

Avigilon Control Center™ und Access Control Manager™ - Vereinheitlichungsanleitung

Für ACC™ Softwareversion 7.14.4 und ACM™ physische oder
virtuelle Version 6.22

© 2018 - 2022, Avigilon Corporation. Alle Rechte vorbehalten. AVIGILON, das AVIGILON-Logo, AVIGILON CONTROL CENTER, ACC, AVIGILON APPEARANCE SEARCH, HDSM, ACCESS CONTROL MANAGER und ACM sind Marken der Avigilon Corporation. Intel und Intel Core sind Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern. 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.

Dieses Dokument wurde anhand von zur Zeit der Veröffentlichung verfügbaren Produktbeschreibungen und Spezifikationen kompiliert und veröffentlicht. Die Inhalte dieses Dokuments und die dargestellten technischen Daten der Produkte können ohne Vorankündigung geändert werden. Avigilon Corporation behält sich das Recht vor, alle diese Änderungen ohne Vorankündigung vorzunehmen. Weder die Avigilon Corporation noch eines ihrer angeschlossenen Unternehmen: (1) garantiert die Vollständigkeit und Genauigkeit der in diesem Dokument enthaltenen Informationen; und (2) ist nicht verantwortlich für die Verwendung von oder auf den Verlass auf die Informationen. Die Avigilon Corporation ist nicht verantwortlich für eventuelle Verluste oder Schäden (einschließlich Folgeschäden), die durch das Vertrauen auf die hierin enthaltenen Informationen entstehen.

Avigilon Corporation
avigilon.com

PDF-ACC7ACM-U-G

Überarbeitung: 2 - DE

05.04.2022

Inhaltsverzeichnis

Einführung	4
Systemanforderungen	4
Avigilon-zertifizierte Lösung	4
ACC-Client-Softwareanforderungen	5
Anforderungen an ACC-Server-Software und Workstation	5
Vereinigungsempfehlungen für ACC und ACM	6
ACM™ und ACC™-Konfiguration	7
Konfigurieren der ACM-Appliance	7
Herstellen einer Verbindung zwischen der ACM-Appliance und einem ACC-Standort	10
Konfigurieren von ACM-Funktionen in ACC	11
Importieren von ACM-Rollen	11
Verknüpfen von Türen mit Kameras	12
Hinzufügen einer Verknüpfung	12
Bearbeiten und Löschen einer Verknüpfung	12
Hinzufügen von Regeln	12
Hinzufügen einer Webseite	13
Überwachen von Türen	14
Türzutritt gewähren	14
Identitätsüberprüfung	14
Identitätssuche	15
Ergebnisse der Identitätssuche	15
Verfeinern von Ergebnissen	15
Speichern von Ergebnissen	16
Durchsuchen der ACM-Appliance im ACC-Client	17
Beschreibung der Regelereignisse und Aktionen	18
Regel-Ereignisse	18
Regelaktionen	20
Regelbedingungen	22
Weitere Informationen	23

Einführung

Die Avigilon Control Center (ACC)-Software kann mit der Access Control Manager (ACM)-Appliance kombiniert werden, um eine verbesserte Sicherheit und Überwachung für Ihr Unternehmen zu bieten.

In diesem Dokument wird beschrieben, wie Sie Ihre ACM-Appliance und Ihre ACC-Software so konfigurieren, dass sie nahtlos interagieren. Sobald Ihre ACM-Appliance, Rollen und Identitäten mit der ACC-Software verbunden sind, können Sie Regeln für die Zugangskontrollereignisse erstellen, Türzugang gewähren und Identitätsprüfungen von ACC durchführen. Sie können Videos, die mit ACM Bedienfelder, Zusatzbedienfelder und Eingaben verbunden sind, als Lesezeichen speichern, exportieren und archivieren.

Systemanforderungen

Für die beste Leistung und volle Funktionalität verwenden Sie die neuesten Versionen der ACC-Client- und Server-Software und des ACM-Systems.

Um auf die ACM-Appliance zugreifen zu können, benötigen Sie:

- Eine Internetverbindung.
- Einen Webbrowser.

Avigilon-zertifizierte Lösung

- Einzelne physische oder virtuelle ACM-Instanz
- 2 Monitor oder 4 Monitor professioneller Hochleistungs-Arbeitsplatz zur Fernüberwachung
 - ACC-Clientsoftware bereits vorinstalliert.
 - Unterstützt Hochauflösungsmonitore.
 - Umfasst die Adapter und Zubehör für eine schnelle Installation.
 - Inklusive Avigilon-Garantie und Support.
- Server — NVR Premium, Standard oder Value
 - Optimiert für Überwachungsanwendungen in einer 24/7/365-Umgebung.
 - ACC -Software ist vorinstalliert, konfiguriert und für eine optimale Systemkompatibilität erweitert.
 - Zertifiziert für die Avigilon-Überwachungsumgebung — ACC-Software, LPR-, Web Endpoint-, Analyse-, HDSM™- und 1-30 MP-Kameras.
 - Hoher Durchsatz von bis zu 1800 Mbit/s.
 - Dokumentierte Netzwerkarchitektur für eine Vielzahl von Anwendungen.
 - Avigilon Garantie und Support inklusive.
 - Zugriff auf das Avigilon-System Design Tool (SDT) zur Berechnung der Speicheranforderungen.

