



Bauer Systemtechnik GmbH, Geschäftsführer: Franz Bauer
Gewerbering 17, D-84072 Au i.d. Hallertau
Tel.: 0049 (0)8752-865809-0, Fax: 0049 (0)8752-9599
E-Mail: info@bauer-tore.de

IP-Kameraserie

Benutzerhandbuch

Einführung

Die VIVOTEK-Serien 9x99 und 9x89-V3 umfassen 8-MP- bzw. 5-MP-KI-Kameras. Beide Serien bieten exzellente Bildqualität und leistungsstarke KI-Analyse direkt am Gerät. Sie sind als Dome- und Bullet-Kameras, für den Innen- und Außenbereich sowie mit Festbrennweiten- und Varioobjektiven für vielfältige Anwendungen erhältlich. Die VIVOTEK-Serien 9x99 und 9x89-V3 verfügen über ein integriertes Trusted Platform Module (TPM) für höchste Cybersicherheit, die neue VIVOTEK RealSight Engine, die aktualisierte VIVOTEK SNV-Software und Smart IR III-Technologie für klare Bilder auch bei schwachem Licht und hohem Kontrast. Beide Serien sind mit einem integrierten Mikrofon ausgestattet und bieten standardmäßig oder optional über ein Kabel Zwei-Wege-Audio und Alarm-I/O. Die Indoor-Dome-Kameras FD9199-H und FD9189-H-V3 unterstützen HDMI-Ausgang für die öffentliche Anzeige und eignen sich für Einzelhandel, Parkplätze, Flughäfen, Bahnhöfe usw. Alle Kameras der Serien 9x99 und 9x89-V3 sind NDAA- und TAA-konform. Weitere Informationen zu beiden Kameraserien finden Sie auf der VIVOTEK-Website.

EHV und EHTV stehen für die funktionalen Merkmale dieser Serien. EHV-Modelle bieten eine erhöhte Temperaturbeständigkeit, fortschrittliche HDR-Technologie und vandalensichere Konstruktion und gewährleisten so einen stabilen Betrieb auch unter rauen Klimabedingungen und in Risikobereichen. EHTV-Modelle bieten dank Fernfokussierung mehr Flexibilität und eignen sich daher ideal für lange Korridore, Eingänge und Überwachungsszenarien mit großer Reichweite, die präzise Justierungen erfordern.

Mit ihren fortschrittlichen Funktionen und vielseitigen Einsatzmöglichkeiten bieten diese Kameras zuverlässige und anpassungsfähige Lösungen für Innen- und Außenbereiche und liefern außergewöhnliche Bildqualität, Langlebigkeit und Flexibilität, um verschiedenen Sicherheits Herausforderungen gerecht zu werden.

Revisionshistorie

Dokumentversion	Bezugsdatum	F/W Ver.	Kommentar
r1.0_241227	27.12.2024	1,2402,43,01 g und darüber	Veröffentlichung der neuen Kamera-Weboberfläche.

Vor Gebrauch lesen

Der Einsatz von Überwachungsgeräten kann in Ihrem Land oder Ihrer Region gesetzlich eingeschränkt sein. Die Netzwerkkamera ist nicht nur eine leistungsstarke, webfähige Kamera, sondern auch Teil eines flexiblen Überwachungssystems. Vor der Installation des Geräts für den vorgesehenen Zweck ist der Benutzer dafür verantwortlich, sicherzustellen, dass der Betrieb den geltenden Gesetzen und Vorschriften entspricht.

Prüfen Sie vor der Installation der Netzwerkkamera anhand der **Packungsinhaltsliste** in der beiliegenden **Kurzanleitung (QIG)**, ob alle Teile vorhanden sind. Lesen Sie unbedingt die Warnhinweise in der Anleitung und befolgen Sie die Installationsanweisungen, um Schäden durch unsachgemäße Montage oder Installation zu vermeiden. So stellen Sie sicher, dass das Gerät ordnungsgemäß funktioniert.

Die Netzwerkkamera zeichnet sich durch ein intuitives Design aus und ist daher auch für Anwender mit grundlegenden Netzwerkkennnissen einfach zu bedienen. Die Benutzeroberfläche ist nach Funktionen wie **Bild, Video & Audio, Erkennung, Aufnahme** und **System kategorisiert**. Die Kamera unterstützt verschiedene Anwendungen, darunter Sicherheitsüberwachung und Videomonitoring. Dank der verfügbaren Konfigurationsoptionen können Anwender die Leistung der Kamera anpassen, ihre Funktionen optimieren und einen einwandfreien Betrieb gewährleisten. Fortgeschrittene Anwender und Entwickler profitieren von dem strukturierten Menüsystem und **den App-** Einstellungen, die eine flexible Integration der Kamera in bestehende Systeme oder die Erweiterung spezifischer Funktionen ermöglichen.

WICHTIG:

Das Gerät wird mit einer RTC-Batterie geliefert. Beachten Sie Folgendes:

Hohe oder niedrige extreme Temperaturen, denen eine Batterie während des Gebrauchs, der Lagerung oder des Transports ausgesetzt sein kann; und niedriger Luftdruck in großer Höhe.

Der Austausch einer Batterie gegen einen falschen Typ kann eine Schutzfunktion außer Kraft setzen (zum Beispiel bei einigen Lithium-Batterietypen).

Die Entsorgung einer Batterie im Feuer oder in einem heißen Ofen sowie das mechanische Zerkleinern oder Zerschneiden einer Batterie können zu einer Explosion führen.

Das Belassen einer Batterie in einer Umgebung mit extrem hohen Temperaturen kann zu einer Explosion oder zum Austreten von brennbaren Flüssigkeiten oder Gasen führen.

Eine Batterie, die einem extrem niedrigen Luftdruck ausgesetzt ist, was zu einer Explosion oder zum Austreten von brennbaren Flüssigkeiten oder Gasen führen kann.

VORSICHT:

Es besteht Brand- oder Explosionsgefahr, wenn die Batterie durch einen falschen Typ ersetzt wird.

Inhaltsthema

Los geht's!

10

- **Verwendung des Geräte-Managers zum Auffinden und Identifizieren von Kameras im LAN**
- **Verwendung von Shepherd zum Auffinden und Identifizieren von Kameras im LAN**
- **Verwendung der Kamera-Weboberfläche für den erstmaligen Zugriff**

Ein neues Passwort für den Root-Benutzer festlegen

Melden Sie sich bei der Web-Benutzeroberfläche der Kamera an.

Einführung in die Web-Benutzeroberfläche der Kamera

Installation

19

- **Verwenden der Videostream-Symbolleiste**
- **Schnelle Kameraeinstellung über das Installationsfeld**

Kontrolle
PTZ

Bild

28

- **Verbesserung der Bildqualität mit VIVOTEK-Kameraeinstellungen**

Allgemeine Einstellungen

Illuminatoren

Bild

Belichtung

- **Optimierung der Bildschärfe durch flexible Fokussteuerung**

(Die Fokuseinstellungen werden nur von VIVOTEK-Zoomkameras des Typs EHTV unterstützt.)

Fokuseinstellungen

- **Verwendung von Datenschutzmaskierung zum Schutz vertraulicher Informationen in Bildern**

Datenschutzmaskierungseinstellungen

- **Anpassen von Bildüberlagerungen zum Hinzufügen zusätzlicher Informationen**

Overlay

Fortschrittlich

Inhaltsthema

Video & Audio

58

- **Optimierung der Überwachungseffizienz durch flexible Videoeinstellungen**

Modus

Strom

- **Konfigurieren der Audioeinstellungen für verbesserte Ein- und Ausgabeleistung**

Audioeinstellungen

Audioclips

- **Konfigurieren von Medienprofilen zur Optimierung der Videoleistung für vielseitige Anwendungen**

Medienprofil

PTZ-Einstellungen

73

- **Mühevolle Verwaltung und Anpassung der PTZ-Einstellungen für eine präzise Kamerasteuerung**

Startseite & Voreinstellungen

Patrouillieren

Präferenz

App

82

- **Erweitern Sie die Kamerafunktionalität mit leistungsstarken Anwendungen**

Trend Micro IoT-Sicherheit

Deep Learning VCA

Detektion

85

- **Smart VCA: Fortschrittliche Videoanalyse für proaktive Sicherheit und präzise Überwachung**

- **Smart Motion: Verbesserte Genauigkeit und Effizienz bei der Überwachung durch Smart Bewegungserkennung**

- **Audioerkennung: Verbesserung der Sicherheit durch Echtzeit-Audioanomalieerkennung für**

Schnelle Antwort

- **Stoßerkennung: Gewährleistet Echtzeitschutz vor physischen Einwirkungen**

- **Manipulationserkennung: Schutz des Überwachungssystems vor visueller Behinderung**

Inhaltsthema

Ereignis

97

- **Ereignis:** Verbesserung der Sicherheit durch automatisierte und anpassbare Ereignisse
- **Kameraverknüpfung:** Verbessern Sie die Koordination mehrerer Kameras und beseitigen Sie tote Winkel mit Camera Link
- **Event-Server & Medien:** Müheloses Event-Management und erhöhte Sicherheit mit Event Server & Medien

Aufnahme

111

- **Aufzeichnung:** Maximieren Sie Überwachung und Speicherung mit maßgeschneiderten Aufzeichnungseinstellungen

System

114

- **Gerät:** Zentralisierte Verwaltung für Systemüberwachung und Kamerakonfiguration
- **Konfigurieren und sichern Sie die Netzwerkverbindung Ihrer Kamera für eine reibungslose Kommunikation**
 - Netzwerkeinstellungen
 - Protokoll
 - Service
 - Sicherheit
- **Benutzerzugriffe und Berechtigungen verwalten für mehr Sicherheit und Kontrolle**
 - Benutzer
 - Privileg
 - Konto gesperrt
- **Wartung:** Firmware-Updates und Konfigurationsmanagement für die Systemwartung
- **Speicherung:** Optimierte Speicherlösungen für zuverlässige Videoaufzeichnung und Datenaufbewahrung
- **Datei:** Mühelose Verwaltung und Abruf von aufgezeichneten Medien
- **Überwachung und Verwaltung von Systemprotokollen und -parametern**
 - Protokolle
 - Audit-Protokoll
 - Parameter
- **Designereinstellungen:** Anpassen des Erscheinungsbilds der Benutzeroberfläche und des Brandings mit den Designereinstellungen

Los geht's!

Nach der Installation der Kamera finden Sie deren IP-Adresse im lokalen Netzwerk schnell über den Geräte-Manager oder Shepherd von VIVOTEK. So greifen Sie auf die Web-Oberfläche der Kamera zu, um Videoüberwachung und verschiedene Kameraeinstellungen vorzunehmen. Beim ersten Zugriff auf die Web-Oberfläche können Sie außerdem ein eigenes Passwort für die Kamera festlegen, um die Datensicherheit zu erhöhen.

Kameras im LAN mithilfe des Geräte-Managers lokalisieren und identifizieren

Der Geräte-Manager ist ein Tool zur Geräteverwaltung, das die Installation und Konfiguration mehrerer VIVOTEK-Geräte (hauptsächlich VIVOTEK-Kameras) über eine Client-Server-Architektur vereinfacht. Dadurch können Geräteverwaltung und -wartung per Fernzugriff durch Installation und Nutzung des Geräte-Manager-Clients durchgeführt werden.

Hier können Benutzer mithilfe des Geräte-Managers die IP-Adresse der Kamera ermitteln, die sie in ihrem lokalen Netzwerk betreiben möchten.

Schritt 1.

Laden Sie die Geräte-Manager-Anwendung von der offiziellen VIVOTEK-Website herunter und installieren Sie sie. (https://www.vivotek.com/products/software/device_manager)

Schritt 2.

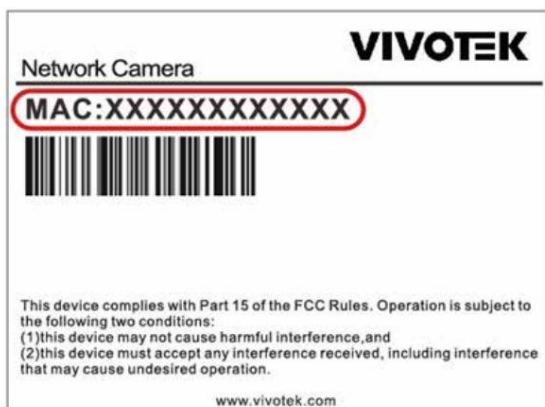
Starten Sie die Geräte-Manager-Anwendung und melden Sie sich an.

Schritt 3.

Klicken Sie auf der Registerkarte „Kamera“ auf „Gerät hinzufügen“, damit der Geräte-Manager Kameras im LAN erkennt.

Schritt 4.

Wählen Sie die Kamera anhand ihrer MAC-Adresse aus und klicken Sie anschließend auf Hinzufügen.



Notiz:

Hier können Benutzer auch die IP-Adresse der Kamera notieren und diese direkt in einen Browser eingeben, um auf die Web-Benutzeroberfläche der Kamera zuzugreifen.

Los geht's!

Schritt 5.

Doppelklicken Sie auf das Kameraelement, das Sie bedienen möchten. Daraufhin öffnet sich die Web-Benutzeroberfläche der Kamera im Browser.

Camera		NVR	Others	             										Q Search
Status	Model		Host Name		IP		MAC		Firmware					
 Unauthorized	FD9199-H				10.42.2.45		0002D1B5CB8F		1.2402.43.01f					

Los geht's!

Verwendung von Shepherd zum Auffinden und Identifizieren von Kameras im LAN

Das Shepherd-Dienstprogramm ist ein Installations- und Verwaltungstool, das die Konfiguration mehrerer Kameras vereinfacht. Mit diesem Tool kann automatisch im Netzwerk nach Kameras gesucht, IP-Adressen zugewiesen, Verbindungen angezeigt, Firmware-/Software-Updates verwaltet und mehrere Kameras gleichzeitig konfiguriert werden.

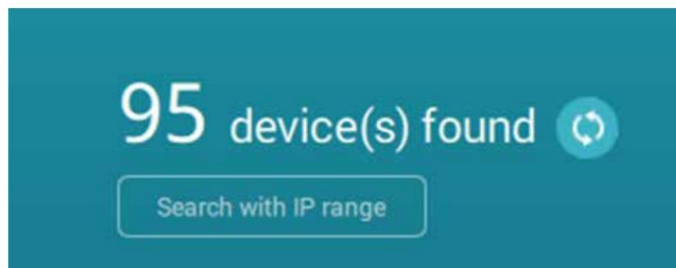
Hier können Benutzer mithilfe des Geräte-Managers die IP-Adresse der Kamera ermitteln, die sie in ihrem lokalen Netzwerk betreiben möchten.

Schritt 1. Laden Sie die Shepherd-Anwendung von der offiziellen VIVOTEK-Website herunter und extrahieren Sie sie. (<https://www.vivotek.com/products/software/shepherd>)

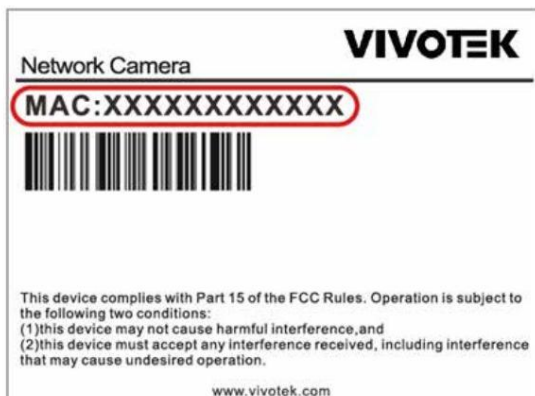
Schritt 2. Suchen und starten Sie die Shepherd-Anwendung.



Schritt 3. Klicken Sie auf das Aktualisierungssymbol, um alle Geräte im LAN zu erkennen.



Schritt 4. Wählen Sie die Kamera anhand ihrer MAC-Adresse aus und doppelklicken Sie darauf. Die Web-Benutzeroberfläche der Kamera wird im Browser geöffnet.



Notiz:

Hier können Benutzer auch die IP-Adresse der Kamera notieren und diese direkt in einen Browser eingeben, um auf die Web-Benutzeroberfläche der Kamera zuzugreifen.

Los geht's!

Verwendung der Kamera-Weboberfläche für den erstmaligen Zugriff

Ein neues Passwort für den Root-Benutzer festlegen

Beim erstmaligen Zugriff auf die Web-Oberfläche der Kamera müssen Benutzer ein neues Passwort für das Standard-Root-Konto festlegen. Bei Bedarf können sie an dieser Stelle auch die Passwortrichtlinie für alle Benutzer der Web-Oberfläche der Kamera anpassen.

Schritt 1. Geben Sie im Feld „Passwort“ das neue Passwort für das Root-Konto ein, das von nun an als Root-Anmeldepasswort verwendet werden soll.

Notiz:

An dieser Stelle können Benutzer auf das Bearbeitungssymbol klicken, um die Passwortrichtlinie für alle Benutzer beim Festlegen von Passwörtern in der Web-Benutzeroberfläche der Kamera zu konfigurieren.

The image shows two side-by-side screenshots from a web interface. The left screenshot is titled 'Set new password' and contains fields for 'User name' (with 'root' entered), 'Password' (with a placeholder 'Enter password' and a toggle icon), 'Confirm Password' (with a placeholder 'Re-enter password' and a toggle icon), and a checkbox for 'Block account when consecutive login fails is detected' which is checked. At the bottom, there is a language dropdown menu set to 'English'. The right screenshot is titled 'Password Policy' and has a close button (X) in the top right corner. It contains the text 'Design your password policy with the following rules' and a progress bar. Below the progress bar are several rules with checkboxes: 'At least 8~64 characters with no spaces.' (checked), 'At least one alphabetic character' (checked), 'At least one special character including !%-.@^_~' (unchecked), 'At least one numeric character' (checked), 'At least one lowercase character' (unchecked), 'At least one uppercase character' (unchecked), and 'Prohibition of a password that is the same as the username' (unchecked). At the bottom right of this panel are 'Save' and 'Cancel' buttons.

Schritt 2. Geben Sie das neue Passwort zur Bestätigung im Feld „Passwort bestätigen“ erneut ein.

Schritt 3. Prüfen Sie, ob der Mechanismus „Konto sperren, wenn mehrere Anmeldefehler gleichzeitig auftreten“ aktiviert ist.

Notiz:

Standardmäßig wird das Konto für 300 Sekunden gesperrt, wenn das Passwort innerhalb von 20 Sekunden fünfmal hintereinander falsch eingegeben wird. Die genauen Einstellungen können später unter System > Benutzerkonten > Kontosperrung angepasst werden.

Schritt 4. Legen Sie die Sprache fest, die in der Web-Benutzeroberfläche der Kamera verwendet werden soll.

Los geht's!

Schritt 5. Bitte lesen Sie die Trend Micro Endbenutzer-Lizenzvereinbarung sorgfältig durch und klicken Sie auf die Schaltfläche „Zustimmen“.



Schritt 6. Klicken Sie auf die Schaltfläche

Anmeldung an der Kamera-Weboberfläche Nach dem

Festlegen des neuen Passworts kann sich der Benutzer bei der ersten Verwendung mit dem Root-Konto an der Kamera-Weboberfläche anmelden.

Schritt 1. Verwenden Sie das Root-Konto und das zugehörige Passwort, um sich beim ersten Zugriff auf die Web-Benutzeroberfläche der Kamera anzumelden.

Login

User name

root

Password

.....



Language

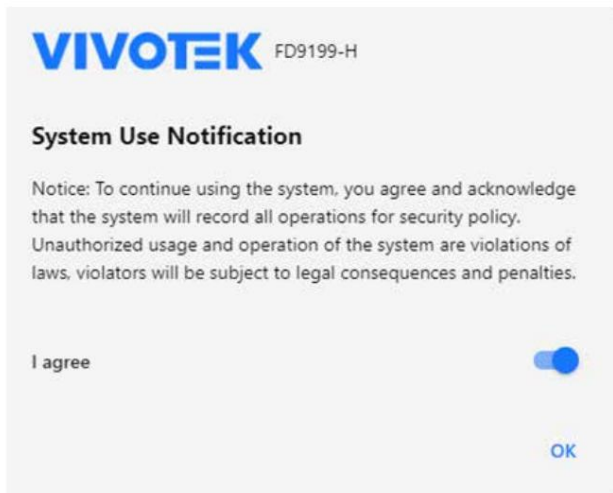
English



Login

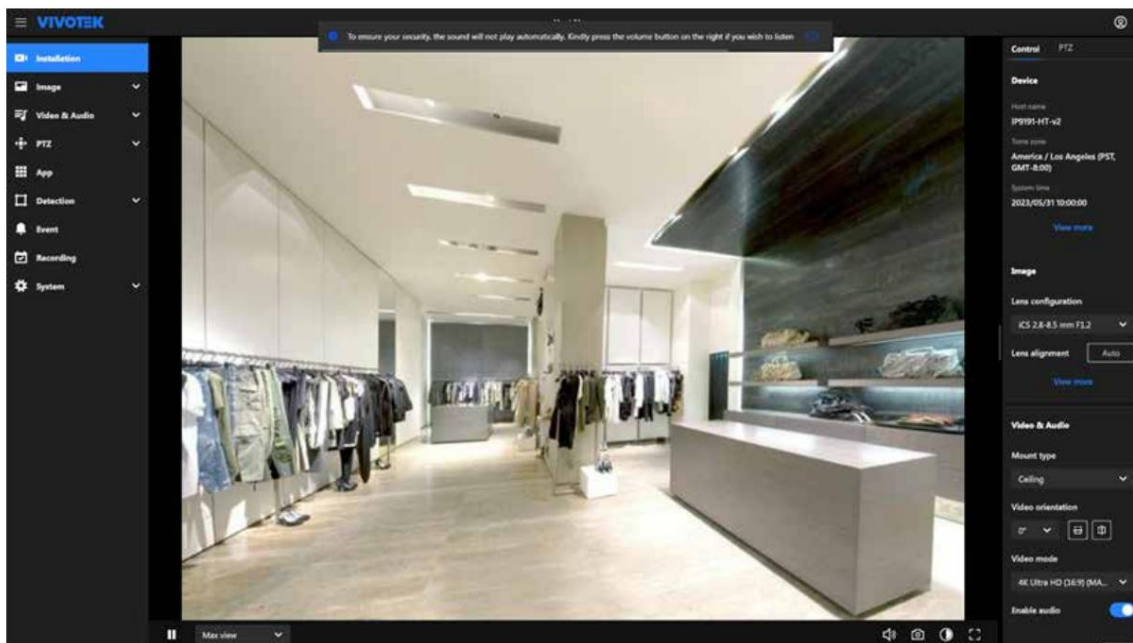
Los geht's!

Schritt 2. Nachdem Sie auf die Web-Benutzeroberfläche der Kamera zugegriffen haben, lesen Sie bitte die **Systemnutzungsbenachrichtigung** sorgfältig durch und stimmen Sie deren Inhalt zu, bevor Sie mit der Konfiguration und dem Betrieb der Kamera über die Web-Benutzeroberfläche der Kamera fortfahren.



Sicherheitshinweis zur Audiowiedergabe:

Die Sicherheitsbenachrichtigung für die Audiowiedergabe dient dem Schutz der Privatsphäre und Sicherheit, indem sie verhindert, dass beim Aufrufen einer Videostreaming-Seite automatisch Audio abgespielt wird.



Die Benachrichtigung erscheint, wenn sich ein Benutzer bei der VIVOTEK Kamera-Weboberfläche mit aktivem Videostreaming anmeldet, um insbesondere eine unbeabsichtigte Audiowiedergabe ohne Zustimmung zu verhindern.

Los geht's!

 To ensure your security, the sound will not play automatically. Kindly press the volume button on the right if you wish to listen 

Wenn der Benutzer keine Aktion ausführt, verschwindet die Benachrichtigung nach 20 Sekunden automatisch; wenn der Benutzer jedoch auf die Lautstärketaste (Symbol) klickt, um den Ton zu aktivieren, verschwindet die Benachrichtigung sofort.

Notiz:

Wenn mehrere Benachrichtigungen gleichzeitig erscheinen (z. B. Erfolgs- oder Fehlermeldungen), werden diese zusätzlichen Benachrichtigungen unterhalb der Hauptmeldung angezeigt, ohne diese Sicherheitsbenachrichtigung zu überschreiben oder zu verdecken.

Einführung in die Web-Benutzeroberfläche der Kamera

Die Web-Benutzeroberfläche der Kamera besteht im Wesentlichen aus drei Teilen: der Titelleiste, der Navigationsleiste und der Inhaltsanzeige.

● Die Titelleiste

Dient primär als Titelanzeige für die Web-Benutzeroberfläche der Kamera und ermöglicht es Benutzern, diese schnell zu identifizieren. Die Funktionen sind von links nach rechts wie folgt angeordnet.



Menü-Ein-/Ausklapptaste

Ermöglicht die Steuerung des Ein- und Ausklappens von Menüs, um die Anzeige von Bildinhalten oder Einstellungen in der Benutzeroberfläche zu maximieren und so ein besseres Benutzererlebnis bei der Bedienung der Kamera zu gewährleisten.

Logo

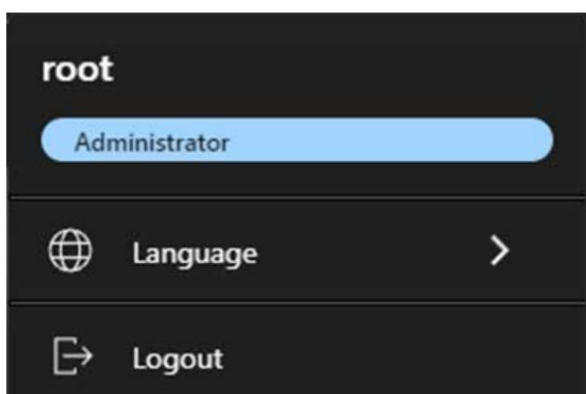
Durch Klicken auf das VIVOTEK-Logo gelangen Nutzer schnell zur offiziellen VIVOTEK-Website, um weitere Produktinformationen zu erhalten. Nutzer können das angezeigte Logo und den Link auch unter **System > Design > Logo anpassen**.

Hostname

Die Web-Benutzeroberfläche der Kamera zeigt den Modellnamen als Standard-Hostnamen an. Benutzer können unter **System > Gerät > Informationen** den Namen in einen aussagekräftigeren Namen ändern.

Kontoinformationen

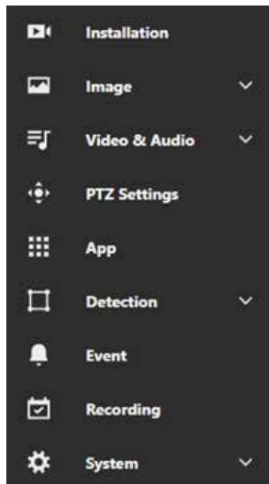
Benutzer können hier die aktuellen Anmeldeinformationen und die zugehörigen Rollenberechtigungen einsehen. Sie können außerdem jederzeit die Systemsprache an ihre Präferenzen anpassen.



Los geht's!

• Die Navigationsleiste

Die Funktionen und Einstellungen innerhalb der Web-Benutzeroberfläche der Kamera sind zentral kategorisiert, damit die Benutzer die gewünschten Konfigurationselemente schnell finden können.



Installation

Der Abschnitt „Installation“ hilft dem Benutzer bei der Einrichtung und Feinabstimmung der Kamera, indem er Optionen für Positionierung, Fokus und Erstkonfiguration bietet, um eine korrekte Ausrichtung und Funktion zu gewährleisten.

Bild

Im Bereich „Bild“ können Benutzer die Bildqualität und das Erscheinungsbild anpassen, einschließlich Einstellungen für Helligkeit, Kontrast, Sättigung, Schärfe, Belichtung, Weißabgleich und Ausrichtung, um eine optimale Videoausgabe zu gewährleisten.

Video & Audio

Im Bereich Video & Audio können Benutzer Videoeinstellungen wie Auflösung, Bitrate, Bildrate und Codecs konfigurieren sowie Audiooptionen wie das Aktivieren der Aufnahme, die Auswahl von Codecs und die Konfiguration von Mikrofon- oder Lautsprechereinstellungen verwalten.

PTZ-Einstellungen

Im Abschnitt PTZ-Einstellungen können Benutzer Schwenk-, Neige- und Zoomfunktionen verwalten, indem sie Bewegungsgeschwindigkeit, voreingestellte Positionen und Patrouillenmuster konfigurieren, um eine präzise und reibungslose Kamerasteuerung zu gewährleisten.

App

Im Bereich „App“ können Benutzer VIVOTEK-spezifische Anwendungen oder Plugins verwalten und mithilfe dieser Anwendungen die Funktionalität der Kamera erweitern.

Detektion

Der Bereich „Erkennung“ nutzt KI-gestützte Algorithmen für umfassende Überwachungsfunktionen, darunter intelligente VCA-Funktionen wie Linienüberschreitungs-, Einbruchs- sowie Bewegungs-, Geräusch-, Erschütterungs- und Manipulationserkennung. Benutzer können Erkennungszonen, Empfindlichkeit und Ereignisauslöser konfigurieren, um eine präzise, intelligente Überwachung und erhöhte Sicherheit in verschiedenen Szenarien zu gewährleisten.

Los geht's!

Ereignis

Im Abschnitt „Ereignisse“ können Benutzer Ereignisauslöser und -bedingungen definieren und Aktionen wie das Senden von Benachrichtigungen, das Aufzeichnen von Videos oder das Aktivieren von Alarmen konfigurieren, um effektiv auf bestimmte Ereignisse zu reagieren.

Aufnahme

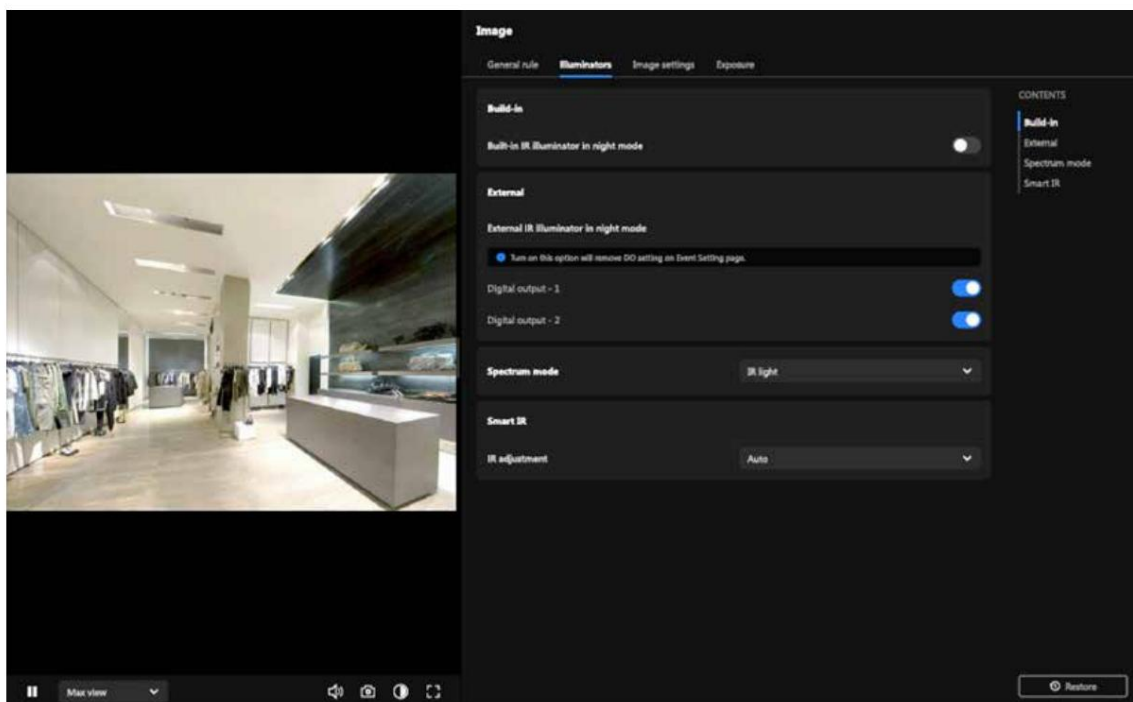
Im Abschnitt „Aufnahme“ können Benutzer Aufnahmemodi konfigurieren, z. B. kontinuierliche, ereignisbasierte oder zeitgesteuerte Aufnahme, und Speicherorte wie SD-Karten oder Netzwerkspeicher festlegen, um das Videomaterial effizient zu verwalten.

System

Der Systembereich bietet Werkzeuge zur Verwaltung von Geräteeinstellungen, Netzwerkkonfigurationen, Benutzerkonten, Wartungsaufgaben, Speicheroptionen, Protokollen und zur Anpassung der Benutzeroberfläche, um optimale Leistung, Sicherheit und Benutzerfreundlichkeit der Kamera zu gewährleisten.

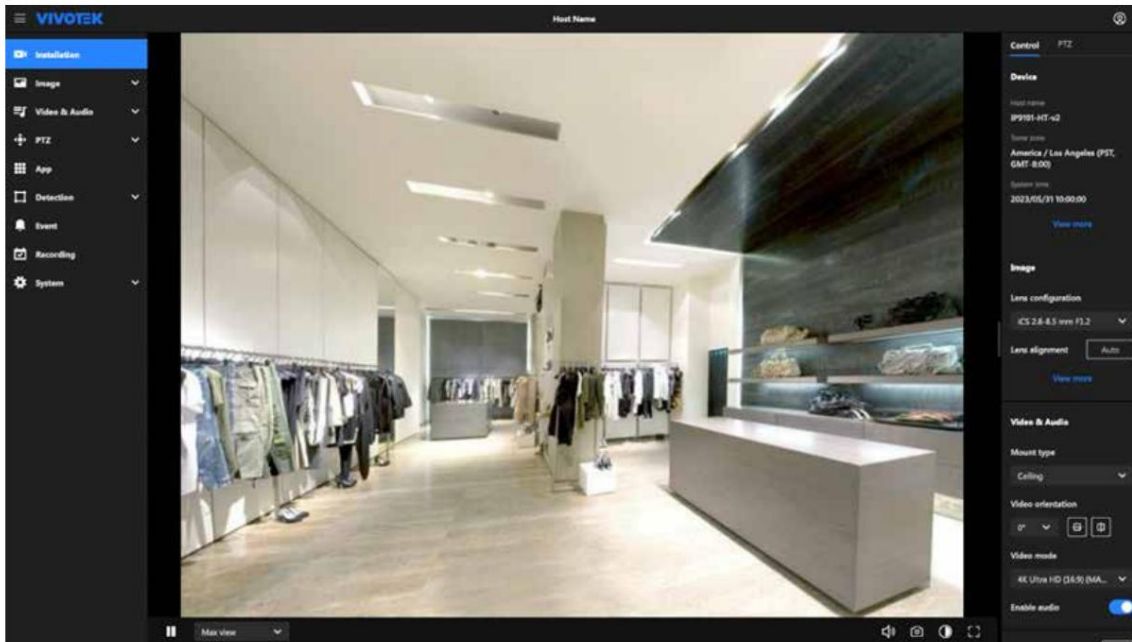
● Die Inhaltsanzeige

Dieser Bereich dient als Hauptarbeitsbereich der Web-Benutzeroberfläche der Kamera. Layout und Inhalt ändern sich je nach den in der Navigationsleiste ausgewählten Kategorien. Die folgenden Bedienungshinweise in diesem Dokument beziehen sich hauptsächlich auf diesen Abschnitt.



Installation

Diese Kategorie dient als erste Ansicht beim Aufrufen der Web-Benutzeroberfläche der Kamera. Ihr Hauptzweck ist es, Benutzern nach der Installation der Kamera zu helfen, die gewünschte Überwachungsansicht unter der Kategorie „Installation“ schnell und bequem einzurichten.



Navigation in der Videostream-Symboleiste für verbesserte Steuerung

Die Videostream-Symboleiste befindet sich am unteren Rand der Web-Benutzeroberfläche der Kamera und bietet Nutzern verschiedene Funktionen, die während des Videostreamings in Echtzeit verwendet werden können. Die Funktionen sind von links nach rechts wie folgt angeordnet.



Pause-/Wiedergabetaste

Wenn Nutzer die im Videostream angezeigten Details ansehen oder bestätigen möchten, können sie die Wiedergabe jederzeit durch Drücken der Pause-Taste anhalten. Durch erneutes Drücken der **Wiedergabe**-Taste wird die Videowiedergabe fortgesetzt.

Medienprofilmenü

Nutzer können je nach Bedarf schnell zwischen den drei verschiedenen Medienprofilen – **Aufnahme**, **Live-Ansicht** und **App-Ansicht** – wechseln und so den Zeitaufwand für die Videoeinstellungen reduzieren. Zudem können Nutzer unter „**Video & Audio** > **Medienprofil**“ Medienprofile hinzufügen oder bearbeiten.

Lautstärkeregelung

Die Nutzer können die Lautstärke des Videostreams ihren Bedürfnissen entsprechend anpassen.

Installation

Schnappschuss-

Schaltfläche: Benutzer können jederzeit Bilder aus dem Videostream aufnehmen.

Umschaltung zwischen

Nacht- und Tagmodus: Je nach Situation (Nacht oder Tag) können Benutzer die Videostream-Anzeige in den Schwarzweiß- oder Farbmodus umschalten.

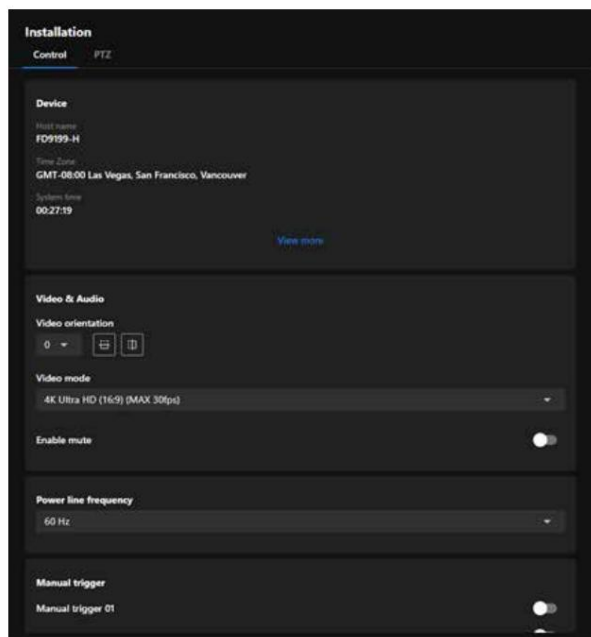
Vollbildanzeige

Benutzer können das Videostreambild im Vollbildmodus anzeigen.

Installation

Effiziente Anpassung der Kameraeinstellungen über das Installationspanel

Das Installationspanel bietet häufig verwendete und wichtige Informationen sowie schnell anpassbare Einstellungen, um Benutzern die Installation und Einrichtung der Kamera effizienter und komfortabler zu gestalten. Darüber hinaus werden die angepassten Einstellungen sofort im Videostream angezeigt.

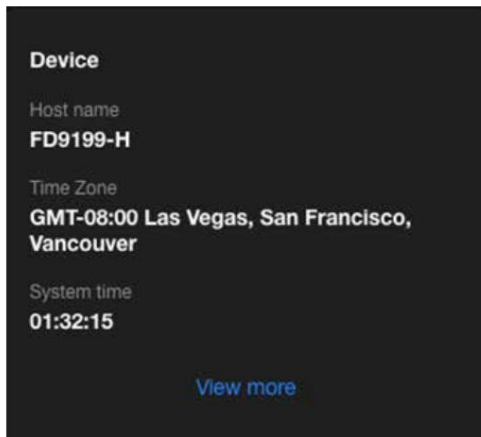


Bedienfeld

Wesentliche Einstellungen und Funktionen, die während des Kamerainstallationsprozesses erforderlich sind, sind in das Bedienfeld integriert, um sicherzustellen, dass die Benutzer die gewünschten Anzeigeeffekte während der Installation der Kamera sehen können.

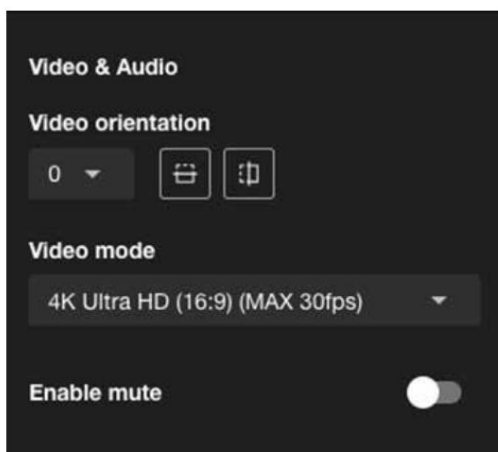
Installation

● Gerät:



Die Gerätekarte dient als Schnellübersicht wichtiger Geräteinformationen und hilft Benutzern sicherzustellen, dass die Identität, Zeitzone und Systemzeit der Kamera für einen reibungslosen Betrieb und die Ereignisverfolgung korrekt konfiguriert sind. Durch Klicken auf „Mehr anzeigen“ gelangen Sie zu System > Gerät > Informationen, wo Sie weitere Einstellungen vornehmen können.

● Video & Audio:



Installation

Videoausrichtung

Die Kamera kann vertikal, seitlich oder geneigt montiert werden, um sich an die Innen- oder Außengestaltung eines Gebäudes anzupassen. Der Innenraum eines Gebäudes kann beispielsweise ein schmaler, rechteckiger Raum wie ein Korridor sein. Ein herkömmliches HD-Bild, etwa im 16:9-Format, wirkt aufgrund seines breiten horizontalen Bildausschnitts unter Umständen unpassend. Durch die Videorotation kann die Kamera den Bildausschnitt in hohen und schmalen Räumen effektiver erfassen.

Drehen	Die hier angegebene Drehung erfolgt im Uhrzeigersinn. Die Drehung kann durch Spiegeln, Umklappen und die Drehung der Linse an verschiedene Montageorte angepasst werden.
Umdrehen	Das Live-Videobild vertikal spiegeln.
Spiegel	Das Live-Videobild horizontal spiegeln.

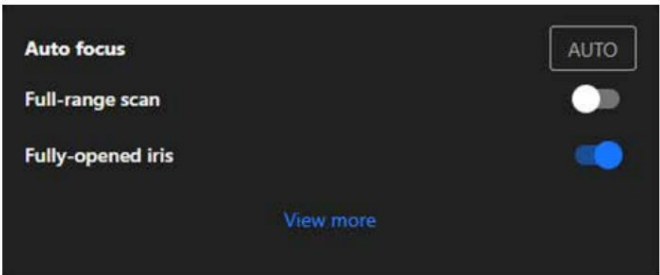
Videomodus

Bezeichnet die Bildverarbeitungsmodi, die von IP-Kameras während der Videoaufnahme und -übertragung verwendet werden. Diese Modi werden je nach Überwachungsumgebung, Netzwerkbandbreite, Speicherbedarf und Anwendungsszenario angepasst, um Bildschärfe und -glätte zu verbessern und so unter verschiedenen Netzwerkbedingungen optimale Leistung und Effizienz zu erzielen.

Stummschaltung aktivieren

Bietet die Möglichkeit, die Audioaufnahme zu aktivieren oder zu deaktivieren. Durch Aktivieren der Funktion wird der Kameraton stummgeschaltet, um jegliche Audioaufnahme zu verhindern.

● **Autofokus (Die Fokuseinstellungen werden nur von VIVOTEK-Zoomkameras des Typs EHTV unterstützt)**



Die Autofokus-Karte in der Kategorie „Installation“ bietet benutzerfreundliche Optionen für schnelle und erweiterte Fokuseinstellungen und gewährleistet so, dass die Kamera unter verschiedensten Installations- und Umgebungsbedingungen klare Bilder aufnimmt. Für detailliertere Anpassungen können Benutzer über den Link „Mehr anzeigen“ auf zusätzliche Einstellungen zugreifen.

Autofokus

Die Autofokus-Funktion ist eine Ein-Klick-Funktion, die die Brennweite der Kamera automatisch anpasst, um das schärfste Bild zu liefern. Dadurch eignet sie sich perfekt für schnelles Einrichten und allgemeines Fokussieren.

Installation

Vollbereichsscan

Die Funktion „Vollbereichsscan“ ermöglicht der Kamera einen umfassenden Scan über den gesamten Brennweitenbereich, um den optimalen Fokuspunkt zu ermitteln. Dadurch werden alle möglichen Fokusdistanzen ausgewertet und somit die bestmögliche Bildschärfe erzielt. Ist die Funktion aktiviert, dauert der Scan etwa 30 bis 80 Sekunden. Ist sie deaktiviert, beschränkt die Kamera die Suche auf den Bereich, in dem der Fokus am wahrscheinlichsten liegt, wodurch sich die Scanzeit auf etwa 15 bis 20 Sekunden reduziert. Der Vollbereichsscan ist besonders vorteilhaft bei der Erstinstallation oder wenn die Kamera ihre Fokuseinstellungen komplett neu kalibrieren muss. Er gewährleistet präzise und zuverlässige Leistung über alle Entfernungen hinweg.

Vollständig geöffnete Iris

Die Option „Vollständig geöffnete Blende“ sorgt dafür, dass die Kamera während des Autofokusvorgangs mit vollständig geöffneter Blende arbeitet. Dadurch wird die Schärfentiefe verringert und der Fokuspunkt präziser bestimmt. Diese Funktion verbessert die Fokusgenauigkeit, insbesondere bei schwachem Licht oder in Situationen, die eine detaillierte Fokussierung erfordern. Sie eignet sich daher ideal für Umgebungen, in denen eine hohe Fokussiergenauigkeit entscheidend ist, wie beispielsweise bei schlechten Lichtverhältnissen oder beim Fotografieren feinsten Details.

Schritte zur Bedienung des Autofokus:

Schritt 1. Fokusmodus auswählen

Für schnelles Fokussieren:

Stellen Sie sicher, dass die Option „Vollbereichsscan“ deaktiviert ist.

In diesem Modus scannt der Autofokus nur den Bereich, in dem eine optimale Fokussierung wahrscheinlich ist; dies dauert etwa 15 bis 20 Sekunden.

Präziser Fokus:

Aktivieren Sie die Option „Vollbereichsscan“.

Die Kamera führt einen vollständigen Scan über ihre gesamte Brennweite durch, was je nach Brennweitenbereich 30 bis 80 Sekunden dauern kann.

Schritt 2. Iris-Modus einstellen

Es wird empfohlen, die Option „Vollständig geöffnete Iris“ zu aktivieren.

Bei vollständig geöffneter Iris wird die Fokussiergenauigkeit durch Minimierung der Schärfentiefe verbessert, insbesondere bei schwachem Licht oder beim Fokussieren auf feine Details.

Schritt 3. Autofokus starten

Klicken Sie auf die Schaltfläche „AUTO“, um den Autofokus-Prozess zu starten.

Die Kamera passt ihren Fokus je nach gewähltem Fokusmodus (Schnellfokus oder Präziser Fokus) und der Blendenöffnung (vollständig geöffnete Blende oder geschlossen) an, um eine optimale Bildschärfe zu gewährleisten.

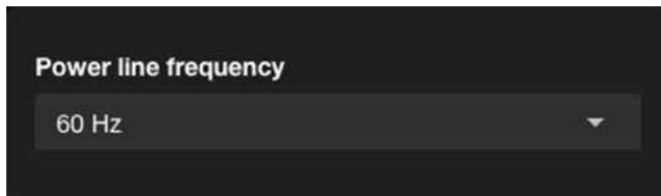
Schritt 4. Zugriff auf die erweiterten Einstellungen

Für weitere Anpassungen klicken Sie auf die Schaltfläche „Mehr anzeigen“, um zur Seite „Bild > Fokuseinstellungen“ zu gelangen.

Auf dieser Seite können Sie den Fokus manuell feinjustieren, den Fokusbereich anpassen und weitere erweiterte Parameter wie die Fokusgeschwindigkeit konfigurieren.

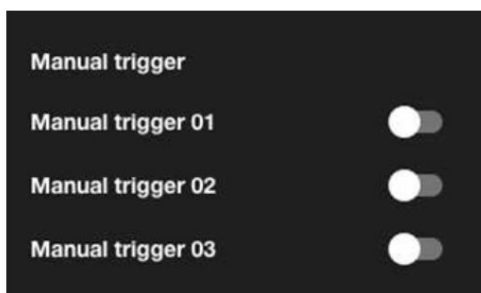
Installation

- **Netzfrequenz:**

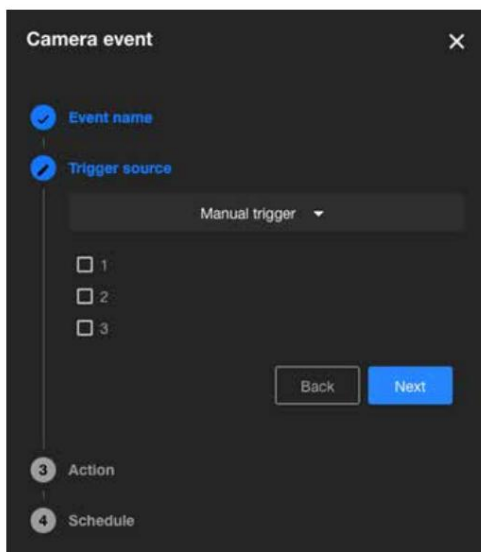


Die Einstellung der Netzfrequenz gewährleistet eine stabile Videoqualität, indem sie es dem Benutzer ermöglicht, die Frequenz der Kamera an das örtliche Stromnetz anzupassen und so ein Flimmern in Bereichen mit Leuchtstoffröhren oder künstlicher Beleuchtung wirksam zu verhindern. Die Auswahl der richtigen Frequenz, z. B. 60 Hz für Nordamerika oder 50 Hz für viele europäische und asiatische Länder, trägt dazu bei, durch Netzstörungen verursachtes Videoflimmern zu eliminieren.

- **Manueller Auslöser:**

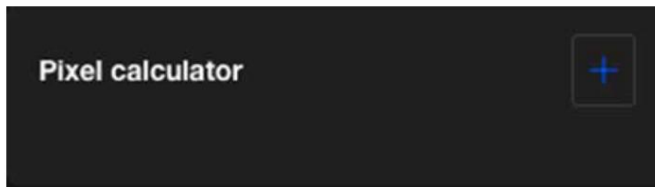


Ermöglicht Benutzern die manuelle Aktivierung von Ereignisauslösern durch Klicken auf den Ein-/Ausschalter im Installationsfenster. Bevor Sie diese Funktion verwenden, fügen Sie bitte Ereignisse hinzu, die mit den manuellen Auslösern 01 bis 03 in der Kategorie „Ereignisse“ verknüpft sind.

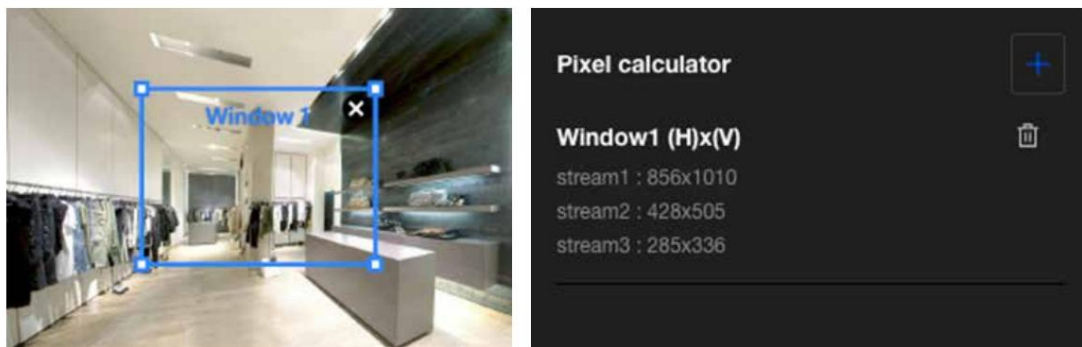


Installation

- **Pixelrechner:**



Klicken Sie auf die Schaltfläche „Hinzufügen“, um ein Fenster für die Pixelberechnung zu erstellen. Bewegen Sie den Cursor über das Fenster, um es im gewünschten Bereich zu positionieren, und passen Sie die Fenstergröße an. Sobald das Fenster konfiguriert ist, wird die Pixelanzahl an seinen Rändern angezeigt. Dies hilft Ihnen zu beurteilen, ob die aktuelle Konfiguration den Anforderungen entspricht.



Mithilfe dieses visuellen Werkzeugs können Sie den Abdeckungsbereich und die Entfernung zum Ziel abschätzen sowie ein Lineal oder ein Objekt bekannter Größe platzieren. Anschließend können Sie einen Berechnungsrahmen zeichnen, der den relevanten Bereich abdeckt. Die berechneten Werte werden am unteren Bildschirmrand angezeigt und helfen Ihnen festzustellen, ob die aktuellen Einstellungen die Anforderungen an die Pixelanzahl erfüllen.

Installation

PTZ-Panel

Das PTZ-Bedienfeld bietet dem Benutzer eine komfortable Möglichkeit, die Position des überwachten Bildes durch Bedienen der Schwenk-, Neige- und Zoomfunktionen anzupassen und schnell zwischen voreingestellten Positionen zu wechseln, um wichtige Bereiche zu überwachen; die PTZ-Funktion wird jedoch nur bei den Medienprofilen 2 und 3 unterstützt, und der Benutzer muss einen unterstützten Stream auswählen, damit sie funktioniert.

● PTZ-Steuerung:



Joystick

Benutzer können den Bildausschnitt des überwachten Bereichs mithilfe des Joysticks verschieben und so den gewünschten Überwachungsbereich auswählen. Durch Drücken der **Home**-Taste wird die Ansicht auf die voreingestellte Ausgangsposition zurückgesetzt. Die Ausgangsposition kann unter **PTZ-Einstellungen > Ausgangsposition & Voreinstellungen festgelegt werden.**

Zoom

Mit der Zoom-Schaltfläche können Benutzer die Ansicht des aktuellen Überwachungsbildschirms beliebig vergrößern oder verkleinern.

Pan & Patrol

Wenn der Benutzer auf die Schaltfläche „**Schwenk**“ klickt, bewegt sich der Überwachungsbildschirm nach links und rechts und zentriert sich dabei auf die aktuelle Ansicht, um den Überwachungsbereich zu erweitern. Durch Klicken auf die Schaltfläche „**Patrouille**“ fährt der Überwachungsbildschirm nacheinander die einzelnen Beobachtungspunkte gemäß der voreingestellten Reihenfolge und den voreingestellten Zeitintervallen an und ermöglicht so die automatische Überwachung mehrerer Bereiche. Benutzer können die gewünschten voreingestellten Positionen und Zeitintervalle für die Patrouille auf der **Seite „PTZ-Einstellungen > Patrouille“ konfigurieren.** Klicken Sie auf die Schaltfläche „**Stopp**“, um das Schwenken oder die Patrouille des aktuellen Überwachungsbildschirms zu beenden.

Voreinstellung

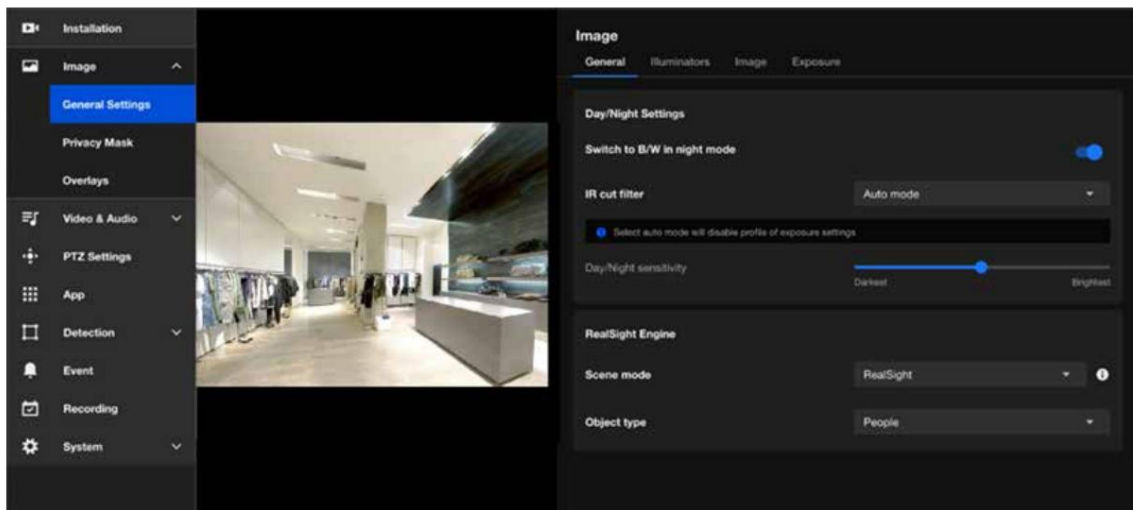
Benutzer können die aktuelle Überwachungsperspektive schnell wechseln, indem sie einen als Voreinstellung festgelegten Bildschirm auswählen. Die Positionen der Voreinstellungen können auf der Seite „**PTZ-Einstellungen > Startseite & Voreinstellungen**“ konfiguriert werden.

Bild

Die Bildbearbeitungssoftware bietet verschiedene Optionen zur Bildanpassung, darunter allgemeine Einstellungen, Datenschutzmaskierung und Overlays, um den Anforderungen unterschiedlicher Anwendungsfälle gerecht zu werden. Diese Einstellungen können die Bildqualität verbessern, die Privatsphäre schützen und zusätzliche Informationen hinzufügen.

Bildqualität mit VIVOTEK-Kameraeinstellungen optimieren

Die allgemeinen Bildeinstellungen dienen in der Regel dazu, die Parameter von Kameras oder Bildverarbeitungssystemen anzupassen und zu optimieren, um sicherzustellen, dass die erzeugten Bilder den erforderlichen Spezifikationen entsprechen. Diese Einstellungen lassen sich in vier Hauptkategorien unterteilen: Allgemein, Beleuchtung, Bild und Belichtung. Im Folgenden finden Sie eine kurze Einführung in jede Kategorie.



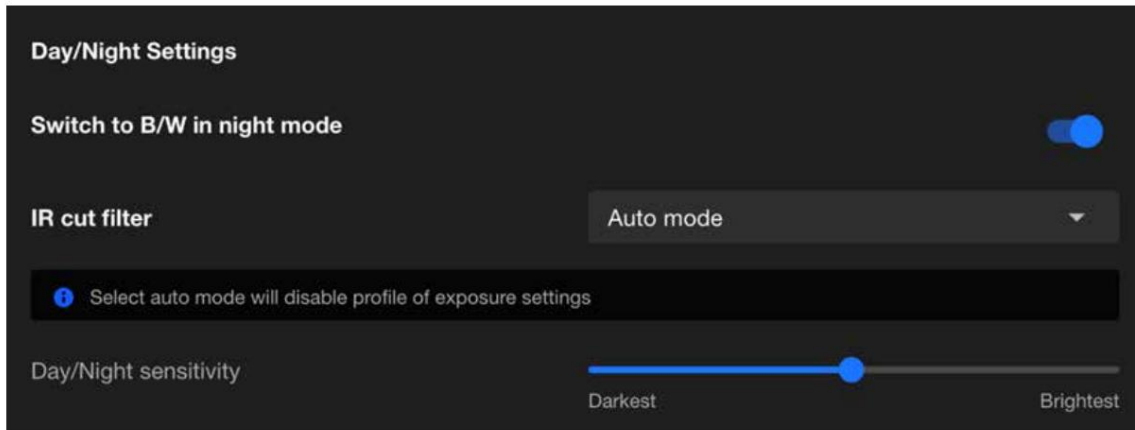
Allgemein

Auf der Seite „Allgemein“ finden Benutzer wichtige Funktionen zur Anpassung der Bildqualität, um eine optimale Kameraleistung in verschiedenen Umgebungen zu gewährleisten.

Bild

- **Tag-/Nacht-Einstellungen**

Die Tag-/Nacht-Einstellungen dienen dazu, die Bildqualität der Kameras unter verschiedenen Lichtverhältnissen zu verbessern.



Im Nachtmodus auf Schwarzweiß umschalten

Nach Aktivierung dieser Funktion schaltet die Kamera im Nachtmodus automatisch auf Schwarzweißdarstellung um.

Dieses Design zielt darauf ab, Bildschärfe und Kontrast bei schwachen Lichtverhältnissen zu verbessern und so auch bei unzureichender Beleuchtung klare Überwachungsaufnahmen zu gewährleisten.

IR-Sperrfilter

Der IR-Sperrfilter ist ein abnehmbarer Filter, der tagsüber Infrarotlicht vom Bildsensor fernhält, um Farbverzerrungen zu vermeiden. Im Nachtmodus entfernt die Kamera diesen Filter automatisch und lässt Infrarotlicht auf den Bildsensor durch. Dies arbeitet mit der integrierten oder externen Infrarotbeleuchtung zusammen, um die Bildempfindlichkeit bei schwachem Licht oder Dunkelheit zu verbessern und so klarere Nachtaufnahmen zu ermöglichen.

Folgende Betriebsmodi stehen für den IR-Sperrfilter zur Verfügung:

- **Automatikmodus (Durch Auswahl des Automatikmodus werden die Belichtungseinstellungen deaktiviert)**

Die Netzwerkkamera entfernt den Filter automatisch, indem sie die Stärke des Umgebungslichts beurteilt.

