung und reduziert die Notwendigkeit des physischen Zugriffs auf das System. Sie müssen die anfänglichen Netzwerkeinstellungen auf der Grundlage Ihrer Netzwerkinfrastruktur konfigurieren, um die Kommunikation zum und vom iDRAC zu ermöglichen.

1. Während des Einschaltstests (POST) F10 drücken.

Hinweis

Der Assistent für die erste Einrichtung des Lifecycle Controllers wird nur zum ersten Mal angezeigt. Wählen Sie mit dem Assistenten für die Ersteinrichtung Sprache und Tastatur aus, konfigurieren Sie Netzwerkeinstellungen, iDRAC-Netzwerkeinstellungen, Konfiguration von Zugangsdaten und sehen Sie sich die Zusammenfassung der Einstellungen an. Um Konfigurationsänderungen später vorzunehmen, wählen Sie auf der Startseite des Lifecycle Controllers die Option **Einstellungen** aus.

2. Konfigurieren Sie die Sprache und Tastatur, und klicken Sie auf **Weiter**.
3. Überprüfen Sie die Produktübersicht und klicken Sie auf **Weiter**.
4. Konfigurieren der Netzwerkeinstellungen des Lifecycle Controllers:
 - 4.1. Wählen Sie in der Dropdown-Liste der **NIC-Karte** den zu konfigurierenden NIC-Port aus.
 - 4.2. Wählen Sie in der Dropdown-Liste **IPv4-Netzwerkeinstellungen > Quelle der IP-Adresse** eine der folgenden Optionen aus:
 - **DHCP**: zeigt an, dass der NIC mit einer IP-Adresse von einem DHCP-Server konfiguriert werden muss. DHCP ist die Standardoption und die DHCP-IP-Adresse wird auf der Seite Netzwerkeinstellungen angezeigt.
 - **Statische IP**: zeigt an, dass die NIC mit einer statischen IP konfiguriert werden muss. Geben Sie die Eigenschaften der IP-Adresse ein, einschließlich **IP-Adresse**, **Subnetzmaske**, **Standard-Gateway** und **DNS-Adresse**. Wenden Sie sich an Ihren Netzwerkadministrator, wenn Sie nicht über diese Informationen verfügen.
 - **No Configuration (Ohne Konfiguration)**: zeigt an, dass die NIC nicht konfiguriert werden darf.
 - 4.1. Wenn VLAN verwendet wird, klicken Sie auf **Aktiviert** und geben Sie die **VLAN-ID** und die **Priorität** unter **Lifecycle Controller VLAN-Einstellungen** ein, um die VLAN-Einstellungen einer NIC zu konfigurieren.
 - 4.2. Klicken Sie auf **Next (Weiter)**. Wenn die Einstellungen des Lifecycle Controllers nicht korrekt konfiguriert wurden, wird eine Fehlermeldung angezeigt.
5. Konfigurieren von iDRAC-Netzwerk und Zugangsdaten:

- 5.1. **IPv4 Configuration > IP Address Source (IP-Adressquelle)** wählen und eine der folgenden Optionen wählen:
 - **Statisch:** zeigt an, dass das Netzwerk mit einer statischen IP konfiguriert werden muss. Geben Sie die Eigenschaften der IP-Adresse ein, einschließlich **IP-Adresse**, **Subnetzmaske**, **Standard-Gateway**, **DNS-Adressquelle** und **DNS-Adresse**. Wenden Sie sich an Ihren Netzwerkadministrator, wenn Sie nicht über diese Informationen verfügen.
 - **DHCP:** zeigt an, dass der NIC mit einer IP-Adresse von einem DHCP-Server konfiguriert werden muss. DHCP ist die Standardoption und die DHCP-IP-Adresse wird auf der Seite Netzwerkeinstellungen angezeigt.
- 5.1. Geben Sie unter **Anmeldeinformationen** den **Benutzernamen** und das **Kennwort** ein, um auf das iDRAC-Netzwerk zu zugreifen.
- 5.2. Klicken Sie auf **Next (Weiter)**.
6. Überprüfen Sie die Zusammenfassung des Lebenszyklus-Controllers und der iDRAC-Netzwerkkonfiguration und klicken Sie auf **Fertig stellen**.

Cybersicherheit

Produktspezifische Informationen zur Cybersicherheit finden Sie im Datenblatt des Produkts auf axis.com.

Ausführliche Informationen zur Cybersicherheit in AXIS OS finden Sie im *AXIS OS Härtingsleitfaden*.

