

Camera Configuration Tool – Benutzerhandbuch

Copyright

MOTOROLA, MOTO, MOTOROLA SOLUTIONS und das Stylized M-Logo sind Marken oder eingetragene Marken von Motorola Trademark Holdings, LLC und werden unter Lizenz verwendet. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber. © 2016 - 2024 Motorola Solutions, Inc. Alle Rechte vorbehalten.

PDF-CCT-C

Überarbeitung: 10 - DE

20240925

Inhalt

Einführung	1
Anmelden bei den Kameras	1
Navigieren durch das Camera Configuration Tool	2
Kamerastatus	2
Ändern der werkseitigen Standardanmeldeinformationen	3
Ändern der Anmeldeinformationen der Verbindung	4
Hinzufügen eines sekundären Admin-Benutzers	4
Finden von Kameras	6
Senden einer Discovery-Übertragung	6
Filtern und Sortieren der Kameras	7
Filtern von Kameras	7
Filter löschen	7
Sortieren von Kameras	7
Bearbeiten der Kameras	8
Bearbeiten einer einzelnen Kamera	8
Bearbeiten mehrerer Kameras	8
Anwenden von Änderungen	9
Einstellungen für sekundäre Medienprofile	9
Festlegen von Registerkarten	11
Zuweisen von IP-Adressen	14
Zuweisen statischer IP-Adressen	14
Einstellen des NTP-Servers	15
Multicast-Netzwerk konfigurieren	16
Verwaltung von Zertifikaten	17
Herunterladen einer Zertifikatsignierungsanforderung	17
Hochladen signierter Zertifikate	18
Anwenden von Zertifikaten	19
Zertifikate löschen	19
Einstellen des Verschlüsselungsmodus	20
Netzwerksicherheit	22
Deaktivieren von HTTP-Verbindungen im Camera Configuration Tool	22
Deaktivieren von HTTP-Verbindungen für eine Kamera	22
Ändern des HTTP- oder HTTPS-Ports	23

Ändern des Kameramodus	24
Konfigurieren der Analyse	25
Beschreibung der Analyse-Einstellung	25
Einrichten der Bewegungserkennung für klassifizierte Objekte	28
Konfigurieren von Analyseereignissen	29
Einrichten eines radiometrischen Analyseereignisses	30
Erweiterte Einstellungen für Wärmeereignisse	32
Temperaturschwellenwert Erweiterte Einstellungen	32
Temperaturänderung Erweiterte Einstellungen	33
Einen Bereich für die radiometrische Erkennung konfigurieren	34
Beschreibungen von Analyseereignissen	34
Konfigurieren der Menschenmengenerkennung	36
Firmware aktualisieren	37
Firmware herunterladen	37
Firmware anwenden	37
Kritische Firmware-Updates	38
Exportieren und Importieren von Einstellungen	39
Exportieren von Einstellungen	39
Bearbeiten der Exportdatei	39
Importieren von Einstellungen	40
Konfigurationsvorlagen	41
Verwenden von Konfigurationsvorlagen zum Anwenden von Einstellungen in einem Massenvorgang	42
Exportieren einer Konfigurationsvorlage	42
Entfernen von Einstellungen aus einer Konfigurationsvorlage (optional)	42
Beispiel 1	43
Beispiel 2	43
Importieren und Anwenden einer Konfigurationsvorlage	43
Verwenden der CCT-Befehlszeile	45
Aufrufen der CCT-Befehlszeile	45
Befehlszeilenparameter	46
Tipps zur Verwendung der Befehlszeile	49
Geräteprotokolle	51

Einführung

Mit dem Camera Configuration Tool von können Sie alle Kameras konfigurieren, die in Ihrem Netzwerk erkannt werden. Sie können allgemeine Einstellungen gleichzeitig auf mehrere Kameras anwenden oder einzelne Kameras an Ihre Standortanforderungen anpassen.

Stellen Sie zur Verwendung dieses Tools sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Alle Kameras, die Sie konfigurieren, sind installiert und physisch mit dem Netzwerk verbunden.
- Das Camera Configuration Tool ist auf einem Computer installiert, der Zugriff auf dasselbe Netzwerk wie die Kameras hat.
- Sie kennen das Kennwort für alle Kameras.

Anmelden bei den Kameras

Standardmäßig werden alle Kameras in Ihrem Netzwerk vom Camera Configuration Tool automatisch erkannt. Die erkannten Kameras sind mit Ihrem unmittelbaren Subnetz oder den für Multicast-Meldungen konfigurierten Subnetzen verbunden.

Bevor Sie die Kameras im System bearbeiten können, müssen Sie sich zunächst bei den Kameras anmelden.

1. Wenn Sie das Camera Configuration Tool starten, werden Sie sofort aufgefordert, sich bei allen erkannten Geräten anzumelden.
 - Geben Sie in die Felder **Benutzername** und **Passwort** die Anmeldeinformationen der Kamera ein. Das Tool geht davon aus, dass alle verbundenen Geräte dieselben Anmeldeinformationen verwenden.
 - Wenn die Kameras die Anmeldeinformationen admin/admin oder administrator/<leer> verwenden, aktivieren Sie das Kontrollkästchen **Verwenden Sie die werkseitigen Standardanmeldeinformationen, wenn die oben genannten Anmeldeinformationen nicht funktionieren..**
 - Das Tool meldet sich nicht bei neuen Kameras an, die keine Anmeldeinformationen haben.
2. Klicken Sie auf **Verbindung mit Geräten herstellen**.

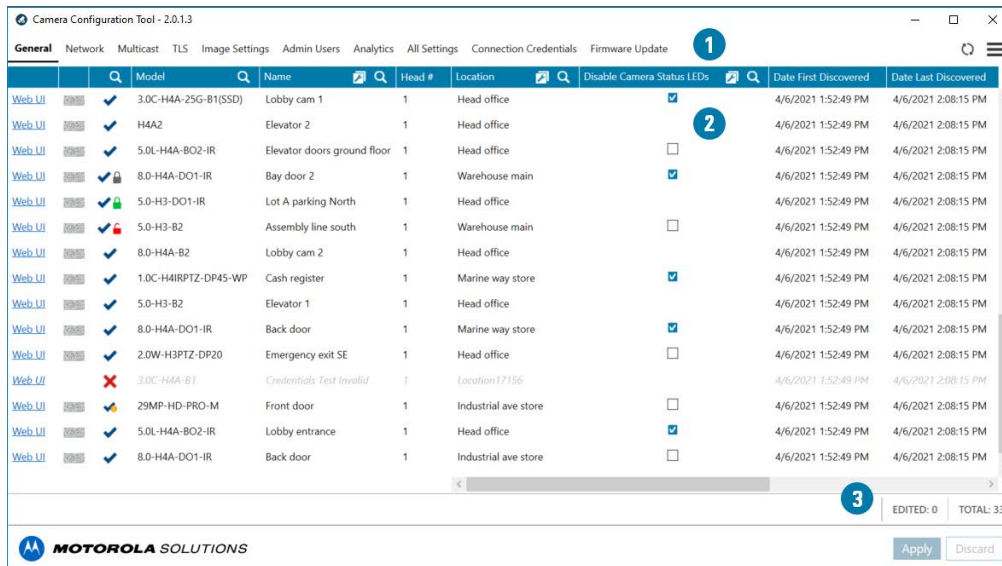
Sie sind mit den ausgewählten Anmeldeinformationen bei den erkannten Kameras angemeldet.


Wenn sich das Tool nicht bei einigen Kameras anmelden konnte, wählen Sie die Registerkarte **Anmeldeinformationen für die Verbindung** und geben Sie manuell die korrekten Anmeldeinformationen für diese Kameras ein. Weitere Informationen finden Sie unter *Ändern der Anmeldeinformationen der Verbindung* auf Seite 4.

Wenn Sie feststellen, dass eine oder mehrere Kameras, die Sie konfigurieren möchten, nicht in der Liste enthalten sind, können Sie die Kameras manuell suchen und der Liste hinzufügen. Weitere Informationen finden Sie unter *Finden von Kameras* auf Seite 6.

Navigieren durch das Camera Configuration Tool




Nachdem Sie sich bei allen Kameras angemeldet haben, zeigt das Anwendungsfenster eine Liste aller Kameras an, die automatisch im System erkannt wurden.










1. **Menüleiste** — Die Registerkarten für die Kameraeinstellungen werden auf der linken Seite angezeigt, und das zusätzliche Aufgabenmenü  ist auf der rechten Seite verfügbar. Weitere Informationen finden Sie unter *Festlegen von Registerkarten* auf Seite 11.
2. **Kameraliste** — Liste der erkannten Kameras und deren zugehörigen Einstellungen.
3. **Implementierungsbereich** — Der Bereich in der rechten unteren Ecke des Anwendungsfensters. Hier wird die Gesamtzahl der erkannten Kameras und die Anzahl der Kameras mit anstehenden Einstellungsänderungen angezeigt. Änderungen werden erst übernommen, wenn Sie auf **Anwenden** klicken.



Kamerastatus

In der Spalte Kamerastatus werden die folgenden Details zu jeder Kamera angezeigt.

-  — erfolgreich bei der Kamera angemeldet.
-  — Erfolgreich bei der Kamera mit admin/admin oder administrator/<leer> Anmeldeinformationen angemeldet. Es wird empfohlen, die Anmeldeinformationen der Kamera zu ändern. Weitere Informationen finden Sie unter *Ändern der werkseitigen Standardanmeldeinformationen* auf der nächsten Seite.
-  — Die Kamera befindet sich in der werkseitigen Standardeinstellung und verfügt über keine Anmeldeinformationen. Ändern Sie die Kameraanmeldeinformationen, um die Kamera zu verwenden. Weitere Informationen finden Sie unter *Ändern der werkseitigen Standardanmeldeinformationen* auf der nächsten Seite.




-  — Versuch, sich bei der Kamera anzumelden.
-  — Anmeldung bei der Kamera ist fehlgeschlagen. Ändern Sie die Anmeldeinformationen auf der Registerkarte **Anmeldeinformationen für die Verbindung**. Weitere Informationen finden Sie unter *Ändern der Anmeldeinformationen der Verbindung* auf der nächsten Seite.
-  — Kommunikation mit der Kamera ist nicht mehr möglich. Dies kann auftreten, wenn die Kamera offline ist oder ein Fehler beim Abrufen der Kameraeinstellungen aufgetreten ist.
-  — Sicher über HTTPS mit einem vertrauenswürdigen Zertifikat verbunden.
-  — Sicher über HTTPS mit einem selbstsignierten Zertifikat verbunden.
-  — Sicher über HTTPS mit einem nicht vertrauenswürdigen Zertifikat verbunden.
-  — Über HTTPS mit ungültigem Zertifikat verbunden.

Ändern der werkseitigen Standardanmeldeinformationen

Wenn sich Kameras im werkseitigen Standardstatus  befinden oder die Anmeldeinformationen admin/admin oder administrator/<leer>  verwenden, ändern Sie bitte die Anmeldeinformationen der Kamera.

1. Wählen Sie die Registerkarte **Administratorbenutzer**.

Hinweis: Wenn Sie Änderungen an den Einstellungen vorgenommen haben, die noch nicht gespeichert wurden, können Sie nicht zu einer anderen Registerkarte wechseln. Verwerfen Sie die Einstellungen, wenn Sie die Registerkarte Administratorbenutzer auswählen möchten.


2. Klicken Sie auf  und wählen Sie entweder  oder .
3. Geben Sie in der Spalte **Administratorbenutzername** einen neuen Benutzernamen für eine oder alle Kameras ein.
4. Geben Sie ein neues Kennwort für eine oder alle Kameras in der Spalte **Administratorpasswort** ein.

Tipp: Aktivieren Sie das Kontrollkästchen neben dem Kennwortfeld, um Ihre Eingabe anzuzeigen.



5. Klicken Sie auf **Anwenden**.

Hinweis: Pelco-Kameras unterstützen kein leeres Kennwortfeld. Für Administratorkonten in Pelco-Kameras muss ein Kennwort festgelegt werden.

Ändern der Anmeldeinformationen der Verbindung

Wenn sich das Camera Configuration Tool nicht bei einer Kamera anmelden konnte, zeigt die Kamera diesen Status an: .

Führen Sie die folgenden Schritte aus, um die Anmeldeinformationen für den Zugriff auf die Kamera zu ändern:

1. Wählen Sie die Registerkarte **Anmeldeinformationen für die Verbindung**.
2. Klicken Sie in die Kamerastatusspalte auf  und aktivieren Sie das Kontrollkästchen .
3. Doppelklicken Sie auf das Feld **Benutzername** oder **Passwort**, um andere Anmeldeinformationen der Kamera einzugeben.

Die von Ihnen geänderten Einstellungen werden gelb hervorgehoben.

Tipp: Aktivieren Sie das Kontrollkästchen neben dem Kennwortfeld, um Ihre Eingabe anzuzeigen.

4. Klicken Sie in der unteren rechten Ecke auf **Anwenden**.

Das Tool versucht, sich mit den neuen Anmeldeinformationen bei den Kameras anzumelden. Der Kamerastatus wird aktualisiert, um die Kameras anzuzeigen, auf die Sie zugreifen können.


Hinzufügen eines sekundären Admin-Benutzers

Hinweis: Wenn die Standard-Administratoranmeldeinformationen verloren gehen, müssen Sie möglicherweise die werkseitigen Standardeinstellungen der Kamera wiederherstellen. Je nach Konfiguration der Kamera ist diese Option möglicherweise nicht möglich.


Um das Standard-Administratorbenutzerkonto auf der Kamera zu schützen, können Sie einen sekundären Admin-Benutzer erstellen.

Sie können das sekundäre Konto anstelle des Standard-Administratorbenutzerkontos für den täglichen Betrieb verwenden. Sie können es auch als Backup verwenden, falls das Standard-Administratorkennwort verloren geht.

1. Wählen Sie die Registerkarte **Administratorbenutzer**.
2. Geben Sie einen neuen Benutzernamen in der Spalte Sekundärer Administratorbenutzername ein.

Wenn Sie für alle Kameras denselben Benutzernamen verwenden möchten, klicken Sie auf  und geben Sie den Benutzernamen ein.

3. Geben Sie ein Kennwort für den neuen Benutzernamen in der Spalte Sekundäres Administratorpasswort ein.

Wenn Sie dasselbe Kennwort für alle Kameras verwenden möchten, klicken Sie auf  und geben Sie das Kennwort ein.


Tipp: Aktivieren Sie das Kontrollkästchen neben dem Kennwortfeld, um Ihre Eingabe anzuzeigen.