- **Tagmodus**

Im Tagesmodus schaltet die Netzwerkkamera den IR-Sperrfilter permanent ein, um zu verhindern, dass Infrarotlicht den Sensor erreicht und die Farben verfälscht werden.

- **Nachtmodus**

Im Nachtmodus schaltet die Netzwerkkamera den IR-Sperrfilter permanent ab, damit der Sensor Infrarotlicht aufnehmen kann. Dies trägt zur Verbesserung der Lichtempfindlichkeit bei.

- **Synchronisierung mit digitalem Eingang**

Wenn ein externes IR-Gerät mit eigenem Lichtsensor angeschlossen ist, kann dessen digitaler Eingang zur Auslösung des IR-Sperrfilters verwendet werden. Dadurch lässt sich die Lichtstärkemessung zwischen Kamera und externem IR-Gerät synchronisieren.

- **Zeitplanmodus**

Die Netzwerkkamera wechselt gemäß einem festgelegten Zeitplan zwischen Tag- und Nachtmodus. Geben Sie die Start- und Endzeit für den Tagmodus ein. Beachten Sie, dass das Zeitformat [hh:mm] ist und die Uhrzeit im 24-Stunden-Format angegeben wird. Standardmäßig sind Start- und Endzeit des Tagmodus auf 07:00 Uhr und 18:00 Uhr eingestellt.

Bild

Tag-/Nachtempfindlichkeit

Passen Sie die Empfindlichkeit des IR-Sperrfilters an die Lichtverhältnisse von Dunkel bis Hell an.

● RealSight-Engine

RealSight Engine ist eine KI-basierte Bildoptimierungstechnologie, die speziell zur Verbesserung der Videoqualität von Netzwerkkameras unter verschiedenen Lichtverhältnissen entwickelt wurde. Zu ihren wichtigsten Funktionen gehören:

1. Automatische Szenenerkennung und Optimierung

Die RealSight Engine erkennt automatisch die Anwesenheit von Personen im Bild und optimiert die Bilddetails, ohne dass manuelle Anpassungen erforderlich sind, und bietet so ein nahtloses Plug-and-Play-Erlebnis.

2. Klare Erfassung von sich bewegenden Objekten

Es reduziert effektiv Bewegungsunschärfe, die durch sich schnell bewegende Objekte verursacht wird, und stellt sicher, dass alle sich bewegenden Motive mit klaren Details erfasst werden, wodurch die Notwendigkeit manueller Verschlusszeitanpassungen entfällt.

3. Verbesserte Nachtsicht

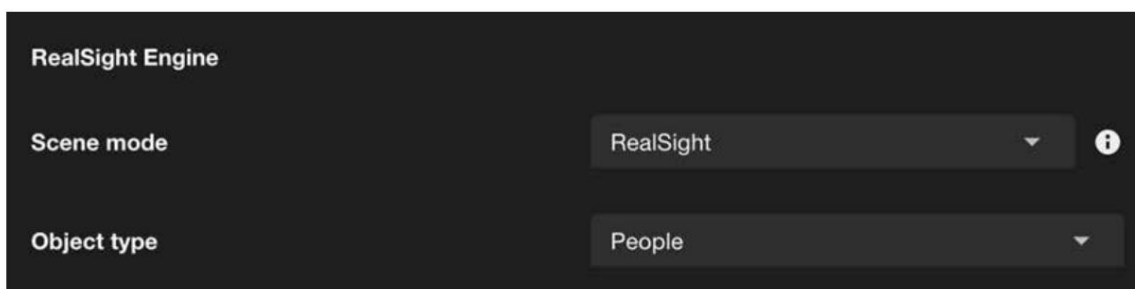
Die Bildverarbeitung verhindert Unschärfen durch Infrarotlichtreflexionen und liefert automatisch klare Nachtaufnahmen und detailreiche Motivmerkmale ohne wiederholte manuelle Belichtungsanpassungen.

4. Verbesserte Sichtbarkeit bei Gegenlicht

Bei schwierigen Gegenlichtsituationen verbessert die RealSight Engine die Helligkeit und Details von Vordergrundmotiven (z. B. Gesichtern) und erhält gleichzeitig die richtige Helligkeit des Hintergrunds bei, wodurch eine klare Sichtbarkeit von Personen auch bei starkem Gegenlicht gewährleistet wird.

5. KI-gestützte Optimierung für überragende Bildqualität

Durch den Einsatz künstlicher Intelligenz passt die RealSight Engine die Kameraeinstellungen dynamisch in Echtzeit an, um die bestmögliche Bildqualität zu erzielen und sich an unterschiedliche Umgebungen und Lichtverhältnisse anzupassen.



Die RealSight Engine verbessert die Überwachungsleistung, indem sie in unterschiedlichsten Szenarien eine überragende Bildqualität gewährleistet und selbst in schwierigen Umgebungen wie schwachem Licht, Gegenlicht oder schnellen Bewegungen wichtige Details erfasst.

Bild

Szenenmodus

Netzwerkcameras, die die RealSight Engine unterstützen, bieten eine „Szenenmodus“-Option, mit der Benutzer je nach den Anforderungen der jeweiligen Überwachungsumgebung die passenden Bildeinstellungen auswählen können.

RealSight	Aktivieren Sie die RealSight Engine-Technologie von VIVOTEK, die mithilfe von KI Szenen automatisch analysiert und die Bildqualität optimiert. Sie eignet sich ideal für Umgebungen mit starken Lichtveränderungen, Gegenlicht oder schwachem Licht und gewährleistet so beste Bildqualität.
Standard	Verwendet die Standardbildeinstellungen der Kamera, ohne spezielle Bildverbesserungstechnologien zu aktivieren. Geeignet für Szenarien mit stabilen Lichtverhältnissen und ohne besondere Anforderungen; liefert Standardbildqualität.

Objektyp

Die RealSight Engine verbessert die Bildqualität ausgewählter Objekttypen. Wählt man beispielsweise „Personen“ als Objekttyp aus, passt die Kamera automatisch Belichtung, Weißabgleich und andere Bildeinstellungen an, um die Klarheit von Personen im Bild zu optimieren.

Illuminatoren

Die Seite „Beleuchtung“ bezieht sich auf die Einstellungen für den Infrarotstrahler (IR-Strahler). Bei schwachem Licht oder völliger Dunkelheit schaltet sich dieser IR-Strahler automatisch ein, um die notwendige Beleuchtung zu gewährleisten und der Kamera klare Bilder zu ermöglichen. Diese Funktion eignet sich besonders für Überwachungsszenarien bei Nacht oder in Umgebungen mit schlechten Lichtverhältnissen.

Bild

• Eingebaut

Die Netzwerkkameras von VIVOTEK sind mit integrierten Infrarot-Strahlern (IR-Strahlern) ausgestattet, die die Bildqualität bei Nacht oder in Umgebungen mit wenig Licht verbessern. Diese integrierten IR-Strahler sorgen für eine gleichmäßige Ausleuchtung und gewährleisten so auch bei Panoramaaufnahmen klare Bilder.



Eingebauter Infrarotstrahler im Nachtmodus

Wenn der eingebaute IR-Strahler im Nachtmodus aktiviert ist, wird er automatisch eingeschaltet, sobald die Kamera schlechte Lichtverhältnisse erkennt und in den Nachtmodus wechselt.

Schutz vor Überbelichtung

Durch die Aktivierung der Anti-Überbelichtungsfunktion wird eine ausgewogene Bildqualität gewährleistet, indem die Belichtung dynamisch an schwierige Lichtverhältnisse angepasst wird. So wird verhindert, dass übermäßig helle Bereiche die Sichtbarkeit oder die Detailerfassung in Überwachungsaufnahmen beeinträchtigen.

RealSight-Engine-Erweiterung

Die KI-gestützte RealSight-Engine liefert eine äußerst realistische Bildwiedergabe und gibt Farben naturgetreu wieder, unbeeinflusst von Umwelteinflüssen. Selbst unter allen Lichtverhältnissen bleiben wichtige Details von Personen mühelos erhalten. Diese Lösung stellt sicher, dass Nutzern kein Detail entgeht und liefert aussagekräftige Bilder für jede Szene – ganz ohne komplizierte Einrichtung. Zu den wichtigsten Funktionen gehören:

• Klare Sichtbarkeit von Personen bei jeder Beleuchtung

Klare Aufnahme bewegter Figuren

Beheben Sie das Problem der Bewegungsunschärfe in zuvor aufgenommenen Bildern, die durch schnelle Personenbewegungen verursacht wurde. Dadurch werden alle Details bewegter Personen erfasst und das Bild automatisch schärfer, ohne dass die Verschlusszeit der Kamera angepasst werden muss.

Bild



Personen sehen, ohne durch Infrarotlichtreflexionen beeinträchtigt zu werden

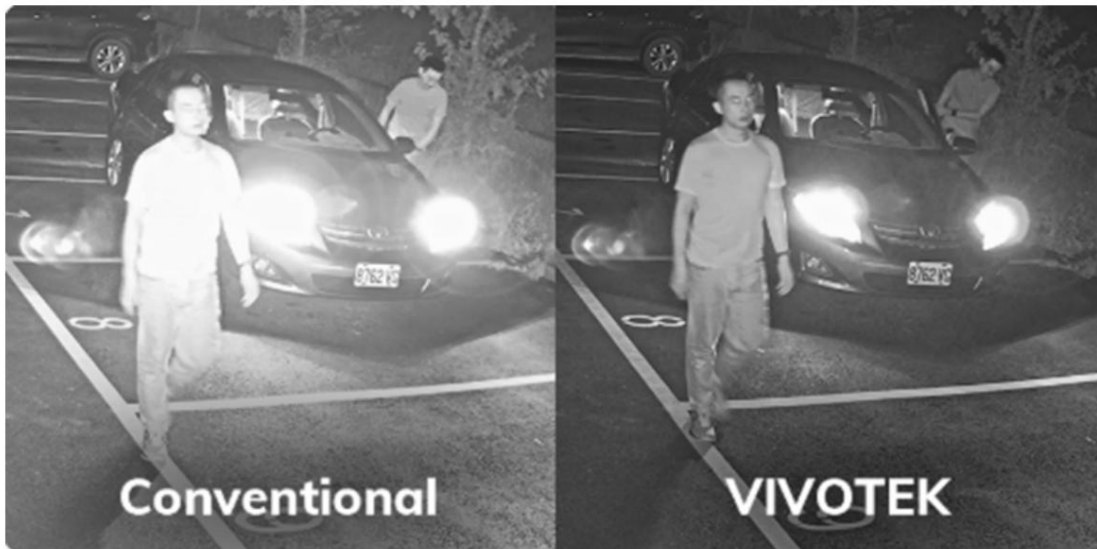
Die RealSight Engine verhindert, dass die Kamera durch Infrarotlicht, das von nahen Objekten reflektiert wird, beeinträchtigt wird, und erfasst automatisch klare Nachtszenen und Personen, ohne dass eine wiederholte manuelle Anpassung der Belichtungszeit der Kamera erforderlich ist.



Bild

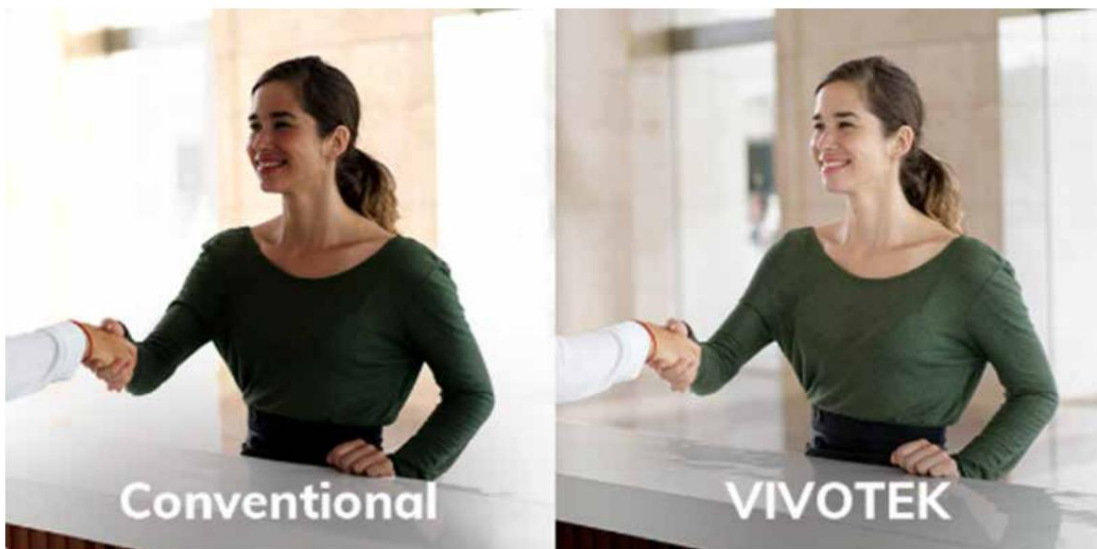
Betrachten Sie Personen, ohne von zusätzlichen Lichtquellen beeinträchtigt zu werden.

Die RealSight-Engine sorgt dafür, dass Kameras nachts nicht durch zusätzliche Lichtquellen beeinträchtigt werden. Sie analysiert die Szene automatisch und ermöglicht so klare Aufnahmen von vorbeigehenden Personen bei Nacht, ohne dass manuelle Anpassungen erforderlich sind.



Porträts sind auch bei Gegenlicht gut sichtbar.

Die RealSight Engine löst das Problem dunkler Porträts bei Gegenlicht. Sie erhält nicht nur die Helligkeit des Hintergrunds, sondern verbessert auch Helligkeit und Details bei Gegenlicht.



Bild

- **Farbtreue Wiedergabe**

- Erfassen und Wiederherstellen echter Farben**

Die RealSight Engine sorgt dafür, dass die Kamera naturgetreue Farben erfasst, ohne von blauen Objekten in der Umgebung beeinträchtigt zu werden. Außerdem entfällt der Zeitaufwand für die manuelle Weißabgleichseinstellung mit weißem Papier.



- Das Filmmaterial bleibt flimmerfrei**

Dank der RealSight Engine wird die Kamera nicht mehr durch das kontinuierliche Flackern von Leuchtstoffröhren oder LED-Interferenzen beeinträchtigt, wodurch Bildstreifen automatisch vermieden werden. Dies reduziert den Bedarf an manuellen Anpassungen der Verschlusszeit an die Umgebungslichtquellen erheblich.
Ist.

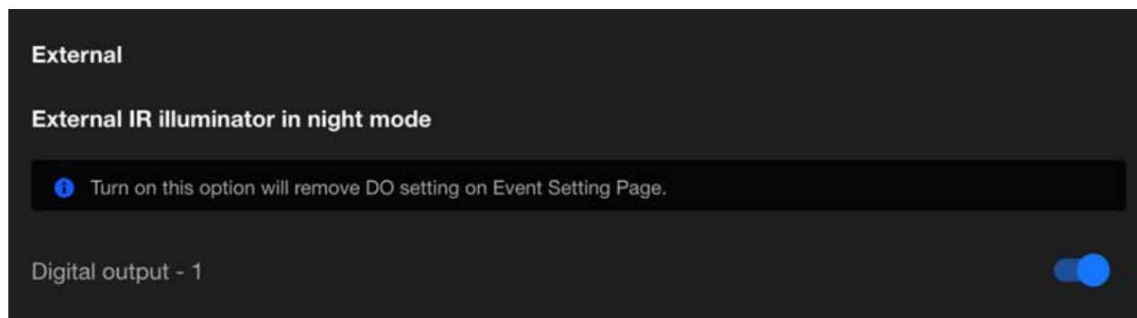


Bild

Stärke

In der RealSight-Engine-Erweiterung steuert die Einstellung der „Stärke“ die Empfindlichkeit bzw. Intensität des Überbelichtungsschutzes. Ein höherer Wert bewirkt, dass das System die Belichtungsparameter proaktiver anpasst, um drastische Lichtveränderungen zu kompensieren, während ein niedrigerer Wert zu sanfteren Anpassungen führt. Dadurch können Benutzer den Überbelichtungsschutz flexibel an die jeweiligen Szenenanforderungen anpassen und so eine optimale Bildqualität gewährleisten.

• Extern

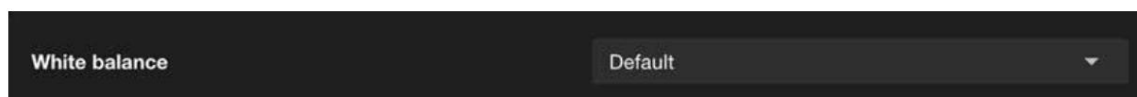


Wenn der externe IR-Strahler im Nachtmodus aktiviert ist, schaltet die Kamera den externen IR-Strahler über den digitalen Ausgang ein. Externe IR-Strahler bieten in der Regel eine höhere Helligkeit oder einen größeren Ausleuchtungsbereich und eignen sich daher ideal für Szenarien, die eine verbesserte Überwachungsleistung bei schwachem Licht erfordern.

Bild

Die IPv4-Karte spielt eine entscheidende Rolle bei der Einrichtung der Netzwerkkonfiguration der Kamera und gewährleistet eine effektive Kommunikation. Sie ermöglicht eine zuverlässige Verbindung, sowohl lokalen als auch Fernzugriff und die problemlose Integration der Kamera in IPv4-basierte Netzwerke. Diese Konfiguration ist unerlässlich für einen stabilen und effizienten Betrieb in unterschiedlichen Netzwerkkumgebungen.

• Weißabgleich



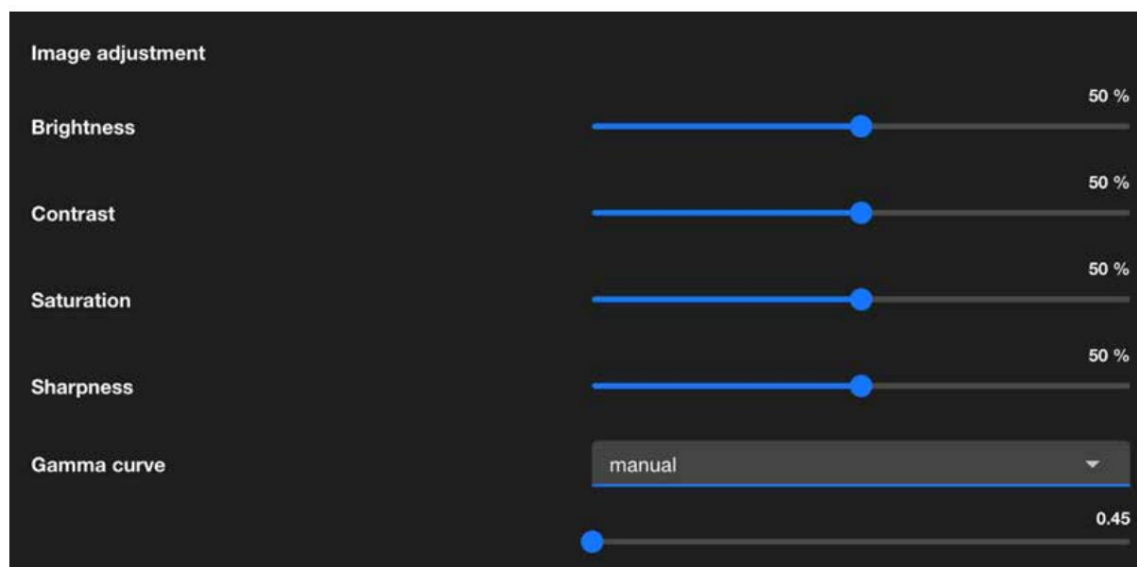
Die Einstellung des Weißabgleichs ist entscheidend, um sicherzustellen, dass die Farben im aufgenommenen Video unter verschiedenen Lichtverhältnissen natürlich wirken.

Bild

Standard	In diesem Modus passt die Kamera den Weißabgleich automatisch an die Lichtverhältnisse an. Es eignet sich für Umgebungen mit wechselnden Lichtquellen, wie z. B. Außenbereiche, in denen Sonnenlicht und Schatten im Laufe des Tages variieren. Die Kamera analysiert kontinuierlich die Szene und passt sich dynamisch an, um eine präzise Farbwiedergabe zu gewährleisten.
Feststrom	Dieser Modus fixiert den Weißabgleich auf die aktuelle automatische Einstellung zum Zeitpunkt der Aktivierung. Es ist nützlich in Umgebungen mit gleichmäßiger Beleuchtung, wo die Aufrechterhaltung eines stabilen Weißabgleichs wichtiger ist als die Anpassung an Veränderungen. Dieser Modus eignet sich beispielsweise ideal für Räume mit fest installierter künstlicher Beleuchtung, wie Büros oder Lagerhallen.
Handbuch	Dieser Modus ermöglicht es dem Benutzer, den Weißabgleich manuell einzustellen, indem er bestimmte Parameter wie RGain (Rot) und BGain (Blau) anpasst. Es bietet maximale Kontrolle und ist ideal für Szenarien mit spezieller Beleuchtung, wie beispielsweise Theaterproduktionen, bei denen präzise Farbanpassungen erforderlich sind. Die Benutzer können die Einstellungen an ihre spezifischen Bedürfnisse anpassen und so die Farbgenauigkeit auch unter besonderen Lichtverhältnissen gewährleisten.

Durch die Auswahl des geeigneten Weißabgleichmodus können Benutzer die Leistung ihrer VIVOTEK-Kameras für eine Vielzahl von Umgebungen und Anwendungsfällen optimieren.

• Bildanpassung



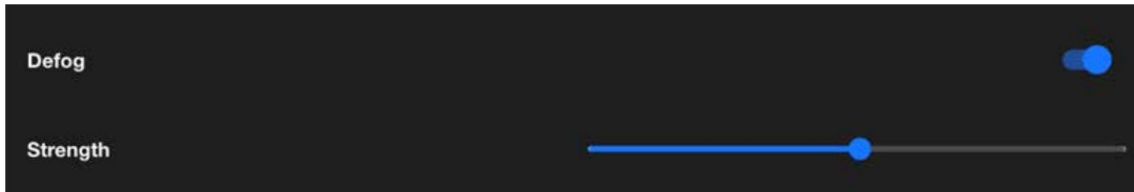
Bild

Bildanpassungen sind unerlässlich, um die visuelle Qualität der aufgenommenen Bilder zu optimieren. Mithilfe dieser Anpassungen können Benutzer das Erscheinungsbild des Videomaterials an ihre spezifischen Bedürfnisse anpassen oder es an unterschiedliche Umgebungsbedingungen anpassen.

Helligkeit	Die Helligkeit steuert die Gesamthelligkeit oder Dunkelheit des Bildes. Eine höhere Helligkeit lässt das gesamte Bild heller erscheinen, eine niedrigere Helligkeit macht es dunkler. Passen Sie die Helligkeit an, um eine klare Sichtbarkeit bei unterschiedlichen Lichtverhältnissen zu gewährleisten, z. B. bei schwachem Licht oder in überbelichteten Bereichen.
Kontrast	Der Kontrast bestimmt den Unterschied zwischen den hellsten und dunkelsten Bildbereichen. Ein höherer Kontrast lässt Schatten dunkler und Lichter heller erscheinen und verstärkt so die Unterscheidung zwischen Objekten. Ein niedrigerer Kontrast führt zu einem flacheren, weniger dynamischen Bild. Nutzen Sie den Kontrast, um die Bildschärfe zu verbessern, indem Sie die Unterscheidung zwischen Objekten in der Szene verstärken.
Sättigung	Die Farbsättigung steuert die Intensität der Farben im Bild. Eine höhere Sättigung lässt die Farben lebendiger und kräftiger wirken, während eine niedrigere Sättigung zu einem gedämpfteren oder grauen Erscheinungsbild führt. Passen Sie die Farbsättigung an, um die Farbintensität für ein optimales Bild auszugleichen, insbesondere in Szenen mit zu kräftigen oder zu blassen Farben.
Schärfe	Die Schärfe bestimmt, wie klar Details und Kanten von Objekten im Bild dargestellt werden. Eine höhere Schärfe verbessert die Kantenschärfe, übermäßige Schärfe kann jedoch zu unnatürlichen Konturen oder Bildrauschen führen. Passen Sie die Schärfe an, um Details hervorzuheben, ohne Artefakte einzuführen, insbesondere in Szenen, die eine präzise Identifizierung erfordern, wie z. B. Nummernschilder oder Gesichtsmarkierungen.
Gammakurve	Die Gammakurve definiert die Tonwertwiedergabe der Kamera und beeinflusst die Helligkeitsverteilung. Durch Anpassen des Gammawerts werden die Mitteltöne des Bildes verändert, ohne die dunkelsten oder hellsten Bereiche wesentlich zu beeinflussen. Nutzen Sie die Gammakorrektur, um Helligkeit und Kontrast des Bildes zu optimieren und so eine bessere visuelle Darstellung unter schwierigen Lichtverhältnissen zu erzielen. *Diese Option ist deaktiviert, wenn die WDR-Funktion aktiviert ist.

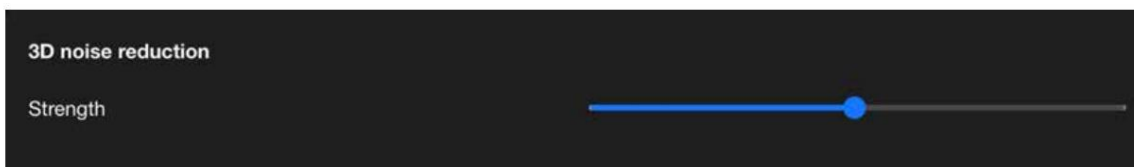
Bild

• Entfeuchten



Die Funktion „Entnebeln“ wurde entwickelt, um die Bildschärfe bei Nebel, Dunst oder Smog zu verbessern. Sie passt Kontrast und Sichtbarkeit des Bildes an, um die Auswirkungen atmosphärischer Bedingungen, die Details verdecken, zu reduzieren. Diese Funktion ist besonders nützlich bei Überwachungsaufnahmen im Freien und gewährleistet eine bessere Objekterkennung und Szenenübersicht trotz schwieriger Wetterbedingungen.

• 3D-Rauschunterdrückung



Die 3D-Rauschunterdrückung wird vor allem in Umgebungen mit schwachem Licht eingesetzt, um Rauschen und Flimmern im Bild zu reduzieren. Sie können die Stärke der Rauschunterdrückung mithilfe des Schiebereglers anpassen. Bitte beachten Sie, dass die Aktivierung dieser Funktion im Videokanal Systemressourcen beansprucht. Bei aktivierter Funktion in Situationen mit schwachem Licht und sich schnell bewegenden Objekten können Nachbilder auftreten. In diesem Fall empfiehlt es sich, die Stärke der Rauschunterdrückung zu reduzieren.

• Elektronischer Bildstabilisator



Die elektronische Bildstabilisierung (EIS) reduziert Bildverwacklungen, die durch äußere Einflüsse wie Wind, Vibrationen oder die Montage der Kamera an instabilen Strukturen verursacht werden. Diese Funktion stabilisiert und glättet das Videomaterial durch Anpassung der Bildausgabe mittels Softwarealgorithmen. Die Aktivierung der elektronischen Bildstabilisierung (EIS) in VIVOTEK-Kameras bietet mehrere entscheidende Vorteile:

• Verbessert die Videoqualität:

EIS reduziert durch Vibrationen verursachte Unschärfe und Bildzittern und sorgt so für flüssigere und klarere Videoaufnahmen.

• Verbessert die Lesbarkeit wichtiger Details:

Durch die Stabilisierung des Bildes wird es einfacher, wichtige Details wie Nummernschilder, Gesichter und Objekte zu erkennen.

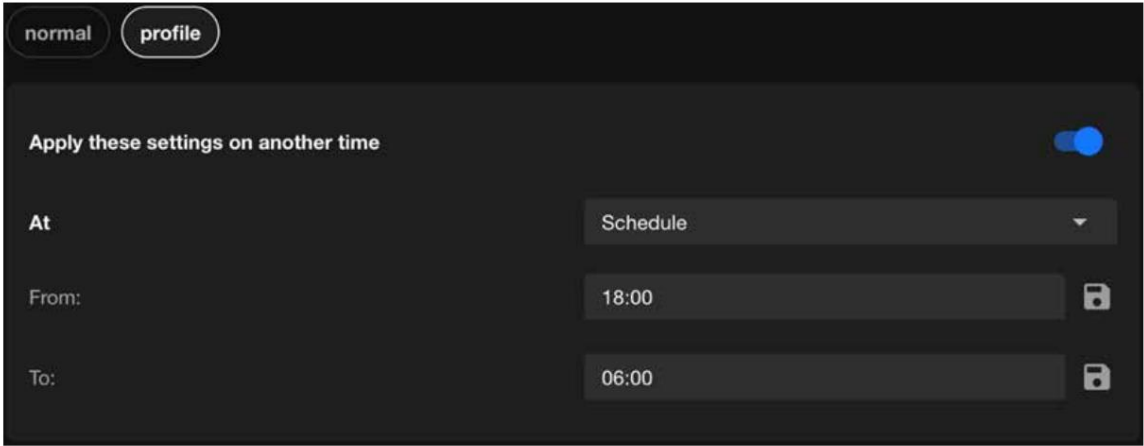
• Optimiert die Leistung der Videoanalyse:

Stabilität trägt dazu bei, Fehlalarme zu reduzieren und die Genauigkeit analytischer Funktionen wie Bewegungserkennung und Objekterkennung zu verbessern.

Diese Vorteile machen EIS zu einem unverzichtbaren Bestandteil für die Aufrechterhaltung einer zuverlässigen Überwachung, insbesondere in Umgebungen, die unvermeidbaren Vibrationen oder Bewegungen ausgesetzt sind.

Bild

● Integrieren Sie bildbezogene Einstellungen in ein Profil



Der Normalmodus der VIVOTEK-Kameras bietet eine Standardbildkonfiguration, die sich ideal für die Überwachung eignet. Über die Profilmodi, insbesondere „Nacht“ und „Zeitplan“, können Benutzer die Bildeinstellungen an spezifische Anforderungen und Zeiträume anpassen und automatisieren. Dies **beschränkt sich nicht auf Tag-Nacht-Übergänge** und bietet so mehr Flexibilität und Kontrolle.

Dieses Design bietet Folgendes:

- Flexible und automatisierte Umschaltung von Bildprofilen.
- Optimierte Bildqualität für verschiedene Anwendungsszenarien.
- Verbesserte betriebliche Effizienz und Ressourcenverwaltung.

VIVOTEK-Kameras gewährleisten eine gleichbleibende Leistung und eine qualitativ hochwertige Überwachung, die auf verschiedene Bedingungen zugeschnitten ist und sowohl die Benutzerfreundlichkeit als auch die Effektivität der Überwachung verbessert.

Zweck und Anwendungsbereiche:

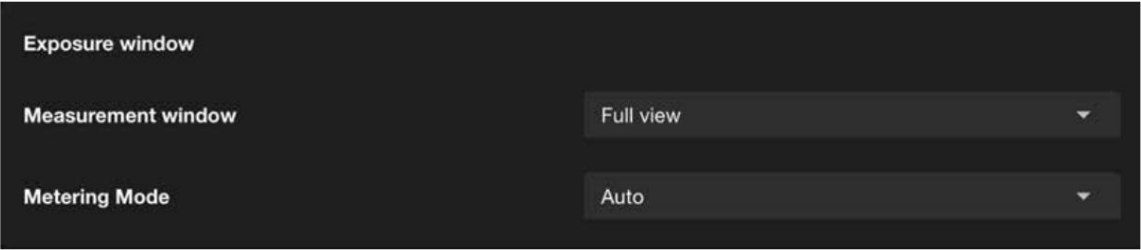
Normal	Bietet Standardbildeinstellungen für den allgemeinen Gebrauch	Geeignet für Umgebungen mit Tageslicht oder gleichmäßiger Beleuchtung
Nacht (Profil)	Optimiert die Bildeinstellungen für schwache Lichtverhältnisse oder Nachtbedingungen	Verbessert die Bildschärfe und Detailgenauigkeit, ideal für die Nachtüberwachung
Zeitplan (Profil)	Automatische Umschaltung der Bildeinstellungen basierend auf einer benutzerdefinierten Zeit	Wendet während festgelegter Zeiträume spezifische Einstellungen an; nicht beschränkt auf Tag/Woche Übergänge in der Nacht

Bild

Belichtung

Die Seite „Bild“ in der Web-Benutzeroberfläche der Kamera steuert, wie viel Licht der Kamerasensor aufnimmt, um ein ausgewogenes Bild zu erzeugen. Die korrekte Belichtung sorgt dafür, dass das Bild weder zu hell (überbelichtet) noch zu dunkel (unterbelichtet) ist und ermöglicht so eine klare Sichtbarkeit von Objekten unter verschiedenen Lichtverhältnissen.

- Integration externer Geräte



Das Belichtungsfenster ermöglicht es dem Benutzer, einen bestimmten Bereich im Sichtfeld der Kamera festzulegen, um die Belichtungseinstellungen zu optimieren. Durch Fokussierung auf diesen Bereich passt die Kamera ihre Belichtungsparameter an, um eine optimale Ausleuchtung auch bei schwierigen Lichtverhältnissen zu gewährleisten. Diese Funktion ist besonders nützlich, wenn verschiedene Bereiche der Szene ungleichmäßig beleuchtet sind. So kann die Kamera die Belichtung kritischer Bereiche priorisieren und die Bildqualität insgesamt verbessern.

Messfenster

Diese Funktion ermöglicht es Benutzern, Messfenster für die Schwachlichtkompensation festzulegen. Befinden sich beispielsweise Objekte vor einem extrem hellen Hintergrund, kann es sinnvoll sein, das helle Sonnenlicht, das durch einen Gebäudeflur scheint, auszuschließen. Folgende Arten von Messfenstern stehen zur Verfügung:

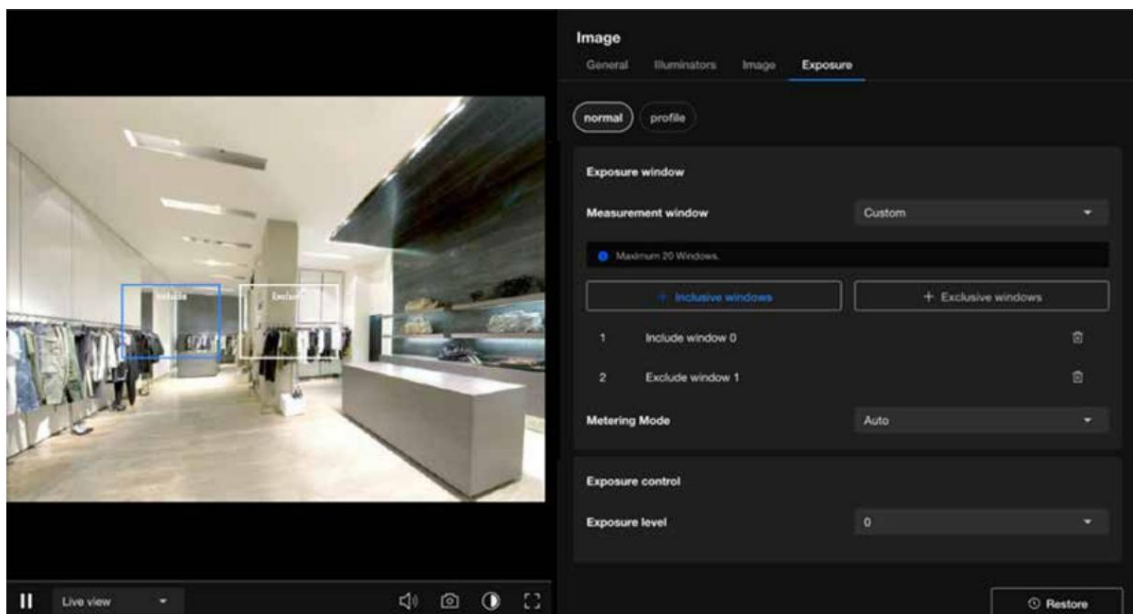
Vollansicht	Diese Option berechnet die Belichtung auf Basis des gesamten Sichtfelds und stellt so sicher, dass die Kamera alle Bereiche innerhalb des Bildausschnitts für die Belichtungsanpassung berücksichtigt.
Brauch	Diese Option ermöglicht es Benutzern, bestimmte Bereiche innerhalb des Bildausschnitts für die Belichtungsmessung manuell zu definieren. Durch Auswahl dieser Einstellung können Benutzer ein oder mehrere Messfenster im Bild zeichnen und so präzise steuern, welche Bereiche die Kamera bei Belichtungskorrekturen priorisieren soll.
Center	Ist diese Option ausgewählt, fokussiert die Kamera auf den zentralen Bildbereich, um die Belichtungseinstellungen zu bestimmen. Dies ist vorteilhaft, wenn sich das Hauptmotiv in der Bildmitte befindet, da so eine optimale Belichtung in diesem Bereich ermöglicht wird.

Bild

Wenn Benutzer den benutzerdefinierten Modus zur Verwendung des Messfensters auswählen, können sie das inklusive und exklusive Fenster selbst definieren.

Inklusive Fenster	Sie werden als „gewichtete Fenster“ bezeichnet. Diesen wird im Berechnungsprozess eine höhere Priorität eingeräumt. Ihre Werte werden in die Endberechnung einbezogen, sofern sie nicht durch überlappende Exklusivfenster beeinflusst werden.
Exklusive Fenster	Diese werden als „ignorierte Fenster“ bezeichnet. Ihre Aufgabe ist es, Teile der inklusiven Fenster auszuschließen, wenn diese sich überschneiden. Sie reduzieren effektiv den Beitrag der sich überschneidenden inklusiven Fenster.

Überschneidet sich ein exklusives Zeitfenster mit einem größeren inklusiven Zeitfenster, wird der exklusive Anteil vom inklusiven Zeitfenster abgezogen. Dadurch wird sichergestellt, dass nur der verbleibende Anteil des inklusiven Zeitfensters in die Berechnung einfließt. Nach Berücksichtigung der Überlappungen zwischen inklusiven und exklusiven Zeitfenstern berechnet das System den Expositionswert anhand des verbleibenden Anteils des inklusiven Zeitfensters mithilfe der gewichteten Mittelwertmethode.



Messmodus

Der Messmodus bestimmt, wie die Kamera ihre Belichtungseinstellungen in Abhängigkeit von unterschiedlichen Lichtverhältnissen anpasst:

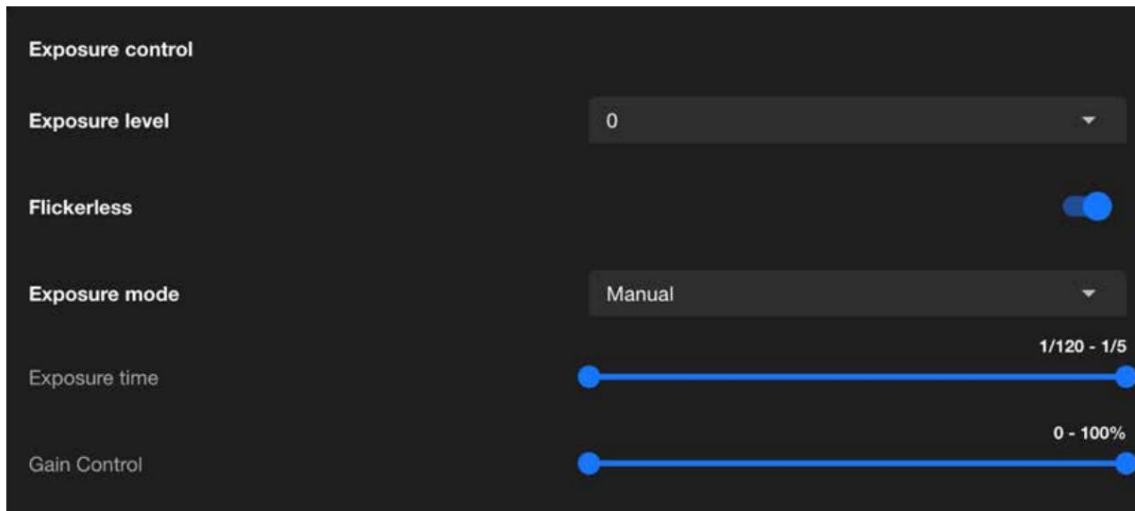
Bild

Auto	Für allgemeine Zwecke, wenn die Szenenbeleuchtung ausgewogen ist.	Die Kamera wertet automatisch die gesamte Szene aus, um die Belichtung auszugleichen. Es stellt sicher, dass die Gesamthelligkeit für typische Szenarien optimiert ist. Geeignet für Umgebungen mit relativ gleichmäßiger Beleuchtung, bei der keine extremen Lichtquellen dominieren.
BLC (Gegenlichtkompensation)	Wenn sich das Objekt vor einer hellen Lichtquelle befindet.	Passt die Belichtung an Werbesituationen an, in denen der Hintergrund viel heller ist als das Motiv (z. B. eine Person, die vor einem hellen Fenster steht). Gewährleistet, dass das Hauptmotiv klar sichtbar und nicht unterbelichtet ist, selbst wenn der Hintergrund überbelichtet wird. Ideal für Szenen mit starker Gegenlichtbeleuchtung.
HLC (High Light Compensation)	Um überbelichtete helle Bereiche zu kontrollieren und sicherzustellen, dass andere Bereiche sichtbar sind.	Der Fokus liegt auf der Reduzierung der Auswirkungen übermäßig heller Lichtquellen in der Szene, wie z. B. Scheinwerfer, Straßenlaternen oder andere intensive Lichtquellen. Dunkelt überbelichtete Bereiche (wie helle Flecken) ab, um die Gesamtbildqualität zu verbessern und gleichzeitig Details in dunkleren Bereichen zu erhalten.

Diese Einstellungen helfen dabei, die Leistung der Kamera für verschiedene Lichtverhältnisse zu optimieren und sicherzustellen, dass wichtige Details effektiv erfasst werden.

Bild

● Expositionskontrolle



Die Belichtungssteuerung regelt die Wechselwirkung von Licht mit dem Kamerasensor, um unter verschiedenen Lichtverhältnissen klare und ausgewogene Bilder zu erzeugen. Ihr Hauptzweck ist die Anpassung der Kameraeinstellungen, um unabhängig von der Umgebung optimale Helligkeit, Schärfe und Detailgenauigkeit zu gewährleisten.

Expositionsniveau

Der Einstellbereich der Belichtungskorrektur liegt typischerweise zwischen -2,0 und +2,0 und dient zur Feinabstimmung der Bildhelligkeit. Diese Einstellung optimiert die Belichtung des Bildes je nach Umgebungslicht und sorgt so für ein klares Bild mit allen Details.

Flimmerfrei

Wenn die Funktion „Flimmerfrei“ aktiviert ist, passt die Kamera ihre Verschlusszeit automatisch an die Flimmerfrequenz von Umgebungslichtquellen wie Leuchtstoffröhren oder LED-Lampen an. Dadurch werden flackernde Streifen oder Flimmereffekte im Bild effektiv eliminiert und für Stabilität und Schärfe gesorgt.

Belichtungsmodus

Der Belichtungsmodus steuert, wie die Kamera die Belichtungsparameter (wie Belichtungszeit und Verstärkung) an unterschiedliche Umgebungslichtverhältnisse anpasst. Sobald der Belichtungsmodus aktiviert und konfiguriert ist, passt die Kamera die Belichtung automatisch oder manuell an die jeweiligen Szenenanforderungen an und stellt so sicher, dass Bildhelligkeit und Details den gewünschten Standards entsprechen.

Expositionszeit

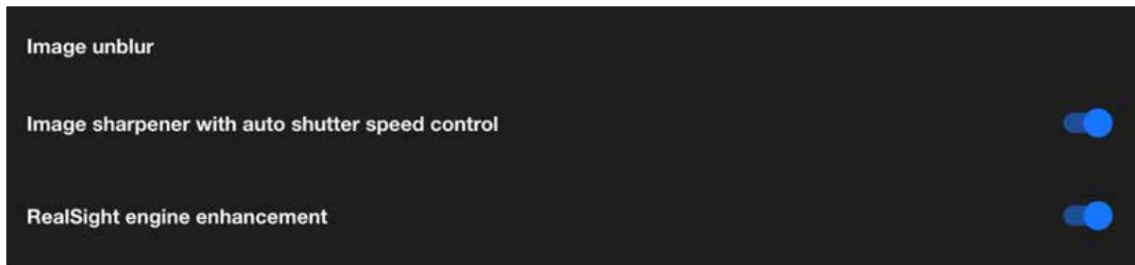
Die Belichtungszeit bezeichnet die Dauer, für die der Kamerasensor dem Licht ausgesetzt ist, typischerweise in Sekunden oder Bruchteilen einer Sekunde angegeben (z. B. 1/120 Sekunde bis 1/5 Sekunde). Hauptzweck dieser Funktion ist die Steuerung von Helligkeit und Schärfe des Bildes, insbesondere bei wechselnden Lichtverhältnissen.

Verstärkungsregelung

Die Verstärkungsregelung dient dazu, die Lichtempfindlichkeit des Kamerasensors anzupassen. Verstärkungseinstellungen werden primär verwendet, um die Bildhelligkeit bei schwachem Licht zu verbessern, können aber das Bildrauschen erhöhen. Diese Funktion trägt dazu bei, dass die Kamera auch bei schlechten Lichtverhältnissen oder hohem Kontrast klare und gut sichtbare Bilder liefert.

Bild

• Bild schärfen



Die Funktion „Bildunschärfe“ wurde speziell für dynamische Szenen entwickelt und reduziert effektiv bewegungsbedingte Unschärfe, um scharfe Bilder von sich schnell bewegenden Objekten zu gewährleisten. Durch die Anpassung der Verschlusszeit und anderer Belichtungsparameter eignet sich diese Funktion ideal für Szenarien, die hochauflösende dynamische Aufnahmen erfordern, wie beispielsweise Verkehrsüberwachung oder Personenkontrolle. Um optimale Ergebnisse zu erzielen, sind jedoch sinnvolle Anpassungen zwischen Helligkeit und Bildqualität notwendig.

Bildschärfung mit automatischer Verschlusszeitensteuerung

Die Kombination von Bildschärfung und automatischer Verschlusszeitensteuerung sorgt für scharfe Bilder. Durch Verkürzung der Verschlusszeit zur Reduzierung von Unschärfe und Anwendung von Bildschärfungstechniken zur Verbesserung der Detailgenauigkeit liefert die Kamera klare Bilder in dynamischen Szenen und passt gleichzeitig automatisch andere Parameter an, um die Helligkeit auszugleichen und so unterschiedlichen Überwachungsanforderungen gerecht zu werden.

RealSight-Engine-Erweiterung

Durch die Nutzung der dynamischen Rauschunterdrückung, der Dynamikbereichsoptimierung und der Bildschärfungsfunktionen der RealSight Engine in Kombination mit der automatischen Verschlusszeitensteuerung wird die Bildschärfe deutlich verbessert. Dadurch liefern VIVOTEK-Kameras auch in schnell bewegten, dynamischen Szenen und bei schwachem Licht stabile, klare und detailreiche Bilder und erfüllen somit die Anforderungen hochwertiger Überwachungstechnik.

• AE-Geschwindigkeitsanpassung



Die AE-Geschwindigkeitsanpassung steuert die Reaktionsgeschwindigkeit der automatischen Belichtung auf Lichtveränderungen und sorgt so für ein ausgewogenes Verhältnis zwischen Bildschärfe und -stabilität. Ziel ist es, in verschiedenen Szenarien optimale Bildqualität zu gewährleisten und durch Lichtschwankungen verursachte Belichtungsschwankungen oder Bildflimmern zu vermeiden. Durch die flexible Anpassung der AE-Geschwindigkeit lassen sich vielfältige Überwachungsanforderungen erfüllen und klare, stabile Bilder sicherstellen.

Bild

Geschwindigkeitsstufe

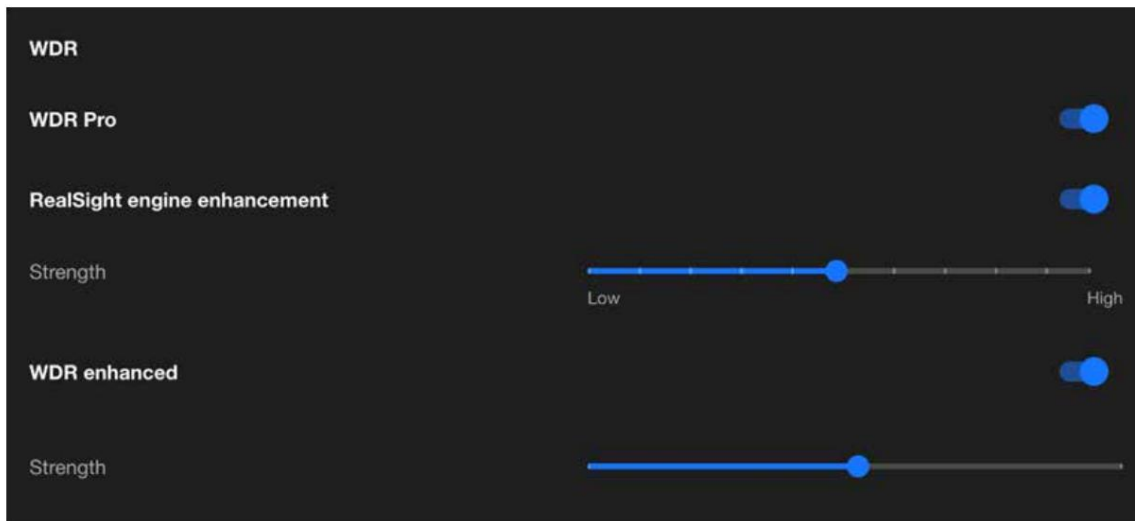
Die Geschwindigkeit der AE-Geschwindigkeitsanpassung sollte anhand der Häufigkeit von Lichtänderungen in der Überwachungsszene konfiguriert werden. Für stabile Szenen empfiehlt sich eine **niedrigere** Geschwindigkeit, während für dynamische Szenen eine **höhere** Geschwindigkeit geeignet ist, um eine gleichmäßige und reaktionsschnelle Helligkeitsanpassung zu gewährleisten. Durch Testen und Feinabstimmung lässt sich ein optimales Gleichgewicht zwischen Bildstabilität und -scharfe erzielen.

Empfindlichkeit

Die Empfindlichkeitseinstellung in der AE-Geschwindigkeitsanpassung steuert die Fähigkeit der Kamera, Lichtveränderungen wahrzunehmen.

Eine **niedrige** Empfindlichkeit eignet sich für ruhige Szenen und sorgt für ein stabiles Bild, während eine **hohe** Empfindlichkeit ideal für sich schnell verändernde Szenen ist und eine Echtzeitreaktion ermöglicht. Durch Testen und Anpassen der Empfindlichkeit an die jeweiligen Szenenanforderungen lässt sich das optimale Gleichgewicht zwischen Lichtanpassungsfähigkeit und Bildstabilität erzielen.

● WDR



Die WDR-Funktion (Wide Dynamic Range) dient primär der Verbesserung der Bildqualität bei kontrastreichen Lichtverhältnissen. Sie gleicht die Helligkeit heller und dunkler Bereiche aus, erhält Details und gewährleistet klare Sicht. Diese Funktion ist unerlässlich für Anwendungen, die eine präzise Überwachung unter verschiedenen Lichtverhältnissen erfordern, wie beispielsweise Eingänge, Tunnel, Banken oder die nächtliche Videoüberwachung.

WDR Pro

WDR Pro ist eine fortschrittliche Funktion mit großem Dynamikumfang von VIVOTEK-Kameras, die außergewöhnliche Bildverarbeitungsfähigkeiten für kontrastreiche Lichtverhältnisse bietet. Sie gleicht Details und Farben in hellen und dunklen Bereichen effektiv aus und gewährleistet so eine hohe Gesamtbildqualität. Damit ist sie die ideale Wahl für Situationen, die höchste Ansprüche an Bilddetails und Lichtmanagement stellen.

RealSight-Engine-Erweiterung

Die RealSight-Engine bietet eine fortschrittliche Stärkesteuering zur Optimierung der WDR Pro-Leistung und verbessert so die Bildverarbeitung. Durch die Anpassung der Stärkeeinstellungen kann die Kamera Details in hellen und dunklen Bereichen kontrastreicher Szenen besser ausbalancieren und die Sichtbarkeit in dunklen Regionen verbessern. Die Auswahl der passenden Stärkeeinstellungen je nach Lichtverhältnissen in verschiedenen Szenen kann die Bildqualität und -stabilität deutlich steigern und den Anforderungen verschiedenster Anwendungen gerecht werden.

Bild

WDR-optimiert

WDR Enhanced ist VIVOTEKs fortschrittlichste Dynamikbereichstechnologie für kontrastreiche Szenen und bietet im Vergleich zu Standard-WDR und WDR Pro eine überlegene Detailwiedergabe in hellen und dunklen Bereichen. Sie eignet sich für Szenarien mit extremen Lichtkontrasten und schnellen Veränderungen und verbessert Bildschärfe und -stabilität deutlich. Dadurch ist sie besonders ideal für Überwachungsanwendungen, die eine hohe Detailgenauigkeit erfordern.

Integrieren Sie expositionsbezogene Einstellungen in ein Profil

The screenshot shows a dark-themed settings menu. At the top, there are two tabs: 'normal' and 'profile', with 'profile' being the active tab. Below the tabs, there is a toggle switch labeled 'Apply these settings on another time' which is turned on. Underneath, there are three rows of settings: 'At' with a dropdown menu showing 'Schedule', 'From:' with a time input field showing '18:00', and 'To:' with a time input field showing '06:00'. Each time input field has a small calendar icon to its right.

Die Belichtungseinstellungen von VIVOTEK-Kameras lassen sich mithilfe der Profilkfunktion präzise anpassen. Dies ermöglicht automatische Anpassungen basierend auf der Zeit (Zeitplan) oder den Lichtverhältnissen (Nacht/Normal). So wird sichergestellt, dass die Kamera in unterschiedlichen Lichtsituationen stets optimale Bildqualität liefert.

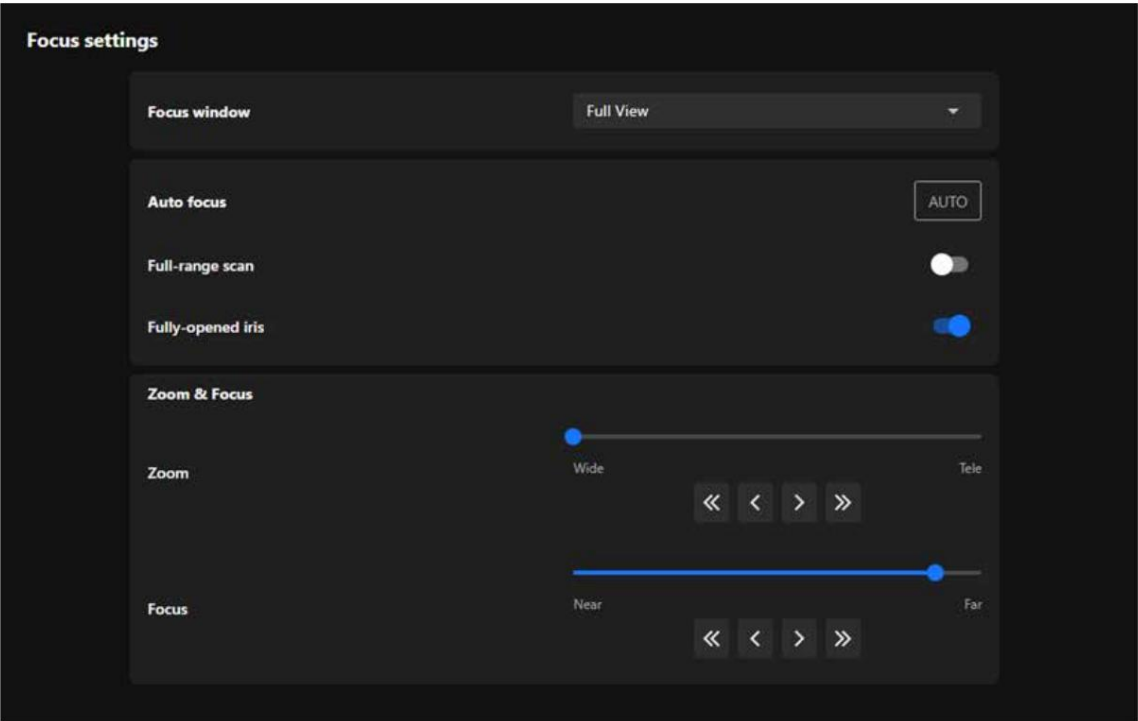
Zweck und Anwendungsbereiche:

Normal	Bietet eine Standardbelichtung für den allgemeinen Gebrauch.	Verschlusszeit, Verstärkung und Belichtungskompensation unter normalen Bedingungen.	Ideal für Tageslicht oder gleichmäßige Beleuchtung Bedingungen
Nacht (Profil)	Optimiert die Belichtung für schwache Lichtverhältnisse	Niedrigere Verschlusszeit, höhere Verstärkung, ausgewogene Belichtung	Verbessert die Sichtbarkeit bei Nacht oder in dunklen Umgebungen
Zeitplan (Profil)	Zeitbasierte Umschaltung der Belichtungsprofile	Benutzerdefinierte Belichtungseinstellungen für bestimmte Zeiträume	Passt sich über den Tag hinaus an individuelle Bedürfnisse an/Übergänge in der Nacht

Bild

Optimierung der Bildschärfe durch flexible Fokussteuerung (Die Fokuseinstellungen werden nur von VIVOTEK-Zoomkameras des Typs EHTV unterstützt.)

Die Fokuseinstellungen der VIVOTEK-Zoomkameras sind ein entscheidendes Werkzeug für optimale Bildschärfe und präzise Überwachung in verschiedenen Szenarien. Mit dieser Einstellung können Benutzer den Fokus der Kamera feinjustieren, um klare und detailreiche Bilder aufzunehmen – egal ob in dynamischen Umgebungen mit sich bewegenden Objekten oder in statischen Szenen, die scharfe Bilder erfordern. Durch die Kombination von Autofokus und manuellem Fokus können Benutzer effizient auf unterschiedliche Entfernungen, Lichtverhältnisse und Überwachungsanforderungen reagieren. Die korrekte Verwendung der Fokuseinstellungen verbessert nicht nur die Bildqualität, sondern auch die Genauigkeit fortschrittlicher Analysefunktionen wie Gesichtserkennung und Kennzeichenerkennung und ist somit ein unverzichtbarer Bestandteil professioneller Überwachungssysteme.



Fokuseinstellungen

Die Fokuseinstellungen in der Bildkonfiguration gewährleisten optimale Bildschärfe und -präzision für Überwachungszwecke. Benutzer können Fokus und Zoom anpassen, um für ihr jeweiliges Überwachungsszenario die besten Ergebnisse zu erzielen. Dieser Bereich bietet Werkzeuge für automatische und manuelle Einstellungen, die dynamische und statische Szenen, unterschiedliche Entfernungen und Lichtverhältnisse berücksichtigen.

- **Fokusfenster**

Ermöglicht es dem Benutzer, den Bereich innerhalb des Kamerabildes zu definieren, in dem der Fokus optimiert werden soll.

Vollansicht	Das gesamte Sichtfeld wird auf Schärfe berücksichtigt.
Brauch	Nutzer können einen bestimmten Bereich für die Fokusoptimierung auswählen.

Bild

- **Autofokus**

Passt den Fokus automatisch an, um ein möglichst schärfstes Bild zu erzielen.

Vollbereichsscan

Ist diese Option aktiviert, scannt die Kamera den gesamten Brennweitenbereich, um die optimale Schärfe zu finden. Dies ist zwar gründlicher, dauert aber länger.

Vollständig geöffnete Iris

Sorgt dafür, dass die Iris beim Fokussieren vollständig geöffnet ist, um Schärfentiefeeffekte zu reduzieren und die Genauigkeit zu verbessern.

AUTO-Taste

Startet den Autofokus-Prozess.

- **Zoom & Fokus**

Die Zoom- und Fokussfunktion bietet dem Benutzer intuitive Bedienelemente, um das Sichtfeld und den Fokus der Kamera für eine präzise Überwachung anzupassen.

Zoom

Ermöglicht die nahtlose Anpassung zwischen Weitwinkel- und Teleaufnahmen mittels Schieberegler oder Tasten für schnelle oder feinabgestimmte Änderungen.

