

# Benutzerhandbuch

Avigilon ACC™ ES Rugged Appliance mit 8 Ports

VMA-RPA-RGD-8P2 und VMA-RPA-RGD-8P4

© 2020, Avigilon Corporation. Alle Rechte vorbehalten. AVIGILON, das AVIGILON-Logo, AVIGILON CONTROL CENTER, ACC und AVIGILON APPEARANCE SEARCH sind Marken der Avigilon Corporation. MAC, MacOS, FINDER und MACINTOSH sind eingetragene Handelsmarken von Apple Inc. FIREFOX ist eine eingetragene Handelsmarke der Mozilla Foundation. Android ist eine Marke von Google LLC. Bei den anderen in diesem Dokument genannten Produktnamen kann es sich um die Marken der jeweiligen Inhaber handeln. Das Fehlen der Symbole™ und® in Verbindung mit einer Marke in diesem Dokument oder überhaupt stellt keine Erklärung des Verzichts an der entsprechenden Marke dar. Die innovativen Lösungen der Avigilon Corporation sind durch in den USA und anderen Gerichtsbarkeiten weltweit angemeldete Patente geschützt (siehe [avigilon.com/patents](http://avigilon.com/patents)). Soweit nicht ausdrücklich schriftlich vereinbart, werden keine Lizenzen in Bezug auf Urheberrechte, Designs, Marken, Patente oder andere Rechte an geistigem Eigentum von der Avigilon Corporation oder seinen Lizenzgebern erteilt.

Dieses Dokument wurde mit Hilfe von Produktbeschreibungen und Spezifikationen erstellt und veröffentlicht, die zum Zeitpunkt der Veröffentlichung verfügbar waren. Die Inhalte dieses Dokuments und die hier dargestellten technischen Daten der Produkte können ohne Vorankündigung geändert werden. Die Avigilon Corporation behält sich das Recht vor, alle diese Änderungen ohne Vorankündigung vorzunehmen. Weder die Avigilon Corporation noch eines ihrer verbundenen Unternehmen: (1) garantiert die Vollständigkeit oder Richtigkeit der in diesem Dokument enthaltenen Informationen; oder (2) ist verantwortlich für die Verwendung oder das Vertrauen in die Informationen. Die Avigilon Corporation ist nicht verantwortlich für Verluste oder Schäden (einschließlich Folgeschäden), die durch das Vertrauen auf die hierin enthaltenen Informationen verursacht werden.

Avigilon Corporation  
avigilon.com

PDF-8PortRuggedAnalytics-A

Revision: 2 - DE

20200707

# Inhaltsverzeichnis

Einführung .....	5
Lieferumfang .....	6
Erforderliche Werkzeuge .....	7
Überblick .....	8
Vorderansicht .....	8
Rückansicht .....	9
Systemanforderungen .....	10
Bildfrequenz der Kamera .....	10
Webbrowser .....	10
Unterstützte Netzwerkkonfigurationen .....	11
Montage einer ACC ES Rugged Appliance mit 8 Ports .....	12
Anschließen einer ACC ES Rugged Appliance mit 8 Ports an ein Netzteil .....	15
Erstmaliges Starten der ACC ES Rugged Appliance mit 8 Ports .....	16
Konfigurieren der Appliance .....	19
ACC ES Admin Webbenutzeroberfläche starten .....	19
Anzeigen des PoE Port-Status .....	21
Verwalten von ACC Diensten und Speicher .....	22
Dienstprotokolle für den Support zur Verfügung stellen .....	23
Neustart des Geräts und Verwalten von Geräteeinstellungen .....	23
Überwachen und Trennen der Speicher-SSD .....	25
Verbinden des Geräts mit Benutzern und Kameras .....	26
Zuweisen eines PoE-Leistungsbudgets .....	27
Bereitstellung von Geräteprotokollen für den Support .....	29
ACC-Client installieren und starten .....	30
Verbinden mit der ACC-Software und ACS .....	31
ACC-Software aktivieren und konfigurieren .....	31
Verbinden mit Avigilon Cloud Services .....	31
Anschließen an externe Geräte .....	32
LED-Anzeigen .....	33
Budgetierung der PoE-Leistung .....	34
Verwaltung von Zertifikaten .....	35

Ersetzen des Webzertifikat .....	36
Laden Sie ein vertrauenswürdigen CA-Zertifikat hoch .....	37
Aktualisieren der Firmware .....	38
Verwendung der Software-Reset-Taste .....	40
Werkseinstellungen wiederherstellen .....	42
Ersetzen der Speicher-SSD .....	44
Fehlerbehebung .....	48
Das Gerät kann nicht erkannt werden .....	48
Netzwerkconfiguration .....	48
Systemzustand überprüfen .....	49
Weitere Informationen .....	50
Technischer Support .....	50
Upgrades .....	50
Feedback .....	50

# Einführung

Die Avigilon ACC ES Rugged Appliance mit 8 Ports ist eine All-in-One-Lösung für die Netzwerkvideoaufzeichnung mit serverseitiger Videoanalyse, die robust für die Installation und den Einsatz in extremen Umgebungen und an entlegenen Standorten entwickelt wurde. Die Appliance bietet folgende Funktionen:

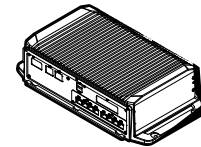
- Ein PoE-Schalter zur Verbindung und Stromversorgung von IP-Kameras.
- Integrierter Server zum Ausführen der Avigilon Control Center-Server-Software.
- Videoanalyse-Engine zur Aktivierung der Erkennung klassifizierter Objekte auf angeschlossenen nicht-analytischen Kameras.

In diesem Handbuch wird beschrieben, wie Sie die Appliance an verschiedenen Orten mit unterschiedlichen Stromanforderungen installieren und das System nach dem Einschalten der Appliance konfigurieren.

# Lieferumfang

Stellen Sie sicher, dass das ACC ES Rugged Appliance mit 8 Ports-Paket Folgendes enthält:

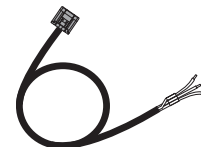
ACC ES Rugged Appliance mit 8 Ports



Schlüssel auf der Vorderseite



Stromversorgungskabel (zum Anschluss an eine vom Benutzer bereitgestellte 9-32 VDC 100 W (min) Stromversorgung)



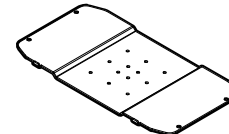
Digitales Ein-/Ausgangskabel



DIN-Halterung



Montageplatte für die DIN-Halterung



4 (vier) Flachkopfschrauben zur Befestigung der DIN-Halterung an der Montageplatte in einer Plastiktüte mit der Bezeichnung DIN-Schiene Nr. 1



4 (vier) Rundkopfschrauben zur Befestigung der ACC ES Rugged Appliance mit 8 Ports an der Montageplatte in einer Plastiktüte mit der Bezeichnung DIN-Schiene Nr. 2



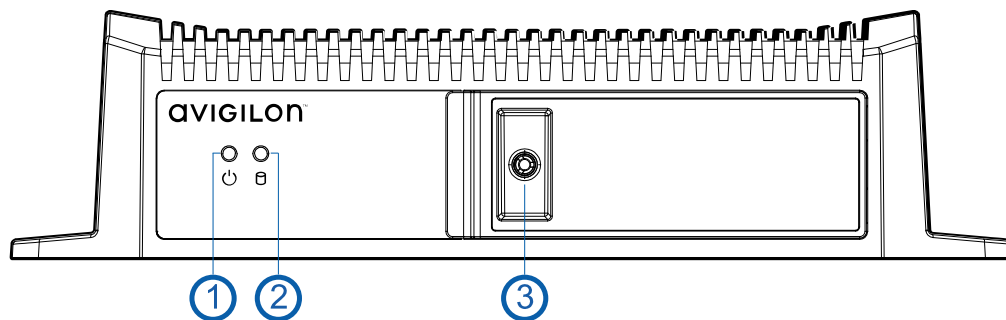
**Wichtig:** Zur Einhaltung von UL 60950-1 muss es sich bei der ACC ES Rugged Appliance mit 8 Ports, wenn sie über ein externes Netzteil mit Strom versorgt wird, um ein UL-gelistetes Netzteil handeln, das für den Einsatz bei Tma 40C geeignet ist, dessen Ausgang ES1 (oder SELV) erfüllt und für 9-32 VDC mit mindestens 100 W ausgelegt ist. Für weitere Informationen wenden Sie sich bitte an Avigilon.

## Erforderliche Werkzeuge

Zum Befestigen der ACC ES Rugged Appliance mit 8 Ports und der DIN-Halterung an der Montageplatte ist lediglich ein Kreuzschlitzschraubendreher Nr. 2 erforderlich.

# Überblick

## Vorderansicht



1. **LED-Anzeige für Stromversorgung**
2. **LED-Anzeige für Festplattenaktivität**

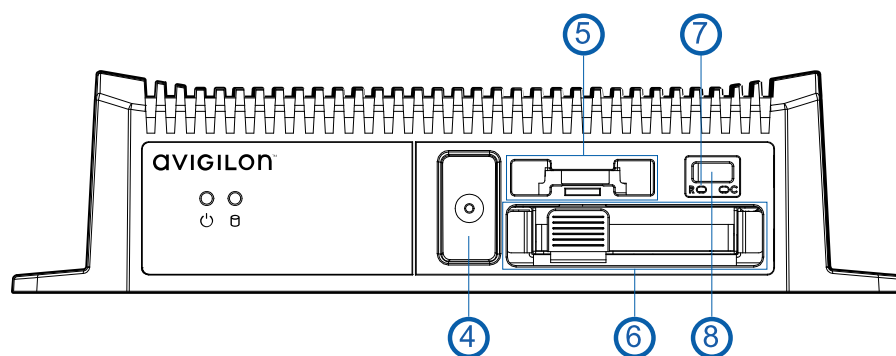
Siehe *LED-Anzeigen* auf Seite 33

3. **Verriegeln (verriegelte Position)**

Die Vorderseite ist normalerweise verriegelt, um den Zugriff auf interne Komponenten zu schützen und zu verhindern, wie oben gezeigt.

4. **Verriegeln (entriegelte Position)**

Entriegeln Sie die Vorderseite mit dem Schlüssel und öffnen Sie sie, um auf die internen Komponenten zuzugreifen (siehe Abbildung unten).



5. **CMOS-Akkubehälter**

Die Stromversorgung des Akkus im Halter behält die internen Zeit- und Datumseinstellungen der Appliance sowie die BIOS-Einstellungen im CMOS-Speicher bei. Wenn die Zeit- und Datumseinstellungen an der Appliance unzuverlässig werden, darf der Akku nur von einem geschulten Techniker ausgetauscht werden.



Es besteht Explosionsgefahr, wenn der Akku nicht korrekt ausgetauscht wird. Nur durch den





gleichen oder gleichwertigen Typ ersetzen, der vom Hersteller empfohlen wird. Entsorgen Sie gebrauchte Akkus gemäß den Anweisungen des Herstellers.

## 6. SSD-Fach

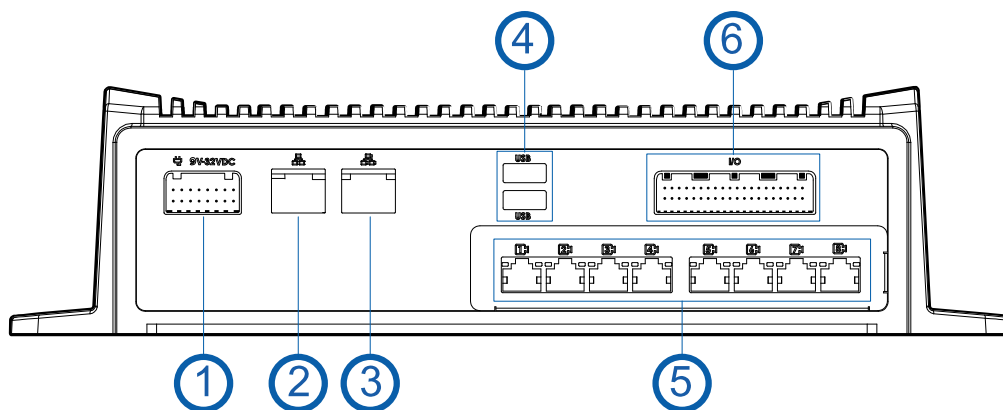
Schieben Sie das Fach hinein und heraus, um auf die Speicher-SSD zuzugreifen. Siehe *Ersetzen der Speicher-SSD* auf Seite 44.

## 7. Reset-Taste

Verwenden Sie diese Schaltfläche für einen Neustart der Appliance.