Sicheres Hochfahren

Das sichere Hochfahren ist eine Funktion, die das Ausführen von nicht sicherer Software auf Ihrem System verhindert. Diese Funktion wird beim Systemstart ausgeführt und nutzt digitale Signaturen, um die Zertifikate der Software und des Betriebssystems zu überprüfen. Auf dem System können nur vertrauenswürdige Software und Betriebssysteme ausgeführt werden.

Trusted Platform Module (TPM)

Das TPM ist eine Komponente, die kryptografische Funktionen zum Schutz von Daten vor unbefugtem Zugriff bereitstellt. Es ist standardmäßig aktiviert und wir empfehlen nicht, es zu deaktivieren.

Secure Component Verification (SCV)

Bei der Fertigung Ihres Geräts im Werk wurde ein Zertifikat erstellt, um sicherzustellen, dass Sie auch wirklich das von Ihnen bestellte Gerät erhalten und das Gerät nach dem Verlassen des Werks nicht manipuliert wurde. Das Werk unterzeichnet das Zertifikat und meldet es im iDRAC an. Wenn Sie das Gerät erhalten, rufen Sie die **AXIS Recorder Toolbox** auf, um zu sehen, ob Ihr Gerät über SCV verfügt, und überprüfen Sie das Zertifikat. So können Sie feststellen, ob das richtige Systeminventar vorhanden ist. Weitere Informationen zu SCV finden Sie auf dell.com.

Um mehr zu den Cybersicherheitsfunktionen von Axis Geräten zu erfahren, gehen Sie auf axis.com/learning/white-papers und suchen Sie nach Cybersicherheit.

Axis Sicherheitsbenachrichtigungsdienst

Axis bietet einen Benachrichtigungsdienst mit Informationen zu Sicherheitslücken und anderen sicherheitsrelevanten Angelegenheiten für Axis Geräte. Um Benachrichtigungen zu erhalten, können Sie sich unter axis.com/security-notification-service registrieren.

Schwachstellen-Management

Um das Risiko für die Kunden zu minimieren, hält sich Axis als **Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)** an Branchenstandards, um entdeckte Schwachstellen in unseren Geräten, unserer Software und unseren Dienstleistungen zu verwalten und darauf zu reagieren. Weitere Informationen zu den Richtlinien von Axis für das Management von Schwachstellen, zur Meldung von Schwachstellen, zu bereits

bekannt gewordenen Schwachstellen und zu entsprechenden Sicherheitshinweisen finden Sie unter axis.com/vulnerability-management.

Sicherer Betrieb von Axis Geräten

Axis Geräte mit werksseitig festgelegten Standardeinstellungen sind mit sicheren Standardschutzeinrichtungen vorkonfiguriert. Es wird empfohlen, das Gerät mit mehr Sicherheit zu konfigurieren. Mehr über den Ansatz von Axis für die Cybersicherheit, einschließlich bewährter Verfahren, Ressourcen und Richtlinien zur Sicherung Ihrer Geräte, lesen Sie auf axis.com/about-axis/cybersecurity.

Fehlerbehebung

Diagnose ausführen

Durch das Ausführen der Diagnose können Sie die Ursache für ein Systemproblem ermitteln. Die Diagnose testet Ihre Systemhardware, ohne dass zusätzliche Geräte erforderlich sind oder Datenverluste riskiert werden.

1. Beim Hochfahren des Systems F10 drücken, um den Lifecycle Controller aufzurufen.
2. Die **Hardwarediagnose** öffnen und **Hardwarediagnose ausführen** anklicken.
3. Notieren Sie den Fehlercode und wenden Sie sich an den technischen Support von Axis.

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.

Eine SupportAssist Sammlung exportieren

Sie können die SupportAssist Sammlung auf ein USB-Laufwerk oder eine Netzwerk-Freigabe (CIFS/NFS) exportieren. Die Sammlung umfasst folgende Daten:

- Hardware
- RAID-Controller-Protokolle

So exportieren Sie die SupportAssist Sammlung:

1. Während des Einschalt-Selbsttests (POST) **F10** drücken, um den Lifecycle Controller zu starten.
2. **Hardware Diagnostics > Export SupportAssist Sammlung** aufrufen.
3. Geschäftsbedingungen lesen und auf **Weiter** klicken.
Sie müssen die Geschäftsbedingungen akzeptieren, damit der technische Support die Daten der SupportAssist Sammlung verwenden kann.
4. Die Datenoptionen auswählen, die in die SupportAssist Sammlung aufgenommen werden sollen, und auf **Weiter** klicken.
5. Die erforderlichen Exporteinstellungen eingeben und auf **Next (Weiter)** klicken.
 - So wird auf ein USB-Laufwerk exportiert: Die USB-Laufwerk-Option auswählen und dann den Namen des USB-Laufwerks auswählen. Die Informationen zum Dateipfad eingeben, an den die Sammlung exportiert werden soll.
 - Um in NFS zu exportieren: Die Option NFS auswählen und die erforderlichen Informationen eingeben.
 - Um in CIFS zu exportieren: Die Option CIFS auswählen und die erforderlichen Informationen eingeben.
Auf **Test Network Connection (Netzwerkverbindung testen)** klicken, um zu überprüfen, ob der Lifecycle Controller eine Verbindung mit der angegebenen IP-Adresse herstellen kann.
Standardmäßig werden die Gateway-IP, DNS-Server-IP, Host-IP und Proxy-IP angepingt.
6. Auswahl überprüfen und auf **Finish (Fertigstellen)** klicken.
Lifecycle Controller ruft die ausgewählten Sammlungsdaten ab und exportiert sie an den angegebenen Speicherort. Dies kann ein paar Minuten dauern.

Fehlerbehebung beim Netzteil

Hinweis

Nach der Installation eines Netzteils einige Sekunden warten, bis das System das Netzteil erkennt und feststellen kann, ob das Netzteil ordnungsgemäß funktioniert.

1. Sicherstellen, dass keine losen Verbindungen vorhanden sind. Zum Beispiel lose Stromkabel.
2. Sicherstellen, dass die LED des Netzteils anzeigt, dass das Netzteil ordnungsgemäß funktioniert.
3. Den Status der Betriebsanzeige am Netzteil überprüfen. Siehe *Technische Daten*, on page 31.
4. Bei einer redundanten Stromversorgungskonfiguration sicherstellen, dass beide Netzteile vom gleichen Typ und der gleichen Wattleistung sind.
5. Sicherstellen, dass nur Netzteile mit EPP-Kennzeichnung (Extended Power Performance) auf der Rückseite verwendet werden.
6. Das Netzteil zurücksetzen.
7. Wenn das Problem weiterhin besteht, den technischen Support von AXIS kontaktieren.

Speicherfehler beheben

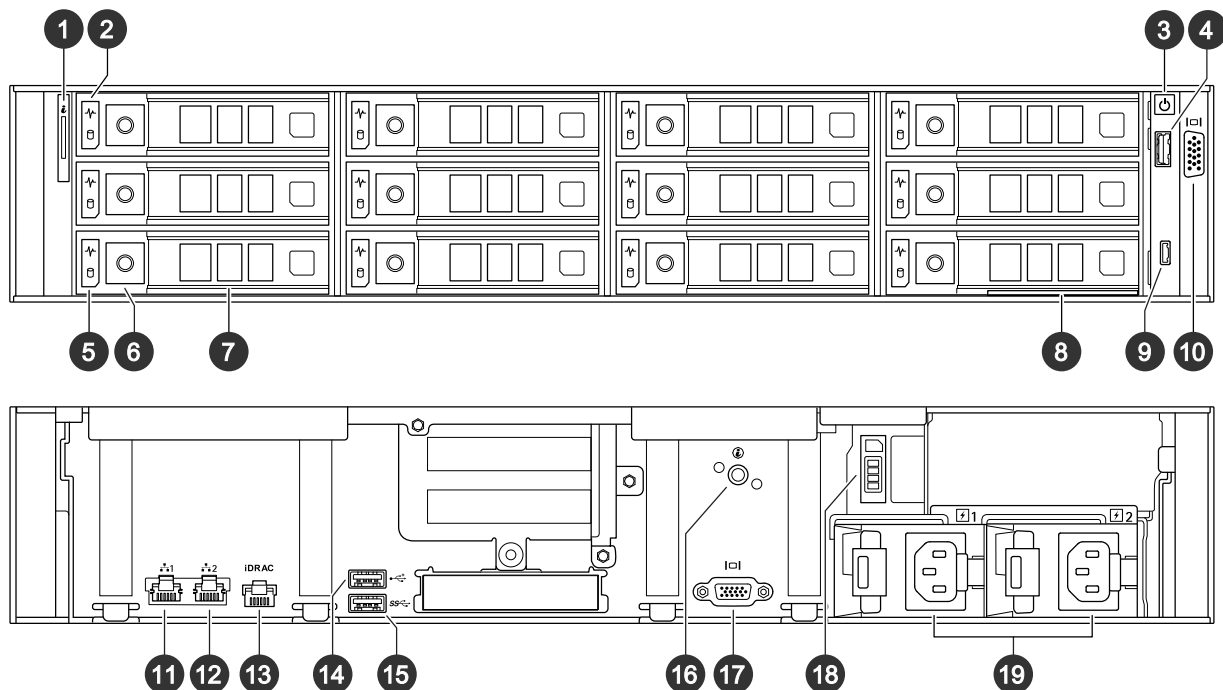
1. Das BIOS auf die neueste Version aktualisieren.
2. Wenn die Fehler weiterhin bestehen, den technischen Support von AXIS kontaktieren.