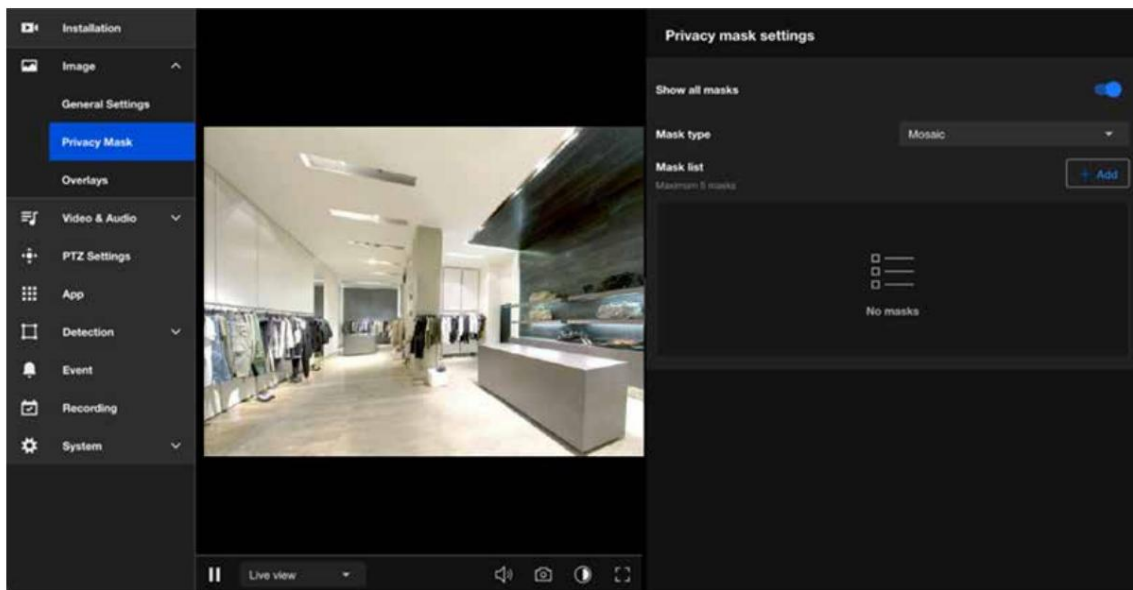
Fokus

Ermöglicht die manuelle Feinabstimmung des Fokus, um die Schärfe von Objekten in unterschiedlichen Entfernungen zu gewährleisten; die Steuerung erfolgt über einen Schieberegler und Richtungstasten.

Bild

Verwendung von Privacy Masking zum Schutz vertraulicher Informationen in Bildern

Der Hauptzweck der Einrichtung einer Datenschutzmaske besteht darin, die Privatsphäre zu schützen, regulatorische Anforderungen zu erfüllen und die Überwachungseffizienz zu steigern. Durch die flexible Anwendung der Datenschutzmaskierungsfunktion in verschiedenen Szenarien werden nicht nur unnötige Datenschutzverletzungen verhindert, sondern auch die Konzentration auf wichtige Überwachungsbereiche ermöglicht, wodurch die Gesamteffektivität der Überwachung und die Einhaltung von Vorschriften verbessert werden.

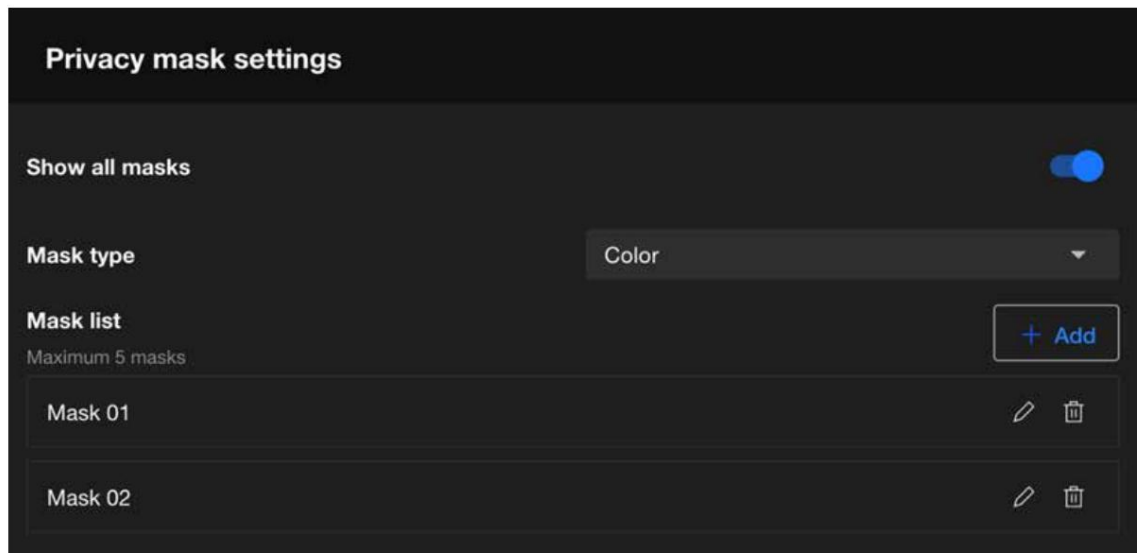


Die wichtigsten Vorteile der Einrichtung einer Sichtschutzmaske sind folgende:

- Entspricht den Datenschutzbestimmungen und reduziert so rechtliche Risiken.
- Vermeidet die Erfassung von Aufnahmen, die nicht im Zusammenhang mit Überwachungszwecken stehen, wodurch die Effizienz der Datenverarbeitung verbessert wird.
- Verringert den Eingriff in die Privatsphäre der überwachten Personen und stärkt so Vertrauen und Akzeptanz.
- Sorgt dafür, dass der Fokus auf den Zielbereichen bleibt, minimiert Ablenkungen und verbessert die Effektivität der Überwachung.

Bild

Datenschutzmaskierungseinstellungen



Schritte zum Hinzufügen einer Datenschutzmaske:

Schritt 1. Klicken Sie in der Maskenliste auf die Schaltfläche +Hinzufügen.

Schritt 2. Zeichnen Sie eine geschlossene Form, um den Bereich abzudecken, den Sie aus Datenschutzgründen in der Vorschau ausblenden möchten. Bildschirm.



Schritt 3. Geben Sie den Namen der Datenschutzmaske ein.

Schritt 4. Klicken Sie auf die Schaltfläche „Speichern“.

Schritte zum Löschen der Datenschutzmaske:

Schritt 1. Klicken Sie auf das Löschesymbol beim Maskenelement.

Schritt 2. Der Maskeneintrag wird direkt gelöscht.

Bild

Schritte zum Bearbeiten der Datenschutzmaske:

Schritt 1. Klicken Sie auf das Bearbeitungssymbol beim Maskenelement.

Schritt 2. Ziehen Sie die Maske in den gewünschten Bereich.

Schritt 3. Klicken und ziehen Sie an den Ecken, um Form (rechteckig, trapezförmig usw.) und Größe so anzupassen, dass der Zielbereich präzise abgedeckt wird.

Schritt 4. Klicken Sie auf die Schaltfläche „Speichern“.

Alle Masken anzeigen

Nachdem der Benutzer die Datenschutzmasken konfiguriert hat, muss die Option „Alle Masken anzeigen“ aktiviert werden, um die konfigurierten Masken auf das Bild anzuwenden.

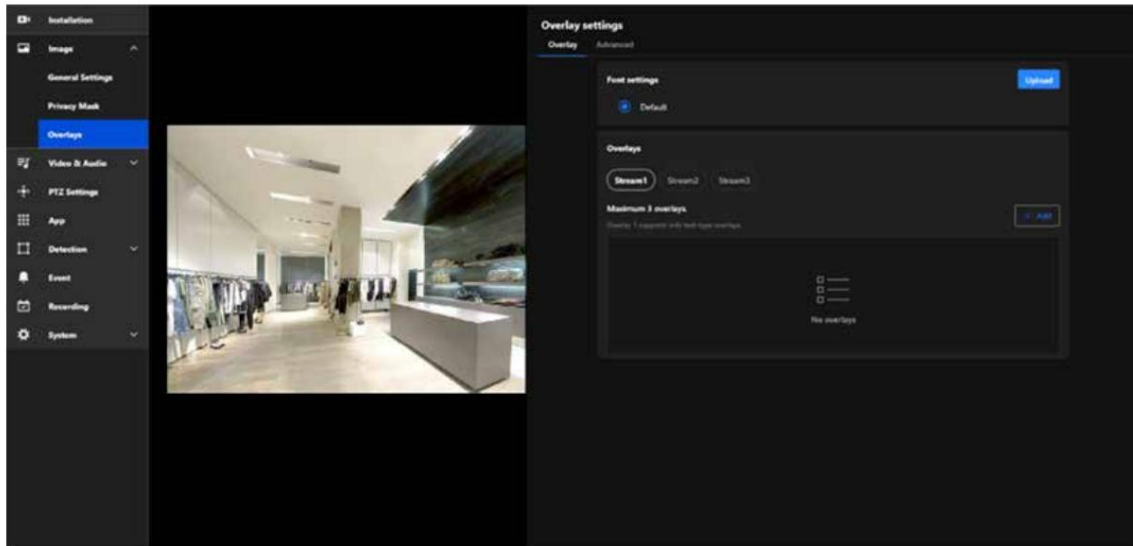
Maskentyp

Privacy Mask bietet zwei Varianten: Farbe (Farbmaskierung) und Mosaik (Mosaikmaskierung). So werden die Anforderungen an den Datenschutz in verschiedenen Anwendungsszenarien erfüllt. Die Farbmaske eignet sich für Fälle, die ein hohes Maß an Privatsphäre und vollständige Verdeckung erfordern, während die Mosaikmaske besser geeignet ist, um Details auszublenden und gleichzeitig das natürliche Erscheinungsbild des Bildes zu erhalten. Die Wahl der passenden Maskenvariante je nach Situation gewährleistet einen effizienten und flexiblen Datenschutz.

Bild

Anpassen von Bildüberlagerungen zum Hinzufügen zusätzlicher Informationen

Die Overlay-Funktion ist ein leistungsstarkes Werkzeug, das die Benutzerfreundlichkeit und Klarheit von Videostreams oder -aufnahmen verbessert, indem es das Einblenden wichtiger Informationen in das Videobild ermöglicht.



Nachfolgend eine Erläuterung der wichtigsten Zwecke und Funktionen:

- **Anzeige wichtiger Informationen:**

Fügt dem Video wichtige Details wie Kameraname, Datum und Uhrzeit, Ort oder benutzerdefinierten Text hinzu und erleichtert so die Identifizierung der Quelle und des Kontextes des Filmmaterials.

- **Verbesserung der Beweiskraft:**

Durch die Einblendung von Zeitstempeln wird sichergestellt, dass Videoaufnahmen als gültige Beweismittel für rechtliche oder Ermittlungszwecke dienen können.

- **Markenbildung und Identifikation:**

Zeigt Logos oder andere Kennzeichen zur Stärkung der Markenbekanntheit an, was insbesondere in kommerziellen oder öffentlichen Anwendungen nützlich ist.

- **Echtzeit-Datenüberwachung:**

Durch die dynamische Textüberlagerung können Echtzeit-Updates (z. B. Sensordaten, Alarmer) direkt im Videobild angezeigt werden, was es wertvoll für die Umgebungsüberwachung oder die Lageerkennung macht.

- **Einhaltung gesetzlicher Bestimmungen und Warnmeldungen:**

Gewährleistet die Einhaltung branchenspezifischer oder regionaler Vorschriften durch die Anzeige erforderlicher Benachrichtigungen oder Warnmeldungen im Videostream.

Bild

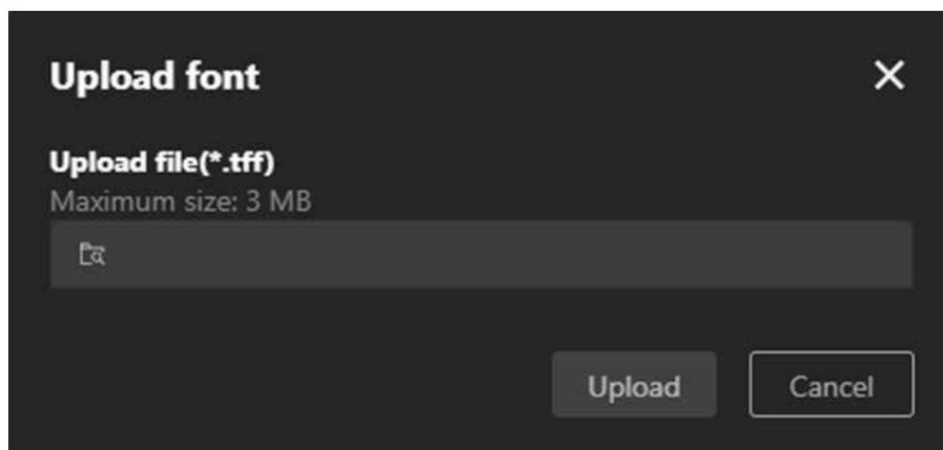
Overlay

Die Overlay-Funktion ermöglicht es Nutzern, Bilder mit Informationen wie Kameranamen und Zeitstempeln anzureichern. Diese Informationen werden direkt in aufgezeichneten oder live gestreamten Videos angezeigt und erleichtern so die spätere Überprüfung und Verwaltung. Beispielsweise können Sie durch Aktivieren der Overlay-Funktion den Kameranamen und die Aufnahmezeit im Videomaterial anzeigen lassen, was für die Verwaltung von Überwachungssystemen und die Ereignisnachverfolgung äußerst hilfreich ist.

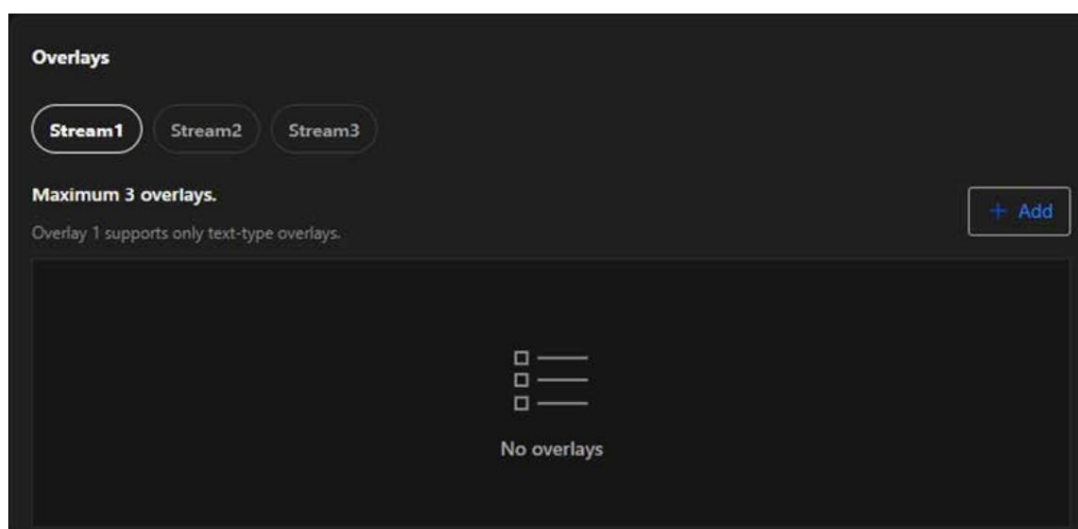
• Schrifteinstellungen



Die Schrifteinstellungen in den Overlay-Einstellungen ermöglichen es Benutzern, das Erscheinungsbild von Text-Overlays in Videostreams anzupassen. Diese Funktion gewährleistet, dass die angezeigten Informationen klar und gut sichtbar sind und den spezifischen Anforderungen verschiedener Überwachungsumgebungen entsprechen.



• Overlays

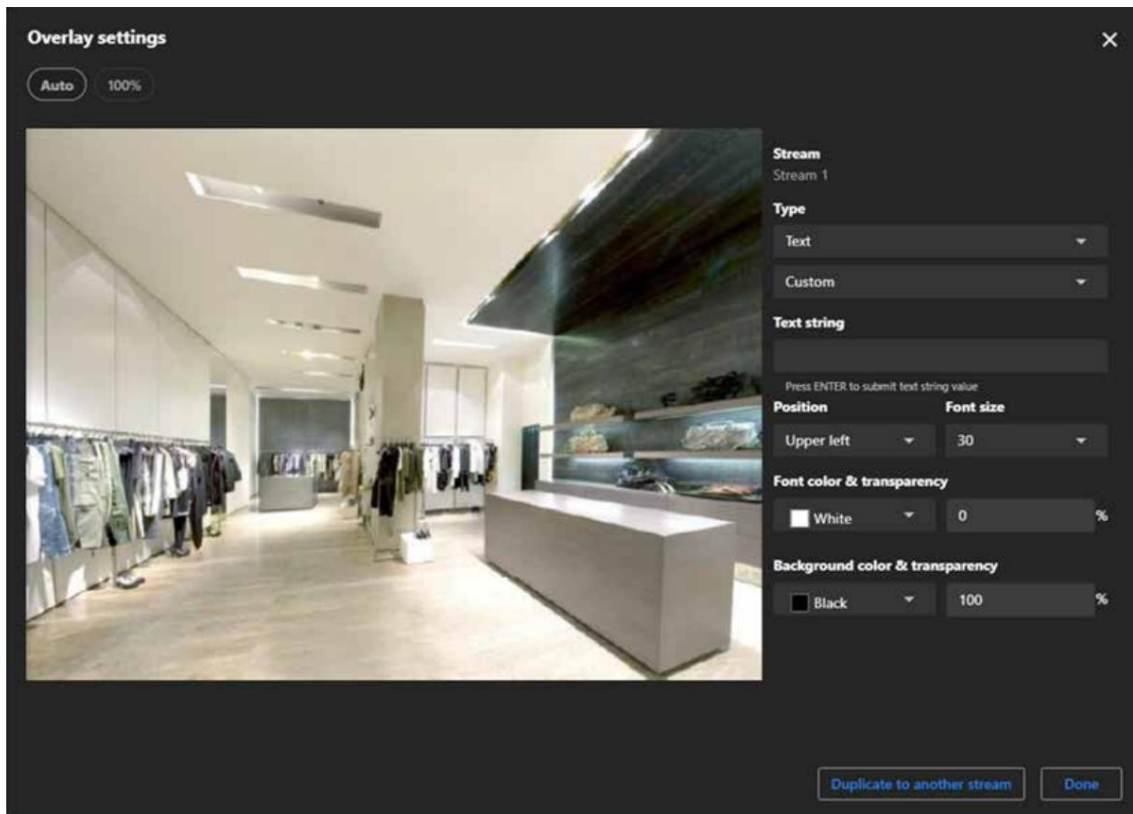


Bild

Schritte zum Festlegen eines

Overlays: Schritt 1. Wählen Sie den Stream (z. B. Stream 1, Stream 2 oder Stream 3) aus, den Sie für das Overlay konfigurieren möchten.

Schritt 2. Klicken Sie auf die Schaltfläche "Hinzufügen", um ein neues Overlay zu erstellen.



Bild

Schritt 3. Wählen Sie den Overlay-Typ:

Text	Datum und Uhrzeit	Das Display kann das vom Benutzer definierte Datums- und Zeitformat anzeigen.
	Datum	Das Display kann das vom Benutzer definierte Datumsformat anzeigen.
	Zeit	Das Display kann das vom Benutzer definierte Zeitformat anzeigen.
	Brauch	Das Display kann benutzerdefinierten Text anzeigen Zelt.
Bild		Das Display kann vom Benutzer hochgeladene 256-Farben-BMP-Bilder anzeigen.
Live-Streaming-Anzeige		Die Live-Streaming-Anzeige ist eine Funktion in den Overlay-Einstellungen, die visuell anzeigt, wann die Kamera aktiv Live-Video streamt.

Schritt 4. Klicken Sie auf das Dropdown-Menü „Position“, um das Overlay zu platzieren (z. B. oben links, unten rechts). Passen Sie die Position manuell an, falls erweiterte Steuerelemente verfügbar sind.

Schritt 5. Wenn Sie „Text“ auswählen, klicken Sie auf das Dropdown-Menü „Schriftgröße“, um die Textgröße anzupassen.

Schritt 6. Wenn Sie „Text“ auswählen, klicken Sie bitte auf die Dropdown-Menüs „Schriftart“ und „Hintergrund“ und wählen Sie die gewünschte Farbe und Transparenz aus.

Schritt 7. Wenn Sie „Bild“ auswählen, klicken Sie bitte auf die Dropdown-Menüs für die Bildtransparenz und wählen Sie die gewünschte Transparenz aus.

Notiz:

Bei Bildüberlagerungen ist darauf zu achten, dass Größe und Auflösung zum Videostream passen.

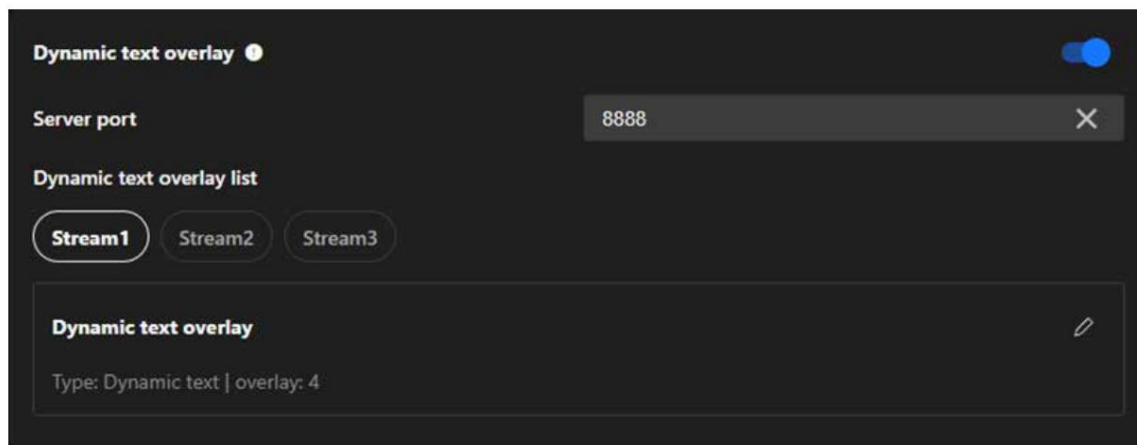
Fortschrittlich

Die Seite „Erweitert“ in den Overlay-Einstellungen bietet vor allem fortgeschrittene Funktionen, mit denen Benutzer die Overlay-Inhalte von Überwachungsvideos an spezifische Anforderungen anpassen können. Diese Einstellungsseite ist besonders nützlich für die Anzeige dynamischer Echtzeitdaten oder in professionellen Anwendungsszenarien und bietet die notwendige Flexibilität und Funktionalität.

Bild

• Dynamische Textüberlagerung

Die dynamische Textüberlagerung ist eine fortschrittliche Funktion der VIVOTEK-Kameras, mit der Benutzer dynamische Echtzeitinformationen aus externen Datenquellen in Überwachungsaufnahmen einblenden können. Diese Funktion erhöht die Praktikabilität und den Informationswert der Aufnahmen und macht sie somit für verschiedene Überwachungsszenarien geeignet.



Schritte zum Festlegen der dynamischen Textüberlagerung:

Schritt 1. Dynamische Textüberlagerung aktivieren

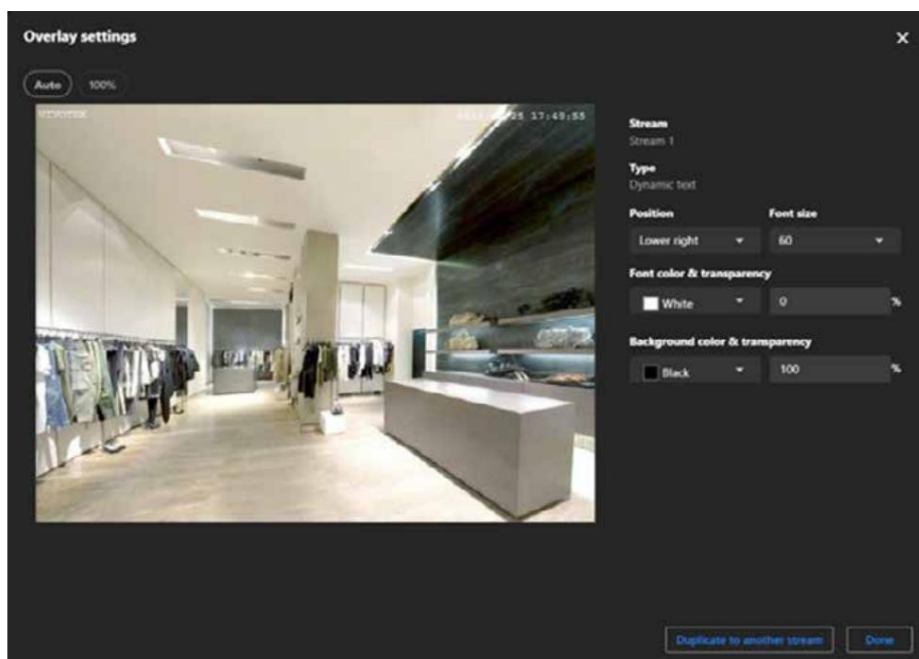
Schritt 2. Stellen Sie sicher, dass der Server-Port auf einen verfügbaren Port eingestellt ist (Standard: 8888) oder geben Sie gegebenenfalls einen anderen ungenutzten Port an.

Schritt 3. Stellen Sie sicher, dass Ihre externe Datenquelle so konfiguriert ist, dass sie Daten an die IP-Adresse der Kamera und den angegebenen Serverport (z. B. 8888) sendet.

Schritt 4. Stellen Sie sicher, dass das Datenformat mit den Anforderungen der Kamera kompatibel ist (Informationen zu zulässigen Formaten finden Sie in der VIVOTEK API-Dokumentation).

Schritt 5. Wählen Sie den Stream aus, dem Sie die dynamische Textüberlagerung hinzufügen möchten.

Schritt 6. Klicken Sie in der „Liste der dynamischen Textüberlagerungen“ auf das Bearbeiten-Symbol (Stift), um die Überlagerungsdetails zu konfigurieren.

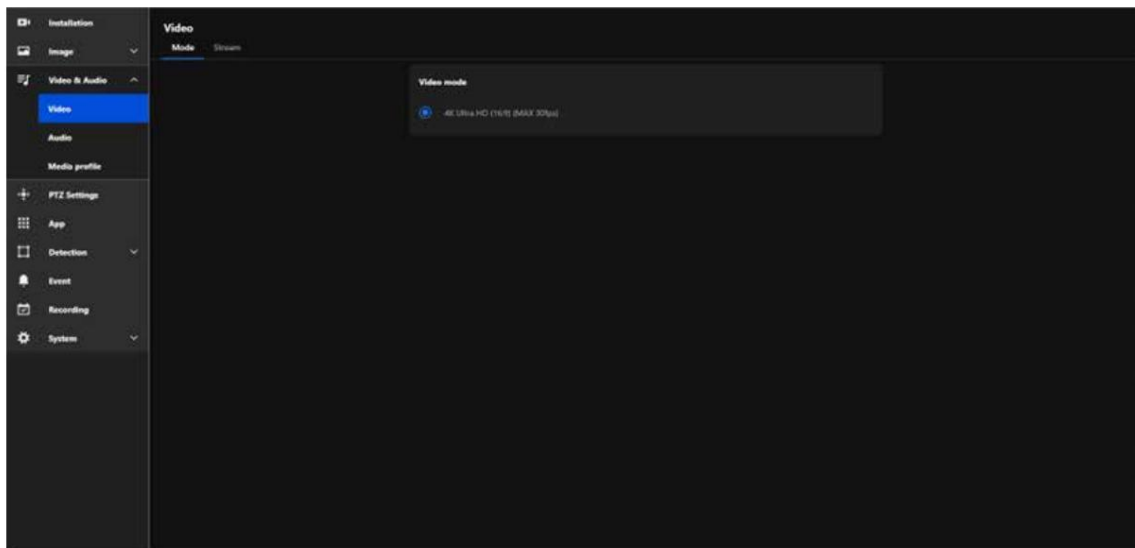


Video & Audio

Die Video- und Audioeinstellungen dienen in erster Linie dazu, durch Anpassung von Auflösung, Bildrate und Komprimierungsformaten eine hohe Video- und Audioqualität zu gewährleisten und gleichzeitig Bandbreite und Speicherplatz durch Multistream-Optionen zu optimieren. Diese Einstellungen verbessern die Überwachungsmöglichkeiten durch hohe Auflösung, flüssige Bildraten und Zwei-Wege-Audio und bieten Flexibilität für verschiedene Szenarien wie Nachtmodus oder Außenaufnahmen. Darüber hinaus verbessern sie die Systemflexibilität und -kompatibilität durch die Unterstützung mehrerer Medienformate und -protokolle für eine nahtlose Integration über verschiedene Geräte hinweg.

Optimierung der Überwachungseffizienz durch flexible Videoeinstellungen

Die Videoeinstellungen sind in die Seite „Modus“ und die Seite „Stream“ unterteilt, die beide primär zur Konfiguration der Videoausgabe der Kamera dienen und dem Benutzer eine flexible Kontrolle über Videoqualität und Ressourcenmanagement ermöglichen.



● Videomodus



Der Videomodus ermöglicht es Benutzern, die Videoleistung der Kamera an spezifische Überwachungsanforderungen anzupassen und dabei ein Gleichgewicht zwischen hoher Videoqualität und Ressourceneffizienz zu erzielen. Die wichtigsten Funktionen sind:

Definiert die Videoauflösung

Der Videomodus legt die maximale Auflösung fest, die die Kamera ausgeben kann, z. B. **4K Ultra HD**, Full HD oder andere Auflösungen, und gewährleistet so qualitativ hochwertige Videoübertragungen.

Video & Audio

Seitenverhältnis festlegen

Konfiguriert das Seitenverhältnis des Videos (z. B. 16:9) und optimiert so das Sichtfeld für moderne Breitbilddisplays.

Steuert die Bildrate

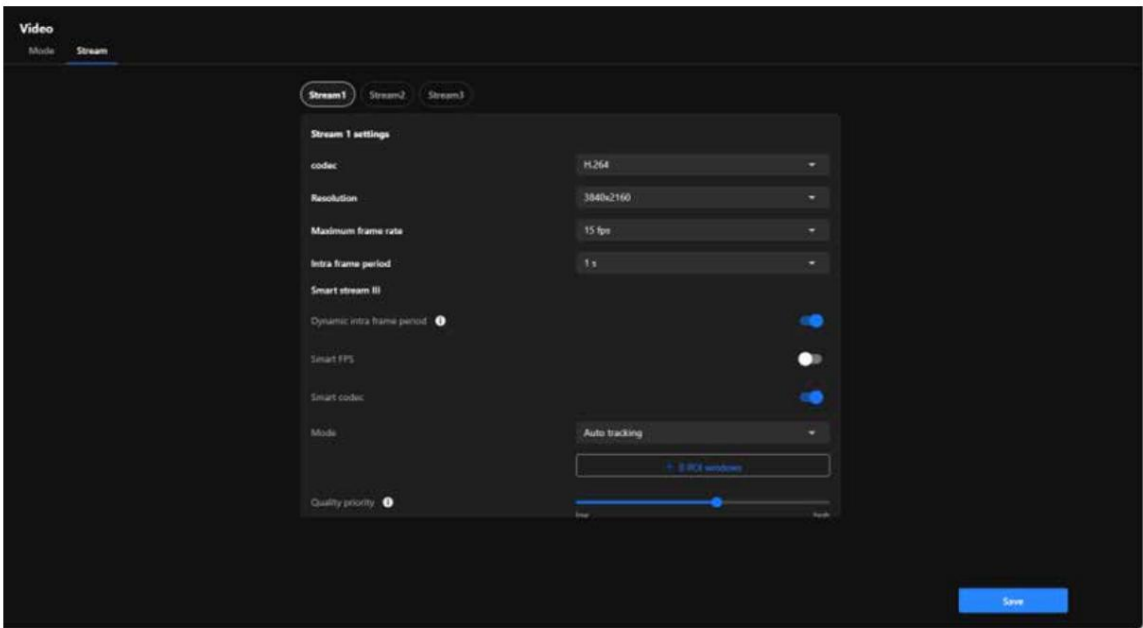
Legt die maximale Anzahl an Bildern pro Sekunde (fps) fest, z. B. 30 fps, für eine flüssige Bewegungserfassung in dynamischen Umgebungen.

Legt Videoparameter fest

Legt die allgemeinen Leistungsgrenzen für das Video fest, einschließlich Auflösung und Bildrate, welche die Klarheit, die flüssige Wiedergabe und die Ressourcennutzung des Videostreams beeinflussen.

● Videostream

Video Stream bietet flexible Videoausgabeoptionen für vielfältige Überwachungsanforderungen bei gleichzeitig optimierter Bandbreiten- und Speichernutzung. Dank Multi-Stream-Konfiguration, intelligenter Komprimierungstechnologie und regionaler Optimierung ist Video Stream ein wichtiges Werkzeug zur Steigerung der Effizienz und Anpassungsfähigkeit von Überwachungssystemen in unterschiedlichsten Anwendungen.



Codec

Definiert das Videokomprimierungsformat.

MJPEG	Hohe Qualität und Klarheit erforderlich, ausreichende Bandbreite vorhanden.
H.264	Dynamische Szenen mit stabiler Bandbreite.
H.265	Umgebungen mit hoher Auflösung oder begrenzter Bandbreite.

Video & Audio

Auflösung

Die Auflösung ist ein entscheidender Parameter der Bildqualität und beeinflusst direkt die Klarheit von Überwachungsvideos, den Speicherbedarf und die Bandbreitennutzung. Bei der Wahl der geeigneten Auflösung müssen der Überwachungszweck, die Anforderungen des jeweiligen Szenarios und die verfügbaren Ressourcen berücksichtigt werden.

Maximale Bildrate

Die maximale Bildrate ist ein Parameter, der die Anzahl der von einer Kamera pro Sekunde aufgenommenen und übertragenen Videobilder bestimmt. Die Bildrate beeinflusst die Videowiedergabe, die Detailgenauigkeit, die Bandbreitennutzung und den Speicherbedarf. Bei der Wahl einer geeigneten Bildrate müssen das Überwachungsszenario, der Zweck und die Systemressourcen berücksichtigt werden. Empfohlene Bildrateneinstellungen:

Hochgeschwindigkeitsbewegungen (z. B. Verkehr, Sport)	30 Bilder pro Sekunde oder höher	Erfasst flüssige, sich schnell bewegende Szenen und eignet sich daher für Szenarien, die eine klare Beobachtung von sich bewegenden Objekten erfordern.
Allgemeine Überwachung (z. B. Geschäfte, Büros)	15 Bilder pro Sekunde	Bietet ein ausgewogenes Verhältnis zwischen Videoqualität und Bandbreitennutzung und ist somit ideal für die meisten alltäglichen Überwachungsaufgaben.
Statische Szenarien (z. B. Lagerhallen, Parkplätze)	10 Bilder pro Sekunde oder weniger	Spart Ressourcen und eignet sich für Szenarien mit Schwerpunkt auf statischen Umgebungen.
Niedrige Bandbreite Umgebungen oder Fernüberwachung	5 Bilder pro Sekunde	Reduziert die Bandbreitennutzung und eignet sich daher ideal für Situationen mit Netzwerkbeschränkungen oder grundlegenden Überwachungsanforderungen.

Video & Audio

Intra-Frame-Periode

Die Intra-Frame-Periode bestimmt, wie oft die Firmware ein Intra-Frame (I-Frame) einfügt. Je kürzer die Dauer, desto besser ist in der Regel die Videoqualität, allerdings auf Kosten einer höheren Netzwerkbandbreite. Empfohlene Einstellungen basierend auf Anwendungsfällen:

Hochdynamische Szenarien (z. B. Verkehrsüberwachung)	1 Sekunde	Erzeugt schnell vollständige Bilder, geeignet zur Erfassung sich schnell bewegender Ziele.
Allgemeine Überwachung (z. B. Büros, Lager)	2 Sekunden	Bietet ein ausgewogenes Verhältnis zwischen Videoqualität, Bandbreite und Speichernutzung und ist somit ideal für die meisten alltäglichen Überwachungsszenarien.
Statische Szenarien (z. B. Lagerhallen)	3 Sekunden oder länger	Reduziert die Anzahl der I-Frames, um Ressourcen zu sparen; geeignet für Szenen mit geringer Variation.
Fernzugriff oder Niedrige Bandbreite Überwachung	1–2 Sekunden	Verhindert Bildverschlechterungen und gewährleistet eine reibungslose und qualitativ hochwertige Fernanzeige.

Smart Stream III

Smart Stream III ist eine fortschrittliche Videooptimierungstechnologie für VIVOTEK-Kameras, die Bandbreite und Speicherplatz dynamisch verwaltet und dabei wichtige Details und Bildqualität beibehält. Durch die intelligente Anpassung von Bildraten, Komprimierungsraten und regionaler Qualität reduziert diese Technologie effektiv den Bandbreiten- und Speicherbedarf und eignet sich daher besonders für Szenarien mit begrenzter Bandbreite oder bei Langzeitaufnahmen. Die Konfigurationseinstellungen für Smart Stream III sind wie folgt:

• Dynamische Intraframe-Periode

Passt die I-Frame-Frequenz automatisch an die Szenenaktivität an. Erreicht eine bessere Optimierung durch ein ausgewogenes Verhältnis zwischen Bildschärfe und Ressourcennutzung.

• Intelligente FPS

Die Bildrate wird dynamisch an die Bewegung in der Szene angepasst. Starke Bewegung erhöht die Bildrate für flüssigere Darstellung, während geringe Bewegung sie verringert, um Bandbreite zu sparen.

• Intelligenter Codec

Nutzt fortschrittliche Komprimierungstechnologie, um Details in Bereichen mit schnellen Bewegungen zu erhalten, während statische Bereiche stark komprimiert werden. Optimiert Bandbreite und Speichernutzung, ohne wichtige Informationen zu verlieren.

• Modus

Definiert, wie die Kamera den relevanten Bereich (ROI) im Video verwaltet und Bildqualität sowie Ressourcennutzung optimiert. Der Modus bietet verschiedene Betriebsoptionen, sodass Benutzer je nach Überwachungsbedarf und Szenenmerkmalen flexibel zwischen automatischer, manueller oder hybrider ROI-Verfolgung wählen können.

Video & Audio

Automatische Verfolgung	Hochdynamische Szenarien (z. B. Verkehr, öffentliche Räume) Automatisierte Verarbeitung, keine manuelle Konfiguration erforderlich Kann sich nicht auf bestimmte statische Bereiche konzentrieren
Handbuch	Statische Szenarien (z. B. Büros, Lagerhallen) Präzise Kontrolle über Interessensgebiete Nicht geeignet für dynamische Umgebungen
Hybrid	Gemischte dynamische und statische Szenarien (z. B. Einzelhandel, Eingangsüberwachung) Gleicht statische und dynamische Anforderungen aus, hohe Flexibilität Möglicherweise ist eine zusätzliche Konfiguration erforderlich.

Wie füge ich das ROI-Fenster hinzu?

Schritt 1. Klicken Sie auf die Schaltfläche „+ ROI Windows“.

Schritt 2. Ziehen Sie die ausgewählten Bereiche per Drag & Drop, um die ROI-Bereiche in der Vorschau anzupassen.

Notiz:

Es können mehrere ROI-Bereiche hinzugefügt werden, um verschiedene kritische Standorte wie Eingänge, Kassen oder Zufahrten gezielt anzusprechen.

Schritt 3. Klicken Sie auf die Schaltfläche Speichern.

Qualitätspriorität Die

Qualitätspriorität ist ein Parameter, der verwendet wird, um die Priorität der Bildqualität festzulegen. Dabei wird für bestimmte ROI-Bereiche eine höhere oder niedrigere Bildqualität bereitgestellt, um ein Gleichgewicht zwischen Ressourcennutzung und Bildschärfe zu schaffen.

Bitratensteuerung

Die Bitratensteuerung dient dazu, die Übertragungsbitrate von Videos anzupassen und so ein Gleichgewicht zwischen Bildqualität und Bandbreitennutzung zu erreichen.

Feste Qualität

Wenn das Überwachungsszenario eine hohe Bildqualität erfordert und die Netzwerk- und Speicherressourcen relativ ausreichend sind, wird die Verwendung der festen Qualität empfohlen, um sicherzustellen, dass keine Bilddetails verloren gehen.

Begrenzte Bitrate

Wenn die Überwachungsumgebung nur über begrenzte Bandbreite oder Speicherkapazität verfügt, empfiehlt es sich, die Option „Begrenzte Bitrate“ zu wählen, um die Ressourcennutzung durch Begrenzung der Bitrate präzise zu steuern.

Video & Audio

Zielqualität

Die Zielqualität legt den angestrebten Qualitätsstandard des Videos fest und weist die Kamera an, das Video zu komprimieren, um die gewünschte Bildschärfe zu erreichen. Zweck und Anwendungsbereiche:

Option	Zweck	Auswirkungen auf den Bach	Anwendung
Maßgeschneidert	Benutzerdefinierte Qualitätseinstellungen	Manuelle Einstellung für präzise Strahlsteuerung	Szenarien, die maßgeschneiderte Strömungsparameter erfordern
Medium	Geringere Anforderungen an die Zielqualität	Geringere Qualität, reduzierte Bitrate	Datenströme mit niedriger Priorität oder Netzwerke mit geringer Bandbreite
Standard	Ausgewogenes Verhältnis von Qualität und Effizienz	Mittlere Qualität mit kontrollierter Bitrate (us-) Alter	Allgemeine Überwachung
Gut	Verbessert die Wasserqualität Das	Bessere Detailgenauigkeit bei gleichzeitig angemessener Bitrate	Belebte Bereiche mit mittleren Detailanforderungen
Ausführlich	Bietet eine hohe Detailgenauigkeit im Videostream.	Höhere Qualität, schärfere Bilder, erhöhte Bitrate	Überwachung, die eine detaillierte Objekterkennung erfordert
Exzellent	Maximiert den Durchfluss Qualität	Höchste Bildschärfe und Bitratennutzung	Hochsicherheitsüberwachung, Aufzeichnung kritischer Beweismittel

Maximale Bitrate

Die maximale Bitrate ist eine Funktion, mit der die Bitrate des Videostreams der Kamera begrenzt wird. Ziel ist es, Bandbreite und Speicherplatz zu schonen und gleichzeitig die Videoqualität zu erhalten. Durch die korrekte Konfiguration der maximalen Bitrate wird nicht nur ein stabiler Systembetrieb sichergestellt, sondern auch die Ressourcenzuweisung optimiert. Daher ist sie ein unverzichtbares Werkzeug in Systemen mit mehreren Kameras und Umgebungen mit geringer Bandbreite.

Politik

Die Funktion und der Zweck der Richtlinie bestehen darin, Flexibilität und Spezifität bei der Videoübertragung zu erreichen, Bildrate und Bildqualität je nach Szenarioanforderungen auszubalancieren und dadurch die Effektivität, Stabilität und Ressourceneffizienz des Überwachungssystems zu verbessern.

Video & Audio

Bildratenpriorität	Geeignet für dynamische Überwachungsszenarien, gewährleistet eine reibungslose Videowiedergabe und ermöglicht so Echtzeitüberwachung und schnelle Reaktion.
Priorität der Bildqualität	Geeignet für statische oder detailreiche Szenarien, bietet es eine höhere Bildschärfe, um wichtige Details effektiv zu erfassen.

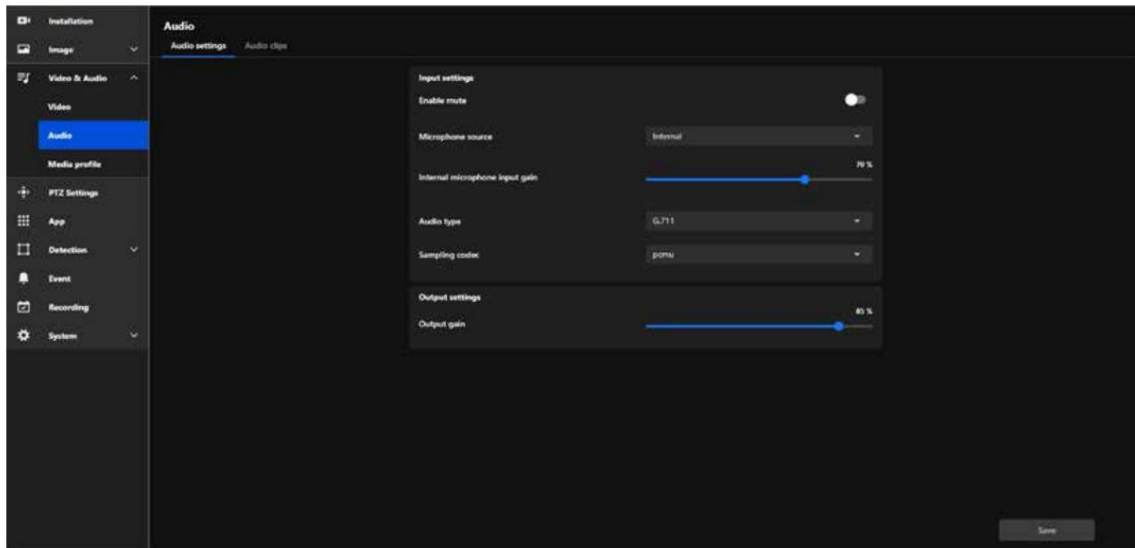
Smart Q

Smart Q ist eine intelligente Bildverwaltungsfunktion, die Bildqualität und Ressourcennutzung dynamisch optimiert. Sie verbessert nicht nur die Effektivität von Überwachungsvideos, sondern auch die Auslastung von Bandbreite und Speicherplatz. Dies ist besonders geeignet für Szenarien, die Langzeitaufzeichnung, Detailgenauigkeit oder ressourcenbeschränkte Überwachungssysteme erfordern.

Video & Audio

Konfigurieren der Audioeinstellungen für verbesserte Ein- und Ausgabe Leistung

Die Gesamtfunktionalität dieser Seite ist auf die umfassende Verwaltung der Audiofunktionen der Kamera ausgelegt und deckt alles ab, von der Echtzeit-Audioeingabe und -ausgabe bis hin zur Verwaltung der Audioclip-Wiedergabe.



Zu seinen Zwecken gehören:

- **Steigerung der Gesamteffektivität der Überwachung durch die Nutzung von Audio zur Unterstützung von Video für eine effizientere Überwachung Sicherheitsüberwachung.**
- **Verbesserung der Kommunikations- und Reaktionsfähigkeit bei Vorfällen durch die Integration von Zwei-Wege-Kommunikation und Alarmfunktionen zur Erfüllung unterschiedlichster situativer Anforderungen.**
- **Bereitstellung flexibler Steuerungs- und Verwaltungstools, die eine einfache Konfiguration sowohl für Echtzeit- als auch für Echtzeitanwendungen ermöglichen Audioverarbeitung und Wiedergabe vorab aufgenommener Audiodateien.**

Ermöglicht die Interaktion mit externen Geräten zur Erweiterung funktionaler Anwendungen. Diese Funktionen machen den Einsatz von Audio in Überwachungsumgebungen flexibler und effizienter.

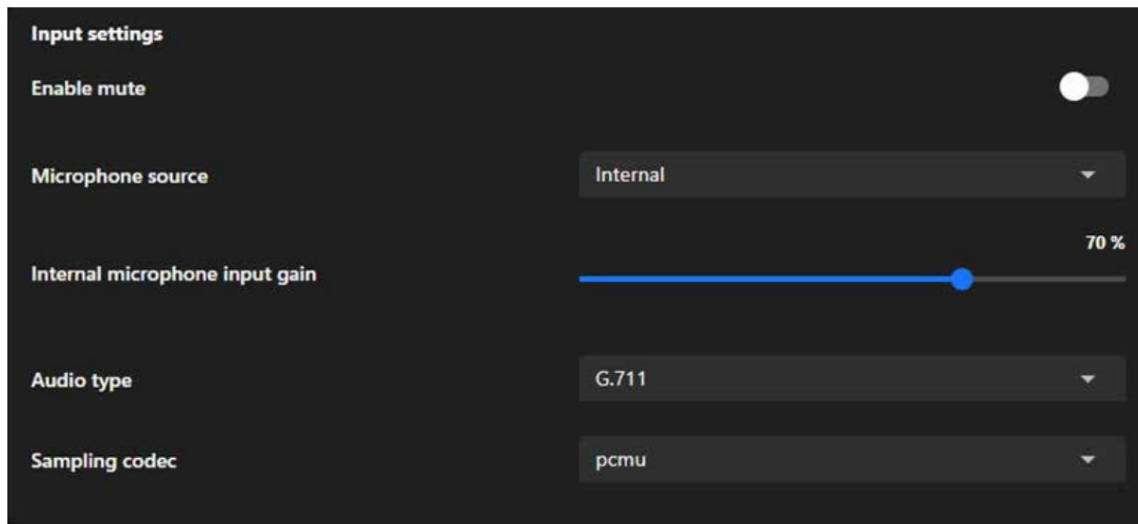
Audioeinstellungen

Ziel dieser Einstellung ist es, detaillierte Konfigurationen für Audioeingang und -ausgang bereitzustellen, die Audiofunktionalität von Überwachungskameras zu optimieren und es Benutzern zu ermöglichen, Audioqualität, Lautstärke und Quelle an ihre spezifischen Bedürfnisse anzupassen.

Video & Audio

• Eingabeeinstellungen

Ziel dieser Einstellung ist es, detaillierte Konfigurationen für Audioeingang und -ausgang bereitzustellen, die Audiofunktionalität von Überwachungskameras zu optimieren und es Benutzern zu ermöglichen, Audioqualität, Lautstärke und Quelle an ihre spezifischen Bedürfnisse anzupassen.



Stummschaltung aktivieren

Die Stummschaltungsfunktion ermöglicht es Benutzern, die Audioeingabe zu deaktivieren und so die Privatsphäre zu wahren oder unerwünschte Tonaufnahmen zu verhindern.

Mikrofonquelle

Die Mikrofonquelle ermöglicht es dem Benutzer, zwischen internen und externen Mikrofonen zu wählen, um sich an unterschiedliche Anforderungen an die Audioaufnahme und unterschiedliche Hardwarekonfigurationen anzupassen.

Verstärkung des internen/externen Mikrofoneingangs

Die interne/externe Mikrofoneingangsverstärkung ermöglicht es dem Benutzer, die Empfindlichkeit des Mikrofons anzupassen und so die Audioaufnahmepegel an unterschiedliche Umgebungsgeräuschbedingungen anzupassen und eine klare Tonaufnahme zu gewährleisten.

Audiotyp

Die Einstellung für den Audiotyp bestimmt das Codierungsformat für Audio und sorgt so für ein ausgewogenes Verhältnis zwischen Qualität, Bandbreitennutzung und Kompatibilität:

AAC

Bietet qualitativ hochwertiges Audio mit effizienter Komprimierung, ideal für Umgebungen, die einen klaren Klang mit minimalen Verzerrungen erfordern.

AAC-Bitrate

Die AAC-Bitrate ist eine Untereinstellung unter „Audiotyp“, die nur bei Auswahl von AAC angezeigt wird. Sie dient zur Feinabstimmung der Qualität und Ressourcennutzung des AAC-Audioformats und ermöglicht es Benutzern, die Konfiguration an praktische Szenarien wie Bandbreiten- oder Speicherbedarf anzupassen.

Video & Audio

G.711

Ein weit verbreiteter Codec für die Echtzeitkommunikation, der eine gute Audioqualität bei geringer Komprimierung bietet und sich für Netzwerke mit ausreichender Bandbreite eignet.

Sampling-Codec

Definiert die Komprimierungsmethode für den ausgewählten Audiotyp (typischerweise G.711), was sich auf die Audioqualität und Kompatibilität auswirkt:

PCMU	Es wird häufig in Nordamerika und Japan eingesetzt und bietet eine etwas höhere Audioqualität mit dem Schwerpunkt auf maximaler Dynamik für optimale Sprachverständlichkeit.
PCMA	Es wird häufig in Europa und anderen Regionen eingesetzt und bietet eine mit PCMU vergleichbare Qualität, ist aber für andere Telekommunikationsstandards optimiert.

G.726

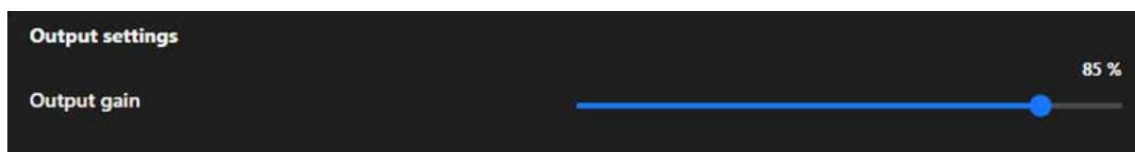
Bietet eine moderate Komprimierung, die Qualität und Bandbreitennutzung in Einklang bringt und sich für Umgebungen mit Bandbreitenbeschränkungen eignet.

G.726 Bitrate

Die G.726-Bitrate ist eine spezielle Konfigurationsoption, die je nach Auswahl des Audiotyps angezeigt wird und nur bei Auswahl von G.726 aktiv ist. Mit dieser Option können Benutzer die Codierungsbitrate weiter anpassen, um die Einstellungen an praktische Anforderungen wie Netzwerkbandbreite oder Speicherplatzbeschränkungen anzupassen.

• Ausgabeeinstellungen

Benutzer können die Lautstärke des Audioausgangs manuell an unterschiedliche Anwendungsumgebungen anpassen.



Ausgangsverstärkung

Benutzer können die Lautstärke der Audioausgabe manuell an verschiedene Anwendungsumgebungen anpassen:

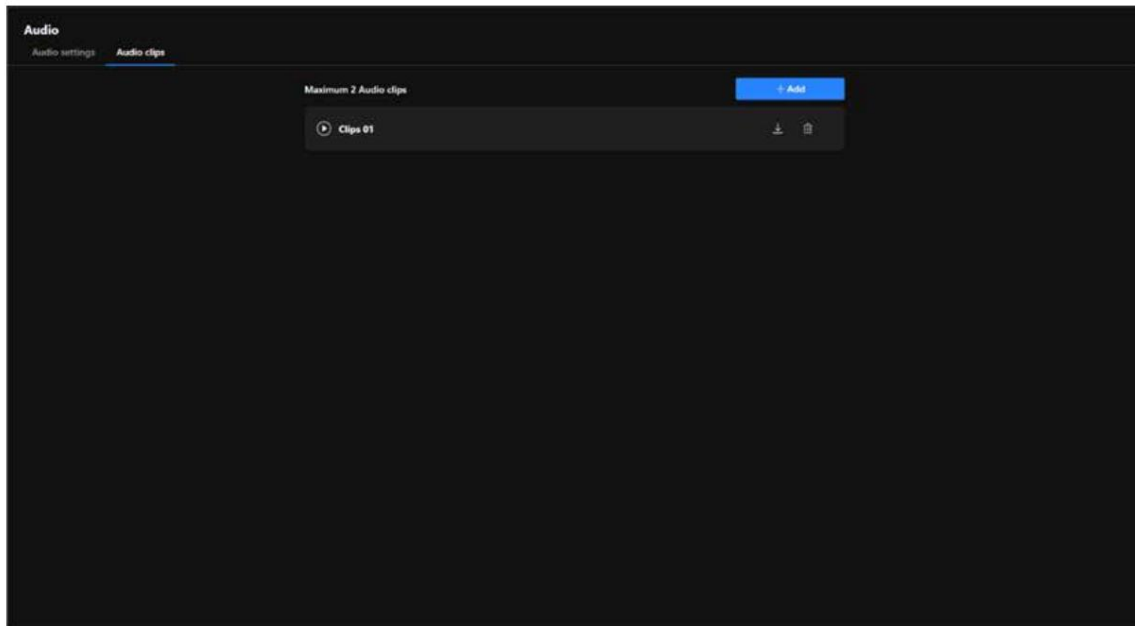
In Szenarien, die eine hohe Lautstärke erfordern (wie z. B. Alarmer oder großflächige Durchsagen), kann die Verstärkung erhöht werden, um die Lautstärke zu steigern.

In Szenarien, die eine geringere Lautstärke erfordern (z. B. im Datenschutzmodus oder im lautlosen Betrieb), kann die Verstärkung reduziert werden, um Audiostörungen zu minimieren.

Video & Audio

Audioclips

Die Funktion „Audio Clips“ wurde entwickelt, um Audio mit Ereignisauslösern zu integrieren und so effizientere Benachrichtigungen, Warnungen und Interaktionen zu ermöglichen. Dadurch wird der Anwendungswert von Kameras in Überwachungs- und Sicherheitsszenarien erhöht.



Zweck der Funktionalität:

Verbesserung der Reaktionsfähigkeit bei Zwischenfällen

Durch das Abspielen von akustischen Warnmeldungen oder Benachrichtigungen kann es in der Nähe befindliches Personal umgehend über Anomalien oder potenzielle Bedrohungen informieren.

Stärkung der Sicherheitsabschreckung

Beim Erkennen von Eindringlingen oder verdächtigen Aktivitäten können vorab aufgezeichnete Warnmeldungen oder Alarmtöne abgespielt werden, um potenzielle Bedrohungen wirksam abzuschrecken.

Erhöhung der Flexibilität der Überwachung

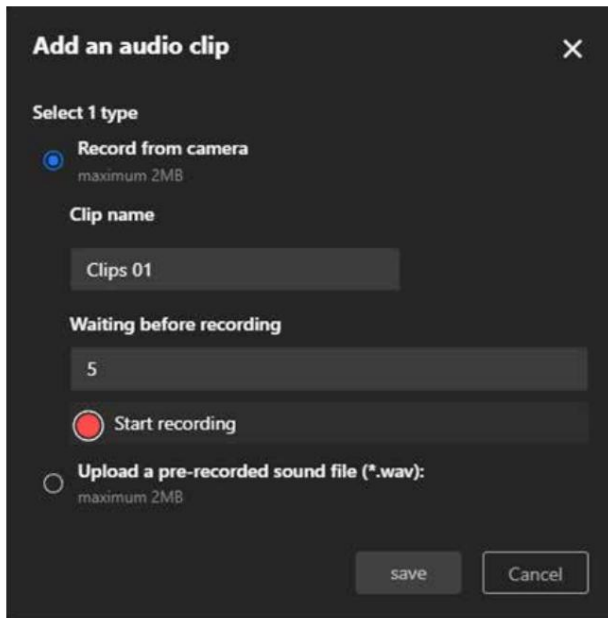
Unterstützung für anpassbare Audioinhalte für verschiedene Szenarien, wie z. B. das Abspielen von Begrüßungsansagen in Geschäften oder das Durchsagen von Verkehrsregeln auf Parkplätzen.

Vereinfachung der betrieblichen Prozesse

Die automatische Audiowiedergabe verringert den Bedarf an manuellen Eingriffen und verbessert so die Effizienz der Überwachung weiter.

Video & Audio

Schritte zum Hinzufügen von Audioclips:



Schritt 1. Wählen Sie unter „1 Typ auswählen“ eine der beiden Optionen für die Audioquelle aus.

Aufnahme von der Kamera

Verwenden Sie das in die Kamera eingebaute Mikrofon, um Audio aufzunehmen. Die maximale Dateigröße beträgt 2 MB.

Laden Sie eine vorab aufgenommene Audiodatei

hoch. Laden Sie eine bereits vorhandene Audiodatei hoch, die im .wav-Format vorliegen und 2 MB nicht überschreiten darf.

Schritt 2. Geben Sie im Feld „Clipname“ einen Namen für den Audioclip ein (z. B. „Clips 01“), um ihn später identifizieren zu können.

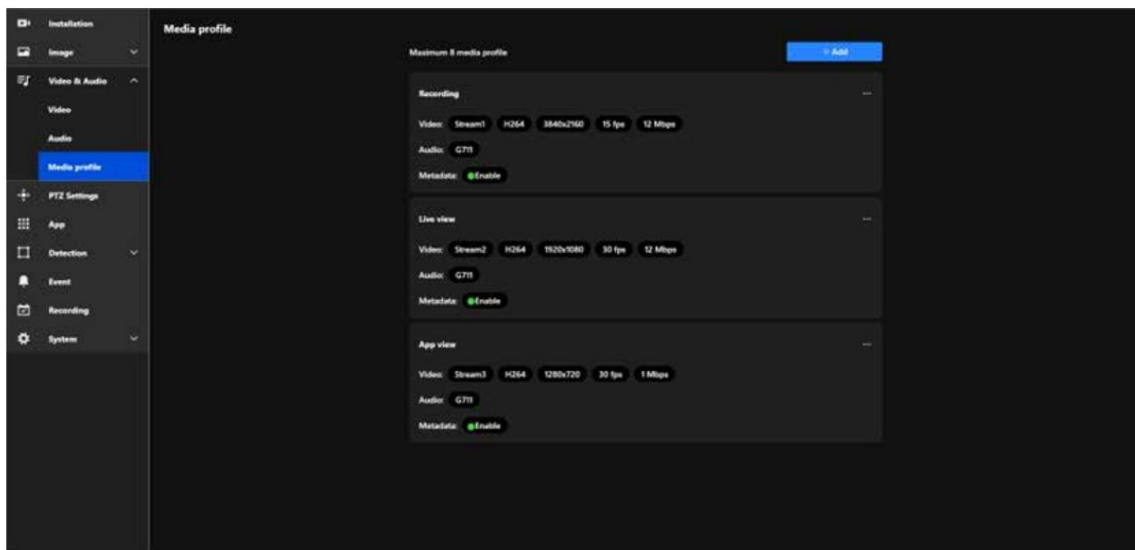
Schritt 3. Geben Sie im Feld „Warten vor der Aufnahme“ die Anzahl der Sekunden ein, um den Beginn der Aufnahme zu verzögern (z. B. 5 Sekunden), um Zeit für die Vorbereitung vor Beginn der Aufnahme zu ermöglichen.