- Arbeitsplätze – HD Video-Appliance oder NVR-Arbeitsplatz
 - Vorinstalliert und konfiguriert mit ACC-Videomanagementsoftware.
 - Hochleistungsfähige Aufnahmekapazität.
 - Unterstützt Hochauflösungsmonitore.
 - Durchsatz von bis zu 400 Mbit/s.
 - Avigilon Garantie und Support inklusive.
 - Zugriff auf Avigilon SDT zum Berechnen des Speicherbedarfs.

ACC-Client-Softwareanforderungen

Systemanforderung	Mindestanforderungen	Empfohlene Anforderungen
Bildschirm-Auflösung	1280 x 1024	1920 x 1200
BETRIEBSSYSTEM*	Windows 8.1 (64-Bit) oder Windows 10 (64-Bit) mit Microsoft .NET 4.6.2	Windows 10 (64-Bit) mit Microsoft .NET 4.6.2
CPU	Intel Dual-Core-CPU (2,0 GHz)	Intel Celeron®-CPU der 8. Generation oder höher
System-RAM	4 GB DDR3	8 GB DDR4
Videokarte	PCI Express®, DirectX 10.0 kompatibel mit 256 MB RAM	NVIDIA® Quadro® P620
Netzwerkkarte	1 Gbit/s	1 Gbit/s
Festplattenspeicher	500 MB freier Festplattenspeicher	500 MB freier Festplattenspeicher

Anforderungen an ACC-Server-Software und Workstation

ACC Server-Software

Systemanforderung	Mindestens	Empfohlen
BETRIEBSSYSTEM*	Windows Server 2012 R2 / 2016 / 2019, Windows 8.1 (64-bit) oder Windows 10 (64-bit)	Windows Server 2016
Prozessor	x86 64-bit (Dual-Core, 1,9 GHz)	Intel® Xeon® E5 v3 (6 Kerne, 1,9 GHz)
Speicher	4 GB DDR3	16 GB DDR4
Speicher	SATA-II 7200 RPM Enterprise Class	SATA-III 7200 RPM Enterprise Class

ACC Server-Workstation

Systemanforderung	Mindestens	Empfohlen
BETRIEBSSYSTEM*	Windows 8.1 (64-Bit) oder Windows 10 (64-Bit)	Windows 10 (64-Bit)

Systemanforderung	Mindestens	Empfohlen
Prozessor	Intel Quad-Core (2,0 GHz)	Intel Celeron®-CPU der 8. Generation oder höher
Speicher	4 GB DDR3	8 GB DDR4
Video	PCI Express®, DirectX 10.0 kompatibel mit 256 MB RAM	NVIDIA® Quadro P620
Speicher	SATA-II 7200 RPM	SATA-III 7200 RPM

* Führen Sie ein Windows-Update aus, bevor Sie die ACC-Software starten.

Vereinigungsempfehlungen für ACC und ACM

- ACC Software-Version 7.14.4 oder höher (ein Standort)
ACC Installation auf einem eigenen Rechner. Zum Beispiel sollten ACC und der SALTO ProAccess SPACE Server nicht auf demselben Rechner installiert werden.
- Physische oder virtuelle ACM-Version 6.22.0 oder höher (eine Instanz)

Hinweis: Neu hinzugefügte ACM Identitäten sind in ACC bis zu 1 Stunde nach dem Hinzufügen nicht verfügbar (wenn die Replizierung stattfindet).

ACM™ und ACC™-Konfiguration

Hinweis: Derzeit werden ACM und ACC-Failover-Systeme nicht unterstützt, wenn eine ACM-Appliance mit einem ACC-Standort verbunden ist.

Um die ACM-Appliance mit dem ACC-Standort zu verbinden, muss Folgendes von einem Administrator durchgeführt werden:

1. Die ACM-Appliance konfigurieren.
2. Die ACM-Appliance mit dem ACC-Standort verbinden.
3. ACM-Funktionen in der ACC-Software konfigurieren.

Jeder Prozess wird nachfolgend beschrieben.

Konfigurieren der ACM-Appliance

Bevor eine ACM-Appliance zu Ihrem ACC-Standort hinzugefügt werden kann, sind mehrere Konfigurationsschritte in der ACM-Appliance erforderlich.

Weitere Informationen zu den folgenden Einstellungen finden Sie in den ACM-Hilfedateien.

Hinweis: Wenn Sie eine ACM-Appliance (Version 5.10.10 SR1 oder höher) verwenden, wurden bereits eine ACC Administrator-Delegierung und -Rolle erstellt. Überprüfen Sie, ob die Delegierung über alle in Schritt 1 aufgeführten Rechte verfügt und dass die Rolle wie in Schritt 3 beschrieben eingerichtet ist.