4. Klicken Sie auf **Anwenden**.

Sie können über das Interface des Kamera-Webbrowsers weitere Administratorbenutzer hinzufügen. Das Camera Configuration Tool zeigt jedoch nur den Standard-Administratorbenutzer und einen anderen Administratorbenutzer auf dieser Registerkarte an.

Finden von Kameras

Wenn eine Kamera nicht automatisch vom Camera Configuration Tool erkannt wird, befindet sie sich möglicherweise in einem anderen Subnetz, das nicht für Multicast-Messaging konfiguriert ist. Sie können manuell nach Kameras suchen und dem Tool zur Konfiguration hinzufügen.

1. Wählen Sie in der rechten oberen Ecke  > **Geräte nach IP-Adresse hinzufügen**.
2. So finden Sie eine Kamera:
 - Geben Sie die IP-Adresse der Kamera in das Feld **Start-IP-Adresse** ein. Lassen Sie das Feld **End-IP-Adresse** leer.
3. So finden Sie mehrere Kameras:
 - Geben Sie den IP-Adressbereich ein. Geben Sie die erste IP-Adresse in das Feld **Start-IP-Adresse** und die letzte IP-Adresse in das Feld **End-IP-Adresse** ein.
Der Bereich Anzahl von IP-Adressen zeigt die Gesamtzahl der IP-Adressen im IP-Bereich an. Das Tool sucht nach nicht mehr als 65.536 Adressen gleichzeitig.
4. Geben Sie für die Kameras **Benutzername** und **Passwort** ein.
5. Aktualisieren Sie die **HTTP-Portnr.** und **HTTPS-Portnr.** wenn benötigt.
6. Klicken Sie auf **Geräte hinzufügen**.

Das Tool durchsucht alle Adressen im IP-Adressbereich und stoppt erst, wenn alle IP-Adressen geprüft wurden oder Sie klicken auf **Abbrechen**.

Tipp: Neue Kameras werden möglicherweise nicht angezeigt, wenn die Kameraliste gefiltert wird. Weitere Informationen finden Sie unter *Filtern und Sortieren der Kameras* auf der nächsten Seite.

Senden einer Discovery-Übertragung

Wenn Sie gerade ein großes System konfigurieren, werden im Netzwerk möglicherweise über einen längeren Zeitraum neue Kameras hinzugefügt. Das Camera Configuration Tool sendet jede Minute eine Discovery-Übertragung, Sie können die Software jedoch zwingen, auch eine Discovery-Übertragung zu senden.


Die Discovery-Übertragung sucht nach neuen Kameras, die mit dem Netzwerk verbunden sind. Jedes Mal, wenn eine neue Kamera erkannt wird, wird sie der Kameraliste hinzugefügt.

- Klicken Sie oben rechts auf .

Filtern und Sortieren der Kameras

Abhängig von der Größe Ihres Standorts müssen Sie möglicherweise über 100 Kameras bearbeiten. Damit Sie sich auf die Kameras konzentrieren können, die Ihre Aufmerksamkeit erfordern, können Sie die aufgelisteten Kameras filtern oder sortieren.

Filtern von Kameras

1. Klicken Sie oben in einer Spalte auf .
2. Wählen Sie Ihre Filterwerte aus oder geben Sie sie ein.
Eine Liste der aktiven Filter wird unten auf der Seite angezeigt.

Filter löschen

- Klicken Sie unten auf der Seite auf **X** für den Filter, den Sie entfernen möchten.

Sortieren von Kameras

- Klicken Sie auf den Spaltennamen, um die Spalte in aufsteigender alphanumerischer Reihenfolge zu sortieren.
- Klicken Sie erneut auf dieselbe Spalte, um die Spalte in absteigender Reihenfolge zu sortieren.
Sie können jede angezeigte Spalte sortieren.


Bearbeiten der Kameras

Im Camera Configuration Tool können Sie alle Kameras bearbeiten, bei denen Sie sich erfolgreich angemeldet haben.

Wechseln Sie zwischen verschiedenen Registerkarten, um die kategorisierten Kameraeinstellungen anzuzeigen und zu bearbeiten. Weitere Informationen finden Sie unter *Festlegen von Registerkarten* auf Seite 11.

Sie können nur die angezeigten Kameras bearbeiten. Um bestimmte Kameras zu bearbeiten, können Sie die Kameraliste filtern. Weitere Informationen finden Sie unter *Filtern und Sortieren der Kameras* auf der vorherigen Seite.

Tipp: Beim Bearbeiten der Kameraeinstellungen können Sie Kamerafilter deaktivieren. Sie können jedoch erst dann neue Filter hinzufügen, nachdem die Einstellungsänderungen übernommen oder verworfen wurden.

Sie können jede Spalte bearbeiten, die  anzeigt.

Bearbeiten einer einzelnen Kamera

Führen Sie einen der folgenden Schritte aus, um eine Einstellung für eine einzelne Kamera zu bearbeiten:


- Wählen Sie eine Einstellung aus den verfügbaren Optionen.
- Doppelklicken Sie auf die Kameraeinstellung und geben Sie einen neuen Wert ein.

Die bearbeitete Einstellung wird gelb hervorgehoben, aber noch nicht angewendet. Siehe *Anwenden von Änderungen* auf der nächsten Seite.

Hinweis: Änderungen an der HD Multisensor Dome-Kamera werden automatisch auf alle Kameraköpfe angewendet.

Bearbeiten mehrerer Kameras

So bearbeiten Sie die gleiche Einstellung für alle Kameras in der Kameraliste:

1. Klicken Sie in der Spaltenüberschrift auf .
2. Wählen Sie die neue Einstellung aus oder geben Sie sie ein.
3. Drücken Sie die Eingabetaste oder klicken Sie auf **Anwenden**, um die Einstellung zu ändern.

Die bearbeiteten Einstellungen werden gelb hervorgehoben, aber noch nicht übernommen. Siehe *Anwenden von Änderungen* unten.


Anwenden von Änderungen

Bearbeitete Einstellungen werden gelb hervorgehoben.

So übernehmen Sie alle Änderungen:

- Klicken Sie auf **Anwenden**, um die Änderungen zu bestätigen.

Wenn die Kamera eine Einstellung ablehnt, wird die Kamerazeile rot und die abgelehnte Einstellung gelb markiert.

Klicken Sie im rechten unteren Implementierungsbereich neben  auf **FEHLGESCHLAGEN**, um nur Kameras mit abgelehnten Einstellungen anzuzeigen.

So löschen Sie alle Änderungen:

- Klicken Sie auf **Verwerfen**.

Einstellungen für sekundäre Medienprofile

Viele Kameras können zusätzlich zu ihrem primären Stream zusätzliche Videostreams oder Medienprofile übertragen. Beispielsweise kann ein sekundärer Stream als Stream mit niedrigerer Auflösung zur Überwachung in Client- oder Mobilfunknetzen mit reduzierter Bandbreitenkapazität verwendet werden. Einige Kameras haben nur ein primäres und sekundäres Profil, einige Kameras haben auch ein tertiäres Profil und andere Kameras haben viele zusätzliche Profile. Primär, Sekundär und Tertiär Medienprofile können mit dem Camera Configuration Tool konfiguriert werden.

Mit dem Camera Configuration Tool können Sie Multicast und Bildeinstellungen für Ihre primären, sekundären und tertiären Streams für anwendbare Kameras konfigurieren. Weitere Informationen finden Sie unter *Festlegen von Registerkarten* auf Seite 11.

Wenn Sie zu den Registerkarten Multicast oder Bildeinstellungen navigieren, wird das **Primär** Medienprofil standardmäßig ausgewählt.

1. Auf den Registerkarten **Multicast** oder **Bildeinstellungen**, in der unteren linken Ecke des Fensters, wählen Sie die Option **Sekundär** oder **Tertiär** aus, um die Seite auf die Einstellungen für dieses Medienprofil zu ändern.

Model	Name	Head #	Encoding	Flicker Control	Enable WDR	Image Rate	Quality
ENC-4PORT	Device46294	1	H264	50Hz	<input type="checkbox"/>	19	9
1.0C-H4IRPTZ-DP45-WP	NotSupportingCertificates	1	H264	50Hz	<input checked="" type="checkbox"/>	19	18
29MP-HD-PRO-M	No WDREnabled	1	H264	60Hz	<input type="checkbox"/>	11	8
1.0C-H4PTZ-DC30	Device84849	1	H264	60Hz	<input checked="" type="checkbox"/>	16	9
2.0MP-HD-H264-B2	Device41632	1	H264	60Hz	<input type="checkbox"/>	13	12
8.0-H4A-DO1-IR	Device69547	1	H264	50Hz	<input checked="" type="checkbox"/>	15	12
3.0C-H4A-B1	Credentials Test Invalid	1					
29MP-HD-PRO-M	Credentials Test Default	1	H264	50Hz	<input checked="" type="checkbox"/>	1	15
5.0L-H4A-B02-IR	Credentials Test Valid	1	H264	60Hz	<input checked="" type="checkbox"/>	7	19
8.0-H4A-DO1-IR	Delete Certificates Test	1	H264	50Hz	<input type="checkbox"/>	17	12
8.0-H4A-DO1-IR	Certificate with long SN	1	H264	60Hz	<input type="checkbox"/>	16	17
2.0W-H3PTZ-DP20	Enable Http Test	1	H264	60Hz	<input type="checkbox"/>	12	20 (Lowest)
16MP-HD-PRO-M	GlobalCredentialsWork	1	H264	50Hz	<input checked="" type="checkbox"/>	19	17
5.0-H3-B2	Upload Certificates Test	1	H264	50Hz	<input checked="" type="checkbox"/>	9	14

Media Profile: Primary Secondary Tertiary

Filtered By: Model x EDITED: 0 FILTERED: 31 TOTAL: 33

MOTOROLA SOLUTIONS Apply Discard

2. Nehmen Sie die erforderlichen Einstellungsänderungen an den Kameras im ausgewählten Medienprofil vor.
3. Klicken Sie in der unteren rechten Ecke des Fensters auf **Anwenden**, um die Einstellungen auf das in Schritt 1 ausgewählte Medienprofil anzuwenden.

Festlegen von Registerkarten

Die Registerkarten in der Menüleiste enthalten eine gefilterte Liste von Einstellungen und Informationen zu jeder Kamera.

Die ersten 6 Spalten sind in jeder Registerkarte gleich:

1. **Webbenutzeroberfläche** — direkter Link zur vollständigen Webbrowser-Oberfläche der Kamera für eine erweiterte Konfiguration.
2. **Live-Video** — ein qualitativ minderwertiger Livestream von der Kamera, der Ihnen hilft, festzustellen, wo die Kamera installiert ist.
3. **Kamerastatus** — erkennt, ob die Kamera online ist und ob Sie sich erfolgreich an der Kamera anmelden konnten.
4. **Modell** — das bestimmte Kameramodell.
5. **Name** — Name der Kamera. Standardmäßig entspricht der Kameraname der Modellnummer.
6. **Kopf Nr.** — identifiziert den Kamerakopf für Multisensorkameras.

Die Registerkarten enthalten die folgenden Details:

Hinweis: Einige Einstellungen werden nicht angezeigt, wenn sie nicht von der Kamera unterstützt werden.

Tab	Einstellungen
Allgemein	<ul style="list-style-type: none">• Ort• Kamerastatus-LEDs deaktivieren• Datum der ersten Erkennung• Datum der letzten Erkennung• Seriennummer• Hersteller• Firmwareversion• Datum: Datum und Uhrzeit der Kamera• PTZ aktivieren: Aktiviert und deaktiviert PTZ-Steuerungen im VMS. Dies kann für Nicht-PTZ-Kameras, die beispielsweise PTZ-Befehle für die Zoomsteuerung verwenden, nützlich sein. Daher sind keine PTZ-Steuerungen erforderlich.• PTZ-Name: Listet alle PTZ-Befehle auf, die die Kamera verwenden kann• Metadaten aktivieren: aktiviert und deaktiviert die Übertragung von Metadatenströmen für die Medienprofile aller Kameras• Konfigurationsvorlage exportieren
Netzwerk	<ul style="list-style-type: none">• DHCP aktivieren

Tab	Einstellungen
	<ul style="list-style-type: none"> • IP-Adresse • Subnetzmaske • Standardgateway • Hostname • NTP-Servermodus • NTP-Server • MAC Adresse • HTTP aktivieren • HTTP-Portnr. • HTTPS-Portnr.
Multicast	<ul style="list-style-type: none"> • Video – Multicast-IP • Video – Multicast-Portnr. • Video – Multicast-TTL • Audio – Multicast-IP • Audio – Multicast-Portnr. • Audio – Multicast-TTL • Metadaten – Multicast-IP • Metadaten – Multicast-Portnr. • Metadaten – Multicast-TTL
TLS	<ul style="list-style-type: none"> • CSR herunterladen • TLS-Zertifikatantragsteller • Aussteller des TLS-Zertifikats • Ablaufdatum • Zertifikatstyp • Signaturalgorithmus • Zertifikate verwalten • Zertifikate • Verschlüsselungsmodus
Bildeinstellungen	<ul style="list-style-type: none"> • Codierung • Flimmerkontrolle • Bildstabilisierung aktivieren: Aktiviert und deaktiviert die elektronische Bildstabilisierung, wodurch andere Funktionen deaktiviert werden. Weitere Informationen finden Sie im Benutzerhandbuch der Überwachungskamera. • WDR aktivieren • Bildrate • Qualität

Tab	Einstellungen
	<ul style="list-style-type: none"> • Maximale Bitrate • Auflösung • Keyframe-Intervall • Kameraköpfe • Kameramodus
Administratorbenutzer	<ul style="list-style-type: none"> • Administratorbenutzername • Administratorpasswort • Sekundärer Administratorbenutzername • Sekundäres Administratorpasswort
Analyse	<ul style="list-style-type: none"> • Kameratyp • Analysemodus der Szene • Rauschfilter aktivieren • Manipulationsempfindlichkeit • Verzögerung des Manipulationsauslösers • Selbstlernsystem aktivieren • Selbstlernsystem zurücksetzen • Videoanalysemodus • Analyseereignisse • Menschenmengenerkennung • ONVIF-Analysemetadaten aktivieren
Alle Einstellungen	Alle verfügbaren Kameraeinstellungen. Scrollen Sie nach rechts, um alle Einstellungen zu sehen, die ausgeblendet sein können.
Anmeldeinformationen für die Verbindung	<ul style="list-style-type: none"> • Benutzername • Passwort
Firmwareupdate	<ul style="list-style-type: none"> • Firmwareversion • Verfügbare Firmwareversion • Upgrade durchführen • Downgrade durchführen


Zuweisen von IP-Adressen

Hinweis: Weisen Sie keine statischen IP-Adressen zu, es sei denn, Sie sind mit der IP-Netzwerkadressierung bestens vertraut. Das Camera Configuration Tool kann keine IP-Adressbereiche, Subnetzmasken, Standard-Gateways oder andere IP-Parameter berechnen oder überprüfen.