Schritt 4. Klicken Sie auf die rote Schaltfläche „Aufnahme starten“, um einen Countdown für die angegebene Zeit zu starten. Anschließend beginnt das System mit der Audioaufnahme und speichert die Aufnahme nach deren Abschluss automatisch zur späteren Wiedergabe.

Video & Audio

Konfigurieren von Medienprofilen zur Optimierung der Videoleistung für Vielseitige Anwendungsmöglichkeiten

Bei VIVOTEK-Kameras zeigt die Funktion „Medienprofil“ primär voreingestellte Streamparameter an und ermöglicht es dem Benutzer, Video, Audio und Metadaten zu aktivieren oder zu deaktivieren. Diese Funktionalität vereinfacht die Streamverwaltung und bietet gleichzeitig die Flexibilität, sich an verschiedene Überwachungsszenarien wie Aufzeichnung, Live-Ansicht und mobilen Zugriff anzupassen, wodurch ein effizientes und effektives Überwachungsmanagement gewährleistet wird.



Vorteile und Funktionen:

Vereinfachtes Stream-Management

Benutzer können Video-, Audio- und Metadatenfunktionen für jedes Profil schnell aktivieren oder deaktivieren.

Clear Stream Display

Das Medienprofil zeigt die vorkonfigurierten Streamparameter (z. B. Auflösung, Bildrate, Bitrate) zur einfachen Identifizierung und Verwaltung an.

Flexible Anwendungsszenarien

Nutzer können mehrere Profile für unterschiedliche Bedürfnisse erstellen, zum Beispiel:

Aufnahme: Hochauflösendes Video aktiviert.

Live-Ansicht: Hohe Bildrate für flüssige Echtzeitwiedergabe.

App-Ansicht: Video mit niedriger Auflösung zur Bandbreiteneffizienz.

Optimiertes Ressourcenmanagement

Durch Aktivieren oder Deaktivieren von Funktionen können Benutzer die Bandbreiten- und Systemressourcennutzung nach Bedarf reduzieren.

Video & Audio

Medienprofil

Das Medienprofil dient zur Anzeige vorkonfigurierter Streamparameter und ermöglicht es Benutzern, bestimmte Funktionen zu aktivieren oder zu deaktivieren, wie zum Beispiel:

Video:

Zeigt die ausgewählten Stream-Einstellungen an und ermöglicht das Aktivieren oder Deaktivieren des Videostreams.

Audio:

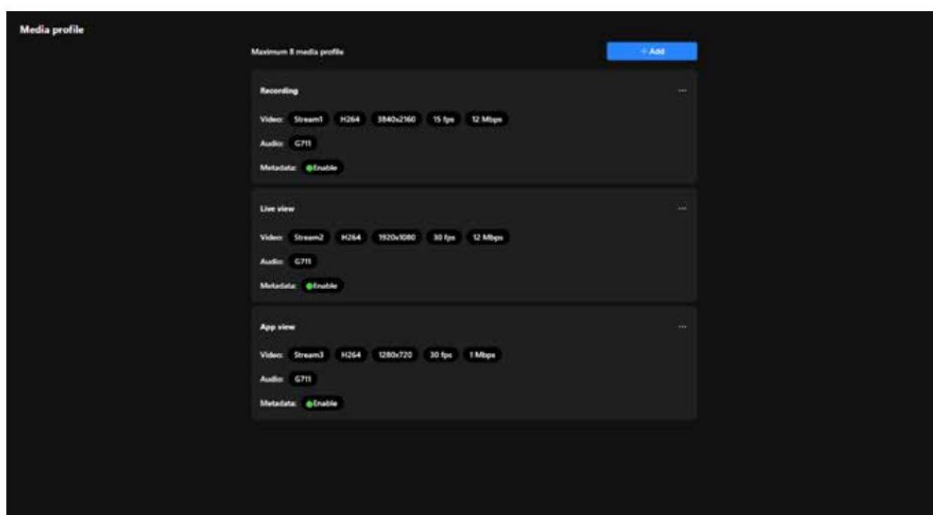
Aktiviert oder deaktiviert die Audiofunktion und zeigt den verwendeten Audiocodec an.

Metadaten:

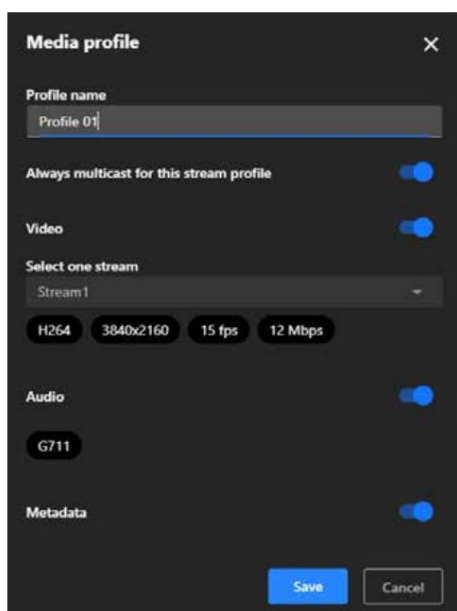
Aktiviert oder deaktiviert Metadatenfunktionen, die weitere Videoanalysen und Ereigniskennzeichnungen unterstützen.

Notiz:

Das Medienprofil erlaubt keine Konfiguration von Videoauflösung, Bildrate oder Bitrate. Diese Parameter sind in den Stream-Einstellungen voreingestellt, und das Medienprofil zeigt lediglich die relevanten Einstellungen an und ermöglicht das Umschalten der Funktionen.



Schritte zum Hinzufügen eines Medienprofils:



Video & Audio

Schritt 1. Suchen Sie auf dem Bildschirm „Medienprofil“ die blaue Schaltfläche „+ Hinzufügen“ und klicken Sie darauf.

Schritt 2. Geben Sie im Feld „Profilname“ einen Profilnamen ein.

Schritt 3. Durch Aktivieren der Option „Für dieses Stream-Profil immer Multicast“ können mehrere Benutzer gleichzeitig auf denselben Videostream zugreifen.

Notiz:

Diese Funktion ist besonders vorteilhaft in Szenarien, die eine effiziente Datenübertragung erfordern, wie beispielsweise groß angelegte Überwachungssysteme. Durch die Verwendung von Multicast sendet die Kamera einen einzigen Videostream, der von mehreren Zuschauern gemeinsam genutzt werden kann. Dies reduziert den Netzwerkbandbreitenverbrauch im Vergleich zum Unicast-Streaming, bei dem separate Streams an jeden Benutzer gesendet werden, erheblich.

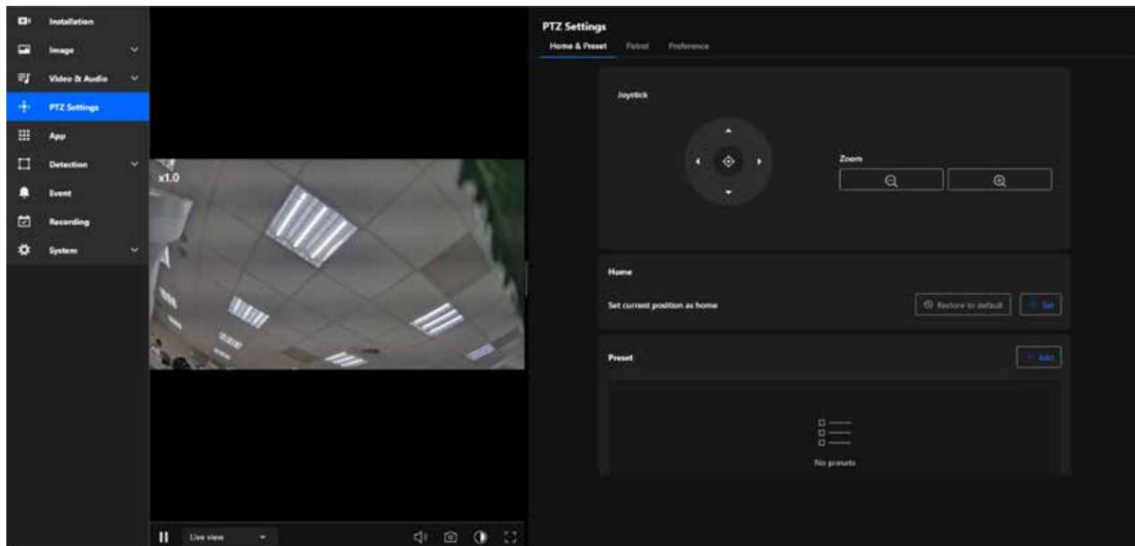
Schritt 4. Aktivieren Sie die Option „Video“ und wählen Sie einen Stream in den Videostream-Einstellungen aus.

Schritt 5. Um die Option „Audio“ zu aktivieren.

Schritt 6. Um die Option „Metadaten“ zu aktivieren.

PTZ-Einstellungen

Die IPv4-Karte spielt eine entscheidende Rolle bei der Einrichtung der Netzwerkkonfiguration der Kamera und gewährleistet eine effektive Kommunikation. Sie ermöglicht eine zuverlässige Verbindung, sowohl lokalen als auch Fernzugriff und die problemlose Integration der Kamera in IPv4-basierte Netzwerke. Diese Konfiguration ist unerlässlich für einen stabilen und effizienten Betrieb in unterschiedlichen Netzwerkimgebungen.



Mühelese Verwaltung und Anpassung der PTZ-Einstellungen für präzise Kamerasteuerung

PTZ Settings bietet umfassende und intuitive Werkzeuge für den flexiblen Betrieb von PTZ-Kameras, darunter Echtzeit-Anpassungen, Voreinstellungsverwaltung und automatisierte Patrouillen. Diese Funktionen steigern die Effizienz der Überwachung und ermöglichen es Anwendern, sich schnell auf wichtige Details zu konzentrieren oder die Anforderungen der großflächigen Szenenüberwachung zu erfüllen.

Startseite & Voreinstellungen

Der Zweck der Registerkarte „Startseite & Voreinstellungen“ in den PTZ-Einstellungen besteht darin, den Benutzern bei der Konfiguration und Verwaltung der primären Blickwinkel und voreingestellten Positionen der Kamera zu helfen, die betriebliche Effizienz zu steigern und schnelle Übergänge zu ermöglichen.

Die Ziele sind folgende:

Vereinfachen Sie die Kamerabedienung

Durch die Konfiguration von Home und Presets können Benutzer schnell zu bestimmten Positionen wechseln und zurückkehren, wodurch der Zeitaufwand für manuelle Anpassungen reduziert wird.

Effizienz der Überwachung steigern

Ermöglicht die effektive Überwachung mehrerer Schlüsselbereiche, insbesondere in Szenarien, die einen häufigen Perspektivwechsel erfordern.

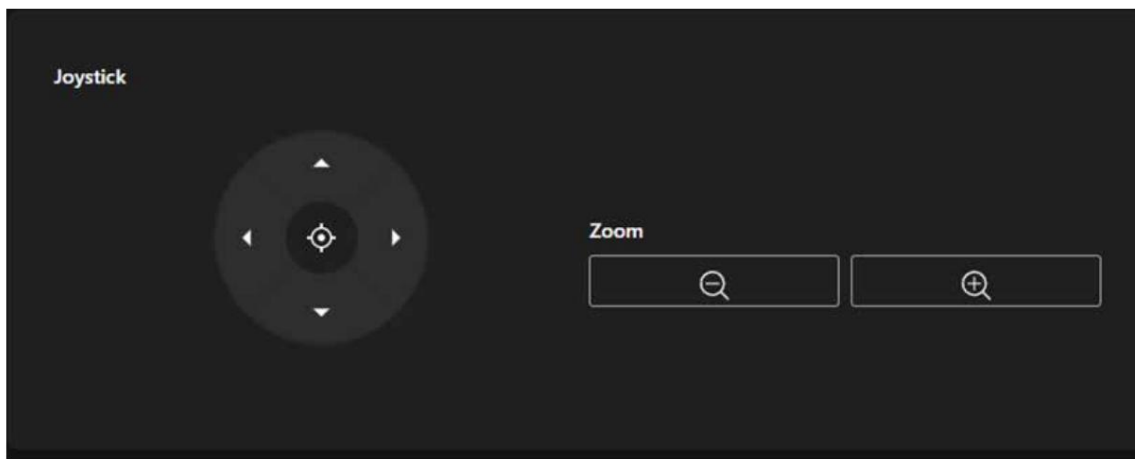
PTZ-Einstellungen

Flexibilität und Präzision erreichen

Ermöglicht es dem Benutzer, die Blickwinkel und Brennweiten der Kamera präzise zu konfigurieren und anzupassen, um den Anforderungen verschiedener Szenarien gerecht zu werden.

● Joystick

Der Joystick ermöglicht dem Benutzer eine präzise Steuerung von Kamerarichtung und Fokus und eignet sich für den Echtzeitbetrieb. Er gewährleistet Flexibilität und Genauigkeit im Überwachungsbereich.



Richtungskontrolle

Bietet einen virtuellen Joystick mit Richtungstasten für oben, unten, links und rechts, der es dem Benutzer ermöglicht, die Schwenk- und Neigefunktion der Kamera in Echtzeit zu bedienen.

Durch Klicken auf die Richtungspfeile wird die Kamera in die entsprechende Richtung bewegt.

Mittelpositionierung

Mit der zentralen Taste kann die Kamera schnell auf ihren aktuellen Mittelpunkt oder ihre Ausgangsposition zurückgesetzt oder neu positioniert werden.

Zoom-Steuerung

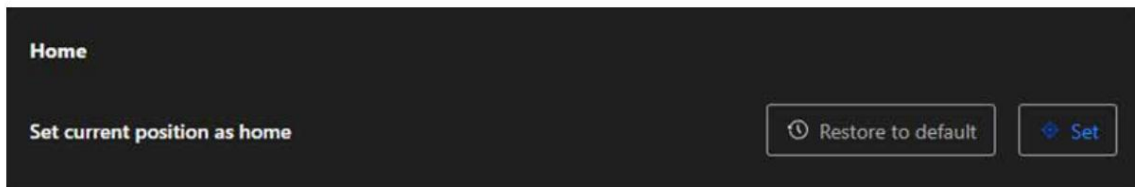
Herauszoomen: Verringert den Zoomfaktor und erweitert so das Sichtfeld der Kamera.

Zoom In: Erhöht den Zoomfaktor und fokussiert so auf Details oder bestimmte Ziele.

PTZ-Einstellungen

● Heim

Die Startseite ermöglicht es Benutzern, den Basis-Blickwinkel der Kamera festzulegen und wiederherzustellen, mit dem Ziel, die Betriebseffizienz zu verbessern, die Kameraverwaltung zu vereinfachen und die Stabilität und Flexibilität des Überwachungsprozesses zu gewährleisten.



Aktuelle Position als Startpunkt festlegen

Durch Drücken der Set-Taste können Benutzer den aktuellen Blickwinkel der Kamera (Richtung und Zoom) als Ausgangsposition festlegen, die als Standard-Basislinie dient.

Auf Standardeinstellungen zurücksetzen

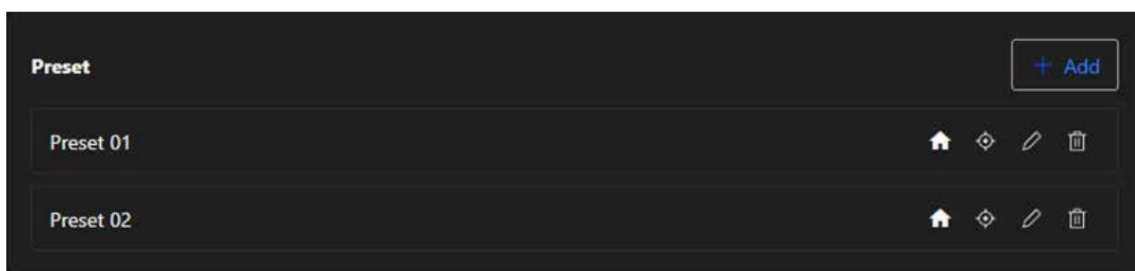
Durch Drücken der Taste „Auf Standard zurücksetzen“ wird die Ausgangsposition der Kamera auf die Werkseinstellungen bzw. die vordefinierte Standardposition zurückgesetzt.

Auf Standardeinstellungen zurücksetzen

Durch Drücken der Taste „Auf Standard zurücksetzen“ wird die Ausgangsposition der Kamera auf die Werkseinstellungen bzw. die vordefinierte Standardposition zurückgesetzt.

● Voreinstellung

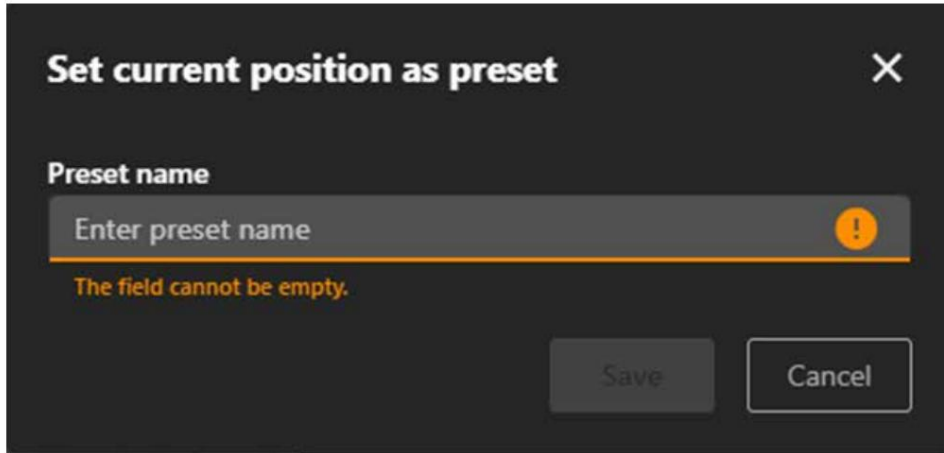
Die Voreinstellung ermöglicht es dem Benutzer, mehrere Überwachungsansichten der Kamera einfach zu verwalten, mit dem Ziel, die Bedienung zu vereinfachen, die Effizienz zu steigern und den Anforderungen einer flexiblen Überwachung in verschiedenen Szenarien gerecht zu werden.



PTZ-Einstellungen

Voreinstellung hinzufügen

Mithilfe der Schaltfläche „+ Hinzufügen“ können Benutzer die aktuelle Kameraansicht (Richtung und Zoom) als neue Voreinstellung speichern und so in Zukunft schnell auf diese Position zugreifen.



Voreingestellte Liste

Gespeicherte Voreinstellungen werden in Listenform angezeigt (z. B. Voreinstellung 01 und Voreinstellung 02). Benutzer können für jede Voreinstellung die folgenden Aktionen durchführen:

Als Zuhause festlegen

Weisen Sie eine voreingestellte Position als Startpunkt zu (über das Haus-Symbol), um einfach zu diesem Punkt zurückkehren zu können.

Auf Voreinstellung umschalten

Klicken Sie auf ein voreingestelltes Element, um die Kamera schnell zu diesem Blickwinkel zu bewegen.

Bearbeiten

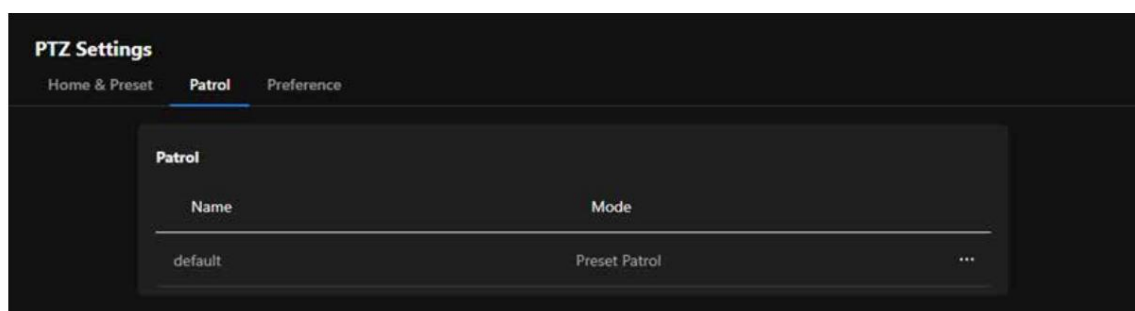
Ändern Sie den Namen oder die zugehörige Ansicht des Presets.

Löschen

Entfernen Sie nicht mehr benötigte Voreinstellungen.

Patrouillieren

Die Patrouillenfunktion nutzt automatisierte Patrouillenrouten, um der Kamera eine effiziente Überwachung mehrerer Überwachungspunkte zu ermöglichen. Dadurch wird der manuelle Eingriff reduziert und ein umfassendes und flexibles Überwachungsmanagement erreicht.



PTZ-Einstellungen

Die Ziele sind folgende:

Erreichen der automatisierten Patrouille

Durch vordefinierte Patrouillenrouten kann sich die Kamera automatisch nacheinander zu verschiedenen Überwachungspunkten bewegen, ideal für großflächige oder gebietsübergreifende Überwachungsanforderungen.

Reduzierung manueller Arbeitsgänge

Die Automatisierungsfunktion macht häufige manuelle Eingriffe überflüssig, erhöht die Effizienz der Überwachung und spart Arbeitskräfte.

Flexible Anpassung an die Szenenanforderungen

Dank individuell anpassbarer Patrouillenrouten und Multimodus-Unterstützung kann sich das System an dynamische Szenarien oder unterschiedliche Überwachungsziele anpassen.

Verbesserung der Sicherheit

Durch die regelmäßige Überwachung aller voreingestellten Punkte stellt das System sicher, dass jeder kritische Bereich zeitnah überwacht wird, wodurch das Risiko von Überwachungslücken verringert wird.

Bearbeiten Sie die Patrouillenroute

Schritt 1. Klicken Sie auf das Symbol „Mehr“ > Schaltfläche „Bearbeiten“.

Klicken Sie auf die Schaltfläche „Bearbeiten“ rechts neben der bestehenden Route.

Edit patrol [X]

Select Preset location

Patrol name
default

Preset list

Preset 01
Preset 02

→

Preset route

1 Preset 01	Dwell time (sec) 1-999	[X]
2 Preset 02	Dwell time (sec) 1-999	[X]

[Save] [Cancel]

Schritt 2. Voreingestellte Punkte auswählen

Die voreingestellte Liste auf der linken Seite zeigt die konfigurierten Punkte an. Durchsuchen Sie die Liste und wählen Sie die Punkte aus, die Sie in Ihre Patrouillenroute aufnehmen möchten.

PTZ-Einstellungen

Schritt 3. Zur Patrouillenroute hinzufügen

Nachdem Sie links einen voreingestellten Punkt ausgewählt haben, klicken Sie auf den Pfeil „ $\rightarrow$ “ in der Mitte, um ihn der Liste der voreingestellten Routen auf der rechten Seite hinzuzufügen.

Schritt 4. Verweilzeit für jeden voreingestellten Punkt einstellen

Weisen Sie in der Liste der voreingestellten Routen jedem hinzugefügten voreingestellten Punkt eine Verweilzeit (in Sekunden) zu. Die Verweilzeit kann zwischen 1 und 999 Sekunden liegen und wird je nach Überwachungsbedarf angepasst.

Schritt 5. Patrouillenbefehl anpassen

Um die Patrouillenreihenfolge voreingestellter Punkte zu ändern, passen Sie deren Positionen in der Liste rechts an (per Drag & Drop oder durch Löschen und erneutes Hinzufügen). Überflüssige voreingestellte Punkte entfernen: Klicken Sie auf das Papierkorbsymbol neben dem jeweiligen Punkt.

Schritt 6. Route speichern

Nachdem Sie alle voreingestellten Punkte, Verweilzeiten und die Reihenfolge bestätigt haben, klicken Sie auf die Schaltfläche „Speichern“ in der unteren rechten Ecke, um die Route zu speichern.

Schritt 7. Patrouillenmodus aktivieren

Kehren Sie zur Kategorie „Installation“ zurück und klicken Sie auf das Patrouillensymbol auf dem PTZ-Bedienfeld, um die Patrouille zu starten.

Präferenz

Die Preference bietet Funktionen wie Geschwindigkeitsanpassung und Zoomanzeige, die es dem Benutzer ermöglichen, die Betriebsparameter der Kamera flexibel an seine Bedürfnisse anzupassen und so ein effizienteres und präziseres Überwachungsmanagement zu erreichen.

PTZ Settings

Home & Preset Patrol **Preference**

Speed

Pan: 0

Tilt: 0

Zoom: 0

Auto pan/patrol: 1

Misc settings

☒ Zoom factor display

Save

PTZ-Einstellungen

Die Ziele sind folgende:

Verbesserung der betrieblichen Flexibilität

Je nach Szenario können unterschiedliche Geschwindigkeitseinstellungen erforderlich sein. Durch Anpassen der Schwenk-, Neige- und Zoomgeschwindigkeit können Benutzer die Kamera präziser steuern.

Anpassung an unterschiedliche Überwachungsbedürfnisse

Im Patrouillenmodus oder im manuellen Betrieb können die Benutzer je nach Wichtigkeit der Szene oder der Geschwindigkeit sich bewegender Ziele geeignete automatische Bewegungs- und Zoomgeschwindigkeiten einstellen.

Verbesserung der Überwachungsgenauigkeit

Die Zoomstufenanzeige ermöglicht es dem Benutzer, die aktuelle Vergrößerung klar zu erkennen, wodurch sie sich für Überwachungsszenarien eignet, bei denen die Fokussierung auf Details erforderlich ist.

Vereinfachung personalisierter Einstellungen

Die Benutzer können Parameter konfigurieren, die ihren betrieblichen Präferenzen entsprechen, wodurch die Gesamteffizienz gesteigert wird.

Geschwindigkeit

Die Speed-Funktion bietet umfassende Kontrolle über die Bewegungsgeschwindigkeit der Kamera, einschließlich Schwenken, Neigen, Zoomen und automatisierter Patrouille, sodass Benutzer die Geschwindigkeit flexibel an die Überwachungsanforderungen anpassen können, um einen präzisen und effizienten Kamerabetrieb zu gewährleisten.

Speed	
Pan	0
Tilt	0
Zoom	0
Auto pan/patrol	1

Schwenken (Horizontale Schwenkgeschwindigkeit)

Steuert die Geschwindigkeit, mit der sich die Kamera nach links und rechts bewegt.

Neigung (Neigungsgeschwindigkeit)

Passt die Geschwindigkeit an, mit der sich die Kamera auf und ab bewegt.

Zoom (Zoomgeschwindigkeit)

Legt die Geschwindigkeit fest, mit der das Objektiv ein- und auszoomt. Ideal, um schnell Details zu fokussieren oder langsam zu zoomen und so einen sanften Übergang zu gewährleisten.

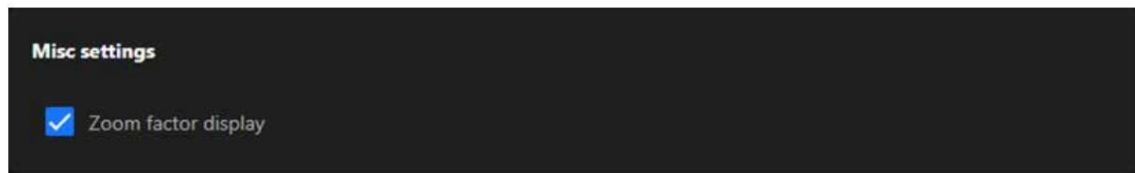
Automatische Schwenk-/Patrouillengeschwindigkeit

Legt die Bewegungsgeschwindigkeit der Kamera im automatischen Schwenk- oder Patrouillenmodus fest. Ermöglicht es Benutzern, die Geschwindigkeit an die jeweiligen Überwachungsanforderungen anzupassen, z. B. eine schnellere Abdeckung großer Bereiche oder eine langsamere Bewegung zur Beobachtung von Details.

PTZ-Einstellungen

Verschiedene Einstellungen

Die Zoomfaktoranzeige in den Sonstigen Einstellungen wurde entwickelt, um die Benutzerkontrolle und den Komfort beim Zoomen zu verbessern und so Präzision und Effektivität bei der Überwachung zu gewährleisten, insbesondere in Szenarien, die häufiges Zoomen oder das Fokussieren auf Details erfordern.



Zoomfaktor-Anzeige

Wenn diese Option ausgewählt ist, zeigt das System den aktuellen Zoomfaktor an, sobald die Zoomfunktion der Kamera verwendet wird. Der Zoomfaktor wird üblicherweise numerisch dargestellt, sodass Benutzer die aktuelle Vergrößerung des Objektivs leicht erkennen können.

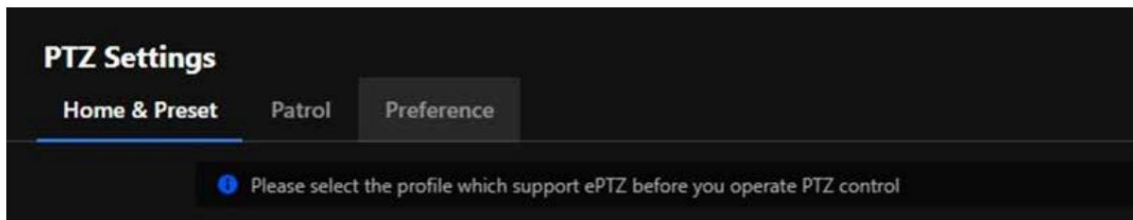


PTZ-Einstellungen

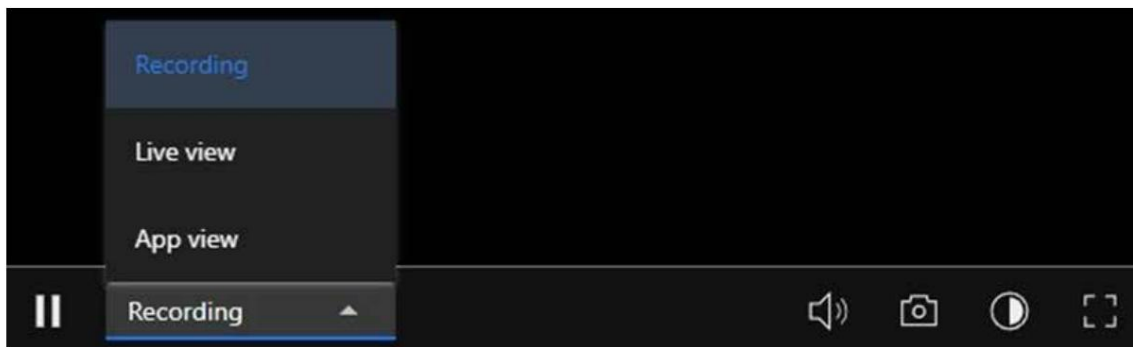
Vorsicht:

PTZ-Einstellungen sind nur für unterstützte Medienprofile verfügbar, insbesondere für das zweite und dritte Profil. Das bedeutet, dass nicht alle Medienprofile PTZ-Einstellungen unterstützen; Benutzer müssen ein unterstütztes Medienprofil auswählen, um die PTZ-Funktion zu aktivieren.

Wenn ein Benutzer zur Seite „PTZ-Einstellungen“ navigiert und das aktuell aktive Medienprofil die PTZ-Funktionalität nicht unterstützt, zeigt das System die Meldung an: „Bitte wählen Sie das Profil aus, das ePTZ unterstützt, bevor Sie die PTZ-Steuerung bedienen.“



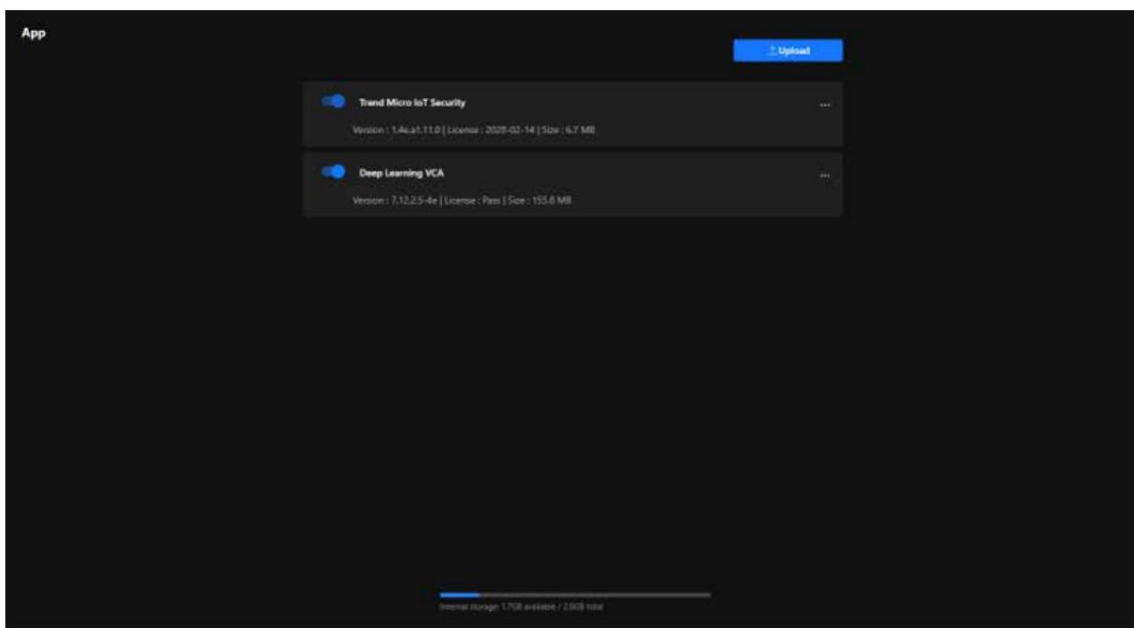
Diese Benachrichtigung dient als Aufforderung an die Benutzer, zu einem geeigneten Profil (2. oder 3.) zu wechseln.



App

Erweitern Sie die Kamerafunktionalität mit leistungsstarken Anwendungen

Die IPv4-Karte spielt eine entscheidende Rolle bei der Einrichtung der Netzwerkkonfiguration der Kamera und gewährleistet eine effektive Kommunikation. Sie ermöglicht eine zuverlässige Verbindung, sowohl lokalen als auch Fernzugriff und die problemlose Integration der Kamera in IPv4-basierte Netzwerke. Diese Konfiguration ist unerlässlich für einen stabilen und effizienten Betrieb in unterschiedlichen Netzwerkkumgebungen.



Trend Micro IoT-Sicherheit

Eine von Trend Micro bereitgestellte Sicherheitsanwendung, die speziell für IoT-Geräte entwickelt wurde. Ihre Hauptfunktionen sind folgende:

Kamerasicherheit verbessern

Schützt die Kamera vor Netzwerkangriffen, die ihren Betrieb stören könnten.

Datenschutz gewährleisten

Gewährleistet die Sicherheit von Videodaten und -einstellungen und verhindert unbefugten Zugriff.

Wartungskosten senken

Minimiert Geräteausfälle oder Datenverluste aufgrund von Sicherheitsproblemen.

Deep Learning VCA

Eine Anwendung zur visuellen Inhaltsanalyse (VCA), ein KI-gestütztes Tool auf Basis von Deep-Learning-Technologie zur intelligenten Videoverarbeitung. Ihre Hauptfunktionen sind folgende:

Verbesserung der Überwachungsgenauigkeit

Verringert Fehlalarme und übersehene Detektionen bei der manuellen Überwachung und ermöglicht so eine intelligente Videoüberwachung.

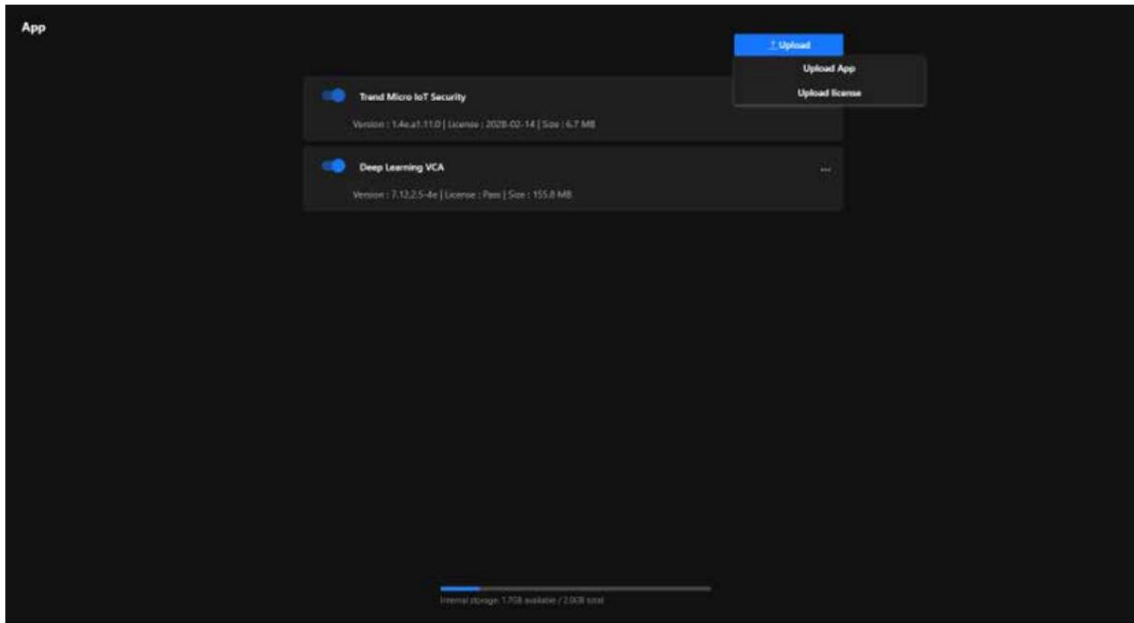
Automatisierte Verwaltung

Erreicht automatische Ereigniserkennung und Alarmauslösung durch KI-Analyse.

App

Bewältigung komplexer Szenarien

Unterstützt Echtzeitüberwachung und -analyse in großflächigen Umgebungen mit hohem Verkehrsaufkommen oder mehreren Fahrzeugen.

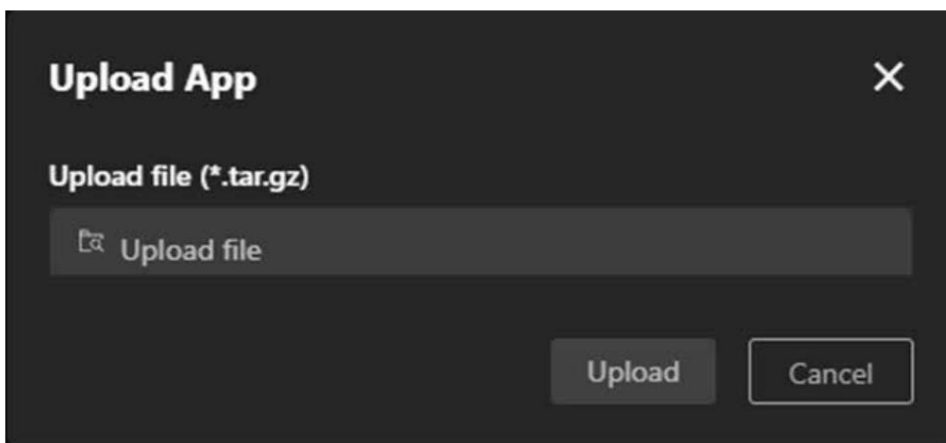


Schritte zum Hochladen der

App: Schritt 1. Klicken Sie auf die Schaltfläche „Hochladen“ in der oberen rechten Ecke der Seite. Es erscheinen zwei Optionen: **App hochladen:** Zum

Hochladen von Anwendungsdateien.

Lizenz hochladen: Zum Hochladen von Anwendungslizenzdateien.



Schritt 2. Klicken Sie auf „App hochladen“. Ein Fenster zum Hochladen von Dateien wird angezeigt. Das akzeptierte Dateiformat ist .tar.gz.

Schritt 3. Klicken Sie auf „Datei hochladen“ und wählen Sie die auf Ihrem Gerät gespeicherte Anwendungsdatei aus.

Schritt 4. Nachdem Sie die Datei überprüft haben, klicken Sie auf „Hochladen“, um die Anwendung hochzuladen.

Schritt 5. Warten Sie, bis der Upload abgeschlossen ist.

Schritt 6. Das System zeigt den Upload-Fortschritt an. Nach Abschluss des Uploads erscheint die Anwendungs- oder Lizenzdatei in der App-Liste.

App

Schritte zum Hochladen der Lizenz

Schritt 1. Klicken Sie auf die Schaltfläche „Hochladen“ in der oberen rechten Ecke der Seite. Es erscheinen zwei Optionen:

Upload-App

Zum Hochladen von Anwendungsdateien.

Upload-Lizenz

Zum Hochladen von Anwendungslizenzdateien.

Schritt 2. Klicken Sie auf „Lizenz hochladen“. Ein Fenster zum Hochladen von Dateien wird angezeigt. Akzeptierte Dateiformate sind *.xml-Dateien.

Schritt 3. Klicken Sie auf Datei hochladen und wählen Sie die entsprechende Lizenzdatei aus.

Schritt 4. Nachdem Sie die Datei überprüft haben, klicken Sie auf „Hochladen“, um die Lizenz hochzuladen.

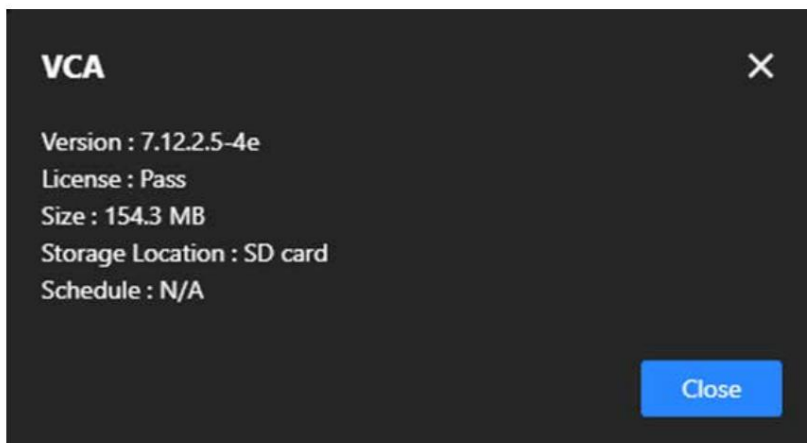
Schritt 5. Warten Sie, bis der Upload abgeschlossen ist.

Schritt 6. Es erscheint die Meldung „Hochladen erfolgreich“.

Das „Mehr“-Symbol jeder Anwendung (klicken Sie auf das Symbol mit den drei Punkten rechts) bietet folgende Funktionen und Zwecke:

Information

Die Funktion „Anwendungsstatus überwachen“ hilft Benutzern, Anwendungsdetails schnell zu erfassen und sicherzustellen, dass Version und Lizenz korrekt sind. Gleichzeitig unterstützt sie die Fehlerbehebung, indem sie wichtige Informationen wie Version und Lizenz bereitstellt, um Probleme effektiv zu diagnostizieren.



Zeitplan

Konfigurieren Sie den Laufzeitplan der Anwendung, um festzulegen, wann sie aktiviert oder deaktiviert werden soll, und definieren Sie spezifische Zeiträume, um Ressourcen zu schonen oder unterschiedlichen Szenarioanforderungen gerecht zu werden. Diese Funktion optimiert die Ressourcennutzung, indem sie unnötigen Langzeitbetrieb der Anwendung verhindert, Rechenleistung spart und sich durch die Automatisierung von Start und Stopp der Anwendung an verschiedene Szenarien anpasst, wodurch die Flexibilität erhöht wird.

Löschen

Schaffen Sie Speicherplatz frei, indem Sie unnötige Anwendungen entfernen, insbesondere wenn der Speicherplatz begrenzt ist, und passen Sie die Funktionalität an, indem Sie ungenutzte oder abgelaufene Anwendungen löschen, um Platz für Neuinstallationen zu schaffen.

Detektion

Die Erkennungsfunktion dient dazu, die automatisierten Überwachungsfunktionen der Kamera zu verbessern, manuelle Eingriffe zu reduzieren und im Falle von Anomalien umgehend die zuständigen Mitarbeiter zu benachrichtigen. Dadurch werden Sicherheit und Effizienz erhöht. Benutzer können die entsprechenden Erkennungsoptionen in der Verwaltungsschnittstelle je nach Bedarf aktivieren und konfigurieren.

Fortschrittliche Videoanalyse für proaktive Sicherheit und Präzision Überwachung

VIVOTEK integriert die fortschrittliche Smart VCA-Funktion (Video Content Analysis) in seine Kameras. Diese nutzt künstliche Intelligenz und maschinelles Lernen, um Videomaterial in Echtzeit zu analysieren. Sie übertrifft herkömmliche Überwachungsmethoden durch intelligentere Erkennungsfunktionen, die über die einfache Bewegungserkennung hinausgehen. Smart VCA kann spezifische Ereignisse oder Verhaltensweisen identifizieren und ist somit ein leistungsstarkes Werkzeug für proaktive Sicherheit und Überwachung.

Intelligenter VCA

Smart VCA (Video Content Analysis) nutzt künstliche Intelligenz und maschinelles Lernen zur Echtzeitanalyse von Videomaterial. Es erweitert die herkömmliche Überwachung durch intelligente Erkennungsfunktionen, die über die einfache Bewegungserkennung hinausgehen. Smart VCA ermöglicht es der Kamera, spezifische Ereignisse oder Verhaltensweisen zu identifizieren und ist somit ein leistungsstarkes Werkzeug für proaktive Sicherheit und Überwachung.

Hauptmerkmale und Vorteile von Smart VCA:

Menschenmengenerkennung

Die Crowd-Erkennung in Smart VCA dient dazu, Bereiche zu identifizieren, in denen die Anzahl der Personen einen vordefinierten Schwellenwert überschreitet. Diese Funktion gewährleistet eine effektive Besucherlenkung im öffentlichen Raum, indem sie Nutzer auf potenzielle Überfüllungssituationen aufmerksam macht. Durch die Echtzeitüberwachung erhöht sie die Sicherheit, unterstützt die Steuerung des Besucherstroms und beugt Gefahrensituationen in sensiblen oder stark frequentierten Bereichen wie Veranstaltungen, Verkehrsknotenpunkten oder Notfall-Evakuierungszonen vor.

Einbruchserkennung

Die Einbruchserkennung in Smart VCA überwacht vordefinierte Zonen und löst Alarme aus, sobald eine unbefugte Person oder ein unbefugtes Objekt den Bereich betritt. Diese Funktion erhöht die Sicherheit, indem sie eingeschränkte oder Hochsicherheitsbereiche proaktiv schützt, unbefugten Zugriff verhindert und sicherstellt, dass kritische Bereiche geschützt und frei von potenziellen Bedrohungen bleiben.

Erkennung von Herumlungern

Die Funktion „Herumlungern“ in Smart VCA identifiziert Personen, die sich ungewöhnlich lange in einem bestimmten Bereich aufhalten. Diese Funktion hilft, verdächtiges Verhalten frühzeitig zu erkennen und ermöglicht es Nutzern, präventive Maßnahmen zu ergreifen, um potenzielle Sicherheitsrisiken wie Vandalismus, Diebstahl oder unbefugte Aktivitäten in sensiblen Bereichen zu minimieren.

Erkennung fehlender Objekte

Die Funktion „Fehlende Objekte erkennen“ in Smart VCA benachrichtigt die Benutzer, wenn ein Objekt aus einem vordefinierten Bereich entfernt wird. Diese Funktion erhöht die Sicherheit, indem sie dazu beiträgt, Diebstahl oder unbefugte Entnahme wichtiger Gegenstände zu verhindern und so sicherzustellen, dass wertvolle Vermögenswerte jederzeit geschützt bleiben.

Detektion

Unbeaufsichtigte Objekterkennung

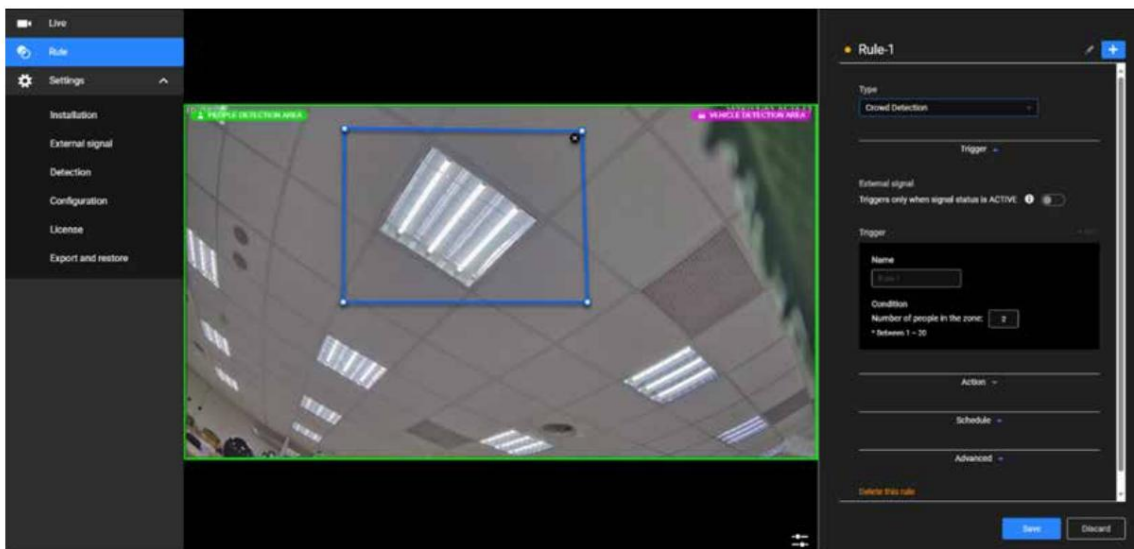
Die Funktion „Unbeaufsichtigte Objekte erkennen“ in Smart VCA identifiziert Gegenstände, die in einem bestimmten Bereich zurückgelassen wurden. Diese Funktion erhöht die Sicherheit, indem sie potenzielle Sicherheitsrisiken, wie beispielsweise unbeaufsichtigtes Gepäck im öffentlichen Raum, frühzeitig erkennt und so eine zeitnahe Untersuchung und Reaktion ermöglicht.

Linienüberschreitungserkennung

Die Linienüberschreitungserkennung in Smart VCA löst eine Warnung aus, sobald ein Objekt oder eine Person eine vom Benutzer definierte virtuelle Grenze überschreitet. Diese Funktion ist unerlässlich für die Überwachung von Grenzen und die Gewährleistung der Perimetersicherheit, um unbefugten Zutritt zu Sperrbereichen zu verhindern und die allgemeine Zutrittskontrolle zu verbessern.

Gesichtserkennung

Die Gesichtserkennung in Smart VCA identifiziert und verfolgt Gesichter im Sichtfeld der Kamera. Diese Funktion verbessert die Zutrittskontrolle, optimiert Identifizierungsprozesse und bietet wertvolle Unterstützung bei der Ereignisanalyse im Rahmen forensischer Untersuchungen. Dadurch werden mehr Sicherheit und Verantwortlichkeit in überwachten Bereichen gewährleistet.



Schritte zum Hinzufügen einer Erkennungsregel

Schritt 1. Zugriff auf die Smart VCA-Einstellungen.

Klicken Sie in der Web-Benutzeroberfläche der Kamera auf die Kategorie „Erkennung“ > Element „Smart VCA“.

Das Smart VCA-Dienstprogramm wird automatisch gestartet.

Notiz:

Smart VCA und Smart Motion teilen sich das gleiche Dienstprogrammfenster.

Schritt 2. Eine Regel hinzufügen.

Klicken Sie im Smart VCA-Dienstprogramm auf die Schaltfläche „Hinzufügen“, um eine Regel hinzuzufügen.

Wählen Sie den Typ aus:

Personenerkennung: Überwachen Sie die Anzahl der Personen in einem bestimmten Bereich.

Einbruchserkennung: Erkennung des unbefugten Zutritts zu einem definierten Bereich.

Erkennung von Herumlungen: Erkennen von Personen, die sich über längere Zeiträume aufhalten.

Erkennung fehlender Objekte: Überwachen Sie das Entfernen von Objekten.

Detektion

Unbeaufsichtigte Objekterkennung: Erkennen von zurückgelassenen Gegenständen.

Linienüberschreitungserkennung: Überwachen von Objekten, die eine virtuelle Grenze überschreiten.

Gesichtserkennung: Gesichter in der Szene erkennen und verfolgen.

Benennen Sie die Regel, zum Beispiel „Publikumszone 1“.

Schritt 3. Den Erfassungsbereich definieren.

Zeichne den Bereich

Verwenden Sie die Maus, um den Erfassungsbereich im Videobild festzulegen (z. B. den überwachten Bereich zu umranden). Passen Sie Größe und Form nach Bedarf an, um den Zielbereich präzise abzudecken.

Bereich basierend auf Merkmalen konfigurieren:

Linienkreuzungserkennung: Zeichnen Sie eine virtuelle Linie und legen Sie die Kreuzungsrichtung fest (A>B oder B>A).

Personenerkennung und Einbruchserkennung: Den genauen Bereich beschreiben.

Fehlendes Objekt/Unbeaufsichtigtes Objekt erkennen: Den Standort des Objekts angeben.

Schritt 4. Auslösebedingungen konfigurieren.

Konfigurieren Sie Bedingungen basierend auf der Funktion, wie zum Beispiel:

Personenerkennung: Legen Sie einen Schwellenwert für die Personenzahl fest (z. B. mehr als 5 Personen).

Erkennung von Herumlungen: Definieren Sie eine Verweildauer (z. B. mehr als 10 Sekunden).

Einbruchserkennung: Aufenthalts- oder Eintrittsbedingungen konfigurieren.

Erkennung fehlender/unbeaufsichtigter Objekte: Auslöser definieren (Objekt entfernt oder hinzugefügt).

Passen Sie die Empfindlichkeit an, um Fehlalarme zu vermeiden.

Schritt 5. Aktionen definieren.

Weisen Sie Aktionen zu, die ausgeführt werden sollen, wenn die Auslösebedingungen erfüllt sind.

Konfigurieren Sie bei Bedarf mehrere verknüpfte Aktionen.

Schritt 6. Einen Zeitplan festlegen.

Immer: Die Regel ist jederzeit aktiviert.

Wiederholter Zeitplan: Geben Sie Daten und Zeiträume an, in denen die Regel aktiv sein soll (z. B. außerhalb der Arbeitszeiten).

Schritt 7. Klicken Sie auf Speichern, um die Regel zu speichern.

Notiz:

Weitere Informationen finden Sie im Benutzerhandbuch des Smart VCA. https://www.vivotek.com/products/analytics/smart_vca

Detektion

Verbesserte Genauigkeit und Effizienz bei der Überwachung mit Intelligente Bewegungserkennung

Die verbesserte Genauigkeit und Effizienz der Überwachung mit intelligenter Bewegungserkennung sind für Anwender von entscheidender Bedeutung, da sie Fehlalarme minimieren und sicherstellen, dass Sicherheitsressourcen auf tatsächliche Bedrohungen konzentriert werden. Durch die präzise Erkennung von Personen und Fahrzeugen bei gleichzeitiger Filterung irrelevanter Bewegungen erreichen Anwender eine zuverlässige Überwachung und reduzieren den Zeitaufwand für unnötige Alarme. Diese hohe Präzision und Effizienz verbessert nicht nur das Lagebewusstsein, sondern steigert auch die operative Effektivität insgesamt und macht die intelligente Bewegungserkennung zu einem unverzichtbaren Werkzeug für den Schutz kritischer Bereiche und die schnelle Reaktion auf potenzielle Risiken.

Smart Motion

Die intelligente Bewegungserkennung dient der Verbesserung der Effizienz und Genauigkeit der Bewegungserkennung in Überwachungssystemen. Zu ihren Hauptzwecken gehören:

Reduzierung von Fehlalarmen

Die intelligente Bewegungserkennung minimiert unnötige Alarme, die durch irrelevante Bewegungen wie sich bewegende Schatten, Lichtveränderungen oder Umwelteinflüsse wie vom Wind verwehte Blätter verursacht werden.

Verbesserung der Sicherheitsüberwachung

Durch die Fokussierung auf bestimmte Bereiche und die Erkennung relevanter Aktivitäten (z. B. Personen oder Fahrzeuge) ermöglicht es den Sicherheitsteams, effektiver auf potenzielle Bedrohungen zu reagieren.

Verbesserung der Genauigkeit der Ereigniserkennung

Intelligente Filter wie die Personen- und Fahrzeugerkennung sorgen dafür, dass nur relevante Ereignisse identifiziert und aufgezeichnet werden, wodurch der Aufwand für die Durchsicht des Videomaterials reduziert wird.

Optimierung von Speicher und Bandbreite

Durch die Aufzeichnung nur kritischer Ereignisse wird die Menge der gespeicherten und übertragenen Daten reduziert, was zu einer effizienteren Speichernutzung und einem geringeren Bandbreitenverbrauch führt.

Ermöglichung von Echtzeitwarnungen

Die intelligente Bewegungserkennung ermöglicht sofortige Benachrichtigungen über relevante Ereignisse und hilft Nutzern so, in kritischen Situationen rechtzeitig zu reagieren.

Vereinfachung der Ereignisanalyse

Durch die Fokussierung auf Ereignisse mit hoher Priorität werden die Nachuntersuchungen vereinfacht und die Effizienz der Videoauswertung verbessert.

Detektion

Schritte zur Konfiguration der intelligenten

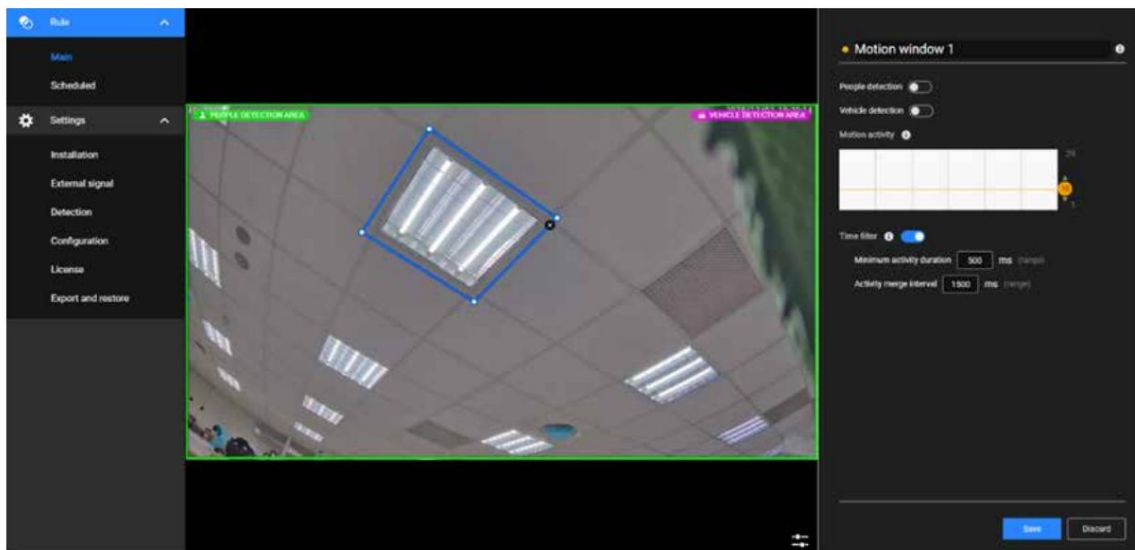
Bewegungserkennung Schritt 1. Greifen Sie auf die Smart VCA-Einstellungen zu.

Klicken Sie in der Web-Benutzeroberfläche der Kamera auf die Kategorie „Erkennung“ > Element „Bewegung“.

Das Smart Motion-Dienstprogramm wird automatisch gestartet.

Notiz:

Smart VCA und Smart Motion teilen sich das gleiche Dienstprogrammfenster.



Schritt 2. Den Erfassungsbereich definieren.

Verwenden Sie die Maus, um eine Form auf dem Live-Feed zu zeichnen und so den Erfassungsbereich festzulegen.

Schritt 3. Bewegungsempfindlichkeit anpassen.

Stellen Sie den Schieberegler für die Bewegungsempfindlichkeit entsprechend Ihrer Umgebung ein (z. B. höher für Innenräume, niedriger für Außenbereiche mit natürlicheren Bewegungen).

Schritt 4. Zeitfilter konfigurieren.

Mindestdauer einer Aktivität: Definieren Sie, wie lange eine Bewegung dauern muss, um als Ereignis zu gelten.

Aktivitätszusammenführungsintervall: Konfigurieren Sie das Intervall, in dem kurz aufeinanderfolgende Ereignisse zusammengeführt werden.

Schritt 5. Objekterkennung aktivieren (optional).

Aktivieren Sie gegebenenfalls die „Personenerkennung“ und/oder die „Fahrzeugerkennung“.