1. Erstellen Sie eine Delegierung für die Integration in die ACC-Software. Diese Delegierung muss über die folgenden Rechte verfügen:
 - Appliance-Liste
 - Liste der Delegierungen
 - Türen – Gewähren
 - Türen-Liste
 - Liste der Identitäten
 - Identitätenanmeldung – Remote
 - Identitätenfoto – Darstellen
 - Eingabeauflistung
 - Bedienfelder-Liste
 - Liste der Partitionen

- Liste der Rollen
- Zusatzbedienfelder-Liste
- Systemzusammenfassung – Auflistung
- REST Appliance-Statusanzeige
- REST Türen abrufen
- REST Identitäten abrufen
- REST Identität abrufen
- REST Eingaben abrufen
- REST Bedienfelder abrufen
- REST Rechtegruppen abrufen
- REST Rollen abrufen
- REST Zusatzbedienfelder abrufen

Hinweis: Delegierungen, die mit "REST" beginnen, sind nur für den internen Gebrauch von Motorola Solutions bestimmt.

2. Wenn zusätzliche Rechte erforderlich sind, z. B. die Partitionenrechte, weil Ihre ACM-Installation partitioniert ist und Sie möchten, dass der ACC-Bediener auf Türen in den Partitionen zugreift, müssen Sie diese Rechte dieser Delegierung hinzufügen oder erstellen Sie eine neue Delegierung mit den Rechten, die der vorkonfigurierten **ACC Administrator**-Delegierung zugewiesen sind.
3. Erstellen Sie eine Weiterleitungsgruppe, um Ereignisse zu definieren, die von der ACM-Appliance an die ACC-Software gesendet werden.
 - a. Geben Sie Folgendes für die Gruppe an:
 - **Zeitplan:** 24 Stunden aktiv
 - **Zeitplanqualifizierer:** Appliance
 - Das Kontrollkästchen **Installiert** muss aktiviert werden
 - b. Fügen Sie die folgenden Ereignistypen zur Weiterleitungsgruppe hinzu:
 - Offengehaltene Tür
 - Aufgebrochene Tür
 - Einbruch
 - Ungültige Anmeldeinformationen
 - Wartung
 - System
 - Manipulation
 - Gültige Anmeldeinformationen
4. Erstellen Sie eine Rolle, mit der die ACC-Software mit der ACM-Appliance kommunizieren kann:

- a. Behalten Sie den Standardwert (Keine) für das **übergeordnete Element** bei.
- b. Behalten Sie den Standardwert (das aktuelle Datum) für das **Anfangsdatum** bei.
- c. Geben Sie im Feld **Enddatum** ein entsprechendes Datum ein, an dem diese Rolle ablaufen soll. Standardmäßig funktioniert die Rolle ein Jahr nach dem Erstellungsdatum nicht mehr.
- d. Aktivieren Sie das Kontrollkästchen **Installiert** und klicken Sie auf **Speichern**.

Zusätzliche Registerkarten werden angezeigt.

- e. Weisen Sie auf der Registerkarte **Delegieren** der Rolle nur die Delegierung zu, die in den vorherigen Schritten erstellt wurde.
 - f. Weisen Sie auf der Registerkarte **Weiterleiten** nur die Weiterleitungsgruppe zu, die in den vorherigen Schritten erstellt wurde.
5. Wenn Sie Active Directory-Identitäten in die ACM-Appliance oder in die ACC-Software importieren, konfigurieren Sie eine LDAP-Zusammenarbeit (Lightweight Directory Access Protocol). Konfigurieren Sie für die Active Directory-Remoteauthentifizierung die Remoteauthentifizierung von externen Domänen.
 6. Erstellen Sie eine dedizierte Identität für die Interaktion mit der ACC-Software.

Hinweis: Um die Sicherheit der Verbindung zwischen der ACM-Appliance und dem ACC-System zu schützen, sollte die dedizierte Identität nur die in diesem Verfahren beschriebenen Berechtigungen haben. Bediener sollten keinen Zugriff auf dieses Konto haben.

- Weisen Sie der Identität einen **Nachnamen, Login** und ein **Passwort** zu. Deaktivieren Sie das Kontrollkästchen **Passwortänderung erzwingen**.
- Das Passwort sollte die Mindestanforderungen an die Passwortstärke Ihres ACC-Standorts erfüllen.

Die Passwortstärke wird dadurch definiert, wie einfach es für einen nicht autorisierten Benutzer zu erraten ist. Es wird dringend empfohlen, dass Sie ein Passwort auswählen, das eine Reihe von Wörtern enthält, die für Sie leicht zu merken sind, aber für andere schwierig zu erraten.

- Geben Sie auf der Registerkarte **Rollen** der Identität nur die Rolle ein, die im vorherigen Schritt angelegt wurde.
7. Wenn Ihre ACM-Appliance Partitionen verwendet, fügen Sie die Identität als Mitglied der Partitionen hinzu, auf die sie vom ACC-Client zugreifen müssen.
 8. Konfigurieren Sie die ACM-Appliance so, dass der gleiche NTP-Zeitserver wie der ACC-Server verwendet wird.

Bei Windows-Systemen bezieht der ACC-Server seine Zeit vom Betriebssystem. Für Hardened OS Appliances von Avigilon kann der NTP-Zeitserver über die Webschnittstelle des Geräts konfiguriert werden.