Zuweisen statischer IP-Adressen

Wenn Sie den Kameras in Ihrem System statische IP-Adressen zuweisen müssen, können Sie dies auf der Registerkarte Netzwerk tun. Auf dieser Registerkarte können Sie den aufgelisteten Kameras einen IP-Adressbereich oder einer Kamera eine bestimmte IP-Adresse zuweisen.

Tipp: Weisen Sie nur IP-Adressen aus Subnetzen zu, auf die Sie zugreifen können. Andernfalls verlieren Sie nach dem Zuweisen der neuen IP-Adressen den Zugriff auf die Kameras. Sie können die Kamera möglicherweise wiederherstellen, indem Sie der MAC-Adresse der Kamera eine neue IP-Adresse zuweisen. Weitere Informationen finden Sie unter *Zuweisen einer IP-Adresse über die MAC-Adresse* auf Seite 1.

1. Wählen Sie die Registerkarte **Netzwerk**.
2. So weisen Sie den den aufgelisteten Kameras einen statischen IP-Adressbereich zu:
 - a. Filtern Sie die Kameraliste, um nur die Kameras anzuzeigen, die Sie ändern möchten.
 - b. Klicken Sie oben in der Spalte IP-Adresse auf .
 - c. Geben Sie die erste IP-Adresse im Bereich in das Feld **Start-IP-Adresse** ein.
 - d. Geben Sie für die IP-Adressen **Subnetzmaske** und **Standardgateway** ein.
 - e. Klicken Sie auf **Anwenden**.

DHCP wird für die Kameras automatisch deaktiviert und die neuen Netzwerkeinstellungen werden gelb hervorgehoben.
3. So weisen Sie eine statische IP-Adresse zu einer Kamera:
 - a. Suchen Sie die zu ändernde Kamera in der Liste aus.
 - b. Doppelklicken Sie auf das Feld **IP-Adresse** und geben Sie die statische IP-Adresse ein.

DHCP ist für die Kamera automatisch deaktiviert.
 - c. Doppelklicken Sie auf die Felder **Subnetzmaske** und **Standardgateway**, um die erforderlichen Werte einzugeben.
4. Klicken Sie in der unteren rechten Ecke des Fensters auf **Anwenden**.

Die neuen IP-Adressen werden auf den Kameras implementiert.

Einstellen des NTP-Servers

Sie können den für jede Kamera verwendeten NTP-Server (Network Time Protocol) aktualisieren.

1. Wählen Sie die Registerkarte **Netzwerk**.
2. Wählen Sie **DHCP** oder **Manuell** in der Spalte NTP-Servermodus aus.
3. Wenn Sie Manuell auswählen, geben Sie in der Spalte NTP-Server die NTP-Serveradresse ein.
4. Klicken Sie auf **Anwenden**.

Multicast-Netzwerk konfigurieren

Für große Netzwerke, in denen mehrere Benutzer gleichzeitig Videos von Kameras gleichzeitig anzeigen können, wird empfohlen, ein Multicast-Netzwerk zu verwenden, um die Leistung gegenüber einem Unicast-System zu steigern. Mit Multicast können Videos mit hohen Megapixeln an eine Reihe von bestimmten Benutzern in einem Netzwerk gestreamt werden, mit klarerem Video und schnellerer Videoübertragung als mit einem Unicast-System. Video-, Audio- und Metadaten-Multicast-Einstellungen können für zusätzliche Flexibilität für Ihr Netzwerk individuell konfiguriert werden.

Multicast-Einstellungen können für jedes Stream-Profil Ihrer Kamera konfiguriert werden. Standardmäßig ist der Primär-Stream ausgewählt, wenn Sie zur Registerkarte **Multicast** navigieren. Weitere Informationen zum Anwenden von Einstellungen auf zusätzliche Stream-Profile finden Sie unter *Einstellungen für sekundäre Medienprofile* auf Seite 9.

Um einen Multicast zu deaktivieren, setzen Sie seine IP auf 0.0.0.0 und seine Portnummer auf 0.

1. Wählen Sie die Registerkarte **Multicast**.
2. Konfigurieren Sie für Video-Multicast die folgenden Einstellungen:

Wichtig: Bei Kameras mit mehreren Profilen müssen die Multicast-IP- und Port-Einstellungen jedes Profils eindeutig sein. Bei Kameras mit mehreren Köpfen müssen die Multicast-IP- und Port-Einstellungen jedes Kopfes und des Profils jedes Kopfprofils eindeutig sein.

- **Video – Multicast-IP:** Geben Sie die IP-Adresse für Ihre Video-Multicast-Übertragung ein.
- **Video – Multicast-Portnr.:** Geben Sie die Portnummer für Ihre Video-Multicast-Übertragung ein. Die Ports müssen gerade nummeriert sein.
- **Video – Multicast-TTL:** Geben Sie die TTL-Einstellung (Time to Leave) für Ihre Multicast-Übertragung von 1 bis 255 ein.

Hinweis: Die TTL-Einstellung kann verwendet werden, um Multicast-Verkehr in einem bestimmten genau definierten Teil des Netzwerks zu halten. Jedes Mal, wenn ein Router ein Multicast-Paket empfängt, verringert er den TTL-Wert um 1, und wenn ein Router ein Paket mit einem TTL-Wert von 1 empfängt, verwirft er das Paket und sendet es nicht weiter. Daher beschränken niedrigere Multicast-TTL-Einstellungen den Multicast-Verkehr auf einen kleineren Teil Ihres Netzwerks. Sie müssen diese Grenzwerte mit Ihren Routern durchsetzen.

3. Konfigurieren Sie die Audio- und Metadaten-Multicast-IP-, Port- und TTL-Einstellungen nach Bedarf.
4. Klicken Sie in der unteren rechten Ecke des Fensters auf **Anwenden**.

Die neuen Multicast-Einstellungen sind auf den Kameras eingerichtet. Die Kameras beginnen erst dann mit der Übertragung in Multicast, wenn der erste Client eine Verbindung zur Kamera herstellt.

Verwaltung von Zertifikaten

Für mehr Sicherheit und Effizienz können Sie Kamerazertifikate verwalten und sichere Netzwerkverbindungen als Massenverarbeitung mit dem Camera Configuration Tool konfigurieren.

Tipp: Sie können auch die Befehlszeile verwenden, um Zertifikate zu verwalten und Batch-Änderungen an Zertifikaten vorzunehmen. Weitere Informationen finden Sie unter *Befehlszeilenparameter* auf Seite 46.

Hinweis:

Durch eine Aktualisierung der Kamera-Firmware wird das aktive Zertifikat der Kamera nicht verändert.

Wenn Sie die Kamera auf die Werkseinstellungen zurücksetzen, wird das benutzerdefinierte Zertifikat gelöscht und zum Standardzertifikat der Kamera gewechselt.

Herunterladen einer Zertifikatsignierungsanforderung

Herunterladen einer Zertifikatsignierungsanforderung (CSR) für jede Kamer oder für mehrere Kameras. Der Zertifikatsignierungsanforderung muss von einer Zertifizierungsstelle signiert sein, um diese auf eine Kamera anwenden zu können.

1. Wählen Sie die Registerkarte **TLS**.
2. Aktivieren Sie das Kontrollkästchen für die Kameras in der Spalte CSR herunterladen.
3. Klicken Sie auf **Anwenden**.
4. Geben Sie ein **Allgemeiner Name** für die CSRs ein. Maximal 64 Zeichen, einschließlich der Präfix, Suffix und Quelle von eindeutigen Daten. Eine Vorschau wird angezeigt, wenn Sie einen Wert eingeben. Das Allgemeiner Name darf nicht leer sein, daher müssen Sie einen Wert für mindestens eines der Felder Präfix, Suffix und Quelle von eindeutigen Daten oder einer beliebigen Kombination dieser Felder eingeben.
 - **Präfix:** Geben Sie ein Präfix für das Allgemeiner Name ein.
 - **Quelle von eindeutigen Daten:** Wählen Sie die Kamera-IDs aus, die an den allgemeinen Namen angehängt werden sollen. Dies ist eine nützliche Kennung beim Herunterladen von CSRs für mehrere Kameras. Optionen: Keiner, Zähler, Name der Kamera, Ort der Kamera, Hostname der Kamera, IP-Adresse der Kamera, MAC-Adresse der Kamera, Seriennummer der Kamera, Allgemeiner Name des aktuellen Zertifikats, oder Automatisch generierte Hexadezimalzahl.
 - **Suffix:** Geben Sie ein Suffix für das Allgemeiner Name ein.

5. Geben Sie ein **Alternativer Antragstellername** für die CSRs ein. Eine Vorschau wird angezeigt, wenn Sie einen Wert eingeben.
 - Um einen in Alternativer Antragstellername bestimmten Benutzer einzugeben, wählen Sie t **Benutzereingabe** als **Quelle der Daten** und geben Sie den Namen in das Feld **Wert des alternativen Antragstellernamens** Feld ein.
 - Um eine Kamera-ID als Alternativer Antragstellername einzugeben, wählen Sie eine der folgenden Optionen aus der **Quelle der Daten** Dropdown-Liste aus: Eine Kopie des allgemeinen Namens, Hostname der Kamera, IP-Adresse der Kamera oder Erster alternativer Antragstellername des aktuellen Zertifikats.
6. Geben Sie die folgenden optionalen Felder ein:
 - **Organisationseinheit** — Der Geschäftsbereich einer Organisation.
 - **Organisation** — Der Name der Organisation.
 - **Ort** — Die Stadt, in der sich die Organisation befindet.
 - **Bundesland oder Kanton** — Das Bundesland oder Kanton, in der sich die Organisation befindet.
 - **Land** — Der aus 2 Buchstaben bestehende Ländercode.

Hinweis: Das Feld **Land** ist bei Pelco-Kameras nicht optional und muss ausgefüllt werden.

7. Klicken Sie auf **CSR herunterladen** und wählen Sie aus, wo die Zertifikatsignierungsanforderung gespeichert werden soll.


Die Zertifikatsignierungsanforderung wird als Zip-Datei heruntergeladen. Reichen Sie diese zur Unterzeichnung bei einer Zertifizierungsstelle ein.

Hochladen signierter Zertifikate

Nachdem die Zertifikatsignierungsanforderung von einer Zertifizierungsstelle signiert wurden, komprimieren Sie alle Zertifikate, die in das Camera Configuration Tool hochgeladen werden sollen.

Hinweis:

- Signierte Zertifikatdateien, die Sie der Zip-Datei hinzufügen, müssen bestimmte Dateierweiterungen aufweisen, wie beispielsweise *.cert*, *.cer* oder *.pem*.
- Um zu sehen, welche Kameras im Camera Configuration Tool vertrauenswürdige Zertifikate haben, müssen Sie die CA-Zertifikatdatei derselben Zip-Datei wie die signierten Zertifikate hinzufügen.

1. Wählen Sie in der rechten oberen Ecke  > **Zertifikate hochladen**.
2. Wählen Sie die Zip-Datei mit den signierten Zertifikaten aus.
3. Überprüfen Sie die Zusammenfassung der signierten Zertifikate.
4. Klicken Sie auf **Hochladen**. Es werden nur Zertifikate für angeschlossene Geräte hochgeladen.
5. Klicken Sie auf **OK**.

Die hochgeladenen Zertifikate können nun auf die jeweiligen Geräte angewendet werden.

Anwenden von Zertifikaten

Nachdem Sie signierte Zertifikate hochgeladen haben, können Sie auswählen, welches Zertifikat für jedes Gerät verwendet werden soll.

1. Wählen Sie die Registerkarte **TLS**.
2. Wählen Sie ein Zertifikat in der Spalte TLS-Zertifikatantragsteller aus.
3. Klicken Sie auf **Anwenden**.

Tipp: Klicken Sie auf **Verwalten**, um Details zu allen verfügbaren hochgeladenen Zertifikaten anzuzeigen, bevor Sie eines auf eine Kamera anwenden.

Zertifikate löschen

Mit dem Camera Configuration Tool können Sie ungültige, abgelaufene, selbstsignierte oder unerwünschte Zertifikate aus einer Kamera entfernen.

Hinweis:

- Sie können ein Zertifikat, das derzeit aktiv ist, nicht löschen. Wenden Sie ein anderes Zertifikat an und löschen Sie das nicht verwendete Zertifikat.
- Das werkseitige selbstsignierte Zertifikat kann nicht gelöscht werden.
- Sie können ein Zertifikat nicht löschen, wenn Sie andere Einstellungen im Kamerakonfigurationstool bearbeiten. Sie müssen die Änderungen Anwenden oder Verwerfen, bevor Sie ein Zertifikat löschen.

1. Wählen Sie die Registerkarte **TLS**.
2. Klicken Sie in der Spalte Zertifikate verwalten auf **Verwalten**.
3. Klicken Sie neben dem zu löschenden Zertifikat auf **Löschen**.
4. Klicken Sie auf **Ja**, um dies zu bestätigen.

Einstellen des Verschlüsselungsmodus

Für eine höhere Sicherheit der Netzwerkkommunikation können Sie die Einhaltung der Sicherheitsanforderungen des Federal Information Processing Standard (FIPS) 140-2 Level 1 oder Level 3 für kryptografische Module für die Server- und Kamerakommunikation aktivieren.

Hinweis:

- Für FIPS 140-2 Level 1 muss eine FIPS-Kameralizenz erworben werden.
- Für FIPS 140-2 Level 3 muss eine CRYPTR-Mikrokarte erworben werden. Die CRYPTR-Karte muss in den SD-Kartensteckplatz der Kamera eingesetzt werden, bevor sie aktiviert werden kann.

1. Wählen Sie die Registerkarte **TLS**.
2. Verwenden Sie in der **Verschlüsselungsmodus**-Spalte die Dropdown-Liste für jede Kamera, um den zu verwendenden Verschlüsselungstyp auszuwählen:
 - **OpenSSL** ist die Standardoption für die Verschlüsselung.
 - **FIPS 140-2 Level 1** aktiviert die FIPS 140-2 Level 1-Verschlüsselung.
 - **NXP TPM** ermöglicht es dem integrierten Trusted Platform Modul (TPM), Ihre Verschlüsselungsschlüssel sicher zu speichern. Nur Kameras, die mit dem integrierten NXP TPM ausgestattet sind, zeigen diese Option an.
 - **CRYPTR FIPS 140-2 Level 3** ermöglicht der installierten CRYPTR-Karte die sichere Speicherung Ihrer Schlüssel.