Notiz:

Weitere Informationen finden Sie im Benutzerhandbuch des Smart VCA. https://www.vivotek.com/products/analytics/smart_vca

Detektion

Verbesserung der Sicherheit durch Echtzeit-Audioanomalieerkennung für Schnelle Antwort

Die Audioerkennung erhöht die Sicherheit durch die kontinuierliche Überwachung des Umgebungsgeräuschpegels und die Identifizierung ungewöhnlicher Geräuschmuster wie laute Geräusche, Glasbruch oder Schreie. Durch die Analyse von Echtzeit-Schalldaten und die Auslösung von Warnmeldungen bei Überschreitung eines vordefinierten Schwellenwerts ermöglicht sie schnelle Reaktionen auf potenzielle Sicherheitsvorfälle oder Notfälle. Dieser proaktive Ansatz stellt sicher, dass kritische Ereignisse auch dann erkannt werden, wenn visuelle Hinweise nicht ausreichen. Er bietet eine zusätzliche Schutzebene und verbessert das Lagebewusstsein insgesamt.

Audioerkennung

Die Audioerkennungsfunktion der VIVOTEK-Kameras ist ein leistungsstarkes Werkzeug zur Erhöhung der Sicherheit. Durch die Echtzeit-Erkennung von Geräusch anomalies verbessert sie die Fähigkeit der Kamera, Vorfälle effektiv zu überwachen und darauf zu reagieren. Zu ihren Hauptfunktionen gehören:

Verbesserung der Sicherheit

Erkennt ungewöhnliche Geräusche (z. B. Glasbruch, Schreie oder Explosionen) und ermöglicht so die frühzeitige Identifizierung potenzieller Gefahren.

Ergänzung der Videoüberwachung

Fügt eine zusätzliche Erkennungsebene in Situationen hinzu, in denen Bewegungs- oder visuelle Auslöser möglicherweise nicht wirksam sind (z. B. in einem ruhigen Bereich ohne sichtbare Bewegung).

Echtzeitwarnungen

Benachrichtigt das Sicherheitspersonal sofort bei der Erkennung ungewöhnlicher Geräusche und ermöglicht so schnellere Reaktionen.

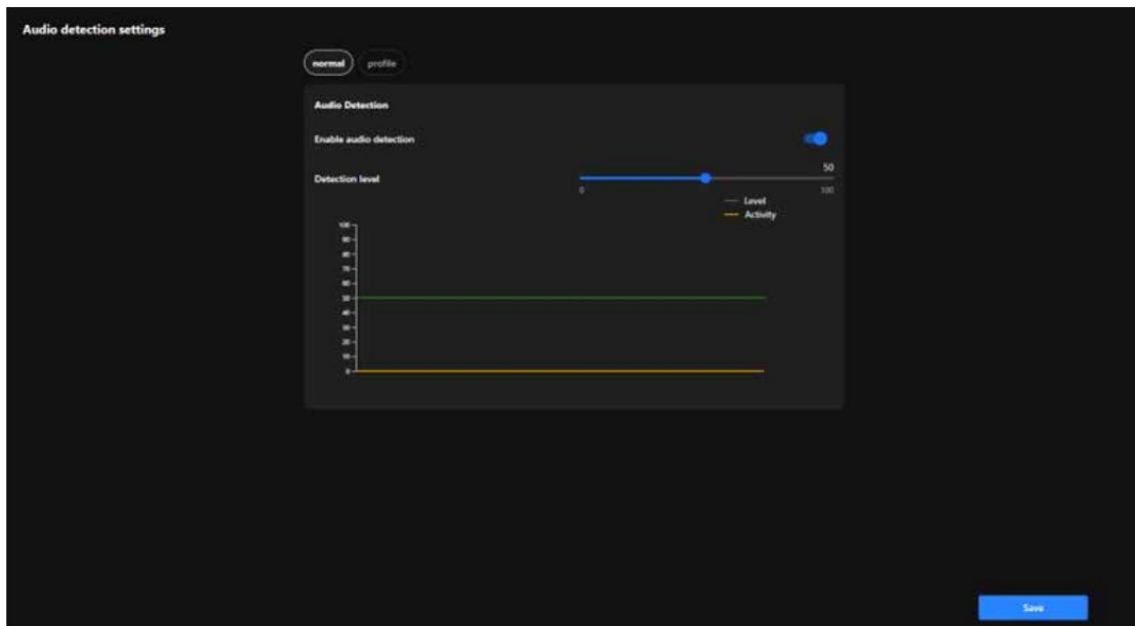
Überwachung von Umweltlärm

Nützlich zur Überwachung des Schallpegels in bestimmten Bereichen, wie Fabriken, Schulen oder öffentlichen Räumen, um Sicherheit und Einhaltung der Vorschriften zu gewährleisten.

Ereignisaufzeichnung

Trägt dazu bei, dass audiobezogene Vorfälle zur Überprüfung und Untersuchung dokumentiert werden.

Detektion



Schritte zur Konfiguration der Audioerkennung Schritt 1.

Öffnen Sie die Einstellungen für die Audioerkennung.

Klicken Sie in der Web-Benutzeroberfläche der Kamera auf die Kategorie „Erkennung“ > Element „Audioerkennung“.

Schritt 2. Audioerkennung aktivieren.

Schalten Sie die Option „Audioerkennung aktivieren“ ein.

Schritt 3. Stellen Sie die Erkennungsstufe ein.

Stellen Sie den Schieberegler für die Erkennungsstufe ein.

Höhere Stufen filtern normale Hintergrundgeräusche heraus und erfassen nur laute oder ungewöhnliche Geräusche.

Niedrige Pegel erfassen selbst geringfügige Audioveränderungen und sind daher in ruhigeren Umgebungen nützlich.

Nutzen Sie das Echtzeitdiagramm, um Folgendes zu beobachten:

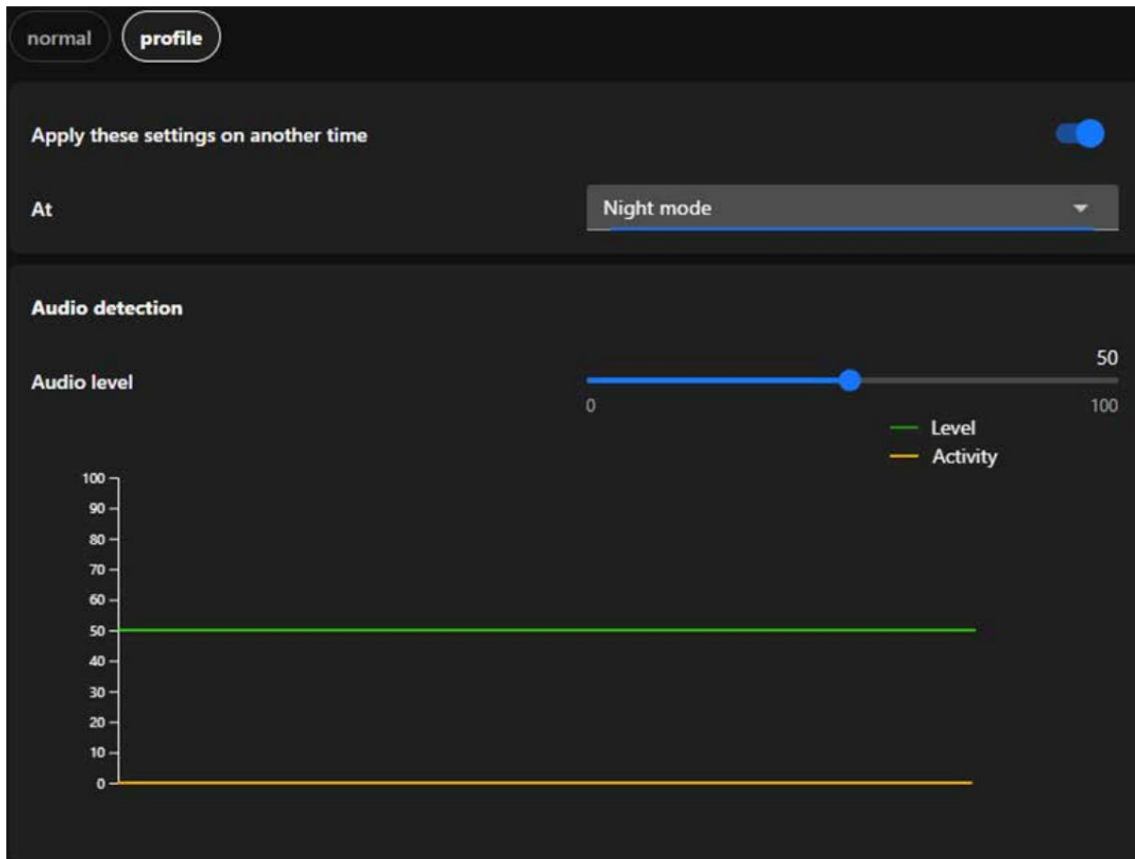
Grüne Linie (Pegel): Stellt die Erkennungsschwelle dar.

Orange Linie (Aktivität): Stellt die aktuellen Audiopegel dar.

Stellen Sie mit dem Schieberegler einen für Ihre Umgebung geeigneten Schwellenwert ein.

Detektion

Integrieren Sie die Einstellungen zur Audioerkennung in ein Profil.



Die Profileinstellungen für die Audioerkennung ermöglichen es Benutzern, Erkennungseinstellungen zu konfigurieren, die auf bestimmte Betriebsmodi wie den Nachtmodus und den Zeitplanmodus zugeschnitten sind. Diese Einstellungen bieten Flexibilität und Präzision für verschiedene Überwachungsanforderungen.

Nachtmodus

Das System wurde für ruhigere Umgebungen mit geringerem Umgebungsgeräuschpegel entwickelt und zeichnet sich durch eine erhöhte Empfindlichkeit gegenüber ungewöhnlichen Geräuschen wie Glasbruch oder lauten Schritten aus, die auf Sicherheitslücken hindeuten könnten. Niedrigere Schwellenwerte für die Geräuscherkennung sorgen dafür, dass selbst geringfügige Störungen einen Alarm auslösen. Das System kann während voreingestellter Nachtzeiten automatisch aktiviert werden.

Zeitplanmodus

Es ermöglicht Nutzern, spezifische Einstellungen während vordefinierter Zeiträume, wie z. B. Arbeitszeiten, Wochenenden oder verkehrsärmeren Zeiten, anzuwenden und so auf Basis vorhersehbarer Geräuschmuster individuelle Erkennungseinstellungen zu gewährleisten. Es ermöglicht eine präzise Planung, wann Audioerkennungsschwellenwerte oder -profile aktiv sein sollen, und passt die Empfindlichkeit an die zu erwartende Geräuschumgebung während des geplanten Zeitraums an.

Detektion

Gewährleistung von Echtzeitschutz vor physischen Einwirkungen

Die Stoßerkennung benachrichtigt Benutzer in Echtzeit, sobald die Kamera Stößen oder Vibrationen ausgesetzt ist, und sorgt so für sofortiges Erkennen versehentlicher Beschädigungen. Diese proaktive Überwachung verbessert die Zuverlässigkeit des Sicherheitssystems, indem sie die Kamera vor Störungen schützt, Ausfallzeiten reduziert und eine durchgängige Überwachung gewährleistet, um kritische Bereiche effektiv zu sichern.

Schockerkennung

Die Stoßerkennungsfunktion der VIVOTEK-Kameras dient der Erkennung von Stößen und Vibrationen. Mithilfe integrierter Sensoren überwacht sie plötzliche Bewegungen oder Erschütterungen und löst bei Erkennung eine sofortige Benachrichtigung aus. Zu ihren Hauptfunktionen gehören:

Schäden verhindern

Schützen Sie die Kamera vor möglichen physischen Schäden durch Manipulation, Vandalismus oder versehentliche Stöße.

Echtzeitwarnungen

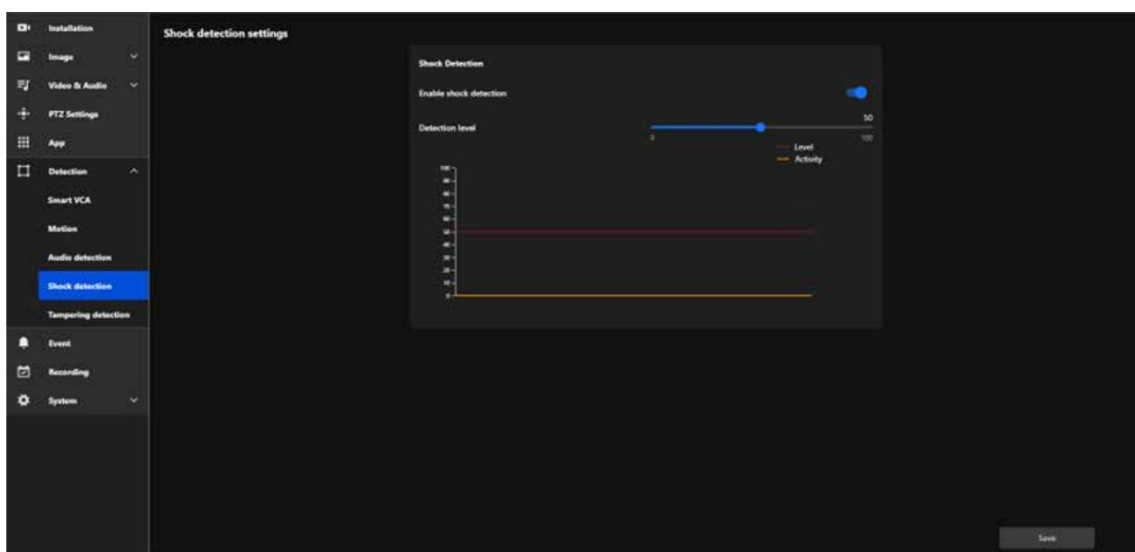
Stellen Sie sicher, dass die Benutzer im Falle einer physischen Störung sofort informiert werden, um eine schnelle Reaktion zu ermöglichen.

Betrieb aufrechterhalten

Helfen Sie mit, die kontinuierliche Funktionsfähigkeit der Kamera sicherzustellen, indem Sie physikalische Störungen umgehend erkennen.

Sicherheit verstärken

Die Zuverlässigkeit des Überwachungssystems wird durch die Vermeidung von Störungen aufgrund physischer Einwirkungen erhöht.



Schritt zur Konfiguration der Schockerkennung

Schritt 1. Öffnen Sie die Einstellungen für die Audioerkennung.

Klicken Sie in der Web-Benutzeroberfläche der Kamera auf die Kategorie „Erkennung“ > Element „Erschütterungserkennung“.

Detektion

Schritt 2. Schockerkennung aktivieren.

Schalten Sie die Option „Erschütterungserkennung aktivieren“ ein.

Schritt 3. Stellen Sie die Erkennungsstufe ein.

Stellen Sie den Schieberegler für die Erkennungsstufe ein.

Höhere Ebenen ignorieren kleinere Auswirkungen und konzentrieren sich auf bedeutendere Ereignisse.

Niedrigere Stufen erfassen leichte Stöße oder Vibrationen.

Betrachten Sie die Diagramme für das Niveau (rote Linie) und die Aktivität (gelbe Linie):

Die rote Linie stellt den konfigurierten Erkennungsschwellenwert dar.

Die gelbe Linie zeigt die Schockaktivität in Echtzeit an.

Stellen Sie den Schieberegler so ein, bis der Schwellenwert Ihren Umgebungsbedingungen entspricht.

Schutz des Überwachungssystems vor Sichtbehinderung

Um optimale Leistung und klare Überwachung zu gewährleisten, ist der Schutz Ihres Überwachungssystems vor Sichtbehinderungen entscheidend.

Überprüfen und warten Sie die Kameras regelmäßig, um Blockaden durch Schmutz, Ablagerungen oder Witterungseinflüsse zu vermeiden. Positionieren Sie die Kameras strategisch so, dass sie nicht durch Vegetation, Gebäudestrukturen oder temporäre Absperrungen verdeckt werden. Erweiterte Funktionen wie Hinderniserkennungsalarme können die Zuverlässigkeit zusätzlich erhöhen und eine lückenlose Überwachung kritischer Bereiche sicherstellen.

Manipulationserkennung

Die Manipulationserkennung ist eine fortschrittliche Kamerafunktion, die Vorfälle wie Blockierung, Unschärfe oder Farbspritzer erkennt. Diese Funktion verbessert die Integrität und Zuverlässigkeit von Überwachungssystemen durch klare und präzise Überwachung und zeitnahe Warnmeldungen. Zu ihren Hauptzwecken gehören:

Sabotage verhindern

Erkennt und benachrichtigt den Benutzer über Versuche, den Betrieb der Kamera zu stören, wie z. B. Abdecken, Unschärfe oder physische Manipulation des Geräts.

Erhaltung der Bildqualität

Überwacht Helligkeit und Fokus, um eine gleichbleibende Videoqualität zu gewährleisten und gibt bei Erkennung von Anomalien entsprechende Warnmeldungen aus.

Verbesserung der Sicherheit

Fügt eine zusätzliche Schutzebene hinzu, indem visuelle Beeinträchtigungen oder böswillige Handlungen erkannt werden, die das Überwachungssystem gefährden.

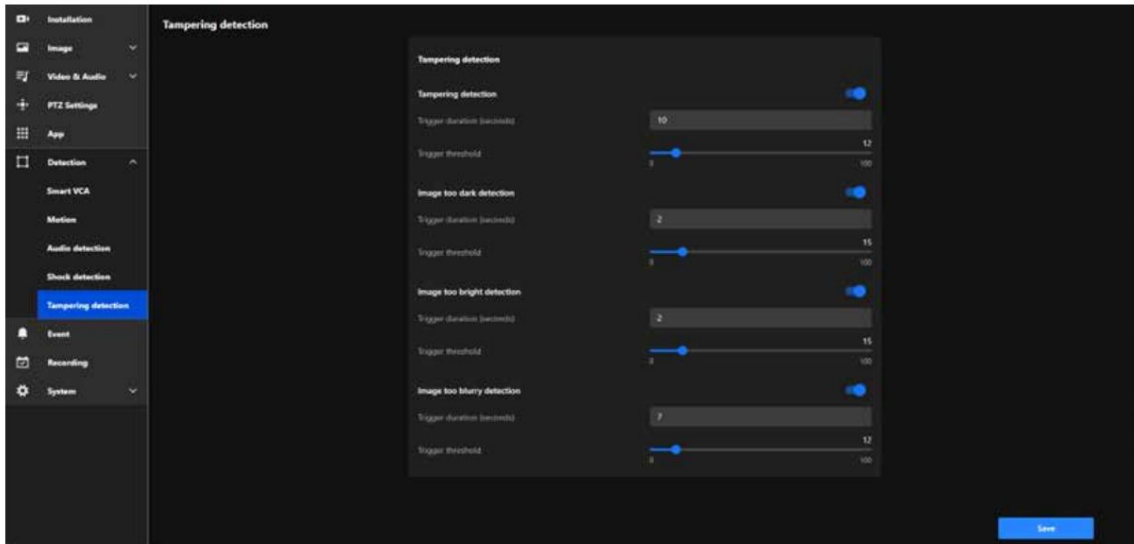
Zeitnahe Antwort

Liefert Echtzeitwarnungen, damit das Sicherheitspersonal sofort auf Manipulationsvorfälle oder visuelle Probleme reagieren kann.

Detektion

Betriebssicherheit

Gewährleistet eine kontinuierliche und qualitativ hochwertige Überwachung, auch in anspruchsvollen oder risikoreichen Umgebungen.



Nachfolgend sind die detaillierten Funktionalitäten und die entsprechenden Einstellungen für jede Funktion aufgeführt:

Manipulationserkennung

Erkennt physische Manipulationen, wie z. B. Blockieren, Abdecken oder Verschieben der Kamera, und sorgt für sofortige Warnmeldungen, um die Integrität der Überwachung zu gewährleisten.

Auslösedauer (Sekunden): Definiert

die Zeitspanne, die eine Manipulation andauern muss, bevor ein Alarm ausgelöst wird.

Auslöseschwelle:

Passt die Empfindlichkeit gegenüber Manipulationsversuchen an. Niedrigere Schwellenwerte führen zu höherer Empfindlichkeit, können aber Fehlalarme auslösen, während höhere Schwellenwerte eine geringere Empfindlichkeit bewirken.

Erkennung: Bild zu dunkel

Erkennt, wenn der Videostream aufgrund absichtlicher Aktionen (z. B. Ausschalten des Lichts) oder Umweltveränderungen ungewöhnlich dunkel wird, und gibt rechtzeitig Warnungen aus, um potenzielle Probleme zu beheben.

Auslösedauer (Sekunden):

Legt die Dauer fest, die das Bild dunkel bleiben muss, um eine Warnung auszulösen.

Auslöseschwelle:

Passt die Empfindlichkeit gegenüber Dunkelheit an. Niedrigere Schwellenwerte erfassen kleinere Veränderungen, während höhere Schwellenwerte den Fokus auf signifikante Dunkelheitsgrade legen.

Erkennung zu heller Bilder

Das System erkennt, wenn der Videostream überbelichtet wird, beispielsweise durch intensives Licht, das auf die Kamera gerichtet ist (z. B. Taschenlampen), wodurch die Sicht beeinträchtigt wird, und gibt sofortige Warnmeldungen aus, um die Integrität der Überwachung zu gewährleisten.

Auslösedauer (Sekunden):

Legt fest, wie lange das Helligkeitsproblem bestehen muss, bevor eine Warnung ausgelöst wird.

Detektion

Auslöseschwelle:

Passt die Empfindlichkeit an Helligkeitsänderungen an. Niedrigere Schwellenwerte erkennen leichte Überbelichtung, während höhere Schwellenwerte nur bei extremen Helligkeitswerten auslösen.

Bild zu vergraben Erkennung

Erkennt, wenn das Videobild aufgrund von Unschärfe, Objektivverschattung oder Umwelteinflüssen wie Kondensation oder Schmutz unscharf wird, und sorgt so für rechtzeitige Warnmeldungen, um eine klare Überwachung zu gewährleisten.

Auslösedauer (Sekunden):

Definiert, wie lange die Unschärfe anhalten muss, um eine Warnung auszulösen.

Auslöseschwelle:

Passt die Empfindlichkeit gegenüber Unschärfe an. Niedrigere Schwellenwerte erkennen leichte Unschärfe, während höhere Schwellenwerte den Fokus auf signifikante Qualitätsbeeinträchtigungen legen.

Ereignis

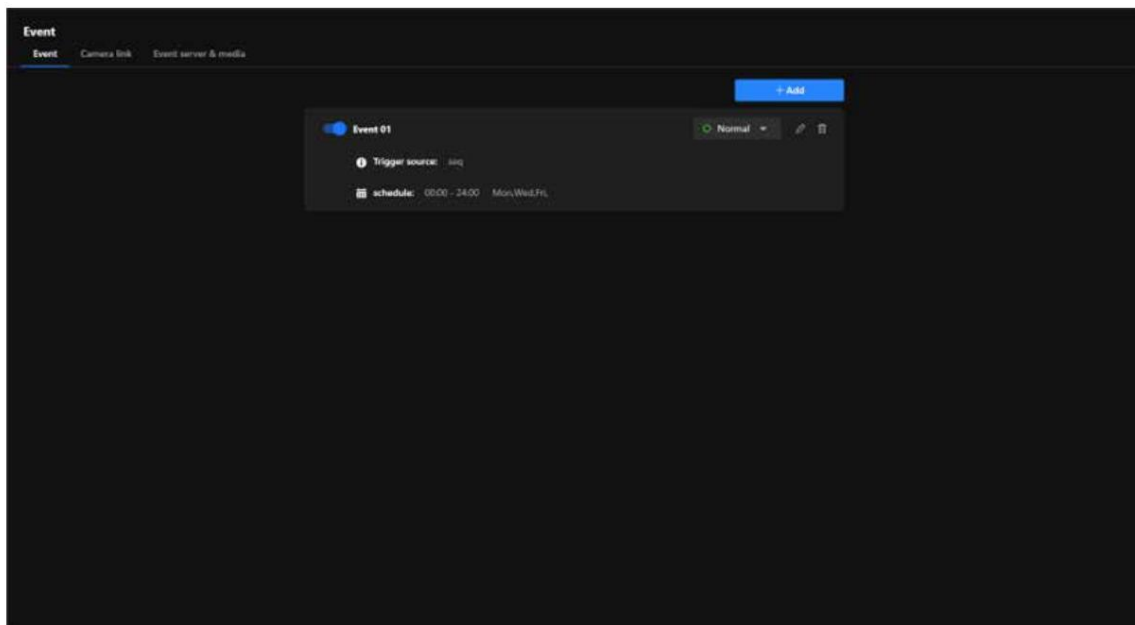
Event ist ein leistungsstarkes Tool zur Verbesserung der Sicherheit durch Automatisierung und intelligente Überwachung. Es ermöglicht Benutzern, spezifische Bedingungen, sogenannte Auslöser, zu definieren, die vorkonfigurierte Aktionen wie Aufzeichnung, Versand von Benachrichtigungen oder Steuerung externer Geräte aktivieren. Durch die Anpassung dieser Ereignisse mit detaillierten Zeitplänen und Bedingungen stellen Benutzer sicher, dass das System proaktiv auf potenzielle Bedrohungen oder Anomalien reagiert. Diese Funktion optimiert nicht nur die Überwachungsabläufe, sondern reduziert auch den Bedarf an ständiger manueller Überwachung und bietet so eine zuverlässige und effiziente Möglichkeit zum Schutz von Eigentum und Vermögenswerten.

Verbesserung der Sicherheit durch automatisierte und anpassbare Ereignisse

Um die Sicherheit durch automatisierte und individuell anpassbare Ereignisse zu erhöhen, können Nutzer spezifische Bedingungen für die Aktivierung von Überwachungsaktionen konfigurieren. Beispielsweise lassen sich Bewegungserkennung, Geräuscherkennung oder Manipulation als Auslöser festlegen. Nach der Auslösung kann die Kamera automatisch Aufnahmen aufzeichnen, Benachrichtigungen per E-Mail versenden oder angeschlossene Geräte wie Alarmanlagen aktivieren. Nutzer können diese Ereignisse weiter anpassen, indem sie Zeitpläne festlegen, z. B. die Überwachung nur nachts aktivieren, oder mehrere Auslöser für komplexere Szenarien verknüpfen. Diese Flexibilität gewährleistet eine proaktive und effiziente Sicherheitslösung, die auf die individuellen Bedürfnisse des Nutzers zugeschnitten ist.

Ereignis

Event ist ein intelligentes Automatisierungstool, das die Effizienz und Effektivität der Sicherheitsüberwachung steigert. Es erkennt spezifische Bedingungen oder Auslöser und führt automatisch vordefinierte Aktionen aus, um auf diese Ereignisse zu reagieren. Dadurch wird der Bedarf an ständiger manueller Überwachung reduziert und eine zeitnahe Reaktion auf kritische Vorfälle gewährleistet.



Hauptzweck der Veranstaltung:

Sicherheit verbessern

Indem Kameras so konfiguriert werden, dass sie sofort auf verdächtige Aktivitäten wie Eindringversuche oder Manipulationen reagieren, können Benutzer Vorfälle verhindern, bevor sie eskalieren.

Ereignis

Steigerung der Effizienz

Durch die Automatisierung von Reaktionen entfällt die Notwendigkeit einer ständigen manuellen Überwachung, wodurch Zeit und Ressourcen gespart werden.

Belege vorlegen

Automatische Aufzeichnung und Momentaufnahme gewährleisten, dass wichtige Momente für Ermittlungen dokumentiert werden.

Proaktive Problemlösungs- Warnungen

bei Geräte- oder Netzwerkproblemen ermöglichen es Benutzern, Probleme schnell zu beheben und so Ausfallzeiten oder Sicherheitslücken zu reduzieren.

Schritte zum Hinzufügen eines

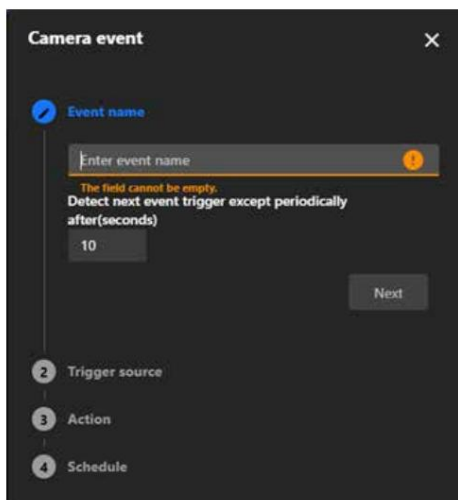
Ereignisses Schritt 1. Geben Sie den Ereignisnamen ein

Klicken Sie auf der Registerkarte „Ereignis“ auf die Schaltfläche „+ Hinzufügen“.

Geben Sie im Feld „Veranstaltungsname“ einen beschreibenden Namen für die Veranstaltung ein.

Legen Sie das Auslöseintervall fest. Dadurch wird bestimmt, wie lange das System wartet, bevor es dasselbe Ereignis erneut erkennt.

Klicken Sie auf Weiter, um fortzufahren.



Schritt 2. Wählen Sie die Triggerquelle aus.

Wählen Sie eine Triggerquelle aus der Liste aus:

Gerät

Diese Auslöser basieren auf der Kamera selbst oder auf externen Geräten, die mit ihr verbunden sind.

Detektion

Diese Auslöser nutzen die in die Kamera integrierten intelligenten Analysefunktionen, um Veränderungen oder Anomalien in der Umgebung zu erkennen.

Aufzeichnung

Diese Auslöser basieren auf dem Aufzeichnungsstatus der Kamera.

VADP

VADP (VIVOTEK Application Development Platform) bietet erweiterte Triggeroptionen, die von kundenspezifischen Anwendungen unterstützt werden.

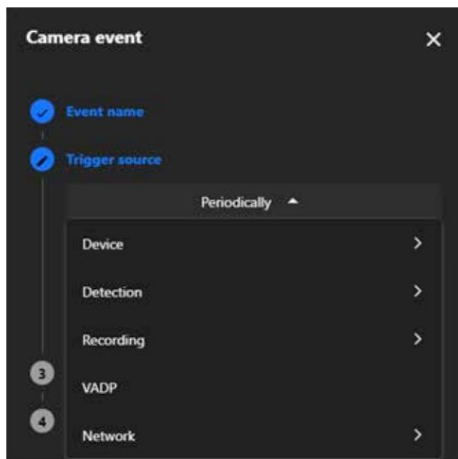
Ereignis

Netzwerk

Diese Auslöser basieren auf dem Netzwerkstatus bzw. den Netzwerkbedingungen.

Konfigurieren Sie alle zusätzlichen Einstellungen für die ausgewählte Triggerquelle.

Klicken Sie auf Weiter, um fortzufahren.



Schritt 3. Aktionen definieren

Wählen Sie die Aktionen aus, die beim Auslösen des Ereignisses ausgeführt werden sollen:

Digitalausgang:

Aktiviert ein externes Gerät, z. B. eine Alarmanlage.

Sichern

Sie die Videoaufnahmen auf einem Speichermedium, falls die Netzwerkverbindung unterbrochen wird.

Audioclips:

Spielt einen vorkonfigurierten Audioclip ab (erfordert vorherige Audioeinstellungen).

Camera Link

Verbindung zu anderen Kameras zur koordinierten Reaktion.

Ereignisserver & Medien

Legen Sie den Speicherort fest, zum Beispiel:

0. SD-Karte

1. NAS

Passen Sie die Aktionseinstellungen nach Bedarf an.

Klicken Sie auf Weiter, um fortzufahren.

Ereignis



Schritt 4. Zeitplan festlegen

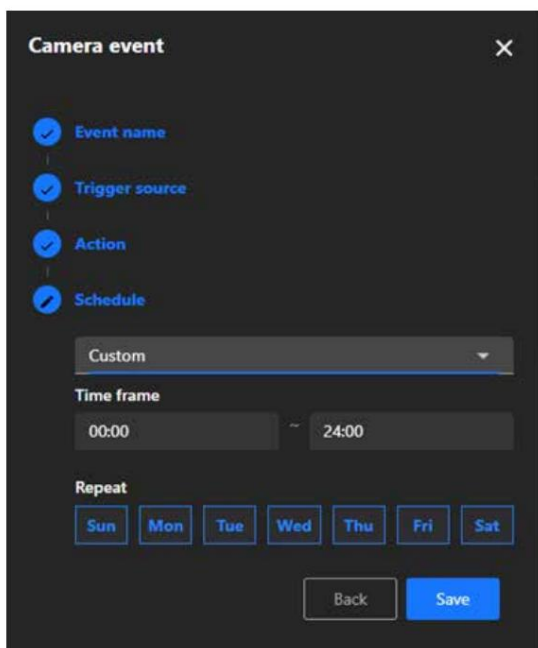
Definiere, wann das Ereignis aktiv sein soll:

Immer: Die Veranstaltung ist immer aktiv.

Bestimmte Zeiten: Konfigurieren Sie das Ereignis so, dass es nur zu bestimmten Zeiten aktiv ist (z. B. nur nachts).

Prüfen Sie den Zeitplan und bestätigen Sie ihn.

Klicken Sie auf Speichern, um die Einrichtung abzuschließen.



Ereignis

Notiz:

Die Arten von Ereignisauslösern:

Gerät	
Periodisch	Das Ereignis wird in regelmäßigen, vom Benutzer festgelegten Abständen ausgelöst.
Systemstart	Das Ereignis wird beim Einschalten der Kamera ausgelöst.
Manueller Auslöser	Das Ereignis wird manuell vom Benutzer ausgelöst.
Digitaler Eingang	Das Ereignis wird durch ein digitales Signal von einem externen Gerät ausgelöst, wie zum Beispiel ein Sensor.
Detektion	
Bewegungserkennung	Das Ereignis wird ausgelöst, wenn die Kamera ein sich bewegendes Objekt in ihrem Sichtfeld erkennt.
Manipulationserkennung	Das Ereignis wird ausgelöst, wenn die Kamera eine Manipulation feststellt, z. B. wenn sie abgedeckt, bewegt oder verdeckt wird.
Audioerkennung	Das Ereignis wird ausgelöst, wenn die Kamera ungewöhnliche Geräusche, wie zum Beispiel plötzliche laute Geräusche, erkennt.
Schockerkennung	Das Ereignis wird ausgelöst, wenn die Kamera physikalische Stöße oder Vibrationen erkennt.
Aufnahme	
Aufzeichnungsbenachrichtigung	Das Ereignis wird ausgelöst, wenn die Aufnahme startet oder stoppt.

Ereignis

VADP	
BruteForceAttack	Das Ereignis wird ausgelöst, wenn wiederholte fehlgeschlagene Anmeldeversuche festgestellt werden, was auf einen möglichen Brute-Force-Angriff auf das Kamerasystem hindeutet.
Cyberangriff	Das Ereignis wird ausgelöst, wenn verdächtige Netzwerkaktivitäten festgestellt werden, die einem Cyberangriff auf die Kamera ähneln.
Lizenzablauf	Das Ereignis wird ausgelöst, wenn die Software- oder Funktionslizenz demnächst abläuft, um die Benutzer im Voraus zu benachrichtigen.
Quarantäne	Das Ereignis wird ausgelöst, wenn in einer festgelegten Quarantänezone unbefugte Verstöße oder Zuwiderhandlungen auftreten.
Gekreuzt	Das Ereignis wird ausgelöst, wenn ein Objekt oder eine Person eine vordefinierte virtuelle Grenze überschreitet.
Objekt ist Überlaufen	Das Ereignis wird ausgelöst, wenn in einem bestimmten Bereich eine Menschenansammlung oder eine hohe Objektdichte festgestellt wird.
Objekte im Inneren	Das Ereignis wird ausgelöst, wenn Objekte einen vom Benutzer definierten Überwachungsbereich betreten.
Objekt lauert herum	Das Ereignis wird ausgelöst, wenn sich Objekte oder Personen über einen längeren Zeitraum in einem bestimmten Bereich aufhalten.
Objekt läuft	Das Ereignis wird ausgelöst, wenn sich schnell bewegende Objekte, wie zum Beispiel laufende Personen, im Sichtfeld der Kamera identifiziert werden.
Verlassene Gegenstände	Das Ereignis wird ausgelöst, wenn Gegenstände in einem überwachten Bereich unbeaufsichtigt gelassen werden. Zone.
Objekte fehlen	Das Ereignis wird ausgelöst, wenn Objekte aus einem vordefinierten Bereich entfernt werden oder daraus verschwinden.
Gesicht	Das Ereignis wird ausgelöst, wenn menschliche Gesichter zu Identifizierungs- oder Verfolgungszwecken erkannt werden.
Verstoßen	Das Ereignis wird ausgelöst, wenn in einem definierten Bereich eine eingeschränkte oder verbotene Handlung stattfindet.

Ereignis

VADP	
Objekt ist eingeschränkt	Das Ereignis wird ausgelöst, wenn Objekte in Sperrzonen gelangen oder sich dort aufhalten, wo sie nicht zugelassen sind.
Netzwerk	
Ablauf des Zertifikats Benachrichtigen	Das Ereignis wird ausgelöst, wenn das Sicherheitszertifikat kurz vor dem Ablauf steht.

Verbessern Sie die Koordination mehrerer Kameras und beseitigen Sie tote Winkel mit Camera Link.

Die Kameraverknüpfung in den Ereigniseinstellungen ermöglicht die nahtlose Integration und Koordination mehrerer Kameras und gewährleistet so eine umfassende Überwachung sowie die Beseitigung potenzieller toter Winkel. Durch die Förderung der Interaktion und der gemeinsamen Reaktion auf Auslöser verbessert diese Funktion das Lagebewusstsein, steigert die Effizienz der Überwachung und bietet eine robuste Lösung für komplexe Sicherheitsumgebungen. Ob bei der Verwaltung großer Anlagen, der Überwachung mehrerer Zonen oder der Sicherstellung einer vollständigen Abdeckung kritischer Bereiche – Camera Link ermöglicht Nutzern intelligente, ereignisgesteuerte Abläufe, die auf ihre spezifischen Bedürfnisse zugeschnitten sind.

Kameraverbindung

Die Camera Link-Funktion ermöglicht es einer Kamera, bei einem Ereignis Aktionen an anderen verbundenen Kameras auszulösen. Beispielsweise kann eine Standardkamera mit einer PTZ-Kamera gekoppelt werden. Wird im Bewegungsfenster Nr. 1 eine Bewegung erkannt, fährt die gekoppelte PTZ-Kamera automatisch in die voreingestellte Position und startet die Objektverfolgung. Diese koordinierte Reaktion gewährleistet eine umfassende Ereignisabdeckung und beseitigt effektiv tote Winkel, indem mehrere Perspektiven in Echtzeit erfasst werden – selbst in komplexen oder großen Überwachungsbereichen.

Hauptzweck der Kameraverbindung

Multi-Kamera-Koordination

Wird ein Ereignis von einer Kamera erfasst, kann dies Aktionen auf anderen verbundenen Kameras auslösen, wie beispielsweise das Abspielen eines Audioclips, das Anfahren einer voreingestellten Position oder das Starten der intelligenten Verfolgung bei PTZ-Kameras. Dadurch eignet sich das System ideal für kleinere Überwachungsszenarien, in denen kein Videomanagementsystem (VMS) für die zentrale Verwaltung zur Verfügung steht.

Zentralisierte Verwaltung

Die Camera-Link-Funktion fasst mehrere Kameras zu einem einheitlichen System zusammen, optimiert so die Abläufe und steigert die Effizienz. Dadurch eignet sie sich besonders für Überwachungssysteme in Sicherheitszentralen, intelligenten Gebäuden oder Gewerbekomplexen.

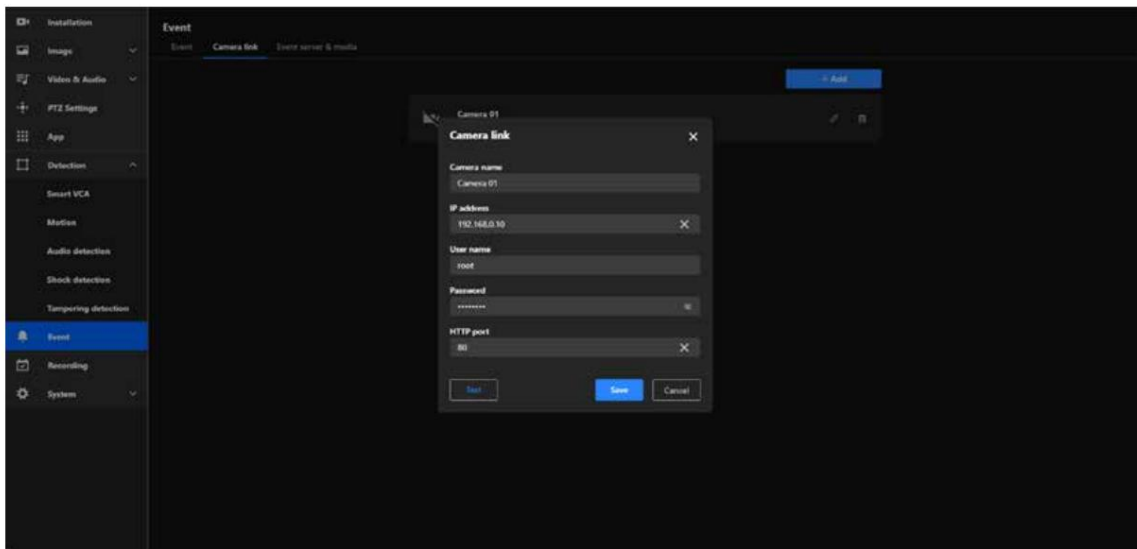
Ereignis

Erhöhte Sicherheit

Die Camera Link-Funktion ermöglicht die Überwachung kritischer Bereiche aus verschiedenen Blickwinkeln, indem sie es anderen Kameras erlaubt, automatisch Aufnahmen aus unterschiedlichen Blickwinkeln zu erfassen, wenn in einer Zone ein Ereignis ausgelöst wird. Dadurch werden tote Winkel effektiv reduziert und das Situationsbewusstsein verbessert.

Datenintegration und Ereignisprotokollierung

Ereignisse und Aufzeichnungen von mehreren Kameras können auf einem Server oder in einem Speichersystem zentralisiert werden, was eine nahtlose Ereignisverfolgung und -analyse ermöglicht.



Schritte zum Hinzufügen eines Kameralinks

Schritt 1. Klicken Sie auf die Schaltfläche „+ Hinzufügen“, um einen neuen Kameralink-Eintrag zu erstellen.

Schritt 2. Kameradetails eingeben:

Kameraname: Geben Sie einen beschreibenden Namen für die verknüpfte Kamera ein.

IP-Adresse: Geben Sie die IP-Adresse der Zielkamera an, die Sie verbinden möchten.

Benutzername: Geben Sie den Benutzernamen ein, der zur Authentifizierung an der Zielkamera erforderlich ist, standardmäßig „root“.

Passwort: Geben Sie das zum Benutzernamen passende Passwort ein.

HTTP-Port: Geben Sie den HTTP-Port an, der von der Zielkamera verwendet wird. Standardmäßig ist dies in der Regel Port 80, sofern er nicht angepasst wurde.

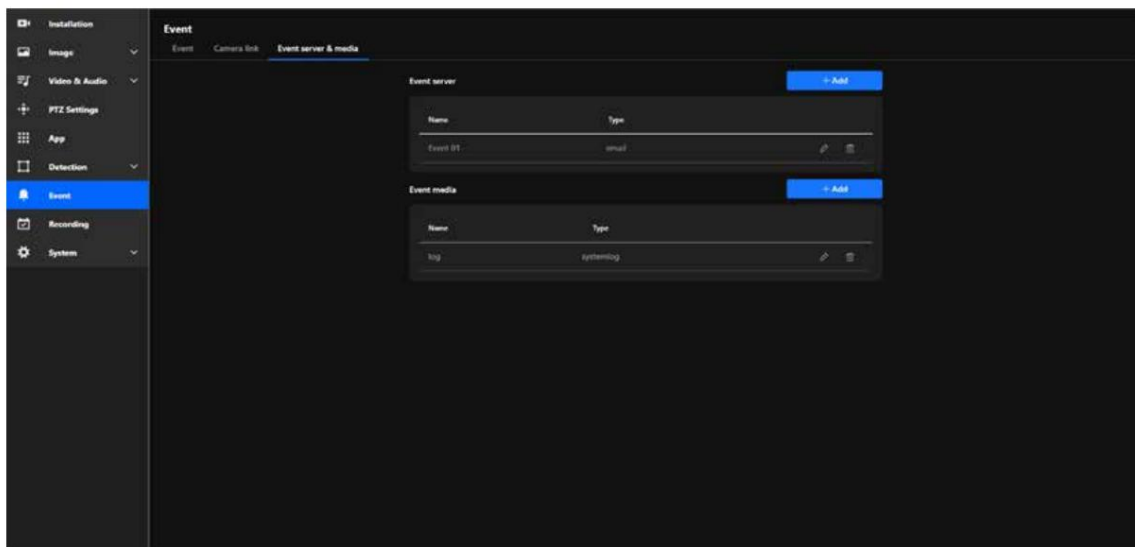
Schritt 3. Klicken Sie auf die Schaltfläche „Testen“, um sicherzustellen, dass die Verbindungsdaten korrekt sind und die Kameraverbindung erfolgreich hergestellt wurde.

Schritt 4. Sobald die Verbindung erfolgreich getestet wurde, klicken Sie auf die Schaltfläche Speichern, um die Kameraverbindungskonfiguration zu speichern.

Ereignis

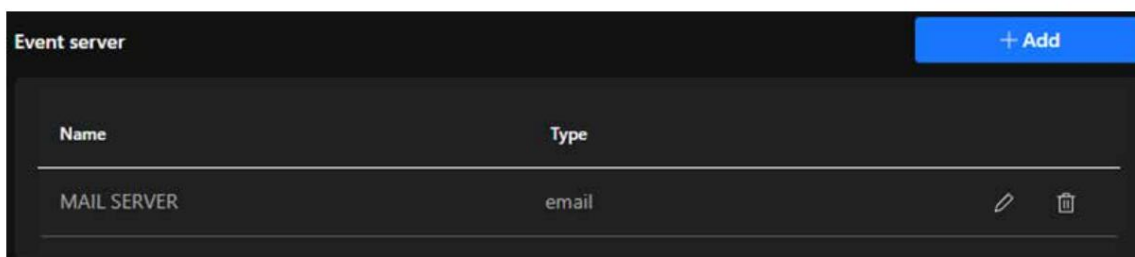
Müheloses Eventmanagement und erhöhte Sicherheit mit Ereignisserver & Medien

Der Event-Server & Media bietet umfassende Funktionen, die das Ereignismanagement vereinfachen, die Sicherheit erhöhen und den Benutzerkomfort steigern. Er gewährleistet die effiziente, zuverlässige und auf die individuellen Bedürfnisse jedes Benutzers zugeschnittene Verarbeitung von Ereignisdaten und ist somit ein unverzichtbares Werkzeug für moderne Überwachungssysteme.



Integration externer Geräte

VIVOTEK bietet mit seinen verschiedenen Event-Server-Typen eine flexible und robuste Event-Management-Lösung, die sich an unterschiedliche Sicherheits- und Überwachungsanforderungen anpassen lässt. Die Hauptfunktionen und -zwecke dieser Server sind folgende:



E-Mail

Diese Lösung versendet E-Mail-Benachrichtigungen an vordefinierte Empfänger, sobald ein Ereignis eintritt, und informiert die Nutzer umgehend mit detaillierten Ereignisinformationen. Sie unterstützt außerdem das Anhängen von Screenshots oder ereignisbezogenen Daten und ist somit ideal für kleinere Installationen oder individuelle Überwachungsanforderungen geeignet.

FTP

Diese Lösung lädt ereignisbezogene Dateien wie Snapshots, Videos oder Protokolle auf einen FTP-Server hoch und bietet so einen zentralen Speicher für Ereignismedien. Sie eignet sich ideal für die Verwaltung von Ereignisdaten in Umgebungen mit stabiler Netzwerkverbindung und ist besonders für große Implementierungen geeignet, die organisierte und effiziente Speicherlösungen erfordern.

Ereignis

SFTP

Diese Lösung lädt ereignisbezogene Dateien sicher und verschlüsselt auf einen SFTP-Server hoch und verbessert so den Datenschutz während der Übertragung. Sie eignet sich ideal für Umgebungen, in denen sensible Informationen vor Abfangen oder Manipulation geschützt werden müssen, und gewährleistet die Einhaltung strenger Sicherheitsrichtlinien und gesetzlicher Vorgaben.

HTTP

Diese Lösung sendet Ereignisbenachrichtigungen oder Daten per HTTP-Anfrage an einen HTTP-Server und ermöglicht so die nahtlose Integration mit Drittsystemen oder -anwendungen für eine effiziente Ereignisverarbeitung. Sie kann Workflows in fortschrittlichen Sicherheitssystemen, Hausautomatisierungssystemen oder Analyseplattformen auslösen und vereinfacht die Integration in Umgebungen, die auf benutzerdefinierten APIs oder HTTP-basierten Lösungen beruhen.

HTTPS

Diese Lösung nutzt das sichere HTTPS-Protokoll für verschlüsselte Kommunikation und gewährleistet so eine sichere Datenübertragung, um unbefugten Zugriff oder Datenlecks zu verhindern. Sie eignet sich ideal für sensible Anwendungen, die Vertraulichkeit erfordern, und wird häufig in modernen, sicheren Netzwerkumgebungen eingesetzt.

Event server ✕

Server name
MAIL SERVER

Server type
E-mail ▾

Sender email address
sender@vivotek.com ✕

Recipient email address
recipient@vivotek.com ✕

Server address
10.1.1.1

User name
User name
root

Password
..... 🔒

Server port
25

☐ This server requires a secure connection

Test Save Cancel

Ereignis

Schritte zum Konfigurieren eines Ereignisservers Schritt

1. Klicken Sie auf die Schaltfläche + Hinzufügen, um einen neuen Server hinzuzufügen.

Schritt 2. Wählen Sie im Popup-Fenster den Servertyp aus, den Sie konfigurieren möchten:

E-Mail: Zum Versenden von Veranstaltungsbenachrichtigungen per E-Mail.

FTP: Zum Hochladen von ereignisbezogenen Dateien (z. B. Schnappschüssen oder Videos) auf einen FTP-Server.

SFTP: Ähnlich wie FTP, verwendet aber für zusätzliche Sicherheit eine verschlüsselte Dateiübertragung.

HTTP: Zum Senden von HTTP-Anfragen mit Ereignisinformationen an ein Drittsystem.

HTTPS: Ähnlich wie HTTP, verwendet aber ein sicheres Kommunikationsprotokoll.

Schritt 3. Klicken Sie auf Weiter, um mit der serverspezifischen Konfiguration fortzufahren.

Schritt 4. Füllen Sie je nach gewähltem Servertyp die erforderlichen Felder aus:

E-Mail-Server:

SMTP-Server: Geben Sie die Adresse des SMTP-Servers ein (z. B. smtp.example.com).

Port: Geben Sie den Port an (z. B. 25, 465 oder 587, abhängig von der SMTP-Konfiguration).

Authentifizierung: Aktivieren Sie die Authentifizierung und geben Sie anschließend Benutzernamen und Passwort für das E-Mail-Konto ein.

Absender-E-Mail-Adresse: Geben Sie die „Von“-Adresse für E-Mail-Benachrichtigungen ein.

E-Mail-Adresse des Empfängers: Geben Sie die E-Mail-Adresse des Empfängers ein, damit dieser Benachrichtigungen erhalten kann.

FTP-Server:

FTP-Serveradresse: Geben Sie die IP-Adresse oder den Domännennamen des FTP-Servers ein.

Port: Standardmäßig ist es 21 (bei Bedarf anpassen).

Benutzername und Passwort: Geben Sie die Zugangsdaten zur Authentifizierung am FTP-Server ein.

Ordnerpfad: Geben Sie den Ordner an, in den die Dateien hochgeladen werden sollen.

SFTP-Server:

Ähnlich wie bei FTP, aber stellen Sie sicher, dass das SFTP-Protokoll unterstützt wird und die Zugangsdaten sicher eingegeben werden.

HTTP-Server:

Server-URL: Geben Sie die vollständige URL des HTTP-Servers ein (z. B. http://example.com/api/event).

HTTPS-Server:

Dasselbe wie bei HTTP, aber stellen Sie sicher, dass die Server-URL mit „https://“ beginnt.

Notiz:

Laden Sie gegebenenfalls Zertifikate hoch und konfigurieren Sie diese für eine sichere Kommunikation.

Schritt 5. Klicken Sie auf die Schaltfläche „Testen“, um zu überprüfen, ob die Kamera erfolgreich eine Verbindung zum Server herstellen kann.

Schritt 6. Nach einem erfolgreichen Test klicken Sie auf „Speichern“, um die Serverkonfiguration zu speichern. Der neue Server wird dann in der Liste der Ereignisservers angezeigt.

Ereignis

Schritt 7. Server mit einem Ereignis verknüpfen

Wechseln Sie zurück zur Registerkarte „Ereignis“.

Erstellen Sie eine neue Veranstaltung oder bearbeiten Sie eine bestehende.

Wählen Sie im Abschnitt „Ereignisserver“ den konfigurierten Server aus.

Definieren Sie die Aktionen und Medien, die an den Server gesendet werden sollen, wenn das Ereignis ausgelöst wird.

Server	Media
☐ SD	none
☒ Event 01	log

Notiz:

Verwenden Sie starke und einzigartige Passwörter für die Serverauthentifizierung, um die Sicherheit zu erhöhen.

Stellen Sie bei HTTPS und SFTP sicher, dass Zertifikate und Verschlüsselungseinstellungen korrekt konfiguriert sind.

Die Serververbindung sollte regelmäßig überwacht und getestet werden, um eine zuverlässige Ereignisverarbeitung zu gewährleisten.

● Veranstaltungsmedien

Die Event-Medieneinstellungen bieten eine leistungsstarke und flexible Medienverwaltungslösung, mit der Benutzer während Ereignissen schnell Mediendateien erstellen, speichern und übertragen können. Dies erfüllt die Anforderungen an Echtzeitüberwachung, Ereignisaufzeichnung und Beweissicherung und verbessert die Effizienz und Zuverlässigkeit von Überwachungssystemen. Die Hauptfunktionen und -zwecke dieser Server sind folgende:

Name	Type
log	systemlog

Schnappschuss

Es wird ein Standbild im Moment des Auslösens des Ereignisses aufgenommen, wodurch eine schnelle visuelle Darstellung des Ereignisses entsteht, die nützlich ist, um bestimmte Momente zu überprüfen oder Schlüsselemente wie Gesichter oder Objekte zu identifizieren.

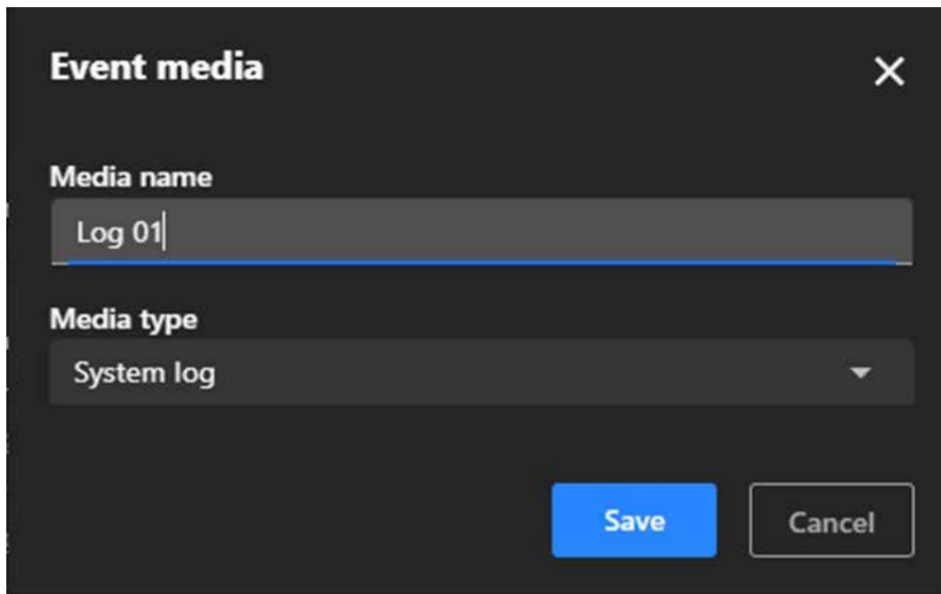
Videoclip

Zeichnet vor, während und nach dem Auslösen des Ereignisses ein kurzes Videosegment auf und bietet so detaillierten Kontext und eine dynamische Sicht auf das Ereignis, um den Benutzern eine gründliche Analyse von Vorfällen wie der Bewegung von Personen oder Objekten zu ermöglichen.

Ereignis

Systemprotokoll

Erfasst Textdaten über das Ereignis, einschließlich der Art des Ereignisses, des Zeitpunkts und der damit verbundenen Systemaktivität, und bietet so eine chronologische Aufzeichnung für Prüfungen und die Fehlerbehebung. Gleichzeitig ist er nützlich für die Überwachung der Systemleistung und die Identifizierung von Anomalien.



Schritte zum Konfigurieren eines Ereignisservers

Schritt 1. Klicken Sie auf die Schaltfläche + Hinzufügen, um eine neue Medienkonfiguration zu erstellen.

Schritt 2. Geben Sie im Feld „Medienname“ einen beschreibenden Namen für das Medium ein.

Schritt 3. Medientyp auswählen

Wählen Sie einen der folgenden Medientypen aus dem Dropdown-Menü aus:

Schnappschuss: Nimmt ein Standbild auf.

Videoclip: Nimmt einen kurzen Videoclip auf.

Systemprotokoll: Speichert Textdaten zum Ereignis.

Schritt 4. Medienspezifische Einstellungen konfigurieren

Schnappschuss:

Quelle: Wählen Sie den Videostream aus, aus dem Schnappschüsse aufgenommen werden sollen.

Voreignispuffer (Sekunden): Legen Sie fest, wie viele Sekunden vor dem Ereignis Momentaufnahmen erfasst werden sollen.

Nachereignispuffer (Sekunden): Legen Sie fest, wie viele Sekunden nach dem Ereignis weiterhin Momentaufnahmen erfasst werden sollen.

Benutzerdefinierte Bildfrequenz (Bilder/Sekunde): Legen Sie die Frequenz für die Bildaufnahme fest (z. B. 1 Bild pro Sekunde).

Dateinamenpräfix: Geben Sie ein benutzerdefiniertes Präfix für Snapshot-Dateinamen ein.

Optional können Sie das Kontrollkästchen aktivieren, um den Dateinamen zur besseren Organisation ein Datums- und Zeit-Suffix hinzuzufügen.

Notiz:

Die Auflösungseinstellung kann die maximale Anzahl der aufnehmbaren Schnappschüsse beeinflussen. Weitere Informationen finden Sie auf der Steam-Seite unter Video & Audio > Video > Steam.

Ereignis

Videoclip:

Quelle: Wählen Sie den Videostream aus, von dem aufgenommen werden soll.

Aufzeichnung vor dem Ereignis (Sekunden): Legen Sie fest, wie viele Sekunden vor dem Ereignis die Aufzeichnung beginnen soll.

Maximale Dauer (Sekunden): Legen Sie die maximale Länge des Videoclips fest (z. B. 5 Sekunden).

Maximale Dateigröße (KB): Geben Sie die maximale Dateigröße für den Videoclip an.

Dateinamenpräfix: Geben Sie ein benutzerdefiniertes Präfix für Videodateinamen ein, um die Dateiidentifizierung zu vereinfachen.

Systemprotokoll:

Dieser Medientyp zeichnet ereignisbezogene Daten wie Ereignistyp, Zeitpunkt und zugehörige Systemaktivitäten auf.

Schritt 5. Nachdem Sie die Einstellungen konfiguriert haben, klicken Sie auf „Speichern“, um die Medienkonfiguration abzuschließen. Diese wird dann in der Liste „Ereignismedien“ angezeigt.

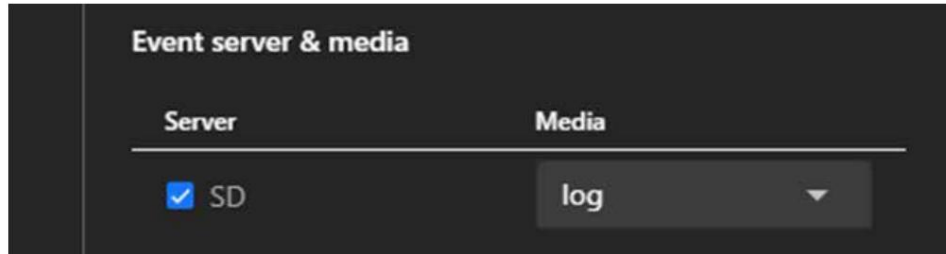
Schritt 6. Event-Medien mit einem Event verknüpfen.

Wechseln Sie zur Registerkarte „Ereignisse“.

Erstellen Sie eine neue Veranstaltung oder bearbeiten Sie eine bestehende.

Wählen Sie in den Ereigniseinstellungen unter dem Abschnitt Ereignismedien die konfigurierten Medien aus.

Dadurch wird sichergestellt, dass die konfigurierten Medien (z. B. Schnappschüsse, Videoclips oder Systemprotokolle) generiert werden, wenn das Ereignis ausgelöst wird.