- a. Klicken Sie in der oberen rechten Ecke auf das Zahnradsymbol, um das Menü Einrichten & Einstellungen zu öffnen, und wählen Sie **Appliance**.
- b. Geben Sie im Feld **Zeitserver** die IP-Adresse des Zeitserver ein.

Sobald diese Einstellungen angewendet wurden, können Sie sich über den ACC-Client mit der ACM-Appliance verbinden.



Herstellen einer Verbindung zwischen der ACM-Appliance und einem ACC-Standort

Verbinden Sie eine ACM-Appliance mit Ihrem ACC-Standort und Sie können durch die Appliance gesteuerte Türen mit von der ACC-Software gesteuerten Kameras verknüpfen. Nachdem Türen und Kameras verbunden sind, können Sie Regeln konfigurieren, die von Türen in der ACC-Software ausgelöst werden.

Hinweis:

Stellen Sie sicher, dass Sie Folgendes haben, bevor Sie beginnen.

- Den Hostnamen oder die IP-Adresse der ACM-Appliance.
- Die ACM-Portnummer unterscheidet sich vom Standardport (443).
- Der Benutzernamen und das Kennwort für die Identität, die geschaffen wurde, um die ACM-Appliance zur ACC-Software hinzuzufügen.

1. Klicken Sie im Menü Neue Aufgabe  auf **Standort-Setup**.
2. Klicken Sie auf .
3. Geben Sie die erforderlichen Anmeldedaten ein.
4. Klicken Sie auf **OK**.

Bestätigen Sie, dass die aufgeführte SHA-256-Fingerabdruck-ID identisch ist. Die Fingerabdruckinformationen werden normalerweise auf der Seite Appliance: Bearbeitung auf der Registerkarte SSL-Zertifikat aufgelistet.

5. Wenn die Fingerabdrücke identisch sind, klicken Sie auf **Vertrauen**.

Wenn sie nicht übereinstimmen, wenden Sie sich an Ihren Systemadministrator.

Die ACM-Appliance ist jetzt unter dem Standort als **AC** Hostname auf der Registerkarte Einrichtung gelistet.

Konfigurieren von ACM-Funktionen in ACC



Importieren von ACM-Rollen

Wichtig: Benutzernamen in der ACC-Software und ACM-Appliance müssen eindeutig sein. Doppelte Namen werden nicht importiert.

Hinweis:

- Durch das Importieren von ACM-Rollen auf einem Standort werden alle Active Directory-Benutzer in der ACC-Software deaktiviert.
- Wenn Ihre ACM-Appliance partitioniert ist, stellen Sie sicher, dass Identitäten Mitglieder der entsprechenden Partitionen sind, damit sie auf die Vereinheitlichungsfunktionen im ACC-Client zugreifen können.

Importieren Sie Rollen aus der ACM-Appliance, um Benutzern Zugriff auf Kameras und Türen zu gewähren. Wenn Sie eine Rolle importieren, importieren Sie auch die Identitäten, die der Rolle zugeordnet sind. Nur Identitäten mit einem Benutzernamen und Passwort in der ACM-Appliance werden importiert.

1. Klicken Sie im Menü Neue Aufgabe  auf **Standort-Setup**.
2. Klicken Sie auf den Standortnamen und dann auf **Nutzer und Gruppen** .
3. Wählen Sie auf der Registerkarte Externes Verzeichnis die Option **Avigilon Access Control Manager** aus der Dropdownliste.
4. Klicken Sie auf **Gruppe hinzufügen**.
5. Wählen Sie eine vorhandene Gruppe aus, die Sie als Vorlage verwenden möchten, und klicken Sie dann auf **OK**. Sie können die Berechtigungen für die Gruppe später bearbeiten.
6. Wählen Sie alle Rollen aus, die Sie importieren möchten.

Sie können die Suchleiste verwenden, um bestimmte Rollen zu finden.

7. Klicken Sie auf **OK**, um die Rollen hinzuzufügen.

Nach dem Import werden Rollen automatisch der Externes Verzeichnis-Liste und der Gruppen-Liste hinzugefügt. Alle der Rolle zugewiesenen Identitäten werden in die Liste Nutzer importiert.

Importierte Rollen können für Ränge, Funktionsberechtigungen und Gerätezugriffsrechte für die importierte Rolle bearbeitet werden. Sie können keine ACC-Benutzer einer ACM-Rolle aus der ACC Client-Software zuweisen.

Importierte Identitäten können nun zu jeder bestehenden Gruppe hinzugefügt werden – zusätzlich zu der Rolle, mit der sie importiert wurden.



Importierte Identitätsinformationen (einschließlich Anmeldeinformationen) werden über die ACM-Appliance verwaltet.

Weitere Informationen zum Verwalten von Gruppen finden Sie in den ACC-Client-Hilfedateien.

Verknüpfen von Türen mit Kameras

Türen, die installiert und mit installierten Bedienfeldern oder Zusatzbedienfeldern verbunden sind, können mit einer beliebigen Anzahl von Kameras an Ihrem Standort verknüpft werden. Sobald eine Verknüpfung erstellt wurde, können autorisierte Benutzer Türen und Identitäten überwachen sowie Regeln in der ACC-Software konfigurieren.

Hinzufügen einer Verknüpfung



1. Klicken Sie im Menü Neue Aufgabe  auf **Standort-Setup**.
2. Wählen Sie die ACM-Appliance aus und klicken Sie auf .
3. Klicken Sie auf **Verknüpfung erstellen**.
4. Aktivieren Sie in der Dropdown-Liste **Eine Tür auswählen** das Kontrollkästchen neben einer Tür.

Hinweis: Die verfügbaren Türen hängen von Ihren Berechtigungen in der ACM-Appliance ab.

5. Aktivieren Sie in der Dropdown-Liste **Mindestens eine Kamera auswählen** das Kontrollkästchen neben allen Kameras, die Sie mit der Tür verknüpfen möchten.
6. Klicken Sie auf **OK**.

Bearbeiten und Löschen einer Verknüpfung


Sie können die Kameras ändern, die mit einer Tür verknüpft sind.

1. Klicken Sie im Menü Neue Aufgabe  auf **Standort-Setup**.
2. Wählen Sie die ACM-Appliance aus und klicken Sie auf .
3. Wählen Sie eine Verknüpfung und klicken Sie auf **Verknüpfung bearbeiten** oder **Verknüpfung löschen**.
4. Klicken Sie auf **OK**.

Hinzufügen von Regeln

Sie können in der ACC-Software Regeln erstellen, die durch ACM-Appliance-Ereignisse ausgelöst werden. Diese Ereignisse können Versuche des Türzutritts und Ausweisleser beinhalten und Live-Video auslösen, das sofort auf allen Bildschirmen des Benutzers angezeigt wird.


Eine Liste der ACM-Regeln, Aktionen und Bedingungen finden Sie unter *Beschreibung der Regelereignisse und Aktionen* auf Seite 18.

1. Klicken Sie im Menü Neue Aufgabe  auf **Standort-Setup**.

2. Klicken Sie auf  und dann auf .

3. Wählen Sie alle Ereignisse aus, die die Regel auslösen sollen.

Wenn in der Regelbeschreibung ein blau unterstrichener Text vorhanden ist, klicken Sie auf den Text, um das Ereignis näher zu definieren.

Klicken Sie nach dem Definieren des Auslöseereignisses auf .

4. Wählen Sie alle Aktionen aus, die als Reaktion auf die Auslöser ausgeführt werden.

Wenn in der Regelbeschreibung ein blau unterstrichener Text vorhanden ist, klicken Sie auf den Text, um die Aktion näher zu definieren.


Klicken Sie nach dem Definieren der Aktion auf .

5. Wählen Sie eine oder mehrere Bedingungen aus, unter denen die Regel ausgeführt wird. Um die Regel immer auszuführen, löschen Sie alle Bedingungen.

Wenn in der Beschreibung der Regel blau unterstrichener Text vorhanden ist, klicken Sie auf den Text, um die Bedingung weitergehend zu definieren.

Wenn die Bedingung definiert ist, klicken Sie auf .

6. Geben Sie einen **Name der Regel:**, eine **Beschreibung der Regel:** ein und weisen Sie einen **Zeitplan:** zu.

7. Klicken Sie auf , um die neue Regel zu speichern.


Hinzufügen einer Webseite



Wenn Sie mit dem Internet verbunden sind, können Sie Webseiten zu einem Standort in Ihrem System Explorer hinzufügen. Bediener können diese Webseiten für den schnellen Zugriff auf Ihre ACM-Appliance oder andere mit Ihrem Überwachungssystem verbundene Seiten verwenden.

1. Klicken Sie im System Explorer mit der rechten Maustaste auf einen Standort oder auf einen Standortordner, und wählen Sie **Neue Webseite...** aus.

2. Geben Sie eine **Beschreibung:** und **Ort:** für die Webseite ein.

3. Wählen Sie eine **Zoom-Niveau:** aus, um die Webseite innerhalb eines Bildelements anzuzeigen.

4. Wird sie nicht angezeigt, klicken Sie auf , um Standortansicht-Editor anzuzeigen, und wählen Sie, wo die Webseite im System Explorer angezeigt werden soll. Die Webseite wird standardmäßig dem zu Beginn ausgewählten Standort hinzugefügt.

- Ziehen Sie im -Standortverzeichnis die Webseite **URL** im rechten Bereich hoch und runter, um festzulegen, wo sie angezeigt wird.
- Falls der Standort über -Ordner verfügt, wählen Sie einen Ort für die Webseite **URL** im linken Bereich. Der rechte Bereich wird aktualisiert und zeigt damit an, was in diesem Verzeichnis gespeichert werden soll.


5. Klicken Sie auf **OK**.

Überwachen von Türen

Nachdem die ACM-Appliance und ACC-Software konfiguriert wurden, ACC können Bediener mit Zugriffsrechten auf die Türen bei ACM die Türaktivität überwachen.

Türzutritt gewähren

Wenn Ihr Standort an ein ACM-Appliance angeschlossen ist, können Sie von jeder Kamera, die mit einer Tür verbunden ist, Türzugriff gewähren.


1. Öffnen Sie das Video der Kamera in einem Bildelement.
2. Bestätigen Sie, dass die Person im Video die Berechtigung hat, die Tür zu benutzen.
3. Klicken Sie im Bildelement oben links auf .

Hinweis: Wenn die Kamera nicht mit einer Tür verknüpft ist, wird das Symbol nicht angezeigt.

Wenn mehrere Türen mit der Kamera verknüpft sind, werden Sie aufgefordert, eine auszuwählen.

Identitätsüberprüfung

Wenn Ihre Kamera mit einer Tür in der ACM-Appliance verbunden ist, können Sie in einem angrenzenden Bildelement autorisierte und nicht autorisierte Türaktivitäten überwachen.

- Klicken Sie in der oberen rechten Ecke eines Bildelements auf  und wählen Sie die Tür aus, die Sie überwachen möchten.

Ein Bildelement zur Identität wird angezeigt. Die letzte Aktivität wird ganz oben angezeigt.

Tipp: Sie können das Ausweisfoto mithilfe des Schiebereglers am oberen Rand des Bildelements zur Überprüfung der Identität größer oder kleiner machen.

Wenn jemand einen ACM-Ausweis scannt, zeigt das Bildelement zur Überprüfung der Identität eine Karte mit den folgenden Informationen an, falls diese verfügbar sind:



- Ausweisfoto
- Vor- und Nachname
- Datum und Uhrzeit
- ACM-Türereignis

Vergleichen Sie das Video mit dem Ausweisfoto, um die Identität der Person zu überprüfen und einen nicht autorisierten Zutritt zu verhindern.

Hinweis: Das Identitätsüberprüfungsbildelement wird nicht aktualisiert, wenn Sie aufgezeichnete Videos oder eine andere Registerkarte anzeigen.

Identitätssuche

Sie können eine Person anhand ihres Namens oder ihrer Ausweis-ID suchen. Bei dieser Suche werden Türereignisse mit dem Ausweis der Person sowie Videos von verknüpften Kameras angezeigt.

1. Klicken Sie im Menü Neue Aufgabe  auf **Identität** .
2. Geben Sie den Namen oder die ID der Person ein und drücken Sie die **Eingabetaste**.
3. Wählen Sie die betreffende Person aus.
4. Klicken Sie auf **Datumsbereich**, um das Datum und die Uhrzeit Ihrer Suche festzulegen.
5. Klicken Sie auf **Türen**, um die Türen auszuwählen, die aufgenommen werden sollen.
6. Klicken Sie auf **Suchen**.



Bis zu 50 der letzten Türereignisse der betreffenden Person werden angezeigt. Unter jedem Türereignis werden Miniaturansichten der Videos von verknüpften Kameras angezeigt. Weitere Informationen finden Sie unter *Ergebnisse der Identitätssuche* unten.

Ergebnisse der Identitätssuche

Ein Suchergebnis kann ein Video von 5 Sekunden vor oder nach einem Türereignis anzeigen. Dieses Video stimmt möglicherweise nicht immer mit der zu untersuchenden Person überein, und einige Suchergebnisse enthalten möglicherweise kein Video, wenn die Kamera zu diesem Zeitpunkt nicht für die Aufnahme vorgesehen war.

Überprüfen und optimieren Sie Ihre Ergebnisse nach Bedarf.

Verfeinern von Ergebnissen

1. Wählen Sie im Bereich **Identitätsdetails** aus, welche Arten von Türereignissen angezeigt werden sollen.
2. Klicken Sie oben links auf **Türen ändern**, um Türen zur Suche hinzuzufügen oder daraus zu entfernen. Klicken Sie auf , um den Datumsbereich zu bearbeiten.
3. Klicken Sie auf eine Miniaturansicht, um das zugehörige Video im Bildelement anzuzeigen. Klicken Sie auf , um das Bild aus dem Video zu vergrößern.
4. Wenn Sie Kameras haben, auf denen die Avigilon Appearance Search-Funktion aktiviert ist und mit

Türen verknüpft sind, wählen Sie **Nur Merkmale**.

Tipp: Bewegen Sie den Mauszeiger über die Miniaturansicht und klicken Sie auf  , um eine Avigilon Appearance Search-Abfrage zu starten.

Speichern von Ergebnissen

- Bewegen Sie den Mauszeiger über eine Miniaturansicht und aktivieren Sie das Kontrollkästchen aller Ergebnisse, die Sie mit einem Lesezeichen versehen oder exportieren möchten.
 - Klicken Sie auf **Lesezeichen**, um das Ereignis für den schnellen Zugriff zu speichern.
 - Klicken Sie auf **Exportieren**, um eine Kopie des Ereignisses herunterzuladen.

Aktivieren Sie für AVI-Videoexporte das Kontrollkästchen **Hintergrund unscharf machen**, um alles außer der erkannten Person zu verdecken.

Durchsuchen der ACM-Appliance im ACC-Client

Wenn eine Webseite für eine ACM-Appliance konfiguriert wurde, können ACC-Bediener über die ACC-Client-Software darauf zugreifen.

Klicken Sie auf und ziehen Sie **URL** aus dem System Explorer in ein Bildelement.

Die Webseite wird in diesem Bildelement angezeigt.

- ACC-Bediener, die mit ihren ACM-Anmeldeinformationen angemeldet sind, werden automatisch bei der ACM-Appliance angemeldet.
- ACC-Bediener ohne ACM-Anmeldeinformationen erhalten beim ersten Öffnen der Webseite möglicherweise eine Zertifikatswarnung. Klicken Sie auf **Vertrauen**, um zur Anmeldeseite zu gelangen.

Hinweis: Wenn die ACM-Sitzung abläuft, müssen sich die Bediener erneut anmelden.

- ACC-Bediener, die mit ihren ACM-Anmeldeinformationen angemeldet sind, werden automatisch erneut angemeldet, wenn sie das Dialogfeld schließen.
- Administratoren können die Timeout-Einstellungen eines Bedieners in der ACM-Appliance ändern.

Beschreibung der Regelereignisse und Aktionen

In den folgenden Tabellen werden die Triggerereignisse, Aktionen und Bedingungen beschrieben, die beim Einrichten einer Regel zur Verfügung stehen.

Hinweis: Einige Aktionen sind nur für die ACC-Enterprise Edition-Software verfügbar.

Regel-Ereignisse

Bei Regelereignissen handelt es sich um die Ereignisse, die eine Regel auslösen.

Zutrittskontrollereignisse

Ereignis	Beschreibung
Türzutritt verweigert	<p>Mögliche Ursachen:</p> <ul style="list-style-type: none">• Unbekannte Karte• Versuch mit abgelaufener Karte• Gültige Karte an einem nicht autorisierten Lesegerät• Versuch mit deaktivierter Karte• Ungültiger Kartenzeitplan• Ungültiger PIN-Code wurde eingegeben• Ungültiger Gebäudecode• Gültige Karte mit falscher Ausgabeebene• Fehler bei Doppelzutrittssperre• Anzahl der Eingabeversuche überschritten• Ungültiger Kartenlesevorgang beim Durchziehen nach vorne• Ungültiger Kartenlesevorgang beim Durchziehen nach hinten• Öffnungsversuch einer gesperrten Tür• Verstoß bei Kontrolle zweier Karten – zweite Karte nicht verwendet• Zutritt verweigert – Anwesenheitsgrenze erreicht• Zutritt verweigert – Bereich deaktiviert• Ungültige Karte – vor Aktivierung• Ungültige Gebäudecodeerweiterung

Ereignis	Beschreibung
	<ul style="list-style-type: none"> • Ungültiges Kartenformat • Ungültige „Nur PIN“-Anforderung • Türmodus lässt keine Karte zu • Türmodus lässt keinen eindeutigen PIN zu
Türzutritt gewährt	<p>Mögliche Ursachen:</p> <ul style="list-style-type: none"> • Lokale Gewährung • Öffnung einer unverschlossenen Tür • Lokale Gewährung – APB-Fehler – nicht verwendet • Lokale Gewährung – APB-Fehler – verwendet • Gebäudecodegewährung – nicht verwendet • Lokale Gewährung – nicht verwendet • Gebäudecodegewährung • Lokale Gewährung – Verwendung ausstehend
Tür geschlossen	Eine Tür schloss sich.
Tür aufgebrochen	Eine Tür wurde gezwungen.
Aufgebrochene Tür geschlossen	Eine erzwungene Tür wurde geschlossen.
Tür offengehalten	Eine Tür wurde offen gehalten.
Offengehaltene Tür geschlossen	Eine offengehaltene Tür wurde geschlossen.
Tür geöffnet	Eine Tür öffnete sich.
Türzwang	<p>Mögliche Ursachen:</p> <ul style="list-style-type: none"> • Zwang erkannt – Zutritt verweigert • Lokale Gewährung – Zwang – nicht verwendet • Lokale Gewährung – Zwang – verwendet
Tür – Ausgangsanforderung	<p>Mögliche Ursachen:</p> <ul style="list-style-type: none"> • Türfreigabe gedrückt, nicht verifiziert • Türfreigabe gedrückt, Tür nicht verwendet • Türfreigabe gedrückt, Tür verwendet • Türfreigabe gedrückt, Verwendung ausstehend • Hostanforderung der Türfreigabe, nicht verifiziert • Hostanforderung der Türfreigabe, Tür nicht verwendet • Hostanforderung der Türfreigabe, Tür verwendet

Ereignis	Beschreibung
	<ul style="list-style-type: none"> • Hostanforderung der Türfreigabe, Verwendung ausstehend
Eingabe aktiviert	Eine installierte ACM Bedienfeld- oder Zusatzbedienfeld-Eingabe wurde aktiviert.
Eingabe deaktiviert	Eine installierte ACM Bedienfeld- oder Zusatzbedienfeld-Eingabe wurde deaktiviert.
Eingabefehler erkannt	Es wurde ein Fehler für eine installierte ACM Bedienfeld- oder Zusatzbedienfeld-Eingabe festgestellt. Manipulationen könnten stattgefunden haben.
Eingabefehler beseitigt	Ein Fehler, der für eine installierte ACM Bedienfeld- oder Zusatzbedienfeld-Eingabe festgestellt wurde, wurde beendet.

Regelaktionen

Regelaktionen sind Reaktionen auf ein Ereignis.

Nutzer-Benachrichtigungsaktionen

Aktion	Beschreibung
Meldungen auf dem Bildschirm ausgeben	Es wird eine Bildschirrmeldung über das Ereignis angezeigt.
E-Mail senden	Eine E-Mail-Benachrichtigung wird an die ausgewählten Empfänger gesendet.
Benachrichtigung an zentrale Überwachungsstation senden	Eine Benachrichtigung wird an die zentrale Überwachungsstation gesendet.
Einen Ton ausgeben	Wenn das Ereignis auftritt wird ein Hinweiston in der ACC Client-Software ausgegeben.

Überwachungsaktionen

Aktion	Beschreibung
Live-Streaming starten	Das zugehörige Live-Video wird angezeigt, sobald das Ereignis auftritt.
Videoanruf über Sprechanlage	Der Video-Intercom-Anruf wird in einem neuen Bildelement mit einem Klingelton geöffnet.
Focus of Attention	Das Ereignisvideo wird in der Focus of Attention-

Aktion	Beschreibung
	Registerkarte angezeigt, wenn es geöffnet ist.
Lesezeichen erstellen	Das Ereignisvideo ist mit einem Lesezeichen versehen.
Eine gespeicherte Ansicht öffnen	Die ausgewählte gespeicherte Ansicht wird automatisch angezeigt.
Live-Streaming auf einem virtuellen Matrix Monitor beginnen	Das Live-Video der ausgewählten Kamera wird automatisch auf dem ausgewählten Virtual Matrix-Bildschirm angezeigt.
Eine Karte auf einem virtuellen Matrix Monitor öffnen	Der ausgewählte Lageplan wird automatisch auf dem ausgewählten Virtual Matrix-Bildschirm angezeigt.
Eine Webseite auf einem virtuellen Matrix Monitor öffnen	Die ausgewählte Webseite wird automatisch auf dem ausgewählten Virtual Matrix-Bildschirm angezeigt.

Geräteaktionen

Aktion	Beschreibung
Gerät neu starten	Die Kamera oder das Gerät wird neu gestartet, wenn das Ereignis eintritt.
Gerät anhalten	Die Kamera oder das Gerät schaltet sich auf Standby, wenn das Ereignis eintritt. Streaming und Aufzeichnungen sind pausiert.
Gerät fortsetzen	Die Standby-Kamera oder das Gerät setzt das Streaming und die Aufzeichnung fort, sobald das Ereignis eintritt.
Digitalen Ausgang aktivieren	Ein digitaler Ausgang wird ausgelöst, wenn das Ereignis eintritt.
Digitalen Ausgang deaktivieren	Ein digitaler Ausgang wird deaktiviert, wenn das Ereignis eintritt.

PTZ-Aktionen

Aktion	Beschreibung
Auf Voreinstellung gehen	Die ausgewählte PTZ-Kamera fährt an die markierte vorgegebene Position, wenn das Ereignis eintritt.
Zu Startvoreinstellung wechseln	Die ausgewählte PTZ-Kamera fährt an die Start-Position, wenn das Ereignis eintritt.
Ein Muster starten	Die ausgewählte PTZ-Kamera durchläuft ein gewähltes Muster, wenn das Ereignis eintritt.

Aktion	Beschreibung
PTZ Aux einstellen	Die ausgewählte PTZ-Kamera startet den markierten Hilfsbefehl, wenn das Ereignis eintritt.
Zusatzeinrichtung entblocken	Die ausgewählte PTZ-Kamera beendet den markierten Hilfsbefehl, wenn das Ereignis eintritt.

Alarm-Aktionen

Alarm	Beschreibung
Einen Alarm auslösen	Ein Alarm wird ausgelöst, wenn das Ereignis eintritt.
Einen Alarm bestätigen	Ein Alarm wird bestätigt, wenn das Ereignis eintritt.

Regelbedingungen

Regelbedingungen sind die Szenarien, die erfüllt werden müssen, bevor die Regel ausgelöst wird.

Geräteereignisse

Bedingung	Beschreibung
Digitaler Eingang ist aktiv	Die Regel wird ausgelöst, wenn der verbundene digitale Eingang aktiv ist, wenn das ausgewählte Ereignis eintritt.
Digitaler Eingang ist nicht aktiv	Die Regel wird ausgelöst, wenn der verbundene digitale Eingang inaktiv ist, wenn das ausgewählte Ereignis eintritt.

Weitere Informationen

Zusätzliche Produktdokumentationen sowie Software- und Firmware-Upgrades finden Sie unter support.avigilon.com.

Technischer Support

Um Kontakt mit dem Avigilon Technischen Support aufzunehmen, besuchen Sie uns unter support.avigilon.com/s/contactsupport.