Wichtig: Wenn Sie die Einstellung auf CRYPTR FIPS 140-2 Level 3 oder NXP TPM ändern, erzeugt die Kamera einen neuen Schlüssel und ein selbstsigniertes Zertifikat. Wenn Sie diese Einstellung aktivieren, ist möglicherweise eine gewisse Zertifikat- und Schlüsselverwaltung erforderlich. Wenn Ihre vorherigen Schlüssel von einer Zertifizierungsstelle (CA) signiert wurden, müssen die neu generierten Schlüssel auch von der Zertifizierungsstelle signiert werden, um die Verbindung zu Ihrer Kamera sicher zu halten.

Weitere Informationen finden Sie unter *Herunterladen einer Zertifikatsignierungsanforderung* auf Seite 17 und *Hochladen signierter Zertifikate* auf Seite 18.

3. Klicken Sie in der unteren rechten Ecke des Fensters auf **Anwenden**.





Wichtig: Wenn Sie diese Einstellung an Ihrer Kamera ändern, muss Ihre Kamera neu gestartet werden, und Sie verlieren den Videostream für diesen Zeitraum. Avigilon empfiehlt, diese Einstellung während unkritischer Betriebszeiten anzuwenden. Das Anwenden dieser Einstellung auf eine einzelne Kamera kann 1 bis 5 Minuten dauern.

Die neuen Einstellungen für den Verschlüsselungsmodus sind auf den Kameras eingerichtet.

Hinweis: Wenn die CRYPTR-Mikrokarte ausgeworfen wird oder unbrauchbar wird, während sie in die Kamera eingesetzt und aktiviert ist, wird die Kamera im FIPS 140-2 Level 1-Modus neu gestartet. Wird die Karte wieder in die Kamera eingelegt, muss erneut CRYPTR FIPS 140-2 Level 3 als Verschlüsselungsmodus gewählt werden, um die CryptR-Mikrokarte weiterhin zum Speichern Ihrer Schlüssel zu verwenden.

Netzwerksicherheit

Standardmäßig versucht das Camera Configuration Tool, mithilfe von sicherem HTTPS eine Verbindung zu Kameras herzustellen. Wenn keine sichere Verbindung verfügbar ist, verwendet das Tool HTTP. Sie können diese Netzwerkeinstellungen verwalten.

Sicher angeschlossene Kameras zeigen eines der Symbole , ,  oder  neben ihren Kamerastatus an.

Deaktivieren von HTTP-Verbindungen im Camera Configuration Tool

Um die Sicherheit zu erhöhen, können Sie verhindern, dass das Camera Configuration Tool eine Verbindung über HTTP herstellt, wenn keine sicheren Verbindungen verfügbar sind. Kameras, die keine Verbindung über HTTPS herstellen können, werden offline angezeigt.

1. Schließen Sie die Anwendung Camera Configuration Tool.
2. Navigieren Sie im Windows Explorer zum Installationsordner. Standardmäßig ist dies `C:\Program Files (x86)\Motorola Solutions\Camera Configuration Tool`.
3. Doppelklicken Sie auf `CCT_DisableHttp.reg`, um zu verhindern, dass die Anwendung HTTP verwendet.
4. Klicken Sie auf **Ja** und dann auf **OK**.
5. Öffnen Sie die Anwendung Camera Configuration Tool.

So aktivieren Sie Verbindungen über HTTP erneut:

1. Schließen Sie die Anwendung Camera Configuration Tool.
2. Navigieren Sie im Windows Explorer zum Installationsordner. Standardmäßig ist dies `C:\Program Files (x86)\Motorola Solutions\Camera Configuration Tool`.
3. Doppelklicken Sie auf `CCT_EnableHttp.reg`.
4. Klicken Sie auf **Ja** und dann auf **OK**.
5. Öffnen Sie die Anwendung Camera Configuration Tool.

Deaktivieren von HTTP-Verbindungen für eine Kamera

Sie können Kameras so konfigurieren, dass nur sichere Verbindungen über HTTPS möglich sind.


1. Wählen Sie die Registerkarte **Netzwerk**.
2. Deaktivieren Sie in der Spalte HTTP aktivieren das Kontrollkästchen, um nur HTTPS zu verwenden.
3. *Optional*. Geben Sie in der Spalte HTTPS-Portnr. die HTTPS-Portnummer ein.
4. Klicken Sie auf **Anwenden**.

Ändern des HTTP- oder HTTPS-Ports

Sie können auswählen, über welche Ports die Kameras über HTTP und HTTPS eine Verbindung zum Netzwerk herstellen sollen.

1. Wählen Sie die Registerkarte **Netzwerk**.
2. Geben Sie in der Spalte HTTP-Portnr. die HTTP-Portnummer ein.
3. Geben Sie in der Spalte HTTPS-Portnr. die HTTPS-Portnummer ein.
4. Klicken Sie auf **Anwenden**.

Ändern des Kameramodus

Verwenden Sie auf der Seite Bildeinstellungen die Option Kameramodus, um den Kameramodus zu ändern. Um dieselbe Einstellung für mehrere Kameras zu konfigurieren, klicken Sie auf .


1. Wählen Sie einen der folgenden Modi aus der Dropdown-Liste:
 - Voller Funktionsumfang — Dies ist der Standardbetriebsmodus. Bietet den vollen Funktionsumfang der Kamera.
 - Hohe Bildrate — Dieser Modus verwendet die höchstmögliche Bildrate, deaktiviert jedoch bestimmte Funktionen. Weitere Informationen finden Sie im Benutzerhandbuch der Überwachungskamera.
 - Dynamische Datenschutzmasken – Dieser Modus ermöglicht Ihnen, dynamische Datenschutzmasken zu erstellen, deaktiviert jedoch bestimmte Funktionen. Weitere Informationen finden Sie im Benutzerhandbuch der Überwachungskamera.
 - Keine Videoanalyse - In diesem Modus wird die Videoanalyse deaktiviert.
2. Klicken Sie auf **Anwenden**.

Hinweis: Das Ändern des Kameramodus kann mehrere Minuten dauern, während der die Kamera neu gestartet wird.

Konfigurieren der Analyse

Wenn Sie über eine Videoanalysekamera verfügen, können Sie die Analyseereinstellungen auf der Registerkarte Analyse in Massenverarbeitung konfigurieren.

Beschreibung der Analyse-Einstellung

In der folgenden Tabelle werden die einzelnen Einstellungen beschrieben. Um dieselbe Einstellung für mehrere Kameras zu konfigurieren, klicken Sie auf .

Spalte	Beschreibung
Kameratyp	<p>Wählen Sie den Kameratyp aus, der angeschlossen wurde.</p> <ul style="list-style-type: none">• Tag-/Nacht-Kamera — Wählen Sie diese Option, wenn die Kamera Video in Farbe oder Schwarzweiß streamen kann. Dieser Kameratyp zeigt in der Regel bei Tag Farbvideos und bei Nacht Schwarzweißvideos an, um möglichst viele Details in der Szene zu erfassen.• Farbkamera — Wählen Sie diese Option, wenn die Kamera nur Farbvideo streamen kann.• Schwarzweißkamera — Wählen Sie diese Option, wenn die Kamera nur Schwarzweißvideo streamen kann.• Wärme — Wählen Sie diese Option, wenn die Kamera FLIR-Video (Forward Looking Infrared) streamen kann.
Analysemodus der Szene	<p>Wählen Sie den Standort, der den Installationsort der Kamera am besten beschreibt.</p> <ul style="list-style-type: none">• Außenbereich — ist für die meisten Außenbereiche geeignet. Diese Einstellung optimiert die Kamera, um Fahrzeuge und Personen zu identifizieren.• Großer Innenbereich — erkennt nur Personen und ist optimiert worden, um Personen in der Nähe von Hindernissen, z. B. Stühlen oder Schreibtischen, zu erkennen, solange Kopf und Torso sichtbar sind.• Innenbereich Nahaufnahme - erkennt nur Personen und ist dafür optimiert, Personen zu erkennen, die sich der Kamera nähern und sich möglicherweise nur teilweise im Bild befinden. In diesem Modus werden die Analyse-Ereignisse Objekt übertritt Lichtschranke und Richtung missachtet für diese Kamera deaktiviert. Der Modus Innenbereich Nahaufnahme ist derzeit nur bei modularen Kameras verfügbar.• Innenbereich (Überkopf) * — ist für Kameras optimiert worden,

Spalte	Beschreibung
	<p>die direkt über Kopf montiert sind. Sie sollte nur verwendet werden, wenn kein Torso im Sichtfeld der Kamera sichtbar ist. Bei jeder Bewegung wird davon ausgegangen, dass es sich um einen Menschen handelt. Kann in Bereichen mit wenig Platz, aber mit hohen Decken oder zur Überwachung von Türen eingesetzt werden. Verwenden Sie diese Funktion nicht mit der Avigilon Appearance Search-Funktion, der Gesichtserkennungsfunktion oder der Selbstlernfunktion, und auch nicht zur Erkennung von Personen, die sich gegen die Menge bewegen.</p> <ul style="list-style-type: none"> • Hohe Empfindlichkeit im Außenbereich * — ist optimiert worden, um eine höhere Empfindlichkeit bei der Erkennung von Personen und Fahrzeugen in schwierigen Außenbereichsumgebungen aufzuweisen. Diese Option kann weitere Fehlalarme erzeugen. Verwenden Sie diese Option nur, wenn Sie eine empfindlichere Einstellung als die Außenbereich-Einstellung für das System benötigen. • Große Reichweite bei Nacht* - priorisiert die Erkennung von Objekten mit großer Reichweite im Freien bei Nacht vor der Klassifizierung und Verfolgung von Objekten während des Tages. Verwendet externe IR-Beleuchtung anstelle der eingebauten IR-Beleuchtung von der Kamera. Die Objektklassifizierung und Verfolgungsgenauigkeit während des Tages ist im Vergleich zu anderen Modi für den Außenbereich reduziert. Nur für H4A-Kameras. <p>* Diese Modi sind für H5A-Kameras nicht verfügbar.</p>
Rauschfilter aktivieren	Aktivieren Sie das Kontrollkästchen, wenn die Kamera zu empfindlich ist und Bewegungen falsch als klassifizierte Objekte erkennt.
Manipulation aktivieren	<p>Aktivieren Sie das Kontrollkästchen, um die Manipulationserkennung zu aktivieren.</p> <p>Manipulation ist eine plötzliche Änderung im Sichtfeld der Kamera, die in der Regel durch eine unerwartete Bewegung der Kamera verursacht wird. Wenn Sie diese Einstellung aktivieren, löst die Kamera bei möglichen menschlichen Eingriffen Alarme aus.</p>
Manipulationsempfindlichkeit	<p>Geben Sie einen Wert zwischen 1 und 10 ein, um festzulegen, wie empfindlich eine Kamera bei Ereignissen sein soll.</p> <p>Legen Sie eine niedrigere Einstellung fest, wenn geringfügige Änderungen in der Szene – wie z. B. sich bewegende Schatten – Manipulationsereignisse verursachen. Wenn die Kamera in geschlossenen Räumen installiert ist und sich die Szene wahrscheinlich nicht ändert, können Sie die Einstellung zur Erfassung ungewöhnlicher Ereignisse erhöhen.</p>




Spalte	Beschreibung
Verzögerung des Manipulationsauslösers	<p>Geben Sie einen Wert zwischen 2-30 ein, um festzulegen, wie viele Sekunden die Kamera warten soll, bevor sie Manipulationsereignisse sendet. Der Standardwert lautet 8.</p> <p>Wenn die Manipulation vor Ablauf der Auslöseverzögerungszeit endet, werden keine Manipulationsereignisse gesendet. Wenn die Zeitspanne abgelaufen ist, die Manipulation aber noch nicht vorbei ist, sendet die Kamera die Ereignisse.</p>
Selbstlernsystem aktivieren	<p>Aktivieren Sie das Kontrollkästchen, um die Selbstlernfunktion zu aktivieren.</p>
Selbstlernsystem zurücksetzen	<p>Klicken Sie auf Zurücksetzen, sobald die Kamera nach der ersten Konfiguration stabil ist.</p> <p>Wenn eine Kamera bewegt oder angepasst oder wenn der Fokus oder die Zoom-Ebene geändert wird, muss das Selbstlernsystem immer zurückgesetzt werden. Die Änderung im Sichtfeld der Kamera beeinflusst die Ergebnisse der Videoanalyse.</p>
Videoanalysemodus	<p>Wählen Sie den Analysemodus, den Sie aktivieren möchten. Sie können nur Analyseereignisse für Kameras konfigurieren, die den Klassifiziertes Objekt-Modus verwenden.</p> <ul style="list-style-type: none"> • Klassifiziertes Objekt — erkennt und klassifiziert Objekte, wie z. B. eine Person oder ein Fahrzeug. Zu den Objekttypen gehören die folgenden Fahrzeugunterklassen: Fahrrad, Pkw, Motorrad, Bus, Großlastwagen, Pickup und Van. • Erkennung einer ungewöhnlichen Bewegung — erkennt Bewegungen und vergleicht Geschwindigkeit, Richtung und Ort der Bewegung mit dem was üblich für eine Szene ist. • Nur Manipulation — erkennt plötzliche Änderungen in der Szene.
Analyseereignisse	<p>Klicken Sie auf Konfigurieren, um Analyseereignisse für die ausgewählte Kamera im Klassifiziertes Objekt-Modus zu verwalten. Weitere Informationen finden Sie unter <i>Konfigurieren von Analyseereignissen</i> auf Seite 29.</p>
ONVIF-Analysemetadaten aktivieren	<p>Wenn diese Option aktiviert ist, sendet die Überwachungskamera ONVIF-Profil M-konforme Analysemetadaten an das VMS.</p>

Hinweis: CCT unterstützt die Anzeige von Begrenzungsrahmen und Konfidenzstufen rund um Objekte, wenn das Profil M aktiviert ist.

Einrichten der Bewegungserkennung für klassifizierte Objekte

Verwenden Sie die Bewegungserkennung für klassifizierte Objekte-Einstellungen, um die Objektbewegungserkennung zu konfigurieren. Diese ermöglicht es Ihnen zu definieren, wann das System Personen oder Fahrzeuge in der Szene erkennt.