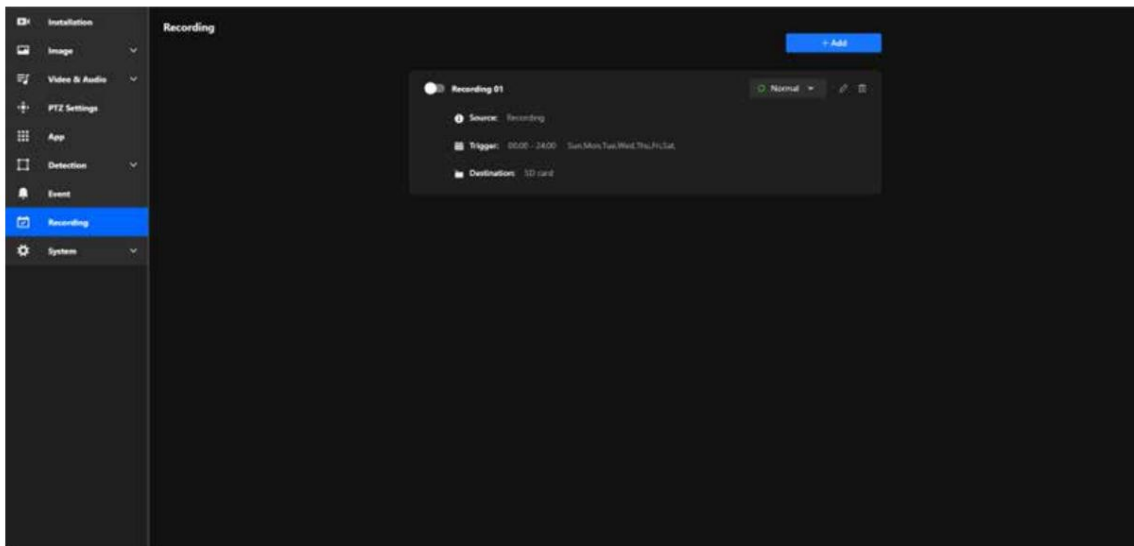


Aufnahme

Maximieren Sie Überwachung und Speicherung durch maßgeschneiderte Aufzeichnungseinstellungen

Die Aufnahmeeinstellungen ermöglichen es Nutzern, ihre Überwachung präzise und effizient anzupassen. Dank flexibler Zeitplanung, ereignisbasierter Auslöser und vielfältiger Speicheroptionen wird sichergestellt, dass wichtige Aufnahmen erfasst und gleichzeitig der Speicherplatz optimal genutzt wird. Ob Sie eine 24/7-Überwachung oder Aufnahmen benötigen, die durch bestimmte Ereignisse wie Bewegung oder Geräusche ausgelöst werden – das System passt sich nahtlos Ihren Bedürfnissen an.

Durch die Möglichkeit, Aufnahmen lokal auf einer SD-Karte oder einem Netzlaufwerk zu speichern, können Benutzer Datensicherheit und -verfügbarkeit gewährleisten. Dieser individuell anpassbare Ansatz vereinfacht die Verwaltung, erhöht die Sicherheit und sorgt für ein beruhigendes Gefühl – ein unverzichtbares Merkmal für jede Überwachungsanlage.



Hauptzweck der Aufzeichnung:

Überwachung und Sicherheit

Gewährleistet die Überwachung kritischer Bereiche und die Erfassung von Videobeweisen, entweder kontinuierlich oder ereignisbezogen.

Ereignisuntersuchung

Ermöglicht es Benutzern, Aufzeichnungen einzusehen, um Vorfälle zu untersuchen oder Aktivitäten zu analysieren.

Effizientes Speichermanagement

Durch die Festlegung spezifischer Zeitpläne und Auslöser werden unnötige Aufnahmen minimiert und Speicherplatz gespart.

Flexibilität für unterschiedliche Szenarien

Erfüllt verschiedene Aufzeichnungsanforderungen, wie z. B. die Überwachung rund um die Uhr oder die selektive Aufzeichnung basierend auf Bewegungserkennung oder bestimmten Zeitrahmen.

Datensicherung und Datenzugriff

Gewährleistet, dass Aufnahmen sicher gespeichert werden und bei Bedarf entweder von lokalen SD-Karten oder über Netzwerkspeicherlösungen abgerufen werden können.

Aufnahme

Schritt 6. Wählen Sie unter „Ziel“ aus, wo die Aufnahmen gespeichert werden sollen:

SD

Aufnahmen werden lokal auf der in die Kamera eingelegten SD-Karte gespeichert. Diese Option eignet sich ideal für Einzelplatzinstallationen oder wenn ausreichend lokaler Speicherplatz vorhanden ist.

IM

Speichern Sie Aufnahmen auf einem NAS-Gerät (Network Attached Storage). Dies ist nützlich für die zentrale Speicherung und einfachere Verwaltung von Videodaten, insbesondere in größeren Überwachungssystemen.

Notiz:

Wird keine SD-Karte erkannt oder ist sie nicht korrekt installiert, erscheint eine Warnmeldung. Stellen Sie sicher, dass eine SD-Karte eingelegt ist, oder konfigurieren Sie die NAS-Einstellungen, bevor Sie fortfahren.

Schritt 7. Sobald alle Felder konfiguriert sind, klicken Sie auf Speichern, um die Einstellungen anzuwenden.

Mit adaptiver Aufzeichnung

Adaptive Aufzeichnung ist eine intelligente Funktion, die die Überwachungseffizienz optimiert, indem sie die Videobildrate dynamisch an Echtzeitereignisse anpasst. Durch die Reduzierung von Bandbreiten- und Speichernutzung bei der routinemäßigen Überwachung und die Sicherstellung einer hohen Videoqualität bei kritischen Ereignissen verbessert Adaptive Aufzeichnung sowohl die Systemleistung als auch das Ressourcenmanagement. Ihre Hauptzwecke sind:

Bandbreiten- und Speicheroptimierung:

Im normalen Überwachungsbetrieb reduziert das System den Bandbreitenverbrauch und die Speichernutzung, indem es ausschließlich I-Frame-Daten sendet.

Erweiterte Ereignisaufzeichnung:

Wird ein Alarm ausgelöst, erhöht sich die Bildrate auf die volle Bildrate, um kritische Momente in hoher Qualität festzuhalten.

Ressourceneffizienz:

Das System optimiert die Nutzung der Bildrate auf Basis des tatsächlichen Bedarfs und gewährleistet so eine effiziente Nutzung der Netzwerk- und Speicherressourcen ohne Leistungseinbußen.

Wie erreicht die adaptive Aufzeichnung die oben genannten Ziele?

1. Dynamische Bildratenanpassung:

Wenn die adaptive Aufzeichnung aktiviert ist, passt die Kamera die Bildrate dynamisch an Alarmauslöser wie Bewegungserkennung, DI-Geräte oder manuelle Auslöser an.

Wenn ein Alarm ausgelöst wird:

Die Kamera zeichnet die Streaming-Daten in voller Bildrate auf, um eine hohe Videoqualität bei kritischen Ereignissen zu gewährleisten.

Wenn kein Alarm ausgelöst wird:

Die Kamera sendet während der normalen Überwachung nur Intra-Frame-Daten (I-Frames), um Bandbreiten- und Speichernutzung zu minimieren.

Aufnahme

2. Bildratensteuerung:

Kein Alarm ausgelöst:

JPEG-Modus: 1 Intra-Frame (I-Frame) pro Sekunde.

H.264-Modus: Zeichnet nur Intra-Frames (I-Frames) auf.

Alarmauslöser:

Erhöht sich automatisch auf die konfigurierte volle Bildrate.

3. Begrenzung der Frame-Periode:

Wenn die Intra-Frame-Periode (I-Frame) auf der Seite Video & Audio > Video > Stream größer als 1 Sekunde ist, reduziert die Firmware sie automatisch auf 1 Sekunde, wenn die adaptive Aufnahme aktiviert ist.



System

Das System fungiert als umfassende Managementzentrale zur Konfiguration und Überwachung des Geräts.

Es bietet essenzielle Werkzeuge zur Verwaltung von Kamerasysteminformationen, Netzwerkkonfigurationen, Benutzerkonten, Speicherlösungen und Wartungsaufgaben. Hauptziel ist die Gewährleistung eines sicheren und effizienten Gerätebetriebs durch Funktionen wie Firmware-Updates, Protokollanalyse und Systemdiagnose. Darüber hinaus verbessert es die Benutzerfreundlichkeit durch anpassbare Designs und optimiert die Datenverwaltung durch die Organisation von Speicher und Dateiverarbeitung. Diese Kategorie spielt eine entscheidende Rolle für die optimale Kameraleistung und die nahtlose Integration in eine Netzwerkkumgebung.

Zentralisierte Verwaltung für Systemüberwachung und Kamerakonfiguration

Das Geräteelement dient als zentrale Schnittstelle zur Überwachung und Konfiguration der wichtigsten Systeminformationen, des Betriebszustands und der Hardwareeinstellungen der Kamera. Es bietet Nutzern Echtzeit-Einblicke in die Systemleistung (CPU, Speicher und Festplatte), ermöglicht die einfache Identifizierung und Verwaltung des Geräts anhand von Netzwerk- und Hardwaredetails, gewährleistet die präzise Zeitsynchronisation von Aufnahmen und Protokollen und erleichtert die Integration externer Geräte über LED- und DIDO-Steuerungen. Insgesamt verbessert es die Verwaltbarkeit, die Leistungsüberwachung und die Betriebsgenauigkeit der Kamera auf benutzerfreundliche Weise.

Das Gerät umfasst vier Funktionskarten, die den Betriebszustand der Kamera, grundlegende Geräteinformationen, die Systemzeitsynchronisation und die Interaktion mit externen Geräten abdecken. Seine Hauptzwecke sind folgende:

- **Echtzeitüberwachung**

Hilft Benutzern dabei, die Ressourcennutzung und die Speicherkapazität der Kamera zu verfolgen.

- **Identifizierung und Management**

Ermöglicht die einfache Identifizierung und Netzwerkverwaltung durch grundlegende Geräteinformationen.

- **Zeitsynchronisation**

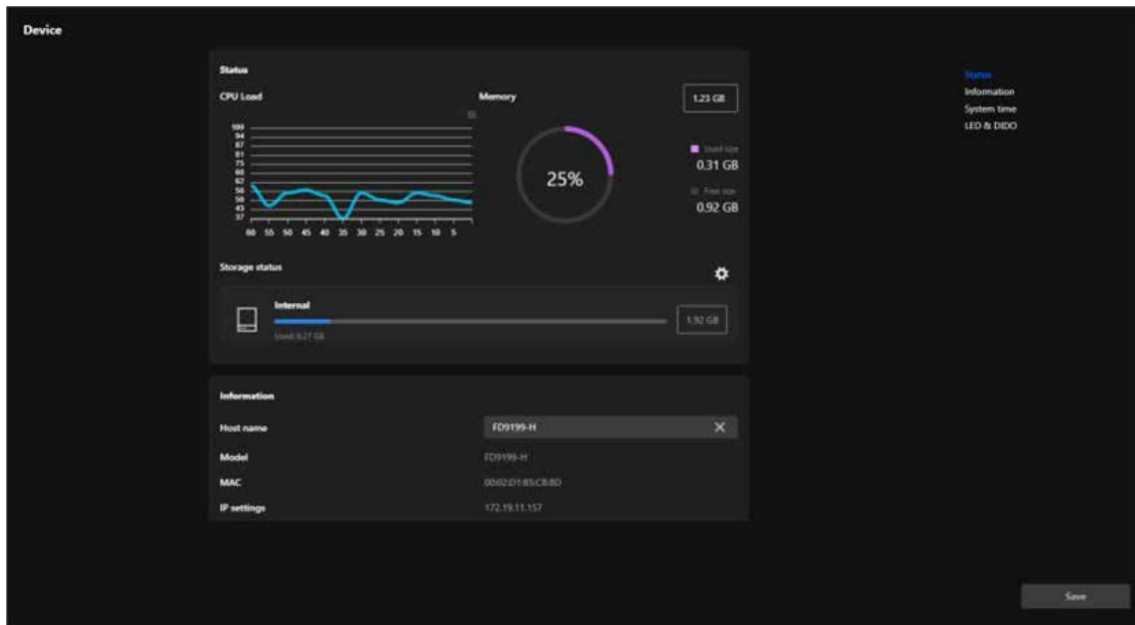
Gewährleistet die Genauigkeit der Aufzeichnungsdateien und Ereignisprotokolle.

- **Integration externer Geräte**

Ermöglicht die Interaktion mit externen Geräten zur Erweiterung funktionaler Anwendungen.

System

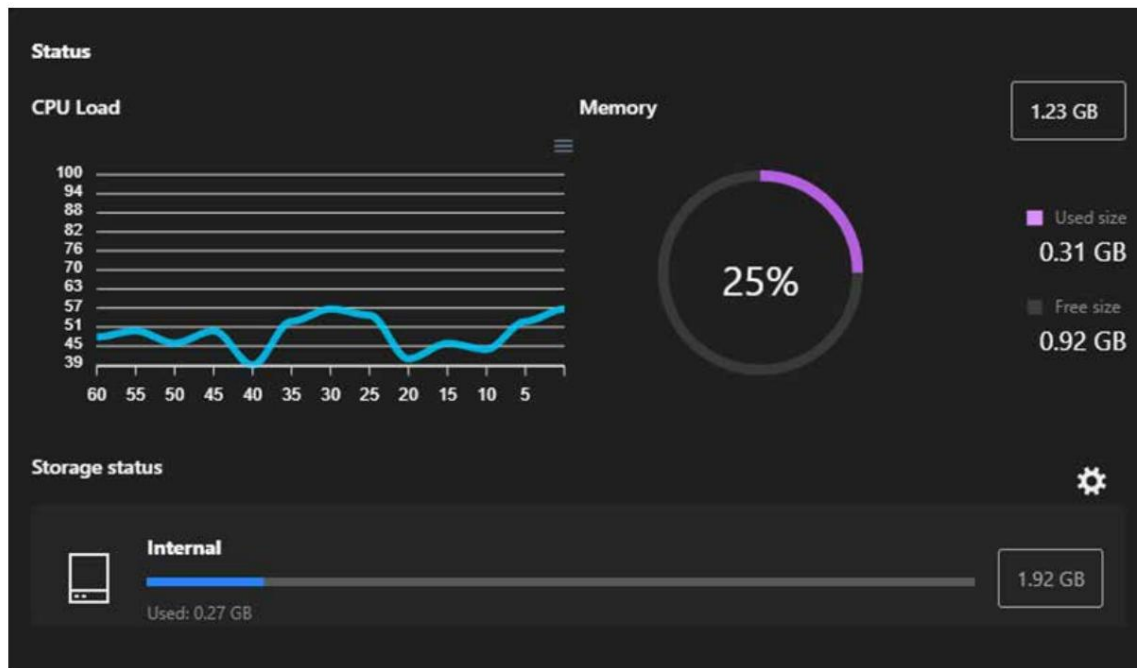
Diese Funktionen dienen dazu, die Benutzerfreundlichkeit, die operative Flexibilität und die Integrationsfähigkeit der Kamera mit anderen Geräten zu verbessern.



System

Status

Die Statuskarte dient als Echtzeit-Dashboard zur Überwachung der Betriebsleistung der Kamera. Durch detaillierte Einblicke in die CPU-, Speicher- und Speichernutzung unterstützt sie Benutzer dabei, eine optimale Geräteleistung zu gewährleisten, die Systemstabilität sicherzustellen und Ressourcenmanagementanforderungen proaktiv zu erfüllen.



- **CPU-Auslastung**

Zeigt die CPU-Auslastung der Kamera in Echtzeit als Liniendiagramm an und verdeutlicht die Schwankungen im Zeitverlauf.

Hilft Benutzern dabei, die Prozessorlastentwicklung zu überwachen und potenzielle Leistungsprobleme zu erkennen.

- **Erinnerung**

Ein Kreisdiagramm visualisiert die Speichernutzung, einschließlich: Gesamtspeicherkapazität, Belegter Speicher und Verfügbarer Speicher.

Detaillierte Angaben zum belegten und freien Speicher werden zur genauen Überwachung angezeigt.

- **Speicherstatus**

Zeigt den Status des internen Speichers an, einschließlich: Gesamtspeicherkapazität, Belegter Speicherplatz und Verfügbarer Speicherplatz, dargestellt durch einen Fortschrittsbalken zur besseren Übersicht.

Beinhaltet Optionen für die weitere Speicherverwaltung über das Zahnradsymbol.

System

Information

Die Informationskarte enthält wichtige Angaben zur Identifizierung, Konfiguration und Wartung der Kamera. Sie vereinfacht die Netzwerkverwaltung, stellt sicher, dass die Kamera auf dem neuesten Stand ist, und ermöglicht den schnellen Zugriff auf wichtige Geräteinformationen, was eine effiziente Verwaltung und Fehlerbehebung unterstützt.

Information	
Host name	FD9199-H ✕
Model	FD9199-H
MAC	00:02:D1:85:CB:8D
IP settings	172.19.11.157
Firmware Version	1.2402.43.01g Upgrade

- **Hostname**

Zeigt den eindeutigen Namen der Kamera an.

Kann vom Benutzer bearbeitet werden, um die Kamera innerhalb eines Netzwerks leichter anzupassen und zu identifizieren.

- **Modell**

Zeigt die Modellnummer der Kamera an.

Hilft dabei, das spezifische Gerät für Wartungs- oder Fehlerbehebungsarbeiten zu identifizieren.

- **MAC-Adresse**

Zeigt die eindeutige MAC-Adresse der Kamera an.

Nützlich für Netzwerkdiagnose, Geräteidentifizierung oder IP-Reservierung.

- **IP-Einstellungen**

Zeigt die aktuelle IP-Adresse der Kamera an.

Ermöglicht es Benutzern, die Netzwerkverbindung und -konfiguration zu überprüfen.

- **Firmware-Version**

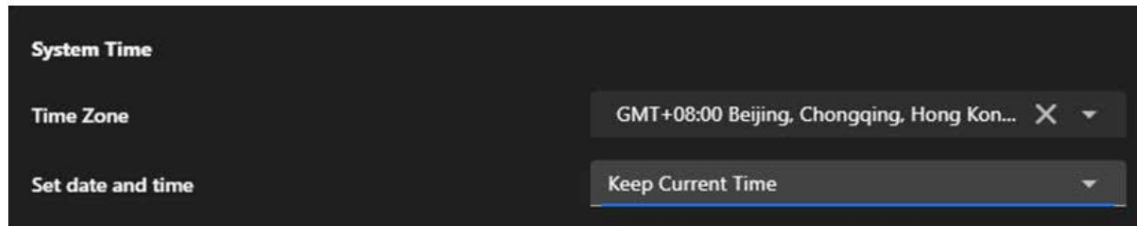
Zeigt die aktuell auf der Kamera installierte Firmware-Version an.

Beinhaltet eine Upgrade-Option, mit der Benutzer die Firmware aktualisieren können, um Zugriff auf die neuesten Funktionen, Fehlerbehebungen und Sicherheitsverbesserungen zu erhalten.

System

Systemzeit

Die Systemzeitkarte ist unerlässlich, um die Genauigkeit der Kamerazeit und deren Synchronisierung mit der Betriebsumgebung zu gewährleisten. Dank flexibler Konfigurationsmöglichkeiten unterstützt sie zuverlässiges Ereignis-Tracking, nahtlose Systemintegration und präzises Protokollmanagement und ermöglicht so eine effiziente und konsistente Überwachung in verschiedenen Setups.



● Zeitzone

Ermöglicht es dem Benutzer, die Zeitzone anhand des Standorts der Kamera auszuwählen (z. B. GMT+08:00 Peking, Chongqing, Hongkong).

Gewährleistet, dass die Kamerazeit mit der Ortszeit übereinstimmt, um eine genaue Aufzeichnung und Ereignisprotokollierung zu gewährleisten.

● Datum und Uhrzeit einstellen

Bietet vier Optionen zur Konfiguration der Kamerazeit:

Aktuelle Zeit beibehalten

Die bestehende Zeitkonfiguration der Kamera wird unverändert beibehalten.

Mit PC synchronisieren

Gleicht die Uhrzeit der Kamera mit der Uhrzeit des angeschlossenen Computers ab und bietet so eine schnelle und bequeme Möglichkeit, die Uhrzeit einzustellen.

Manuell

Ermöglicht es Benutzern, Datum und Uhrzeit manuell einzustellen, was für spezielle Anwendungsfälle geeignet ist, die benutzerdefinierte Zeiteinstellungen erfordern.

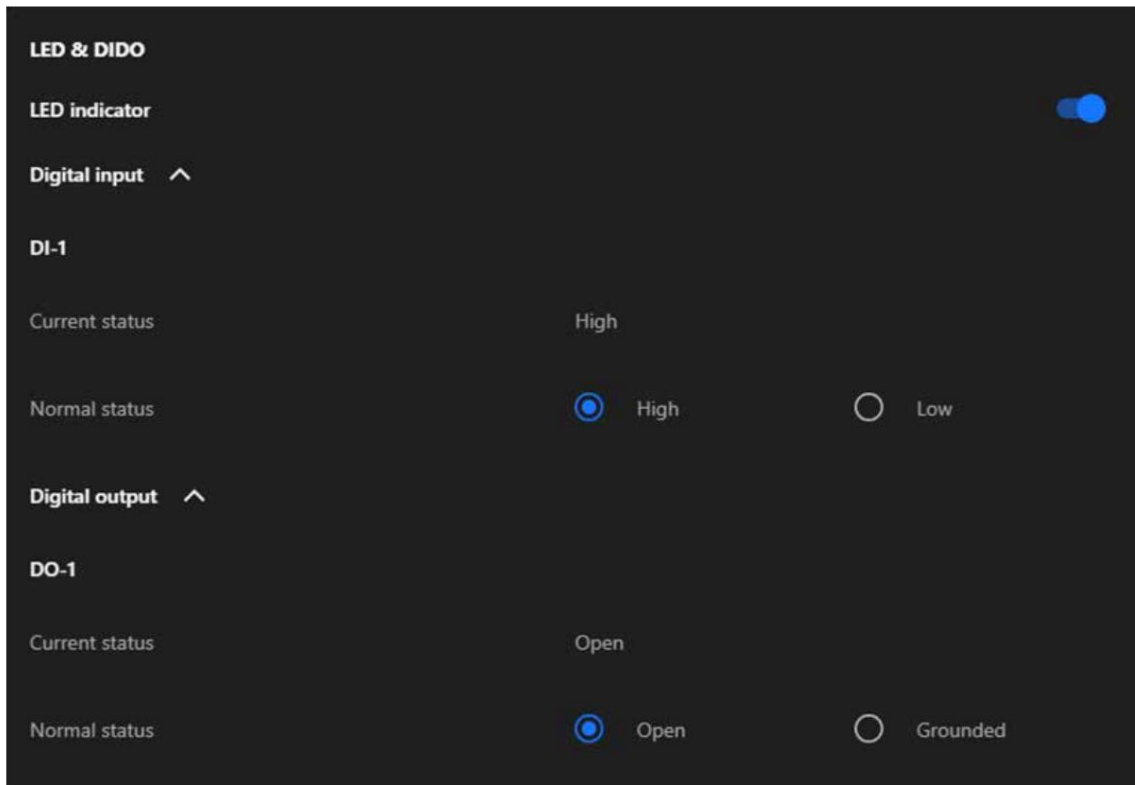
Synchronisierung mit dem NTP-Server

Synchronisiert die Kamerazeit mit einem Network Time Protocol (NTP)-Server, um genaue, automatische Zeitaktualisierungen zu gewährleisten.

System

LED & DIDO

Die LED- und DIDO-Karte dient als Schnittstelle zwischen der Kamera und ihrer Umgebung. Durch die Steuerung der LED-Anzeige und die Verwaltung der digitalen Ein-/Ausgangsschnittstellen ermöglicht sie die nahtlose Integration der Kamera in externe Geräte, erweitert deren Funktionalität und unterstützt eine Vielzahl von Automatisierungs- und Überwachungsanwendungen.



- **LED-Anzeige**

Ein Kippschalter zum Ein- und Ausschalten der LED-Anzeige der Kamera.

Wenn die LED aktiviert ist, liefert sie eine visuelle Rückmeldung über den Betriebszustand der Kamera (z. B. Einschalten, Aufnahme oder Aktivitätserkennung).

- **Digitaler Eingang**

DI-1 Aktueller Status

Zeigt den Echtzeitstatus des digitalen Eingangs an (z. B. High oder Low).

DI-1 Normaler Status

Ermöglicht dem Benutzer, den erwarteten Normalzustand für den digitalen Eingang (entweder High oder Low) zu konfigurieren. Wird zur Integration externer Sensoren (z. B. Bewegungsmelder oder Alarmanlagen) verwendet.

System

- **Digitalausgang**

- DO-1 Aktueller Status**

- Zeigt den aktuellen Zustand des digitalen Ausgangs an (z. B. offen oder geerdet).

- DO-1 Normalzustand**

- Ermöglicht dem Benutzer, den Normalzustand des digitalen Ausgangs (entweder offen oder geerdet) festzulegen. Wird zur Ansteuerung externer Geräte (z. B. Alarme, Leuchten oder Aktoren) verwendet.

- Notiz:

- Hoch/Tief im DI**

- Spiegelt das von externen Geräten empfangene Eingangssignal wider, das zur Überwachung des Status von Sensoren oder Auslösern verwendet wird.

- Offen/Geerdet in DO**

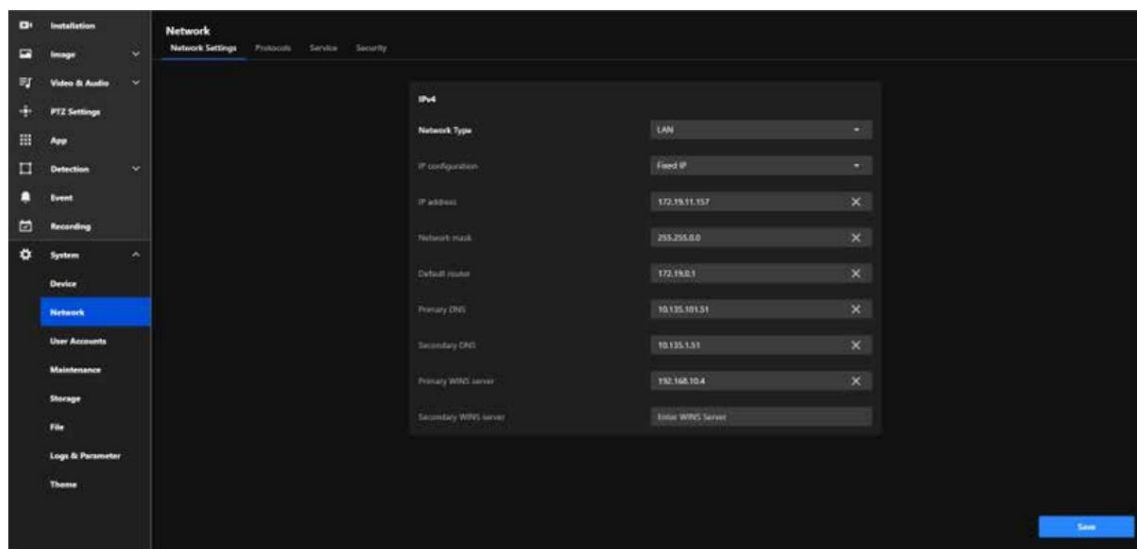
- Steuert das an externe Geräte gesendete Ausgangssignal, das zum Aktivieren oder Deaktivieren angeschlossener Geräte wie Alarmanlagen oder Aktuatoren verwendet wird.

Tore.

System

Konfigurieren und sichern Sie die Netzwerkverbindung Ihrer Kamera für Nahtlose Kommunikation

Die Netzwerkkomponente bietet umfassende Werkzeuge zur Konfiguration der Netzwerkverbindung der Kamera und gewährleistet so eine zuverlässige Kommunikation, Fernzugriff und sichere Integration mit anderen Geräten und Systemen. Diese Konfiguration ist entscheidend für Echtzeitüberwachung, Fernverwaltung und Datenübertragung über verschiedene Netzwerkinfrastrukturen.



Die wichtigsten funktionalen Zwecke sind folgende:

- **Netzwerkintegration**

Ermöglicht es der Kamera, sich über die entsprechenden IP-Einstellungen mit lokalen Netzwerken oder dem Internet zu verbinden und so Fernzugriff und -überwachung zu ermöglichen.

- **Kundenspezifische Konfiguration**

Bietet flexible Netzwerkparametereinstellungen (z. B. statische oder dynamische IP-Adresse), um die Kompatibilität mit verschiedenen Netzwerkkumgebungen zu gewährleisten.

- **Zuverlässige Kommunikation**

Gewährleistet eine reibungslose Kommunikation mit externen Systemen (z. B. NVRs oder Cloud-Plattformen) durch die korrekte Konfiguration von Gateways, DNS und Protokollen.

- **Sicherheit**

Unterstützt sichere Verbindungen und Zugriffskontrollen, um die Kamera und ihre Daten vor unberechtigtem Zugriff oder Bedrohungen zu schützen.

- **Effiziente Überwachung und Wartung**

Unterstützt die Fehlersuche und Diagnose im Netzwerk mithilfe von Tools wie WINS und DNS-Einstellungen, um einen kontinuierlichen Betrieb zu gewährleisten.

System

Netzwerkeinstellungen

Durch die Bereitstellung detaillierter Konfigurationsoptionen sowohl für IPv4 als auch für IPv6 stellt die Registerkarte „Netzwerkeinstellungen“ sicher, dass die Kamera sich nahtlos mit unterschiedlichsten und komplexen Netzwerkimgebungen verbinden und in diesen funktionieren kann.

IPv4

Die IPv4-Karte spielt eine entscheidende Rolle bei der Einrichtung der Netzwerkkonfiguration der Kamera und gewährleistet eine effektive Kommunikation. Sie ermöglicht eine zuverlässige Verbindung, sowohl lokalen als auch Fernzugriff und die problemlose Integration der Kamera in IPv4-basierte Netzwerke. Diese Konfiguration ist unerlässlich für einen stabilen und effizienten Betrieb in unterschiedlichen Netzwerkimgebungen.

IPv4	
Network Type	LAN
IP configuration	Fixed IP
IP address	172.19.11.157
Network mask	255.255.0.0
Default router	172.19.0.1
Primary DNS	10.135.101.51
Secondary DNS	10.135.1.51
Primary WINS server	192.168.10.4
Secondary WINS server	Enter WINS Server

System

IPv4

• Netzwerktyp

Ermöglicht dem Benutzer die Auswahl des Netzwerkverbindungstyps:

UND	Eine standardmäßige kabelgebundene Netzwerkverbindung, die typischerweise verwendet wird, wenn die Kamera über Ethernet mit einem lokalen Netzwerk verbunden wird.
PPPoE (Punkt-zu-Punkt) Protokoll über Ethernet)	Ein Protokoll für direkte Internetverbindungen, das häufig eine Authentifizierung mit Benutzername und Passwort des Internetanbieters (ISP) erfordert. Es wird üblicherweise in DSL-Netzen oder dann verwendet, wenn die Kamera ohne Router direkt mit dem Internet verbunden werden soll.

• IP-Konfiguration

Bietet zwei Konfigurationsoptionen:

DHCP	Weist der Kamera dynamisch eine IP-Adresse über einen Netzwerk-DHCP-Server zu; geeignet für Netzwerke mit automatischer Adressvergabe.
Feste IP-Adresse	Weist der Kamera eine statische IP-Adresse zu, um eine konsistente und zuverlässige Identifizierung im Netzwerk zu gewährleisten.

• IP-Adresse

Zeigt die IPv4-Adresse der Kamera an oder legt sie fest. Diese dient als eindeutiger Bezeichner der Kamera innerhalb des Netzwerks.

• Netzwerkmaske

Definiert die Subnetzmaske, die den Bereich der Geräte bestimmt, die direkt mit dem Netzwerk kommunizieren können. Kamera.

• Standardrouter

Legt das Standardgateway für die Weiterleitung des Netzwerkverkehrs über das lokale Subnetz hinaus fest, beispielsweise für den Zugriff auf das Internet oder externe Server.

• Primärer und sekundärer DNS

Konfiguriert DNS-Server so, dass Domännennamen in IP-Adressen aufgelöst werden, wodurch Funktionen wie der Fernzugriff über Hostnamen anstelle von IP-Adressen ermöglicht werden.

• Primärer und sekundärer WINS-Server

Gibt WINS-Server an, um NetBIOS-Namen in IP-Adressen aufzulösen. Dies wird typischerweise in Windows-basierten Umgebungen verwendet, um die Namensauflösung zu erleichtern.

IPv6

Die IPv6-Karte im Tab „Netzwerkeinstellungen“ ermöglicht der Kamera den Betrieb in Netzwerken der nächsten Generation und unterstützt die automatische oder manuelle IP-Adresszuweisung, die Subnetzkonfiguration und die Namensauflösung. Dadurch ist die Kamera für moderne und zukünftige Netzwerkumgebungen gerüstet und bietet verbesserte Konnektivität und Anpassungsfähigkeit.



- IP-Konfiguration**

Ermöglicht dem Benutzer die Auswahl der Zuweisungsmethode für die IPv6-Adresse:

Auto	Erhält automatisch eine IPv6-Adresse mittels SLAAC (Stateless Address Autoconfiguration) oder DHCPv6, abhängig von der Netzwerkkonfiguration.
Handbuch	Ermöglicht bei Bedarf die manuelle Eingabe einer statischen IPv6-Adresse.

- Präfixlänge**

Legt die Subnetzpräfixlänge fest, welche die Größe des Subnetzes und den Adressbereich bestimmt, der direkt mit der Kamera kommunizieren kann. Eine Präfixlänge von 64 ist in IPv6-Konfigurationen üblich.

- Standardrouter**

Konfiguriert das Standardgateway für den ausgehenden Datenverkehr der Kamera zu externen Netzwerken und gewährleistet so die Kommunikation über das lokale IPv6-Subnetz hinaus.

- Primärer DNS**

Ermöglicht dem Benutzer, den primären DNS-Server für die Auflösung von Domännennamen in IPv6-Netzwerke festzulegen.

System

Protokolle

Der Reiter „Protokolle“ dient der Konfiguration verschiedener Kommunikationsprotokolle, die die Interaktion der Kamera mit anderen Geräten, Systemen und Netzwerken ermöglichen. Er enthält fünf wichtige Protokollkarten: HTTP & HTTPS, RTSP, SIP, SNMP und Bonjour. Jede dieser Karten erfüllt spezifische Zwecke für Kommunikation, Streaming und Netzwerkerkennung.

HTTP & HTTPS

Die HTTP- und HTTPS-Karte ist unerlässlich für die Konfiguration eines sicheren und zuverlässigen webbasierten Zugriffs auf die Kamera. Sie bietet die Flexibilität, sowohl verschlüsselte (HTTPS) als auch unverschlüsselte (HTTP) Protokolle zu verwenden, gewährleistet Kompatibilität mit modernen Sicherheitsstandards und unterstützt Redundanz und Anpassungsmöglichkeiten für verschiedene Einsatzszenarien.

The screenshot shows the 'HTTP & HTTPS' configuration panel. It includes the following settings:

- Allow access through:** A dropdown menu set to 'HTTP & HTTPS'.
- Http authentication:** A dropdown menu set to 'Digest'.
- HTTP port:** A text input field containing '80' with a clear button (X).
- Secondary HTTP port:** A toggle switch is turned on (blue). Below it, a text input field contains '8080' with a clear button (X).
- HTTPS port:** A text input field containing '443' with a clear button (X).
- TLS version:** A dropdown menu set to 'TLS v1.2 or v1.3'.
- HTTPS certificate:** A dropdown menu set to 'default certificate'.
- Access name:** A dropdown menu with a downward arrow.

System

- **Zugriff erlauben durch**

Ermöglicht es Benutzern, die Protokolle für den Zugriff auf die Kamera auszuwählen:

HTTP-only	Ermöglicht den Zugriff über das unverschlüsselte HTTP-Protokoll.
Nur HTTPS	Ermöglicht den Zugriff über das verschlüsselte HTTPS-Protokoll.
HTTP & HTTPS	Unterstützt beide Protokolle gleichzeitig für flexible Zugriffsoptionen.

- **HTTP-Authentifizierung**

Konfiguriert die Authentifizierungsmethode für den HTTP-Zugriff:

Basic	Eine einfachere Methode, bei der die Anmeldeinformationen im Klartext übermittelt werden (weniger sicher).
Verdauen	Eine sicherere Methode unter Verwendung gehashter Anmeldeinformationen.

- **HTTP-Port**

Legt den primären Port für die HTTP-Kommunikation fest (Standard: 80).

- **Sekundärer HTTP-Port**

Bietet einen zusätzlichen HTTP-Port (z. B. 8080) für den Zugriff auf die Kamera als Backup oder Alternative.

- **HTTPS-Port**

Legt den Port für die HTTPS-Kommunikation fest (Standard: 443) und gewährleistet so einen verschlüsselten und sicheren Zugriff.

- **TLS-Version**

Bietet Optionen zur Auswahl des Verschlüsselungsprotokolls für HTTPS:

Nur TLS v1.2	Zur Kompatibilität mit älteren Systemen.
Nur TLS v1.3	Für maximale Sicherheit durch Verwendung des neuesten Protokolls.
TLS v1.2 oder v1.3	Bietet Flexibilität, indem beides unterstützt wird.

System

• HTTPS-Zertifikat

Verwaltet das für die HTTPS-Kommunikation verwendete digitale Zertifikat:

• Standardzertifikat

Nutzt das in der Kamera integrierte Zertifikat.

• Zugriffsname

Bietet Optionen zur Anpassung oder Verwaltung des Hostnamens oder der Zugriffs-URL der Kamera und vereinfacht so die Identifizierung und Verbindung.

RTSP

Die RTSP-Karte dient zur Konfiguration der Echtzeit-Video- und Audio-Streaming-Einstellungen der Kamera. Sie ermöglicht die nahtlose Integration mit externen Systemen, den sicheren Zugriff auf Live-Feeds und eine optimierte Netzwerkleistung durch Multicast und Qualitätsüberwachung. Dadurch ist sie eine entscheidende Komponente für den Einsatz der Kamera in professionellen Überwachungs- und Mediumumgebungen.

The screenshot shows a dark-themed configuration window titled "RTSP". It contains several settings:

- Authentication:** A dropdown menu currently set to "Digest".
- RTSP port:** A text input field containing "554" with a clear button (X) to its right.
- RTP video port:** A text input field containing "5556" with a clear button (X) to its right.
- RTP audio port:** A text input field containing "5558" with a clear button (X) to its right.
- RTP metadata port:** A text input field containing "6556" with a clear button (X) to its right.
- Access name:** A label followed by a downward arrow icon.
- RTCP port info:** A label followed by a downward arrow icon.
- Multicast settings:** A label followed by a downward arrow icon.

System

- **Authentifizierung**

Konfiguriert die Authentifizierungsmethode für den RTSP-Zugriff:

Deaktivieren	Deaktiviert die Authentifizierung und ermöglicht so den uneingeschränkten Zugriff auf RTSP-Streams.
Basic	Verwendet Klartext-Anmeldeinformationen zur Authentifizierung (weniger sicher, geeignet für geschlossene Netzwerke).
Verdauen	Verwendet gehashte Anmeldeinformationen zur Authentifizierung und bietet damit eine sicherere Option für offene oder sensible Umgebungen.

- **RTSP-Port**

Legt die Portnummer für die RTSP-Kommunikation fest (Standard: 554). Wird zur Initialisierung von RTSP-Sitzungen zwischen Kamera und Client verwendet.

- **RTP-Videoanschluss**

Legt den Port für die Übertragung von Videostreams fest (Standard: 5556).

- **RTP-Audioanschluss**

Gibt den Port für die Übertragung von Audiostreams an (Standard: 5558).

- **RTP-Metadatenport**

Legt den Port für das Senden von Metadaten (z. B. Zeitstempel oder Ereignisinformationen) zusammen mit den Video- und Audiostreams fest (Standard: 6556).

- **Zugriffsname**

Bietet Optionen zum Konfigurieren oder Anpassen des Zugriffsnamens (URL-Pfad) für RTSP-Streams und vereinfacht so den Zugriff für Drittsysteme oder Benutzer.

- **RTCP-Portinformationen**

Konfiguriert RTCP-Ports (Real-Time Control Protocol), die zur Überwachung der Dienstgüte (QoS) der Streaming-Sitzung und zur Rückmeldung über Probleme wie Paketverlust oder Jitter verwendet werden.

- **Multicast-Einstellungen**

Unterteilt in drei Bereiche: Video, Audio und Metadaten, jeder mit spezifischen Einstellungen.

- **Stream (nur für Video)**

Gibt an, welcher Videostream per Multicast übertragen werden soll (z. B. Stream 1 oder Stream 2).

- **IP-Version**

Ermöglicht die Auswahl von IPv4 oder IPv6 für Multicast-Datenverkehr.

- **Multicast-Adresse**

Weist jedem Stream eine eindeutige Multicast-IP-Adresse zu (z. B. 239.xxx für IPv4 oder FF00::/8 für IPv6).

System

- **Multicast-Port**

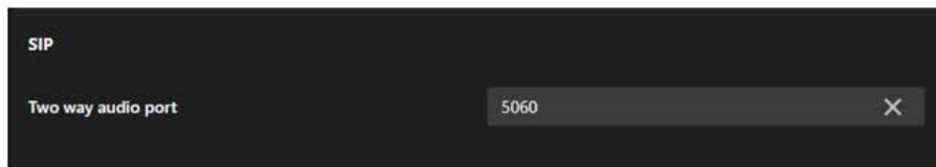
Konfiguriert die Portnummer für Multicast-Streaming (z. B. 5556 für Video, 5558 für Audio).

- **Multicast TTL (Time-to-Live)**

Legt die Anzahl der zulässigen Netzwerk-Hops für Multicast-Pakete fest und steuert so deren Verbreitungsbereich.

SCHLUCK

Die SIP-Karte ist unerlässlich für die Konfiguration der bidirektionalen Audiokommunikationsfunktionen der Kamera über das SIP-Protokoll. Sie ermöglicht die Integration in SIP-basierte Systeme, unterstützt Audiointeraktion in Echtzeit und gewährleistet Flexibilität durch anpassbare Porteneinstellungen. Damit ist sie ein entscheidendes Merkmal für Anwendungen, die interaktive Kommunikation erfordern.



- **Zwei-Wege-Audioanschluss**

Der Zwei-Wege-Audioanschluss konfiguriert den Port (Standard: 5060), der für die SIP-basierte Audiokommunikation verwendet wird, sodass die Kamera Audiostreams senden und empfangen kann, um in Echtzeit mit anderen SIP-kompatiblen Geräten zu interagieren.

SNMP

Dieser Abschnitt erklärt die Verwendung von SNMP auf der Netzwerkkamera. Das Simple Network Management Protocol (SNMP) ist ein Anwendungsschichtprotokoll, das den Austausch von Verwaltungsinformationen zwischen Netzwerkgeräten ermöglicht. Es unterstützt Netzwerkadministratoren bei der Fernverwaltung von Netzwerkgeräten und der einfachen Suche und Behebung von Netzwerkproblemen. SNMP besteht aus den folgenden drei Hauptkomponenten:

- **Manager**

Netzwerkmanagementstation (NMS), ein Server, der Anwendungen ausführt, die verwaltete Geräte überwachen und steuern.

- **Agent**

Ein Softwaremodul der Netzwerkmanagementstation auf einem verwalteten Gerät, das den Status der verwalteten Geräte an das NMS überträgt.

- **Verwaltetes Gerät**

Ein Netzwerkknoten in einem verwalteten Netzwerk. Beispiele hierfür sind: Router, Switches, Bridges, Hubs, Computer-Hosts, Drucker, IP-Telefone, Netzwerkkameras, Webserver und Datenbanken.

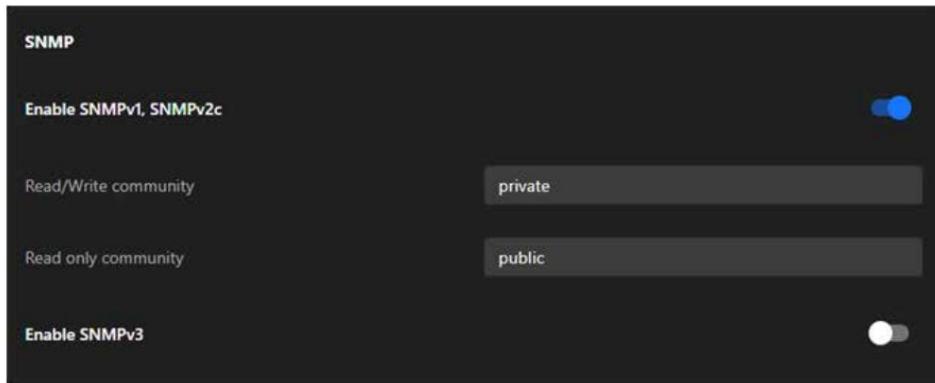
Notiz:

Bevor Sie die SNMP-Einstellungen auf dieser Karte konfigurieren, aktivieren Sie bitte zuerst Ihr NMS.

System

- **SNMPv1 und SNMPv2c aktivieren**

Wählen Sie die Option aus und geben Sie die Namen der Lese-/Schreib-Community und der Nur-Lese-Community entsprechend Ihren NMS-Einstellungen ein.



SNMP

Enable SNMPv1, SNMPv2c ☒

Read/Write community

Read only community

Enable SNMPv3 ☐

- **SNMPv3 aktivieren**

Diese Option beinhaltet kryptografische Sicherheit, ein höheres Sicherheitsniveau, mit dem Sie das Authentifizierungspasswort und das Verschlüsselungspasswort festlegen können.

- **Lese-/Schreibsicherheitsname**

Wählen Sie je nach Ihren NMS-Einstellungen „Lesen/Schreiben“ oder „Nur Lesen“ und geben Sie den Community-Namen ein.

- **Authentifizierungstyp**

Wählen Sie MD5 oder SHA als Authentifizierungsmethode.

- **Authentifizierungspasswort**

Geben Sie das Passwort zur Authentifizierung ein (mindestens 8 Zeichen).

System

• Verschlüsselungspasswort

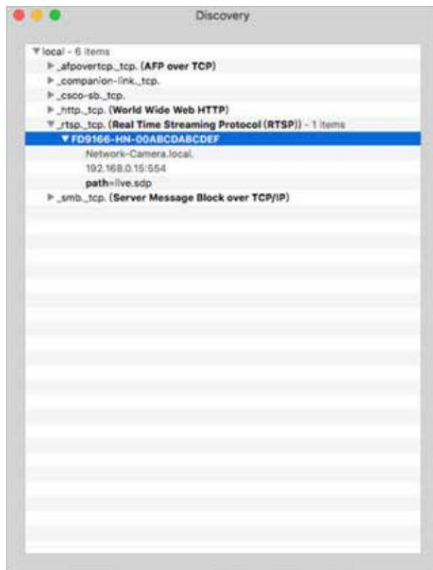
Geben Sie ein Passwort für die Verschlüsselung ein (mindestens 8 Zeichen).

• Guten Morgen

Um von einem MAC-Computer aus auf die Kamera zuzugreifen, öffnen Sie Safari, klicken Sie auf Bonjour und wählen Sie die Kamera aus einer Dropdown-Liste aus.

Unter Safari > Einstellungen können Sie Ihren Benutzernamen und Ihr Passwort eingeben. Geben Sie beim ersten Zugriff auf die Kamera das Root-Passwort ein. Die Hauptseite der Kamera wird in Ihrem Browser geöffnet.

System



• Discovery Utility für Bonjour-Dienste

In einigen neueren iOS-Versionen ist die Bonjour-Option möglicherweise nicht mehr verfügbar. Um dieses Problem zu beheben, können Sie das Discovery-Dienstprogramm verwenden, das als Ersatz für den Bonjour-Browser dient. Gehen Sie wie folgt vor, um loszulegen:

• Installieren Sie Discovery aus dem Mac App Store

Das zuvor als **Bonjour Browser** bekannte , aktualisierte **Discovery-** Dienstprogramm wird nun ausschließlich im Mac App Store vertrieben.

Systemvoraussetzungen: Discovery benötigt macOS 10.12 (Sierra) oder neuer.

<http://www.tildesoft.com/files/BonjourBrowser.dmg>

• Installieren Sie Discovery für iOS

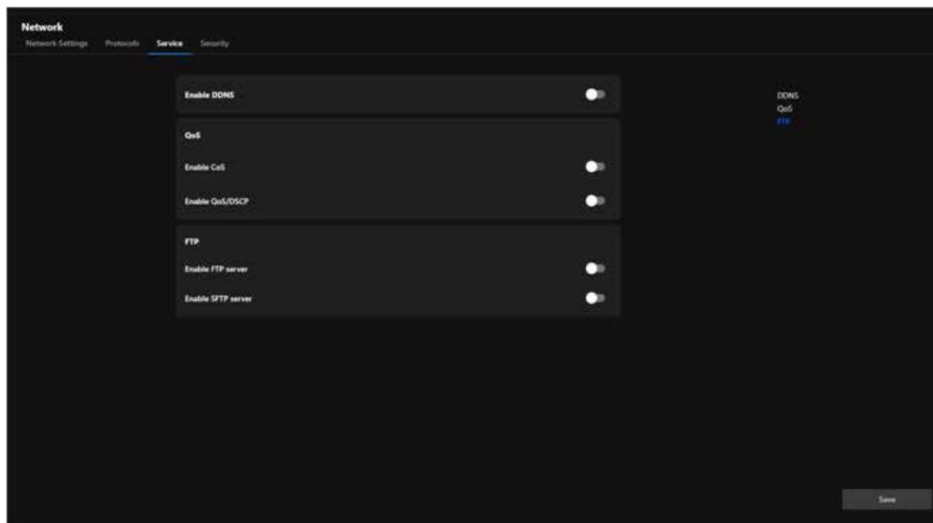
Discovery ist auch für iOS-Geräte verfügbar und kann im App Store heruntergeladen werden.

<https://itunes.apple.com/us/app/discovery-dns-sd-browser/id305441017?mt=8>

System

Service

Der Reiter „Dienste“ bietet wichtige Optionen zur Verwaltung von Netzwerkdiensten. Dazu gehören die Aktivierung des dynamischen Domain Name Systems (DDNS) für einen reibungslosen Fernzugriff auch mit dynamischen IP-Adressen, die Konfiguration von Quality-of-Service-Einstellungen (QoS) zur Priorisierung des Kameradatenverkehrs im Netzwerk sowie die Aktivierung von FTP- oder SFTP-Servern für eine sichere und effiziente Dateiübertragung. Diese Funktionen gewährleisten zuverlässige Verbindungen, erhöhte Datensicherheit und verbesserte Leistung und erfüllen so vielfältige Überwachungsanforderungen.



System

● DDNS

Die Karte integriert sich in DDNS-Dienste von Drittanbietern, um den mit der Kamera verknüpften Domainnamen dynamisch zu aktualisieren, sobald sich deren IP-Adresse ändert. Benutzer benötigen gültige Zugangsdaten und einen bei ihrem DDNS-Anbieter registrierten Hostnamen, um diese Funktion nutzen zu können. Der Unterschied zwischen den Anbietermodi „Dynamisch“ und „Benutzerdefiniert“ ermöglicht Flexibilität je nach DDNS-Tarif oder Anbietervorgaben des Benutzers.

DDNS aktivieren:

Ermöglicht dem Benutzer, die DDNS-Funktionalität zu aktivieren oder zu deaktivieren.

Anbieter:

Über ein Dropdown-Menü können Benutzer den DDNS-Dienstanbieter auswählen, beispielsweise mit Optionen wie „Dyndns.org (Dynamic)“ oder „Dyndns.org (Custom)“. Der ausgewählte Anbieter bestimmt, wie Hostname und Anmeldeinformationen für die DDNS-Verbindung konfiguriert werden.

Hostname:

Es gibt ein Eingabefeld, in dem der eindeutige Hostname angegeben werden kann, der beim ausgewählten DDNS-Anbieter registriert ist (z. B. yourcamera.dyndns.org). Dieser wird für den Fernzugriff auf die Kamera verwendet.

Benutzername:

Eingabefeld für den vom DDNS-Anbieter benötigten Benutzernamen.

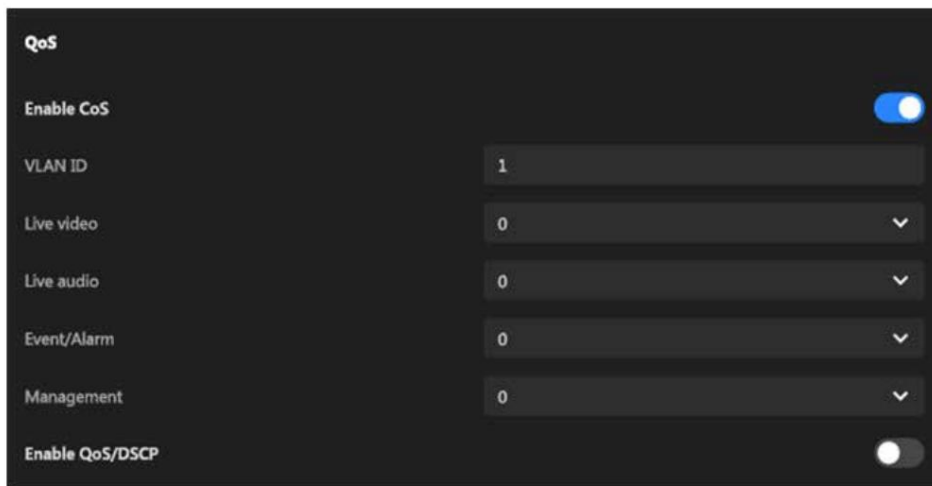
Passwort:

Eingabefeld für das Passwort des DDNS-Kontos. Ein verstecktes Feld gewährleistet die Vertraulichkeit bei der Eingabe.

System

• QoS

Die QoS-Karte ermöglicht es Benutzern, die Priorität verschiedener Datenströme flexibel an die Anforderungen der Netzwerkkumgebung anzupassen. Bei aktiviertem CoS ist die Integration mit VLANs möglich, wodurch sich die Karte für Ethernet-Netzwerke eignet. Die Aktivierung von QoS/DSCP ist hingegen besser für IP-Netzwerke geeignet. Diese Einstellungen tragen zur Verbesserung der Zuverlässigkeit und Effizienz der Kameradatenübertragung bei, was insbesondere dann entscheidend ist, wenn mehrere Geräte dasselbe Netzwerk nutzen.



QoS	
Enable CoS	☒
VLAN ID	1
Live video	0
Live audio	0
Event/Alarm	0
Management	0
Enable QoS/DSCP	☐

CoS (Class of Service) aktivieren:

Ein Kippschalter zum Aktivieren oder Deaktivieren der CoS-Funktionalität.

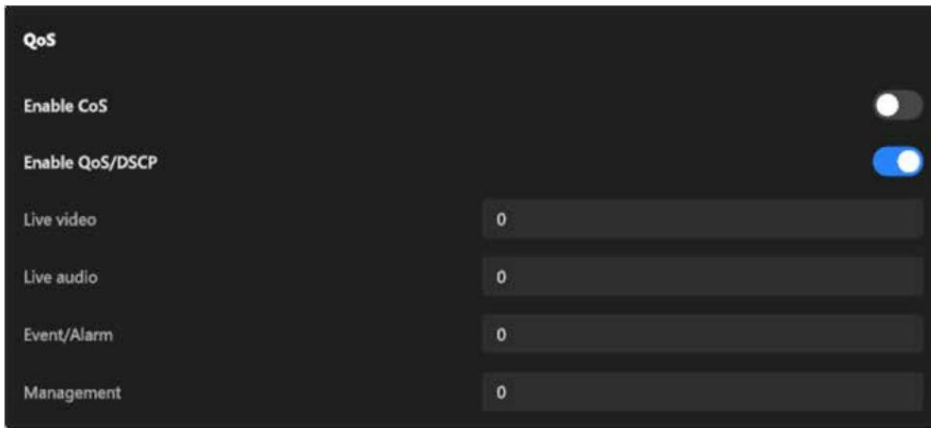
VLAN-ID:

Gibt das VLAN-Tag zur Identifizierung des virtuellen LANs an, zu dem die Kamera gehört.

System

Prioritätseinstellungen für jeden Datentyp (Live-Video, Live-Audio, Ereignis/Alarm, Verwaltung):

Jedem Datentyp (Live-Video, Live-Audio, Ereignis/Alarm, Management) kann über ein Dropdown-Menü von 0 bis 7 eine Prioritätsstufe zugewiesen werden, wobei höhere Zahlen eine höhere Übertragungspriorität bedeuten. Dies ermöglicht eine präzise Steuerung des Datenverkehrs innerhalb eines Ethernet-Netzwerks.



QoS	
Enable CoS	☐
Enable QoS/DSCP	☒
Live video	0
Live audio	0
Event/Alarm	0
Management	0

QoS/DSCP (Differentiated Services Code Point) aktivieren:

Ein Kippschalter zum Aktivieren oder Deaktivieren der DSCP-Funktionalität.

DSCP-Werte für jeden Datentyp (Live-Video, Live-Audio, Ereignis/Alarm, Management):

Benutzer können für jeden Datentyp (Live-Video, Live-Audio, Ereignis/Alarm, Management) einen DSCP-Wert konfigurieren. Diese Werte bestimmen die Priorität der Daten in IP-Netzwerken und gewährleisten so eine korrekte Verkehrsklassifizierung und effizientes Routing.

System

• FTP

Die FTP-Karte bietet die Flexibilität, je nach Betriebs- und Sicherheitsanforderungen des Nutzers FTP für einfache und effiziente Dateiübertragungen oder SFTP für sichere, verschlüsselte Übertragungen zu verwenden. Die konfigurierbare Portkonfiguration gewährleistet Kompatibilität mit verschiedenen Netzwerkkonfigurationen. Host-Schlüssel in SFTP erhöhen zusätzlich Vertrauen und Sicherheit bei der Client-Server-Kommunikation. Diese Funktionalität ist besonders nützlich für die automatisierte Speicherung oder Sicherung von Überwachungsdaten an entfernten Standorten.

FTP

Enable FTP server ☒

FTP port 21

Enable SFTP server ☒

SFTP port 22

Host Key

MD5:c8:c1:dd:55:83:87:65:ce:98:57:f8:92:f5:c3:ef:91 (RSA)
MD5:dc38:05:d5:67:4f:58:c3:ed:32:ae:52:89:3d:d5:96 (ED25519)

FTP-Server aktivieren:

Ein Kippschalter zum Aktivieren oder Deaktivieren der FTP-Serverfunktionalität.

FTP-Port:

Legt den für den FTP-Dienst verwendeten Port fest (Standardwert ist 21). Benutzer können diesen Wert an ihre Netzwerk- oder Sicherheitsanforderungen anpassen.

SFTP-Server aktivieren:

Ein Kippschalter zum Aktivieren oder Deaktivieren der SFTP-Serverfunktionalität.

SFTP-Port:

Legt den für den SFTP-Dienst verwendeten Port fest (Standard ist 22). Benutzer können diesen Port bei Bedarf ändern, um Konflikte zu vermeiden oder bestimmte Sicherheitsrichtlinien einzuhalten.

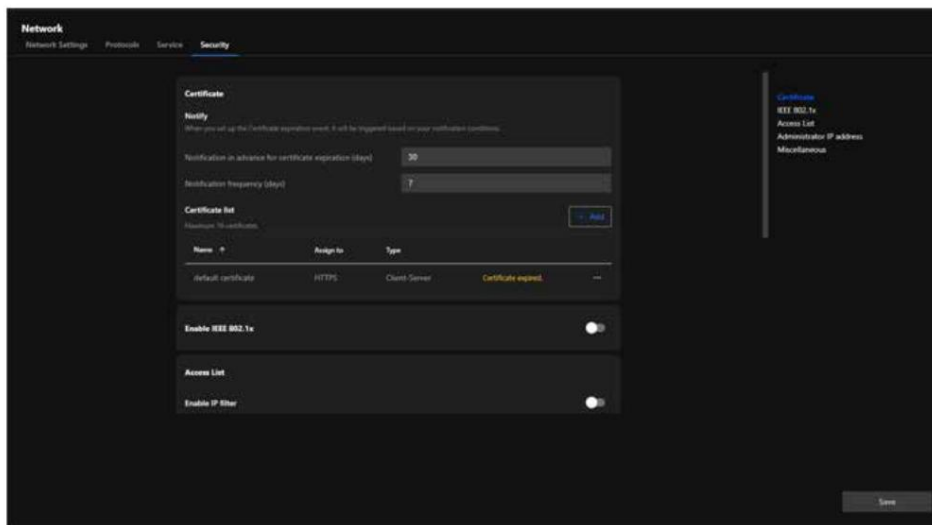
Host-

Schlüssel: Zeigt die Host-Schlüsselinformationen des Servers an, einschließlich Hash-Werte (z. B. RSA- und ED25519-Schlüssel). Diese Schlüssel werden zur Authentifizierung des Servers und zur Gewährleistung sicherer Verbindungen zwischen Client und Server verwendet.