## 8. USB 3.0-Port

# Rückansicht



## 1. Stromanschluss

## 2. Uplink-Port des Unternehmensnetzwerks

Akzeptiert eine 1GbE-Ethernet-Verbindung zum allgemeinen Netzwerk, um Benutzern den Zugriff auf das Webinterface und das angeschlossene Kameravideo zu ermöglichen.

## 3. Uplink-Port des Kameranetzwerks

Akzeptiert eine 1-GbE-Ethernet-Verbindung zur Verbindung mit anderen PoE-Switches und -Kameras.

## 4. USB 2.0-Ports

## 5. PoE-Switch-Komponente

Verbinden Sie die Kameras mit der PoE-Switch-Komponente mit 10/100 Geschwindigkeit, um die Kameras mit Strom zu versorgen und Videos aufzunehmen. Der Schalter ist in der Lage, insgesamt 60 Watt Leistung bereitzustellen, die auf alle PoE-Ports verteilt wird.

## 6. E/A-Anschluss

Ermöglicht das Anschließen externer E/A-Geräte. Die beiden Kabelenden sind für den digitalen Eingang und den digitalen Ausgang gekennzeichnet. Weitere Informationen finden Sie unter *Anschließen an externe Geräte* auf Seite 32.

# Systemanforderungen

## Bildfrequenz der Kamera

Die ACC ES Rugged Appliance mit 8 Ports kann Analysen für nicht-analytische Kameras bieten. Für eine optimale Analyseleistung sollte die Quellkamera mindestens 10 Bilder pro Sekunde (ips) streamen.

## Webbrowser

Die Verwaltungseinstellungen für die Appliance werden über eine Weboberfläche verwaltet, auf die von jedem Windows-, Mac- oder Mobilgerät aus mit einem der folgenden Webbrowser zugegriffen werden kann:

- Mozilla Firefox Browser-Version 3.6 oder später
- Google Chrome Browser 8.0 oder höher
- Microsoft Edge™ Browser 25 oder höher
- Safari 5.0 oder höher
- Chrome auf Android™ 2.2 oder höher
- Safari auf Apple® iOS 5 oder höher.
- Windows Internet Explorer Browser-Version 7.0 oder höher

**Hinweis:** Der Webbrowser muss für die Annahme von Cookies konfiguriert sein, damit das Webinterface ordnungsgemäß funktionieren kann.

# Unterstützte Netzwerkkonfigurationen

**Hinweis:** Der Kamera-Uplink-Port unterstützt keine dynamisch schaltenden DHCP-Server.

Netzwerkanschlüsse	Kamerazugriff auf Webinterface	Unterstützte IP-Konfigurationen		Anmerkungen
		Unternehmens-LAN Uplink	Kamera-LAN Uplink	
<b>Nur Unternehmens-LAN-Uplink</b>	Nein	Statisch oder DHCP-zugewiesen	Nicht verbunden (als DHCP lassen)	Kamera-LAN-Uplink und angeschlossene Kameras werden Zeroconf IP-Adressen verwenden.
<b>Nur Kamera-LAN-Uplink</b>	Ja	Nicht verbunden (als DHCP lassen)	Statisch, DHCP-zugewiesen, DHCP-Zeroconf	
<b>Unternehmen und Kamera LAN-Uplink</b>	nur über Kamera-LAN-Uplink	Statisch, DHCP-zugewiesen, DHCP-Zeroconf	Statisch, DHCP-zugewiesen, DHCP-Zeroconf	Unternehmens- und Kamera-LAN-Uplinks müssen sich in verschiedenen Subnetzen befinden.

# Montage einer ACC ES Rugged Appliance mit 8 Ports

Sie können die ACC ES Rugged Appliance mit 8 Ports an fast jeder ebenen Fläche montieren, die ihr Gewicht in jeder Ausrichtung tragen kann, oder an einer DIN-Schiene in einer von vier Ausrichtungen. Mit Ausnahme der Montage an einer DIN-Schiene mit der mitgelieferten Montageplatte und der DIN-Schienehalterung und den Schrauben müssen Sie Schrauben und Anker oder Schrauben und Muttern bereitstellen, die für die Oberfläche geeignet sind, auf der Sie die Appliance montieren.

**Tipp:** Montieren Sie die Appliance an einer beliebigen Oberfläche oder an einer DIN-Schiene, bevor Sie die Appliance dauerhaft einschalten, Kameras an sie anschließen und mit der Aufnahme beginnen. Wenn Sie Ihre Appliance vor der Montage aufstellen möchten, empfehlen wir Ihnen, die Stromversorgung der Appliance auszuschalten und alle Kabel nach Abschluss der Installation und vor der Montage zu trennen.

## So befestigen Sie die Appliance auf einer ebenen Oberfläche:

Der Sockel der Appliance verfügt an jeder Ecke über Befestigungslöcher, um die Appliance an jeder flachen Oberfläche in jedem Winkel und in jeder Ausrichtung zu befestigen:

1. Stellen Sie die Appliance so auf, dass die Rückwand in die Richtung zeigt, in der die Strom- und Kabelanschlüsse am leichtesten zugänglich sind.
2. Markieren Sie die Positionen der Schraubenlöcher auf der Oberfläche.
3. Bohren Sie Löcher für die Anker und setzen Sie die Anker in die Wand ein. Wenn Sie Holz-, Beton- oder Mauerwerkschrauben verwenden, bohren Sie die entsprechenden Löcher.
4. Befestigen Sie die Appliance mit den von Ihnen bereitgestellten Befestigungselementen an der Oberfläche.

## So befestigen Sie die DIN-Schienehalterung und die Montageplatte an der Appliance:

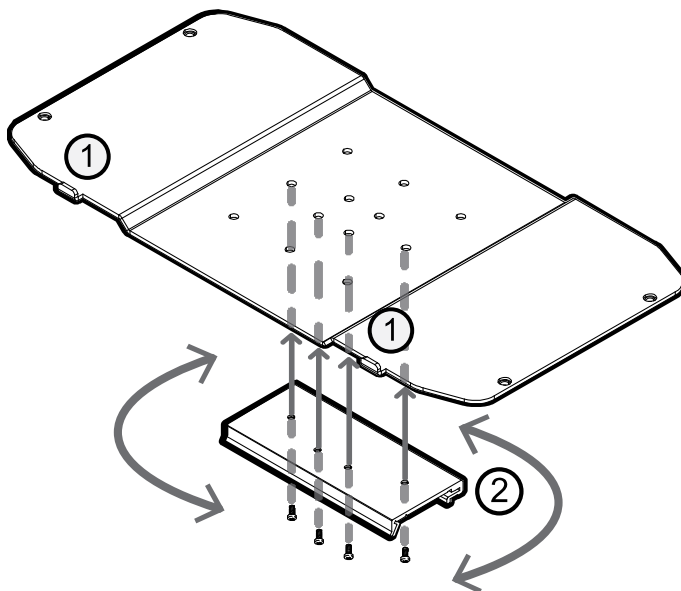
Eine Montageplatte, eine Halterung und Schrauben zum Befestigen der Halterung an der Platte sind im Lieferumfang enthalten. Die DIN-Schienehalterung wird mit dem gekrümmten Teil nach oben an einer DIN-Schiene befestigt. Die ACC ES Rugged Appliance mit 8 Ports hat auf der Rückseite Metalllaschen, die in passende Schlitzlöcher in der Montageplatte passen.

Die Halterung kann in einer von vier Positionen an der Montageplatte befestigt werden. Auf diese Weise können Sie die Appliance in verschiedenen Positionen an der Schiene befestigen, um den besten Zugang zur Vorder- und Rückseite zu erhalten:

- Vorne oder hinten nach oben oder unten
- Vorne oder hinten nach rechts oder links

**Tipp:** Wenn Sie die ACC ES Rugged Appliance mit 8 Ports an einer DIN-Schiene montieren, bestimmen Sie die korrekte Ausrichtung der Halterung zur Montageplatte und bringen Sie die Halterung an der Montageplatte an, bevor Sie die Montageplatte an der Appliance befestigen. Dadurch lässt sich leichter sicherstellen, dass die Appliance in einer optimalen Position installiert wird.

1. Bestimmen Sie die Position, an der die DIN-Schienehalterung an der Montageplatte befestigt werden soll.
2. Richten Sie die DIN-Schienehalterung an den vorgebohrten Gewindebohrungen in der richtigen Ausrichtung auf der Montageplatte aus und befestigen Sie sie mit den 4 (vier) Flachkopfschrauben in der Plastiktüte mit der Bezeichnung **DIN-Schiene Nr. 1**. Die Laschen auf der Rückseite der Appliance passen nur in die Schlitzlöcher auf einer Seite der Halterung.



① Kennzeichnet die Laschen auf der Montageplatte, die in die Schlitzlöcher auf der Rückseite der Appliance passen.

② Kennzeichnet die Oberkante der DIN-Halterung.

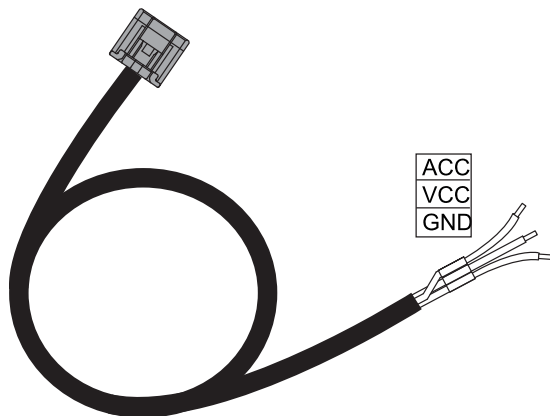
Bei der Beispielausrichtung wird die Appliance so auf die Halterung gesetzt, dass die Vorderseite der Appliance nach oben zeigt.



# Anschließen einer ACC ES Rugged Appliance mit 8 Ports an ein Netzteil

Die ACC ES Rugged Appliance mit 8 Ports kann mit dem mitgelieferten Netzkabel von jedem geeigneten 9–32-Volt-Gleichstromnetzteil mit 100 W (min.) gespeist werden.

Das mitgelieferte Netzkabel verfügt an einem Ende über einen Stecker, der in den Stromanschluss an der Rückseite der Appliance eingesteckt wird, und am hinteren Ende über drei Kabel mit der Bezeichnung ACC (Zubehör), VCC und GND.



Um eine dauerhafte Stromverbindung herzustellen (nicht geschaltet), schließen Sie sowohl das ACC- als auch das VCC-Kabel an die positive Seite der Stromquelle an. Schließen Sie das Erdungskabel an die Erdungsseite der Stromquelle an.

Verwenden Sie das ACC-Kabel, um eine Verbindung zu einem geschalteten Stromsignal herzustellen (z. B. zu einem Fahrzeugzubehörsignal in einem Fahrzeug). Das System wird eingeschaltet, wenn das ACC-Kabel an die positive Seite der Stromquelle angeschlossen wird. Das System wechselt in den Standby-Modus mit geringem Stromverbrauch, wenn das ACC-Kabel von der positiven Seite der Stromquelle getrennt wird.

# Erstmaliges Starten der ACC ES Rugged Appliance mit 8 Ports

Installieren Sie das ACC ES Rugged Appliance mit 8 Ports an einem Ort, der frei von Staub und Partikeln sowie Vibrationen ist und innerhalb des angegebenen Betriebstemperaturbereichs liegt. Andernfalls werden jegliche resultierenden Probleme nicht durch die Garantie gedeckt.

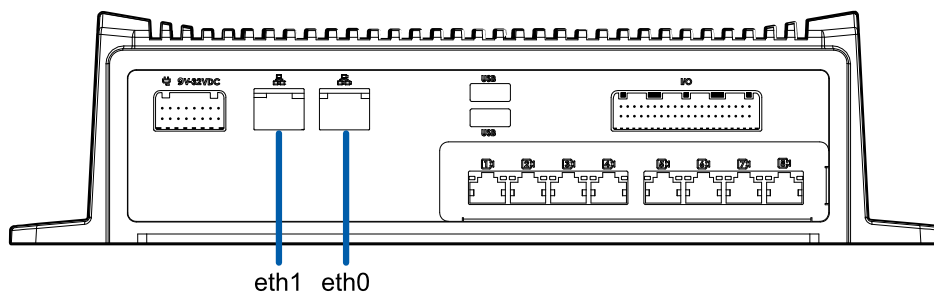
Sie müssen das Gerät zum ersten Mal konfigurieren, bevor Sie es mit Ihrem Sicherheitsnetzwerk verbinden.