Die Kamera muss für die Verwendung von Klassifiziertes Objekt Videoanalysemodus konfiguriert sein.

1. Wählen Sie die Registerkarte **Analyse**.
2. Klicken Sie in der Spalte Analyseereignisse auf **Konfigurieren**.
3. Wählen Sie **Bewegungserkennung für klassifizierte Objekte** und klicken Sie dann auf **Bearbeiten**.
4. Legen Sie den Überwachungsbereich (Region of Interest – ROI) fest, in dem Bewegung erkannt wird. Ereignisse werden nur ausgelöst, wenn sich die untere Mitte des Begrenzungsrahmens des erfassten Objekts in der ROI befindet.
 - Klicken Sie auf die gelben Markierungen am Rand und ziehen Sie sie. Für die Feinabstimmung der Form der Einblendung werden automatisch zusätzliche Markierungen hinzugefügt.
 - Klicken und ziehen Sie, um die grüne Einblendung zu verschieben.
 - Klicken Sie auf , um einen auszuschließenden Bereich hinzuzufügen. Der auszuschließende Bereich wird innerhalb der grünen Überlagerung hinzugefügt. Die Bewegung klassifizierter Objekte wird *nicht* in Ausschlussbereichen erkannt.
 - Um einen Ausschlussbereich zu löschen, wählen Sie einen Ausschlussbereich aus und klicken Sie dann auf .
 - Klicken Sie auf , um die standardmäßige grüne Einblendung wiederherzustellen.
5. Bestimmen Sie die Objekte, die vom System erkannt werden.
 - a. Aktivieren Sie das Kontrollkästchen **Person**, um Personen in dem Bereich zu erkennen.
 - b. Aktivieren Sie die Kontrollkästchen **Fahrzeug**, um Fahrzeuge in dem Bereich zu erkennen.
 - a. Klicken Sie auf die Kontrollkästchen neben den Fahrzeuguntertypen, um sie abzuwählen.
 - c. Passen Sie mithilfe des **Empfindlichkeit**-Schiebereglers die Empfindlichkeit des Systems hinsichtlich der Erkennung von klassifizierten Objekten an.

Wenn Sie den Schieberegler auf **Niedrig** einstellen, erkennt das Videoanalysegerät weniger Objekte, da das System sehr sicher sein muss, dass es eine Person oder ein Fahrzeug erkannt hat, bevor Sie über ein Ereignis benachrichtigt werden.

Wenn Sie den Schieberegler auf **Hoch** einstellen, erkennt das Videoanalysegerät mehr Objekte, da das System bei der Objektklassifizierung nicht so sicher sein muss, bevor Sie über ein Bewegungsereignis benachrichtigt werden.

Bei zu niedriger Einstellung des Schiebers kann es vorkommen, dass das System die Bewegung des klassifizierten Objekts verpasst. Ist der Schieberegler zu hoch eingestellt, generiert das System womöglich eine höhere Zahl falsch klassifizierter Objektbewegungserkennungen.

- d. Legen Sie im Feld **Erkennungszeit** fest, wie lange sich ein Objekt bewegen muss, bevor ein Bewegungserkennungsereignis für klassifizierte Objekte ausgelöst wird.
6. Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern.

Konfigurieren von Analyseereignissen

Sie können Analyseereignisse für einzelne Kameras über das Camera Configuration Tool hinzufügen, bearbeiten und löschen.

- Klicken Sie in der Spalte Analyseereignisse auf **Konfigurieren**. Das Dialogfeld Analyseereignisse wird angezeigt.

So fügen Sie ein Analyseereignis hinzu:

1. Klicken Sie auf **Ereignis hinzufügen**.
2. Geben Sie einen Namen für das Ereignis ein.
3. Aktivieren Sie das Kontrollkästchen **Aktiviert**. Wenn das Kontrollkästchen deaktiviert ist, werden durch das Videoanalyseereignis keine Ereignisse erkannt oder ausgelöst.
4. Wählen Sie **Aktivität**: aus. Eine Beschreibung der einzelnen Optionen finden Sie unter *Beschreibungen von Analyseereignissen* auf Seite 34.
5. Konfigurieren Sie die grüne Videoüberlagerung, um den Überwachungsbereich (Region of Interest – ROI) festzulegen.

Hinweis: Analyseereignisse werden nur ausgelöst, wenn sich die untere Mitte des Begrenzungsrahmens des erfassten Objekts in der ROI befindet oder den Strahl überquert.

6. Wählen Sie die **Objekttypen**:, auf die sich das Ereignis bezieht.
7. Klicken Sie auf **Erweiterte Optionen anzeigen** und konfigurieren Sie die verfügbaren Einstellungen:
 - **Empfindlichkeit**: — die Wahrscheinlichkeit, dass ein Objekt das Ereignis auslöst. Je höher die Empfindlichkeit, desto eher wird ein Ereignis für Objekte ausgelöst, die mit geringer Wahrscheinlichkeit erkannt werden. Der Standardwert lautet 8.
 - **Anzahl von Objekten** — die Anzahl der Objekte, die zum Auslösen des Ereignisses erforderlich sind.
 - **Erkennungszeit**: — die Mindestdauer des Ereignisses, bevor das System ein Ereignis auslöst. Der Standardwert beträgt je nach Aktivität 0 bis 30 Sekunden.
 - **Timeout** — die maximale Dauer des Ereignisses. Ereignisse, die nach dieser Zeit noch aktiv sind, lösen ein neues Ereignis aus. Der Standardwert beträgt 60 Minuten.
 - **Unzulässige Richtung**: — der Pfeil im Kreis bestimmt die Richtung, in die Objekte nicht bewegt werden sollen.
8. Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern.

So bearbeiten Sie ein Analyseereignis:

1. Wählen Sie ein Ereignis aus und klicken Sie auf **Bearbeiten**.
2. Nehmen Sie dann im Dialogfeld die gewünschten Änderungen vor.

Hinweis: Wenn Sie den Namen des Ereignisses ändern, funktionieren damit verknüpfte Regeln oder Ereignisse u. U. nicht mehr.

So löschen Sie ein Analyseereignis:

- Wählen Sie ein Ereignis aus und klicken Sie auf **Löschen**.

Einrichten eines radiometrischen Analyseereignisses

Verwenden Sie die Einstellungen Wärme für Analyseereignisse, um Ereignisse des Typs Temperaturschwellenwert oder Temperaturänderung mit einer unterstützten radiometrischen Wärmekamera zu konfigurieren.

Diese Arten von Ereignissen werden nur von Wärmebildkameras mit radiometrischen Funktionen unterstützt.

1. Wählen Sie die Registerkarte **Analyse**.
2. Klicken Sie in der Spalte Analyseereignisse auf **Konfigurieren**.
3. Klicken Sie auf **Ereignis hinzufügen**.
4. Geben Sie einen Namen für das Ereignis in das Feld **Name:** ein. Stellen Sie sicher, dass das Kontrollkästchen **Aktiviert** aktiviert ist.
5. Wählen Sie die Registerkarte **Wärme** aus, um die Einstellungen für Wärmeereignisse zu konfigurieren.
6. Bei Bedarf können Sie die Einstellung für den **Emissionsgrad** für die Wärmebildkamera anpassen.


Tipp: Der Emissionsgrad eines Materials oder einer Oberfläche gibt an, wie effektiv es/sie Wärmeenergie abgibt. Wenn Sie diese Einstellung ändern, wird ein Offset angewendet, der auf der Effizienz der verschiedenen Materialien bei der Abstrahlung von Wärmeenergie basiert. Sie sollten diese Einstellung anpassen, wenn Ihre Wärmebildkamera auf ein großes Objekt oder eine Oberfläche gerichtet ist, das/die einen anderen Emissionsgrad als den Standardwert aufweist. Im Tooltip neben dieser Einstellung finden Sie einige empfohlene Emissionsgradeinstellungen für verschiedene gängige Materialien. Dies ist eine globale Einstellung und gilt für die Wärmebildkamera als Ganzes.

7. Wählen Sie im Bereich **Aktivität:** die Art des zu konfigurierenden Temperaturereignisses aus.
 - **Temperaturschwellenwert:** Wählen Sie eine Temperaturschwellenwertaktivität aus, wenn ein Ereignis ausgelöst werden soll, wenn die Kamera eine Temperatur im definierten Messbereich erfasst, die einen definierten Temperaturschwellenwert erreicht oder überschreitet. Konfigurieren Sie die folgenden Einstellungen für den Temperaturschwellenwert:

- a. Wählen Sie im Bereich **Temperatur** aus, ob der eingestellte Temperaturschwellenwert ausgelöst wird, wenn die gemessene Temperatur über oder unter der eingestellten Temperatur liegt oder mit ihr übereinstimmt.
- b. Stellen Sie die Temperatur ein, die das Temperaturschwellenwertereignis auslöst. Verwenden Sie das Dropdown-Menü, um die Temperatur entweder in Celsius oder in Fahrenheit einzustellen.
- c. Legen Sie die Mindestzeit fest, die die auslösende Bedingung für den Temperaturschwellenwert vorliegen muss, bevor ein Alarm im Feld **Mindestdauer:** generiert wird. Die Dauer kann auf 1-1800 Sekunden eingestellt werden.
- **Temperaturänderung:** Wählen Sie eine Temperaturänderungsaktivität aus, wenn ein Ereignis ausgelöst werden soll, wenn die Kamera feststellt, dass sich die Temperatur im definierten Messbereich um einen bestimmten Wert geändert hat. Konfigurieren Sie die folgenden Einstellungen für die Temperaturänderung:
 - a. Wählen Sie im Bereich **Temperatur** aus, ob das Ereignis eine Temperaturänderung nach oben oder nach unten erkennen soll, indem Sie entweder die Option **Steigt um** oder **Sinkt um** auswählen.
 - b. Legen Sie fest, inwieweit sich die Temperatur ändern muss, um das Ereignis auszulösen. Verwenden Sie das Dropdown-Menü, um die Temperatur entweder in Celsius oder in Fahrenheit einzustellen.
 - c. Legen Sie im Feld **Dauer** fest, innerhalb welcher Zeit die Temperaturänderung erfolgen muss, um das Ereignis auszulösen.
 - d. Aktivieren Sie das Feld **Anfangswert**, wenn Sie eine Anfangstemperatur für das Temperaturänderungsereignis festlegen möchten. Temperaturänderungsereignisse werden nicht ausgelöst, wenn die Bedingungen für Temperaturänderungsereignisse oberhalb oder unterhalb dieses festgelegten Schwellenwerts erfüllt sind. Geben Sie den Wert für die Anfangstemperatur in das Feld **Anfangswert** ein.

Tipp: Wenn Sie beispielsweise einen Anfangswert: von **20°C** haben und ein Temperaturänderungsereignis des Typs *Sinkt um* konfigurieren, das auf **15°C** eingestellt ist, muss die Temperatur auf 5°C sinken, um das Ereignis auszulösen. Alle anderen Temperaturabsenkungen um 15°C, z. B. von 25°C auf 10°C, lösen das Ereignis nicht aus.

8. Wählen Sie im Bereich **Messmodus:** aus, wie Sie die Temperatur im Bild messen möchten.
 - **Punkterkennung:** Wählen Sie die Punkterkennung, um Temperaturänderungen an einem bestimmten Punkt oder Pixel im Videobild zu erkennen. Klicken Sie auf das grüne Kreuz und ziehen Sie es so, dass es den Teil des Videobildes markiert, in dem Sie Temperaturänderungen erkennen möchten. Der ausgewählte Punkt sollte nicht am Rand des Überwachungsbereichs liegen. Temperaturmessungen am Rand des Überwachungsbereichs sind möglicherweise nicht so genau.

- **Kastenerkennung:** Wählen Sie die Rahmenerkennung, um die Temperaturveränderungen in einem Überwachungsbereich zu erkennen.
 - a. Definieren Sie den Überwachungsbereich, in dem Temperaturänderungen erkannt werden sollen. Überwachungsbereiche für Wärmeereignisse sollten nicht am Rand des Überwachungsbereichs liegen. Temperaturmessungen am Rand des Überwachungsbereichs sind möglicherweise nicht so genau.
 - Ziehen Sie an den gelben Punkten in der Ecke, um die Form der grünen Einblendung zu verändern.
 - Klicken und ziehen Sie, um die grüne Einblendung zu verschieben.
 - Klicken Sie auf , um die standardmäßige grüne Einblendung wiederherzustellen.
 - b. Zusätzlich zur Einstellung des Überwachungsbereichs können Sie aus den folgenden Optionen auswählen, wie die Temperatur innerhalb des Überwachungsbereichs gemessen werden soll, und das Ereignis auslösen:
 - **Durchschnittstemperatur in ROI:** Die Kamera berechnet die durchschnittliche Temperatur innerhalb des Überwachungsbereichs und vergleicht sie mit den Ereigniseinstellungen.
 - **Höchsttemperatur in ROI:** Die Kamera nimmt die höchste gemessene Temperatur innerhalb des Überwachungsbereichs und vergleicht sie mit den Ereigniseinstellungen.
 - **Mindesttemperatur in ROI:** Die Kamera nimmt die niedrigste gemessene Temperatur innerhalb des Überwachungsbereichs und vergleicht sie mit den Ereigniseinstellungen.
- 9. Legen Sie den Wert für **Timeout** fest. Dies ist die maximale Dauer des Ereignisses. Ereignisse, die nach dieser Zeit noch aktiv sind, lösen ein neues Ereignis aus. Der Standardwert beträgt 60 Minuten.
- 10. Klicken Sie bei Bedarf auf die Schaltfläche **Erweiterte Einstellungen** um die erweiterten Einstellungen für dieses Ereignis zu konfigurieren. Die meisten Standard-Wärmeereignisse können mit den erweiterten Standardeinstellungen konfiguriert werden, jedoch bei Bedarf angepasst werden. Weitere Informationen finden Sie unter *Erweiterte Einstellungen für Wärmeereignisse* unten.
- 11. Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern.

Erweiterte Einstellungen für Wärmeereignisse

Die folgenden erweiterten Einstellungen für Wärmeereignisse können auf der Seite *Erweiterte Einstellungen* konfiguriert werden. Diese Einstellungen sind je nach Art des von Ihnen konfigurierten Wärmeereignisses anders.