System

Sicherheit

Der Reiter „Sicherheit“ bietet umfassende Optionen zur Verbesserung der Netzwerksicherheit. Benutzer können Zertifikate für verschlüsselte Kommunikation verwalten, die Zugriffskontrolle mittels IP-Filterung und IEEE 802.1x-Authentifizierung implementieren und den administrativen Zugriff auf bestimmte IP-Adressen beschränken. Durch die Nutzung dieser Funktionen gewährleisten Benutzer eine sichere Datenübertragung, verhindern unbefugten Zugriff und schützen die Kamera in einfachen wie komplexen Netzwerkumgebungen. Dieser Reiter wurde entwickelt, um die Sicherheitsanforderungen moderner Überwachungssysteme zu erfüllen und einen zuverlässigen Schutz vor potenziellen Bedrohungen zu bieten.



Zertifikat

Die Zertifikatskarte bietet eine robuste und zentrale Lösung für die Zertifikatsverwaltung. Durch die Unterstützung von HTTPS-Verschlüsselung gewährleistet sie eine sichere Kommunikation zwischen Kamera und externen Systemen und schützt Daten vor Abhören und Manipulation. Die Benachrichtigungsfunktion informiert Benutzer über abgelaufene Zertifikate und hilft so, damit verbundene Risiken zu minimieren. Die Möglichkeit, mehrere Zertifikate zu verwalten, bietet Flexibilität für verschiedene Netzwerkkonfigurationen und -anforderungen.

System

Zertifikat

Certificate

Notify
When you set up the Certificate expiration event, it will be triggered based on your notification conditions.

Notification in advance for certificate expiration (days)

Notification frequency (days)

Certificate list
Maximum 16 certificate [+ Add](#)

Name	Assign to	Type	
Default	HTTPS	Client server	...

Benachrichtigung: Konfiguriert die Benachrichtigungseinstellungen für

den Ablauf des Zertifikats. • **Benachrichtigung im Voraus für den Ablauf des Zertifikats (Tage):**

Legt fest, wie viele Tage vor Ablauf der Gültigkeit das System eine Benachrichtigung versendet.

• **Benachrichtigungshäufigkeit (Tage):**

Legt die Häufigkeit wiederholter Benachrichtigungen fest.

Zertifikatsliste:

Unterstützt die Verwaltung von bis zu 16 Zertifikaten und zeigt detaillierte Informationen zu jedem Zertifikat an, einschließlich:

• **Name:**

Der Name des Zertifikats.

• **Zuweisen an:**

Die Anwendung oder das Protokoll, dem das Zertifikat zugeordnet ist (z. B. HTTPS). • **Typ:** Der Zweck

des Zertifikats (z. B. Client-Server).

• **Zeigt den aktuellen Status jedes Zertifikats an, z. B. „Zertifikat abgelaufen“.**

System

- Schritte zum Hinzufügen eines Zertifikats:

Add certificate

Client certificate

 **Create self-signed certificate**
Signed by the camera itself.

 **Create a certificate request and install**
Camera generates a certificate request. Applies to a CA to obtain a certificate file, and then uploads it to the camera.

 **Upload a certificate and private key**
Using existing certificate and private key.

CA certificate

 **Upload a CA certificate**
Using existing CA certificate

Continue

System

- Schritte zum Hinzufügen eines

Zertifikats: Option 1. Erstellen Sie ein selbstsigniertes Zertifikat für das Clientzertifikat.

- **Schritt 1. Klicken Sie auf die Schaltfläche „+Hinzufügen“.** Daraufhin öffnet sich das Fenster

„Zertifikat hinzufügen“. • **Schritt 2. Wählen Sie**

„Selbstsigniertes Zertifikat erstellen“. • **Schritt 3. Füllen Sie die erforderlichen Felder aus, einschließlich:**

Name: Geben Sie einen Namen für das Zertifikat ein (z. B. „Zertifikat 01“).

Zertifikatsland: Geben Sie den Ländercode an (z. B. „TW“).

Bundesland oder Provinz und Ort: Geben Sie den Ort an (z. B. „Asien“).

Organisation und Organisationseinheit: Geben Sie die Organisationsdetails ein.

Allgemeiner Name: Geben Sie den Domainnamen an (z. B. „www.vivotek.com“).

Gültigkeit: Geben Sie den Gültigkeitszeitraum in Tagen an (z. B. „397“). •

- **Schritt 4: Klicken Sie auf „Erstellen“, um die Zertifikatserstellung zu starten.** •

Schritt 5: Die Meldung „Erfolgreich generiert“ bedeutet, dass der Vorgang abgeschlossen ist.

The screenshot shows a dark-themed dialog box titled "Create certificate" with a close button (X) in the top right corner. Below the title is the subtitle "Create self-signed certificate". The form contains the following fields:

- Name:** A text input field containing "Cert 01".
- Certificate country:** A text input field containing "TW".
- State or province:** A text input field containing "Asia".
- Locality:** A text input field containing "Asia".
- Organization:** A text input field containing "VIVOTEK Inc."
- Organization unit:** A text input field containing "VIVOTEK Inc."
- Common name:** A text input field containing "www.vivotek.com".
- Validity:** A text input field containing "397".

At the bottom of the dialog, there are two buttons: "Back" on the left and "Create" on the right.

System

- Schritte zum Hinzufügen eines Zertifikats:

Option 2. Erstellen Sie eine Zertifikatsanforderung und installieren Sie das Clientzertifikat.

- Schritt 1. Klicken Sie auf die Schaltfläche „+Hinzufügen“. Daraufhin öffnet sich das Fenster „Zertifikat hinzufügen“.
- Schritt 2. Wählen Sie „Zertifikatsanforderung erstellen und installieren“.
- Schritt 3. Füllen Sie die erforderlichen Felder analog zum selbstsignierten Zertifikat aus (Name, Ort, Organisation, Gebräuchlicher Name).
- Schritt 4. Klicken Sie auf „Erstellen“, um die Zertifikatsgenerierung zu starten.
- Schritt 5. Eine Meldung mit dem Hinweis „Erfolgreich hochgeladen“ bedeutet, dass die Zertifikatsanforderung generiert wurde. erfolgreich.
- Schritt 6. Klicken Sie auf die Schaltfläche „Zertifikatsanforderung kopieren“, um die Details der Zertifikatsanforderung (CSR) zu kopieren.
- Schritt 7. Verwenden Sie den kopierten CSR, um ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle zu beantragen, die Ihnen dann einen CSR ausstellt. signierte Zertifikatsdatei (z. B. a.crt-Datei).
- Schritt 8. Nachdem Sie das signierte Zertifikat von der Zertifizierungsstelle erhalten haben, kehren Sie zum selben Fenster zurück, klicken Sie auf Datei hochladen und wählen Sie die von der Zertifizierungsstelle bereitgestellte .crt-Datei aus.
- Schritt 9. Klicken Sie auf Erstellen, um die Installation des Zertifikats abzuschließen.
- Schritt 10. Eine Meldung mit dem Hinweis „Erfolgreich hochgeladen“ bedeutet, dass der Vorgang abgeschlossen ist.

Create certificate ✕

Create a certificate request and install

Name
Cert 02

Certificate country
TW

State or province
Asia

Locality
Asia

Organization
VIVOTEK Inc.

Organization unit
VIVOTEK Inc.

Common name
www.vivotek.com

Back Create

System

- Schritte zum Hinzufügen eines

Zertifikats: Option 3: Zertifikat und privaten Schlüssel für das Client-Zertifikat hochladen. • Schritt 1:

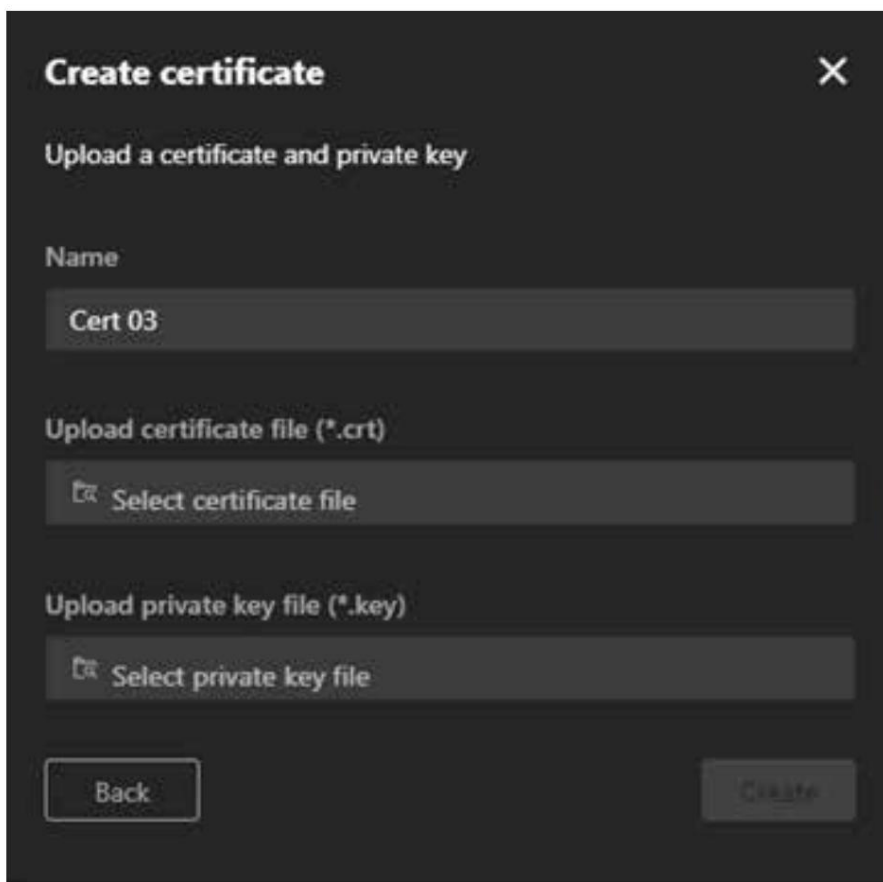
Klicken Sie auf „+Hinzufügen“. Das Fenster „Zertifikat hinzufügen“ wird angezeigt. • Schritt 2: Wählen Sie

„Zertifikat und privaten Schlüssel hochladen“. • Schritt 3: Geben Sie den

Zertifikatsnamen ein (z. B. „Cert 03“). • Schritt 4: Verwenden Sie die

Optionen „Zertifikatdatei hochladen (*.cert)“ und „Private-Key-Datei hochladen (*.key)“, um die Zertifikate und den privaten Schlüssel hochzuladen.
jeweilige Dateien.

• Schritt 5. Klicken Sie auf Erstellen, um das Zertifikat hinzuzufügen.



The image shows a dark-themed dialog box titled "Create certificate" with a close button (X) in the top right corner. The main heading inside is "Upload a certificate and private key". Below this, there is a "Name" label followed by a text input field containing "Cert 03". Underneath, there are two file upload sections: "Upload certificate file (*.cert)" with a button labeled "Select certificate file", and "Upload private key file (*.key)" with a button labeled "Select private key file". At the bottom of the dialog, there are two buttons: "Back" on the left and "Create" on the right.

System

- Schritte zum Hinzufügen eines

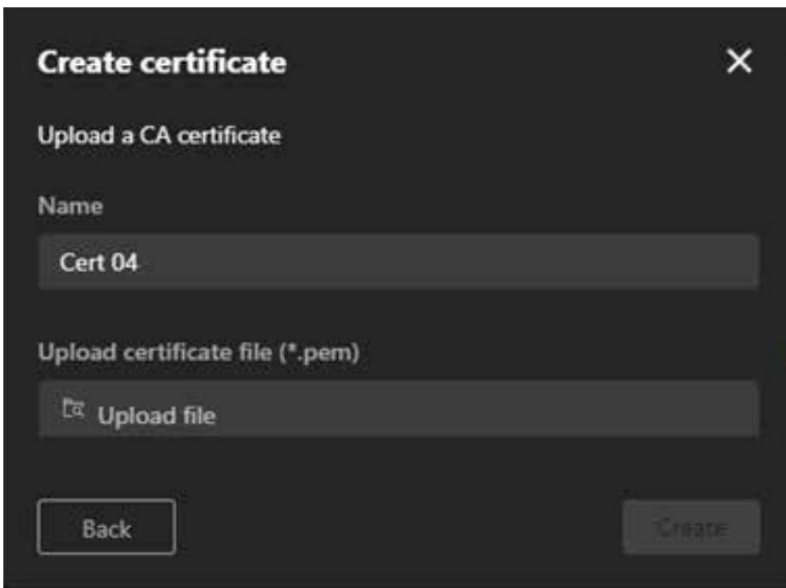
Zertifikats: Option 4: Hochladen eines CA-Zertifikats für die CA-

Zertifizierung • Schritt 1: Klicken Sie auf die Schaltfläche „+Hinzufügen“. Das Fenster „Zertifikat hinzufügen“ wird angezeigt. • Schritt 2: Wählen

Sie „CA-Zertifikat hochladen“. • Schritt 3: Geben Sie den

Zertifikatsnamen ein (z. B. „Cert 04“). • Schritt 4: Verwenden Sie die Option „Zertifikatdatei hochladen

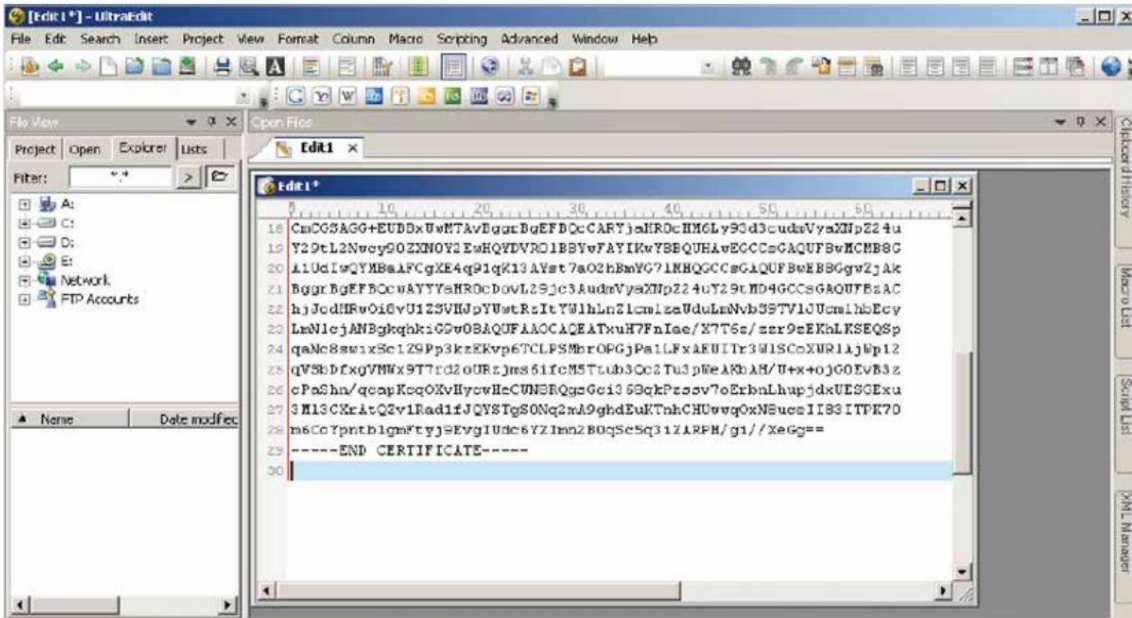
(*.pem)“, um das CA-Zertifikat hochzuladen. • Schritt 5: Klicken Sie auf „Erstellen“, um den Vorgang abzuschließen.



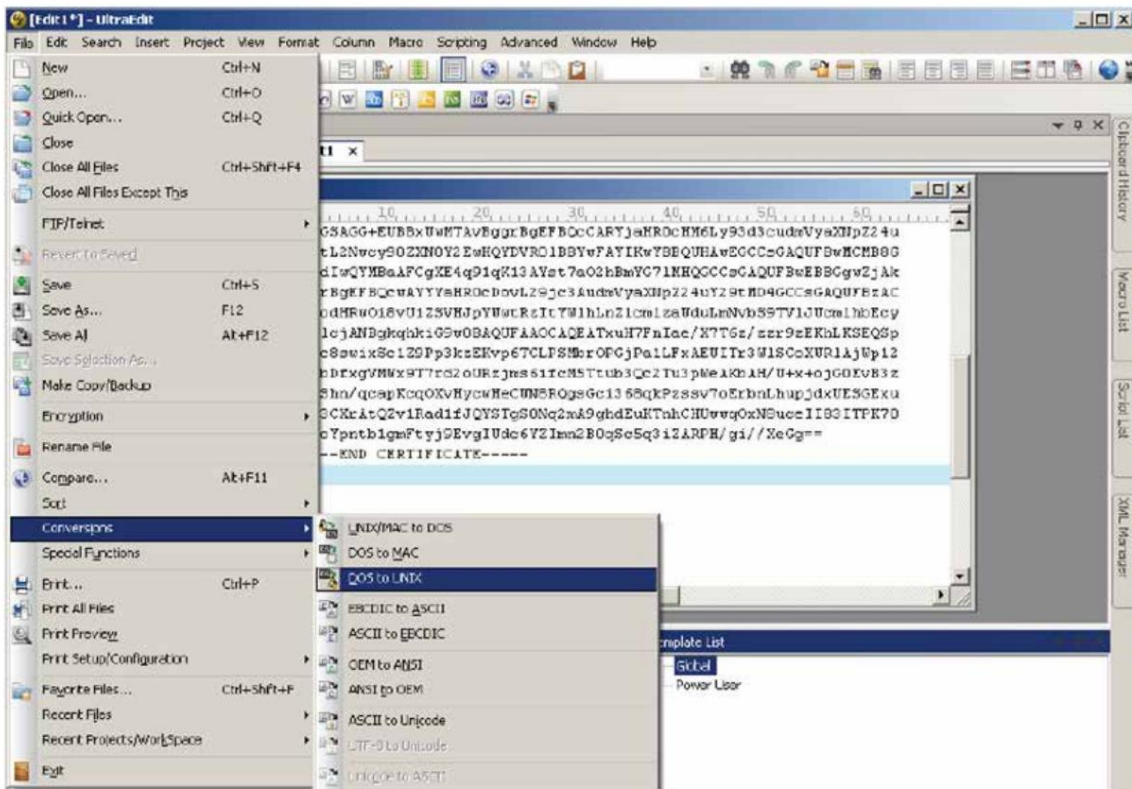
The screenshot shows a dark-themed dialog box titled "Create certificate" with a close button (X) in the top right corner. Below the title, the section "Upload a CA certificate" is active. It contains a "Name" label followed by a text input field containing "Cert 04". Below this is the label "Upload certificate file (*.pem)" followed by a file upload button with a folder icon and the text "Upload file". At the bottom left is a "Back" button, and at the bottom right is a "CREATE" button.

System

- Schritt 3. Öffnen Sie eine neue Bearbeitung, fügen Sie den Zertifikatsinhalt ein und drücken Sie am Ende des Inhalts die Eingabetaste, um eine leere Zeile einzufügen.

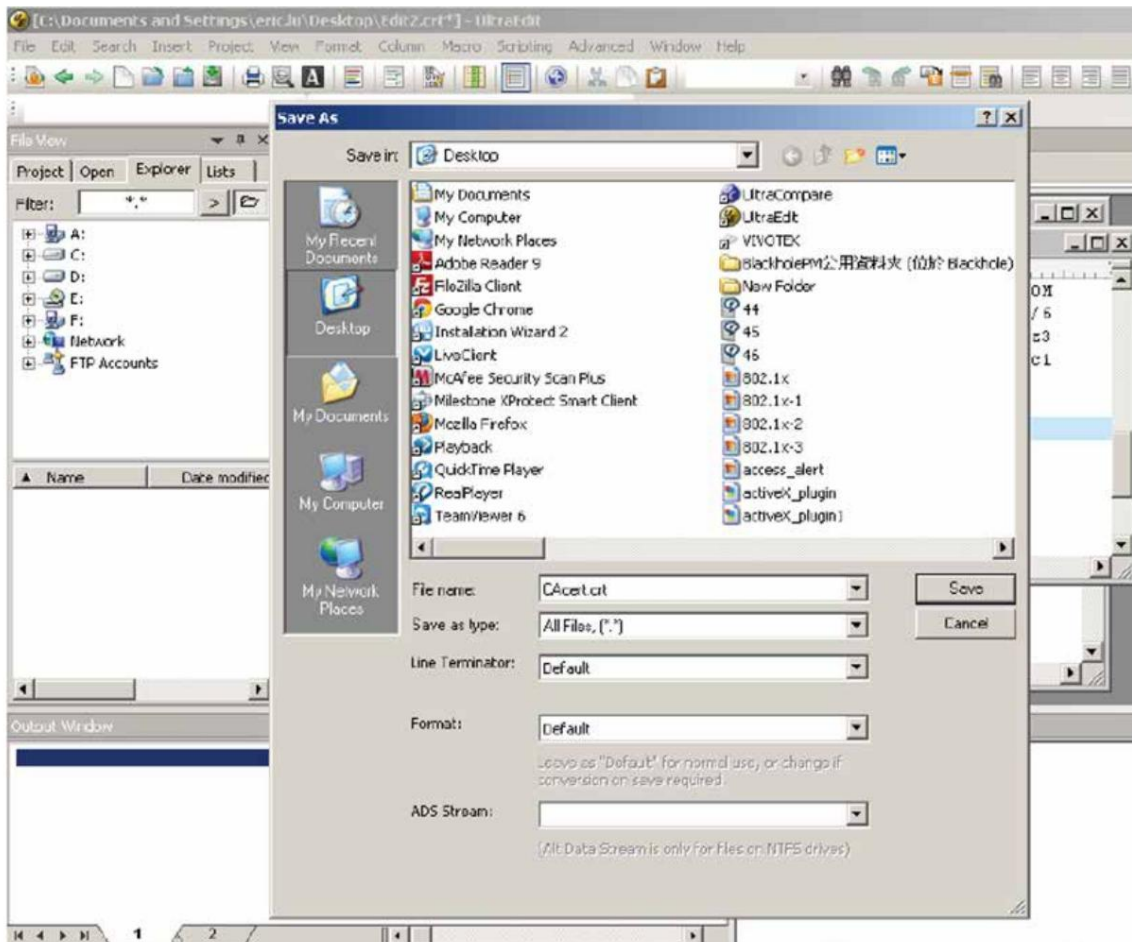


- Schritt 4. Dateiformat von DOS in UNIX konvertieren. Menü „Datei“ öffnen > Konvertierungen > DOS zu Unix.

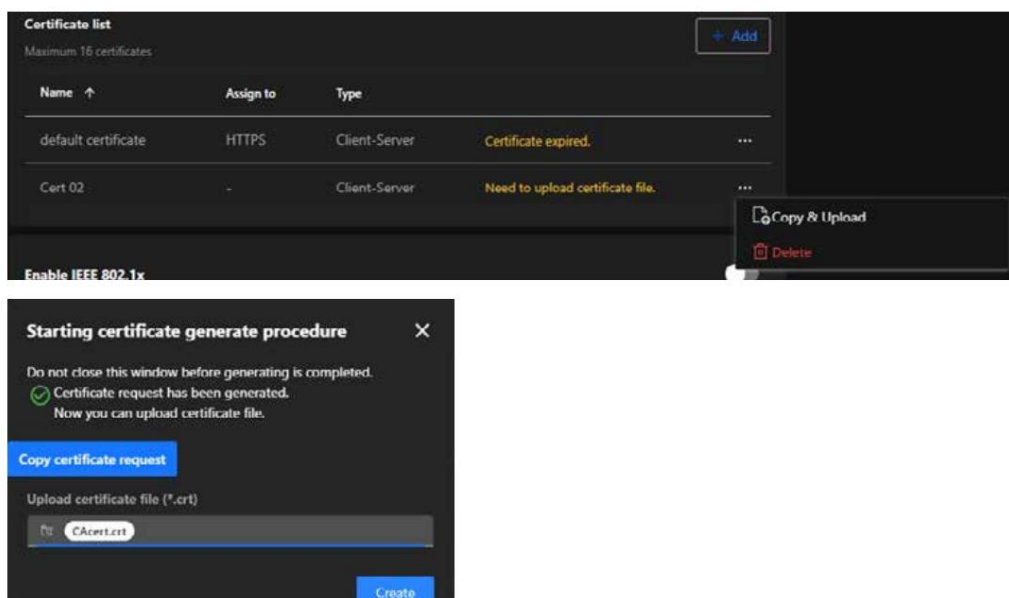


System

- Schritt 5. Speichern Sie die Änderung mit der Dateieindung „.crt“ und einem Dateinamen wie „CAcert.crt“.



- Schritt 6. Kehren Sie zur ursprünglichen Firmware-Sitzung zurück, verwenden Sie das Symbol „Mehr“ > Schaltfläche „Kopieren & Hochladen“, um die CRT-Zertifikatsdatei zu finden, und klicken Sie auf Erstellen, um die Zertifizierung zu aktivieren.



System

LED & DIDO

Aktivieren Sie diese Funktion, wenn Ihre Netzwerkumgebung IEEE 802.1x verwendet, eine portbasierte Netzwerkzugriffskontrolle. Die Netzwerkgeräte, der zwischengeschaltete Switch/Access Point/Hub und der RADIUS-Server müssen 802.1x unterstützen und die Einstellungen aktivieren.

Der 802.1x-Standard dient der Erhöhung der Sicherheit lokaler Netzwerke und ermöglicht die Authentifizierung von Netzwerkgeräten (Clients), die an einen Netzwerkanschluss (kabelgebunden oder drahtlos) angeschlossen sind. Werden alle Zertifikate zwischen Client und Server verifiziert, wird eine Punkt-zu-Punkt-Verbindung hergestellt; schlägt die Authentifizierung fehl, wird der Zugriff über diesen Port gesperrt. 802.1x nutzt das bestehende Protokoll Extensible Authentication Protocol (EAP) zur Kommunikation.

Die Komponenten eines geschützten Netzwerks mit 802.1x-Authentifizierung:



- **Sie bitten:**

Ein Client-Endbenutzer (Kamera), der eine Authentifizierung anfordert.

- **Authentifikator (ein Zugriffspunkt oder ein Schalter):**

Ein „Vermittler“, der nicht autorisierte Endbenutzer daran hindert, mit dem Authentifizierungsdienst zu kommunizieren. Ist.

- **Authentifizierungsserver (in der Regel ein RADIUS-Server):**

Prüft das Clientzertifikat und entscheidet, ob die Zugriffsanfrage des Endbenutzers akzeptiert wird.

Netzwerkcameras unterstützen zwei EAP-Authentifizierungsmethoden: **EAP-PEAP** und **EAP-TLS**. Bitte führen Sie die folgenden Schritte aus, um die 802.1x-Einstellungen zu aktivieren:

- **Schritt 1. Bevor Sie die Netzwerkkamera mit dem geschützten Netzwerk nach 802.1x verbinden, wenden Sie bitte ein digitales Zertifikat einer Zertifizierungsstelle (z. B. Ihres Netzwerkadministrators) an, das von einem RADIUS-Server validiert werden kann.**

System

- **Schritt 2.** Schließen Sie die Netzwerkkamera an einen PC oder ein Notebook außerhalb des geschützten LANs an. Öffnen Sie die Konfigurationsseite der Netzwerkkamera wird wie unten dargestellt angezeigt. Wählen Sie EAP-PEAP oder EAP-TLS als EAP-Methode. Geben Sie in den folgenden Feldern Ihre von der Zertifizierungsstelle ausgestellte ID und Ihr Passwort ein und laden Sie anschließend die zugehörigen Zertifikate hoch.

The image shows two screenshots of a web-based configuration interface for a network camera. The top screenshot is titled 'IEEE 802.1x' and has a toggle switch turned on. It contains the following fields: 'EAP method' set to 'EAP-PEAP', 'Identity' with a text input 'Enter identity', 'Password' with a text input 'Enter password' and a password icon, and 'CA certificat' with a dropdown menu 'Select one certificate'. The bottom screenshot is titled 'Enable IEEE 802.1x' and also has a toggle switch turned on. It contains: 'EAP method' set to 'EAP-TLS', 'Identity' with a text input 'Enter identity', 'Upload CA certificate file (.crt)' with a dropdown menu 'Select one certificate', and 'Upload client certificate file (.crt)' with a dropdown menu 'Select one certificate'.

- **Schritt 3.** Sobald alle Einstellungen abgeschlossen sind, verbinden Sie die Netzwerkkamera mit einem 802.1x-fähigen Switch im geschützten LAN. Die Geräte starten dann automatisch die Authentifizierung.

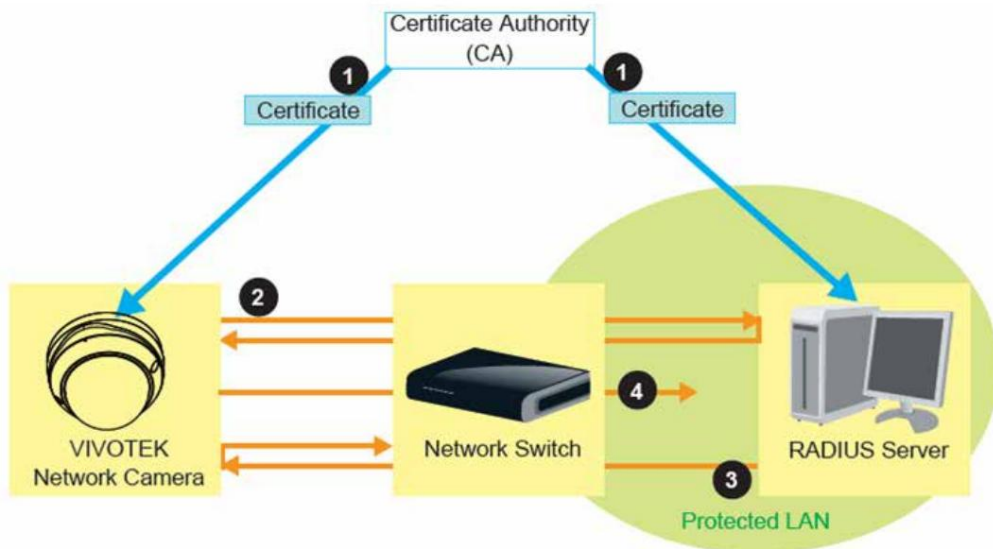
- **Notiz:**

Der Authentifizierungsprozess für 802.1x:

- **Schritt 1.** Die Zertifizierungsstelle (CA) stellt die erforderlichen signierten Zertifikate für die Netzwerkkamera bereit. (der Bittsteller) und der RADIUS-Server (der Authentifizierungsserver).
- **Schritt 2.** Eine Netzwerkkamera fordert über einen Switch (den 802.1X-Switch) Zugriff auf das geschützte LAN an. Der Client übermittelt seine Identität und sein Clientzertifikat, die dann vom Switch an den RADIUS-Server weitergeleitet werden. Dieser verwendet einen Algorithmus zur Authentifizierung der Netzwerkkamera und sendet eine Bestätigung oder Ablehnung an den Switch zurück.
- **Schritt 3.** Der Switch leitet außerdem das Zertifikat des RADIUS-Servers an die Netzwerkkamera weiter.

System

- Schritt 4. Unter der Annahme, dass alle Zertifikate validiert wurden, ändert der Switch anschließend den Zustand der Netzwerkkamera. autorisiert und hat über einen vorkonfigurierten Port Zugriff auf das geschützte Netzwerk.



Zugriffsliste

Diese Funktion ist besonders nützlich in Umgebungen, in denen die Kamera einem größeren Netzwerk oder dem Internet ausgesetzt ist, da sie sicherstellt, dass nur vertrauenswürdige Geräte oder Netzwerke Zugriff haben.

Access List

Enable IP filter ☒

Policy ☐ Allow ☒ Deny

IP address

Maximum 10 IP address

IPv4

255.255.255.255

192.168.0.1/24

255.168.0.1-255.168.0.255

System

- **IP-Filter aktivieren**

Ein Kippschalter zum Aktivieren oder Deaktivieren der IP-Filterfunktion.

- **Politik**

Erlauben:

Nur den angegebenen IP-Adressen wird der Zugriff auf die Kamera gestattet. Alle anderen IP-Adressen werden gesperrt.

Verweigern: Blockiert den Zugriff der angegebenen IP-Adressen auf die Kamera. Alle anderen IP-Adressen sind zugelassen.

- **IP-Adresse**

Ein Abschnitt zur Definition von bis zu 10 IP-Adressen oder -Bereichen, deren Zugriff je nach der ausgewählten Richtlinie entweder erlaubt oder verweigert wird.

- **IPv4-Liste**

Zeigt die Liste der konfigurierten IP-Adressen oder -Bereiche an. Einträge können über das Papierkorbsymbol neben der jeweiligen Adresse entfernt werden. Jeder Eintrag kann Folgendes darstellen: Eine einzelne IP-

Adresse (z. B. 192.168.0.1).

Eine Netzwerk-IP-Adresse (z. B. 192.168.0.1/24).

Ein bestimmter IP-Adressbereich (z. B. 255.168.0.1-255.168.0.255).

Schritte zum Hinzufügen einer IP-Adresse zur Zugriffsliste:

Schritt 1. Klicken Sie auf die Schaltfläche „+Hinzufügen“, um das Fenster „IP-Adresse

hinzufügen“ zu öffnen. **Schritt 2.** Wählen Sie im Dropdown-Menü „IP-Typ“ den gewünschten Typ aus:

IPv4: Für Standard-IPv4-Adressen oder -Bereiche.

Schritt 3. Wählen Sie im Dropdown-Menü „Regel“ eine der folgenden Optionen aus:

Einzeln: Eine einzelne IP-Adresse zulassen oder verweigern.

Netzwerk: Den Zugriff für ein gesamtes Subnetz erlauben oder verweigern.

IP-Adressbereich: Zur Definition eines bestimmten IP-Adressbereichs.

Schritt 4. Geben Sie die IP-Adresse ein:

Geben Sie basierend auf der ausgewählten Regel die entsprechenden Details im Feld IP-Adresse ein: Für

Einzeln: Geben Sie eine IP-Adresse ein (z. B. 192.168.0.10).

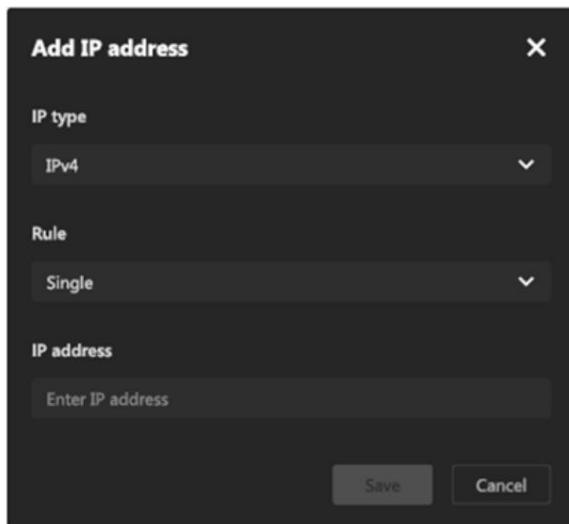
Für Netzwerk: Geben Sie eine IP-Adresse und ihre Subnetzmaske ein.

Für den IP-Bereich: Geben Sie die Start- und End-IP-Adresse ein.

Schritt 5. Klicken Sie auf Speichern, um die IP-Adresse oder den IP-Adressbereich zur Zugriffsliste hinzuzufügen.

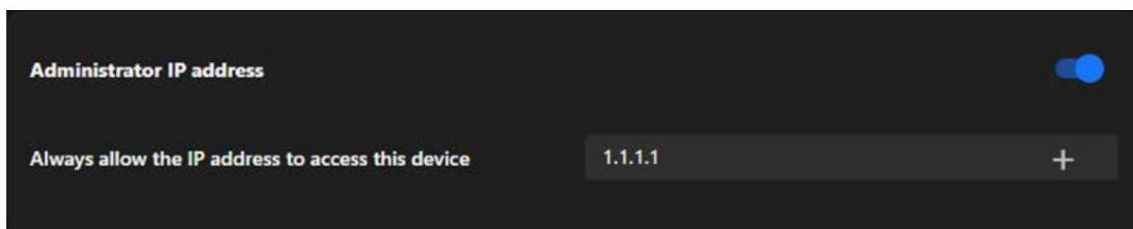
System

Schritt 6. Der neue Eintrag wird nun im IPv4-Abschnitt der Zugriffsliste angezeigt.



Administrator-IP-Adresse

Die Administrator-IP-Adresse bietet eine einfache und dennoch effektive Möglichkeit, den administrativen Zugriff zu sichern und gleichzeitig zu gewährleisten, dass autorisiertes Personal das Gerät auch in komplexen oder eingeschränkten Netzwerkkumgebungen jederzeit verwalten kann.



- **Gewähren Sie der IP-Adresse immer den Zugriff auf dieses Gerät:**

Sie können dieses Element aktivieren und die IP-Adresse des Administrators in dieses Feld eintragen, um sicherzustellen, dass der Administrator jederzeit eine Verbindung zum Gerät herstellen kann.

Schritte zum Festlegen der Administrator-IP-Adresse:

Schritt 1. Geben Sie die vertrauenswürdige IP-Adresse ein:

Geben Sie die IP-Adresse ein, die stets über Administratorzugriff verfügen soll.

Schritt 2. Aktivieren Sie die Funktion:

Schalten Sie den Kippschalter ein, um die Einstellung zu aktivieren.

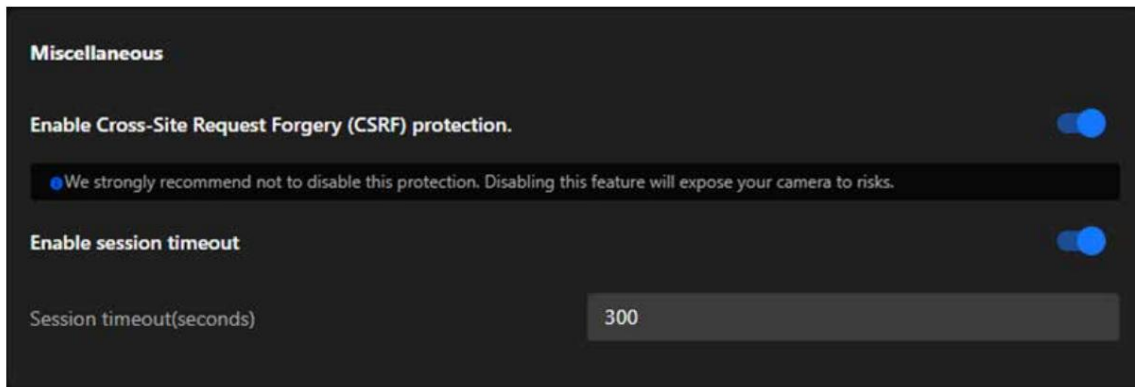
Schritt 3. Änderungen speichern:

Stellen Sie sicher, dass die Konfiguration gespeichert wird, damit die Einstellung wirksam wird.

System

Verschiedenes

Die Option „**Sonstiges**“ in den Einstellungen der VIVOTEK-Kamera bietet zusätzliche Sicherheitsoptionen zur Verbesserung der Sicherheit und Benutzerfreundlichkeit des Geräts. Sie konzentriert sich auf den Schutz vor Cross-Site-Request-Forgery-Angriffen (CSRF) und die Verwaltung von Sitzungs-Timeouts für Benutzerkonten.



- **Cross-Site Request Forgery (CSRF)-Schutz aktivieren:**

Verhindert, dass unautorisierte Befehle von einer bössartigen Website im Namen eines authentifizierten Benutzers an die Kamera gesendet werden.

Notiz:

Es wird dringend davon abgeraten, diese Funktion zu deaktivieren, da die Deaktivierung die Kamera erheblichen Sicherheitsrisiken aussetzen könnte.

- **Sitzungs-Timeout aktivieren:**

Automatische Abmeldung des Benutzers nach einer definierten Inaktivitätszeit, um unbefugten Zugriff zu verhindern.

- **Sitzungs-Timeout (Sekunden):**

Eingabefeld zur Angabe der Dauer (in Sekunden), bevor die Sitzung abläuft. Standardwert: 300 Sekunden (5 Minuten).

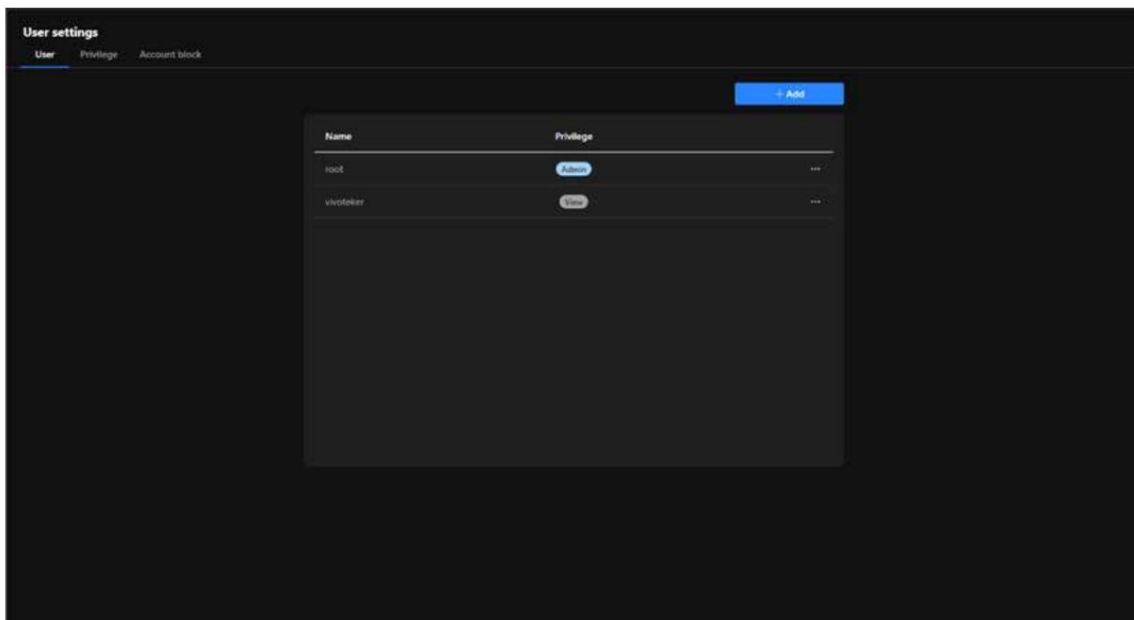
System

Benutzerzugriffe und Berechtigungen verwalten für mehr Sicherheit und Kontrolle

Die Benutzerkontenverwaltung ist für die Zugriffsverwaltung der VIVOTEK-Kamera von entscheidender Bedeutung. Sie ermöglicht Systemadministratoren die Erstellung und Kontrolle von Benutzerkonten, die Definition von Berechtigungen und die Durchsetzung von Sicherheitsmaßnahmen wie der Kontosperrung. Dadurch wird sichergestellt, dass die Kamera sicher und verwaltbar ist und nur autorisierten Benutzern zugänglich ist.

Benutzer

Die Benutzerkarte bietet wichtige Werkzeuge zur Verwaltung von Benutzerkonten, zur Gewährleistung eines sicheren Zugriffs und zur Zuweisung geeigneter Berechtigungen. Sie trägt zur Aufrechterhaltung einer kontrollierten Umgebung bei, indem sie Administratoren die Definition von Rollen, die Überwachung der Benutzeraktivitäten und die Verbesserung der Sicherheit des Kamerasystems ermöglicht.



System

• Schritte zum Hinzufügen eines Benutzerkontos:

The screenshot shows a dark-themed dialog box titled "Add a user" with a close button (X) in the top right corner. The dialog contains the following fields and elements:

- User Name:** A text input field containing "vivoteker". Below the field is an orange warning icon and the text "user name should be unique".
- Password:** A password input field with masked characters "....." and a toggle icon for visibility.
- Your password must have:** A list of requirements with green checkmarks:
 - ✓ 8~64 Length of character; no space allowed
 - ✓ At least one alphabetic character
 - ✓ At least one numeric character
- Strength:** A green progress bar and the label "Strong".
- Confirm Password:** A password input field with masked characters "....." and a toggle icon for visibility.
- Privilege:** A dropdown menu currently showing "Viewer".
- Buttons:** "Save" and "Cancel" buttons at the bottom.

Schritt 1. Klicken Sie auf die Schaltfläche „+ Hinzufügen“.

Suchen Sie die Schaltfläche „+ Hinzufügen“ und klicken Sie darauf, um das Formular „Benutzer hinzufügen“ zu öffnen.

Schritt 2. Geben Sie den Benutzernamen

ein. Geben Sie im Feld „Benutzername“ einen eindeutigen Benutzernamen ein.

Notiz:

Der Benutzername darf mit keinem bereits existierenden Kontonamen übereinstimmen.

Schritt 3. Passwort festlegen Geben

Sie im Feld „Passwort“ ein Passwort ein, das folgende Kriterien erfüllt: 8–64 Zeichen lang (Leerzeichen sind nicht erlaubt).

Enthält mindestens einen alphabetischen Buchstaben.

Enthält mindestens ein numerisches Zeichen.

Stellen Sie sicher, dass die Passwortstärkeanzeige auf „Stark“ steht, um optimale Sicherheit zu gewährleisten.

Schritt 4. Passwort bestätigen Geben Sie das

Passwort im Feld „Passwort bestätigen“ erneut ein, um zu überprüfen, ob es übereinstimmt.

System

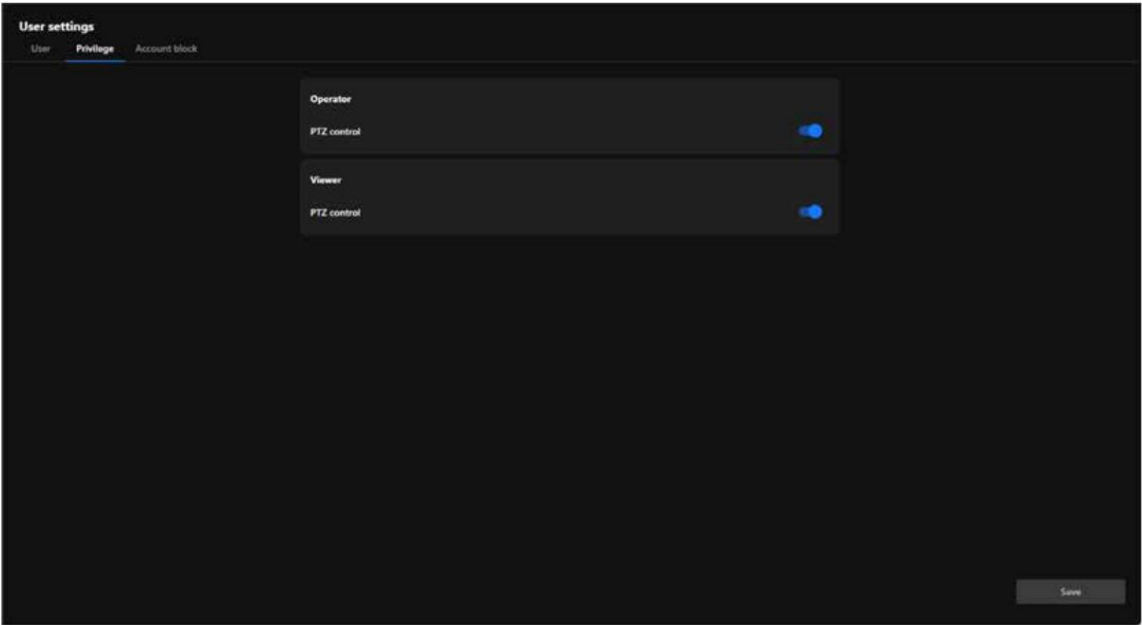
Schritt 5. Berechtigungsstufe zuweisen

Wählen Sie im Dropdown-Menü „Berechtigungen“ die gewünschte Berechtigungsstufe für den neuen Benutzer aus:

Administrator	Volle Kontrolle.
Operator	Steuerung von DO, Weißlichtbeleuchtung, Schnappschuss und PTZ nicht möglich; Zugriff auf die Kamerakonfigurationsseite nicht möglich.
Zuschauer	Steuern Sie DO, Weißlichtbeleuchtung, Ansicht, Hören, PTZ und Sprechen über die Kameraschnittstelle.

Privileg

Die Berechtigungskarte im Bereich „Benutzerkonten“ ermöglicht Administratoren die Verwaltung der spezifischen Berechtigungen verschiedener Benutzerrollen. Dies gewährleistet eine detaillierte Kontrolle darüber, welche Aktionen Benutzer ausführen können, insbesondere für Benutzer mit eingeschränkten Zugriffsrechten wie Operator oder Betrachter.



System

Konto gesperrt

Die Kontosperrung ist eine wichtige Sicherheitsfunktion, die Administratoren dabei unterstützt, verdächtige Anmeldeversuche automatisch zu blockieren und so Brute-Force-Angriffe effektiv zu verhindern und die Systemsicherheit zu erhöhen. Dank flexibler Einstellungsmöglichkeiten und der Verwaltung von Sperrlisten gewährleistet diese Funktion einen stabilen und sicheren Betrieb des Kamerasystems auch in Umgebungen mit mehreren Benutzern.

User settings

User Privilege **Account block**

Condition setting

Enable account block ☒

Block source IP ☒

Consecutive login fails

Interval of consecutive fails

Block time

Block list

Name	Source IP	Ending time	
vivoteker	10.135.21.63	12/11/2024, 11:26:09 AM	Unblock

[Save](#)

• Bedingungseinstellung

Kontosperrung aktivieren

Aktiviert oder deaktiviert die Kontosperrfunktion. Ist diese aktiviert, blockiert das System automatisch verdächtige Anmeldeversuche basierend auf den definierten Bedingungen.

Quell-IP blockieren

Blockiert die IP-Adresse, die für übermäßige fehlgeschlagene Anmeldeversuche verantwortlich ist, und schränkt so weitere Zugriffsversuche von dieser Quelle ein.

Aufeinanderfolgende Anmeldefehler

Legt die Anzahl aufeinanderfolgender fehlgeschlagener Anmeldeversuche fest, die zur Sperrung führen. Ist der Wert beispielsweise auf 5 gesetzt, wird eine IP-Adresse nach 5 aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen gesperrt.

Intervall aufeinanderfolgender Ausfälle

Definiert den Zeitraum (in Sekunden), innerhalb dessen aufeinanderfolgende fehlgeschlagene Versuche als Auslöser für eine Sperrung gewertet werden.

Blockzeit

Legt die Dauer (in Sekunden) fest, für die die betreffende IP-Adresse gesperrt bleibt. Bei einer Einstellung von beispielsweise 300 Sekunden kann die IP-Adresse 5 Minuten lang keine weiteren Anmeldeversuche unternehmen.

System

- **Sperrliste**

Zeigt eine Liste der aktuell gesperrten IP-Adressen oder Benutzerkonten an: Name: Zeigt den

von der Sperrung betroffenen Benutzernamen an.

Quell-IP: Gibt die IP-Adresse an, die die Sperrung ausgelöst hat.

Endzeitpunkt: Zeigt den genauen Zeitpunkt an, zu dem die Sperre abläuft.

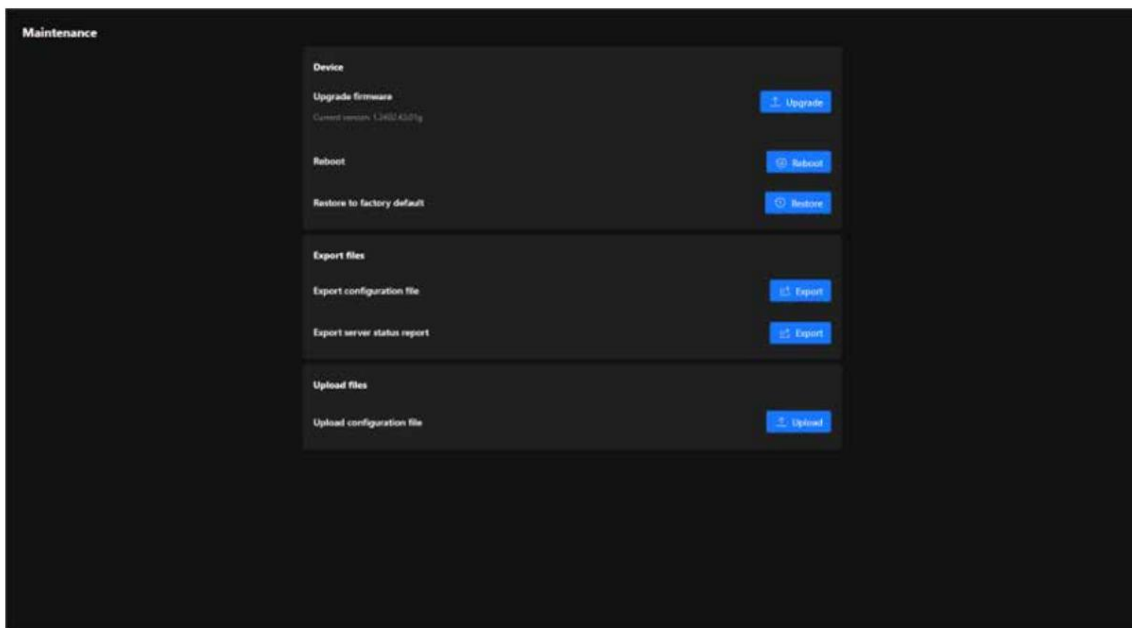
Entsperren:

Ermöglicht Administratoren, eine gesperrte IP-Adresse oder ein gesperrtes Konto manuell aus der Liste zu entfernen.

System

Firmware-Updates und Konfigurationsmanagement für das System Wartung

Die Wartungsfunktion bietet eine zentrale Plattform für Firmware-Updates, die Sicherung und Wiederherstellung von Konfigurationen sowie das Zurücksetzen des Systems auf die Werkseinstellungen. Diese Tools gewährleisten einen effizienten Betrieb der VIVOTEK-Kamera, halten sie auf dem neuesten Stand und ermöglichen eine einfache Verwaltung für Administratoren von Überwachungssystemen.



Wartung

Die Wartungsseite unter der Kategorie „System“ bietet Werkzeuge zur Verwaltung der Geräte-Firmware, der Konfiguration und der Betriebsstabilität. In diesem Bereich können Administratoren wichtige Wartungsaufgaben durchführen, um die optimale Funktion der Kamera sicherzustellen. Nachfolgend finden Sie eine Übersicht über die Funktionen und den Zweck:

- **Gerät**

Die Gerätekarte bietet Werkzeuge für Firmware-Updates, Systemneustarts und das Zurücksetzen auf Werkseinstellungen. Diese Funktionen gewährleisten, dass die Kamera stets aktuell, funktionsfähig und bei Bedarf für neue Konfigurationen oder Fehlerbehebungen bereit bleibt.

System

Durch Firmware-Upgrades

bleibt die Kamera auf dem neuesten Stand mit den aktuellsten Funktionen, Leistungsverbesserungen und Sicherheitspatches. Gewährleistet Kompatibilität mit neuen Technologien und erweiterte Systemfunktionalität.

Angezeigte Informationen: Zur

Information wird die aktuelle Firmware-Version (z. B. 1.2402.43.01g) angezeigt.

Aktion:

Durch Klicken auf die Schaltfläche „Upgrade“ können Benutzer eine neue Firmware-Datei hochladen und das Gerät aktualisieren.

Neustart

Startet die Kamera neu, um ihre Systemprozesse zu aktualisieren, ohne die Konfigurationen zu ändern. Nützlich, um Änderungen anzuwenden oder vorübergehende Probleme zu beheben.

Aktion:

Durch Klicken auf die Schaltfläche „Neustart“ wird ein Neustart der Kamera ausgelöst.

Die Option „Auf Werkseinstellungen

zurücksetzen“ stellt die Kamera auf die ursprünglichen Werkseinstellungen zurück und entfernt alle benutzerdefinierten Konfigurationen. Diese Option ist hilfreich, um hartnäckige Probleme zu beheben oder das Gerät für einen erneuten Einsatz vorzubereiten.

Aktion:

Durch Klicken auf die Schaltfläche „Wiederherstellen“ werden alle Konfigurationen gelöscht und die Standardeinstellungen wiederhergestellt.

● Exportdateien

Die Exportdateien-Karte bietet Administratoren Werkzeuge zum Exportieren wichtiger Kameradaten, wie z. B. Konfigurationseinstellungen und Statusberichte. Diese Funktionen erleichtern das Erstellen von Backups, die Diagnose von Problemen und das Übertragen von Einstellungen auf mehrere Geräte.



Die Exportkonfigurationsdatei

erstellt eine Sicherungskopie der aktuellen Kameraeinstellungen. Diese Datei kann verwendet werden, um die Kameraeinstellungen bei Bedarf wiederherzustellen.

Um eine einheitliche Bereitstellung zu gewährleisten, sollte die gleiche Konfiguration auch auf anderen Kameras vorgenommen werden.

Aktion:

Durch Klicken auf die Schaltfläche „Exportieren“ wird die Konfigurationsdatei auf das lokale System heruntergeladen.

System

Exportserver-Statusbericht

Erstellt und exportiert einen Bericht mit dem Betriebsstatus der Kamera, einschließlich Diagnosedaten und Protokollen. Dies ist nützlich für:

Leistungsanalyse und Identifizierung potenzieller Probleme.

Statusinformationen werden zur Fehlerbehebung an Supportteams oder Systemadministratoren weitergegeben.

Aktion:

Durch Klicken auf die Schaltfläche „Exportieren“ wird der Serverstatusbericht zur weiteren Analyse heruntergeladen.

• Dateien hochladen

Die Option „Dateien hochladen“ ermöglicht Administratoren, vorkonfigurierte Kameraeinstellungen durch Hochladen einer Konfigurationsdatei wiederherzustellen oder anzuwenden. Diese Funktion ist besonders nützlich für die Systemwiederherstellung oder die Bereitstellung standardisierter Konfigurationen auf mehreren Geräten.



Konfigurationsdatei hochladen

Diese Funktion ermöglicht die Wiederherstellung der Kameraeinstellungen mithilfe einer zuvor exportierten Konfigurationsdatei. Dadurch wird die Übertragung von Konfigurationen auf mehrere Kameras vereinfacht und die Wiederherstellung im Falle von Systemrücksetzungen oder Datenverlust beschleunigt.

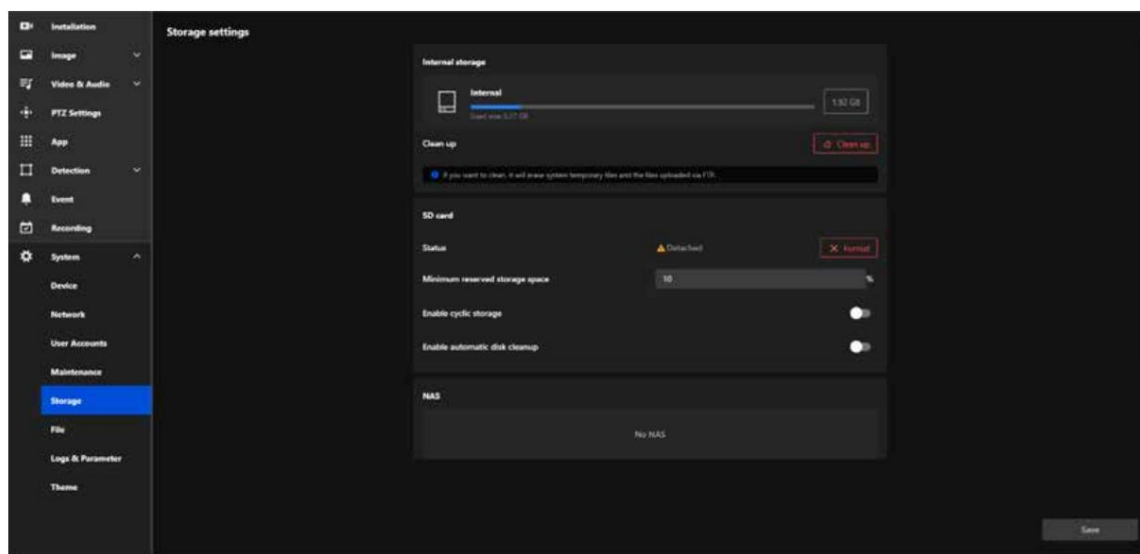
Aktion:

Durch Klicken auf die Schaltfläche „Hochladen“ können Benutzer eine Konfigurationsdatei von ihrem lokalen System auswählen und anwenden. die Kamera.

System

Optimierte Speicherlösungen für zuverlässige Videoaufzeichnung und Datenaufbewahrung

Der Speicherbereich bietet umfassende Tools zur Verwaltung und Optimierung der Speicherressourcen der Kamera. Ob interner Speicher, SD-Karten oder externe NAS-Geräte – dieser Bereich gewährleistet zuverlässige Videoaufzeichnung und effiziente Datenspeicherung. Funktionen wie zyklische Speicherung, Einstellungen für reservierten Speicherplatz und automatische Bereinigung ermöglichen Administratoren einen unterbrechungsfreien Betrieb und eine optimale Speicherausnutzung.

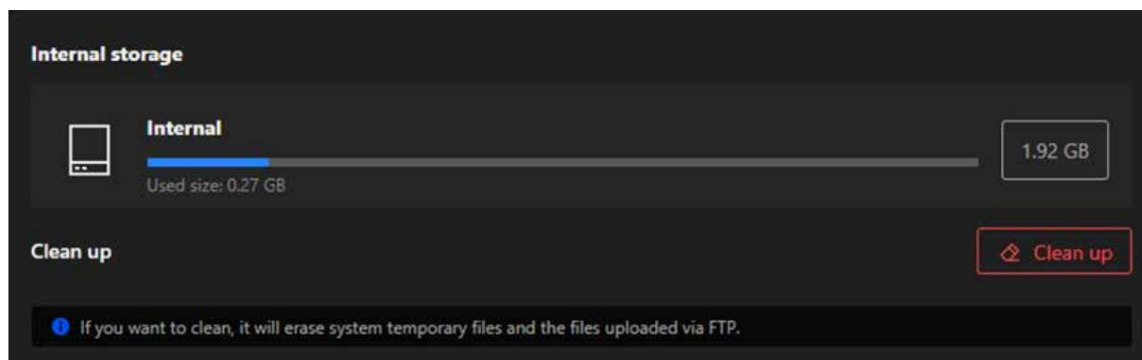


● Speichereinstellungen

Die Speichereinstellungen dienen der Verwaltung von Speichermedien und der Optimierung des für Videoaufnahmen, Dateispeicherung und Systemvorgänge genutzten Speicherplatzes. Dieser Abschnitt bietet Administratoren Werkzeuge zur Überwachung, Bereinigung und Konfiguration von Speicheroptionen, um einen effizienten Kamerabetrieb und die Speicherung wichtiger Daten zu gewährleisten.

● Interner Speicher

Die interne Speicherkarte dient der Verwaltung und Überwachung der internen Speichernutzung der Kamera. Sie bietet einen Überblick über die Speicherkapazität, die aktuelle Nutzung und Werkzeuge zur Optimierung der Speichernutzung durch das Entfernen unnötiger Dateien.



System

Speicherübersicht

Angezeigte Informationen:

Gesamtkapazität: Zeigt die Gesamtspeicherkapazität des internen Speichers an (z. B. 1,92 GB).

Belegter Speicherplatz: Zeigt die aktuell belegte Speichermenge an (z. B. 0,27 GB).

Nutzungsanzeige: Stellt visuell das Verhältnis von belegtem zu verfügbarem Speicherplatz dar.

Die Funktion

„Aufräumen“ gibt internen Speicherplatz frei, indem unnötige Dateien gelöscht werden,

wie zum Beispiel: Temporäre Systemdateien.

Dateien wurden per FTP hochgeladen.

Aktion:

Durch Klicken auf die Schaltfläche „Bereinigen“ wird der Bereinigungsprozess gestartet, die angegebenen Dateien werden gelöscht und mehr Speicherplatz für wichtige Daten freigegeben.

SD-Karte

Die SD-Karte ermöglicht Administratoren die Verwaltung und Überwachung von Nutzung, Status und Einstellungen der SD-Karte. Diese Funktionalität ist entscheidend für die zuverlässige Datenspeicherung und die kontinuierliche Videoaufzeichnung bzw. Dateispeicherung.

SD card

Status ⚠ Detached ✖ Format

Minimum reserved storage space %

Enable cyclic storage ☒

Enable automatic disk cleanup ☒

Maximum duration for keeping files days

Status

Zeigt den aktuellen Status der SD-Karte an (z. B. „Abgetrennt“, wenn keine Karte eingelegt oder erkannt wird).

Aktionen:

Mit der Schaltfläche „Formatieren“ können Sie alle Dateien löschen und die SD-Karte für die Verwendung initialisieren.

Mindestens reservierter Speicherplatz: Reserviert

einen Prozentsatz der Gesamtkapazität der SD-Karte, um zu verhindern, dass diese vollständig belegt wird und so sicherzustellen, dass kritische Vorgänge fortgesetzt werden können.

Aktionen:

Geben Sie einen Prozentsatz (z. B. 10 %) ein, um Speicherplatz zu reservieren.

System

Die Option „Zyklische

Speicherung aktivieren“ ermöglicht das automatische Überschreiben der ältesten Daten auf der SD-Karte, sobald diese voll ist, und gewährleistet so eine kontinuierliche Aufzeichnung.

Aktion:

Aktivieren oder deaktivieren Sie diese Funktion, um das Speicherverhalten zu steuern.

Die automatische Datenträgerbereinigung

aktiviert die automatische Löschung unnötiger oder älterer Dateien, um Speicherplatz freizugeben.

Abhängigkeit: Durch

Aktivieren dieser Funktion wird die Option „Maximale Aufbewahrungsdauer für Dateien“ aktiviert.

Aktionen:

Aktivieren Sie diese Funktion, um die automatische Bereinigung veralteter Dateien zu ermöglichen.

Maximale Aufbewahrungsdauer für Dateien: Legt eine

bestimmte Aufbewahrungsdauer für Dateien auf der SD-Karte fest (z. B. 7 Tage). Dateien, die älter als die angegebene Dauer sind, werden automatisch gelöscht.

Aktionen:

Geben Sie die gewünschte Anzahl an Tagen für die Aufbewahrung der Dateien in das Textfeld ein.

So bereiten Sie die SD-Karte vor:

Schritt 1. Legen Sie eine SD-Karte in den Steckplatz der Kamera ein.

Schritt 2. Überprüfen Sie das Statusfeld, um sicherzustellen, dass die SD-Karte erkannt wurde.

Schritt 3. Wenn die SD-Karte neu ist oder neu initialisiert werden muss: Klicken

Sie auf die Schaltfläche „Formatieren“, um ihren Inhalt zu löschen und sie für die Verwendung vorzubereiten.

So konfigurieren Sie die Speichereinstellungen:

Schritt 1. Legen Sie den minimal reservierten Speicherplatz fest: Geben Sie

einen Prozentsatz (z. B. 10 %) ein, um einen Teil der Kapazität der SD-Karte zu reservieren.

Schritt 2. Zyklische Speicherung aktivieren:

Aktivieren Sie diese Funktion, damit die ältesten Dateien überschrieben werden, wenn die SD-Karte voll ist.

Schritt 3. Automatische Datenträgerbereinigung aktivieren (optional):

Aktivieren Sie diese Option, um die Bereinigungsfunktionen zu aktivieren.

Geben Sie die maximale Aufbewahrungsdauer für Dateien ein (z. B. 7 Tage), um den Aufbewahrungszeitraum für Dateien festzulegen.

Um eine kontinuierliche Aufzeichnung zu

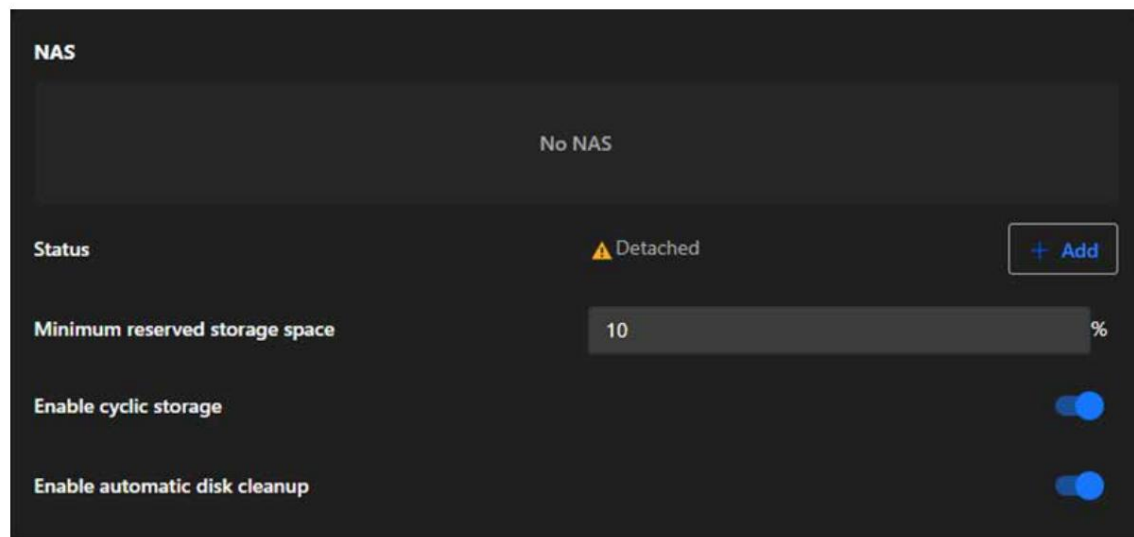
gewährleisten: Schritt 1. Stellen Sie sicher, dass sowohl die zyklische Speicherung als auch die automatische Datenträgerbereinigung aktiviert sind.

Schritt 2. Überprüfen Sie regelmäßig den Status, um sicherzustellen, dass die SD-Karte ordnungsgemäß funktioniert.

System

• IM

Die NAS-Karte ermöglicht Administratoren die Integration eines NAS-Geräts (Network Attached Storage) für erweiterten und skalierbaren Speicherplatz. Dadurch wird sichergestellt, dass die Speicherkapazität der Kamera erweitert und Daten sicher an einem zentralen Ort gespeichert werden können.



NAS-Status

Zeigt den Verbindungsstatus des NAS-Geräts an (z. B. „Getrennt“, wenn keine Verbindung hergestellt werden kann).

Aktionen:

Klicken Sie auf „+ Hinzufügen“, um ein NAS-Gerät zu konfigurieren und anzuschließen.

Die Einstellung „Mindestspeicherplatz

reserviert“ stellt sicher, dass ein bestimmter Prozentsatz des NAS-Speichers reserviert bleibt, um zu verhindern, dass das System den NAS vollständig belegt.

Aktionen:

Administratoren können einen Prozentsatz (z. B. 10 %) eingeben, um Speicherplatz für kritische Zwecke zu reservieren.

Die Option „Zyklische

Speicherung aktivieren“ ermöglicht es der Kamera, die ältesten auf dem NAS gespeicherten Dateien zu überschreiben, wenn der Speicher voll ist, wodurch eine unterbrechungsfreie Aufnahme gewährleistet wird.

Aktionen:

Diese Funktion kann je nach Speicherverwaltungseinstellungen ein- oder ausgeschaltet werden.

Die Option „Automatische

Datenträgerbereinigung aktivieren“ automatisiert die Bereinigung veralteter oder unnötiger Dateien auf dem NAS, um ausreichend Speicherplatz freizuhalten.

Aktionen:

Aktivieren Sie diese Funktion, um die automatische Dateilöschung auf Basis systemdefinierter Kriterien zu aktivieren.

System

NAS-Konfigurationsschritte Schritt

1. NAS-Speichereinstellungen öffnen: Klicken Sie

bei der NAS-Karte auf + Hinzufügen, um das Konfigurationsfenster zu öffnen.

Schritt 2. Netzwerkspeicherort festlegen: Geben Sie

den Pfad zum NAS-Speicherordner ein (z. B. \\NASDevice\SharedFolder).

Schritt 3. Arbeitsgruppe eingeben (optional): Geben

Sie bei Bedarf die Arbeitsgruppe an, zu der das NAS-Gerät gehört.

Schritt 4. Benutzerdaten angeben: Geben Sie

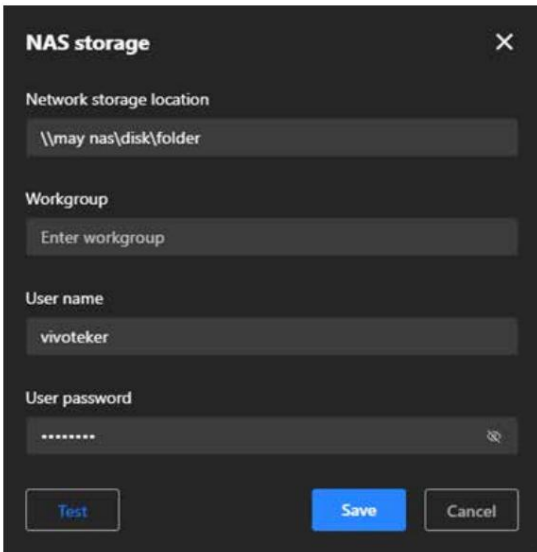
den Benutzernamen und das Passwort ein, die zur Authentifizierung und zum Zugriff auf das NAS-Gerät erforderlich sind.

Schritt 5. Verbindung testen: Klicken Sie

auf Testen, um sicherzustellen, dass die Kamera erfolgreich eine Verbindung zum angegebenen NAS-Speicherort herstellen kann.

Schritt 6. Konfiguration speichern:

Klicken Sie auf Speichern, um die Einstellungen anzuwenden und die Verbindung herzustellen.



The image shows a dark-themed dialog box titled "NAS storage" with a close button (X) in the top right corner. It contains four input fields: "Network storage location" with the text "\\may nas\disk\folder", "Workgroup" with the placeholder "Enter workgroup", "User name" with the text "vivoteker", and "User password" with masked characters "*****" and a toggle icon. At the bottom, there are three buttons: "Test" (blue), "Save" (blue), and "Cancel" (grey).

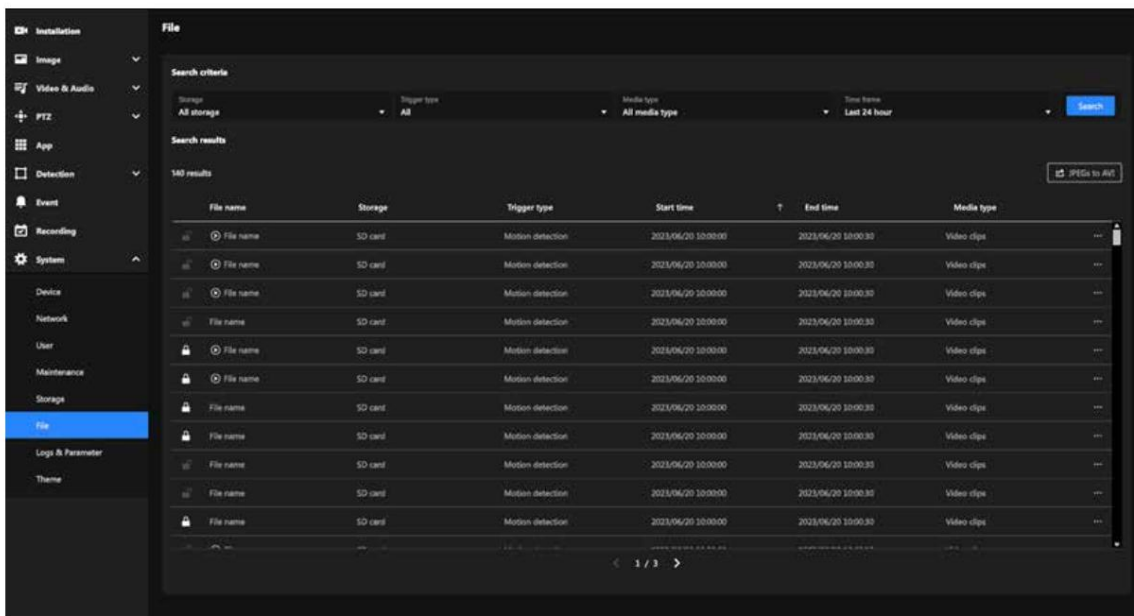
System

Mühe lose Verwaltung und Wiedergabe von aufgezeichneten Medien

Der Bereich „Dateien“ bietet eine benutzerfreundliche Oberfläche zur Verwaltung aufgezeichneter Mediendateien. Mithilfe von Such- und Filterfunktionen können Benutzer gezielt Aufnahmen nach Speichertyp, Auslöser, Medienformat und Zeitraum finden. Zudem lassen sich Dateien sperren, Aufnahmen exportieren und Medien konvertieren, um eine effiziente Verwaltung und Archivierung zu gewährleisten. Dies sichert eine übersichtliche Speicherung und den schnellen Zugriff auf wichtige Daten.

Datei

Der Bereich „Dateien“ ermöglicht Nutzern das effiziente Suchen, Filtern und Verwalten aufgezeichneter Mediendateien. Zu den wichtigsten Funktionen gehören erweiterte Suchkriterien, die Dateispernung zur Datenaufbewahrung sowie Optionen zum Exportieren oder Konvertieren von Aufnahmen. Hauptzweck ist die Optimierung der Medienorganisation, die Gewährleistung einer sicheren Speicherung und die Unterstützung des schnellen Zugriffs für detaillierte Analysen.



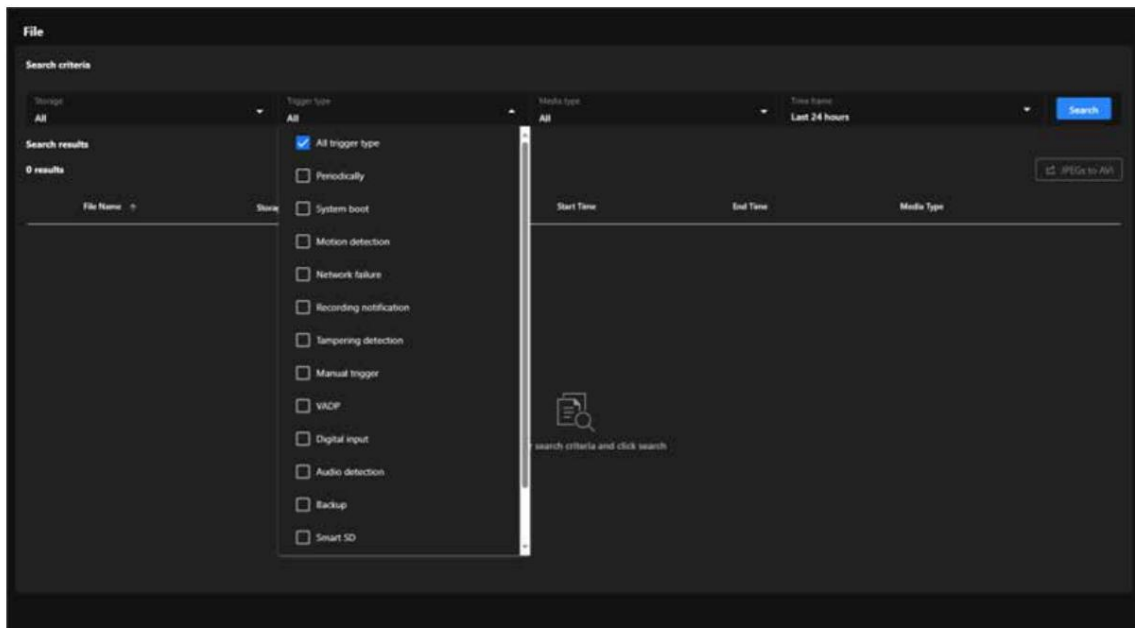
Suchkriterien

Ermöglicht es Benutzern, ihre Suche nach aufgezeichneten Dateien anhand spezifischer Parameter zu verfeinern, wodurch das Auffinden relevanter Aufnahmen erleichtert wird.

Suchfilter:

- **Speicher:** Filtern Sie nach Speichertyp (z. B. SD-Karte, NAS oder alle Speichergeräte).
- **Auslösertyp:** Suche nach Dateien, die durch bestimmte Ereignisse ausgelöst werden (z. B. Bewegungserkennung, manuelle Aufzeichnung).
- **Medientyp:** Filtern Sie nach Medientyp (z. B. Videoclips, Schnappschüsse).
- **Zeitraumen:** Geben Sie einen Zeitraum an (z. B. die letzten 24 Stunden, einen benutzerdefinierten Zeitraum), um die Suche einzugrenzen.

System



Suchergebnisse

Dateiname:

Name der aufgezeichneten Datei.

Speicherort: Gibt den Speicherort der Datei an (z. B. SD-Karte).

Auslösertyp:

Zeigt das Ereignis an, das die Aufzeichnung ausgelöst hat (z. B. Bewegungserkennung).

Start- und Endzeit:

Gibt den Zeitbereich für jede Aufnahme an.

Medientyp:

Gibt den Typ der Mediendatei an (z. B. Videoclips).

Search results						
140 results						
File name	Storage	Trigger type	Start time	↑	End time	Media type
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips
File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips

System

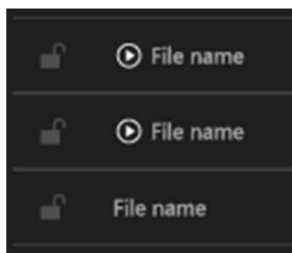
● Notiz:

Schaltfläche zum Sperren/Entsperren von Dateien:

Gesperrte Dateien, die durch ein Schlosssymbol gekennzeichnet sind, sind vor automatischem Löschen geschützt, und ihre Aufbewahrung kann über die Sperr-/Entsperrschaltfläche verwaltet werden.

Wiedergabetaste:

Nur Dateien mit aufgezeichneten Daten und Wiedergabeberechtigung zeigen die Wiedergabetaste an.



Dateioptionen (Symbol „Mehr“)

Jede Datei in den Ergebnissen verfügt über zusätzliche Optionen, die über das Drei-Punkte-Menü zugänglich sind:

• Herunterladen:

Ermöglicht das Speichern der Datei auf Ihrem Gerät. Schritte: **Schritt 1:** Klicken

Sie auf das Dreipunkt-Menü neben einer Datei. **Schritt 2 :** Wählen Sie

„Herunterladen“.

Schritt 3. Die Datei wird an Ihrem Standard-Downloadspeicherort gespeichert.

• Löschen:

Entfernt die Datei endgültig aus dem Speicher. Schritte: **Schritt 1.** Klicken Sie auf

das Dreipunkt-Menü neben einer Datei.

Schritt 2. Wählen Sie „Löschen“.

Schritt 3. Bestätigen Sie die Löschung in der Popup-Aufforderung.

🔒	⏮ File name	SD card	Motion detection	2023/06/20 10:00:00	2023/06/20 10:00:30	Video clips	⋮
🔒	⏮ File name	SD card	Motion detection	2023/06/20 10:00:00	2023/06/20 10:00:30	Download	
🔒	File name	SD card	Motion detection	2023/06/20 10:00:00	2023/06/20 10:00:30	Delete	
🔒	File name	SD card	Motion detection	2023/06/20 10:00:00	2023/06/20 10:00:30	Video clips	⋮

● JPEGs in AVI konvertieren

Die Funktion „JPEGs zu AVI“ ermöglicht es Benutzern, aufeinanderfolgende JPEG-Bildsequenzen in ein abspielbares AVI-Videoformat zu konvertieren. Diese Funktion ist besonders nützlich, wenn Benutzer das Videomaterial als durchgehendes Video ansehen möchten, anstatt einzelne Bilder zu analysieren.

Schritte zur Konvertierung von JPEGs in

AVI: Schritt 1. Klicken Sie auf die Schaltfläche „JPEGs zu AVI“.

Schritt 2. Aktivierung der Auswahlfunktion:

Neben jeder Snapshot-Datei wird ein Kontrollkästchen angezeigt, mit dem Benutzer manuell auswählen können, welche Dateien in die AVI-Konvertierung einbezogen werden sollen.

System

Schritt 3. Zwei neue Schaltflächen erscheinen:

Kombinieren

Mit dieser Schaltfläche kann der Benutzer den Konvertierungsprozess bestätigen und starten. Sie wird erst aktiviert, nachdem mindestens eine Datei ausgewählt wurde.

Stornieren

Durch Klicken auf diese Schaltfläche wird der Konvertierungsmodus beendet, alle Auswahlen werden gelöscht und die ursprüngliche Dateiansicht wiederhergestellt.

Schritt 4. Beginnen Sie mit dem Zusammenfügen zu einer einzigen AVI-Datei.

Search criteria

Storage

All storage

Trigger type

All

Media type

All media type

Time frame

Last 24 hour

Search

Search results

Select snapshot file types for combining into AVI format0 file selected

ContinueCancel

☐	File name	Storage	Trigger type	Start time	↑	End time	Media type	
☐	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Snapshot	...
☒	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips	...
☐	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Snapshot	...
☒	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips	...
☐	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Snapshot	...
☐	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Snapshot	...
☒	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips	...
☒	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Video clips	...
☐	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Snapshot	...
☐	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Snapshot	...
☐	File name	SD card	Motion detection	2023/06/20 10:00:00		2023/06/20 10:00:30	Snapshot	...

1 / 3

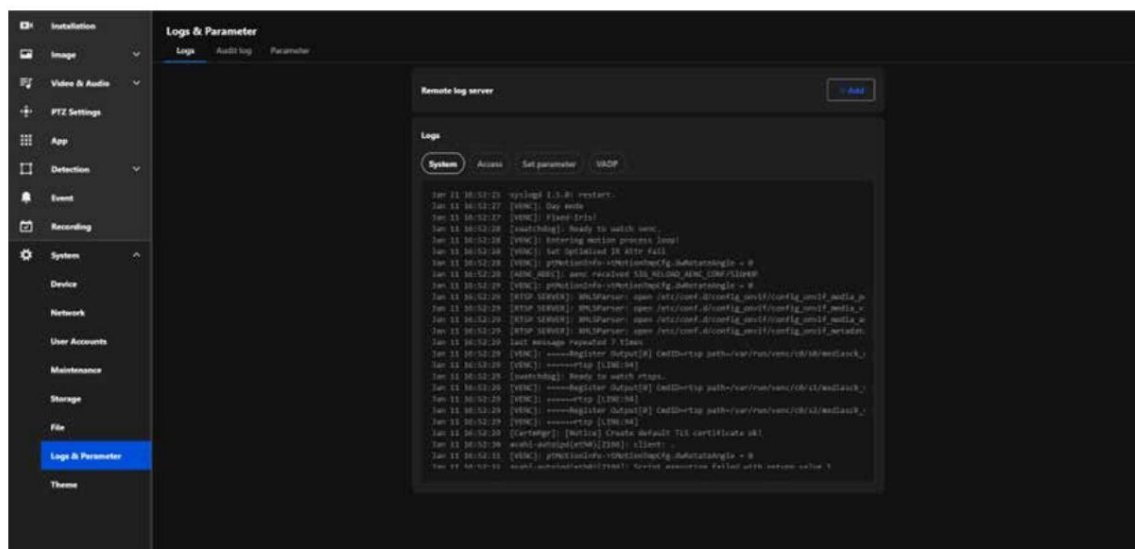
System

Überwachung und Verwaltung von Systemprotokollen und -parametern

Effektives Systemmanagement setzt die Fähigkeit voraus, detaillierte Protokolle und Parameter zu überwachen und zu analysieren. Dieser Abschnitt bietet Werkzeuge zum Anzeigen und Verwalten von System-, Zugriffs- und Konfigurationsprotokollen. So können Benutzer Probleme diagnostizieren, Aktivitäten verfolgen und eine optimale Leistung gewährleisten. Funktionen wie die Integration eines Remote-Protokollservers und die Parameterverwaltung bieten Administratoren die notwendigen Kontrollmöglichkeiten, um Sicherheit und Betriebseffizienz sowohl in Einzelkamera- als auch in Mehrkamerasystemen sicherzustellen.

Protokolle & Parameter

Der Bereich „Protokolle & Parameter“ in den Systemeinstellungen der VIVOTEK-Kamera bietet detaillierte Einblicke in Systemereignisse, Benutzeraktivitäten und Konfigurationsänderungen. Er erleichtert die Fehlersuche, Überwachung und Aufrechterhaltung der Gesamtleistung und Sicherheit der Kamera.

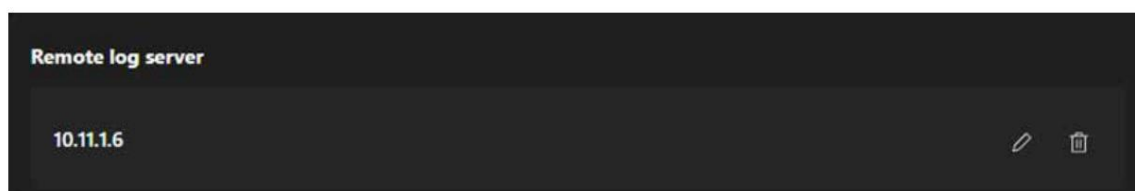


Protokolle

Die Protokolle bieten Nutzern umfassende Werkzeuge zur Überwachung und Verwaltung von Systemaktivitäten, Benutzerzugriffen und Konfigurationsänderungen an der Kamera. Durch die Möglichkeit der lokalen Protokollanzeige in Echtzeit und der Integration mit einem Remote-Protokollserver unterstützt diese Registerkarte Nutzer bei der Fehlerbehebung, der Nachverfolgung von Sicherheitsereignissen und der Einhaltung von Betriebsrichtlinien. Sie ist eine unverzichtbare Ressource zur Gewährleistung der Systemzuverlässigkeit, zur Erhöhung der Sicherheit und zur Unterstützung der zentralen Protokollverwaltung in Umgebungen mit mehreren Geräten.

● Remote-Protokollserver

Der Remote-Log-Server bietet eine effiziente, sichere und skalierbare Lösung für die Kameraprotokollverwaltung und ist daher besonders wertvoll bei groß angelegten Installationen oder Umgebungen mit strengen Datenaufbewahrungsrichtlinien.



System

Schritte zum Einrichten des Remote-Protokollservers:

Schritt 1. Klicken Sie auf die Schaltfläche „+Hinzufügen“.

Schritt 2. Geben Sie im Textfeld „IP-Adresse“ die IP-Adresse des Remote-Servers ein.

Schritt 3. Geben Sie im Textfeld „Port“ die Portnummer des Remote-Servers ein.

Schritt 4. Klicken Sie nach Abschluss der Schritte auf Speichern, um die Einstellung zu aktivieren.

● Protokolle

Die Protokolle liefern Benutzern detaillierte Aufzeichnungen über Systemaktivitäten, Zugriffsversuche, Konfigurationsänderungen und die Anwendungsleistung. Sie vereinfachen die Fehlersuche, indem sie Benutzern helfen, Probleme zu identifizieren, erhöhen die Sicherheit durch die Überwachung des Zugriffs und gewährleisten Transparenz im Konfigurationsmanagement. Diese Funktion ist besonders nützlich für die Aufrechterhaltung der Systemstabilität, die Verfolgung unautorisierter Zugriffe und die Diagnose von Anwendungs- oder Konfigurationsproblemen. Die Protokolle bestehen aus den folgenden Kategorien, die jeweils für die Aufzeichnung spezifischer Informationstypen konzipiert sind:

System:

Es werden wichtige Systemaktivitäten aufgezeichnet, darunter Gerätestart, Neustart, Fehlermeldungen und Moduswechsel, um die Systemstabilität zu ermitteln und potenzielle Probleme zu identifizieren.

System

Logs

SystemAccessSet parameterVADP

```
Jan 11 16:52:25 syslogd 1.5.0: restart.
Jan 11 16:52:27 [VENC]: Day mode
Jan 11 16:52:27 [VENC]: Fixed-Iris!
Jan 11 16:52:28 [swatchdog]: Ready to watch venc.
Jan 11 16:52:28 [VENC]: Entering motion process loop!
Jan 11 16:52:28 [VENC]: Set Optimized IR Attr fail
Jan 11 16:52:28 [VENC]: ptMotionInfo->tMotionTmpCfg.dwRotateAngle = 0
Jan 11 16:52:28 [AENC_ADEC]: aenc received SIG_RELOAD_AENC_CONF/SIGHUP
Jan 11 16:52:29 [VENC]: ptMotionInfo->tMotionTmpCfg.dwRotateAngle = 0
Jan 11 16:52:29 [RTSP SERVER]: XMLSParser: open /etc/conf.d/config_onvif/config_onvif_media_p
Jan 11 16:52:29 [RTSP SERVER]: XMLSParser: open /etc/conf.d/config_onvif/config_onvif_media_v
Jan 11 16:52:29 [RTSP SERVER]: XMLSParser: open /etc/conf.d/config_onvif/config_onvif_media_a
Jan 11 16:52:29 [RTSP SERVER]: XMLSParser: open /etc/conf.d/config_onvif/config_onvif_metadati
Jan 11 16:52:29 last message repeated 7 times
Jan 11 16:52:29 [VENC]: =====Register Output[0] CmdID=rtsp path=/var/run/venc/c0/s0/mediasck_
Jan 11 16:52:29 [VENC]: =====rtsp [LINE:94]
Jan 11 16:52:29 [swatchdog]: Ready to watch rtsp.
Jan 11 16:52:29 [VENC]: =====Register Output[0] CmdID=rtsp path=/var/run/venc/c0/s1/mediasck_
Jan 11 16:52:29 [VENC]: =====rtsp [LINE:94]
Jan 11 16:52:29 [VENC]: =====Register Output[0] CmdID=rtsp path=/var/run/venc/c0/s2/mediasck_
Jan 11 16:52:29 [VENC]: =====rtsp [LINE:94]
Jan 11 16:52:29 [CertMgr]: [Notice] Create default TLS certificate ok!
Jan 11 16:52:30 avahi-autoipd(eth0)[2166]: client: .
Jan 11 16:52:31 [VENC]: ptMotionInfo->tMotionTmpCfg.dwRotateAngle = 0
Jan 11 16:52:31 avahi-autoipd(eth0)[2166]: Script execution failed with return value 1
```

Zugang:

Protokolliert alle Zugriffsversuche auf die Kamera, einschließlich An- und Abmeldevorgänge, wodurch sie sich zur Überwachung unautorisierter Zugriffsversuche und zur Gewährleistung der Systemsicherheit eignet.

Logs

SystemAccessSet parameterVADP

```
Aug 15 13:45:24 [RTSP SERVER]: Start one session, IP=192.168.200.1
Aug 15 13:45:56 last message repeated 3 times
Aug 15 13:55:41 [RTSP SERVER]: Stop one session, IP=192.168.200.1
Aug 20 23:35:02 [RTSP SERVER]: Start one session, IP=172.19.1.177
Aug 20 23:37:25 [RTSP SERVER]: Stop one session, IP=172.19.1.177
Jan 20 11:52:41 [RTSP SERVER]: Start one session, IP=172.19.11.180
Jan 20 11:52:43 [RTSP SERVER]: Stop one session, IP=172.19.11.180
Jan 20 12:00:50 [RTSP SERVER]: Start one session, IP=172.19.11.180
Jan 20 12:00:56 [RTSP SERVER]: Stop one session, IP=172.19.11.180
Jan 20 12:04:44 [RTSP SERVER]: Start one session, IP=172.19.11.180
Jan 20 12:58:13 [RTSP SERVER]: Start one session, IP=172.19.11.180
Jan 20 12:58:14 [RTSP SERVER]: Stop one session, IP=172.19.11.180
Jan 20 13:30:01 [RTSP SERVER]: Start one session, IP=172.19.11.180
Jan 20 13:30:25 [RTSP SERVER]: Stop one session, IP=172.19.11.180
Feb 4 12:00:46 [RTSP SERVER]: Start one session, IP=172.19.11.180
Feb 4 12:00:49 [RTSP SERVER]: Stop one session, IP=172.19.11.180
Dec 3 14:34:04 [RTSP SERVER]: Start one session, IP=172.19.11.180
Dec 3 14:35:14 [RTSP SERVER]: Stop one session, IP=172.19.11.180
Dec 3 14:35:16 [RTSP SERVER]: Start one session, IP=172.19.11.180
Dec 3 14:35:30 [RTSP SERVER]: Stop one session, IP=172.19.11.180
Dec 3 14:35:33 [RTSP SERVER]: Start one session, IP=172.19.11.180
Dec 3 14:35:33 [RTSP SERVER]: Stop one session, IP=172.19.11.180
Dec 3 14:35:35 [RTSP SERVER]: Start one session, IP=172.19.11.180
Dec 3 14:36:01 [RTSP SERVER]: Stop one session, IP=172.19.11.180
```

System

Parameter festlegen:

Es werden alle am System vorgenommenen Konfigurationsänderungen erfasst, um Benutzern bei der Überprüfung und Verwaltung von Anpassungen zu helfen und gleichzeitig die Fehlerbehebung bei konfigurationsbezogenen Problemen zu erleichtern.

Logs

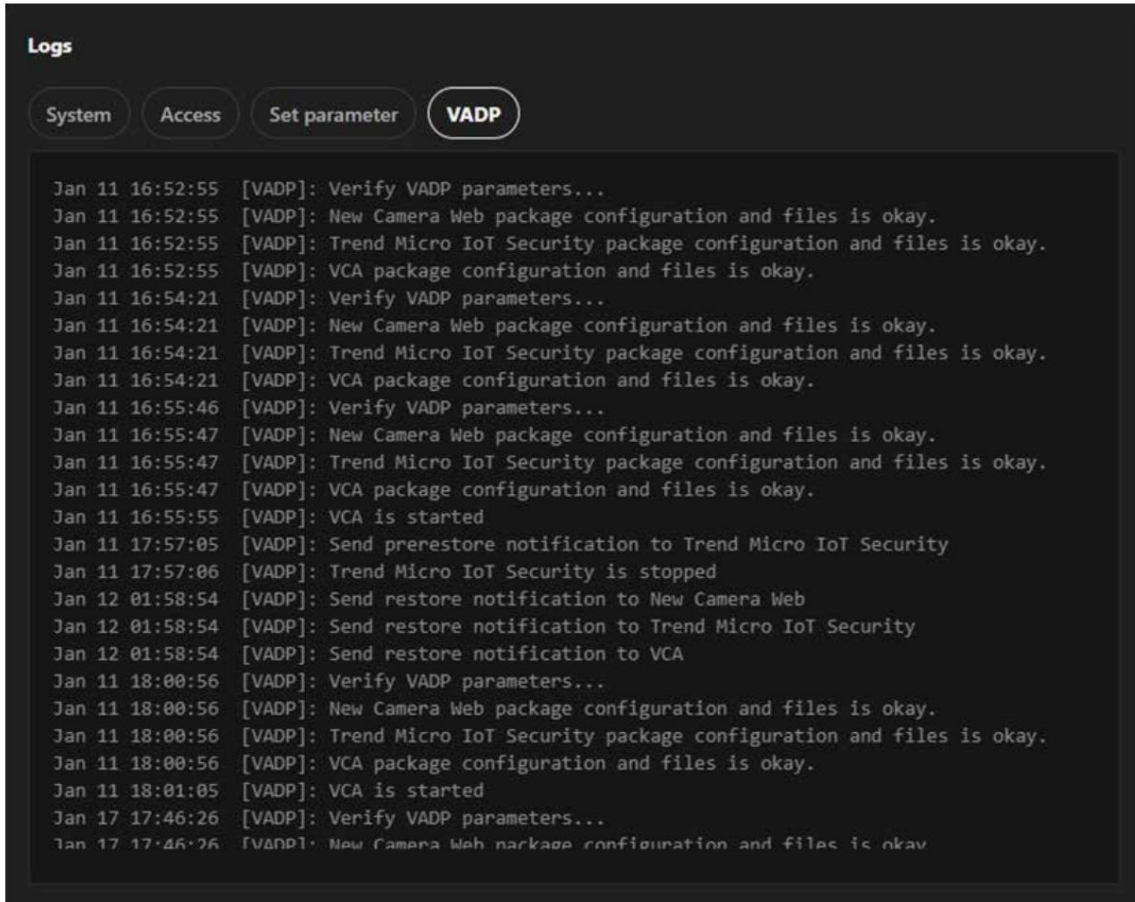
System Access **Set parameter** VADP

```
Jan 11 16:52:27 [CONFIGER]: Set videoin_c0_s0_overlay0_text_actualseize=30
Jan 11 16:52:27 [CONFIGER]: Set videoin_c0_s0_overlay1_text_actualseize=30
Jan 11 16:52:27 [CONFIGER]: Set videoin_c0_s0_overlay2_text_actualseize=30
Jan 11 16:52:27 [CONFIGER]: Set videoin_c0_s0_overlay3_text_actualseize=30
Jan 11 16:52:27 [CONFIGER]: Set videoin_c0_s1_overlay0_text_actualseize=24
Jan 11 16:52:27 [CONFIGER]: Set videoin_c0_s1_overlay1_text_actualseize=24
Jan 11 16:52:27 [CONFIGER]: Set videoin_c0_s1_overlay2_text_actualseize=24
Jan 11 16:52:27 [CONFIGER]: Set videoin_c0_s1_overlay3_text_actualseize=24
Jan 11 16:52:28 [CONFIGER]: Set videoin_c0_s2_overlay0_text_actualseize=20
Jan 11 16:52:28 [CONFIGER]: Set videoin_c0_s2_overlay1_text_actualseize=20
Jan 11 16:52:28 [CONFIGER]: Set videoin_c0_s2_overlay2_text_actualseize=20
Jan 11 16:52:28 [CONFIGER]: Set videoin_c0_s2_overlay3_text_actualseize=20
Jan 11 16:52:28 [CONFIGER]: Set videoin_c0_s0_overlay0_text_actualseize=30
Jan 11 16:52:28 [CONFIGER]: Set videoin_c0_s0_overlay1_text_actualseize=30
Jan 11 16:52:28 [CONFIGER]: Set videoin_c0_s0_overlay2_text_actualseize=30
Jan 11 16:52:28 [CONFIGER]: Set videoin_c0_s0_overlay3_text_actualseize=30
Jan 11 16:52:29 [CONFIGER]: Set videoin_c0_s1_overlay0_text_actualseize=24
Jan 11 16:52:29 [CONFIGER]: Set videoin_c0_s1_overlay1_text_actualseize=24
Jan 11 16:52:29 [CONFIGER]: Set videoin_c0_s1_overlay2_text_actualseize=24
Jan 11 16:52:29 [CONFIGER]: Set videoin_c0_s1_overlay3_text_actualseize=24
Jan 11 16:52:30 [CONFIGER]: Set status_c0_daynight=day
Jan 11 16:52:30 [CONFIGER]: Set videoin_c0_s2_overlay0_text_actualseize=20
Jan 11 16:52:30 [CONFIGER]: Set videoin_c0_s2_overlay1_text_actualseize=20
Jan 11 16:52:30 [CONFIGER]: Set videoin_c0_s2_overlay2_text_actualseize=20
Jan 11 16:52:30 [CONFIGER]: Set videoin_c0_s2_overlay3_text_actualseize=20
```

System

VADP:

Protokolle im Zusammenhang mit der VIVOTEK Anwendungsentwicklungsplattform, die die Ausführung von Anwendungen auf der Kamera dokumentieren (falls zutreffend) und bei der Diagnose von Problemen bei der Anwendungsentwicklung und Laufzeit helfen.



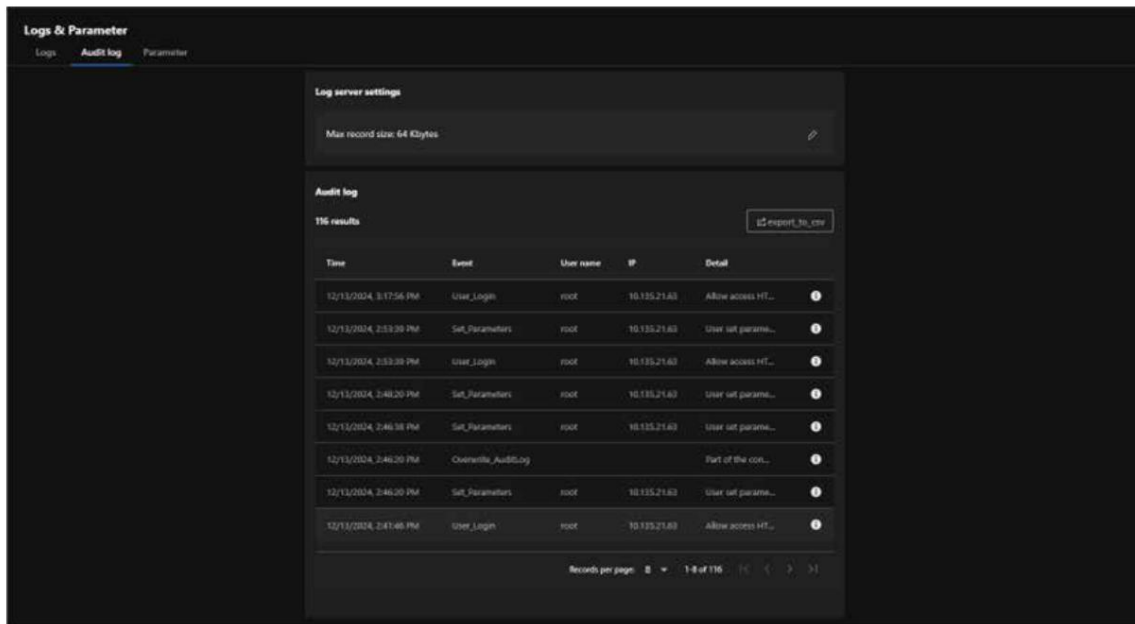
The screenshot shows a web interface for viewing logs. At the top, there's a 'Logs' header. Below it, there are four tabs: 'System', 'Access', 'Set parameter', and 'VADP'. The 'VADP' tab is currently selected and highlighted with a white border. Below the tabs, there is a scrollable area containing a list of log entries. Each entry consists of a timestamp and a message in square brackets. The messages describe various system events such as verifying parameters, checking package configurations for New Camera Web, Trend Micro IoT Security, and VCA, and starting/stopping services.

```
Jan 11 16:52:55 [VADP]: Verify VADP parameters...
Jan 11 16:52:55 [VADP]: New Camera Web package configuration and files is okay.
Jan 11 16:52:55 [VADP]: Trend Micro IoT Security package configuration and files is okay.
Jan 11 16:52:55 [VADP]: VCA package configuration and files is okay.
Jan 11 16:54:21 [VADP]: Verify VADP parameters...
Jan 11 16:54:21 [VADP]: New Camera Web package configuration and files is okay.
Jan 11 16:54:21 [VADP]: Trend Micro IoT Security package configuration and files is okay.
Jan 11 16:54:21 [VADP]: VCA package configuration and files is okay.
Jan 11 16:55:46 [VADP]: Verify VADP parameters...
Jan 11 16:55:47 [VADP]: New Camera Web package configuration and files is okay.
Jan 11 16:55:47 [VADP]: Trend Micro IoT Security package configuration and files is okay.
Jan 11 16:55:47 [VADP]: VCA package configuration and files is okay.
Jan 11 16:55:55 [VADP]: VCA is started
Jan 11 17:57:05 [VADP]: Send prerestore notification to Trend Micro IoT Security
Jan 11 17:57:06 [VADP]: Trend Micro IoT Security is stopped
Jan 12 01:58:54 [VADP]: Send restore notification to New Camera Web
Jan 12 01:58:54 [VADP]: Send restore notification to Trend Micro IoT Security
Jan 12 01:58:54 [VADP]: Send restore notification to VCA
Jan 11 18:00:56 [VADP]: Verify VADP parameters...
Jan 11 18:00:56 [VADP]: New Camera Web package configuration and files is okay.
Jan 11 18:00:56 [VADP]: Trend Micro IoT Security package configuration and files is okay.
Jan 11 18:00:56 [VADP]: VCA package configuration and files is okay.
Jan 11 18:01:05 [VADP]: VCA is started
Jan 17 17:46:26 [VADP]: Verify VADP parameters...
Jan 17 17:46:26 [VADP]: New Camera Web package configuration and files is okay
```

System

Das Audit-

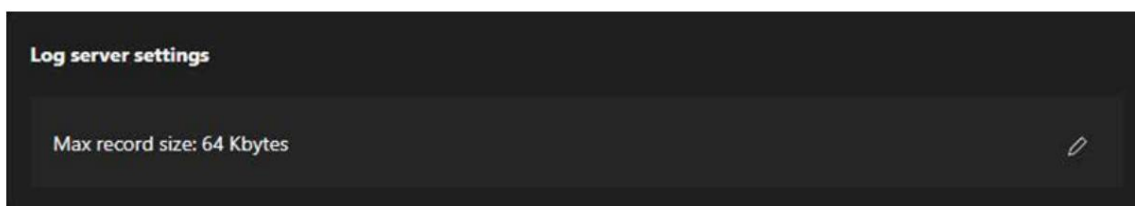
Protokoll zeichnet alle administrativen Vorgänge und Aktivitäten auf, die an der Kamera durchgeführt werden. Es dient dazu, das Nutzerverhalten zu verfolgen, die Systemsicherheit zu erhöhen, Transparenz im Management zu gewährleisten und Compliance-Anforderungen zu erfüllen. Durch die detaillierte Protokollierung von Nutzeraktionen unterstützt es Administratoren bei der Analyse von Problemen, der Fehlerbehebung und der Bereitstellung zuverlässiger historischer Daten für Audits.



Time	Event	User name	IP	Detail
12/11/2024, 9:17:56 PM	User_login	root	10.135.21.63	Allow access HT...
12/11/2024, 2:53:39 PM	Set_Parameters	root	10.135.21.63	User set param...
12/11/2024, 2:53:39 PM	User_login	root	10.135.21.63	Allow access HT...
12/11/2024, 2:46:20 PM	Set_Parameters	root	10.135.21.63	User set param...
12/11/2024, 2:46:38 PM	Set_Parameters	root	10.135.21.63	User set param...
12/11/2024, 2:46:20 PM	Overwrite_AuditLog			Part of the con...
12/11/2024, 2:46:20 PM	Set_Parameters	root	10.135.21.63	User set param...
12/11/2024, 2:41:45 PM	User_login	root	10.135.21.63	Allow access HT...

Die Einstellungen für den

Protokollserver ermöglichen es Benutzern, die Speicherkapazität für Protokolle anzupassen, um ausreichend Speicherplatz für die Aufzeichnung von Verwaltungsaktivitäten zu gewährleisten.



Log server settings
Max record size: 64 Kbytes

Audit-Protokoll

Enthält detaillierte Aufzeichnungen über jeden Verwaltungsvorgang, einschließlich der folgenden Felder:

Zeit:

Der genaue Zeitpunkt, zu dem die Handlung stattfand.

Ereignis:

Die Art der durchgeführten Aktion (z. B. „User_Login“ für Anmeldungen, „Set_Parameters“ für Parameteranpassungen).

Benutzername:

Der Benutzername der Person, die die Aktion ausführt (z. B. „root“).

IP:

Die IP-Adresse des Geräts, das die Aktion auslöst.

Detail:

Detaillierte Beschreibungen der Aktionen, wie z. B. „Zugriff über HTTP erlauben“ oder „Vom Benutzer festgelegte Parameter“.

System

Audit log					
116 results				export_to_csv	
Time	Event	User name	IP	Detail	
12/13/2024, 3:17:56 PM	User_Login	root	10.135.21.63	Allow access HT...	
12/13/2024, 2:53:39 PM	Set_Parameters	root	10.135.21.63	User set parame...	
12/13/2024, 2:53:39 PM	User_Login	root	10.135.21.63	Allow access HT...	
12/13/2024, 2:48:20 PM	Set_Parameters	root	10.135.21.63	User set parame...	
12/13/2024, 2:46:38 PM	Set_Parameters	root	10.135.21.63	User set parame...	
12/13/2024, 2:46:20 PM	Overwrite_AuditLog			Part of the con...	
12/13/2024, 2:46:20 PM	Set_Parameters	root	10.135.21.63	User set parame...	
12/13/2024, 2:41:46 PM	User_Login	root	10.135.21.63	Allow access HT...	
Records per page: 8 1-8 of 116 < < > >					

Exportfunktion: Mit der

Schaltfläche „**Exportieren nach CSV**“ können Benutzer Audit-Logs als CSV-Dateien exportieren, um sie zu archivieren, weiterzugeben oder weiter zu analysieren.

System

Anpassen des Erscheinungsbilds der Benutzeroberfläche und des Brandings mit Designeinstellungen

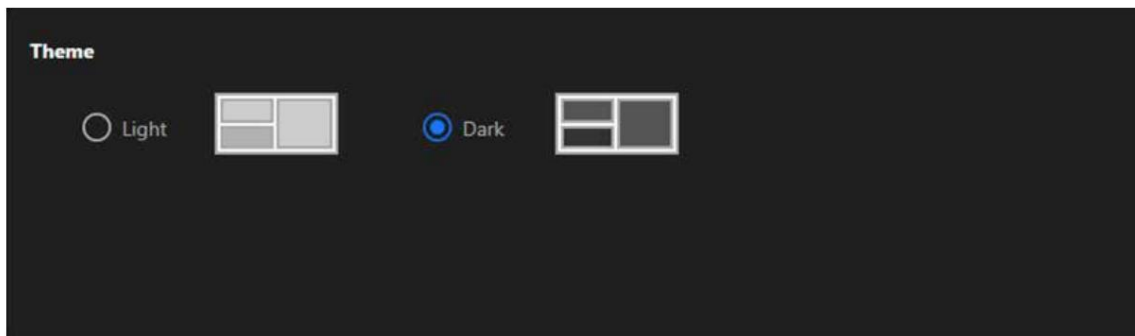
Im Bereich „Designeinstellungen“ können Nutzer die Benutzeroberfläche der Kamera an ihre Vorlieben anpassen und so das Nutzererlebnis optimieren. Durch die Möglichkeit, zwischen hellem und dunklem Modus zu wechseln, lässt sich die Oberfläche an unterschiedliche Lichtverhältnisse anpassen. Darüber hinaus ermöglicht die Option, ein eigenes Logo hochzuladen und einen Hyperlink zu konfigurieren, Unternehmen und Projekten, ihre Markenidentität direkt in der Systemoberfläche zu präsentieren. Diese Funktion vereint Funktionalität und Anpassbarkeit und gewährleistet so sowohl Benutzerfreundlichkeit als auch eine professionelle Darstellung.

Designeinstellungen

Die Designeinstellungen bestehen aus zwei Abschnitten: Design und Logo. Jeder Abschnitt bietet spezifische Anpassungsoptionen zur Verbesserung der Benutzerfreundlichkeit und des Brandings.

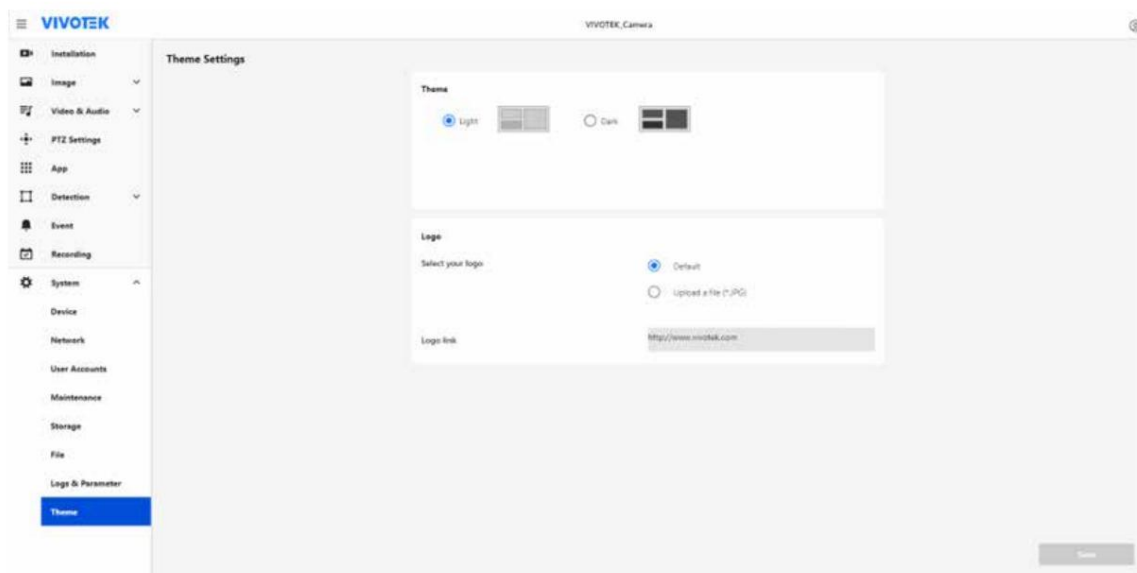
• Thema

Ermöglicht es dem Benutzer, zwischen hellen und dunklen Anzeigemodi der Benutzeroberfläche zu wechseln, um sich an unterschiedliche Arbeitsumgebungen anzupassen, wodurch der Benutzerkomfort erhöht und die Augenbelastung bei wechselnden Lichtverhältnissen reduziert wird.



Hellmodus:

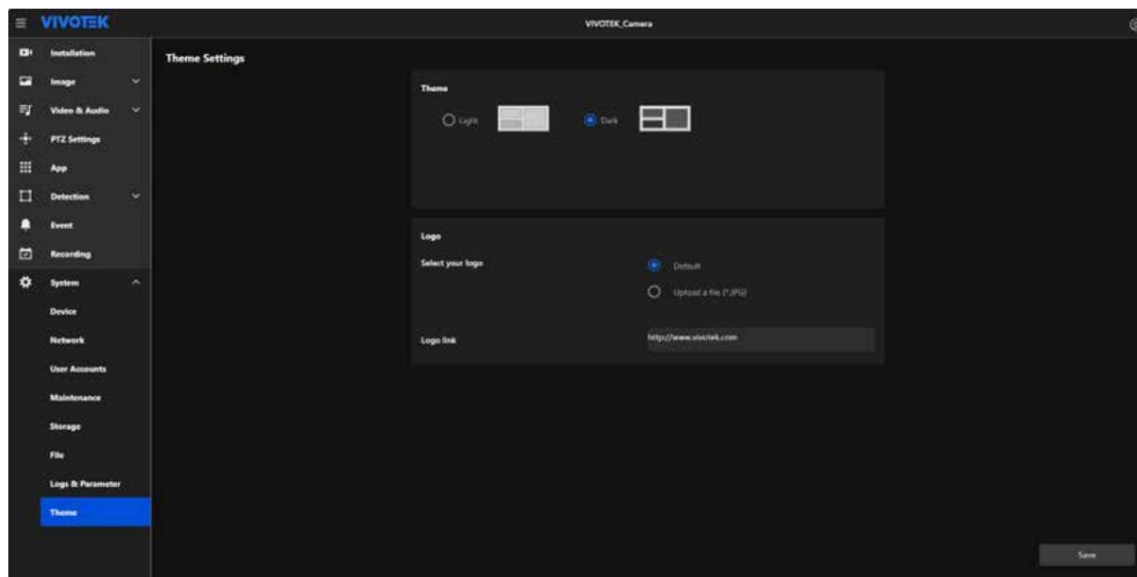
Mit hellem Hintergrund gestaltet, ideal für helle Umgebungen.



System

Dunkelmodus:

Verwendet einen dunklen Hintergrund, wodurch Blendeefekte reduziert und die Sichtbarkeit bei schlechten Lichtverhältnissen verbessert werden.



Bedienung:

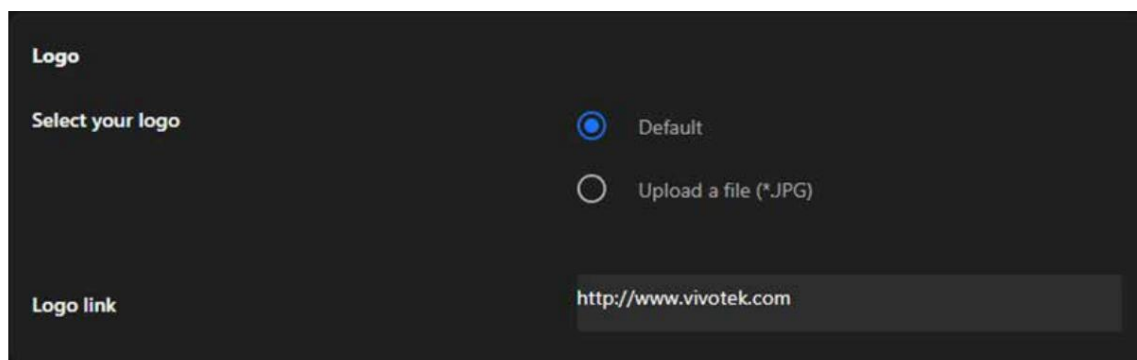
Schritt 1. Wählen Sie den gewünschten Modus (Hell oder Dunkel) durch Anklicken der entsprechenden Option.

Schritt 2. Die Vorschau der Benutzeroberfläche ändert sich dynamisch, um das ausgewählte Design widerzuspiegeln.

Schritt 3. Klicken Sie auf die Schaltfläche „Speichern“, um die Änderungen zu übernehmen.

Logo

Ermöglicht es Unternehmen oder Benutzern, die Benutzeroberfläche mit ihrem individuellen Logo zu personalisieren und so die Markenbekanntheit und Professionalität zu steigern. Gleichzeitig bietet es die Möglichkeit, einen anklickbaren Hyperlink für das Logo zu konfigurieren, der die Benutzer auf eine bestimmte Webseite weiterleitet, beispielsweise auf eine Unternehmenswebsite oder eine Supportseite.



Wählen Sie Ihr Logo aus:

Standard	Verwendet das im System integrierte Standardlogo.
Laden Sie eine Datei hoch (*.JPG)	Ermöglicht Benutzern das Hochladen einer benutzerdefinierten Logodatei im JPG-Format zur Personalisierung.

System

Logo-Link:

Ermöglicht es Benutzern, dem Logo einen Hyperlink zuzuweisen, der auf eine bestimmte Webseite (z. B. die Unternehmenswebsite) weiterleitet.

Notiz:

Anzeige

Das ausgewählte oder hochgeladene Logo wird in der Titelleiste der Benutzeroberfläche angezeigt und ist somit für alle Benutzer sichtbar. Durch Anklicken des Logos werden die Benutzer zur konfigurierten URL weitergeleitet.