**Wichtig:** Wenn statische IPs erforderlich sind, muss ein Laptop die IP-Adresse des Geräts manuell konfigurieren. Stellen Sie sicher, dass dem Laptop keine der folgenden IP-Adressen zugewiesen ist: 169.254.100.99 oder 169.254.100.100, und dass er eine IP-Subnetzmaske von 255.255.0.0 hat.

1. Schließen Sie das Gerät an die Stromversorgung an und warten Sie, bis es gestartet ist. Das Starten beim ersten Einschalten kann einige Minuten dauern.

Überprüfen Sie, dass die LED-Anzeigen der Appliance den korrekten Status anzeigen. Weitere Informationen finden Sie unter *LED-Anzeigen* auf Seite 33.

2. Wenn Sie das Gerät mit einer statischen IP-Adresse konfigurieren, verbinden Sie einen DHCP-fähigen Port an Ihrem konfigurierenden Laptop mit einem Ethernet-Kabel direkt mit dem *Kameranetzwerk-*Port (eth0) auf dem Gerät. Andernfalls schließen Sie das Gerät über den *Unternehmensnetzwerk--*Port (eth1) an das Unternehmensnetzwerk an.



3. Finden Sie auf dem angeschlossenen Laptop oder dem Netzwerkarbeitsplatz die Appliance. Verwenden Sie den Datei-Explorer auf einem Windows-Computer oder Finder® auf einem Macintosh-Computer.

Sie müssen nach einem Netzwerkgerät mit der Bezeichnung „VMA-RPA-RGD-8Px-<Seriennummer>“ suchen. Wenn Sie die Appliance nicht finden können, siehe *Fehlerbehebung* auf Seite 48.

4. Klicken Sie auf , um das Gerät in einem unterstützten Webbrowser zu öffnen. Eine Liste der unterstützten Webbrowser finden Sie unter *Systemanforderungen* auf Seite 10.



**Wichtig:** Das ACC ES Rugged Appliance mit 8 Ports ist mit einem selbstsignierten Zertifikat konfiguriert, das im Webbrowser eine Verbindungswarnung generiert.

5. Klicken Sie über alle Verbindungsmeldungen, die vom Webbrowser angezeigt werden, hinaus. Sie sehen zwei Warnmeldungen, die sich je nach Webbrowser geringfügig unterscheiden. Je nach Webbrowser:
  - Chrome – Klicken Sie auf **Erweitert** auf dem ersten Bildschirm und **Weiter mit <IP-Adresse> (unsicher)** auf dem zweiten Bildschirm.
  - Firefox – Klicken Sie auf **Erweitert** auf dem ersten Bildschirm und auf dem zweiten Bildschirm klicken Sie auf **Ausnahme hinzufügen**, aktivieren Sie **Diese Ausnahme dauerhaft speichern**, und klicken Sie auf **Sicherheitsabfrage bestätigen**.
6. Der Browser zeigt eine Sicherheitswarnung an, die Sie darüber informiert, dass die Verbindung zwischen der Webbenutzeroberfläche und dem Gerät nicht vertrauenswürdig ist, da das Gerät ein selbstsigniertes Webzertifikat verwendet. Dies wird erwartet und Sie können die Warnung ignorieren und zum ACC ES Admin Webbenutzeroberfläche fortfahren.

Die Sicherheitsstufe, die durch die mit dem Gerät mitgelieferten Zertifikate geboten wird, sollte für jede Organisation ausreichend sein, die keine Public Key Infrastructure (PKI) auf ihren internen Servern einsetzt.

**Wichtig:** Für Organisationen, die ihre eigene PKI bereitstellen, können die Zertifikate des Geräts über das ACC ES Admin Webbenutzeroberfläche verwaltet werden, nachdem das Gerät installiert und mit Strom versorgt wurde. Das standardmäßige selbstsignierte Webzertifikat kann ersetzt werden, signierte Zertifikate von Zertifizierungsstellen, die nicht mit dem Gerät geliefert werden, können hinzugefügt werden, und die signierten Zertifikate von Zertifizierungsstellen für öffentliche Server wie Google Mail, die mit dem Gerät geliefert werden, können deaktiviert werden. Weitere Informationen finden Sie unter *Verwaltung von Zertifikaten* auf Seite 35.

7. Wenn Sie durch das Webinterface aufgefordert werden, geben Sie ein neues Passwort für den Administrator-Benutzernamen ein.

Das Stärke-Messgerät misst die Komplexität Ihres Passworts: Rot ist zu einfach, Gelb ist ziemlich komplex und Grün ist komplex. Die Komplexität misst die Schwierigkeit, Ihr Passwort zu erkennen, und nicht, wie sicher Ihr Passwort ist. Ein komplexes Passwort wird empfohlen.

Die Seite wird aktualisiert und Sie werden aufgefordert, sich anzumelden.

8. Geben Sie `Administrator` als Benutzername und Ihr neues Passwort ein.

Das Dashboard-Bedienfeld des Webinterface wird angezeigt.

9. Legen Sie die Sprache für das Webinterface sowie einen benutzerfreundlichen Hostnamen und die Zeitzone fest. In der Navigationsleiste klicken Sie auf **Gerät**, um das Gerät-Bedienfeld zu öffnen. Im:
  - a. Allgemein-Bedienfeld wählen Sie Sprache aus der Dropdown-Liste.
  - b. Hostname -Bereich ersetzen Sie optional die Seriennummer der Appliance durch einen aussagekräftigen Hostnamen für die Appliance.
  - c. Zeit -Bedienfeld, geben Sie Zeitzone an und identifizieren Sie die Zeitquelle in der NTP-Dropdown- und Server-Liste.

Weitere Informationen finden Sie unter *Neustart des Geräts und Verwalten von Geräteeinstellungen* auf Seite 23.

10. Wählen Sie aus, wie die Appliance IP-Adressen vom Netzwerk bezieht. In der Navigationsleiste klicken Sie auf **Netzwerk**, um das Netzwerk-Bedienfeld zu öffnen. Wählen Sie für jeden verwendeten Netzwerkanschluss Automatisch oder geben Sie die Einstellungen manuell ein.

Weitere Informationen finden Sie unter *Verbinden des Geräts mit Benutzern und Kameras* auf Seite 26.

11. Wenn zum Konfigurieren des Geräts ein Laptop verwendet wurde:
  - a. Verbinden Sie ein Ethernetkabel von dem Gerät mit dem *Unternehmensnetzwerk*-Port.
  - b. Trennen Sie den Konfigurations-Laptop vom *Kameranetzwerk*-Port.
12. Schließen Sie die Kameras an die PoE-Anschlüsse an.

Weitere Informationen über das Webinterface finden Sie unter *Konfigurieren der Appliance* auf Seite 19

Nun können Sie die ACC ES Rugged Appliance mit 8 Ports mit einem ACC-Standort verbinden. Sie können dann das Gerät konfigurieren und Kameras mit der AvigilonControl Center Client-Software für den täglichen Betrieb einrichten. Weitere Informationen finden Sie unter *Verbinden mit der ACC-Software und ACS* auf Seite 31.

# Konfigurieren der Appliance

Der ACC ES Rugged Appliance mit 8 Ports kann über das ACC ES Admin Webbenutzeroberfläche konfiguriert werden, auf das von jedem kompatiblen Browser im Netzwerk zugegriffen werden kann. Mit dem ACC ES Admin Webbenutzeroberfläche können Sie die ACC ES Rugged Appliance mit 8 Ports-Servereinstellungen konfigurieren, die die Zeiterfassung des Systems bestimmen und die einen Neustart aus der Ferne bzw. eine Aktualisierung des Systems erlauben. Sie können außerdem die ACC Client-Software auf eine Workstation herunterladen, mit der Sie auf das ACC ES Admin Webbenutzeroberfläche zugreifen.

Beginnen Sie mit der Sicherung der Systemeinstellungen für den Rekorder, nachdem Sie ihn konfiguriert haben. Diese Einstellungen umfassen das Passwort ACC und die Einstellungen für die Kameraverbindungen. Weitere Informationen zum Sichern der Standort- und Serverkonfigurationen finden Sie im *Avigilon ACC Client-Benutzerhandbuch*.

In diesem Abschnitt wird der Begriff „Gerät“ zur Identifizierung der Appliance verwendet.

## ACC ES Admin Webbenutzeroberfläche starten

Sie können von einer Netzwerkarbeitsstation mit Netzwerkzugriff auf das Gerät auf das ACC ES Admin Webbenutzeroberfläche zugreifen.

Verwenden Sie beim ersten Zugriff auf das ACC ES Admin Webbenutzeroberfläche Ihres Geräts eine der folgenden Methoden:

- **So finden Sie das Gerät**

1. Öffnen Sie die Registerkarte Netzwerk im Datei-Explorer (Windows) oder im Finder (Macintosh), um das Gerät zu suchen.

Sie müssen nach einem Netzwerkgerät mit der Bezeichnung „VMA-RPA-RGD-8Px-<Seriennummer>“ suchen.

2. Klicken Sie mit der rechten Maustaste und wählen Sie **Gerätewebseite anzeigen**, um die Anmeldeseite des Geräts in Ihrem Standard-Webbrowser zu öffnen.

- **Mit der IP-Adresse oder dem Hostnamen**

1. Öffnen Sie einen Webbrowser von einem Netzwerkarbeitsplatz mit Netzwerkzugriff auf das Gerät.
2. Geben Sie die IP-Adresse oder den Hostnamen in den Webbrowser ein, um die Anmeldeseite des Geräts zu öffnen:

`https://<Device IP address >|<Device hostname>/`

Zum Beispiel: `https://169.254.100.100/` oder `https://my_AvigilonDevice/` , wobei `my_AvigilonDevice/` der im Bedienfeld Gerät konfigurierte Hostname ist.

**Hinweis:** Für den Fall, dass Sie die IP-Adresse oder den Hostnamen vergessen haben, die während des Installationsvorgangs konfiguriert wurden, wird diese Information in der ACC Client-Software auf der Einrichtung-Registerkarte des Servers aufgeführt.

**Tipp:** Setzen Sie ein Lesezeichen für die URL der Anmeldeseite für das Gerät.

### An- und Abmelden im ACC ES Admin Webbenutzeroberfläche:

1. Geben Sie den Benutzernamen und das Passwort für das ACC ES Admin Webbenutzeroberfläche ein, um sich anzumelden.


Der Benutzername ist immer `administrator`. Benutzen Sie das Passwort, das konfiguriert wurde, als Sie sich zum ersten Mal auf dem Gerät angemeldet haben. Weitere Informationen finden Sie unter *Erstmaliges Starten der ACC ES Rugged Appliance mit 8 Ports* auf Seite 16.

Der Benutzername ist immer `administrator`. Benutzen Sie das Passwort, das konfiguriert wurde, als Sie sich zum ersten Mal auf dem Gerät angemeldet haben. Weitere Informationen finden Sie unter *Erstmaliges Starten der ACC ES Rugged Appliance mit 8 Ports* auf Seite 16.

Die ACC ES Admin Webbenutzeroberfläche-Startseite wird in Ihrem Webbrowser angezeigt.

2. Klicken Sie auf das „Abmelden“-Symbol rechts im oberen Banner, um sich vom ACC ES Admin Webbenutzeroberfläche abzumelden.

Auf der ACC ES Admin Webbenutzeroberfläche-Startseite wird **Dashboard** in der seitlichen Navigationsleiste ausgewählt und die Dashboard-Statusfelder werden angezeigt:

- **ACC-Server**— Zeigt **Wird ausgeführt**, wenn die ACC-Server-Software in Betrieb ist, andernfalls wird **Angehalten** angezeigt. Das Bedienfeld enthält technische Informationen zum Gerät: Standortname, Servername, Server-ID, Serverversion, Softwareversion, Anzahl der verfügbaren Kamerakanäle und die maximale Anzahl der zulässigen ACC Client-Instanzen.
- **System**— Zeigt **Bereit** wenn das Gerät voll funktionsfähig ist und **Wird neu gestartet...** dann **Wird initialisiert...** wenn das Gerät neu gestartet wird. Der Bereich enthält technische Informationen zu Ihrem Gerät: Produktname, Teilenummer, Seriennummer und Firmware-Version.
- **Netzwerk**— Zeigt Informationen über die zwei Uplink-Ports auf dem Gerät an. Klicken Sie auf , um das [Netzwerk-Bedienfeld](#) zu öffnen. Siehe *Verbinden des Geräts mit Benutzern und Kameras* auf Seite 26.
- **PoE** — Zeigt Statusinformationen zu jedem PoE-Port an. Mit den Symbolen im Bedienfeld können Sie schnell erkennen, wie viele Ports verwendet werden, welchen Status und welche Geschwindigkeit sie haben und ob die Verbindung nach oben oder unten verläuft. Klicken Sie auf , um das [PoE-Bedienfeld zu öffnen](#). Siehe *Anzeigen des PoE Port-Status* auf der nächsten Seite.

Verwenden Sie die Menüoptionen unter Dienste und System in der Dashboard-Navigationsleiste, um auf alle anderen Web-Oberflächenfelder zuzugreifen.

- **Dienste** — Erweitern Sie **ACC** in der linken Seitenleiste, um auf Folgendes zu navigieren
  - Die Seite **Server** ist zur Steuerung des ACC-Servers auf dem Gerät bestimmt. Siehe *Verwalten von ACC Diensten und Speicher* auf der nächsten Seite
  - Die Seite **Protokolle** ist zum Anzeigen von ACC-Serverdienstprotokollen bestimmt. Siehe *Dienstprotokolle für den Support zur Verfügung stellen* auf Seite 23.
- **System** — Rufen Sie die fünf Optionen auf, um das Gerät zu konfigurieren und seinen Status anzuzeigen:
  - **Gerät.** Siehe:
    - *Neustart des Geräts und Verwalten von Geräteeinstellungen* auf Seite 23
    - *Aktualisieren der Firmware* auf Seite 38
    - *Verwaltung von Zertifikaten* auf Seite 35
  - **Speicher.** Siehe *Überwachen und Trennen der Speicher-SSD* auf Seite 25.
  - **Netzwerk.** Siehe *Verbinden des Geräts mit Benutzern und Kameras* auf Seite 26.
  - **PoE.** Siehe:
    - *Zuweisen eines PoE-Leistungsbudgets* auf Seite 27.
    - *Budgetierung der PoE-Leistung* auf Seite 34
  - **Protokolle.** Siehe *Bereitstellung von Geräteprotokollen für den Support* auf Seite 29

## Anzeigen des PoE Port-Status

Das Bedienfeld PoE zeigt den Status für jeden Port in der Spalte Status an. Die Statusmöglichkeiten sind:

Grün	Mit Strom versorgt	Ein PoE-Gerät ist am Port angeschlossen und funktioniert normal.
	Hoher Energieverbrauch	PoE+ ist eingeschaltet.
Grau	Verbindung getrennt	Es ist kein Gerät an den Port angeschlossen.
	Keine Stromversorgung	Die PoE-Port-Stromversorgung ist von der PoE-Seite im ACC ES Admin Webbenutzeroberfläche ausgeschaltet
Gelb	Überlastet	Ein PoE-Gerät ist am Port angeschlossen, erhält aber keinen Strom. Dieser Status tritt typischerweise auf, wenn ein Port überlastet ist oder das Gerät mehr Strom benötigt als geplant usw.
	Schwachstrom	Das Gerät erhält zu wenig Strom vom Port.
Rot	Fehler	Das Gerät ist in einem Störungszustand.

**Tipp:** Wenn eine Kamera vom Gerät getrennt und dann wieder angeschlossen wird, müssen Sie möglicherweise diese Seite aktualisieren, um den neuesten Status und die Budgetwerte anzuzeigen.

## Verwalten von ACC Diensten und Speicher

Auf dem **Server**-Bedienfeld benutzen Sie den:

- Allgemein-Bereich:

Um...	Gehen Sie so vor...
Schließen Sie erst alle Dienste, bevor Sie das Gerät abschalten.	Klicken Sie auf <b>Anhalten</b> .
Starten Sie alle Dienste, nachdem sie heruntergefahren wurden.	Klicken Sie auf <b>Starten</b> .
Formatieren Sie das Speicherlaufwerk.	Klicken Sie auf <b>Erneut initialisieren</b> , um alle Konfigurationen und aufgezeichneten Videodaten zu löschen.

- Speicherverwaltung-Bereich:

So können Benutzer Videos von diesem Gerät mit der ACC-Client-Software archivieren:

1. Klicken Sie auf **Aktiviert**.
2. Wählen Sie in der Dropdownliste Protocol (Protokoll) eine der folgenden Optionen aus:
  - **CIFS (CIFS)** — Gemeinsames Internet-Dateisystem. Die Netzwerkpfad weist in der Regel folgendes Format auf: `//<Hostname oder IP> / <Pfad>`
  - **NFS (NFS)** — Netzwerk-Dateisystem. Die Netzwerkpfad weist in der Regel folgendes Format auf: `<Hostname oder IP> : <Pfad>`
3. Geben Sie im Feld **Netzwerkpfad** den Pfad zum gewünschten Speicherort für archivierte Videos ein.
4. Wenn der Netzwerkpfad eine Authentifizierung erfordert, geben Sie die Anmeldeinformationen in die Felder Benutzername und Passwort ein.
5. Klicken Sie auf **Anwenden**.

- Service- und RTP-Port-Bereiche

Um die UDP- und TCP-Ports, die zur Kommunikation mit der Appliance dienen, zu ändern:

- Geben Sie im Bereich Dienstports den **Basis**-Wert ein, der für die HTTP-, HTTPS- und UDP-Ports verwendet werden soll, und klicken Sie auf **Anwenden**. Die Liste der Ports wird aktualisiert.
- Geben Sie im Bereich RTP-Ports den **Basis**-Wert ein, der für die UDP-Ports verwendet werden soll, und klicken Sie auf **Anwenden**. Der Bereich der für RTP verfügbaren Ports wird aktualisiert.

**Wichtig:** Diese Änderungen können erst nach einem Neustart des Systems wirksam werden. Lassen Sie einen Neustart zu, wenn Sie dazu aufgefordert werden.

## Dienstprotokolle für den Support zur Verfügung stellen

Verwenden Sie die Seite Protokolle, um Dienstprotokolle anzuzeigen. Die Protokolle werden in der Regel vom technischen Support von Avigilon angefordert, um ein Problem zu beheben.

Standardmäßig zeigt die Seite 100 Warnmeldungen aus den Protokollen an.

In der Regel unterstützt Sie der technische Support von Avigilon beim Zugriff auf und bei der Filterung der Protokolle in diesem Bereich, um die erforderlichen Protokolle zu isolieren. Anschließend kopieren Sie die Protokolle und fügen sie in eine Textdatei ein, speichern sie und senden sie an den technischen Support von Avigilon.

Sie können die Protokolle filtern, um die gewünschten Informationen anzuzeigen:

1. Wählen Sie in der Dropdownliste die Art des gewünschten Anwendungsprotokolls aus. Die Optionen lauten:
  - **Ausnahmeprotokolle**
  - **FCP-Protokolle**
  - **Serverprotokolle**
  - **WebEndpoint-Protokolle**
2. Wählen Sie in der Dropdownliste **Protokolle maximal** die Anzahl der Protokollmeldungen, die jedes Mal angezeigt werden sollen.
3. Geben Sie Text in das Feld **Filter** ein, um einen Filter auf die Protokollanzeigen anzuwenden.
4. Klicken Sie auf die Schaltfläche **Sync**, um die aktualisierten Protokolle anzuzeigen.

## Neustart des Geräts und Verwalten von Geräteeinstellungen

Auf dem Gerät-Bedienfeld benutzen Sie den:

- **Allgemein**-Bereich um:
  - **Neu starten** das Gerät vom ACC ES Admin Webbenutzeroberfläche. Sie können den Fortschritt des Geräts beim Neustart von der ACC ES Admin Webbenutzeroberfläche überwachen (Weitere Informationen finden Sie unter *ACC ES Admin Webbenutzeroberfläche starten* auf Seite 19).
  - Wählen Sie in der Dropdownliste eine **Sprache** für das ACC ES Admin Webbenutzeroberfläche aus.
- **Hostname**-Bereich, um ein neues **Hostname** einzugeben. Klicken Sie auf **Anwenden**, um die Änderungen vorzunehmen.

Der Standard-Hostname ist derselbe wie der Servername. Der Servername hat die Form *<Modell>-<Seriennummer>*

- **Passwort** -Bereich, um das Administratorpasswort zu ändern:

**Hinweis:** Sie können nur das Passwort auf dem ACC ES Admin Webbenutzeroberfläche ändern, nicht den Standard-Benutzernamen *Administrator*.

1. Um Ihr Passwort zu ändern, bestätigen Sie Ihre Identität, indem Sie Ihr aktuelles Passwort in das Feld **Altes Passwort** eingeben.
2. Geben Sie das neue Passwort im Feld **Neues Passwort** ein.
3. Geben Sie das neue Passwort erneut im Feld **Passwort bestätigen** ein.

**VORSICHT** — Sie verlieren Videoaufzeichnungen und Konfigurationsdaten, wenn Sie Ihr Passwort vergessen. Um das Administratorpasswort zurückzusetzen, müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen. Weitere Informationen zur Durchführung einer Werkswiederherstellung finden Sie unter *Werkseinstellungen wiederherstellen* auf Seite 42.

- **Zeit** -Bereich, um anzupassen, wie das Gerät die Zeit feststellt:
  - Wählen Sie in der Dropdownliste **Zeitzone** aus. Die Zeitzone, die Sie hier festlegen, wird von den in der ACC-Client-Software definierten Aufzeichnungs-Zeitplänen verwendet.
  - Wählen Sie im NTP-Feld, ob Sie die synchronisierte Zeit über einen Network Time Protocol (NTP)-Server (empfohlen) beibehalten möchten.

Wählen Sie:

- **DHCP**, um automatisch einen vorhandenen NTP-Server im Netzwerk zu verwenden.
- **Manuell**, um die Adresse des NTP-Servers in der Liste Server einzugeben. Steuerelemente zum Hinzufügen, Löschen und Neuordnen von Adressen in der Liste sind aktiviert.
- **Aus** wenn Sie keinen NTP-Server verwenden.



**Hinweis:** Der Standardsatz von NTP-Servern ist immer in der Server-Liste vorhanden. Die Standardliste kann nicht neu angeordnet oder gelöscht werden:

- 0.pool.ntp.org
- 1.pool.ntp.org
- 2.pool.ntp.org
- 3.pool.ntp.org

Klicken Sie auf **Anwenden**, um die Zeiteinstellungen zu speichern.

- **Firmware aktualisieren** -Bereich, um die neueste Version der Firmware auf Ihrem Gerät zu installieren oder die Firmware neu zu installieren, wenn sie beschädigt wird. Weitere Informationen finden Sie unter *Aktualisieren der Firmware* auf Seite 38.
- **Zertifikate**-Bereich zum Verwalten der vom ACC ES Admin Webbenutzeroberfläche und vom Gerät verwendeten Zertifikate. Weitere Informationen finden Sie unter *Verwaltung von Zertifikaten* auf Seite 35.




## Überwachen und Trennen der Speicher-SSD

Auf dem **Speicher**-Bedienfeld des ACC ES Rugged Appliance mit 8 Ports können Sie:

- Die Speicherkapazität und den Status der austauschbaren Speicher-SSD anzeigen.
- Den Status des Speicher-SSD auf Auswerfen setzen, bevor es zum Austausch aus der Appliance entfernt wird, falls es einmal ausfallen sollte.


**Wichtig:** Die Speicher-SSD muss durch eine SSD mit derselben Kapazität ersetzt werden (2TB für das VMA-RPA-8P2-Modell oder 4TB für das VMA-RPA-8P4-Modell).

Klicken Sie in der Navigationsleiste auf **Speicher**, um das Speicher-Bedienfeld zu öffnen. Sie können eine der folgenden Aktionen im Fensterbereich im Speicher-Bedienfeld ausführen:





Um...	Gehen Sie so vor...
Die Kapazität und den Status der SSD anzeigen.	Klicken Sie in der Navigationsleiste auf <b>Speicher</b> . Wenn das Gerät: <ul style="list-style-type: none"><li>• Ordnungsgemäß funktioniert Bereit und  angezeigt wird.</li><li>• Nicht richtig funktioniert Fehler und  angezeigt wird.</li></ul>
Details zur SSD anzeigen.	1. Klicken Sie auf das  oben rechts im Bereich, um den Bereich mit den Speicherdetails zu öffnen.


## Um...



## Gehen Sie so vor...


2. Klicken Sie auf , um Details zum Laufwerk anzuzeigen, einschließlich Modell- und Seriennummern.

Die SSD auswerfen.

1. Klicken Sie auf . Der Status ändert sich zu  und  ändert sich zu , was bedeutet, dass alle Dienste gestoppt wurden.

**Tipp:** Wenn Sie die SSD nicht entfernen möchten, klicken Sie auf , um die SSD erneut anzuschließen.

2. Sie können jetzt die SSD von der Appliance entfernen. Siehe *Ersetzen der Speicher-SSD* auf Seite 44.
3. Nachdem Sie die Ersatz-SSD im Rahmen installiert und wieder in die Appliance eingesetzt haben, ändert sich der Status auf . Nach Abschluss ändert sich der Status auf .

**Wichtig:** Wenn sich der Status auf  ändert, haben Sie eine inkompatible SSD eingelegt. Sie können erst fortfahren, wenn Sie eine SSD mit der gleichen Kapazität wie das ursprünglich werkseitig installierte Laufwerk einlegen.

## Verbinden des Geräts mit Benutzern und Kameras

Im Netzwerk-Bedienfeld können Sie die Netzwerkverbindungen des Geräts ändern. Zwei Netzwerkverbindungen werden unterstützt: eine für ein Unternehmensnetzwerk und eine für ein Kameranetzwerk.

**Hinweis:** Das Unternehmens- und das Kameranetzwerk müssen sich in unterschiedlichen IP-Subnetzen befinden.

Das Unternehmensnetzwerk ist das Netzwerk, das in der Regel Benutzern Zugriff auf das Gerät gewährt. Benutzer, die Videos mit der ACC Client-Software überwachen, würden dieses Netzwerk zur Verbindung mit dem Gerät verwenden.

**Wichtig:** Bevor Sie die Appliance als neuen ACC-Standort hinzufügen oder die Appliance mit einem bestehenden ACC-Standort zusammenführen, müssen Sie zunächst ihre IP-Adresse festlegen. Es wird dringend empfohlen, sich im gleichen IP-Subnetz wie die anderen Server am ACC-Standort zu befinden.

Das Kameranetzwerk ist ein geschlossenes Netzwerk, das in der Regel nur Kameras enthält. So wird die Interferenz mit der Videoaufzeichnung reduziert.

Wenn Sie ein ONVIF-Gerät mit dem Kameranetzwerk verbinden, konfigurieren Sie es so, dass die Appliance als Zeit- / NTP-Server verwendet wird, wenn auf der Appliance ACC 7.x oder höher ausgeführt wird.

Weitere Informationen über die Netzwerkverbindungen finden Sie unter *Unterstützte Netzwerkkonfigurationen* auf Seite 11.

Sie können im Netzwerk-Bedienfeld jeden der folgenden Schritte ausführen:

Um...	Gehen Sie so vor...
Legen Sie fest, wie das Gerät eine IP-Adresse für jedes Netzwerk erhält.	Aktivieren Sie im Bedienfeld Netzwerk in den einzelnen Bereichen das <b>Automatisch IP</b> , um automatisch verbundene Netzwerke zu erkennen (Standardeinstellung), oder deaktivieren Sie sie, um die Verbindungen manuell festzulegen. Geben Sie die entsprechenden Werte in die folgenden Felder ein, wenn Sie die Verbindungseinstellungen manuell eintragen: <ul style="list-style-type: none"><li>• <b>IP-Adresse</b></li><li>• <b>Subnetzmaske</b></li><li>• <b>Standardgateway</b></li></ul> Klicken Sie auf <b>Anwenden</b> , um Ihre Änderungen zu speichern.
Legen Sie fest, wie das Gerät eine benannte Adresse von einem DNS-Server erhält.	Aktivieren Sie <b>Automatisch DNS</b> , um verbundene DNS-Server automatisch zu erkennen (Standardeinstellung), oder deaktivieren Sie sie, um die DNS-Server manuell anzugeben. Steuerelemente zum Hinzufügen und Löschen von Adressen in der Liste und das Neuordnen von Adressen sind aktiviert, wenn <b>Automatisch DNS</b> deaktiviert ist.

## Zuweisen eines PoE-Leistungsbudgets

Verwenden Sie das **PoE**-Bedienfeld, um zu sehen, wie viel Strom den angeschlossenen Geräten zur Verfügung steht und von ihnen verbraucht wird. Die Standardeinstellung für alle Ports ist Auto. Diese Einstellung erkennt und budgetiert automatisch den Stromverbrauch des an den Port angeschlossenen Geräts. Für jeden Port können Sie diese Einstellung manuell vornehmen oder die Stromversorgung komplett ausschalten. Wenn Sie die Ausgangsleistung der Ports manuell anpassen möchten, müssen Sie ein PoE-Leistungsbudget berechnen, siehe *Budgetierung der PoE-Leistung* auf Seite 34.

**Tipp:** Wenn Sie einen PoE-Leistungsinjektor mit mittlerer Reichweite für Kameras verwenden, die Hochleistungs-PoE benötigen, sollten Sie diesen PoE-Port auf Aus setzen.

So öffnen Sie das PoE-Bedienfeld:

- Klicken Sie im PoEstatus-Bedienfeld auf der ACC ES Admin WebbenutzeroberflächeStartseite auf .
- Klicken Sie in der Dashboard-Navigationsleiste auf **PoE**.

#### Um...

Sehen Sie, wie viel Strom den angeschlossenen Geräten zur Verfügung steht und von ihnen verbraucht wird.

#### Gehen Sie so vor...

Sehen Sie sich die beiden Leisten oben im Bedienfeld an:

- Die Leiste **Budget** zeigt den Gesamtleistungsbedarf für alle an die PoE-Ports angeschlossenen Geräte an.
- Die Leiste **Verbrauch** zeigt die aktuell von allen angeschlossenen Geräten verwendete Stromstärke an.

Passen Sie die von jedem PoE-Port verbrauchten Strom an.

**Tipp:** Sie können die **Stromversorgung**-Leiste auch verwenden, um die Kamera ferngesteuert einzuschalten. Nach dem Einstellen der Stromversorgung auf Aus, warten Sie bis die Kamera abschaltet. Ändern Sie dann die Stromversorgung-Einstellung auf **Auto** oder **Manuell**.

**Tipp:** Geräte, die sowohl PoE als auch PoE+ (802.3at) unterstützen, können mit einem manuellen 15W-Budget in den Nicht-PoE+-Modus (802.3af) gezwungen werden.

Verwenden Sie die **Stromversorgung**-Leiste für jeden Port, um ein PoE-Leistungsbudget zu konfigurieren:

- Klicken Sie auf **Aus**, um die Stromversorgung für den Port zu deaktivieren. Wenn deaktiviert, gibt der Port keine Leistung mehr ab, kann aber als eine Standard-Netzwerk-Verbindung für ein beliebiges Gerät dienen.
- Klicken Sie auf **Auto**, um abhängig vom Betriebsmodus automatisch Strom an das angeschlossene Gerät zu senden.
- Klicken Sie auf **Manuell**, um einen Wert für das Leistungsbudget in Watt einzugeben. Stellen Sie sicher, dass das Budget mögliche Verlustleistung am Kabel einschließt.

Beachten Sie, dass Ihre Einstellungen nicht umgesetzt werden, bis Sie auf **Anwenden** klicken.

Nachdem Sie auf **Anwenden** geklickt haben, lassen Sie das System neu starten, wenn die folgende Meldung angezeigt wird:

*Beim Anwenden von Änderungen werden Geräte mit PoE-Stromversorgung u. U. aus- und wieder eingeschaltet.*

Nachdem die neuen Leistungseinstellungen übernommen wurden, aktualisiert das ACC ES Admin Webbenutzeroberfläche automatisch den Bildschirm und zeigt die aktualisierten Einstellungen an.

## Bereitstellung von Geräteprotokollen für den Support

Verwenden Sie das Systemprotokolle-Bedienfeld, um die Geräteprotokolle anzuzeigen. Die Protokolle werden in der Regel vom technischen Support von Avigilon angefordert, um ein Problem zu beheben.

Standardmäßig zeigt die Seite 100 Warnmeldungen aus den Protokollen an.

In der Regel unterstützt Sie der technische Support von Avigilon beim Zugriff auf und bei der Filterung der Protokolle in diesem Bereich, um die erforderlichen Protokolle zu isolieren. Anschließend kopieren Sie die Protokolle und fügen sie in eine Textdatei ein, speichern sie und senden sie an den technischen Support von Avigilon.

Sie können die Protokolle filtern, um die gewünschten Informationen anzuzeigen:

1. Wählen Sie in der Dropdownliste die Art des gewünschten Anwendungsprotokolls aus. Die Optionen lauten:
  - **Systemprotokolle**
  - **Startprotokolle**
  - **Webserverprotokolle**
2. Wählen Sie in der Dropdownliste **Protokolle maximal** die Anzahl der Protokollmeldungen, die jedes Mal angezeigt werden sollen.
3. Geben Sie Text in das Feld **Filter** ein, um einen Filter auf die Protokollanzeigen anzuwenden.
4. Klicken Sie auf die Schaltfläche **Sync**, um die aktualisierten Protokolle anzuzeigen.

# ACC-Client installieren und starten

Wenn Sie die erste Avigilon-Appliance in Ihrem Sicherheitsnetzwerk installieren, können Sie die ACC Client-Software auf einem Netzwerkarbeitsplatz oder auf dem Computer installieren, den Sie für den Zugriff auf das Webinterface verwenden. Andernfalls fügen Sie die Appliance als neuen Standort in Ihrem Sicherheitsnetzwerk hinzu oder fügen Sie sie mit Hilfe der ACC Client-Software auf einem Netzwerkarbeitsplatz in einen bestehenden Standort ein.

**Wichtig:** Bevor Sie die Appliance als neuen ACC-Standort hinzufügen oder die Appliance mit einem bestehenden ACC-Standort zusammenführen, müssen Sie zunächst ihre IP-Adresse festlegen. Es wird dringend empfohlen, sich im gleichen IP-Subnetz wie die anderen Server am ACC-Standort zu befinden.


Sie können die neueste Version der ACC Client-Software auf einem Netzwerkarbeitsplatz mit Netzwerkzugriff auf das Internet installieren:

1. Öffnen Sie einen Webbrowser von einem Netzwerkarbeitsplatz mit Netzwerkzugang zum Internet.
2. Laden Sie die ACC Client-Software kann von der Avigilon Webseite: [avigilon.com/support/software](http://avigilon.com/support/software) herunter. Klicken Sie sich durch die Installationssoftware, um die neueste Version der ACC Client-Software zu erhalten.


**Hinweis:** Wenn Sie zum ersten Mal auf die Webseite zugreifen, von der Sie die Software herunterladen, werden Sie aufgefordert, sich zu registrieren. Geben Sie alle erforderlichen Informationen ein und klicken Sie auf **Registrierung abschließen**. Ihre Registrierung wird automatisch akzeptiert und Sie werden zur Webseite weitergeleitet.

3. Installieren Sie die ACC-Client-Software auf einem Netzwerkarbeitsplatz mit Netzwerkzugriff zu dem Gerät.

So öffnen Sie die ACC Client-Software:

- Doppelklicken Sie auf das Desktop-Verknüpfungssymbol .
- Wählen Sie im Menü "Start" **Alle Programme** oder **Alle Apps > Avigilon > Avigilon Control Center Client**.

So schließen Sie die ACC Client-Software:

1. Klicken Sie oben rechts auf .
2. Klicken Sie auf **Ja**.

# Verbinden mit der ACC-Software und ACS

Sobald Sie Ihre -Appliance bereitgestellt haben, sollten Sie Ihre ACC-Software aktivieren und eine Verbindung zu Avigilon Cloud Services (ACS) herstellen.

## ACC-Software aktivieren und konfigurieren

- [Ersteinrichtung des ACC™-Systems und Workflow-Anleitung](#)
- [ACC 7 Help Center](#)

Ausdruckbare Ausgaben dieser Handbücher sind auf der Avigilon Webseite: [avigilon.com/support/software/](https://www.avigilon.com/support/software/) verfügbar.

## Verbinden mit Avigilon Cloud Services

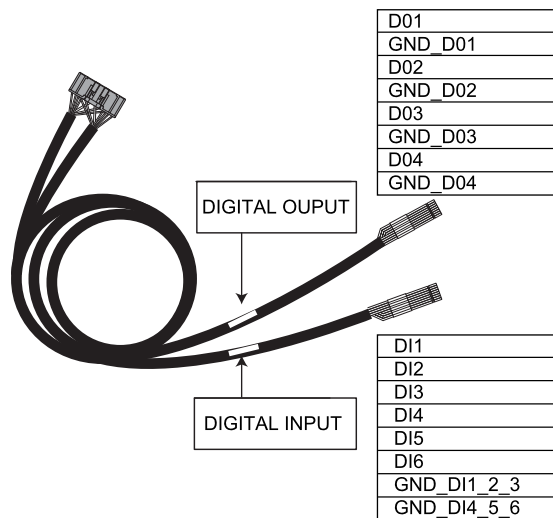
Nachdem Sie Ihre ACC-Software aktiviert haben, können Sie Ihren ACC-Standort kostenlos mit der Cloud verbinden und von den Möglichkeiten und Funktionen Gebrauch machen, die einen zentralen Zugriff über verteilte Systeme hinweg ermöglichen.

Um Ihren Standort mit den Avigilon Cloud Services zu verbinden, siehe [help.avigilon.com/cloud](https://help.avigilon.com/cloud).

Informationen zu den Cloud Services finden Sie unter [Avigilon Cloud Services Support](#).

# Anschließen an externe Geräte

Externe Geräte werden über das digitale E/A-Kabel, das in den digitalen E/A-Anschluss auf der Rückseite des Geräts eingesteckt ist, an der ACC ES Rugged Appliance mit 8 Ports angeschlossen. Details für die 8 gekennzeichneten Eingangsleitungen und die 8 gekennzeichneten Ausgangsleitungen sind unten gezeigt.



PIN	Funktion	Beschreibung
DI1	IN1	<b>Alarmeingänge</b> — Active-Low-Eingänge. Zum Aktivieren verbinden Sie den Eingang mit dem Erdungsstift (GND). Um zu deaktivieren, getrennt lassen.
DI2	IN2	
DI3	IN3	
DI4	IN4	
DI5	IN5	
DI6	IN6	
GND_DI1_2_3	Erdungsstift für die Eingänge 1, 2 und 3	
GND_DI4_5_6	Erdungsstift für die Eingänge 4, 5 und 6	
D01	AUS1	<b>Ausgänge</b> — Form-A-Trockenkontaktausgänge. Im aktivierten Zustand sind die Klemmen angeschlossen. Im deaktivierten Zustand sind die Klemmen getrennt.
GND_D01		
D02	OUT2	
GND_D02		
D03	OUT3	
GND_D03		
D04	OUT4	
GND_D04		








**Hinweis:** Kontakte sind normalerweise offen.

Die maximale Last beträgt 48 V, 0,3 A.



# LED-Anzeigen

Die folgende Liste beschreibt was die LEDs auf der ACC ES Rugged Appliance mit 8 Ports anzeigen.

		Symbole	LED-Status	Beschreibung
LEDs auf der Vorderseite	Status		Rot	Gerät ist eingeschaltet und läuft
			Gelb	Speicherlaufwerkaktivität
LEDs auf der Rückseite	PoE-Schalter		Links	Ein: Port liefert PoE-Stromversorgung
				Aus: Port liefert keine PoE-Stromversorgung
			Gelb	Blinkend: Der Port liefert keine PoE-Stromversorgung, aber die PoE-Kamera ist angeschlossen
			Rechts	An: Netzwerk-Link ist vorhanden
				Aus: Netzwerk-Link ist nicht vorhanden
			Grün	Blinkend: Netzwerkaktivität ist vorhanden
Uplink-Ports für Unternehmen und Kameras		Rechts	An: Netzwerk-Link ist vorhanden	
			Aus: Netzwerk-Link ist nicht vorhanden	
		Grün	Blinkend: Netzwerkaktivität ist vorhanden	

# Budgetierung der PoE-Leistung

Die PoE-Switch-Komponente im Avigilon ACC ES Rugged Appliance mit 8 Ports kann insgesamt 64 W Leistung an die angeschlossenen Geräte ausgeben. Jeder PoE-Port ist in der Lage, 16 W an Standard-PoE-Geräte und 30 W an PoE+-Geräte abzugeben. Dies bedeutet, dass das Gerät in der Regel bis zu 4 Standard-PoE-Geräte und bis zu 2 PoE+ Geräte unterstützen kann.

Fortgeschrittene Benutzer können das PoE-Leistungsbudget für jeden Port so anpassen, dass die benötigten Kameras konstant unterstützt werden.

Wenn Sie sich dafür entscheiden, das PoE-Budget an jedem Port manuell anzupassen, beachten Sie, dass Sie auch eine mögliche Verlustleistung im Kabel berücksichtigen müssen. Wenn die Höhe der Verlustleistung im Kabel nicht bekannt ist, verwenden Sie die folgenden Schätzungen:

- Wenn das Gerät weniger als oder gleich ( $\leq$ ) 16 W verwendet, ist mit einer Verlustleistung von 2,5 W zu rechnen.
- Wenn das Gerät mehr als ( $>$ ) 16 W verbraucht, ist mit einer Verlustleistung von 4,5 W zu rechnen.

Um das empfohlene Leistungsbudget für jeden Port zu berechnen, verwenden Sie die folgende Gleichung:

$$\text{Leistungsbudget} = \langle \text{Stromverbrauch der Kamera} \rangle + \langle \text{erwartete Verlustleistung des Kabels} \rangle$$

**Beispiel:** Verbinden Sie die folgenden 4 Kameras mit einem ACC ES Rugged Appliance mit 8 Ports:

2 x HD Dome-Kameras	$(9 \text{ W} + 2,5 \text{ W}) \times 2$	= 23 W
1 x HD PTZ-Kamera	$25,5 \text{ W} + 4,5 \text{ W}$	= 30 W
1 x HD Mikro-Dome	$4 \text{ W} + 2,5 \text{ W}$	= 6,5 W
<b>Insgesamt</b>		= 59,5 W

Die gesamte Leistungsaufnahme der 4 Kameras liegt innerhalb der Grenzen der PoE-Switch-Komponente.

**Hinweis:** Wenn Sie die benötigte Leistung für einen PoE-Port falsch berechnen, wird der gesamte PoE-Schalter möglicherweise heruntergefahren, wenn die Gesamtleistung 64 W übersteigt.

# Verwaltung von Zertifikaten

Vertrauenswürdige Zertifikate werden vom Gerät verwendet, um andere Server und Clients zu authentifizieren, zu denen eine Verbindung hergestellt werden muss, und um diese Verbindungen zu sichern. Avigilon bietet ein selbstsigniertes Webzertifikat zum Sichern der Verbindung zum ACC ES Admin Webbenutzeroberfläche und zum WebEndpoint-Dienst sowie eine Reihe signierter Zertifikate auf Systemebene von bekannten vertrauenswürdigen Zertifizierungsstellen, um sichere Verbindungen zu allen erforderlichen Servern sicherzustellen. Optional können Sie Ihre eigenen Zertifikate und Zertifizierungsstellen bereitstellen.

Die Sicherheitsstufe, die durch die mit dem Gerät mitgelieferten Zertifikate geboten wird, sollte für jede Organisation ausreichend sein, die keine Public Key Infrastructure (PKI) auf ihren internen Servern einsetzt.

Die Zertifikatverwaltungsfunktion auf der Appliance steuert nur das Appliance-Webzertifikat, das von ACC ES Admin Webbenutzeroberfläche und dem ACC WebEndpoint-Produkt verwendet wird. Innerhalb des ACC-Servers werden die durch diese Funktion konfigurierten Zertifizierungsstellen nur zum Überprüfen sicherer E-Mail-Server verwendet, die von den ACC-E-Mail- und Central Station Monitoring-Funktionen verwendet werden. ACC Server zu ACC Server- und ACC Server zu ACC Client-Verbindungen werden nicht mithilfe der Appliance-Zertifikatverwaltungsfunktion gesteuert oder validiert.

Wenn Ihre Organisation beispielsweise einen öffentlichen E-Mail-Server wie Google Mail verwendet und E-Mail-Benachrichtigungen ausgelöst werden, greift ACC auf den Google Mail-Server zu und erhält ein Zertifikat zur Identifizierung des Google Mail-Servers. Die ACC-Software überprüft das Zertifikat, indem sie bestätigt, dass die Zertifizierungsstelle, die das Google Mail-Zertifikat signiert hat, aus der Liste der bekannten vertrauenswürdigen Zertifizierungsstellen stammt und die Verbindung gesichert ist.

**Hinweis:** Die signierten Zertifikate, die mit dem Gerät geliefert werden, sind die gleichen wie die, die mit Mozillas Browser ausgeliefert werden, und sind öffentlich vom [Debian-Projekt](#) erhältlich. Mit den Zertifikaten können SSL-basierte Anwendungen die Authentizität von SSL-Verbindungen überprüfen. Avigilon kann weder bestätigen noch leugnen, ob die Zertifizierungsstellen, deren Zertifikate in dieser Appliance enthalten sind, in irgendeiner Weise auf Vertrauenswürdigkeit oder RFC 3647-Konformität geprüft wurden. Die volle Verantwortung für deren Bewertung liegt beim lokalen Systemadministrator.

Organisationen, die ihre eigenen PKI implementieren, können den Bereich Zertifikate des ACC ES Admin Webbenutzeroberfläche verwenden, um Zertifikate auf dem Gerät zu verwalten.

Zum Beispiel können Sie:

- Ersetzen Sie das standardmäßige selbstsignierte Webzertifikat durch das Zertifikat Ihrer eigenen Organisation.
- Dem Gerät Zertifizierungsstellen hinzufügen, z. B. interne Zertifizierungsstellen, die in Ihrer Organisation verwendet werden.
- Alle CA-Zertifikate auf Systemebene deaktivieren (und aktivieren).

# Ersetzen des Webzertifikat

Verwalten Sie das Webzertifikat des Geräts von der Registerkarte Webzertifikat im Bereich Zertifikate. Der ACC ES Admin Webbenutzeroberfläche- und WebEndpoint-Dienst verwenden dieses Zertifikat, um sich bei Geräten zu authentifizieren, die eine Verbindung zu ihnen herstellen. Es kann immer nur ein Webzertifikat aktiv sein.

Sie können das Standard- Webzertifikat durch ein benutzerdefiniertes Zertifikat ersetzen.

**Wichtig:** Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen (auch als Werksreset bezeichnet), müssen Sie Ihr benutzerdefiniertes Zertifikat neu laden.

Das Erhalten eines neuen Webzertifikat erfolgt in drei Schritten:

1. Senden Sie dem von Ihrer Organisation verwendeten Zertifikatsaussteller ein Anforderung der Zertifikatsignierung (CSR), und der Aussteller sendet Ihnen eine neue Zertifikatdatei und eine private Schlüsseldatei zurück (normalerweise per E-Mail). Sie können eine CSR auf der Registerkarte Webzertifikat oder mithilfe der bevorzugten Methode des Zertifikatsausstellers generieren, wenn diese die CSR von der ACC ES Admin Webbenutzeroberfläche nicht akzeptieren:
  - a. Öffnen Sie die Web-Benutzeroberfläche, klicken Sie in der Navigationsleiste auf Gerät und scrollen Sie nach unten zum Bereich Zertifikate.
  - b. Klicken Sie auf der Registerkarte Webzertifikat auf Anforderung der Zertifikatsignierung.
  - c. Füllen Sie das Standard-CSR-Formular mit den Informationen aus, die von der von Ihnen verwendeten PKI definiert wurden, und klicken Sie auf Generieren.  
  
Die CSR-Datei generate.csr wird in Ihrem Download-Ordner gespeichert.
  - d. Senden Sie die Datei an den Zertifikatsaussteller Ihrer Organisation.

**Tipp:** Wenn der Zertifikatsaussteller die CSR nicht akzeptiert, verwenden Sie die bevorzugte Methode des Zertifikatsausstellers, um die CSR zu generieren.

2. Nachdem Sie die CRT-Datei mit dem neuen Zertifikat vom Zertifikatsaussteller erhalten haben, speichern Sie sie an einem Speicherort, auf den das Gerät zugreifen kann.

3. Laden Sie das neue Zertifikat auf das Gerät hoch:
  - a. Öffnen Sie die Web-Benutzeroberfläche, klicken Sie in der Navigationsleiste auf Gerät und scrollen Sie nach unten zum Bereich Zertifikate.
  - b. Klicken Sie auf der Registerkarte Webzertifikat auf Hochladen.
  - c. Geben Sie im Dialogfeld Webzertifikat hochladen einen Namen für das Zertifikat ein, klicken Sie auf und navigieren Sie zur CRT-Datei oder ziehen Sie sie per Drag & Drop in den Bereich Drop '.crt' certificate (pem) file here or click to upload.
    - Wenn die Zertifikatdatei mit der zuletzt aus der ACC ES Admin Webbenutzeroberfläche generierten CSR-Datei erstellt wurde, ist Hochladen aktiviert.
    - Klicken Sie andernfalls auf und navigieren Sie zur .key-Datei oder ziehen Sie sie per Drag & Drop in den Bereich Drop '.key' private key (pem) file here or click to upload. Hochladen ist aktiviert.
  - d. Klicken Sie auf Hochladen.
4. Klicken Sie auf der Registerkarte Webzertifikat auf den Namen des hochgeladenen Zertifikats, um es zu aktivieren. Dadurch wird auch das vorherige Zertifikat deaktiviert.

**Hinweis:** Wenn die Zertifikatdatei (.crt) mit einer CSR erstellt wurde, die von der bevorzugten Methode des Zertifikatausstellers generiert wurde (oder nicht mit der neuesten CSR-Datei auf dem Gerät generiert wurde), wiederholen Sie diesen Schritt, um die private Schlüsseldatei hochzuladen.

## Laden Sie ein vertrauenswürdigen CA-Zertifikat hoch

Verwalten Sie signierte Zertifikate von internen Zertifizierungsstellen, die auf den internen Servern Ihres Unternehmens bereitgestellt werden, auf der Registerkarte Benutzerzertifizierungsstellen des Zertifikate.

Beispielsweise kann ein interner E-Mail-Server in einer Organisation, die eine eigene PKI bereitstellt, der ACC-Software beim Versuch, auf den Mailserver zuzugreifen, ein von einer Zertifizierungsstelle signiertes Zertifikat bereitstellen, das nicht zu den bekannten vertrauenswürdigen Zertifizierungsstellen gehört. Das Zertifikat kann nur überprüft werden, wenn ein von dieser Zertifizierungsstelle signiertes Zertifikat auf die Registerkarte Benutzerzertifizierungsstellen des Bereichs Zertifikate hochgeladen wurde.

Wenn Sie ein signiertes Zertifikat von einer Zertifizierungsstelle hochladen müssen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Web-Benutzeroberfläche, klicken Sie in der Navigationsleiste auf Gerät und scrollen Sie nach unten zum Bereich Zertifikate.
2. Klicken Sie auf die Registerkarte Benutzerzertifizierungsstellen.
3. Klicken Sie auf Hochladen.
4. Geben Sie im Dialogfeld Benutzerzertifizierungsstelle hochladen einen Namen für das Zertifikat ein und klicken oder ziehen Sie es per Drag & Drop, um die Datei hochzuladen. Sie können jeweils nur eine Datei hochladen.

# Aktualisieren der Firmware

Sie können die Firmware aktualisieren, indem Sie das ACC ES Admin Webbenutzeroberfläche verwenden.

**Hinweis:** Sie können die Firmware auch von einem mit dem Gerät verbundenen ACC Client aktualisieren. Sie können über die Vorgehensweise zum Aktualisieren von Servern an einem Standort in den Hilfedateien nachlesen, die mit dem ACC-Client bereitgestellt werden.

Aktualisieren Sie die Firmware, um sicherzustellen, dass die Appliance mit der neuesten Software läuft, um von veralteter Software zu aktualisieren oder um beschädigte Firmware zu ersetzen. Wenn Sie die Firmware aktualisieren, bleiben alle Ihre aktuellen Einstellungen und alle aufgezeichneten Videos erhalten.

Um die Firmware zu aktualisieren oder erneut zu installieren, laden Sie die neueste Version der Firmware-Datei (. fp .) von der Avigilon-Webseite: [partners.avigilon.com](https://partners.avigilon.com) herunter und:

1. Wenn Sie während der Verwendung des ACC ES Admin Webbenutzeroberfläche über Ihren Webbrowser auf das Internet zugreifen können, navigieren Sie im Dashboard zum Info-Bedienfeld und klicken Sie auf **Firmware-Updates**.
2. Speichern Sie die Datei an einem Speicherort, auf den das ACC ES Admin Webbenutzeroberfläche zugreifen kann.

Um die Firmware vom ACC ES Admin Webbenutzeroberfläche aus zu aktualisieren:

1. Navigieren Sie zum Gerätebedienfeld.
2. Scrollen Sie bei Bedarf, um den Firmware aktualisieren-Bereich anzuzeigen;
3. Verwenden Sie eine der folgenden Methoden:
  - Drag-and-Drop
    1. Navigieren Sie mit Windows Explorer zum Speicherort der heruntergeladenen Firmware-Datei.
    2. Klicken Sie auf die Datei im Explorer-Fenster und ziehen Sie sie über den **FP-Datei hierher ziehen oder klicken, um hochzuladen**-Bereich.
  - Klicken Sie zum Hochladen darauf
    1. Klicken Sie auf den **FP-Datei hierher ziehen oder klicken, um hochzuladen**-Bereich. Das Dialogfeld „Windows Öffnen“ wird angezeigt.
    2. Navigieren Sie mit Windows Explorer zum Speicherort der heruntergeladenen Firmware-Datei.
    3. Klicken Sie im Dialogfeld „Öffnen“ auf die Datei und anschließend auf **Öffnen**.
4. Klicken Sie auf **OK**, um zu bestätigen, dass Sie fortfahren möchten. Eine Fortschrittsanzeige für den Upload wird angezeigt. Warten Sie, bis die Datei hochgeladen und überprüft wurde. Nachdem die Datei überprüft wurde, wird das Gerät neu gestartet. Die Meldung Verbindung mit

Webbenutzeroberfläche unterbrochen erscheint während des Neustarts des Geräts. Dieser Vorgang kann einige Minuten dauern. Nach dem Neustart des Geräts wird die Verbindung zum ACC ES Admin Webbenutzeroberfläche in Ihrem Webbrowser wiederhergestellt.

Sie können ein laufendes Firmware-Upgrade nur während der Upload- und Verifizierungsphase abbrechen. Klicken Sie auf **Upload abbrechen**, bevor die Datei hochgeladen wurde.

**Hinweis:** Tritt während des Uploads oder der Aktualisierung ein Fehler auf oder wenn die Firmware beschädigt wurde, werden Sie dazu aufgefordert, die Datei zu entfernen.

# Verwendung der Software-Reset-Taste

Wenn die ACC ES Rugged Appliance mit 8 Ports auf einen Systemfehler stößt und Sie ihn nicht von der Stromquelle trennen oder die Appliance einschalten können, verwenden Sie die Reset-Taste, während die Appliance noch eingeschaltet ist, um sie neu zu starten.

**Hinweis:** Die Rücksetzfunktion setzt auch die Kameraverbindungen zurück, so dass Sie während des Zurücksetzens alle aufgezeichneten Videos verlieren. Während des Zurücksetzens zeichnet die Appliance nicht auf. Aufgezeichnete Videos gehen jedoch nicht verloren.

Die Reset-Taste befindet sich hinter dem verriegelten Bedienfeld an der Vorderseite der ACC ES Rugged Appliance mit 8 Ports:

So setzen Sie die Appliance zurück:

1. Entriegeln und öffnen Sie die Vorderseite mit dem mitgelieferten Schlüssel.

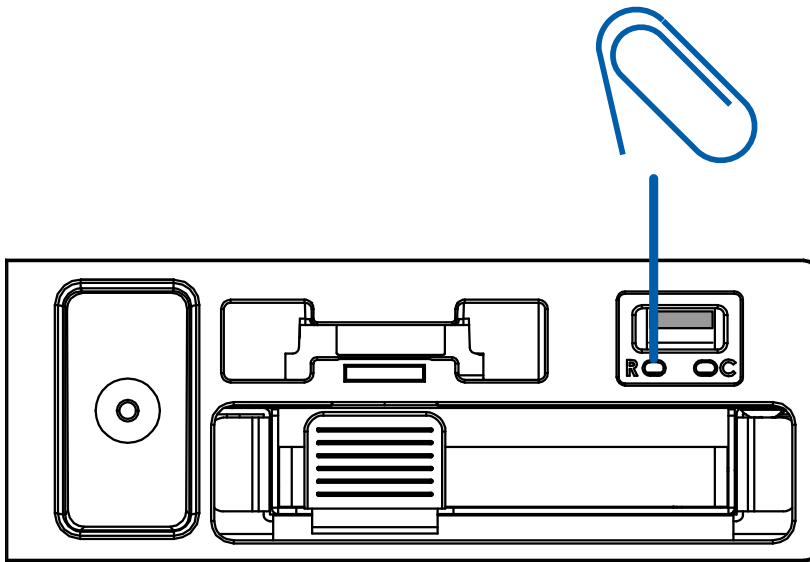
**Tipp:** Drehen Sie den Schlüssel um 180 Grad gegen den Uhrzeigersinn, um die Vorderseite zu entriegeln. Die Vorderseite fällt ab und wird mit einem Gurt am Gerät befestigt.


2. Nachdem Sie den Reset-Schalter am Gerät gefunden haben, verwenden Sie eine gerade Büroklammer oder ein ähnliches Werkzeug und drücken Sie den Reset-Schalter vorsichtig und lassen Sie ihn wieder los.



Wenden Sie keine übermäßige Kraft an. Ein zu tiefes Einführen des Werkzeugs führt zur Beschädigung des Geräts und zur Erlöschung der Garantie.





3. Stellen Sie sicher, dass die Appliance vollständig neu gestartet und die Aufzeichnung fortgesetzt wurde:
  - a. Rufen Sie die ACC ES Admin Webbenutzeroberfläche-Anmeldeseite auf und melden Sie sich an. Weitere Informationen finden Sie unter *ACC ES Admin Webbenutzeroberfläche starten* auf Seite 19.
  - b. Überprüfen Sie auf dem Speicherbereich der Webinterface-Startseite, ob der Status  ist.

# Werkseinstellungen wiederherstellen

Wenn die ACC Server-Software nicht mehr wie erwartet funktioniert, oder wenn Sie Ihr Administratorpasswort vergessen haben, können Sie die ACC ES Rugged Appliance mit 8 Ports auf die werkseitigen Standardeinstellungen zurücksetzen. Ein USB-Speicherlaufwerk ist erforderlich, um den Wiederherstellungsprozess abzuschließen.

**Hinweis:** Bei der Wiederherstellung der werkseitigen Standardeinstellungen werden alle Konfigurationseinstellungen gelöscht, einschließlich aller benutzerdefinierten Zertifikate, die Sie installiert haben, sowie aufgezeichnete Videos. Nachdem die werkseitigen Standardeinstellungen wiederhergestellt wurden, können Sie die letzte Systemsicherung wiederherstellen, bevor die Funktionsprobleme aufgetreten sind. Möglicherweise müssen Sie auch das benutzerdefinierte Zertifikat neu laden und die ACC Server-Software auf die neueste Version aktualisieren.

Wenn die Appliance Teil eines zusammengelegten Standorts oder einer Familienkonfiguration von übergeordneten und untergeordneten Standorten ist, gibt es zusätzliche Schritte, die Sie in der ACC Client-Software ausführen müssen und die in diesem Verfahren angegeben sind.

1. Bereiten Sie das USB-Speicherlaufwerk vor. Es muss:
  - a. FAT32-formatiert sein.
  - b. Eine Datei beliebiger Größe mit dem Namen `factory_restore` enthalten.
2. Stecken Sie das USB-Speicherlaufwerk in einen der USB-Ports.
3. Wenn die Appliance Teil eines zusammengelegten Standorts oder einer Familienkonfiguration von übergeordneten und untergeordneten Standorten ist:
  - a. Entfernen Sie sie vor dem Zurücksetzen von dem Standort.
  - b. Wenn die Appliance nicht Teil eines zusammengelegten Standorts ist, deaktivieren Sie die Lizenzen.
4. Schalten Sie die ACC ES Rugged Appliance mit 8 Ports aus und wieder ein. Sie können:
  - Trennen Sie die Appliance vom Stromnetz und schließen Sie es wieder an.
  - Setzen Sie die Appliance zurück (siehe *Verwendung der Software-Reset-Taste* auf Seite 40)
  - Starten Sie die Appliance über das Geräte-Bedienfeld der Web-Benutzerschnittstelle neu (siehe *Neustart des Geräts und Verwalten von Geräteeinstellungen* auf Seite 23)
5. Sobald die Datei `factory_restore` beim erneuten Einschalten der Appliance erkannt wird, werden die aktuellen Einstellungen und Daten gelöscht, das ursprüngliche Firmware-Image der Fabrik wiederhergestellt und die ACC ES Rugged Appliance mit 8 Ports neu gestartet.
6. Starten Sie nach dem Neustart der ACC ES Rugged Appliance mit 8 Ports die Webbenutzeroberfläche und stellen Sie sicher, dass die werkseitigen Standardeinstellungen wiederhergestellt wurden.

7. Entfernen Sie das USB-Speicherlaufwerk.

**Wichtig:** Wenn Sie das USB-Speicherlaufwerk nach dem Wiederherstellen der werkseitigen Standardeinstellungen nicht entfernen, wird der Wiederherstellungsvorgang erneut ausgeführt.

8. Aktualisieren Sie gegebenenfalls die Firmware der Appliance.
9. Wenn die Appliance Teil eines Standort-Clusters oder einer Familienkonfiguration von übergeordneten und untergeordneten Standorten ist:
  - a. Greifen Sie auf die WebUI zu und geben Sie die richtige IP-Adresse über die Web-UI erneut ein. Es wird dringend empfohlen, sich im gleichen IP-Subnetz wie die anderen Server des ACC-Standorts zu befinden.
  - b. Wenn die Appliance nicht Teil eines zusammengelegten Standorts ist, aktivieren Sie seine Lizenzen.
  - c. Fügen Sie die Appliance wieder mit dem Standort oder der Standortfamilie zusammen oder schließen Sie sie wieder an.

# Ersetzen der Speicher-SSD

Sie können das Speicher-SSD des ausgefallenen oder noch funktionierenden ACC ES Rugged Appliance mit 8 Ports austauschen. Es kann ohne Ausschalten der Appliance entfernt und ersetzt werden. Sie befindet sich in einem Fach hinter der verriegelten Vorderseite der Appliance. Das Fach wird in die Appliance hinein- und herausgeschoben.

**Wichtig:** Die Speicher-SSD muss durch eine SSD mit derselben Kapazität ersetzt werden (2TB für das VMA-RPA-8P2-Modell oder 4TB für das VMA-RPA-8P4-Modell).

Die Systemeinstellungen für die ACC-Software (einschließlich des ACC-Passworts und der Einstellungen für die Kameraverbindungen) sowie die Regeln für die selbstlernende Videoanalyse, etwaige Aufnahmelizenzen und aufgezeichnete Videos werden auf der Wechseldatenträger-SSD der ACC ES Rugged Appliance mit 8 Ports gespeichert. Wenn eine Speicher-SSD ausfällt, können keine dieser Daten vom ausgefallenen Laufwerk abgerufen werden.

Das Web-UI-Administratorpasswort, die IP-Adresse der Appliance und die NTP-Konfigurationseinstellungen werden nicht auf der SSD gespeichert und gehen nicht verloren.

**Tipp:** Beginnen Sie mit der regelmäßigen Sicherung der Systemeinstellungen für die Appliance, nachdem Sie sie konfiguriert haben, damit sie wiederhergestellt werden können, falls Sie das Speicher-SSD einmal austauschen müssen.

Unabhängig davon, ob eine ausgefallene oder eine funktionierende SSD ersetzt wird, sind einige Ausfallzeiten erforderlich. Die gesamte Aufzeichnung wird gestoppt, sobald die SSD im ausgeworfenen Zustand ist, und kann erst gestartet werden, wenn ein Backup der vorherigen Einstellungen wiederhergestellt oder die ACC ES Rugged Appliance mit 8 Ports neu konfiguriert wird, als ob sie neu installiert wäre, und die ACC- und Aufzeichnungslizenzen wieder aktiviert werden.

**Bevor** ein Speicher-SSD ersetzt wird, müssen Sie die Aufzeichnungslizenzen deaktivieren, die dem ACC ES Rugged Appliance mit 8 Ports hinzugefügt wurde.

**Nachdem** die SSD ersetzt wurde:

- Reaktivieren Sie die Lizenzen.
- Stellen Sie die ACC-Systemeinstellungen aus einer Sicherung der Standorteinstellungen wieder her.


**Tipp:** Es wird empfohlen, die Systemeinstellungen wiederherzustellen, bevor Sie die Firmware auf der Appliance aktualisieren, wenn eine neuere Version der Firmware für die Appliance verfügbar ist.




- Aktualisieren Sie auf die neueste Version der Firmware, falls eine solche verfügbar ist
- Die Regeln für Videoaufnahmen und Videoanalysen beginnen wie bei einer neu installierten Appliance von vorne.

Um ein Speicher-SSD zu ersetzen, verwenden Sie das folgende Verfahren:

1. Deaktivieren Sie alle mit der ACC ES Rugged Appliance mit 8 Ports verknüpften Lizenzen. Weitere Informationen zum Deaktivieren von Standortlizenzen finden Sie in der ACC Hilfe oder im *Avigilon ACC Client-Benutzerhandbuch*.
2. Initiieren Sie den Auswurfstatus für die SSD:

**Wichtig:** Bevor Sie die SSD physisch von der Appliance trennen und entfernen können, müssen Sie den Auswurfstatus im Speicherbereich der Startseite des Webinterfaces initiieren.

- a. Melden Sie sich bei der ACC ES Admin Webbenutzeroberfläche an. Weitere Informationen finden Sie unter *ACC ES Admin Webbenutzeroberfläche starten* auf Seite 19.
- b. Klicken Sie in der Navigationsleiste auf **Speicher**. Weitere Informationen finden Sie unter *Überwachen und Trennen der Speicher-SSD* auf Seite 25.
- c. Klicken Sie auf der Startseite des Webinterfaces im Bereich Speicher auf .

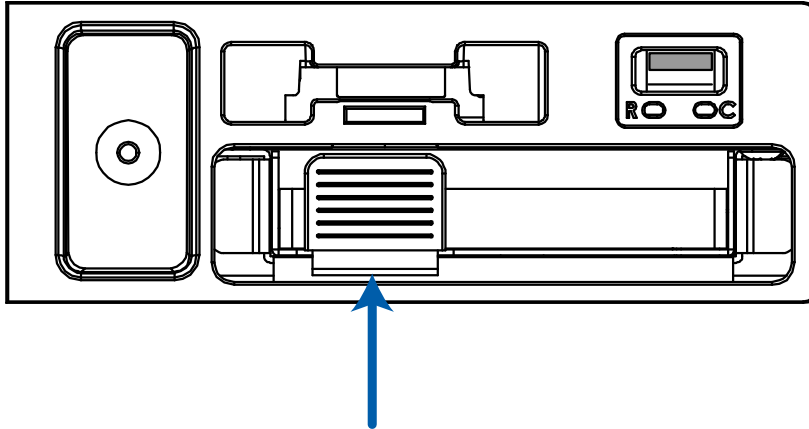
Der Status ändert sich zu  und  ändert sich zu , was bedeutet, dass alle Dienste gestoppt wurden.

**Hinweis:** Alle Aufzeichnungs- und Softwaredienste auf der Appliance werden gestoppt, wenn eine funktionierende Speicher-SSD ausgeworfen wird. Die Aufzeichnung wird nach dem Neustart der Softwaredienste fortgesetzt, wenn dieselbe Speicher-SSD erneut in die Appliance eingesetzt wird.

3. Entriegeln und öffnen Sie die Vorderseite mit dem mitgelieferten Schlüssel.


**Tipp:** Drehen Sie den Schlüssel um 180 Grad gegen den Uhrzeigersinn, um die Vorderseite zu entriegeln. Die Vorderseite fällt ab und wird mit einem Gurt am Gerät befestigt.

4. Suchen Sie die blaue Aufreißlasche des SSD-Fachs.



5. Entfernen der SSD:

- a. Ziehen Sie das Fach mit dem Zeigefinger hinter der blauen Lasche mit etwas Kraft aus der Appliance. Durch physisches Öffnen des Fachs wird die SSD von der Appliance getrennt.

**Wichtig:** Warten Sie ungefähr 10 Sekunden, bis sich der Status auf  ändert. Dies zeigt an, dass die Appliance das Entfernen der SSD erkannt hat, bevor Sie fortfahren.

- b. Heben Sie das Fach aus der Schiebeschublade.
- c. Entfernen Sie die vier Schrauben, mit denen die SSD am Fach befestigt ist. Bewahren Sie sie sicher auf, um die Ersatz-SSD wieder anzuschließen.
- d. Entfernen Sie die SSD aus dem Fach.

Der Status der SSD im Bereich Speicher auf der Startseite des Webinterfaces bleibt , während die SSD entfernt wird.

6. Einsetzen der SSD:

- a. Legen Sie die SSD in das Fach.
- b. Befestigen Sie die Ersatz-SSD am Fach.  
Verwenden Sie die vier Schrauben, die nach dem Entfernen der Original-SSD aufbewahrt wurden.
- c. Legen Sie das Fach auf die Schiebeschublade.
- d. Drücken Sie die blaue Lasche nach innen, bis Sie ein leises Klicken hören, während die SSD eine physische Verbindung zur Appliance herstellt.

Der Status des SSD im Bereich Speicher auf der Startseite des Webinterfaces ändert sich auf .

Wenn die SSD physisch wieder verbunden wird, ändert sich der Status auf .

7. Stellen Sie die jüngste Sicherung der ACC-Systemeinstellungen wieder her oder konfigurieren Sie die ACC ES Rugged Appliance mit 8 Ports so, als wäre sie neu installiert. Weitere Informationen zum Sichern der ACC-Systemeinstellungen finden Sie im *AvigilonACC Client-Benutzerhandbuch*
8. Installieren Sie die neueste Version der Appliance-Firmware, wenn eine neuere Version verfügbar ist. Weitere Informationen finden Sie unter *Aktualisieren der Firmware* auf Seite 38.
9. Aktivieren Sie alle Lizenzen, die auf dem ACC ES Rugged Appliance mit 8 Ports verwendet werden. Weitere Informationen zum Aktivieren von Standortlizenzen finden Sie in der ACC Hilfe oder im *Avigilon ACC Client-Benutzerhandbuch*.

**Wichtig:** Wenn Sie die Lizenzen nicht reaktivieren können, wenden Sie sich an den Avigilon Technischen Support unter [avigilon.com/contact](https://www.avigilon.com/contact).

# Fehlerbehebung

## Das Gerät kann nicht erkannt werden

Wenn Sie das Gerät während der Hardwareinstallation mit dem Datei-Explorer (Windows) oder Finder (Macintosh) nicht finden können und es mit Ihrem Netzwerk verbunden ist, versuchen Sie Folgendes:

- Greifen Sie über Ihren Webbrowser auf die Appliance mit der URL `https://VMA-RPA-RGD-8Px<serial number>` zu
- Verwenden Sie das Address Resolution Protocol (ARP), um die IP-Adresse des Geräts festzustellen:
  1. Suchen und notieren Sie die MAC-Adresse (MAC), die auf dem Seriennummernschild angegeben ist, als Referenz.
  2. Öffnen Sie ein Eingabeaufforderungsfenster und geben Sie den folgenden Befehl ein:

```
arp -a
```
  3. Scrollen Sie durch die Rückmeldung und suchen Sie nach der IP-Adresse, die der MAC-Adresse entspricht.
- Finden Sie die der DHCP-zugewiesenen IP-Adresse in der ACC Client-Software:
  1. Laden Sie die ACC-Client-Software auf den Konfigurations-Laptop herunter, dann installieren und öffnen Sie sie. Weitere Informationen finden Sie unter *ACC-Client installieren und starten* auf Seite 30.

**Hinweis:** Der Benutzername und das Passwort für das Webinterface unterscheidet sich von dem Administratorbenutzernamen und -passwort für den ACC-Server.

3. Zeigen Sie die Registerkarte Server Einrichtung an.
4. Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse mit diesem Format ein:

```
https://<IP-Adresse>
```

## Netzwerkconfiguration

Der ACC ES Rugged Appliance mit 8 Ports bezieht standardmäßig eine IP-Adresse im Netzwerk über DHCP. Wenn Sie ACC ES Rugged Appliance mit 8 Ports für die Verwendung einer statischen IP-Adresse oder einer bestimmten Netzwerkkonfiguration einrichten müssen, finden Sie weitere Informationen dazu unter *Verbinden des Geräts mit Benutzern und Kameras* auf Seite 26.



## Systemzustand überprüfen

Sie können den Zustand der Systemkomponenten in der Standortintegrität Client-Software ACC überprüfen. Weitere Informationen finden Sie unter [Standortzustand](#) im *ACC Client-Benutzerhandbuch*.

## Weitere Informationen

Weitere Produktdokumentationen finden Sie bei Avigilon unter [avigilon.com](http://avigilon.com).

### Technischer Support

Um Kontakt mit dem Avigilon Technischen Support aufzunehmen, besuchen Sie uns unter [avigilon.com/contact-us](http://avigilon.com/contact-us).

### Upgrades

Software- und Firmware-Upgrades werden zum Download angeboten, sobald sie verfügbar sind. Suchen Sie nach verfügbaren Upgrades auf: <http://avigilon.com/support-and-downloads/>.

### Feedback

Wir schätzen Ihr Feedback. Senden Sie Kommentare zu unseren Produkten und Dienstleistungen an [feedback@avigilon.com](mailto:feedback@avigilon.com).

## Beschränkte Garantie und Technischer Support

Avigilon Garantiebestimmungen für dieses Produkt werden unter [avigilon.com/warranty](http://avigilon.com/warranty) bereitgestellt.

Wenden Sie sich zur Inanspruchnahme von Garantieleistungen und technischem Support an den technischen Support von Avigilon: [avigilon.com/contact-us/](http://avigilon.com/contact-us/).