Temperaturschwellenwert *Erweiterte Einstellungen*

- **Empfindlichkeit:** Definieren Sie die Empfindlichkeit der Temperaturschwellenwerterkennung. Die Empfindlichkeit korreliert mit der Konfidenz der erfüllten Regelbedingung. 1 erfordert die höchste Konfidenz und hat höhere Chancen auf falsch negative Ereignisse. 10 erfordert die niedrigste Konfidenz und hat höhere Chancen auf falsch positive Ereignisse.

- **Signifikante Temperaturänderung:** Legen Sie fest, ob ein neues Ereignis zusätzlich zu einer bereits ausgelösten Ereignisbedingung ausgelöst werden soll, wenn sich die Temperatur um den angegebenen Prozentsatz ändert. Geben Sie einen Wert zwischen 0,0 (0 %) und 1,0 (100 %) ein. Legen Sie 0 fest, wenn keine neuen Ereignisse ausgelöst werden sollen.
- **Absolute signifikante Temperaturänderung:** Legen Sie fest, ob ein neues Ereignis zusätzlich zu einer bereits ausgelösten Ereignisbedingung ausgelöst werden soll, wenn sich die Temperatur um den angegebenen Wert ändert. Geben Sie einen Wert zwischen 1°C und 50°C ein. Legen Sie 0 fest, wenn keine neuen Ereignisse ausgelöst werden sollen.
- **Signifikante Änderung der Pixelanzahl:** Legen Sie fest, ob ein neues Ereignis zusätzlich zu einer bereits ausgelösten Ereignisbedingung ausgelöst werden soll, wenn sich die Anzahl der Pixel, die die Ereignisbedingung erfüllen, um den angegebenen Prozentsatz ändert. Geben Sie einen Wert zwischen 0,0 (0 %) und 1,0 (100 %) ein. Legen Sie 0 fest, wenn keine neuen Ereignisse ausgelöst werden sollen.
- **Absolute signifikante Pixeländerung:** Legen Sie fest, ob ein neues Ereignis zusätzlich zu einer bereits ausgelösten Ereignisbedingung ausgelöst werden soll, wenn sich die Anzahl der Pixel, die die Ereignisbedingung erfüllen, um den angegebenen Wert ändert. Geben Sie eine Zahl zwischen 1 und 200 Pixel ein. Legen Sie 0 fest, wenn keine neuen Ereignisse ausgelöst werden sollen.
- **Maximale Zeit zum Ignorieren:** Legen Sie fest, wie lange die Ereignisbedingung nicht vorliegen darf, bevor das ausgelöste Ereignis beendet wird. Geben Sie eine Zahl zwischen 0 und 1800 Sekunden ein. Dieser Wert muss kürzer als der Wert für Timeout sein.
- **Aktualisierung der Mindestbegrenzung:** Legen Sie die Mindestzeit fest, die ab der letzten Auslösung vergehen muss, bevor ein neues Ereignis ausgelöst werden kann. Geben Sie eine Zahl zwischen 0 und 10 Minuten ein. Geben Sie 0 ein, um neue Ereignisse, die ausgelöst werden, nicht zu begrenzen.
- **Hysterese:** Definieren Sie die Offset-Temperatur oberhalb/unterhalb der eingestellten Temperaturschwelle, die überschritten werden muss, um das Ereignis zu beenden. Geben Sie eine Zahl zwischen 1°C und 50°C ein.
- **Übereinstimmungsbereich:** Legen Sie einen \pm -Bereichswert fest, der bei Temperaturereignissen des Typs „Übereinstimmung“ zur Solltemperatur addiert wird. Dadurch wird der Temperaturbereich für passende Ereignisse erweitert. Wenn Sie z. B. eine Temperatur von 5°C und einen Übereinstimmungsbereich von 3°C festlegen, kann das Ereignis in einem Bereich von 2°C bis 8°C ausgelöst werden. Geben Sie einen Wert zwischen 1°C und 50°C ein.

Temperaturänderung Erweiterte Einstellungen

- **Empfindlichkeit:** Definieren Sie die Empfindlichkeit der Temperaturänderungserkennung. Die Empfindlichkeit korreliert mit der Konfidenz der erfüllten Regelbedingung. 1 erfordert die höchste Konfidenz und hat höhere Chancen auf falsch negative Ereignisse. 10 erfordert die niedrigste Konfidenz und hat höhere Chancen auf falsch positive Ereignisse.
- **Maximale Zeit zum Ignorieren:** Legen Sie fest, wie lange die Ereignisbedingung nicht vorliegen darf, bevor das ausgelöste Ereignis beendet wird. Geben Sie eine Zahl zwischen 0 und 1800 Sekunden ein. Dieser Wert muss kürzer als der Wert für Timeout sein.
- **Aktualisierung der Mindestbegrenzung:** Legen Sie die Mindestzeit fest, die ab der letzten Auslösung vergehen muss, bevor ein neues Ereignis ausgelöst werden kann. Geben Sie eine Zahl zwischen 0 und 10 Minuten ein. Geben Sie 0 ein, um neue Ereignisse, die ausgelöst werden, nicht zu begrenzen.



- **Hysterese:** Definieren Sie die Offset-Temperatur oberhalb/unterhalb der eingestellten Temperaturschwelle, die überschritten werden muss, um das Ereignis zu beenden. Geben Sie eine Zahl zwischen 1°C und 50°C ein.

Einen Bereich für die radiometrische Erkennung konfigurieren

Beschreibungen von Analyseereignissen

Die folgende Tabelle zeigt die Aktivität:-Optionen, die beim Konfigurieren von Analyseereignissen verwendet werden können. Weitere Informationen und erweiterte Optionen finden Sie unter *Konfigurieren von Analyseereignissen* auf Seite 29.



Hinweis: Die Region of Interest (ROI) ist wie ein Teppich oder Stolperdraht. Ereignisse werden nur ausgelöst, wenn sich die untere Mitte des Begrenzungsrahmens des erfassten Objekts in der ROI befindet oder den Strahl überquert.

Aktivität:	Beschreibung
Objekte im zu überwachenden Bereich (Region of Interest, ROI)	<p>Das Ereignis wird ausgelöst, wenn die ausgewählte Anzahl von Objekten länger als die Erkennungszeit in der ROI vorhanden ist. Das Objekt kann von innerhalb des Überwachungsbereichs angezeigt werden oder beim Zutritt von außerhalb.</p> <p>Es wird nur ein Ereignis aktiviert, wenn die angegebene Anzahl von Objekten im Bereich erkannt wird. Zusätzliche Objekte im Bereich werden keine zusätzlichen Ereignisse auslösen.</p>
Herumlungernde Objekte	<p>Das Ereignis wird für jedes Objekt ausgelöst, das länger als die Erkennungszeit innerhalb der ROI bleibt. Jedes Objekt löst ein separates Ereignis aus.</p> <p>Das Ereignis wird zurückgesetzt, wenn das Objekt die ROI verlässt oder das Ereignis abläuft.</p>
Objekte im Lichtschrankenbereich	<p>Das Ereignis wird ausgelöst, wenn die angegebene Anzahl von Objekten innerhalb der Erkennungszeit den Strahl in der angegebenen Richtung überschritten hat.</p> <p>Wenn die Anzahl der Objekte 1 ist, wird das Ereignis nach Ablauf der Erkennungszeit ausgelöst.</p> <ul style="list-style-type: none"> ◦ Zum Ändern der Richtung des Strahls klicken Sie auf . ◦ Für die Erkennung von Objekten, die sich in beliebiger Richtung des Strahls bewegen, klicken Sie auf .
Objekt taucht auf oder	<p>Das Ereignis wird einmalig für jedes Objekt im Überwachungsbereich für</p>

Aktivität:	Beschreibung
tritt in Bereich ein	<p>länger als die Erkennungszeit ausgelöst. Das Objekt kann innerhalb der ROI erscheinen oder von außerhalb des Überwachungsbereichs eintreten.</p> <p>Dieses Videoanalyseereignis verursacht viele Alarme. Wenn beispielsweise 20 Objekte innerhalb der ROI erkannt werden, werden 20 Ereignisse ausgelöst – einer für jedes Objekt.</p>
Objekt nicht im Bereich anwesend	Das Ereignis wird ausgelöst, wenn keine Objekte länger als die Erkennungszeit in der ROI vorhanden sind.
Objekte treten in Bereich ein	<p>Das Ereignis wird ausgelöst, wenn die angegebene Anzahl von Objekten im Sichtfeld (FoV) erkannt wird und innerhalb der Erkennungszeit die ROI betreten wird.</p> <p>Wenn die Anzahl der Objekte 1 ist, wird das Ereignis nach Ablauf der Erkennungszeit ausgelöst.</p> <p>Die ROI muss kleiner als das FoV der Kamera sein, um das Objekt zu erkennen, bevor es in die ROI gelangt. Objekte, die im ROI erscheinen, lösen kein Ereignis aus.</p> <p>Es wird nur ein Ereignis aktiviert, wenn die angegebene Anzahl von Objekten im Bereich erkannt wird. Zusätzliche Objekte im Bereich werden keine zusätzlichen Ereignisse auslösen.</p>
Objekte verlassen Bereich	<p>Das Ereignis wird ausgelöst, wenn die angegebene Anzahl von Objekten innerhalb der ROI erkannt wird und die ROI innerhalb der Erkennungszeit verlassen wird.</p> <p>Wenn die Anzahl der Objekte 1 ist, wird das Ereignis nach Ablauf der Erkennungszeit ausgelöst.</p> <p>Die ROI muss kleiner sein als das FoV der Kamera.</p>
Objekt hält im Bereich an	Das Ereignis wird ausgelöst, wenn die Bewegung eines klassifizierten Objekts innerhalb der ROI erkannt wird, und dann länger als die Erkennungszeit stillsteht. Ein Ereignis wird für jedes Objekt aktiviert, das sich nicht mehr bewegt. Ein Objekt kann nur bis zu 15 Minuten lang überwacht werden kann.
Richtung missachtet	Das Ereignis wird für jedes Objekt ausgelöst, das sich länger als die Erkennungszeit innerhalb von 22 Grad der unzulässigen Richtung bewegt. Ein Ereignis wird für jedes klassifizierte Objekt aktiviert, das sich in eine unzulässige Richtung bewegt.
Objekte in Bereich automatisch nachverfolgen	Das Ereignis wird ausgelöst, wenn sich der ausgewählte Objekttyp in den Überwachungsbereich bewegt, wodurch die Kamera automatisch neu positioniert wird, um das Objekt zu verfolgen. Eine Rückkehr zur voreingestellten Position erfolgt, sobald das Objekt nicht mehr sichtbar ist.

Konfigurieren der Menschenmengenerkennung

Verwenden Sie die Regeln für die Erkennung von Menschenmengen, um die Menschenmengenerkennung zu konfigurieren. Damit können Sie festlegen, wann das System eine Menschenmenge in der Szene erkennt.

1. Wählen Sie die Registerkarte **Analyse**.
2. Klicken Sie in der Spalte „Menschenmengenerkennung“ auf **Konfigurieren**.
3. Wählen Sie die Regel für die Menschenmengenerkennung aus, die Sie bearbeiten möchten:
 - Ungewöhnliche Zunahme der Menschenmenge - Dieses Ereignis wird ausgelöst, wenn die Menschenmenge überraschend größer wird.
 - Menschenmenge - Dieses Ereignis wird ausgelöst, wenn die Anzahl der Personen über eine konfigurierbare Zeitdauer hinweg überschritten wird.
 - Ungewöhnliche Menschenmenge - Dieses Ereignis wird ausgelöst, wenn eine ungewöhnlich große Menschenmenge festgestellt wird.
4. Definieren Sie den **Einschlussbereich**, in dem Menschenansammlungen erkannt werden.
 - Klicken Sie auf die gelben Markierungen am Rand und ziehen Sie sie. Für die Feinabstimmung der Form der Einblendung werden automatisch zusätzliche Markierungen hinzugefügt.
 - Klicken und ziehen Sie, um die grüne Einblendung zu verschieben.
 - Klicken Sie auf , um den Stream neu zu starten, wenn ein Stream-Fehler auftritt.
 - Klicken Sie auf , um den Einschlussbereich auf den Standardwert zurückzusetzen.
5. Aktivieren Sie im Bereich „Einstellungen“ das Kontrollkästchen **Aktiviert**, um die Menschenmengen-Erkennungsregel zu aktivieren.
6. Definieren Sie die Voraussetzungen, die erforderlich sind, damit die Menschenmengen-Erkennungsregel ein Ereignis auslöst.
 - a. Anzahl der Personen - die Mindestanzahl an Personen, die in der definierten Zone erkannt werden müssen, um ein Ereignis auszulösen.
 - b. Schwellenwertzeit - die Zeitspanne, die die festgelegte Anzahl von Personen in der definierten Zone verbleiben muss, bevor ein Ereignis ausgelöst wird.
 - c. Timeout - die Zeitspanne, nach der das Ereignis abgebrochen wird.
 - d. Empfindlichkeit - die Empfindlichkeit korreliert mit der Wahrscheinlichkeit, dass die Regelbedingung erfüllt wird. 1 erfordert höchstes Vertrauen (höhere Wahrscheinlichkeit von falsch-negativen Ergebnissen) und 10 erfordert geringstes Vertrauen (höhere Wahrscheinlichkeit von falsch-positiven Ergebnissen). Bei der derzeitigen Empfindlichkeitsstufe lösen Objekte mit einem Vertrauensgrad von 50 % und mehr Ereignisse aus.
7. Klicken Sie auf **Anwenden**, um Ihre Einstellungen zu speichern, ohne das Fenster „Menschenmengenerkennung“ zu schließen.
8. Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und das Fenster „Menschenmengenerkennung“ zu verlassen.

Firmware aktualisieren


Mit dem Camera Configuration Tool können Sie Firmware-Updates auf alle Kameras in Ihrer Kameraliste anwenden. Laden Sie die Firmware herunter und wenden Sie sie auf die angeschlossenen Kameras an.


Firmware herunterladen

1. Gehen Sie zur Website Ihrer Kamera und laden Sie die Kamera-Firmware `.fp`-Datei für Ihr Modell herunter.
2. Speichern Sie die Firmware `.fp`-Dateien in das Firmware-Verzeichnis im Installationsordner. Der Standardpfad lautet: `C:\Program Files (x86)\Motorola Solutions\Camera Configuration Tool\firmware`

Löschen Sie die `.fp`-Datei aus dem Verzeichnis, um Firmware-Dateien zu entfernen, die nicht mehr verwendet werden.

Firmware anwenden

Tipp: Um die verfügbare heruntergeladene Firmware anzuzeigen, wählen Sie oben rechts  **>** **Lokales Firmware-Repository anzeigen.**

1. Wählen Sie die Registerkarte **Firmwareupdate** und filtern Sie die angezeigten Kameras nach Bedarf.
2. Klicken Sie in der Spalte Verfügbare Firmwareversion auf .
3. Wählen Sie die Firmware aus und klicken Sie auf **Anwenden**. Die ausgewählte Firmware wird nur auf die entsprechenden Kameramodelle angewendet.
4. Aktivieren Sie das Kontrollkästchen in der Spalte **Upgrade durchführen** oder der Spalte **Downgrade durchführen**. Sie müssen ein Kontrollkästchen aktivieren, um die Firmware auf der Kamera zu installieren.
Die Kontrollkästchen werden nur angezeigt, wenn sich die ausgewählte Firmware von der Version auf der Kamera unterscheidet.
5. Klicken Sie auf **Anwenden**.

Die Firmware wird an die Kameras gesendet und installiert. Die Kameras können neu starten und offline gehen, um die Aktualisierung abzuschließen.

Je nach Anzahl der Kameras und der Netzwerkgeschwindigkeit kann der Aktualisierungsvorgang sehr lange dauern.

Kritische Firmware-Updates

Wichtig: Manchmal ist ein kritisches Firmware-Update erforderlich, um den Kamerabetrieb aufrecht zu erhalten. Wir empfehlen Ihnen, diese kritischen Updates so schnell wie möglich einzuspielen. Diese Updates können länger dauern als üblich und sollten zu einem günstigen Zeitpunkt durchgeführt werden, damit Ihnen keine Videos aus dieser Kamera fehlen.

Wenn das Camera Configuration Tool feststellt, dass ein kritisches Update erforderlich ist, wird unten auf dem Bildschirm eine Meldung über das Update angezeigt.

Hinweis: Wenn Sie Änderungen an den Einstellungen vorgenommen haben, stellen Sie sicher, dass Sie diese unter Anwenden vornehmen, bevor Sie das wichtige Update starten. Nicht gespeicherte Änderungen werden bei der Aktualisierung verworfen.

1. Klicken Sie auf die Schaltfläche **Kameras aktualisieren** in der Meldung, um eine Liste aller Kameras zu erstellen, die aktualisiert werden müssen und für die die gewünschte Aktualisierung ausgewählt wurde.
2. Klicken Sie auf **Anwenden**, um die Aktualisierung durchzuführen.
3. Es erscheint eine Meldung, die darauf hinweist, dass die Aktualisierung länger als üblich dauern kann. Klicken Sie auf **OK**, um fortzufahren.

Alternativ können Sie die Aktualisierung auch in der Registerkarte Firmwareupdate durchführen. Weitere Informationen finden Sie unter *Firmware anwenden* auf der vorherigen Seite.

Exportieren und Importieren von Einstellungen

Sie können die Kameraliste in eine kommagetrennte Wertedatei (.csv) exportieren. Die CSV-Datei enthält alle verfügbaren Einstellungen der Kamera.

Sie können die Einstellungen wieder in das Camera Configuration Tool importieren und die Einstellungen auf die Kameraliste anwenden.

Tipp: Sie können auch die Befehlszeile verwenden, um Einstellungen für Geräte zu importieren oder zu exportieren, die mit dem Camera Configuration Tool verbunden sind. Weitere Informationen finden Sie unter *Befehlszeilenparameter* auf Seite 46.

Exportieren von Einstellungen

Sie können die Einstellungen der Überwachungskameras exportieren, um sie zu bearbeiten, und wieder importieren, um die Einstellungen in die Kameraliste zu übernehmen. Die exportierte Datei kann auch als Backup der aktuellen Kameraeinstellungen dienen.

1. (Optional) Filtern Sie die Kameraliste.
Nur die aufgelisteten Kameras sind beim Export enthalten. Weitere Informationen finden Sie unter *Filtern und Sortieren der Kameras* auf Seite 7.
2. Wählen Sie in der rechten oberen Ecke  > **Geräteeinstellungen exportieren**.
3. Wählen Sie die entsprechende Option, um die Datei entweder mit oder ohne Analyseeinstellungen zu exportieren:
 - **[[[Undefined variable UI_CCT.ExportWithAnalytics]]]**: Der Export der Überwachungskameras mit Analysefunktionen erfordert zwei oder mehr Zeilen pro Kamera in der exportierten .csv-Datei.
 - **[[[Undefined variable UI_CCT.ExportWithoutAnalytics]]]**: Der Export der Kameraeinstellungen ohne Analysefunktionen beschränkt jede Kamera auf eine Zeile in der .csv-Datei.
4. Benennen und speichern Sie die Exportdatei im Dialogfeld Speichern als.

Bearbeiten der Exportdatei


Sie können eine exportierte Datei bearbeiten und die Änderungen anschließend wieder in das Camera Configuration Tool importieren.

Wenn Sie die Exportdatei bearbeiten, beachten Sie bitte Folgendes:

- Löschen oder ordnen Sie die Spalten nicht neu.
Durch Löschen oder Ändern der Reihenfolge der Spalten wird die Datei beschädigt und die importierte Datei kann nicht erneut importiert werden.
- Wechseln Sie nicht die MAC Adresse der Kamera.
Das Camera Configuration Tool verwendet die MAC Adresse der Kamera, um die geänderten Kameras zu identifizieren.
- Wenn Sie eine statische IP-Adresse auf eine Kamera anwenden, ändern Sie die Spalteneinstellung **DHCPEnabled** in „*Falsch*“.
Wenn die Spalteneinstellung **DHCPEnabled** auf „*Wahr*“ eingestellt ist, wird die neue statische IP-Adresse nicht angewendet.

Importieren von Einstellungen

Sie können eine aktualisierte CSV-Datei in das Camera Configuration Tool importieren, um Massenänderungen an der Kameraliste vorzunehmen.

1. Wählen Sie in der rechten oberen Ecke  > **Geräteeinstellungen importieren**.
2. Wählen Sie im Dialogfeld Öffnen die CSV-Datei der Kameraeinstellungen aus und öffnen Sie diese.
Eine Bestätigungsmeldung wird angezeigt. Die Meldung enthält die Anzahl der in der Importdatei aufgeführten Geräte und die Anzahl der Geräte, die das Camera Configuration Tool bearbeiten kann.
Wenn die Einstellungsdatei Fehler enthält, wird eine Fehlermeldung angezeigt. Die Fehlermeldung beinhaltet eine Liste der Probleme, die in der Einstellungsdatei korrigiert werden müssen. Korrigieren Sie die Einstellungsdatei und versuchen Sie es erneut.
3. Klicken Sie auf **Geräte bearbeiten**.
Die Einstellungen werden in das Camera Configuration Tool importiert. Geänderte Einstellungen werden gelb hervorgehoben.
4. Klicken Sie auf **Anwenden**, um die Änderungen zu implementieren.

Konfigurationsvorlagen

Konfigurationsvorlagen sind Dateien, die eine Reihe vordefinierter Einstellungen von einer Kamera erfassen. Diese Vorlagen können verwendet werden, um die gleichen Einstellungen auf anderen Kameras zu verwenden, was den Konfigurationsprozess vereinfacht. Einstellungen, die nicht in der Konfigurationsvorlage aufgeführt sind, müssen über alternative Methoden angewendet werden.

Konfigurationsvorlagen unterstützen die folgenden Einstellungen:

- SmartCompression aktivieren
- SmartCompression Minimale Bildrate
- SmartCompression Ruhemodus-Keyframe-Intervall
- SmartCompression-Bandbreitenreduzierung
- SmartCompression Qualität des Hintergrunds
- SmartCompression Verzögerung nach Bewegung
- SmartCompression Qualität
- SmartCompression Max. Bitrate
- SmartCompression Modus für inaktive Szenen aktivieren
- Sommerzeit/Zeitzone
- Tag-/Nachtmodus/Schwellenwert
- Gegenlichtkompensation aktiviert
- Gegenlichtkompensationsstufe
- Digitale Entfeuchtung aktiviert
- Digitale Entnebelungsstufe
- Farbmodus
- Sättigung
- Schärfe
- Helligkeit
- Kontrast
- Weißabgleichsmodus
- Weißabgleich – Rot
- Weißabgleiche – Blau
- IPV6 aktivieren
- WS-Erkennung aktivieren/deaktivieren
- Geschwindigkeitsbegrenzung voreinstellen
- Geschwindigkeitsbegrenzung für Schwenken/Neigen
- Digitaler Zoom aktiviert

Verwenden von Konfigurationsvorlagen zum Anwenden von Einstellungen in einem Massenvorgang

Sie können eine Konfigurationsvorlage exportieren, die die für eine Kamera konfigurierten Kameraeinstellungen enthält. Anschließend können Sie die Konfigurationsvorlage importieren und auf mehrere Kameras gleichzeitig anwenden.

Exportieren einer Konfigurationsvorlage

Hinweis: Stellen Sie sicher, dass Sie als Einstellungen für die Kamera in der Web-Benutzeroberfläche die gewünschten Werte festgelegt haben, bevor Sie die Konfigurationsvorlage exportieren.

1. Wechseln Sie zur Seite *Allgemein*.
2. Klicken Sie in der Spalte **Konfigurationsvorlage exportieren** auf *Exportieren*.
3. Speichern Sie die JSON-Datei auf Ihrem lokalen Computer.
4. Sehen Sie sich die Informationen zum *Konfigurationsstatus* im Popup-Fenster an. Fehler werden im Abschnitt mit der *Fehlerübersicht* aufgeführt.
5. Klicken Sie auf **OK**.
6. Sie können die Konfigurationsvorlage als JSON-Datei in einem beliebigen Texteditor öffnen, um die konfigurierten Einstellungen zu überprüfen.

Entfernen von Einstellungen aus einer Konfigurationsvorlage (optional)

Sie können einen Textabschnitt entfernen, den Sie während der Aktualisierung nicht auf andere Kameras anwenden möchten. Die in der Konfigurationsvorlage aufgeführten Einstellungen überschreiben die konfigurierten Einstellungen der zu aktualisierenden Kameras. Durch das Entfernen der Einstellungen werden die Einstellungen der Kameras nicht entfernt. Es wird verhindert, dass diese während des Updates überschrieben werden.

Wichtig: Wir empfehlen nicht, die Konfigurationsvorlage zu verwenden, um einzelne Einstellungen zu bearbeiten. Verwenden Sie die Konfigurationsvorlage stattdessen, um Textabschnitte zu löschen, die nicht in einem Massenvorgang auf andere Kameras angewendet werden sollen.

Gehen Sie wie folgt vor, um Einstellungen aus der Konfigurationsvorlage zu entfernen:

1. Öffnen Sie die JSON-Datei der Konfigurationsvorlage in einem Texteditor.
2. Überprüfen Sie die Einstellungen und lassen Sie die aus, die von dem Update betroffen sein sollen.
3. Speichern Sie die aktualisierte Datei.

Beispiel 1

Sie können eine Gruppe von Einstellungen entfernen, indem Sie sie aus der Konfigurationsvorlage löschen. Sie können beispielsweise die Einstellungen für den Farbmodus entfernen, indem Sie den folgenden Textabschnitt löschen:

```
"ColorMode": {
  "Preset": "Avigilon",
  "Brightness": 50,
  "Saturation": 40,
  "Contrast": 50,
  "Sharpness": 50
}
```

Beispiel 2



Alternativ müssen Sie möglicherweise einen Textabschnitt löschen, um eine einzelne Einstellung zu entfernen. Sie können beispielsweise den Netzwerkabschnitt entfernen, indem Sie den folgenden Textabschnitt löschen:

```
"Network": [
  {
    "Identifizier": {
      "Name": "eth0"
    },
    "IPv6": {
      "Enabled": false
    }
  }
]
```

Importieren und Anwenden einer Konfigurationsvorlage

Sie können die Konfigurationsvorlage als JSON-Datei importieren und auf andere Kameras anwenden. Eine Konfigurationsvorlage kann derzeit nur auf Kameras desselben Modells angewendet werden.

Hinweis: Öffnen Sie die Konfigurationsvorlage und prüfen Sie die Einstellungen in der JSON-Datei, bevor Sie sie auf Kameras anwenden. Die in der Konfigurationsvorlage aufgeführten Einstellungen überschreiben die konfigurierten Einstellungen der zu aktualisierenden Kameras. Weitere Informationen finden Sie unter *Entfernen von Einstellungen aus einer Konfigurationsvorlage (optional)* auf der vorherigen Seite.

1. Filtern Sie die Liste der Kameras, um nur die Kameras anzuzeigen, auf die Sie die Konfigurationsvorlage anwenden möchten. Anweisungen finden Sie unter *Filtern und Sortieren der Kameras* auf Seite 7.
2. Klicken Sie auf das Symbol  im CCT-
3. Klicken Sie auf **Konfigurationsvorlage importieren**.
4. Suchen Sie die JSON-Datei und wählen Sie sie aus.
5. Überprüfen Sie die Informationen unter *Geräteeinstellungen importieren*:
 - Ausgewählte Datei: Name und Speicherort der JSON-Datei, die von Ihrem lokalen Computer hochgeladen wurde.
 - Anwendbares Modell: Das Kameramodell, auf das die Konfigurationsvorlage angewendet werden kann.
 - Anzahl der zutreffenden Geräte: Listet den Gerätenamen, die Modellnummer und die IP-Adresse von Geräten auf, die aktualisiert werden.
6. Klicken Sie auf **Weiter** und dann auf **Übernehmen**.
7. Überprüfen Sie die Informationen unter *Konfigurationsvorlage importieren*:
 - Erfolgreich angewendete Geräte: Listet den Gerätenamen, die Modellnummer und die IP-Adresse von Geräten auf, die erfolgreich aktualisiert wurden.
 - Fehlgeschlagene Geräte: Listet den Gerätenamen, die Modellnummer und die IP-Adresse von Geräten auf, die nicht erfolgreich aktualisiert wurden.
8. Klicken Sie im Berichtsbereich auf die Schaltfläche **OK**, um einen Bericht zu erstellen.
9. Überprüfen Sie die Informationen zum *Konfigurationsstatus*, um zu sehen, welche Einstellungen erfolgreich angewendet wurden. Das Symbol  weist auf einen Fehler hin.
10. Wählen Sie die Dreiecksymbole aus, um zusätzliche Einstellungen anzuzeigen. Sie müssen die Einstellung auswählen, um die *Fehlerübersicht* anzuzeigen.
11. Klicken Sie auf **OK**.
12. Klicken Sie auf **Liste der erfolgreichen IPs herunterladen**, um eine Liste der aktualisierten IP-Adressen der Kameras zu speichern. Die Liste wird als TXT-Datei gespeichert.
13. Klicken Sie auf **Liste der fehlgeschlagenen IPs herunterladen**, um eine Liste der IP-Adressen der Kameras zu speichern, die nicht aktualisiert werden konnten. Die Liste wird als TXT-Datei gespeichert.
14. Klicken Sie auf **Schließen**.

Verwenden der CCT-Befehlszeile

Mit der CCT-Befehlszeile können Sie Aktionen über die Befehlszeile ausführen und Batch-Änderungen für Standorte mit einer großen Anzahl von Kameras vornehmen. Mit diesen Batch-Jobs können Sie Einstellungen importieren oder exportieren oder die Zertifikate Ihrer Kameras verwalten.

Hinweis: Es wird empfohlen, diese Funktionen nur dann über die Befehlszeile auszuführen, wenn Sie mit der Verwendung von Befehlszeilen bereits vertraut sind.

Aufrufen der CCT-Befehlszeile

Bevor Sie Batch-Änderungen über die Befehlszeile vornehmen können, müssen Sie diese starten und zur richtigen Datei navigieren.

1. Öffnen Sie die Befehlszeile auf Ihrem Computer. Geben Sie „CMD“ in der Suchleiste am unteren Bildschirmrand ein und starten Sie die Eingabeaufforderungs-App.
2. Wechseln Sie zu Ihrem Camera Configuration Tool-Ordner. Um zum Standardspeicherort zu gelangen, geben Sie „C:\Programme (x86)\Motorola Solutions\Camera Configuration Tool“ ein und drücken die **Eingabetaste**.
3. Sobald Sie sich im richtigen Ordner befinden, geben Sie „CCT-Batch.exe“ ein und drücken die **Eingabetaste**.

Die Hilfeinformationen zu CCT Batch Job werden angezeigt. In dieser Hilfe finden Sie eine Zusammenfassung aller Befehle und Aktionen, die Sie ausführen können, sowie einige Beispiele für die Eingabe der Befehle. Die Exit-Codes werden ebenfalls bereitgestellt, damit Sie eine Rückmeldung erhalten, ob eine Aktion erfolgreich war.

Tipp: Orientieren Sie sich bei der Eingabe Ihrer Befehle an den Beispielen in der Hilfe zu CCT Batch-Jobs.

Befehlszeilenparameter

Die folgenden Parameter werden hier als Referenz angegeben und sind auch in der CCT Batch Job-Hilfe aufgeführt.

Befehl	Funktion	Beschreibung
-a <code>--addIP <IP-Adresse></code> <code>--addIP <Start-IP>-<Ende-IP></code>	Kamera anhand der IP-Adresse oder eines Bereichs von IP-Adressen, an die die folgenden Befehle gesendet werden sollen, identifizieren.	Verwenden Sie diesen Befehl, um eine einzelne Kamera anhand ihrer IP-Adresse oder eine Reihe von Kameras anhand eines IP-Adressenbereichs zu identifizieren und mit ihnen zu verbinden. Zum Beispiel: <code>-a 192.168.1.1-192.168.1.120</code> Leerzeichen im IP-Bereich sind nicht zulässig. Die identifizierten Kameras sind jene Kameras, an die die folgenden Import-, Export- oder Zertifikatsbefehle gesendet werden. Dieser Befehl wird zusammen mit den Befehlen -u , -p , -t und -s verwendet, um die Kamerainformationen einzugeben, die für die Verbindung mit der/den Kamera(s) erforderlich sind.
-u <code>--user <Benutzername></code>	Benutzernamen der Kamera(s) eingeben, an die Sie einen Befehl senden möchten.	Verwenden Sie diesen Befehl zusammen mit dem Befehl -a , um den Benutzernamen der Kamera einzugeben.
-p <code>--password <Kennwort></code>	Kennwort für die Kamera(s) eingeben, an die Sie einen Befehl senden möchten.	Verwenden Sie diesen Befehl zusammen mit dem Befehl -a , um das Kennwort der Kamera einzugeben.
-t <code>--httpPort <Portnummer></code>	HTTP-Portnummer eingeben, die für die Verbindung mit der/den Kamera(s) erforderlich ist.	Verwenden Sie diesen Befehl zusammen mit dem Befehl -a , um den HTTP-Port anzugeben, der für die Verbindung mit der/den Kamera(s) verwendet werden soll. Dieser Parameter ist optional. Wird diese Option übersprungen, verwendet CCT Batch den Standardport 80.
-s <code>--httpsPort</code>	HTTPS-Portnummer eingeben, die für die Verbindung mit der/den Kamera(s) erforderlich ist.	Verwenden Sie diesen Befehl zusammen mit dem Befehl -a , um den

Befehl	Funktion	Beschreibung
<Portnummer>		HTTPS-Port anzugeben, der für die Verbindung mit der/den Kamera(s) verwendet werden soll. Dieser Parameter ist optional. Wird diese Option übersprungen, verwendet CCT Batch den Standardport 443.
-f -- forceActionExecute	Erzwingt die Ausführung des eingegebenen Befehls unabhängig von Problemen.	Verwenden Sie diesen Befehl mit einem der anderen Befehle, um die Ausführung des Befehls zu erzwingen. Dadurch werden Befehle auf allen Geräten ausgeführt, die eine Verbindung herstellen können, und alle Geräte, die offline, in einem schwebenden Zustand oder unerreichbar sind, werden übersprungen.
<div style="border: 1px solid #00aaff; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p>Tipp: Wenn Sie einen Befehl ohne die Force-Option senden und eine der Kameras nicht erreicht werden kann, wird der Befehl abgebrochen.</p> </div>		
-e --export "<Datei.csv>"	Exportiert die Einstellungen der ausgewählten Kamera(s) als .csv-Datei.	Mit diesem Befehl werden die Einstellungen aller über den Befehl -a angeschlossenen Kameras in eine .csv-Datei exportiert. Geben Sie nach dem Befehl den Namen und den Speicherort der .csv-Datei an.
-i --import "<Datei.csv>"	Importiert die Einstellungen für die ausgewählte(n) Kamera(s) aus einer .csv-Datei.	Mit diesem Befehl werden die Einstellungen in einer .csv-Datei auf alle über den Befehl -a angeschlossenen Kameras importiert. Geben Sie nach dem Befehl den Namen und den Speicherort der .csv-Datei an.
-d --downloadCsr "<Betreff und SAN>" "<Datei.zip oder Datei.csr>"	Lädt eine Zertifikatssignierungsanforderung (CSR) für die ausgewählte(n) Kamera(s) herunter.	Verwenden Sie diesen Befehl, um eine CSR im PEM-Format in eine .zip- oder .csr-Datei für die über den Befehl -a verbundene(n) Kamera(s) herunterzuladen. Fügen Sie nach dem

Befehl	Funktion	Beschreibung
		<p>Befehl -d den zu verwendenden CSR-Betreff und SAN (alternativer Name des Betreffs) sowie den Dateinamen und -typ hinzu, unter dem die CSR heruntergeladen werden soll.</p> <div data-bbox="971 407 1422 768" style="border: 1px solid #00aaff; padding: 10px; margin-top: 10px;"> <p>Tipp: Weitere Informationen über den Befehl -d und seine Parameter, einschließlich aller Optionen und Beispiele, erhalten Sie, wenn Sie <code>CCT-Batch.exe --csrHelp</code> eingeben.</p> </div>
<p>-c</p> <pre>--uploadCrt "<Datei.zip oder Datei.crt>"</pre>	<p>Lädt ein Zertifikat hoch und macht es zum aktiven Zertifikat für die ausgewählte(n) Kamera(s).</p> <p>Dies kann in Verbindung mit dem Befehl <code>remove</code> verwendet werden, um unerwünschte Zertifikate zu entfernen.</p>	<p>Verwenden Sie diesen Befehl, um ein signiertes Zertifikat in einer <code>.zip</code>- oder <code>.csr</code>-Datei hochzuladen und dieses Zertifikat zum aktiven Zertifikat für die über den Befehl -a verbundene(n) Kamera(s) zu machen. Geben Sie nach dem Befehl -c den Pfad und den Namen des hochzuladenden Zertifikats ein.</p> <div data-bbox="971 1136 1422 1497" style="border: 1px solid #00aaff; padding: 10px; margin-top: 10px;"> <p>Tipp: Sie können auch das <i>alte</i> Zertifikat, das Sie ersetzen, oder <i>alle</i> nicht verwendeten Zertifikate als Teil des Upload-Befehls entfernen, indem Sie -r OLD oder -r ALL nach dem Upload-Befehl hinzufügen.</p> </div>
<p>-r</p> <pre>--removeCrt <Zertifikat-ID></pre> <pre>--removeCrt <Zertifikat-ID>;<Zertifikat-ID></pre>	<p>Entfernt bestimmte Zertifikate von Ihrer(n) ausgewählten Kamera(s).</p>	<p>Verwenden Sie diesen Befehl, um unerwünschte Zertifikate von der/den Kamera(s) zu entfernen, die mit dem Befehl -a verbunden sind. Geben Sie nach dem Befehl -r die Zertifikats-ID des zu entfernenden Zertifikats ein. Wenn Sie mehrere Zertifikate entfernen, setzen Sie ein Semikolon zwischen die verschiedenen Zertifikats-</p>

Befehl	Funktion	Beschreibung
		<p>IDs. Zertifikats-IDs sind nicht mit dem Betreff oder der Seriennummer des Zertifikats verbunden. Rufen Sie die Zertifikats-IDs mit dem Befehl -I ab.</p> <div style="border: 1px solid #00aaff; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p>Tipp: In Verbindung mit dem Upload-Befehl -c können Sie das <i>alte</i> Zertifikat, das ersetzt wird, oder <i>alle</i> unbenutzten Zertifikate gleichzeitig mit dem Hochladen des Zertifikats entfernen, indem Sie -r OLD oder -r ALL nach dem Upload-Befehl hinzufügen.</p> </div>
<p>-l --listCrt</p>	<p>Listet die Zertifikate und Zertifikatsinformationen für die ausgewählte(n) Kamera(s) auf.</p>	<p>Verwenden Sie diesen Befehl, um die Zertifikate der über den Befehl -a verbundenen Kamera(s) aufzulisten. Dadurch wird eine Liste der Zertifikats-ID, des Ablaufdatums und des gemeinsamen Namens aller Zertifikate für diese Kameras generiert. Dem aktiven Zertifikat wird ein Ausrufezeichen vorangestellt und es wird grün hervorgehoben, abgelaufene Zertifikate werden rot hervorgehoben, und selbstsignierte oder nicht vertrauenswürdige Zertifikate sind grau.</p>

Tipps zur Verwendung der Befehlszeile

Beachten Sie die folgenden Tipps, wenn Sie CCT Batch-Befehle über die Befehlszeile ausführen:

- Ein Exit-Code von **0** bedeutet, dass der Befehl erfolgreich ausgeführt wurde. Alle anderen Exit-Codes sind in der Hilfe zu CCT Batch aufgeführt.


Tipp: Sie können den Exit-Code des letzten abgeschlossenen Batch-Jobs aus dem System abrufen:

- CMD.exe: Geben Sie die Variable `%errorlevel%` ein. Beispiel: `echo %errorlevel%`.
- PowerShell: Geben Sie die Variable `$LastExitCode` ein. Beispiel: `echo $LastExitCode`.

- Es kann einige Minuten dauern, bis CCT Batch nach der Eingabe eines Befehls nach Kameras sucht.
- Wenn sich eine der Kameras, zu denen Sie eine Verbindung herstellen, nicht in einem Zustand befindet, in dem sie angemeldet werden kann, wird der Batch-Prozess angehalten, sofern nicht der Befehl `-f` force verwendet wird.
- Wenn das Passwort leer ist, verwenden Sie stattdessen Anführungszeichen (`""`). Wenn Sie PowerShell verwenden, können Sie kein leeres Kennwort verwenden.
- Wenn das Passwort ein Leerzeichen enthält, setzen Sie es auf beiden Seiten in Anführungszeichen (`" "`). Dies wird jedoch in PowerShell nicht funktionieren.

Geräteprotokolle

Um Ihnen beim Überprüfen und Untersuchen von Problemen zu helfen, können Sie eine Kopie der Kameraprotokolle herunterladen und einen Livestream der Protokollmeldungen verfolgen.

1. Filtern Sie die Kameraliste, um nur die Kameras anzuzeigen, die Sie protokollieren möchten.
2. Wählen Sie in der rechten oberen Ecke  > **Geräteprotokolle**.
3. Klicken Sie im Fenster Geräteprotokolle auf **Protokolle in Datei schreiben**.
4. Wählen Sie einen Speicherort für die Protokolldatei.

Die vorhandenen Kamera-Protokolle werden automatisch heruntergeladen. Das System fährt fort, die Live-Kameraprotokolle zu streamen und aufzuzeichnen, bis Sie auf **Anhalten** klicken oder das Geräteprotokolle-Fenster schließen. Während die Protokolle gestreamt werden, können Sie die Kameras weiterhin mit dem Camera Configuration Tool bearbeiten.

Die linke Geräte-Liste im Fenster Geräteprotokolle enthält die in der Protokolldatei enthaltenen Kameras. In der rechten Protokolle-Liste befinden sich die Protokollmeldungen in chronologischer Reihenfolge.

Der Protokolldatenstrom wird automatisch zur neuesten Nachricht gescrollt, bis Sie auf eine Nachricht im Datenstrom klicken. An dieser Stelle stoppt das automatische Scrollen, so dass Sie die Nachricht lesen können, während der Protokollstrom fortgesetzt wird. Damit die Anwendung das automatische Scrollen wieder aufnimmt, ziehen Sie die Scrollleiste an das Ende.

Sie können anhand der Seriennummer erkennen, auf welches Gerät in der Protokollmeldung verwiesen wird. Wenn eine Kamera offline geht, stoppt die Kamera die Aufzeichnung, bis sie wieder online ist. Die anderen Kameras in der Liste Geräte streamen ihre Protokolle weiter.

Die Protokolldatei, die Sie gespeichert haben, hat das TXT-Format. Sie können das gespeicherte Protokoll auch in einem Textleser anzeigen.

Bei jedem Öffnen des Geräteprotokolle-Fensters wird das vorherige Protokoll angezeigt. Wenn Sie auf Protokolle in Datei schreiben klicken, wird die Liste Geräte mit den neuesten gefilterten Kameras aktualisiert und eine neue Protokolldatei gespeichert.