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*.

Produktübersicht

Vorder- und Rückseite



- 1 Systemabfrage Taste und -anzeige
- 2 Festplattenstatus-LED
- 3 Netzschalter/Netz-LED
- 4 USB 2.0 Port
- 5 LED für Laufwerksaktivität
- 6 Entriegelungstaste für den Festplatteneinschub
- 7 Einschub für Festplatte
- 8 Beschriftung
- 9 iDRAC-Schnittstelle
- 10 VGA-Port
- 11 1 GbE Ethernet Port 1
- 12 1 GbE Ethernet Port 2
- 13 iDRAC-Ethernet-Schnittstelle
- 14 USB 2.0 Port
- 15 USB-3.0-Port
- 16 Systemabfrage Taste und -anzeige
- 17 VGA-Port
- 18 Einschub für Solid State Drive
- 19 Netzteile

Technische Daten

LED-Betriebsanzeigen

LED	Beschreibung	Aktion
Laufwerksanzeige	Bei Laufwerksfehlern leuchtet die LED-Anzeige durchgehend gelb.	Überprüfen Sie das Systemereignisprotokoll, um zu ermitteln, ob das Laufwerk einen Fehler hat.
Temperaturanzeige	Wenn im System ein Temperaturfehler auftritt, leuchtet	Stellen Sie sicher, dass keine der folgenden Bedingungen gegeben ist:

	die LED-Anzeige durchgehend gelb. Beispielsweise wenn die Umgebungstemperatur außerhalb eines Bereichs liegt oder ein Lüfterausfall vorliegt.	• Ein Lüfter wurde entfernt oder ist defekt. • Systemabdeckung, Zuluftführungen oder Luftfilterhalterung wurden entfernt. • Umgebungstemperatur ist zu hoch. • Der äußere Luftstrom ist blockiert.
Elektrische Anzeige	Wenn im System ein elektrischer Fehler auftritt, leuchtet die LED-Anzeige durchgehend gelb. Dies kann beispielsweise eine Spannung außerhalb des Bereiches oder ein Defekt am Netzteil oder am Spannungsregler sein.	Überprüfen Sie das Systemereignisprotokoll oder die Systemmeldungen auf das spezifische Problem. Wenn es ein Problem mit dem Netzteil gibt, überprüfen Sie die LED am Netzteil. Setzen Sie das Netzteil neu ein.
Speicheranzeige	Bei Speicherfehlern leuchtet die LED-Anzeige durchgehend gelb.	Überprüfen Sie das Systemereignisprotokoll oder die Systemmeldungen auf die Position des defekten Speichers. Setzen Sie das Speichermodul erneut ein.
PCIe-Anzeige	Wenn ein Problem mit einer PCIe-Karte auftritt, leuchtet die LED-Anzeige durchgehend gelb.	System neu starten. Aktualisieren Sie alle erforderlichen Treiber für die PCIe-Karte. Installieren Sie die Karte erneut.

Systemzustand und ID-Anzeigen

LED	Beschreibung	Aktion
Durchgehend blau	Das System ist eingeschaltet, das System ist fehlerfrei und der System-ID-Modus ist nicht aktiv.	Taste für Systemzustand und System-ID drücken, um in den System-ID-Modus zu wechseln.
Blinkt blau	Der System-ID-Modus ist aktiv.	Taste für Systemzustand und System-ID drücken, um in den Systemzustands-Modus zu wechseln.
Durchgehend gelb	Das System befindet sich im abgesicherten Modus.	
Blinkt gelb	Bei dem System ist ein Fehler aufgetreten.	Systemereignisprotokoll auf die spezifische Fehlermeldung überprüfen.

iDRAC Direkt-LED-Anzeigen

LED	Beschreibung
Zwei Sekunden grün	Laptop oder Tablet ist angeschlossen.

Blinkt grün (zwei Sekunden eingeschaltet und zwei Sekunden ausgeschaltet)	Laptop oder Tablet ist angeschlossen und wird erkannt.
Aus	Laptop oder Tablet sind nicht eingesteckt.

NIC-Anzeigen

LED	Beschreibung
Verbindungs- und Aktivitätsanzeigen sind deaktiviert	Der NIC ist nicht mit dem Netzwerk verbunden.
Verbindungsanzeige ist grün und Aktivitätsanzeige blinkt grün	Der NIC ist mit der maximalen Portgeschwindigkeit mit einem gültigen Netzwerk verbunden, und Daten werden gesendet oder empfangen.
Verbindungsanzeige ist gelb und Aktivitätsanzeige blinkt grün	Der NIC ist mit weniger als der maximalen Portgeschwindigkeit mit einem gültigen Netzwerk verbunden, und Daten werden gesendet oder empfangen.
Verbindungsanzeige ist grün und Aktivitätsanzeige ist ausgeschaltet	Der NIC ist mit der maximalen Portgeschwindigkeit mit einem gültigen Netzwerk verbunden, und es werden keine Daten gesendet oder empfangen.
Verbindungsanzeige ist gelb und Aktivitätsanzeige ist ausgeschaltet	Der NIC ist mit weniger als der maximalen Portgeschwindigkeit mit einem gültigen Netzwerk verbunden, und es werden keine Daten gesendet oder empfangen.

Netzteilanzeigen (PSU)

LED	Beschreibung
Grün	Eine gültige Stromquelle ist an das Netzteil angeschlossen, und das Netzteil ist betriebsbereit.
Blinkt gelb	Es liegt bei diesem Netzteil ein Problem vor.
Nicht eingeschaltet	Das Netzteil ist nicht mit einer Stromversorgung verbunden.

Blinkt grün	Die Firmware des Netzteils wird aktualisiert. ▲ VORSICHT Trennen Sie während der Aktualisierung der Firmware weder das Netzkabel noch das Netzteil vom Stromnetz. Sollte die Aktualisierung der Firmware unterbrochen werden, funktionieren die Netzteile nicht mehr.
Blinkt grün und schaltet sich aus	Wenn ein Netzteil mit Hot Plugging betrieben wird, blinkt es fünfmal grün mit einer Frequenz von 4 Hz und schaltet sich aus. Dies weist auf einen Netzteilfehler in Bezug auf Effizienz, Funktionsumfang, Integritätsstatus oder unterstützte Spannung hin. ▲ VORSICHT • Wenn zwei Netzteile installiert sind, müssen beide Netzteilarten die gleiche Art von Kennzeichnung aufweisen. Beispiel: Kennzeichnung als Extended Power Performance (EPP). Das Kombinieren von Netzteilen aus früheren Generationen von PowerEdge-Servern wird nicht unterstützt, selbst wenn die Netzteile die gleiche Nennleistung haben. Dies führt zu einem Netzteilfehler oder einem Fehler beim Einschalten des Systems. • Wenn zwei Netzteile verwendet werden, müssen sie vom gleichen Typ sein und die gleiche maximale Ausgangsleistung aufweisen. • Beim Korrigieren eines Netzteilfehlers das Netzteil mit der blinkenden Anzeige ersetzen. Der Austausch des Netzteils zur Erzeugung eines übereinstimmenden Paares kann zu einem Fehler und einem unerwarteten Herunterfahren des Systems führen. Um von einer Konfiguration mit hoher Leistung zu einer Konfiguration mit niedriger Leistung zu wechseln oder umgekehrt, müssen Sie das System ausschalten.

Laufwerksanzeigen

LED	Beschreibung
Blinkt zweimal pro Sekunde grün	Das Laufwerk wird identifiziert oder die Entfernung wird vorbereitet.
Aus	Das Laufwerk kann nun entfernt werden. Hinweis Der Laufwerks-Indikator bleibt ausgeschaltet, bis alle Laufwerke nach dem Einschalten des Systems initialisiert sind. Während dieser Zeit können die Laufwerke nicht entfernt werden.
Blinkt grün, gelb und schaltet sich dann aus	Es liegt ein unerwarteter Laufwerksfehler vor.

Blinkt viermal pro Sekunde gelb	Ein Laufwerksfehler ist aufgetreten.
Blinkt langsam grün	Das Laufwerk wird wiederhergestellt.
Durchgehend grün	Das Laufwerk ist online.
Blinkt drei Sekunden grün, drei Sekunden lang gelb und schaltet sich dann nach sechs Sekunden aus	Die Wiederherstellung wurde gestoppt.

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.

T10177845_de

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB