Netzwerkvideorekorder

Benutzerhandbuch

Rechtliche Hinweise

Über dieses Handbuch

Das Handbuch enthält Anweisungen zur Verwendung und Verwaltung des Produkts. Bilder, Diagramme und alle weiteren Informationen sind nur zur Beschreibung und Erklärung vorgesehen. Änderungen der im Handbuch enthaltenen Informationen aufgrund von Firmware-Aktualisierungen oder aus anderen Gründen bleiben jederzeit vorbehalten. Die neueste Version des Handbuchs finden Sie auf der Website von Hikvision (***https://www.hikvision.com/***).
Bitte verwenden Sie dieses Handbuch unter Anleitung und Unterstützung von Fachleuten, die für den Support des Produkts geschult sind.

Marken

HIKVISION und andere Marken und Logos von Hikvision sind das Eigentum von Hikvision in verschiedenen Ländern.
Andere hier erwähnte Marken und Logos sind Eigentum ihrer jeweiligen Inhaber.
HDMI: Die Begriffe „HDMI“ und „HDMI High-Definition Multimedia Interface“ sowie das HDMI-Logo sind Handelsnamen oder eingetragene Marken der HDMI Licensing Administrator, Inc., in den Vereinigten Staaten und anderen Ländern.

Haftungsausschluss

DIESES HANDBUCH UND DAS BESCHRIEBENE PRODUKT MIT SEINER HARDWARE, SOFTWARE UND FIRMWARE WERDEN, SOWEIT GESETZLICH ZULÄSSIG, IN DER „VORLIEGENDEN FORM“ UND MIT „ALLEN FEHLERN UND IRRTÜMERN“ BEREITGESTELLT. HIKVISION ÜBERNIMMT KEINE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN, EINSCHLIESSLICH, JEDOCH NICHT DARAUF BESCHRÄNKT, MARKTGÄNGIGKEIT, ZUFRIEDENSTELLENDE QUALITÄT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. DIE NUTZUNG DES PRODUKTS DURCH SIE ERFOLGT AUF IHRE EIGENE GEFAHR. IN KEINEM FALL IST HIKVISION IHNEN GEGENÜBER HAFTBAR FÜR BESONDERE, ZUFÄLLIGE, DIREKTE ODER INDIREKTE SCHÄDEN, EINSCHLIESSLICH, JEDOCH NICHT DARAUF BESCHRÄNKT, VERLUST VON GESCHÄFTSGEWINNEN, GESCHÄFTSUNTERBRECHUNG, DATENVERLUST, SYSTEMBESCHÄDIGUNG, VERLUST VON DOKUMENTATIONEN, SEI ES AUFGRUND VON VERTRAGSBRUCH, UNERLAUBTER HANDLUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT), PRODUKTHAFTUNG ODER ANDERWEITIG, IN VERBINDUNG MIT DER VERWENDUNG DIESES PRODUKTS, SELBST WENN HIKVISION ÜBER DIE MÖGLICHKEIT DERARTIGER SCHÄDEN ODER VERLUSTE INFORMIERT WAR.
SIE ERKENNEN AN, DASS DAS INTERNET VON SICH AUS EIN SICHERHEITSRISIKO DARSTELLT UND HIKVISION KEINE VERANTWORTUNG FÜR FUNKTIONSMÄNGEL, DATENSCHUTZLÜCKEN ODER ANDERE SCHÄDEN ÜBERNIMMT, DIE DURCH CYBER-ANGRIFFE, HACKER-ANGRIFFE, VIRUSINFEKTIONEN ODER ANDERE INTERNET-SICHERHEITSRISIKEN ENTSTEHEN; HIKVISION BIETET GEGEBENENFALLS JEDOCH SCHNELLE TECHNISCHE HILFE AN.
SIE STIMMEN ZU, DIESES PRODUKT GEMÄSS ALLEN GELTENDEN GESETZEN ZU VERWENDEN, UND

SIE SIND ALLEIN DAFÜR VERANTWORTLICH, DASS IHRE NUTZUNG DEN ANWENDBAREN GESETZEN ENTSPRICHT. INSBESONDERE SIND SIE VERANTWORTLICH FÜR DIE VERWENDUNG DIESES PRODUKTS AUF EINE WEISE, DIE KEINEN VERSTOSS GEGEN DIE RECHTE DRITTER DARSTELLT, EINSCHLIESSLICH, JEDOCH NICHT DARAUF BESCHRÄNKT, ÖFFENTLICHKEITSRECHTE, GEISTIGE EIGENTUMSRECHTE ODER DATENSCHUTZRECHTE. SIE DÜRFEN DIESES PRODUKT NICHT FÜR VERBOTENE ENDANWENDUNGEN VERWENDEN, EINSCHLIESSLICH DER ENTWICKLUNG ODER PRODUKTION VON MASSENVERNICHTUNGSWAFFEN, DER ENTWICKLUNG ODER PRODUKTION VON CHEMISCHEN ODER BIOLOGISCHEN WAFFEN, JEGLICHER AKTIVITÄTEN IN BEZUG AUF NUKLEARSPRENGSTOFFE ODER UNSICHERE KERNBRENNSTOFFKREISLÄUFE ODER ZUM MISSBRAUCH DER MENSCHENRECHTE.
BEI KONFLIKTEN ZWISCHEN DIESEM HANDBUCH UND GELTENDEM RECHT GILT LETZTERES.

Regulierungsinformationen

FCC-Informationen

Bitte beachten Sie, dass Änderungen oder Modifizierungen, die nicht ausdrücklich von der für die Einhaltung der Vorschriften verantwortlichen Partei genehmigt wurden, dazu führen können, dass die Betriebserlaubnis für das Gerät erlischt.
FCC-Konformität: Dieses Gerät wurde getestet und entspricht den Grenzwerten für digitale Geräte der Klasse A gemäß Teil 15 der FCC-Vorschriften. Diese Grenzwerte wurden erlassen, um einen angemessenen Schutz gegen nachteilige Störungen bei gewerblichen Installationen zu gewährleisten. Dieses Gerät erzeugt, nutzt und strahlt Funkfrequenzenergie ab und kann, sofern es nicht in Übereinstimmung mit der Bedienungsanleitung installiert und betrieben wird, Störungen der Funkkommunikation verursachen. Der Betrieb dieses Geräts in einem Wohnbereich führt möglicherweise zu Störungen; in diesem Fall hat der Nutzer auf seine Kosten für eine Behebung der Störungen zu sorgen.

FCC-Bedingungen

Dieses Gerät entspricht Abschnitt 15 der FCC- Bestimmungen. Der Betrieb ist unter den folgenden zwei Bedingungen gestattet:

1. Dieses Gerät darf keine Störungen verursachen.
2. Dieses Gerät muss empfangene Störungen aushalten, einschließlich jener, die zu einem unerwünschten Betrieb führen.

EU-Konformitätserklärung

CE

Dieses Produkt und – falls zutreffend – das mitgelieferte Zubehör sind mit dem „CE“-Zeichen gekennzeichnet und erfüllen daher die gültigen harmonisierten Europäischen Normen, die in der EMV-Richtlinie 2014/30/EU und der RoHS-Richtlinie 2011/65/EU aufgelistet sind.

2012/19/EU (Elektroaltgeräte-Richtlinie): Produkte, die mit diesem Symbol gekennzeichnet sind, dürfen innerhalb der Europäischen Union nicht mit dem Hausmüll entsorgt werden. Für ordnungsgemäßes Recycling geben Sie dieses Produkt an Ihren örtlichen Fachhändler zurück oder entsorgen Sie es an einer der Sammelstellen. Für weitere Informationen siehe: ***http://www.recyclethis.info***.

2006/66/EC (Batterierichtlinie): Dieses Produkt enthält eine Batterie, die innerhalb der Europäischen Union nicht über den Hausmüll entsorgt werden darf. Spezifische Hinweise zu Batterien siehe die Produktdokumentation. Die Batterie ist mit diesem Symbol gekennzeichnet, das zusätzlich die Kürzel „Cd“ für Cadmium, „Pb“ für Blei oder „Hg“ für Quecksilber enthalten kann. Für ordnungsgemäßes Recycling geben Sie die Batterie an Ihren örtlichen Fachhändler zurück oder entsorgen Sie sie an einer der Sammelstellen. Für

weitere Informationen siehe: ***http://www.recyclethis.info***.

Konformität mit Industry Canada ICES-003

Dieses Gerät erfüllt die Anforderungen der Normen CAN ICES-3 (A)/NMB-3(A).

Anwendbare Modelle

Dieses Handbuch gilt für die folgenden Modelle:

Tabelle 1-1 Anwendbare Modelle

Serie	Modell
DS-9600NI-I8(B)	DS-9608NI-I8(B)
	DS-9616NI-I8(B)
	DS-9632NI-I8(B)
	DS-9664NI-I8(B)
DS-9600NI-I16(B)	DS-9616NI-I16(B)
	DS-9632NI-I16(B)
	DS-9664NI-I16(B)
DS-9600NI-I8	DS-9608NI-I8
	DS-9616NI-I8
	DS-9632NI-I8
	DS-9664NI-I8
DS-9600NI-I16	DS-9616NI-I16
	DS-9632NI-I16
	DS-9664NI-I16
DS-8600NI-I8	DS-8608NI-I8
	DS-8616NI-I8
	DS-8632NI-I8
	DS-8664NI-I8
DS-8600NI-I8/24P	DS-8632NI-I8/24P
DS-7600NI-I2	DS-7608NI-I2
	DS-7616NI-I2
	DS-7632NI-I2
DS-7600NI-I2/P	DS-7608NI-I2/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P

Serie	Modell
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4(B)	DS-7716NI-I4(B)
	DS-7732NI-I4(B)
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
DS-7700NI-I4/P(B)	DS-7716NI-I4/P(B)
	DS-7732NI-I4/P(B)
DS-7800NI-I2	DS-7808NI-I2
	DS-7816NI-I2
	DS-7832NI-I2
DS-7800NI-I2/P	DS-7808NI-I2/8P
	DS-7816NI-I2/16P
	DS-7832NI-I2/16P
DS-7900NI-I4	DS-7916NI-I4
	DS-7932NI-I4
DS-7900NI-I4/P	DS-7916NI-I4/16P
	DS-7932NI-I4/16P
	DS-7932NI-I4/24P

Sicherheitshinweis

- Die ordnungsgemäße Konfiguration aller Passwörter und anderer Sicherheitseinstellungen liegt in der Verantwortung der installierenden Person und/oder des Endbenutzers.
- Bei der Verwendung des Produkts müssen die elektrischen Sicherheitsbestimmungen des Landes oder der Region strikt eingehalten werden.
- Drücken Sie den Stecker fest in die Steckdose. Schließen Sie nicht mehrere Geräte an ein Netzteil an. Schalten Sie das Gerät aus, bevor Sie Zubehörteile und Peripheriegeräte anschließen oder trennen.
- Stromschlaggefahr! Trennen Sie vor Wartungsarbeiten alle Stromquellen.
- Das Gerät muss an eine geerdete Netzsteckdose angeschlossen werden.
- Die Steckdose sollte sich in der Nähe des Geräts befinden und muss einfach zugänglich sein.
- ϟ weist auf gefährliche Spannung hin, sodass die an die Klemmen angeschlossene externe Verkabelung von einer fachkundigen Person installiert werden muss.
- Stellen Sie das Gerät niemals an einem instabilen Ort auf. Es könnte umfallen und schwere oder sogar tödliche Verletzungen verursachen.
- Die Eingangsspannung muss SELV (Schutzkleinspannung) und LPS (Stromquelle mit begrenzter Leistung) nach IEC60950-1 entsprechen.
- Hoher Berührungsstrom! Vor Anschluss an die Stromversorgung erden.
- Sollten sich Rauch, Gerüche oder Geräusche in dem Gerät entwickeln, so schalten Sie es unverzüglich aus und ziehen Sie den Netzstecker; dann wenden Sie sich an den Kundendienst.
- Verwenden Sie das Gerät möglichst in Verbindung mit einer unterbrechungsfreien Stromversorgung (USV) und verwenden Sie eine vom Hersteller empfohlene Festplatte.
- Dieses Produkt enthält eine Knopfzellenbatterie. Wird die Batterie verschluckt, kann dies innerhalb von 2 Stunden zu schweren inneren Verätzungen und zum Tod führen.
- Das Gerät ist nicht für den Einsatz an Orten geeignet, an denen sich wahrscheinlich Kinder aufhalten.
- VORSICHT: Bei einem Austausch der Batterie durch einen falschen Typ besteht Explosionsgefahr.
- Unsachgemäßer Austausch der Batterien durch einen falschen Typ kann eine Schutzvorrichtung umgehen (z. B. bei einigen Lithium-Batterietypen).
- Entsorgen Sie Batterien nicht durch Verbrennen, in einem heißen Ofen oder durch Zerkleinern oder Zerschneiden. Das kann zu einer Explosion führen.
- Bewahren Sie Batterien nicht in einer Umgebung mit extrem hoher Temperatur auf. Das kann zu einer Explosion oder zum Auslaufen von entflammbarer Flüssigkeit oder Gas führen.
- Setzen Sie Batterien keinem extrem niedrigen Luftdruck aus. Das kann zu einer Explosion oder zum Auslaufen von entflammbarer Flüssigkeit oder Gas führen.
- Gebrauchte Batterien vorschriftsgemäß entsorgen.
- Halten Sie Körperteile von Lüfterflügeln und Motoren fern. Unterbrechen Sie die Stromversorgung während der Wartung.
- Halten Sie Körperteile von den Motoren fern. Unterbrechen Sie die Stromversorgung während der Wartung.

Sicherheits- und Warnhinweise

Bevor Sie Ihr Gerät anschließen und in Betrieb nehmen, beachten Sie bitte die folgenden Hinweise:

- Das Gerät ist nur zur Verwendung in Innenräumen bestimmt. Installieren Sie es in einer gut belüfteten, staubfreien und trockenen Umgebung.
- Achten Sie darauf, dass der Rekorder ordnungsgemäß in einem Baugruppenträger oder Regal befestigt ist. Schwere Stöße infolge von Stürzen können zur Schäden an der empfindlichen Elektronik im Rekorder führen.
- Schützen Sie das Gerät vor tropfenden oder spritzenden Flüssigkeiten. Auf dem Gerät dürfen keine mit Flüssigkeit gefüllten Gegenstände, wie z. B. Vasen, abgestellt werden.
- Stellen Sie keine offenen Feuerquellen (wie brennende Kerzen) auf dem Gerät ab.
- Die Belüftung darf nicht durch Abdecken der Lüftungsöffnungen mit Gegenständen behindert werden, wie z. B. Zeitungen, Tischdecken, Vorhänge usw. Die Öffnungen dürfen niemals dadurch blockiert werden, dass das Gerät auf ein Bett, ein Sofa, einen Teppich oder eine ähnliche Oberfläche gestellt wird.
- Bei bestimmten Modellen müssen Sie die korrekte Verkabelung der Klemmen für den Anschluss an ein Wechselstromnetz beachten.
- Bestimmte Modelle wurden ggf. für den Anschluss an ein IT-Stromverteilungssystem angepasst.
-  kennzeichnet den Batteriehalter selbst und zeigt die Position der Zelle(n) innerhalb des Batteriehalters an.
- + kennzeichnet den/die Pluspol(e) von Geräten, die mit Gleichstrom betrieben werden oder Gleichstrom erzeugen. – kennzeichnet den/die Minuspol(e) von Geräten, die mit Gleichstrom betrieben werden oder Gleichstrom erzeugen.
- Lassen Sie für eine ausreichende Belüftung mindestens 200 mm (7,87“) Platz zwischen Gerät und Umgebung.
- Bei bestimmten Modellen müssen Sie die korrekte Verkabelung der Klemmen für den Anschluss an ein Wechselstromnetz beachten.
- Verwenden Sie nur die im Benutzerhandbuch bzw. in den Benutzerhinweisen aufgeführten Netzteile.
- Der USB-Anschluss des Geräts wird nur zum Anschließen einer Maus, einer Tastatur, eines USB-Sticks oder eines WLAN-Dongles verwendet.
- Verwenden Sie nur die im Benutzerhandbuch bzw. in den Benutzerhinweisen aufgeführten Netzteile.
- Berühren Sie keine scharfen Kanten oder Ecken.

Dokument-Konventionen

Um die Beschreibung zu vereinfachen, lesen Sie bitte die folgenden Konventionen.

- „Rekorder“ oder „Gerät“ bezieht sich hauptsächlich auf Videorekorder.
- „IP-Gerät“ bezieht sich hauptsächlich auf Netzwerkkameras (IP-Kamera), IP-Dome (Speed Dome), DVS (Digital Video Server) oder NVS (Network Video Server).
- „Kanal“ bezieht sich hauptsächlich auf den Videokanal im Videorekorder.

Symbol-Konventionen

Die in diesem Dokument verwendeten Symbole sind wie folgt definiert.

Symbol	Beschreibung
Vorsicht	Weist auf eine gefährliche Situation hin, die bei Nichtbeachtung der Warnung zu Tod oder schweren Verletzungen führen kann.
Achtung	Weist auf eine potenziell gefährliche Situation hin, die bei Nichtbeachtung der Warnung zu Schäden am Gerät, Datenverlust, Leistungsminderung oder unerwarteten Ergebnissen führen kann.
Hinweis	Liefert zusätzliche Informationen zur Betonung oder Ergänzung wichtiger Punkte im Text.

Inhalt

Kapitel 1 Grundlegende Funktionsweise

1.1 Aktivieren Sie Ihr Gerät

1.1.1 Standardbenutzer und IP-Adresse

- Standard-Administratorkonto: admin.
- Standard-IPv4-Adresse: 192.168.1.64.

1.1.2 Aktivierung über das lokale Menü

Für den erstmaligen Zugang müssen Sie das Gerät aktivieren, indem Sie ein Admin-Passwort einrichten. Vor der Aktivierung ist kein Betrieb möglich. Sie können das Gerät ebenfalls über Webbrowser, SADP oder Client-Software aktivieren.

Schritte

1. Geben Sie das Admin-Passwort zweimal ein.

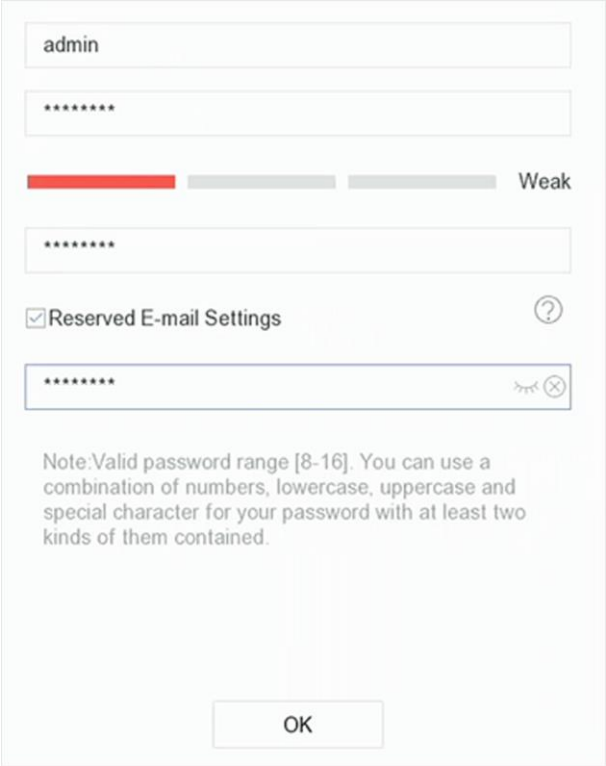


Abbildung 1-1 Aktivierung über das lokale Menü

Warnung

Wir empfehlen dringend, dass Sie ein starkes Passwort eigener Wahl erstellen (mindestens 8 Zeichen, einschließlich mindestens drei der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Wir empfehlen weiterhin, dass Sie Ihr Passwort regelmäßig monatlich oder wöchentlich zurücksetzen, insbesondere im Hochsicherheitssystem, um die Sicherheit Ihres Produkts zu erhöhen.

2. Geben Sie das Passwort ein, um die IP-Kameras zu aktivieren.
3. Optional: Aktivieren Sie **Reserved E-mail Settings**, um das Passwort später zurücksetzen zu können.
4. Klicken Sie auf **OK**.

Hinweis

Nachdem das Gerät aktiviert wurde, müssen Sie das Passwort sorgfältig aufbewahren.

Was folgt als Nächstes

Wenn Sie **Reserved E-mail Settings** aktiviert haben, legen Sie die für die Passwortrücksetzung reservierte E-Mail-Adresse fest.

1.1.3 Aktivierung über SADP

Die SADP-Software wird zur Erkennung des Onlinegeräts, zur Aktivierung des Geräts und zum Zurücksetzen des Passworts benötigt.

Bevor Sie beginnen

Sie finden die SADP-Software auf dem mitgelieferten Datenträger oder können sie von der offiziellen Website herunterladen. Installieren Sie sie gemäß den Anweisungen.

Schritte

1. Schließen Sie das Netzteil des Videorekorders an eine Steckdose an und schalten Sie ihn ein.
2. Führen Sie die SADP-Software aus, um nach Onlinegeräten zu suchen.
3. Überprüfen Sie den Rekorderstatus in der Geräteliste und wählen Sie den inaktiven Rekorder aus.

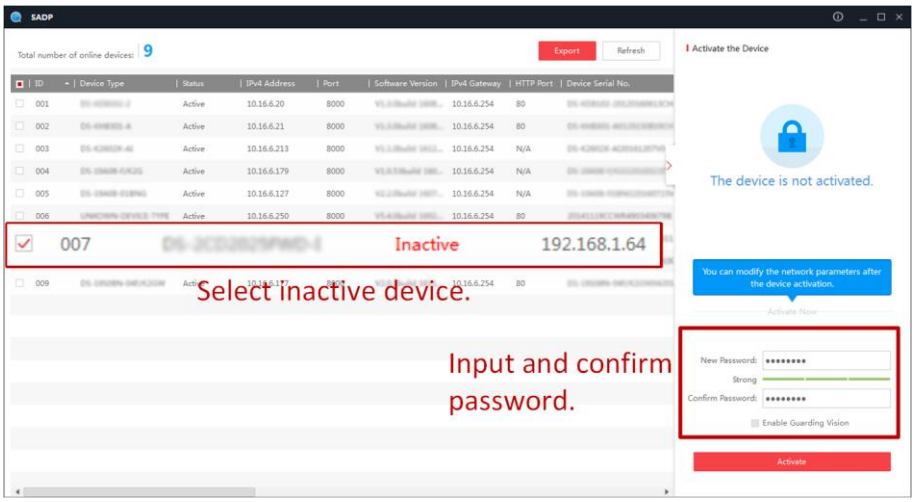


Abbildung 1-2 Aktivierung über SADP

4. Legen Sie ein Passwort fest und geben Sie es in das Passwortfeld ein. Bestätigen Sie das Passwort anschließend.

Hinweis

Wir empfehlen dringend, dass Sie ein starkes Passwort eigener Wahl erstellen (mindestens 8 Zeichen, einschließlich mindestens drei der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Wir empfehlen weiterhin, dass Sie Ihr Passwort regelmäßig monatlich oder wöchentlich zurücksetzen, insbesondere im Hochsicherheitssystem, um die Sicherheit Ihres Produkts zu erhöhen.

5. Klicken Sie auf **Activate**.

1.1.4 Aktivieren über die Client-Software

Bei der Client-Software handelt es sich um eine vielseitige Software zur Videoverwaltung für zahlreiche verschiedene Geräte.

Bevor Sie beginnen

Sie finden die Client-Software auf dem mitgelieferten Datenträger oder können sie von der offiziellen Website herunterladen. Installieren Sie sie gemäß den Anweisungen.

Schritte

1. Führen Sie die Client-Software aus. Die Systemsteuerung wird angezeigt, wie unten dargestellt.

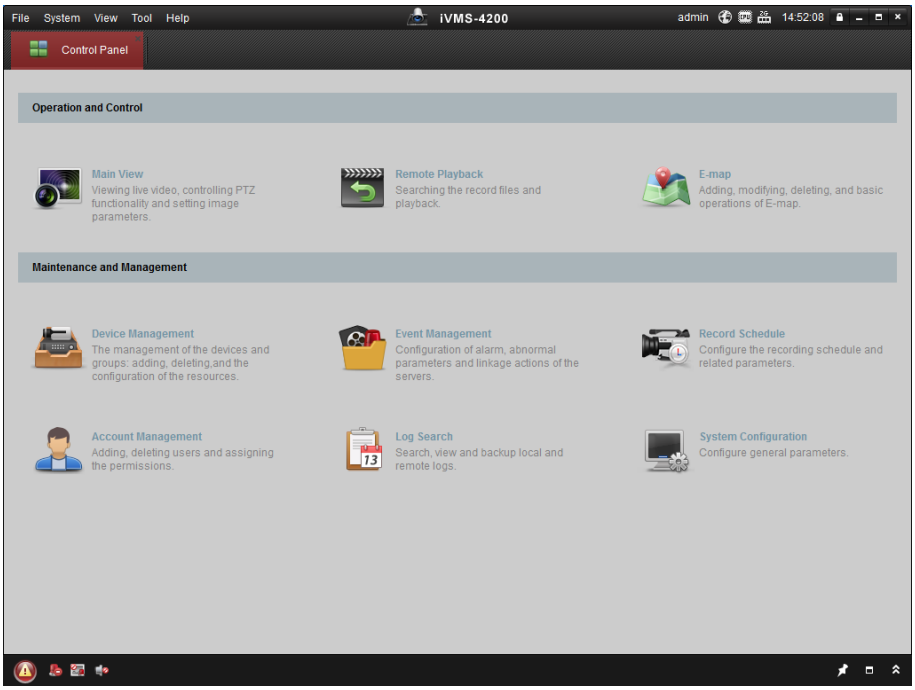


Abbildung 1-3 Systemsteuerung

2. Klicken Sie auf **Device Management**, um das entsprechende Menü aufzurufen, wie unten dargestellt.

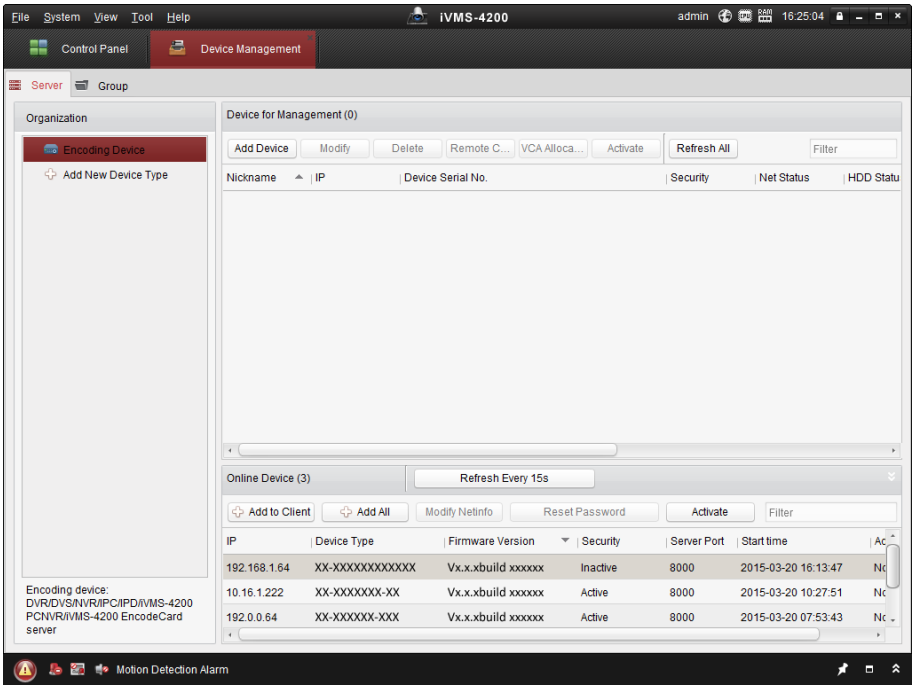


Abbildung 1-4 Menü für die Geräteverwaltung

3. Überprüfen Sie den Rekorderstatus in der Geräteliste und wählen Sie einen inaktiven Rekorder aus.
4. Klicken Sie auf **Activate**. Der Aktivierungsdialog wird angezeigt.

5. Legen Sie ein Passwort fest und geben Sie es in das entsprechende Feld ein. Bestätigen Sie das Passwort anschließend.

Hinweis

Wir empfehlen dringend, dass Sie ein starkes Passwort eigener Wahl erstellen (mindestens 8 Zeichen, einschließlich mindestens drei der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Wir empfehlen weiterhin, dass Sie Ihr Passwort regelmäßig monatlich oder wöchentlich zurücksetzen, insbesondere im Hochsicherheitssystem, um die Sicherheit Ihres Produkts zu erhöhen.

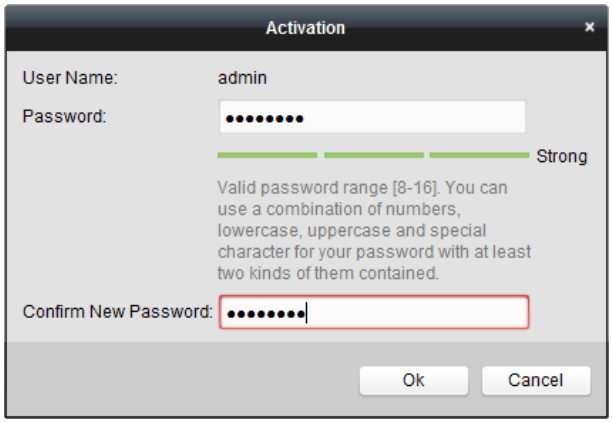


Abbildung 1-5 Aktivierung

6. Klicken Sie auf **OK**, um die Aktivierung zu starten.
7. Klicken Sie auf **Modify Netinfo**, damit der Dialog zum Ändern von Netzwerkeinstellungen angezeigt wird, wie unten dargestellt.

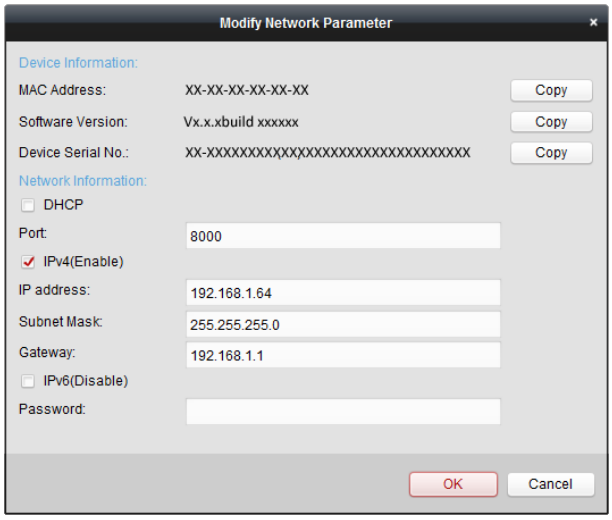


Abbildung 1-6 Netzwerkparameter ändern

8. Ändern Sie die IP-Adresse des Rekorders so, dass das Subnetz dem Computer entspricht. Ändern Sie die IP-Adresse manuell. Aktivieren Sie das Kontrollkästchen **Enable DHCP**.
9. Geben Sie das Passwort ein, um Ihre Änderung der IP-Adresse zu aktivieren.

1.1.5 Aktivierung über den Webbrowser

Der Zugriff auf den Rekorder kann über einen Webbrowser erfolgen. Sie können einen der folgenden Webbrowser verwenden: Internet Explorer 6.0 und höher, Apple Safari, Mozilla Firefox oder Google Chrome. Zu den unterstützten Auflösungen gehören 1024x768 und höher.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie sich im selben Netzwerksegment wie Ihr Gerät befinden.

Schritte

1. Geben Sie die IP-Adresse im Webbrowser ein und drücken Sie die **Eingabetaste**.

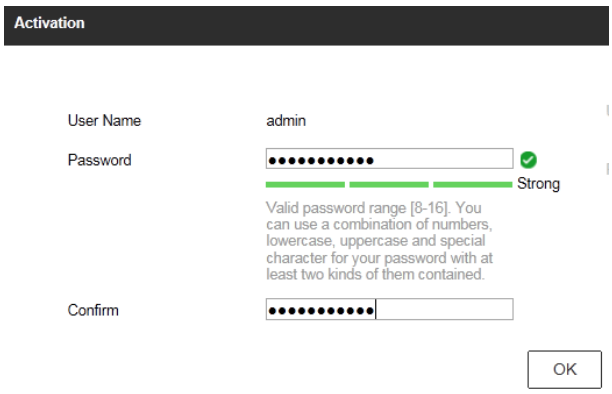


Abbildung 1-7 Aktivierung per Webbrowser

2. Stellen Sie das Passwort für das Admin-Benutzerkonto ein.

Hinweis

Wir empfehlen dringend, dass Sie ein starkes Passwort eigener Wahl erstellen (mindestens 8 Zeichen, einschließlich mindestens drei der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Wir empfehlen weiterhin, dass Sie Ihr Passwort regelmäßig monatlich oder wöchentlich zurücksetzen, insbesondere im Hochsicherheitssystem, um die Sicherheit Ihres Produkts zu erhöhen.

3. Klicken Sie auf **OK**.
4. Optional: Legen Sie die Sicherheitsfragen und die E-Mail für die Passwortwiederherstellung fest oder exportieren Sie die GUID-Datei für das Zurücksetzen des Passworts.
5. Klicken Sie auf **OK**.
6. Installieren Sie das Plugin, bevor Sie das Live-Video ansehen und das Gerät verwalten. Möglicherweise müssen Sie den Webbrowser schließen, um die Installation des Plugins abzuschließen.

1.2 Konfigurieren der TCP/IP-Einstellungen

Die TCP/IP-Einstellungen müssen ordnungsgemäß konfiguriert sein, bevor das Gerät über ein Netzwerk betrieben werden kann. Sowohl IPv4 als auch IPv6 sind verfügbar.

Schritte

1. Gehen Sie zu **System** → **Network** → **TCP/IP**.

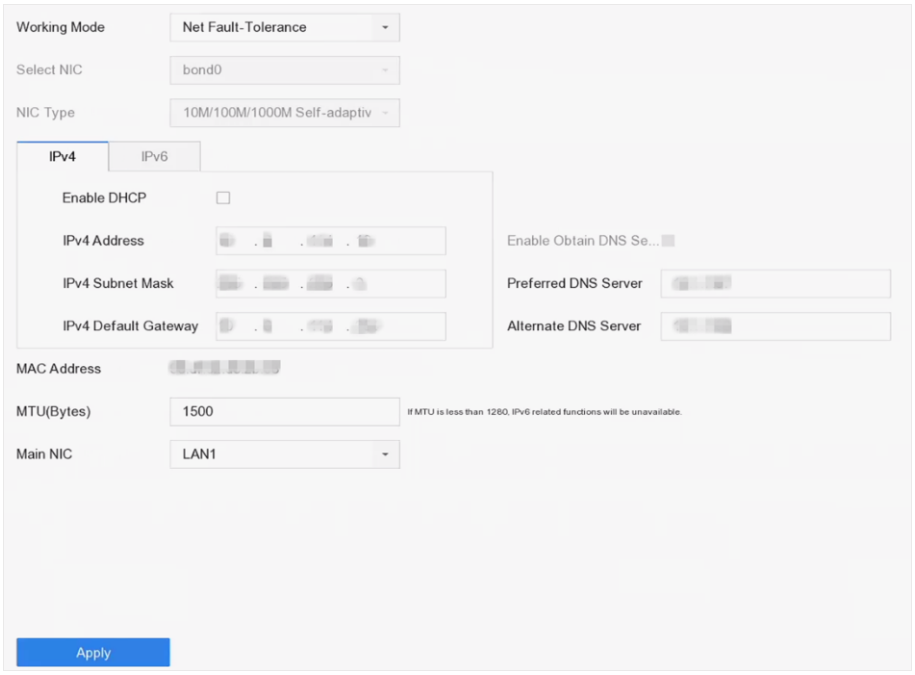


Abbildung 1-8 TCP/IP-Einstellungen

2. Stellen Sie **Working Mode** auf **Net-Fault Tolerance** oder **Multi-Address Mode** ein.

   Netzwerkfehlertoleranz

   Die beiden NIC-Karten verwenden die gleiche IP-Adresse, und Sie können „LAN1“ oder „LAN2“ als Haupt-NIC wählen. Auf diese Weise aktiviert das Gerät bei Ausfall einer NIC-Karte automatisch die andere Standby-NIC-Karte, um den Normalbetrieb des Systems zu gewährleisten.

   Multi-Adressenmodus

   Die Parameter der beiden NIC-Karten können unabhängig voneinander konfiguriert werden. Sie können „LAN1“ oder „LAN2“ unter „Select NIC for parameter settings“ wählen. Wählen Sie eine NIC-Karte als Standardroute. Wenn sich das System mit dem Extranet verbindet, werden die Daten über die Standardroute weitergeleitet.
3. Klicken Sie auf **IPv4** oder **IPv6**.
4. Legen Sie die entsprechenden Parameter fest.
5. Klicken Sie auf **Apply**.

Hinweis

- Aktivieren Sie das Kontrollkästchen **Enable DHCP**, um IP-Einstellungen automatisch zu erhalten, wenn ein DHCP-Server im Netzwerk verfügbar ist.
- Der gültige MTU-Wertebereich ist 500 bis 9676.

1.3 Festplatteneinstellungen

Stellen Sie sicher, dass die Speichermedien des Videorekorders in Ordnung sind. Sie können mindestens eine Festplatte installieren und initialisieren oder ein RAID erstellen und initialisieren.

1.4 Netzwerkkamera hinzufügen

Bevor Sie Live-Videos empfangen oder Videodateien aufnehmen können, müssen Sie die Netzwerkkameras zur Verbindungsliste des Geräts hinzufügen.

Bevor Sie beginnen

Vergewissern Sie sich, dass die Netzwerkverbindung gültig und korrekt ist und dass die hinzuzufügende IP-Kamera aktiviert ist.

Schritte

1. Klicken Sie in der Menüleiste auf .
2. Klicken Sie in der Titelleiste auf die Registerkarte **Custom Add**.

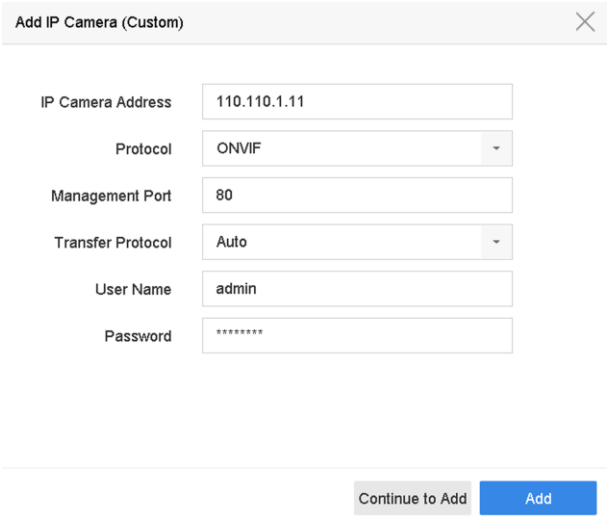


Abbildung 1-9 IP-Kamera hinzufügen

3. Geben Sie IP-Adresse, Protokoll, Verwaltungsport und weitere Informationen zur IP-Kamera ein.
4. Geben Sie den Anmeldebenutzernamen und das Passwort der IP-Kamera ein.
5. Klicken Sie auf **Add**, um das Hinzufügen der IP-Kamera zu beenden.
6. Optional: Klicken Sie auf **Continue to Add**, um weitere IP-Kameras hinzuzufügen.

1.4.1 Automatische Suche der Online-Netzwerkkamera hinzufügen

Schritte

1. Klicken Sie im Hauptmenü auf .
2. Klicken Sie unten auf **Number of Unadded Online Device**.
3. Wählen Sie die automatisch gesuchten Online-Netzwerkkameras.
4. Klicken Sie auf **Add**, um die Kamera mit dem gleichen Anmeldepasswort wie der Videorekorder hinzuzufügen.

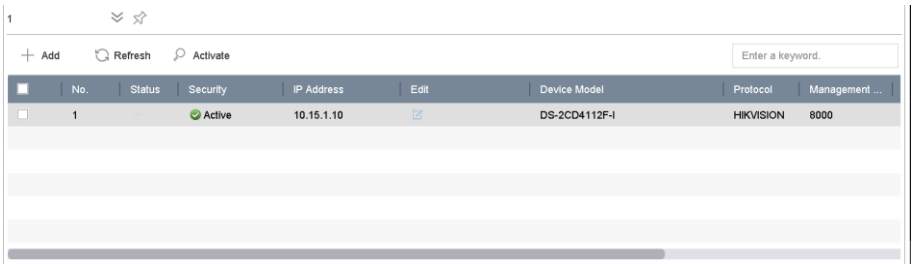


Abbildung 1-10 Automatisch gesuchte Online-Netzwerkkamera hinzufügen

Hinweis

Wurde die hinzuzufügende Netzwerkkamera nicht aktiviert, können Sie sie in der Liste der Netzwerkkameras im Kamera-Management aktivieren.

1.4.2 Netzwerkkamera manuell hinzufügen

Bevor Sie Live-Videos ansehen oder Videodateien aufnehmen können, müssen Sie dem Gerät Netzwerkkameras hinzufügen.

Bevor Sie beginnen

Stellen Sie sicher, dass die Netzwerkverbindung gültig und korrekt ist und die Netzwerkkamera aktiviert ist.

Schritte

1. Klicken Sie im Hauptmenü auf .
2. Klicken Sie auf **Custom Adding**.
3. Legen Sie folgende Parameter fest: **IP Camera Address**, **Protocol**, **Management Port**, **Transfer Protocol**, **User Name** und **Password**. Es kann eine Management-Portnummer von 1 bis 65535 eingestellt werden.

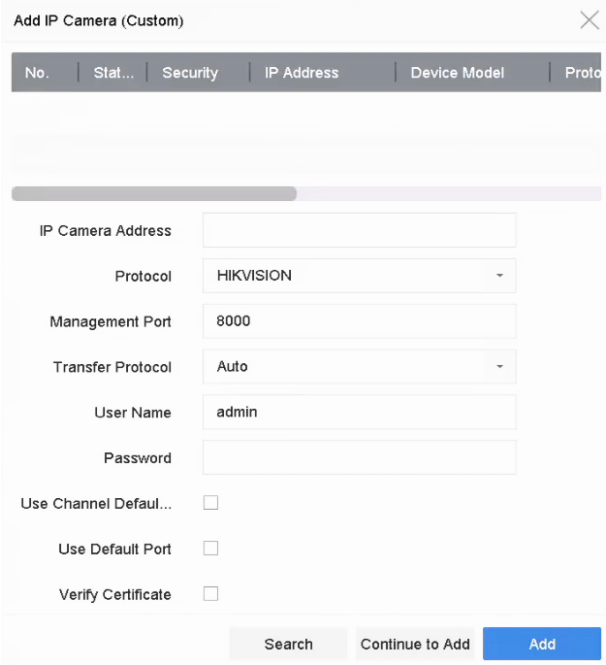


Abbildung 1-11 Netzwerkkamera hinzufügen

4. Optional: Aktivieren Sie das Kontrollkästchen **Use Channel Default Password**, um das Standardpasswort zum Hinzufügen der Kamera zu verwenden.
5. Optional: Aktivieren Sie das Kontrollkästchen **Use Default Port**, um den Standard-Verwaltungsport zum Hinzufügen der Kamera zu verwenden. Für den SDK-Dienst ist der Standardportwert 8000. Für den erweiterten SDK-Dienst ist der Standardwert 8443.

Hinweis

Die Funktion ist nur verfügbar, wenn Sie das HIKVISION-Protokoll verwenden.

6. Optional: Aktivieren Sie das Kontrollkästchen **Verify Certificate**, um die Kamera mit Zertifikat zu verifizieren. Das Zertifikat dient als Identifizierung für die Kamera mit besser gesicherter Authentifizierung. Bei der Verwendung dieser Funktion muss zuerst das Netzwerkkamera-Zertifikat auf das Gerät importiert werden. Einzelheiten siehe .

Hinweis

Die Funktion ist nur verfügbar, wenn Sie das HIKVISION-Protokoll verwenden.

7. Klicken Sie auf **Add**.
8. Optional: Wählen Sie **Continue to Add**, um weitere Netzwerkkameras hinzuzufügen.

1.4.3 Netzwerkkamera über PoE hinzufügen

Die PoE-Schnittstellen ermöglichen es dem Gerätesystem, die elektrische Energie sicher über das Ethernetkabel an die angeschlossenen PoE-Kameras weiterzuleiten. Die Anzahl unterstützter PoE-

Kameras variiert je nach Gerätemodul. Wenn Sie den PoE-Port deaktivieren, können Sie die Online-Netzwerkkameras ebenfalls verbinden. Der PoE-Port unterstützt die Plug-and-Play-Funktion.

PoE-Kamera hinzufügen

Schritte

1. Gehen Sie zu **Camera** → **Camera** → **PoE Settings**.
2. Aktivieren oder deaktivieren Sie den Langstrecken-Netzwerkkabelmodus durch Auswahl von **Long Distance** oder **Short Distance**.

   Langstreckenübertragung

   Langstrecken-Netzwerkübertragung (100 bis 300 m) über PoE-Schnittstelle.

   Kurzstreckenübertragung

   Kurzstrecken-Netzwerkübertragung (< 100 m) über die PoE-Schnittstelle.

Hinweis

- Die PoE-Ports sind standardmäßig im Kurzstreckenmodus aktiviert.
- Die Bandbreite der am PoE-Port über langes Netzwerkkabel (100 bis 300 m) angeschlossenen IP-Kamera darf 6 MP nicht überschreiten.
- Die zulässige maximale Länge des Netzwerkkabels ist möglicherweise kleiner als 300 m, je nach IP-Kameramodell und dem Kabelmaterial.
- Wenn die Übertragungsreichweite 100 bis 250 m erreicht, müssen Sie ein CAT5E- oder CAT6-Netzwerkkabel für den Anschluss am PoE-Port verwenden.
- Wenn die Übertragungsreichweite 250 bis 300 m erreicht, müssen Sie ein CAT6-Netzwerkkabel für den Anschluss am PoE-Port verwenden.
- Eine Liste der IP-Kameras, die über ein langes Netzwerkkabel mit PoE verbunden sind (100 bis 300 m), finden Sie in Anhang 20.3.

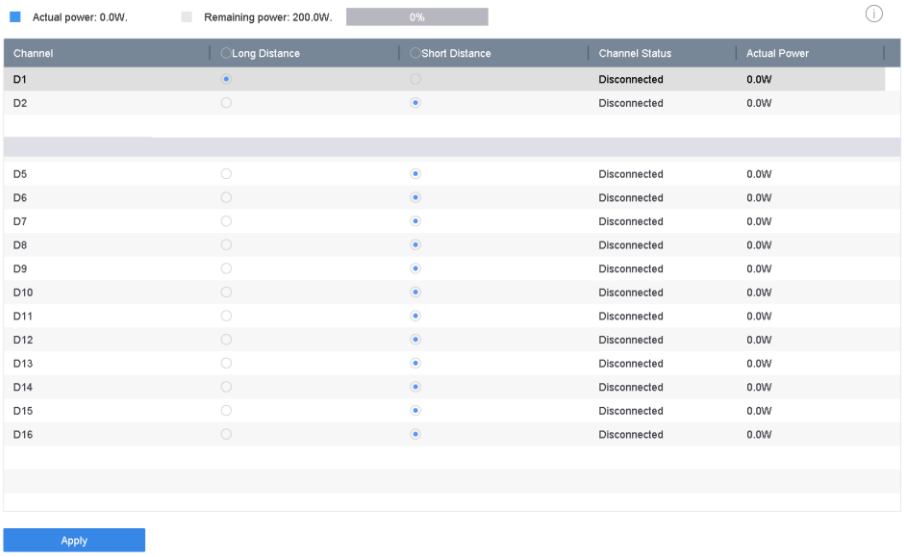


Abbildung 1-12 PoE-Kamera hinzufügen

3. Klicken Sie auf **Apply**.
4. Schließen Sie die PoE-Kameras über Netzwerkkabel an die Geräte-PoE-Ports an.
5. Gehen Sie zu **Camera** → **Camera** → **IP Camera**, um Kamerabild und Informationen abzurufen.

Nicht-PoE-Netzwerkkamera hinzufügen

Sie können den PoE-Port deaktivieren, indem Sie „Manual“ wählen, wobei der aktuelle Kanal als normaler Kanal verwendet werden kann und die Parameter ebenfalls bearbeitet werden können.

Schritte

1. Gehen Sie zu **Camera** → **Camera** → **IP Camera**.
2. Führen Sie den Mauszeiger auf ein Fenster ohne verbundene IP-Kamera und klicken Sie auf .

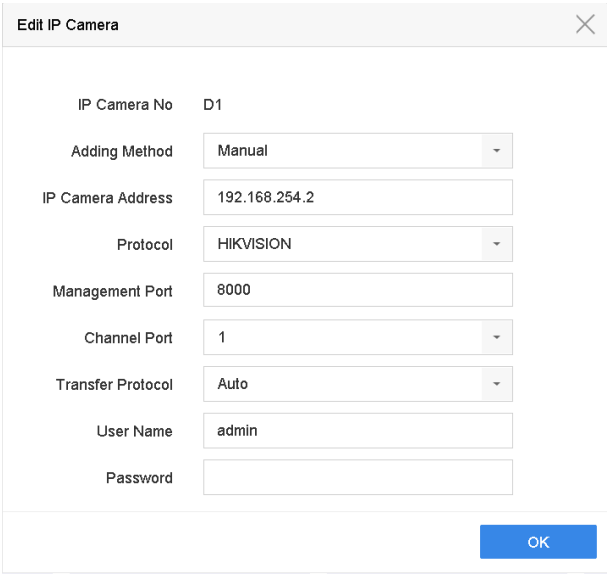


Abbildung 1-13 Netzwerkkamera bearbeiten

3. Wählen Sie als **Adding Method** die Option **Manual**.

Plug-and-Play

Die Kamera ist an der PoE-Schnittstelle angeschlossen. Ihre Parameter können nicht bearbeitet werden. Gehen Sie zu **System** → **Network** → **TCP/IP**, um die IP-Adresse des PoE-Ports zu ändern.

Manuell

Fügen Sie die IP-Kamera ohne Anschluss am Netzwerk hinzu.

4. Geben Sie **IP address**, **User Name** und **Password** ein.
5. Klicken Sie auf **OK**.

1.4.4 Angepasstes Protokoll konfigurieren

Zum Verbinden der noch nicht konfigurierten Netzwerkkameras mit den Standard-Protokollen können Sie die angepassten Protokolle dafür konfigurieren. Das System bietet 16 angepasste Protokolle.

Schritte

1. Gehen Sie zu **More Settings** → **Protocol**.

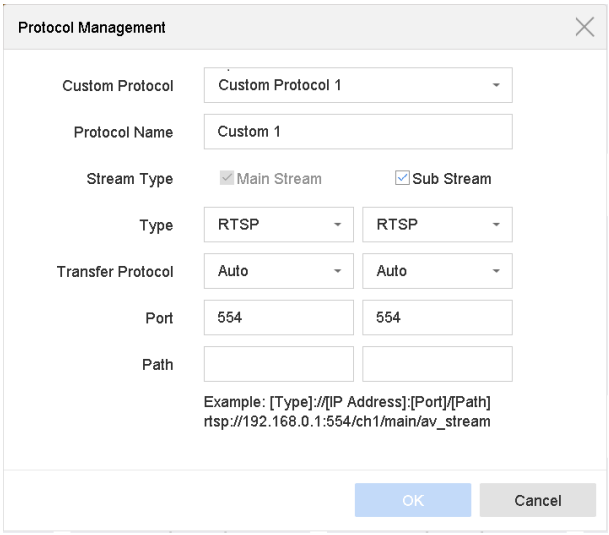


Abbildung 1-14 Protokoll-Management

2. Legen Sie die Protokollparameter fest.

Typ

Die Netzwerkkamera, die das angepasste Protokoll übernimmt, muss den Erhalt des Streams durch Standard-RTSP unterstützen.

Pfad

Wenden Sie sich an den Hersteller der Netzwerkkamera, um die URL (Uniform Resource Locator) für Haupt-Stream und Sub-Stream zu erhalten.

Hinweis

Der Protokolltyp und die Übertragungsprotokolle müssen durch die hinzuzufügende Netzwerkkamera unterstützt werden.

3. Klicken Sie auf **OK**.
   Nachdem Sie das angepasste Protokoll hinzugefügt haben, können Sie es unter **Protocol** aufrufen.

1.5 Plattformzugriff

1.5.1 EHome konfigurieren

Das EHome-Protokoll ist ein nicht offenes Push-Mode-Protokoll, das auf TCP/UDP basiert und die Kommunikation zwischen dem System und mobilen Geräten (z. B. Kamera, MNVR) ermöglicht. Das System ist ein Server, und Sie können das Gerät im System registrieren. Das Protokoll ist für die Anwendung der dynamischen Geräte-IP-Adresse geeignet.

Schritte

1. Gehen Sie zu **System** → **Network** → **Advanced** → **Platform Access**.

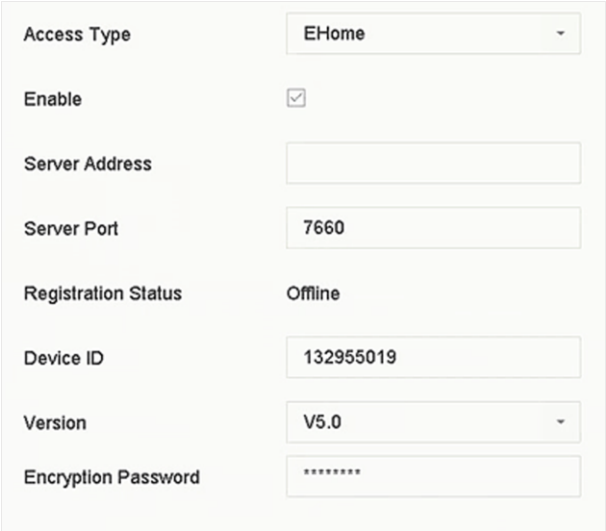


Abbildung 1-15 EHome-Einstellungen

2. Wählen Sie als **Access Type** die Option **EHome**.
3. Aktivieren Sie das Kontrollkästchen **Enable**.

Hinweis

Durch die Aktivierung von „EHome“ wird der Zugriff auf andere Plattformen deaktiviert.

4. Legen Sie die entsprechenden Parameter fest.

Server Address

IP-Adresse des Plattformservers.

Server Port

Der Plattformserver-Port liegt zwischen 1024 und 65535. Der tatsächliche Port muss von der Plattform bereitgestellt werden.

Device ID

Die Geräte-ID muss von der Plattform bereitgestellt werden.

Version

EHome-Protokollversion, nur V5.0 ist verfügbar.

Encryption Password

Bei Verwendung von EHome V5.0 ist ein Verschlüsselungskennwort erforderlich, das die sicherere Kommunikation zwischen dem Gerät und der Plattform ermöglicht. Geben Sie sie zur Überprüfung ein, nachdem das Gerät bei der EHome-Plattform registriert wurde.

5. Klicken Sie auf **Apply**, um die Einstellungen zu speichern und das Gerät neu zu starten.

Was folgt als Nächstes

Sie können den Registrierungsstatus (online oder offline) sehen, nachdem das Gerät neu gestartet wurde.

1.5.2 Hik-Connect konfigurieren

Hik-Connect bietet eine Mobiltelefon-App und einen Plattform-Service, mit der Sie auf Ihren Videorekorder zugreifen und ihn verwalten können, sodass Sie einen bequemen Fernzugriff auf das Überwachungssystem erhalten.

Schritte

1. Gehen Sie zu **System** → **Network** → **Advanced** → **Platform Access**.
2. Aktivieren Sie das Kontrollkästchen **Enable**, um die Funktion zu aktivieren. Anschließend öffnet sich das Fenster „Service Terms“.
   1) Geben Sie den **Verifizierungscode** ein.
   2) Scannen Sie den QR-Code, um die Nutzungsbedingungen und die Datenschutzerklärung anzuzeigen.
   3) Aktivieren Sie das Kontrollkästchen **The Hik-Connect service will require internet access**. **Lesen Sie die Nutzungsbedingungen und die Datenschutzerklärung, bevor Sie den Service aktivieren**, wenn Sie den Nutzungsbedingungen und der Datenschutzerklärung zustimmen.
   4) Klicken Sie auf **OK**.

Hinweis

- Hik-Connect ist standardmäßig deaktiviert.
- Der Verifizierungscode ist standardmäßig leer. Er muss 6 bis 12 Buchstaben (Groß- und

Kleinschreibung) oder Ziffern enthalten.

3. Optional: Konfigurieren Sie die folgenden Parameter.
   - Aktivieren Sie das Kontrollkästchen **Custom** und geben Sie die gewünschte **Server Address** ein.
   - Aktivieren Sie das Kontrollkästchen **Enable Stream Encryption**; dann muss der Verifizierungscode für den Fernzugriff und die Live-Ansicht eingegeben werden.
4. Koppeln Sie Ihr Gerät mit einem Hik-Connect-Konto.
   1) Scannen Sie den QR-Code mit einem Smartphone und laden Sie die Hik-Connect-App herunter. Sie können sie auch unter ***https://appstore.hikvision.com*** oder mit dem QR-Code unten herunterladen. Weitere Informationen finden Sie im *Benutzerhandbuch zum mobilen Client für Hik-Connect*.

Abbildung 1-16 Hik-Connect herunterladen

   2) Verwenden Sie Hik-Connect, um den QR-Code des Geräts zu scannen und das Gerät zu koppeln.

Hinweis

Wenn das Gerät bereits an ein Konto gebunden ist, können Sie auf **Unbind** klicken, um die Koppelung mit dem aktuellen Konto aufzuheben.

5. Klicken Sie auf **Apply**.

Was folgt als Nächstes

Sie können über Hik-Connect auf Ihren Videorekorder zugreifen.

Kapitel 2 IoT

Mit der IoT-Funktion (Internet of Things) können Sie Verbindungen zwischen Ihrem Videorekorder und IoT-Geräten herstellen, einschließlich Zugangskontroll- und Alarmgeräten. Der Videorekorder empfängt Alarme von angeschlossenen IoT-Geräten. Sie können Verknüpfungsaktionen wie das Auslösen der Aufzeichnung und die Vollbildüberwachung konfigurieren, wenn ein IoT-Alarm auftritt.

2.1 IoT-Gerät hinzufügen

Hinweis

Die maximale Anzahl an IoT-Kanälen ist die Hälfte der maximalen Anzahl an Netzwerkkameras bei Ihrem Videorekorder.

2.1.1 Zugangskontrollgerät hinzufügen

Fügen Sie Hikvision-Alarmhost und Video-Gegensprechanlagen hinzu, um deren Alarme zu empfangen. Sie können Verknüpfungsaktionen wie das Auslösen der Aufzeichnung und die Vollbildüberwachung konfigurieren, wenn ein Alarm auftritt.

Bevor Sie beginnen

Installieren Sie die Zugangskontrollgeräte. Stellen Sie sicher, dass die Netzwerkkommunikation zwischen Zugangskontrollgeräten und Videorekorder einwandfrei ist.

Schritte

1. Gehen Sie zu **Business Application** → **IoT** → **Access Control** → **Device Management**.
2. Klicken Sie auf **Add**.

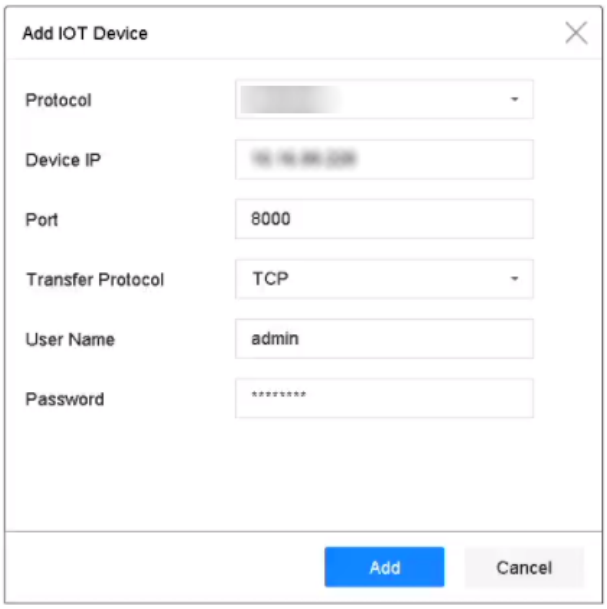


Abbildung 2-1 Zugangskontrolle

3. Geben Sie die Informationen zum Zugangskontrollgerät ein. **Device IP**, **Port**, **User Name** und **Password** müssen mit dem Zugangskontrollgerät übereinstimmen.
4. Optional: Aktivieren Sie bei Geräten mit mehreren Zugangskontrollkanälen oder Videokanälen den Zugangskontrollkanal und den Videokanal nach Ihren Wünschen.

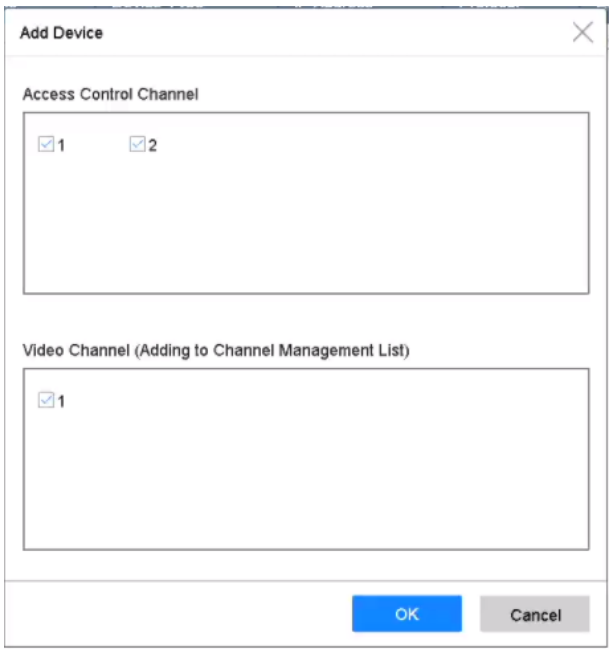


Abbildung 2-2 Gerät hinzufügen

5. Klicken Sie auf **Add**.

Was folgt als Nächstes

- Klicken Sie auf , um das Live-Video des zugehörigen Kanals abzurufen.

Hinweis

Für Zugangskontrollgeräte ohne Videokanal. Sie müssen zuerst den Auslöserkanal in der Konfiguration der Verknüpfungsaktion auswählen. Weitere Informationen finden Sie unter ***Verknüpfungsaktionen konfigurieren***.

Klicken Sie auf , um die Informationen zu den hinzugefügten Zugangskontrollgeräten zu bearbeiten.

2.1.2 Alarmgerät hinzufügen

Fügen Sie Alarmgeräte der Hersteller Hikvision, Luminite, GJD oder Optex hinzu, um deren Alarme zu empfangen. Sie können Verknüpfungsaktionen wie das Auslösen der Aufzeichnung und die Vollbildüberwachung konfigurieren, wenn ein Alarm auftritt.

Bevor Sie beginnen

Installieren Sie die Alarmgeräte. Stellen Sie sicher, dass die Netzwerkkommunikation zwischen Alarmgeräten und Videorekorder einwandfrei ist.

Schritte

1. Gehen Sie zu **Business Application** → **IoT** → **Alarm** → **Device Management**.
2. Klicken Sie auf **Add**.

Abbildung 2-3 Alarmgerät

3. Geben Sie die Informationen zum Zugangskontrollgerät ein. Die Informationen müssen mit dem hinzuzufügenden Alarmgerät übereinstimmen.
4. Klicken Sie auf **Add**.

Was folgt als Nächstes

- Klicken Sie auf , um das Live-Video des zugehörigen Kanals abzurufen.

Hinweis

Für Zugangskontrollgeräte ohne Videokanal. Sie müssen zuerst den Auslöserkanal in der Konfiguration der Verknüpfungsaktion auswählen. Weitere Informationen finden Sie unter ***Verknüpfungsaktionen konfigurieren***.

.

Klicken Sie auf , um die Informationen zu den hinzugefügten Alarmgeräten zu bearbeiten.

2.2 Verknüpfungsaktion und Scharfschaltplan konfigurieren

Konfigurieren Sie die Verknüpfungsaktionen und den Scharfschaltplan für die Zugangskontroll- oder Alarmgeräte. Verknüpfungsaktionen werden ausgelöst, wenn der entsprechende Alarm auftritt.

Schritte

1. Klicken Sie auf eines hinzugefügten IoT-Geräts.

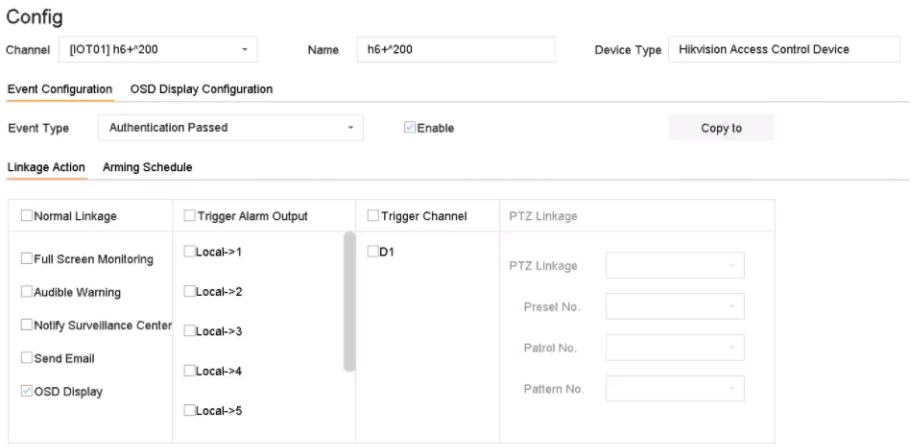


Abbildung 2-4 IoT konfigurieren

2. Wählen Sie **Event Type**. Die folgende Konfiguration ist nur für den ausgewählten Ereignistyp gültig.
3. Aktivieren Sie das Kontrollkästchen **Enable**.
4. Aktivieren Sie die Verknüpfungsaktionen nach Ihren Wünschen. Detaillierte Schritte finden Sie unter ***Verknüpfungsaktionen konfigurieren***.

Hinweis

Full Screen Monitoring und **OSD Display** sind nur für den ausgewählten **Trigger Channel** gültig.

5. Klicken Sie auf **Arming Schedule**.

6. Konfigurieren Sie den Scharfschaltplan. Detaillierte Schritte finden Sie unter ***Scharfschaltplan konfigurieren***. Die Verknüpfungsaktion ist nur während des festgelegten Plans gültig.
7. Klicken Sie auf **Apply**.

2.3 OSD konfigurieren

Sie können von IoT-Geräten eingehende Alarminformationen in einem Live-Bild anzeigen.

Schritte

1. Klicken Sie auf eines hinzugefügten IoT-Geräts.
2. Aktivieren Sie das Kontrollkästchen **OSD Display** im Menü mit der Ereigniskonfiguration.
3. Wählen Sie **Trigger Channel**.
4. Klicken Sie auf **OSD Display Configuration**.

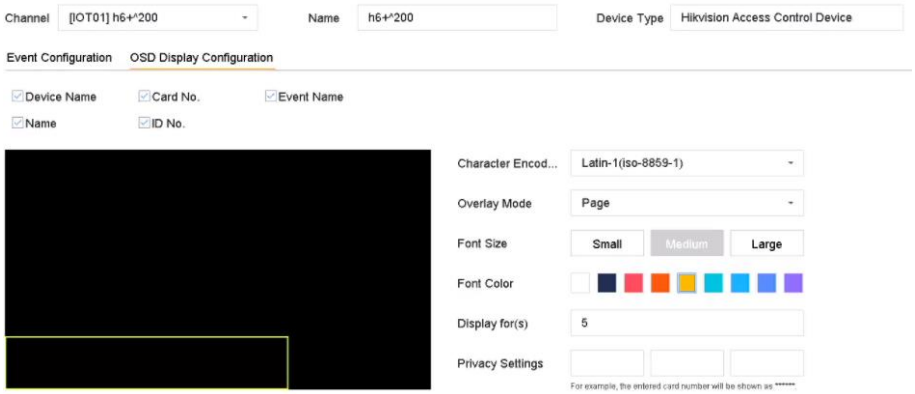


Abbildung 2-5 OSD-Konfiguration

5. Wählen Sie aus, welche Elemente (z. B. **Device Name**, **Card No.**, **Event Name**, **Name** und **ID No.**) in der Live-Ansicht gezeigt werden sollen. Die Elemente gelten nur für Zugangskontrollgeräte.
6. Konfigurieren Sie die OSD-Eigenschaften.

   Overlay-Modus – Scrollen

   Das OSD scrollt automatisch, um die neuen Alarminformationen anzuzeigen.

   Overlay-Modus – Seite

   Wenn das aktuelle OSD keine weiteren Alarminformationen anzeigen kann, wechselt es automatisch zur neuen Seite.

   Datenschutzeinstellungen

   Geben Sie die zu maskierenden Datenschutzinformationen ein. Maskierte Datenschutzinformationen werden durch einen Asterisken ersetzt. Zu den Datenschutzinformationen gehören **Event**, **Device**, **Card**, **Name** und **ID**.
7. Passen Sie das Viereck des gelben Rahmens im Vorschaufenster an, um die OSD-Größe und OSD-Position des IoT einzustellen.
8. Klicken Sie auf **Apply**.

2.4 IoT-Datensatz durchsuchen

Durchsuchen Sie Alarme nach Zeit, Ereignistyp oder Kanal.

Schritte

1. Gehen Sie zum Menü mit dem Datensatz der Ereignisaufzeichnung.
   - Zugangskontrolle: Gehen Sie zu **Business Application → IoT → Access Control → Card Swiping Record**.
   - Alarmgerät: Gehen Sie zu **Business Application → IoT → Alarm → Search Data**.

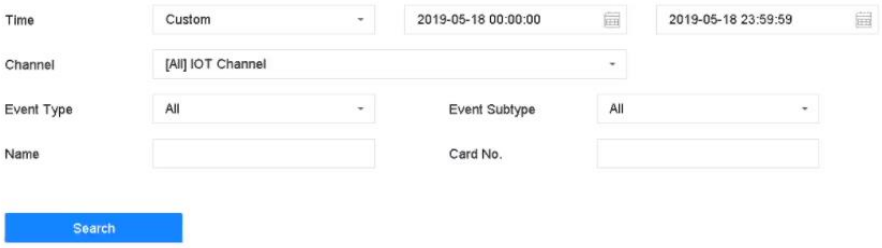


Abbildung 2-6 Ereignisdatensatz suchen (Zugangskontrolle)

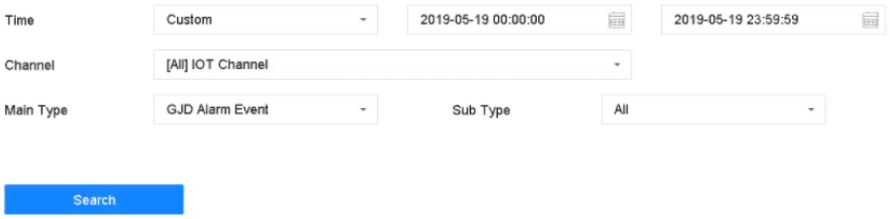


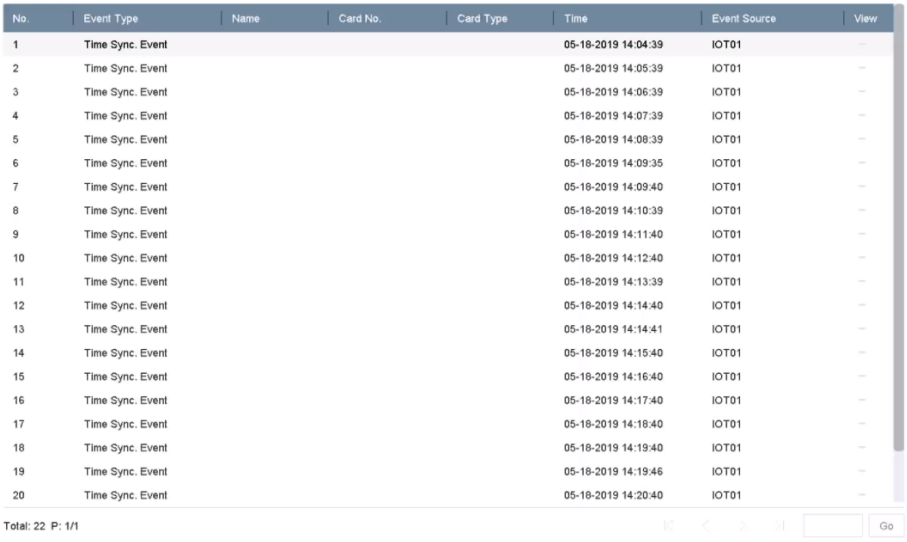
Abbildung 2-7 Ereignisdatensatz suchen (Alarmgerät)

2. Geben Sie die Suchbedingungen ein.

Hinweis

Name/Card No.: Bei einem Kartendurchzugereignis lädt das Zugangskontrollgerät den Kartennamen und die Kartennummer in den Videodatensatz hoch. Sie können das Ereignis nach Kartennamen oder Kartennummer suchen.

3. Klicken Sie auf **Search**.



No.	Event Type	Name	Card No.	Card Type	Time	Event Source	View
1	Time Sync. Event				05-18-2019 14:04:39	IOT01	
2	Time Sync. Event				05-18-2019 14:05:39	IOT01	
3	Time Sync. Event				05-18-2019 14:06:39	IOT01	
4	Time Sync. Event				05-18-2019 14:07:39	IOT01	
5	Time Sync. Event				05-18-2019 14:08:39	IOT01	
6	Time Sync. Event				05-18-2019 14:09:35	IOT01	
7	Time Sync. Event				05-18-2019 14:09:40	IOT01	
8	Time Sync. Event				05-18-2019 14:10:39	IOT01	
9	Time Sync. Event				05-18-2019 14:11:40	IOT01	
10	Time Sync. Event				05-18-2019 14:12:40	IOT01	
11	Time Sync. Event				05-18-2019 14:13:39	IOT01	
12	Time Sync. Event				05-18-2019 14:14:40	IOT01	
13	Time Sync. Event				05-18-2019 14:14:41	IOT01	
14	Time Sync. Event				05-18-2019 14:15:40	IOT01	
15	Time Sync. Event				05-18-2019 14:16:40	IOT01	
16	Time Sync. Event				05-18-2019 14:17:40	IOT01	
17	Time Sync. Event				05-18-2019 14:18:40	IOT01	
18	Time Sync. Event				05-18-2019 14:19:40	IOT01	
19	Time Sync. Event				05-18-2019 14:19:46	IOT01	
20	Time Sync. Event				05-18-2019 14:20:40	IOT01	

Total: 22 P: 1/1 Go

Abbildung 2-8 Suchergebnis (Zugangskontrolle)

No.	Channel	Time	Main Type	Sub Type	Status	Data	View
1	IOT03	05-18-2019 14:49:56	GJD Alarm Event	PIR Detection alarm			

Abbildung 2-9 Suchergebnis (Alarmgerät)

2.5 IoT-Video/-Bild

Konfigurieren Sie den Ereignisaufzeichnungs- oder Aufnahmeplan für den ausgewählten Auslöserkanal. Der Kanal zeichnet automatisch Videos oder Bilder auf, wenn ein IoT-Alarm auftritt.

2.5.1 Ereignisaufzeichnung/-erfassung konfigurieren

Der Videorekorder kann Videos oder Bilder aufnehmen, wenn ein IoT-Alarm auftritt.

Schritte

1. Klicken Sie auf eines hinzugefügten IoT-Geräts.
2. Wählen Sie den gewünschten **Event Type**.
3. Aktivieren Sie das Kontrollkästchen **Enable**.
4. Aktivieren Sie das Kontrollkästchen **Trigger Channel**, wenn Sie bei einem Alarm Ereignisvideos aufzeichnen oder Bilder aufnehmen möchten.

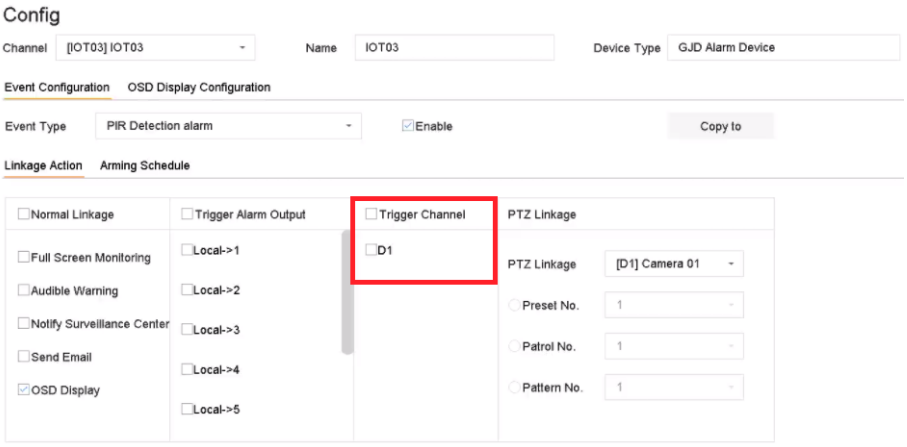


Abbildung 2-10 Auslöserkanal

5. Klicken Sie auf **Apply**.
6. Konfigurieren Sie den Ereignisaufzeichnungs- oder Erfassungsplan. Hier sehen Sie ein Beispiel für die Konfiguration der Ereignisaufzeichnung.
   1) Gehen Sie zu **Storage** → **Schedule** → **Record**.
   2) Wählen Sie **Camera No.** und aktivieren Sie das Kontrollkästchen **Enable Schedule**. Die Kamera sollte der in Schritt 4 ausgewählten Kamera entsprechen.
   3) Wählen Sie **Event** als Aufnahmetyp.
   4) Verschieben Sie die Zeitleiste mit der Maus, um den Ereigniserkennungs-Aufnahmeplan einzustellen. Weitere Informationen finden Sie unter ***Planaufzeichnung konfigurieren***.
   5) Klicken Sie auf **OK**.

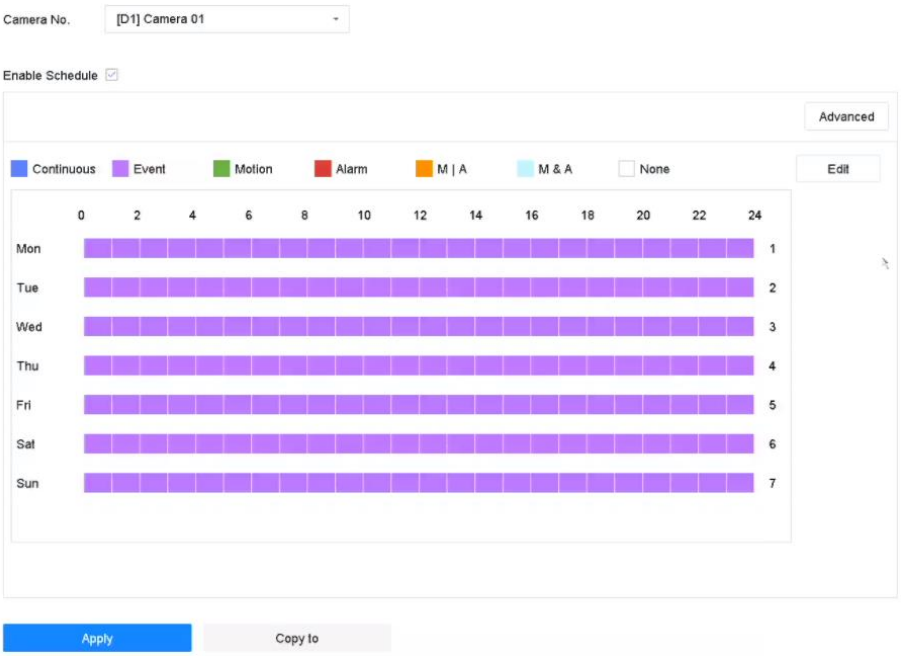


Abbildung 2-11 Ereignisaufzeichnung

Ergebnis

Wenn ein Alarm auftritt, startet der ausgewählte Auslöserkanal die Ereignisaufzeichnung.

2.5.2 IoT-Video/-Bild suchen

Suchen Sie nach Videos oder Bildern, die durch ein IoT-Ereignis ausgelöst wurden.

Schritte

1. Gehen Sie zu **File Management** → **All Files**.

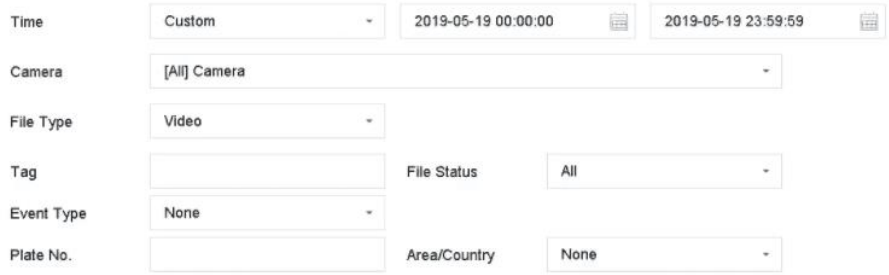


Abbildung 2-12 Video/Bild eines Suchereignisses

2. Legen Sie die Suchbedingungen fest.

   Kamera

   Wählen Sie dies als ausgewählte Auslöserkanäle in der Konfiguration der IoT-Verknüpfungsaktion aus.

   Ereignistyp

   Wählen Sie das gewünschte IoT-Ereignis aus.

   Dateityp

   Sie können das IoT-Video oder IoT-Bild durchsuchen.

3. Klicken Sie auf **Search**.

Kapitel 3 Live-Ansicht

Die Live-Ansicht zeigt das von jeder Kamera erhaltene Videobild in Echtzeit an.

3.1 Live-Ansicht starten

Klicken Sie in der Hauptmenüleiste auf , um die Live-Ansicht aufzurufen.

- Wählen Sie ein Fenster aus und doppelklicken Sie auf eine Kamera in der Liste, um das Video von der Kamera im ausgewählten Fenster wiederzugeben.
- Verwenden Sie die Symbolleiste am unteren Rand des Wiedergabefensters, um Aufnahme, Sofortwiedergabe, Audio ein/aus, Digitalzoom, Live-Ansichtsstrategie, Informationsanzeige und Aufnahmestart/-ende usw. anzuwählen

3.1.1 Einstellungen der Live-Ansicht konfigurieren

Die Einstellungen der Live-Ansicht können angepasst werden. Sie können die Ausgabeschnittstelle, die Verweilzeit der Bildschirmanzeige, die Stummschaltung oder das Einschalten des Audiosignals, die Bildschirmnummer für jeden Kanal usw. konfigurieren

Schritte

1. Gehen Sie zu **System** → **Live View** → **General**.

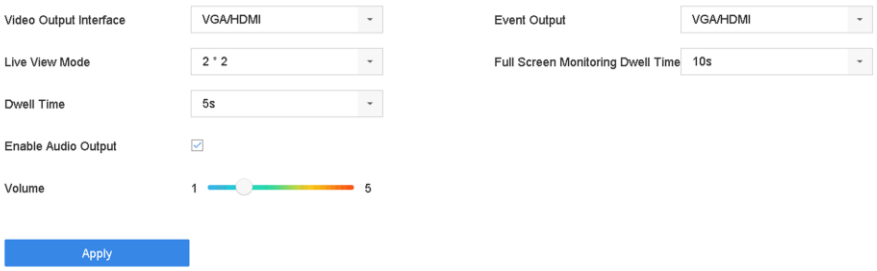


Abbildung 3-1 Live-Ansicht allgemein

2. Konfigurieren Sie die Parameter der Live-Ansicht.

Video Output Interface

Wählen Sie den zu konfigurierenden Videoausgang.

Live View Mode

Wählen Sie den Anzeigemodus für die Live-Ansicht, beispielsweise 2x2, 1x5 usw.

Dwell Time

Die Zeit in Sekunden, die zwischen dem Umschalten der Kameras bei Verwendung der automatischen Umschaltung in der Live-Ansicht gewartet wird.

Enable Audio Output

Aktiviert/deaktiviert den Audioausgang für den gewählten Videoausgang.

Volume

Stellt Lautstärke, Wiedergabe und Gegensprechen für die gewählte Ausgangsschnittstelle ein.

Event Output

Stellt den Ausgang für die Anzeige des Ereignisvideos ein.

Full Screen Monitoring Dwell Time

Stellt in Sekunden ein, wie lange der Bildschirm für Alarmereignisse angezeigt wird.

3. Klicken Sie auf **OK**.

3.1.2 Layout der Live-Ansicht konfigurieren

Die Live-Ansicht zeigt das von jeder Kamera erhaltene Videobild in Echtzeit an.

Benutzerdefiniertes Layout der Live-Ansicht konfigurieren

Schritte

1. Gehen Sie zu **System** → **Live View** → **View**.
2. Klicken Sie auf **Set Custom Layout**.
3. Klicken Sie im Menü mit der benutzerdefinierten Layoutkonfiguration auf .
4. Bearbeiten Sie den Layoutnamen.
5. Wählen Sie in der Symbolleiste den Modus für die Fensterteilung aus.

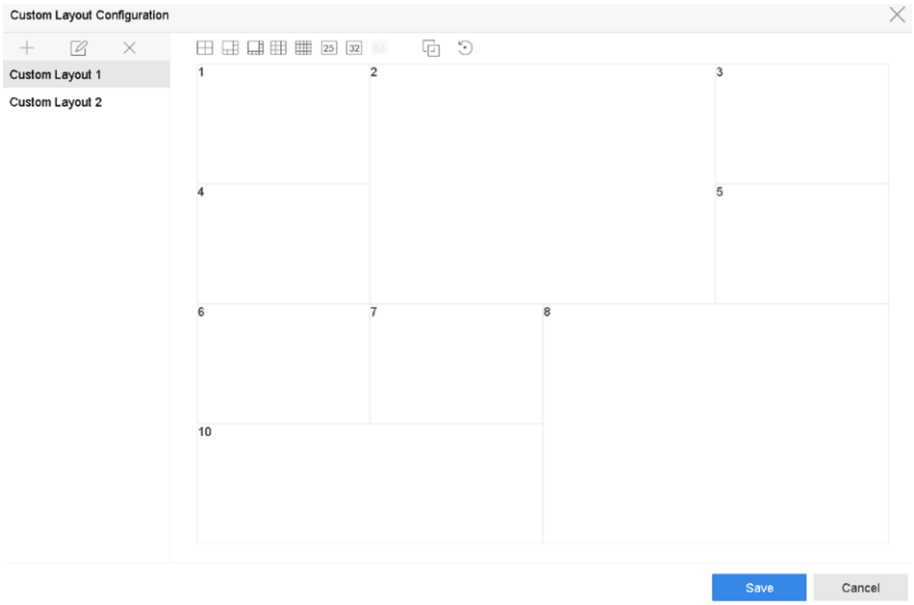


Abbildung 3-2 Layout der Live-Ansicht konfigurieren

6. Wählen Sie mehrere Fenster aus und klicken Sie auf , um die Fenster zu verbinden. Die ausgewählten Fenster müssen sich im rechteckigen Bereich befinden.

7. Klicken Sie auf **Save**.
   Das erfolgreich konfigurierte Layout wird in der Liste angezeigt.
8. Optional: Wählen Sie ein Layout für die Live-Ansicht aus der Liste und klicken Sie auf , um den Namen zu bearbeiten, oder auf , um den Namen zu löschen.

Live-Ansichtsmodus konfigurieren

Schritte

1. Gehen Sie zu **System** → **Live View** → **View**.
2. Wählen Sie die Videoausgangsschnittstelle aus.
3. Wählen Sie in der Symbolleiste ein Layout oder ein benutzerdefiniertes Layout aus.
4. Wählen Sie ein Teilfenster aus und doppelklicken Sie auf eine Kamera in der Liste, um die Kamera mit dem Fenster zu verknüpfen.

Hinweis

- Sie können auch die Kamera anklicken und in das gewünschte Fenster der Live-Ansicht ziehen, um die Reihenfolge der Kameras einzustellen.
- Sie können die Nummer im Textfeld eingeben, um die Kamera in der Liste schnell zu finden.

5. Klicken Sie auf **Apply**.
6. Optional: Klicken Sie auf , um die Live-Ansicht für alle Kanäle zu starten, oder klicken Sie auf , um alle Kanäle der Live-Ansicht zu stoppen.

3.1.3 Zwischen Haupt- und Zusatzanschluss wechseln

Nur das Bild, das am Hauptanschluss angezeigt wird, kann in das Hauptmenü gelangen und den Gerätebetrieb ermöglichen.
Sie können im Live-Ansichtsmodus auf klicken oder zu **System** → **Live View** → **General** gehen, um zwischen Haupt- und Zusatzanschluss zu wechseln,
wenn Ihr Gerät über 2 HDMI-Schnittstellen und 2 VGA-Schnittstellen verfügt; wenn HDMI1 und VGA1 die Hauptanschlüsse sind und die Videoausgabe gleichzeitig bereitgestellt wird; wenn HDMI2 und VGA2 zusätzliche Anschlüsse sind und die Videoausgabe gleichzeitig bereitgestellt wird.

3.2 Digitalzoom

Der Digital-Zoom vergrößert das Livebild in verschiedenen Vergrößerungen (1x bis 16x).

Schritte

1. Starten Sie die Live-Ansicht und klicken Sie in der Symbolleiste auf .
2. Bewegen Sie den Schieberegler oder scrollen Sie mit dem Mausrad, um das Bild in verschiedenen Vergrößerungen (1x bis 16x) zu vergrößern/verkleinern.

Abbildung 3-3 Digital-Zoom

3.3 Fischaugenansicht

Das Gerät unterstützt die Fischaugen-Kameraerweiterung in der Live-Ansicht oder im Wiedergabemodus.

Bevor Sie beginnen

- Die Ansichtsfunktion mit Fischaugenerweiterung wird nur unterstützt von
- Die angeschlossene Kamera muss die Fischaugenansicht unterstützten.

Schritte

1. Starten Sie die Live-Ansicht und klicken Sie auf , um den Fischaugen-Erweiterungsmodus aufzurufen.
2. Wählen Sie den Erweiterungsansichtsmodus.

   180°-Panorama ()Umschalten der Live-Ansicht zur 180°-Panoramasicht. 360°-Panorama ()Umschalten der Live-Ansicht zur 360°-Panoramasicht. PTZ-Erweiterung ()Die PTZ-Erweiterung ist die Nahaufnahme eines bestimmten Bereichs in der Fischaugenansicht oder der Panoramaerweiterung. Sie unterstützt die elektronische PTZ-Funktion, die auch als e-PTZ.Radial-Erweiterung bezeichnet wird ()Im radialen Erweiterungsmodus wird die gesamte Weitwinkelansicht der Fischaugenkamera dargestellt. Dieser Anzeigemodus wird als Fischaugenansicht bezeichnet, weil er der Sicht des konvexen Auges eines Fisches entspricht. Das Objektiv produziert gekrümmte Bilder eines großen Bereichs, während die Perspektive und die Winkel von Gegenständen im Bild verzerrt werden.

3.4 3D-Positionierung

Die 3D-Positionierung vergrößert/verkleinert einen spezifischen Livebildbereich.

Schritte

1. Starten Sie die Live-Ansicht und klicken Sie auf .
2. Bild vergrößern/verkleinern.
   – Vergrößern: Klicken Sie auf die gewünschte Position im Videobild und ziehen Sie zum Vergrößern einen Rechteckbereich nach unten rechts.
   – Verkleinern: Ziehen Sie ein Rechteck nach oben links, um die Position in die Mitte zu verschieben und den Rechteckbereich zu verkleinern.

3.5 Kanal-Null-Codierung konfigurieren

Aktivieren Sie die Kanal-Null-Codierung, wenn Sie von einem Webbrowser oder einer CMS-Software (Client Management System) eine Fernansicht vieler Kanäle in Echtzeit benötigen, um den Bandbreitenbedarf zu verringern, ohne die Bildqualität zu beeinträchtigen.

Schritte

1. Gehen Sie zu **System** → **Live View** → **Channel-Zero**.
2. Aktivieren Sie **Enable Channel-Zero Encoding**.

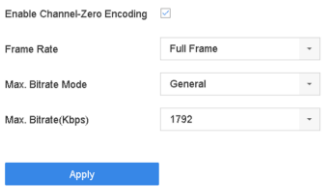


Abbildung 3-4 Null-Kanal-Codierung

3. Konfigurieren Sie **Frame Rate**, **Max. Bitrate Mode** und **Max. Bitrate**. Eine höhere Bildrate und Bitrate erfordern eine höhere Bandbreite.
4. Klicken Sie auf **Apply**.
   Sie können alle Kanäle auf einem Bildschirm mit CMS oder Webbrowser abrufen.

3.6 PTZ-Steuerung

3.6.1 PTZ-Parameter konfigurieren

Folgen Sie den nachstehenden Anleitungen zum Einstellen der PTZ-Parameter. Die PTZ-

Parameterkonfiguration muss erfolgen, bevor Sie die PTZ-Kamera steuern können.

Schritte

1. Klicken Sie auf in der Schnelleinstellungs-Symbolleiste der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf **PTZ Parameters Settings**, um die PTZ-Parameter einzustellen.

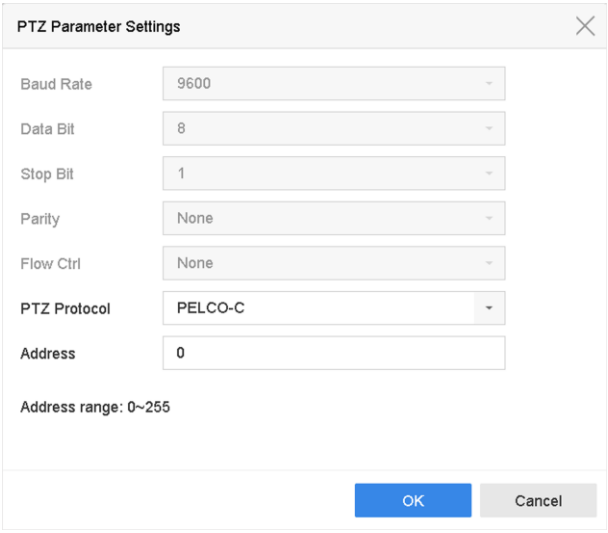


Abbildung 3-5 Einstellung der PTZ-Parameter

3. Bearbeiten Sie die PTZ-Kameraparameter.

Hinweis

Alle Parameter müssen den PTZ-Kameraparametern genau entsprechen.

4. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

3.6.2 Voreinstellung einstellen

Voreinstellungen zeichnen die PTZ-Position und den Status von Zoom, Fokus, Blende usw. auf. Sie können eine Voreinstellung aufrufen, um die Kamera schnell an die vordefinierte Position zu führen.

Schritte

1. Klicken Sie auf in der Schnelleinstellungs-Symbolleiste der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf die Richtungstasten, um die Kamera an eine Position zu führen.
3. Stellen Sie Zoom, Fokus und Blende ein.
4. Klicken Sie unten rechts in der Live-Ansicht auf , um die Voreinstellung festzulegen.

Abbildung 3-6 Voreinstellung festlegen

5. Wählen Sie die Nummer der Voreinstellung (1 bis 255) aus der Dropdown-Liste aus.
6. Geben Sie den Namen der Voreinstellung ein.

7. Klicken Sie auf **Apply**, um die Voreinstellung zu speichern.
8. Optional: Klicken Sie auf **Cancel**, um die Standortinformationen der Voreinstellung zu löschen.
9. Optional: (Optional) Klicken Sie unten rechts in der Live-Ansicht auf , um die konfigurierten Voreinstellungen anzuzeigen.

Abbildung 3-7 Konfigurierte Voreinstellungen anzeigen

3.6.3 Voreinstellung aufrufen

Eine Voreinstellung ermöglicht es der Kamera, auf eine bestimmte Position zu zeigen, wie beispielsweise ein Fenster, wenn ein Ereignis eintritt.

Schritte

1. Klicken Sie auf in der Schnelleinstellungs-Symbolleiste der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie unten rechts in der Live-Ansicht auf , um die Voreinstellung festzulegen.
3. Wählen Sie die Nummer der Voreinstellung aus der Dropdown-Liste aus.
4. Klicken Sie auf **Call**, um sie aufzurufen, oder klicken Sie unten rechts in der Live-Ansicht auf die konfigurierte Voreinstellung, um sie aufzurufen.

Abbildung 3-8 Voreinstellung aufrufen (1)

Abbildung 3-9 Voreinstellung aufrufen (2)

3.6.4 Tour festlegen

Mit einer Tour können Sie die PTZ auf Eckpunkte verschieben und für eine bestimmte Dauer dort halten, bevor Sie zum nächsten Eckpunkt übergehen. Die Eckpunkte entsprechen den Voreinstellungen.

Schritte

1. Klicken Sie auf in der Schnelleinstellungs-Symbolleiste der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf **Patrol**, um Touren zu konfigurieren.

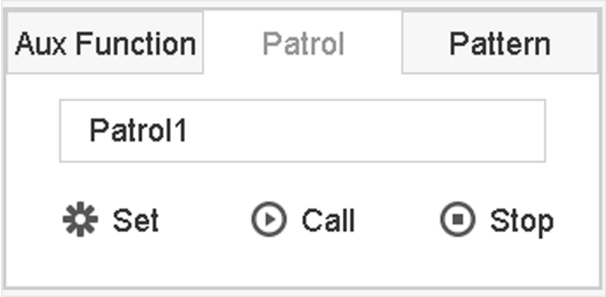


Abbildung 3-10 Tourkonfiguration

3. Wählen Sie die Tournummer.
4. Klicken Sie auf **Set**.

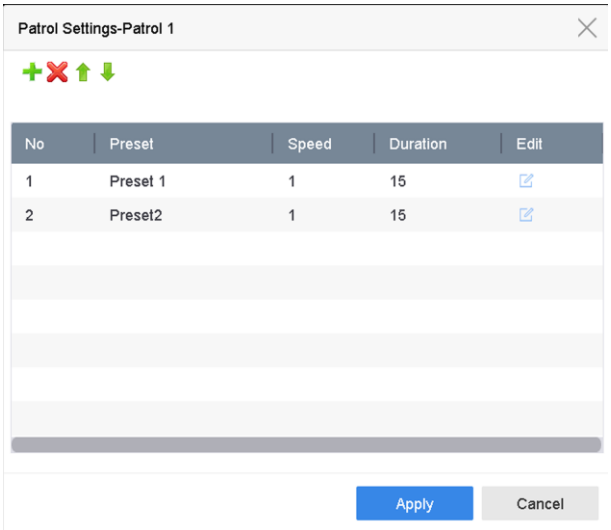


Abbildung 3-11 Toureinstellungen

5. Klicken Sie auf ✚, um der Tour einen Eckpunkt hinzuzufügen.

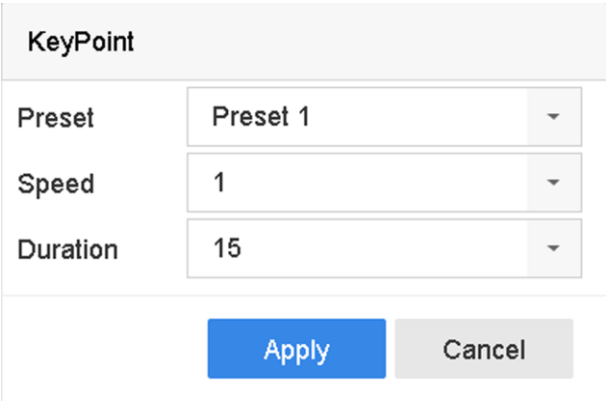


Abbildung 3-12 Eckpunktkonfiguration

1) Konfigurieren Sie die Eckpunktparameter.

Preset

Bestimmt die Reihenfolge, in der die PTZ-Kamera die Tour durchläuft.

Speed

Bestimmt die Geschwindigkeit, mit der sich die PTZ-Kamera von einem Eckpunkt zum nächsten bewegt.

Duration

Bestimmt die Verweildauer am entsprechenden Eckpunkt.

2) Klicken Sie auf **Apply**, um die Eckpunkte der Tour zu speichern.

6. Die andere Variante geht wie folgt.

OperationDescriptionOperationDescription❌Wählen Sie einen zu löschenden Eckpunkt aus. Bearbeiten Sie den hinzugefügten Eckpunkt. ⬆Passen Sie die Reihenfolge der Eckpunkte an. ⬇ Passen Sie die Reihenfolge der Eckpunkte an.

7. Klicken Sie auf **Apply**, um die Toureinstellungen zu speichern.

3.6.5 Tour aufrufen

Das Aufrufen einer Tour lässt die PTZ-Kamera dem vordefinierten Tourpfad folgen.

Schritte

1. Klicken Sie auf in der Schnelleinstellungs-Symbolleiste der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf dem PTZ-Bedienfeld auf **Patrol**.

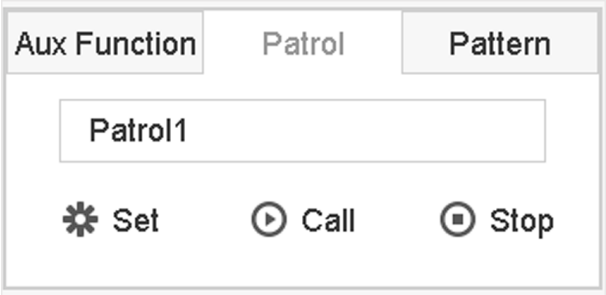


Abbildung 3-13 Tourkonfiguration

3. Wählen Sie eine Tour aus.
4. Klicken Sie auf **Call**, um die Tour zu starten.
5. Optional: Klicken Sie auf **Stop**, um die Tour zu beenden.

3.6.6 Muster festlegen

Muster können durch die Aufnahme der Bewegung der PTZ-Kamera eingestellt werden. Sie können das Muster aufrufen, damit sich die PTZ-Kamera entsprechend dem vordefinierten Tourpfad bewegt.

Schritte

1. Klicken Sie auf in der Schnelleinstellungs-Symbolleiste der Live-Ansicht der PTZ-Kamera.

2. Klicken Sie auf **Pattern**, um ein Muster zu konfigurieren.

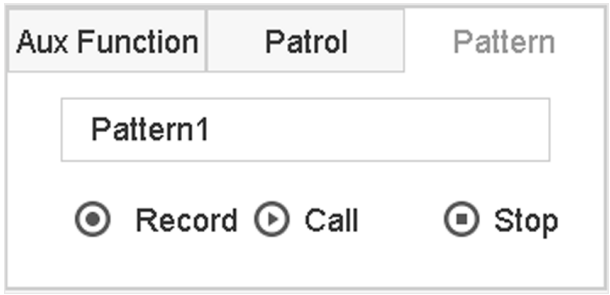


Abbildung 3-14 Musterkonfiguration

3. Wählen Sie die Musternummer.
4. Stellen Sie das Muster ein.
   1) Klicken Sie auf **Record**, um die Aufnahme zu starten.
   2) Klicken Sie auf die entsprechenden Schaltflächen im Bedienfeld, um die PTZ-Kamera zu bewegen.
   3) Klicken Sie auf **Stop**, um die Aufnahme zu beenden. Die PTZ-Bewegung wird als Muster aufgezeichnet.

3.6.7 Muster aufrufen

Folgen Sie der Vorgehensweise zum Bewegen der PTZ-Kamera gemäß den vordefinierten Mustern.

Schritte

1. Klicken Sie auf in der Schnelleinstellungs-Symbolleiste der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf **Pattern**, um das Muster zu konfigurieren.

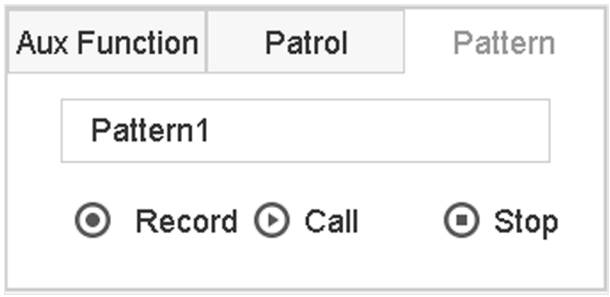


Abbildung 3-15 Musterkonfiguration

3. Wählen Sie ein Muster aus.
4. Klicken Sie auf **Call**, um das Muster zu starten.
5. Optional: Klicken Sie auf **Stop**, um das Muster zu beenden.

3.6.8 Lineare Suchgrenzen einstellen

Der lineare Scan löst eine Suche in horizontaler Richtung im vordefinierten Bereich aus.

Bevor Sie beginnen

Vergewissern Sie sich, dass die angeschlossene IP-Kamera die PTZ-Funktion unterstützt und ordnungsgemäß angeschlossen ist.

Hinweis

Diese Funktion wird nur von einigen Modellen unterstützt.

Schritte

1. Klicken Sie auf in der Schnelleinstellungs-Symbolleiste der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf die Pfeiltasten, um die Kamera an eine Stelle zu bewegen, und klicken Sie auf **Left Limit** oder **Right Limit**, um die Stelle mit der entsprechenden Grenze zu verbinden.

   Hinweis

   Die Hochgeschwindigkeits-Kuppelkamera sucht linear von der linken Grenze zur rechten Grenze, und Sie müssen die linke Grenze links von der rechten Grenze einstellen. Außerdem darf der Winkel von der linken zur rechten Grenze nicht mehr als 180º betragen.

3.6.9 One-Touch-Parken

Bestimmte Hochgeschwindigkeits-Kuppelkameramodelle können so konfiguriert werden, dass sie nach einer gewissen Zeit der Inaktivität (Parkzeit) automatisch eine vordefinierte Parkaktion (Suche, Voreinstellung, Tour usw.) starten.

Bevor Sie beginnen

Bevor Sie diese Funktion verwenden, vergewissern Sie sich, dass die angeschlossene Kamera einen linearen Scan unterstützt und sich im HIKVISION-Protokoll befindet.

Schritte

1. Klicken Sie auf in der Schnelleinstellungs-Symbolleiste der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf **Park (Quick Patrol)**, **Park (Patrol 1)** oder **Park (Preset 1)**, um die Parkaktion zu aktivieren.

   Park (Quick Patrol)

   Die Kuppelkamera startet die Tour nach der Parkzeit der Reihe nach ab der vordefinierten Voreinstellung 1 bis Voreinstellung 32. Nicht definierte Voreinstellungen werden übersprungen.

   Park (Patrol 1)

   Die Kamera bewegt sich nach Ablauf der Parkzeit gemäß dem vorgegebenen Pfad der Tour 1.

   Park (Preset 1)

Die Kuppelkamera bewegt sich nach der Parkzeit zur vordefinierten Voreinstellung 1.

Hinweis

Die Parkzeit kann nur über das Konfigurationsmenü der Kuppelkamera eingestellt werden. Der Standardwert ist 5 Sekunden.

3. Optional: Klicken Sie auf **Stop Park (Quick Patrol)**, **Stop Park (Patrol 1)** oder **Stop Park (Preset 1)**, um die Parkaktion zu deaktivieren.

Kapitel 4 Aufzeichnung und Wiedergabe

4.1 Aufzeichnung

4.1.1 Aufzeichnungsparameter konfigurieren

Gehen Sie zu **Camera** → **Video Parameters**.

Haupt-Stream

Der Haupt-Stream bezieht sich auf den primären Stream, der die auf der Festplatte aufgezeichneten Daten beeinflusst, und bestimmt direkt Ihre Aufnahmequalität und Bildgröße. Im Vergleich zum Sub-Stream kann der Haupt-Stream eine höhere Videoqualität mit höherer Auflösung und Bildrate liefern.

Frame Rate (FPS - Frames Per Second)

Bezieht sich auf die Anzahl der Einzelbilder pro Sekunde. Eine höhere Bildrate ist vorteilhaft, wenn Bewegung im Videostream ist, weil die Bildqualität durchgehend aufrechterhalten bleibt.

Resolution

Die Bildauflösung ist ein Maß für die Detailtreue eines Digitalbilds. Je größer die Auflösung, desto größer die Detailgenauigkeit. Die Auflösung kann als Anzahl der Pixelspalten (Breite) mal die Anzahl der Pixelreihen (Höhe) angegeben werden, z. B. 1024 × 768.

Bitrate

Die Bitrate (in kBit/s oder MBit/s) wird oft als Geschwindigkeit bezeichnet, definiert aber die Anzahl der Bits pro Zeiteinheit und nicht die Distanz pro Zeiteinheit.

Enable H.264+

H.264+ kombiniert intelligente Analysetechnologie mit vorausschauender Codierung, Rauschunterdrückung und langfristiger Bitratensteuerung, um eine niedrigere Bitrate zu erzielen. Dies spielt eine wichtige Rolle bei der Senkung der Speicherkosten und sorgt für eine höhere Kapitalrendite.

Enable H.265+

H.265+ ist eine optimierte Verschlüsselungstechnologie, die auf der standardmäßigen H.265/HEVC-Komprimierung basiert. Bei H.265+ ist die Videoqualität fast identisch wie H.265/HEVC, jedoch mit weniger Übertragungsbandbreite und Speicherkapazität.

Hinweis

- Eine höhere Auflösung, Bildrate und Bitrate sorgen für eine bessere Videoqualität, doch wird dabei auch mehr Internet-Bandbreite benötigt und mehr Speicherplatz auf der Festplatte

verbraucht.

- Die Verschlüsselungstechnologie H.264+ oder H.265+ ist nur für bestimmte Modelle verfügbar.

Sub-Stream

Der Sub-Stream ist ein zweiter Codec, der parallel zum Haupt-Stream läuft. Er erlaubt Ihnen, die ausgehende Internet-Bandbreite zu reduzieren, ohne Ihre direkte Aufnahmequalität zu beeinträchtigen.
Der Sub-Stream wird oft ausschließlich von Apps verwendet, um Live-Videos anzuzeigen. Benutzer mit begrenzter Internetgeschwindigkeit können am meisten von dieser Einstellung profitieren.

Bild

Bezieht sich auf die Livebildaufnahme im Dauer- oder Ereignisaufzeichnungstyp. (**Storage** → **Capture Schedule** → **Advanced**

Picture Quality

Stellen Sie die Bildqualität auf niedrig, mittel oder hoch ein. Eine höhere Bildqualität führt zu einem höheren Speicherplatzbedarf.

Interval

Das Intervall der Erfassung des Livebildes.

Capture Delay Time

Dauer der Erfassung von Bildern.

Erweiterte Aufnahmeeinstellungen konfigurieren

Schritte

1. Gehen Sie zu **Storage** → **Schedule** → **Record**.
2. Aktivieren Sie das Kontrollkästchen **Enable**, um eine geplante Aufnahme zu aktivieren.
3. Klicken Sie auf **Advanced**, um die erweiterten Parameter einzustellen.

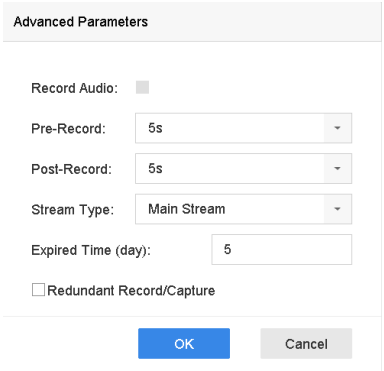


Abbildung 4-1 Erweiterte Aufzeichnungseinstellungen

Record Audio

Aktiviert oder deaktiviert die Audioaufzeichnung.

Pre-record

Eingestellte Aufnahmezeit vor der geplanten Zeit bzw. dem Ereignis. Wird ein Alarm beispielsweise um 10:00 Uhr ausgelöst und Sie haben die Vor-Aufnahmezeit als 5 Sekunden eingestellt, beginnt die Kamera mit der Aufnahme um 9:59:55.

Post-record

Eingestellte Aufnahmezeit nach der geplanten Zeit bzw. dem Ereignis. Endet eine alarmausgelöste Aufnahme beispielsweise um 11:00 Uhr und Sie haben die Nach-Aufnahmezeit als 5 Sekunden eingestellt, läuft die Aufnahme bis 11:00:05.

Stream Type

Haupt-Stream und Sub-Stream sind zur Aufnahme wählbar. Bei Auswahl des Sub-Streams können Sie mit dem gleichen Speicherplatz länger aufnehmen.

Expired Time

Dauer, für die eine Aufnahmedatei auf der Festplatte gehalten wird. Nach Ablauf der Frist wird die Datei gelöscht. Wird die Ablaufzeit auf 0 eingestellt, so wird die Datei nicht gelöscht. Die tatsächliche Aufbewahrungszeit der Datei sollte durch die Kapazität der Festplatte bestimmt werden.

Redundant Record/Capture

Durch Aktivierung der redundanten Aufnahme oder Bilderfassung speichern Sie die Aufnahme- und Bilddatei auf der redundanten Festplatte.

4.1.2 Zugriff auf H.265-Stream aktivieren

Das Gerät kann automatisch zum H.265-Stream der IP-Kamera (der das H.265-Videoformat unterstützt) für den Erstzugriff umschalten.
Gehen Sie zu **Camera** → **More Settings** → **H.265 Auto Switch Configuration**, um die Funktion zu aktivieren.

4.1.3 ANR

Die ANR-Funktion (Automatic Network Replenishment) ermöglicht es der IP-Kamera, Aufnahmedateien lokal zu speichern, wenn das Netzwerk getrennt ist. Wenn das Netzwerk wieder verbunden ist, werden die Dateien ins Gerät hochgeladen.

Schritte

1. Melden Sie sich über einen Webbrowser bei Ihrem Gerät an und gehen Sie zu **Configuration** → **Storage** → **Schedule Settings** → **Advanced** .
2. Aktivieren Sie das Kontrollkästchen **Enable ANR**.
3. Klicken Sie auf **OK**.

4.1.4 Manuelle Aufzeichnung

Sie können auf  klicken, um die Videoaufzeichnung in der Live-Ansicht manuell zu starten oder zu beenden.

4.1.5 Planaufzeichnung konfigurieren

Die Kamera startet/beendet die Aufzeichnung automatisch gemäß dem konfigurierten Aufnahmeplan.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie die Festplatten im Gerät installiert bzw. die Netzwerkfestplatten hinzugefügt haben, bevor Sie Videodateien, Bilder und Protokolldateien speichern.
- Um **Motion**, **Alarm**, **M | A** (Bewegung oder Alarm), **M & A** (Bewegung und Alarm) und **Event** zu aktivieren, müssen Sie die Einstellungen für Bewegungserkennung, Alarmeingang und andere Ereignisse konfigurieren. Siehe für Einzelheiten.

Schritte

1. Gehen Sie zu **Storage** → **Schedule** → **Record**.
2. Wählen Sie eine Kamera aus.
3. Aktivieren Sie das Kontrollkästchen **Enable Schedule**.
4. Wählen Sie einen Aufnahmetyp aus.

   Continuous

   Geplante Aufnahme.

   Event

   Aufnahme, die durch alle ereignisbasierten Alarme ausgelöst wird.

   Motion

   Aufnahme, die durch die Bewegungserkennung ausgelöst wird.

   Alarm

   Aufnahme, die durch einen Alarm ausgelöst wird.

   M/A

   Aufnahme, die durch Bewegungserkennung oder Alarm ausgelöst wird.

   M&A

   Aufnahme, die durch Bewegungserkennung und Alarm ausgelöst wird.

   POS

   Aufnahme, die durch POS und Alarm ausgelöst wird.
5. Verschieben Sie die Zeitleiste mit der Maus, um den Aufnahmeplan einzustellen.

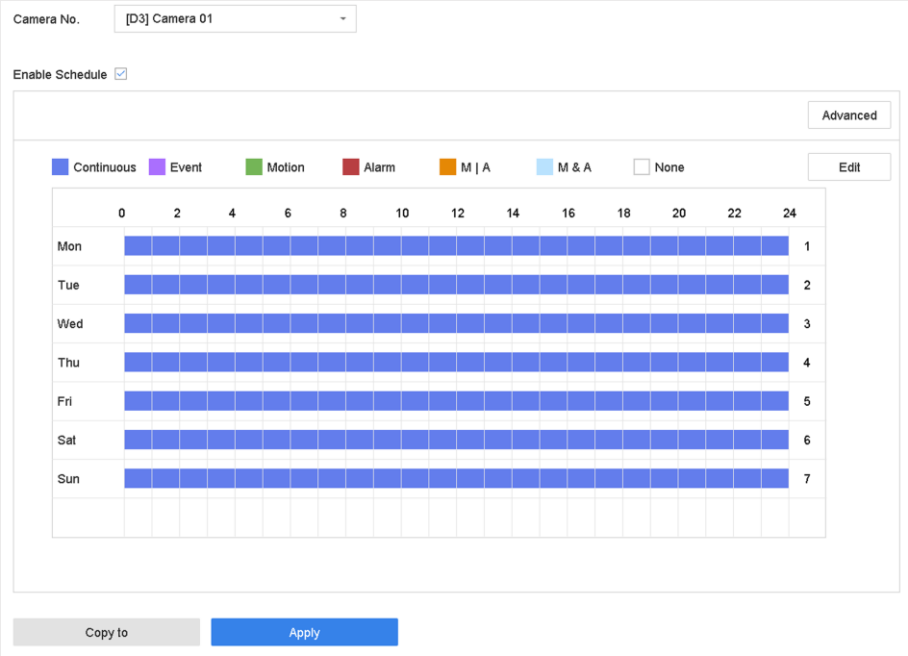


Abbildung 4-2 Aufnahmeplan

Hinweis

- Wiederholen Sie die obigen Schritte zur Planung von Aufnahme oder Bilderfassung an jedem Tag der Woche.
- Die kontinuierliche Aufzeichnung wird standardmäßig auf jeden Tag angewendet.

6. Optional: Kopieren Sie den Aufnahmeplan auf andere Kamera(s).
   1) Klicken Sie auf **Copy to**.
   2) Wählen Sie den/die Kamera(s) zum Duplizieren der gleichen Planeinstellungen aus.
   3) Klicken Sie auf **OK**.
7. Klicken Sie auf **Apply**.

4.1.6 Feiertagsaufnahme konfigurieren

An freien Tagen möchten Sie möglicherweise einen anderen Plan für die Aufzeichnung haben. Mit dieser Funktion können Sie den Aufnahmeplan für das Jahr auf Feiertagsaufnahme einstellen.

Schritte

1. Gehen Sie zu **System** → **Holiday**.
2. Wählen Sie ein Feiertagselement aus der Liste aus.
3. Klicken Sie auf , um den ausgewählten Feiertag zu bearbeiten.
4. Aktivieren Sie das Kontrollkästchen **Enable**.

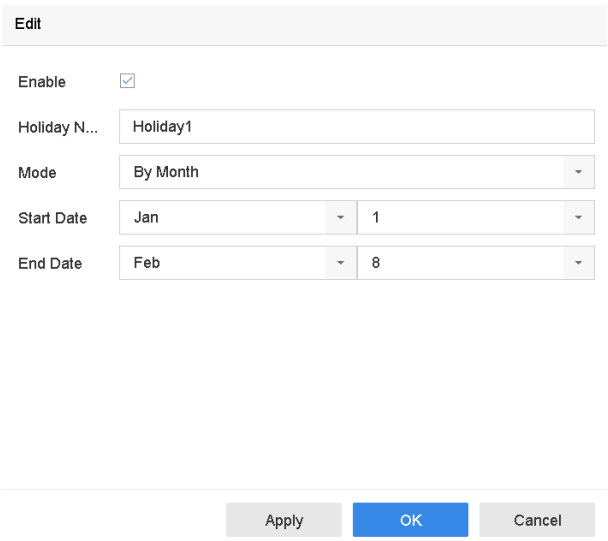


Abbildung 4-3 Feiertagseinstellungen bearbeiten

5. Legen Sie **Holiday Name**, **Mode**, **Start Date** und **End Date** fest.
6. Klicken Sie auf **OK**.
7. Stellen Sie den Feiertagsaufnahmeplan ein. Weitere Informationen finden Sie unter ***Planaufzeichnung konfigurieren***.

4.2 Wiedergabe

4.2.1 Sofortwiedergabe

Die Sofortwiedergabe ermöglicht dem Gerät die Wiedergabe der in den letzten fünf Minuten aufgenommenen Videodateien. Wenn kein Video gefunden wird, bedeutet das, dass in den letzten fünf Minuten keine Aufnahme erfolgt ist.

Nachdem Sie die Kamera in der **Live View** ausgewählt haben, können Sie den Mauszeiger zur Symbolleiste am unteren Fensterrand führen und auf klicken, um die Sofortwiedergabe zu starten.

Abbildung 4-4 Wiedergabemenü

4.2.2 Video normal wiedergeben

Gehen Sie zu **Playback**. Wählen Sie Datum und Kamera(s) aus und verwenden Sie die Symbolleiste unten, um die Wiedergabevorgänge auszuführen. Siehe dazu ***Wiedergabevorgänge***. Sie können eine oder mehrere Kameras anklicken, um die gleichzeitige Wiedergabe mehrerer Kamerabilder zu starten.

Hinweis

256-fache Abspielgeschwindigkeit wird unterstützt.

Abbildung 4-5 Normale Videoschnittstelle wiedergeben

4.2.3 Intelligent gesuchtes Video wiedergeben

Im intelligenten Wiedergabemodus kann das Gerät Videos mit Informationen zur Bewegungs-,

Linien- oder Eindringungserkennung analysieren und diese rot markieren.
Gehen Sie zu **Playback**. Klicken Sie auf **Smart** und in der Symbolleiste unten dann auf Bewegungserkennung ( ), Linienüberschreitungserkennung ( ) oder Eindringungserkennung ( ), um das Video zu suchen und nach Ihren Wünschen wiederzugeben.
Bei bestimmten Kameramodellen, die Personen und Fahrzeuge erkennen, können Sie auf und klicken, um nach Personen und Fahrzeugen zu suchen. Bei der Wiedergabe von Videos mit Menschen und Fahrzeugen können keine Videos mit Linienüberschreitungserkennung ( ) oder Eindringungserkennung ( ) angezeigt werden, die auf den Videos mit Menschen und Fahrzeugen basieren.

Abbildung 4-6 Wiedergabe über Smart Search

4.2.4 Benutzerdefiniert gesuchte Dateien wiedergeben

Sie können Videos nach benutzerdefinierten Suchbedingungen abspielen.

Schritte

1. Gehen Sie zu **Playback**.
2. Wählen Sie die Kamera(s) aus der Liste aus.
3. Klicken Sie links unten auf **Custom Search**.
4. Geben Sie Suchbedingungen wie **Time**, **File Status**, **Event Type** usw. ein.

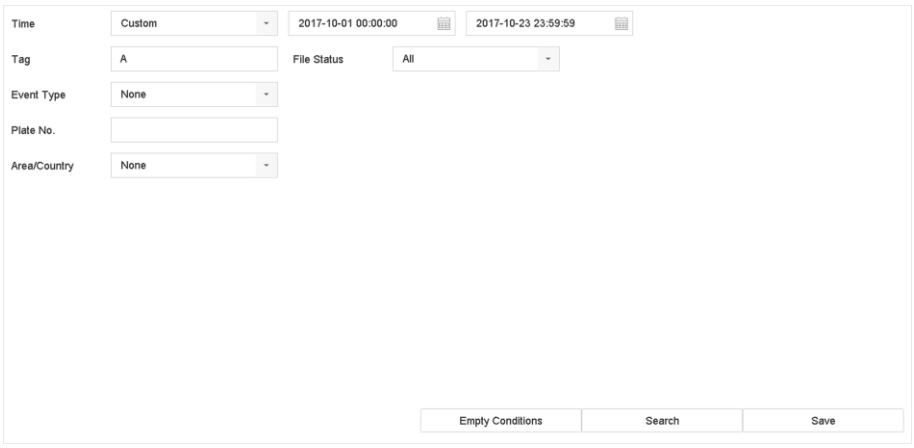


Abbildung 4-7 Benutzerdefinierte Suche

5. Klicken Sie auf **Search**.

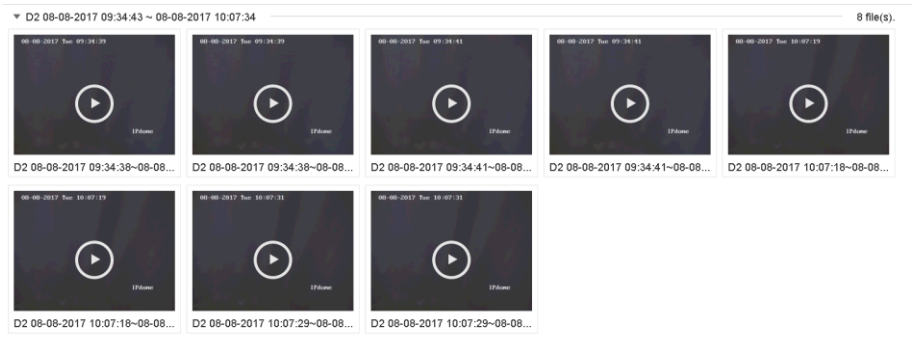


Abbildung 4-8 Benutzerdefiniert gesuchte Videodateien

6. Wählen Sie eine Datei aus und starten Sie die Wiedergabe des Videos im Menü mit den Suchergebnissen.

4.2.5 Tag-Dateien wiedergeben

Mit dem Video-Tag können Sie Informationen wie Personen und Orte zu einem bestimmten Zeitpunkt während der Wiedergabe aufzeichnen. Sie können Video-Tags verwenden, um nach Videodateien und Zeitpunkten zu suchen.

Tag-Dateien hinzufügen

Schritte

1. Gehen Sie zu **Playback**.
2. Suchen Sie Videodateien und spielen Sie diese ab.
3. Klicken Sie auf , um das Tag als Kennzeichnung hinzuzufügen.
4. Bearbeiten Sie die Tag-Informationen.
5. Klicken Sie auf **OK**.

Hinweis

Einer einzelnen Videodatei können max. 64 Tags hinzugefügt werden.

Tag-Dateien wiedergeben

Schritte

1. Gehen Sie zu **Playback**.
2. Klicken Sie unten links auf **Custom Search**.
3. Geben Sie Suchbedingungen wie Zeit oder Tag ein.

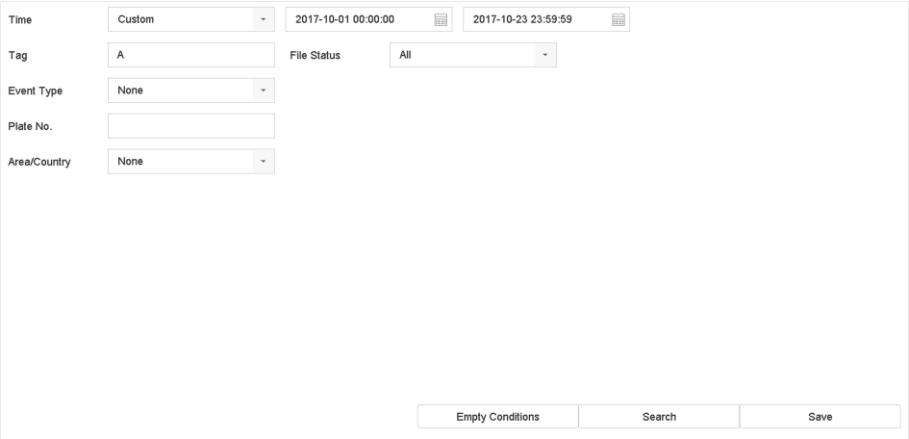


Abbildung 4-9 Tag-Suche

4. Klicken Sie auf **Search**.

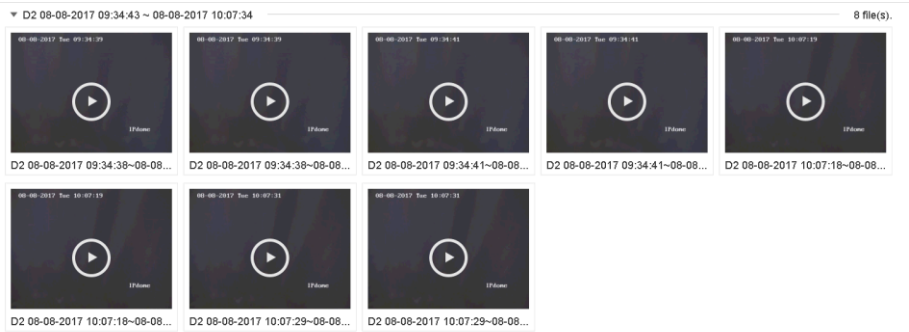


Abbildung 4-10 Durchsuchte Tag-Dateien

5. Wählen Sie eine Tag-Datei aus und spielen Sie das Video im Menü mit den Suchergebnissen ab.

4.2.6 Wiedergabe nach Teilzeiträumen

Die Videodateien können in mehreren Teilzeiträumen gleichzeitig auf dem Bildschirm

wiedergegeben werden.

Schritte

1. Gehen Sie zu **Playback**.
2. Klicken Sie unten links auf .
3. Wählen Sie eine Kamera aus.
4. Legen Sie Startzeit und Endzeit für die Suche nach Videos fest.
5. Wählen Sie die verschiedenen Mehrfachzeiträume unten rechts, z. B. „4-Period“.

Hinweis

Entsprechend der definierten Anzahl geteilter Bildschirme können die Videodateien des gewählten Datums in durchschnittliche Segmente zur Wiedergabe unterteilt werden. Gibt es beispielsweise Videodateien zwischen 16:00 und 22:00, und der 6-fach-Bildschirmmodus ist gewählt, dann können die Videodateien für 1 Stunde auf allen Bildschirmen gleichzeitig angezeigt werden.

4.2.7 Externe Dateien wiedergeben

Sie können Dateien von externen Speichergeräten wiedergeben.

Bevor Sie beginnen

Schließen Sie das Speichergerät mit den Videodateien an Ihr Gerät an.

Schritte

1. Gehen Sie zu **Playback**.
2. Klicken Sie unten links auf .
3. Klicken Sie auf oder doppelklicken Sie auf die Datei, um sie wiederzugeben.

4.3 Wiedergabevorgänge

4.3.1 Videoclips bearbeiten

Sie können Videoclips während der Wiedergabe schneiden und exportieren.

Schritte

1. Gehen Sie zu **Playback**
2. Klicken Sie in der unteren Symbolleiste auf .
3. Legen Sie Startzeit und Endzeit fest. Sie können auf klicken, um den Zeitraum festzulegen, oder ein Zeitsegment in der Zeitleiste festlegen.
4. Klicken Sie auf , um den Videoclip auf einem Speichergerät zu speichern.

4.3.2 Miniaturbildansicht

Mit der Miniaturbildansicht im Wiedergabemenü finden Sie leicht die gewünschten Videodateien auf der Zeitleiste.
Führen Sie den Mauszeiger im Wiedergabemodus auf die Zeitleiste, um Miniaturbilder als Vorschau zu erhalten.

Abbildung 4-11 Miniaturansicht

Sie können auf ein Miniaturbild klicken, um in die Vollbildwiedergabe zu gelangen.

Kapitel 5 Bildaufnahme

5.1 Parameter konfigurieren

Bezieht sich auf die Livebildaufnahme bei der Dauer- oder Ereignisaufzeichnung.
Sie können die Bildparameter unter **Storage** → **Capture Schedule** → **Advanced** bearbeiten.

Resolution

Stellen Sie die Bildauflösung ein.

Picture Quality

Stellen Sie die Bildqualität auf niedrig, mittel oder hoch ein. Eine höhere Qualität erfordert mehr Speicherplatz.

Interval

Aufnahmeintervall für Live-Bilder.

Capture Delay Time

Dauer der Erfassung von Bildern.

5.2 Aufnahmeplanung konfigurieren

Das Gerät nimmt automatisch Bilder gemäß dem Zeitplan auf.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Festplatten oder Netzwerkfestplatten zur Speicherung installiert haben.

Schritte

1. Gehen Sie zu **Storage** → **Capture Schedule**.
2. Wählen Sie eine Kamera aus.
3. Legen Sie den Zeitplan für die Bilderfassung fest. Weitere Informationen zu den Zeitplaneinstellungen finden Sie unter ***Planaufzeichnung konfigurieren***.

5.3 Feiertags-Aufnahmeplan konfigurieren

Sie können den Aufnahmeplan an Feiertagen des Jahres festlegen. Der Rekorder folgt während der Feiertage dem Feiertags-Aufnahmeplan als Priorität.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Festplatten oder Netzwerkfestplatten zur Speicherung installiert haben.

Schritte

1. Gehen Sie zu **System** → **Holiday**.
2. Wählen Sie ein Feiertagselement aus der Liste aus und klicken Sie auf .
3. Aktivieren Sie das Kontrollkästchen **Enable**.
4. Bearbeiten Sie Feiertagsparameter wie Name, Modus oder Datum.

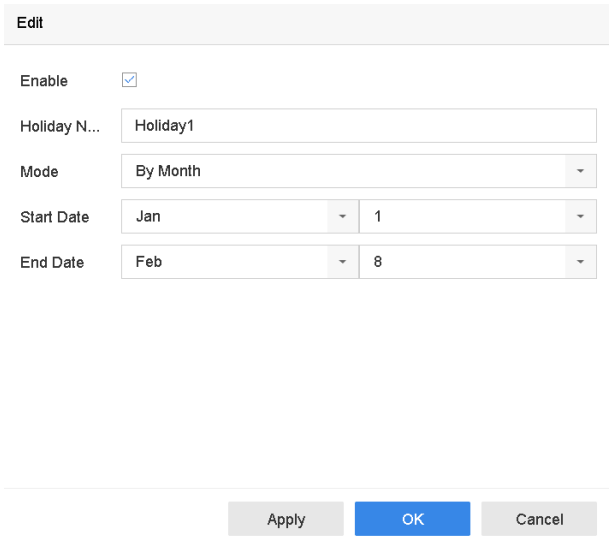


Abbildung 5-1 Feiertagseinstellungen bearbeiten

5. Klicken Sie auf **OK**.
6. Stellen Sie den Feiertagserfassungsplan ein. Weitere Informationen zu den Planeinstellungen finden Sie im Kapitel ***Planaufzeichnung konfigurieren***.

Kapitel 6 Ereignis

6.1 Normal-Ereignisalarm

6.1.1 Bewegungserkennungsalarme konfigurieren

Die Bewegungserkennung ermöglicht dem Gerät die Erkennung sich bewegender Objekte im Überwachungsbereich und das Auslösen von Alarmen.

Schritte

1. Gehen Sie zu **System** → **Event** → **Normal Event** → **Motion Detection**.
2. Wählen Sie eine Kamera aus.
3. Aktivieren Sie das Kontrollkästchen **Enable**.
4. Legen Sie die Bewegungserkennungsregel fest.

Für Kameras mit Personen- und Fahrzeugerkennung.	Klicken Sie auf **Draw Area**, um die Erkennungsbereiche auf dem Vorschaubildschirm zu zeichnen. Stellen Sie für **Target Detection** die Option **Human Body** oder **Vehicle** ein, um alle Alarme zu verwerfen, die nicht von Menschen oder Fahrzeugen ausgelöst werden.
Für Kameras ohne Personen- und Fahrzeugerkennung.	Klicken Sie auf **Full screen**, um den Vollbildschirm als Erkennungsbereich festzulegen, oder ziehen Sie den Mauszeiger über den Vorschaubildschirm, um den benutzerdefinierten Erkennungsbereich zu zeichnen.

5. Stellen Sie **Sensitivity** ein (0-100). Mit der Empfindlichkeit können Sie kalibrieren, wie leicht eine Bewegung den Alarm auslöst. Ein höherer Wert führt zu einer schnelleren Auslösung der Bewegungserkennung.
6. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
7. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.

6.1.2 Videoverlustalarme konfigurieren

Die Videoverlusterkennung erkennt den Videoverlust eines Kanals und ergreift Maßnahmen als Reaktion auf den Alarm.

Schritte

1. Gehen Sie zu **System** → **Event** → **Normal Event** → **Video Loss**.
2. Wählen Sie eine Kamera aus.
3. Aktivieren Sie das Kontrollkästchen **Enable**.

4. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
5. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.

6.1.3 Videomanipulationsalarme konfigurieren

Die Videomanipulationserkennung löst einen Alarm aus, wenn das Kameraobjektiv verdeckt wird, und leitet entsprechende Maßnahmen ein.

Schritte

1. Gehen Sie zu **System** → **Event** → **Normal Event** → **Video Tampering**.
2. Wählen Sie eine Kamera aus.
3. Aktivieren Sie das Kontrollkästchen **Enable**.
4. Stellen Sie den Videomanipulationsbereich ein. Ziehen Sie mit der Maus auf dem Vorschaubildschirm den angepassten Videomanipulationsbereich.
5. Stellen Sie **Sensitivity** ein (0-2). Es stehen 3 Stufen zur Verfügung. Mit der Empfindlichkeit wird eingestellt, wie leicht eine Bewegung den Alarm auslöst. Ein höherer Wert löst die Videomanipulationserkennung schneller aus.
6. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
7. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.

6.1.4 Sensoralarme konfigurieren

Legen Sie die Handhabung für einen externen Sensoralarm fest.

Schritte

1. Gehen Sie zu **System** → **Event** → **Normal Event** → **Alarm Input**.
2. Wählen Sie ein Alarmeingabeelement aus der Liste aus und klicken Sie auf .
3. Wählen Sie den Alarmeingang aus.
4. Bearbeiten Sie den Alarmnamen.
5. Aktivieren Sie das Kontrollkästchen **Input**.
6. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
7. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.

6.1.5 Ausnahmealarme konfigurieren

Ausnahmeereignisse können konfiguriert werden, um den Ereignishinweis in der Live-Ansicht aufzunehmen und Alarmausgänge und Verknüpfungsaktionen auszulösen.

Schritte

1. Gehen Sie zu **System** → **Event** → **Normal Event** → **Exception**.
2. Optional: Aktivieren Sie den Ereignishinweis, um ihn in der Live-Ansicht anzuzeigen.
   1) Aktivieren Sie das Kontrollkästchen **Enable Event Hint**.
   2) Klicken Sie auf , um den/die Ausnahmetyp(en) für den Ereignishinweis zu wählen.

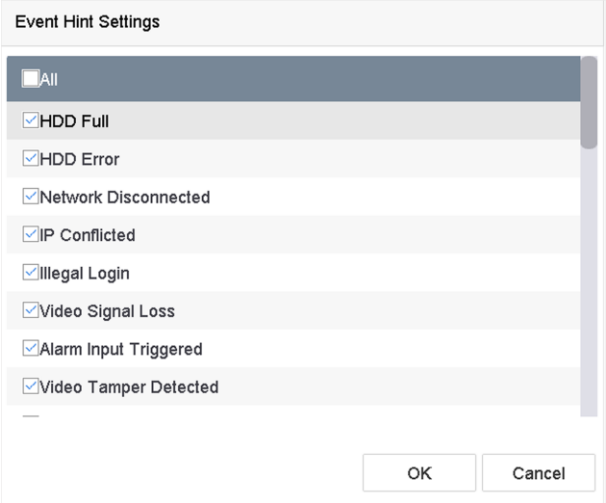


Abbildung 6-1 Einstellungen für Ereignishinweise

3. Wählen Sie einen Ausnahmetyp aus.

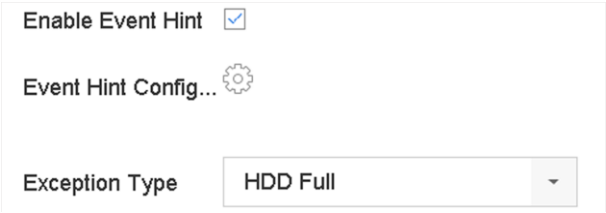


Abbildung 6-2 Umgang mit Ausnahmen

4. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.

6.1.6 Kombialarm konfigurieren

Ein Kombialarm kombiniert Ereignisse mit Alarmeingängen. Der Kombialarm wird ausgelöst, wenn er Alarme von Alarmeingängen und Alarmereignissen empfängt. Zu den Ereignistypen gehören Bewegungserkennung, Videomanipulationserkennung und andere intelligente Ereignisse, wie z. B. Linienüberschreitungserkennung, Eindringungserkennung usw.

Bevor Sie beginnen

Stellen Sie sicher, dass dem Kanal je nach Wunsch ein Ereignisalarm zugewiesen wurde und der Alarmeingang konfiguriert wurde (siehe ***Sensoralarme konfigurieren***).

Schritte

1. Gehen Sie zu **System** → **Event** → **Normal Event** → **Alarm Input**.
2. Wählen Sie ein Alarmeingabeelement aus der Liste aus und klicken Sie auf .
3. Wählen Sie für **Settings** die Option **Input**.
4. Klicken Sie auf **Combined Alarm**.
5. Wählen Sie den gewünschten Kanal aus.
6. Wählen Sie **Combined Alarm Event**.
7. Klicken Sie auf **Apply**.

Hinweis

Der Kombialarm-Scharfschaltplan und die Verknüpfungsaktion sind identisch mit den ausgewählten Ereignissen.

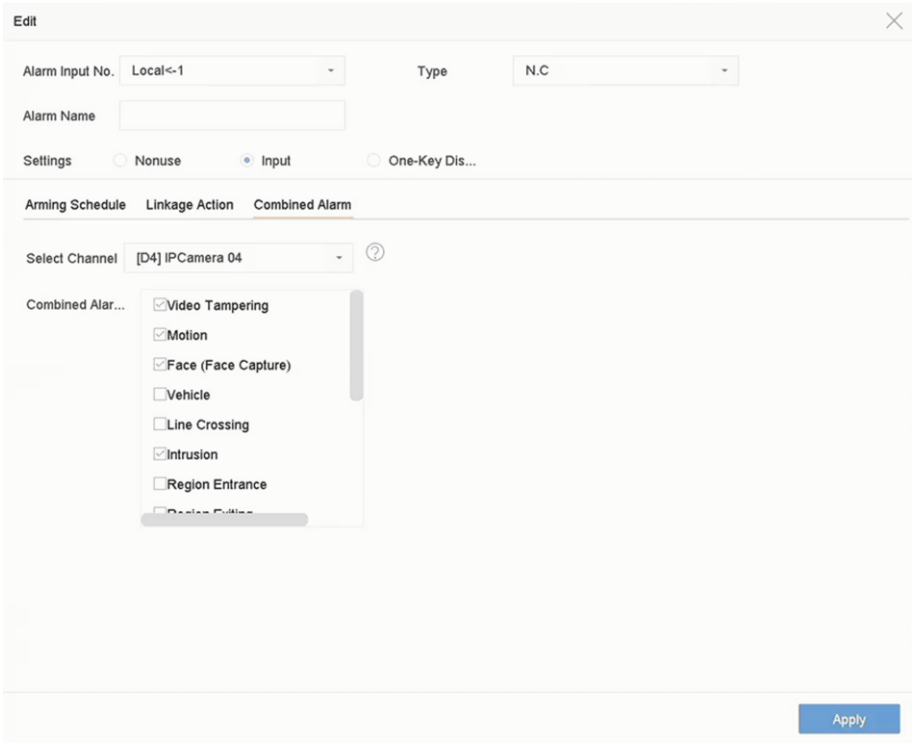


Abbildung 6-3 Kombialarm

6.2 VCA-Ereignisalarm

Das Gerät unterstützt den Empfang von VCA-Erkennungen, die von angeschlossenen IP-Kameras gesendet werden. Aktivieren und konfigurieren Sie zunächst die VCA-Erkennung im IP-Kamera-Einstellungsmenü.

Hinweis

- VCA-Erkennungen müssen von der angeschlossenen IP-Kamera unterstützt werden.
- Detaillierte Anweisungen zur VCA-Erkennung finden sich im Netzwerkkamera-Benutzerhandbuch.

6.2.1 Gesichtserkennung

Die Gesichtserkennung erkennt das Gesicht, das in der Überwachungsszene erscheint. Verknüpfungsaktionen können ausgelöst werden, wenn ein menschliches Gesicht erkannt wird.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Klicken Sie auf **Face Detection**.

Abbildung 6-4 Gesichtserkennung

3. Wählen Sie die zu konfigurierende Kamera aus.
4. Aktivieren Sie das Kontrollkästchen **Enable Face Detection**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Gesichtserkennung zu speichern.
6. Stellen Sie die Erkennungsempfindlichkeit ein. Empfindlichkeitsbereich: [1 - 5]. Je höher der Wert, desto leichter wird das Gesicht erkannt.
7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***
8. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***
9. Klicken Sie auf **Apply**.

6.2.2 Temperaturüberwachung

Nach dem Verbinden mit den angegebenen Wärmebildkameras kann das Gerät die Ergebnisse der Temperaturmessung anzeigen und Sie mit einem akustischen Alarm benachrichtigen, wenn eine normale oder abnormale Temperatur erkannt wird.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihre Wärmebildkamera diese Funktion unterstützt und ordnungsgemäß konfiguriert ist.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Wählen Sie den optischen Kanal der Wärmebildkamera aus.
3. Klicken Sie auf **Face Capture**.
4. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Gesichtserkennung zu speichern.
5. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
6. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***. Wenn bei der Erkennung abnormaler Temperaturen nur Verknüpfungsaktionen erfolgen sollen, gehen Sie zu **More** und aktivieren Sie das Kontrollkästchen **Abnormal Body Temperature**.

Hinweis

Die abnormale Temperatur wird von der Wärmebildkamera erkannt und definiert.

7. Gehen Sie zu **Audio Alert** und aktivieren Sie das Kontrollkästchen **Normal Temperature** oder **Abnormal Temperature**. Sie werden durch einen akustischen Alarm benachrichtigt, wenn die Kamera normale oder abnormale Temperaturen erkennt.

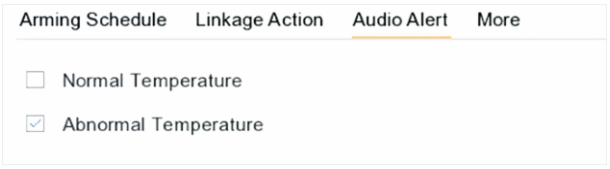


Abbildung 6-5 Audioalarm

8. Klicken Sie auf **Apply**.

Was folgt als Nächstes

- Sie können die Option für **Target Detection** in der Live-Ansicht aktivieren, um die Erkennungsergebnisse anzuzeigen.
- Sie können zu **File Management** → **Smart Search** → **Search by Appearance** gehen, um die Erkennungsergebnisse zu suchen.

6.2.3 Fahrzeugerkennung konfigurieren

Die Fahrzeugerkennung ist für die Überwachung des Straßenverkehrs verfügbar. In der Fahrzeugerkennung kann ein vorbeigefahrenes Fahrzeug erkannt und das Kennzeichen erfasst werden. Sie können ein Alarmsignal senden, um die Überwachungszentrale zu benachrichtigen und das aufgenommene Bild auf einen FTP-Server hochzuladen.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Wählen Sie die zu konfigurierende Kamera aus.
3. Klicken Sie auf **Vehicle**.

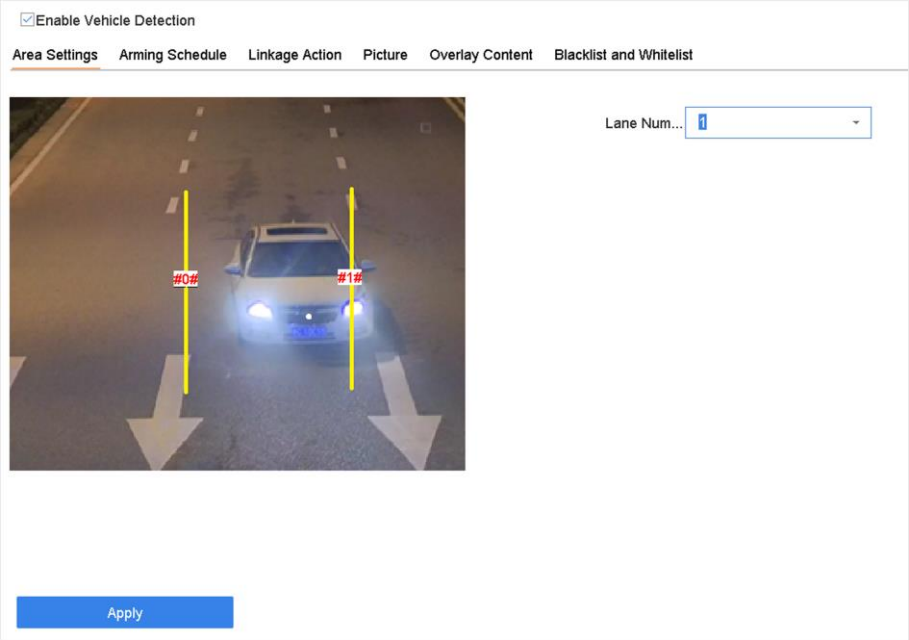


Abbildung 6-6 Fahrzeugerkennung

4. Aktivieren Sie das Kontrollkästchen **Enable Vehicle Detection**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Fahrzeugerkennungsbilder zu speichern.
6. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***
7. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***
8. Konfigurieren Sie die Regeln für **Area Settings**, **Picture**, **Overlay Content** und **Blacklist and Whitelist**.

   Area Settings

   Bis zu 4 Fahrspuren sind wählbar.

   Blacklist und Whitelist

   Sie können die Datei zuerst exportieren, um ihr Format zu prüfen, sie bearbeiten und auf das Gerät importieren.
9. Klicken Sie auf **Apply**.

Hinweis

Siehe das Benutzerhandbuch der Netzwerkkamera für detaillierte Anweisungen zur Fahrzeugerkennung.

6.2.4 Linienüberschreitungserkennung

Die Linienüberschreitungserkennung erkennt Personen, Fahrzeuge und Objekte, die eine vorgegebene virtuelle Linie überqueren. Die Erfassungsrichtung kann als bidirektional, von links

nach rechts oder von rechts nach links eingestellt werden.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Klicken Sie auf **Line Crossing**.

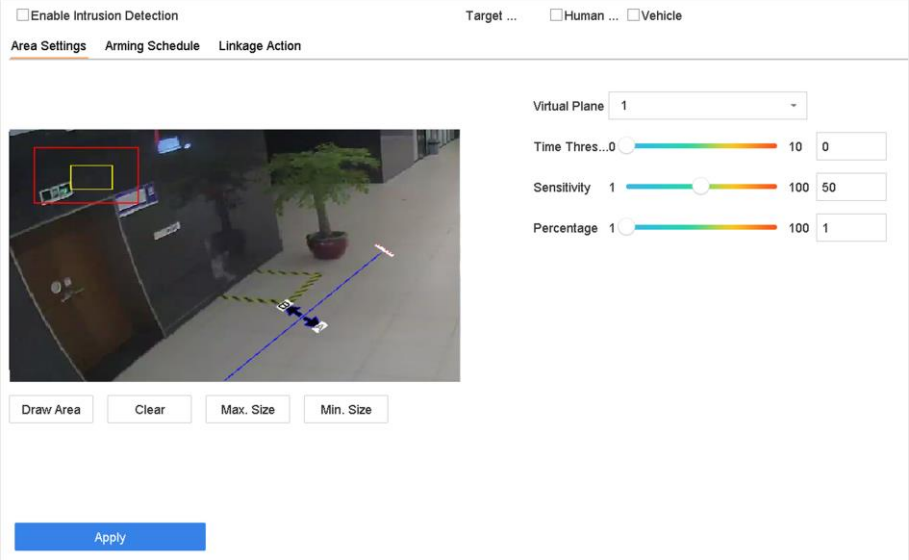


Abbildung 6-7 Linienüberschreitungserkennung

3. Wählen Sie eine Kamera aus.
4. Aktivieren Sie die Option **Enable Line Crossing Detection**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Linienüberschreitungserkennung zu speichern.
6. Legen Sie die Regeln und Erkennungsbereiche für die Linienüberschreitung fest.
   1) Wählen Sie einen Scharfschaltbereich aus.
   2) Wählen Sie für **Direction** die Option **A<->B**, **A->B** oder **A<-B** aus.

      A<->B

      Nur der Pfeil auf der B-Seite wird angezeigt. Überschreitet ein Objekt die konfigurierte Linie in einer beliebigen Richtung, kann dies erkannt und ein Alarm ausgelöst werden.

      A->B

      Nur ein Objekt, das die konfigurierte Linie von der A-Seite zur B-Seite überschreitet, wird erkannt.

      B->A

      Nur ein Objekt, das die konfigurierte Linie von der B-Seite zur A-Seite überschreitet, wird erkannt.
   3) Stellen Sie die Erkennungsempfindlichkeit ein. Je höher der Wert, desto einfacher wird der Erkennungsalarm ausgelöst.
   4) Klicken Sie auf **Draw Region**.
   5) Zeichnen Sie im Vorschaufenster eine virtuelle Linie.

7. Optional: Zeichnen Sie die maximale Größe/Mindestgröße für Ziele. Nur Ziele ab der Mindestgröße bis zur maximalen Größe lösen die Linienüberschreitungserkennung aus.
   1) Klicken Sie auf **Max. Size/Min. Size**.
   2) Zeichnen Sie einen Bereich im Vorschaufenster.
   3) Klicken Sie auf **Stop Drawing**.
8. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
9. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
10. Klicken Sie auf **Apply**.

6.2.5 Eindringungserkennung

Die Eindringungserkennung erkennt Personen, Fahrzeuge und andere Objekte, die in eine vordefinierte virtuelle Region eindringen und sich dort aufhalten. Wenn ein Alarm ausgelöst wird, können spezifische Maßnahmen ergriffen werden.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Klicken Sie auf **Intrusion**.

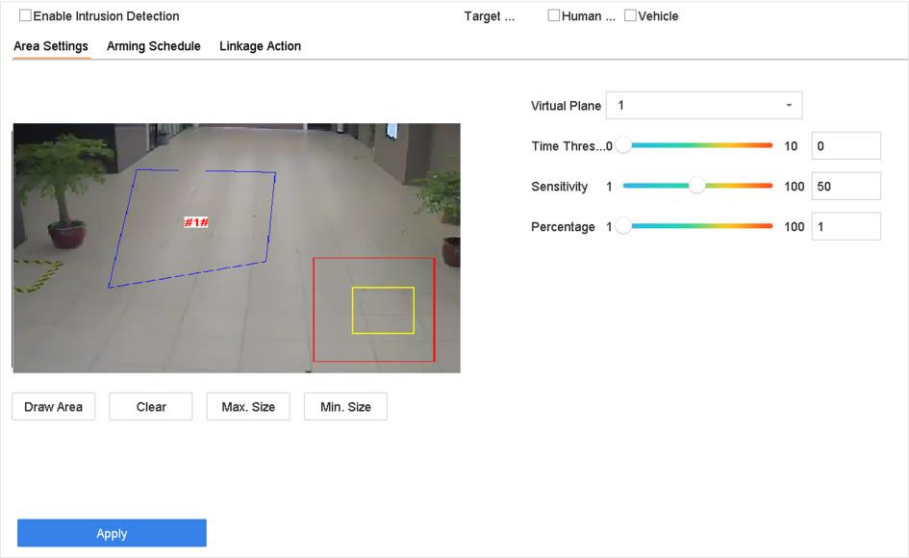


Abbildung 6-8 Eindringungserkennung

3. Aktivieren Sie das Kontrollkästchen **Enable Intrusion Detection**.
4. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Eindringungserkennungsbilder zu speichern.
5. Legen Sie die Erkennungsregeln und Erkennungsbereiche fest.
   1) Wählen Sie einen virtuellen Bereich aus. Bis zu 4 virtuelle Bereiche sind wählbar.
   2) Legen Sie **Time Threshold** und **Sensitivity** fest.

Time Threshold

Die Zeit, die ein Objekt in dem Bereich verweilt. Überschreitet die Aufenthaltsdauer des Objekts im definierten Erfassungsbereich die Schwelle, löst das Gerät einen Alarm aus.

Sensitivity

Die Größe des Objekts, das den Alarm auslösen kann. Je höher der Wert, desto leichter wird der Erkennungsalarm ausgelöst.

3) Klicken Sie auf **Draw Area**.
4) Zeichnen Sie im Vorschaufenster ein Viereck.

6. Optional: Zeichnen Sie die maximale Größe/Mindestgröße für Ziele. Nur Ziele ab der Mindestgröße bis zur maximalen Größe lösen die Linienüberschreitungserkennung aus.
   1) Klicken Sie auf **Max. Size/Min. Size**.
   2) Zeichnen Sie einen Bereich im Vorschaufenster.
   3) Klicken Sie auf **Stop Drawing**.
7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
8. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
9. Klicken Sie auf **Apply**.

6.2.6 Eintrittsüberwachung

Die Eintrittsüberwachung erkennt Objekte, die in einen vordefinierten virtuellen Bereich eintreten.

Schritte

1. Gehen Sie zu **System Management** → **Event Settings** → **Smart Event**.
2. Klicken Sie auf **Region Entrance Detection**.

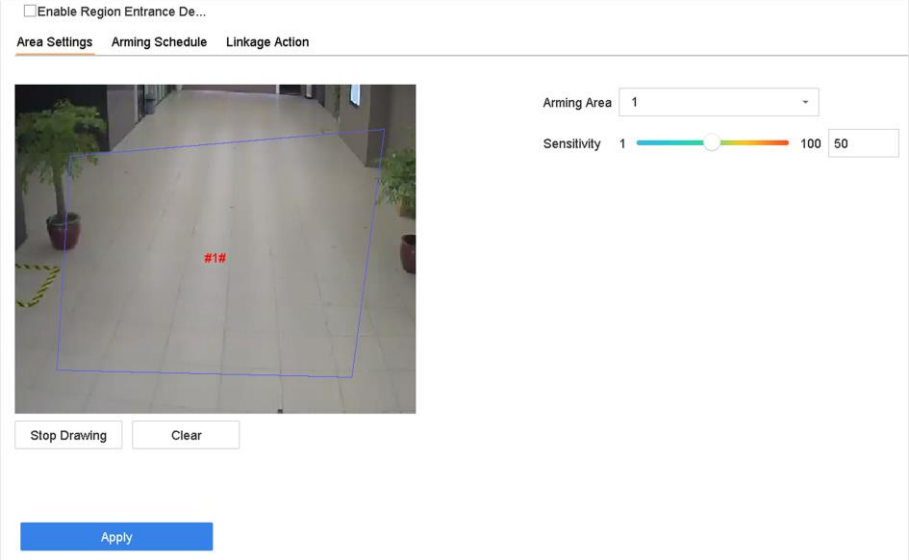


Abbildung 6-9 Eintrittsüberwachung

3. Wählen Sie eine Kamera aus.
4. Aktivieren Sie das Kontrollkästchen **Enable Region Entrance Detection**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die aufgenommenen Bilder der Eintrittsüberwachung zu speichern.
6. Legen Sie Erkennungsregeln und Erkennungsbereiche fest.
   1) Wählen Sie **Arming Region**. Bis zu 4 Regionen sind wählbar.

2) Legen Sie den Wert für **Sensitivity** fest. Je höher der Wert, desto leichter wird der Erkennungsalarm ausgelöst. Der Bereich ist [0 - 100].
3) Klicken Sie auf **Draw Region** und zeichnen Sie ein Viereck im Vorschaufenster.

7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
8. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
9. Klicken Sie auf **Apply**.

6.2.7 Austrittsüberwachung

Die Austrittsüberwachung erkennt Objekte, die aus einem vordefinierten virtuellen Bereich austreten.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Klicken Sie auf **Region Exiting**.

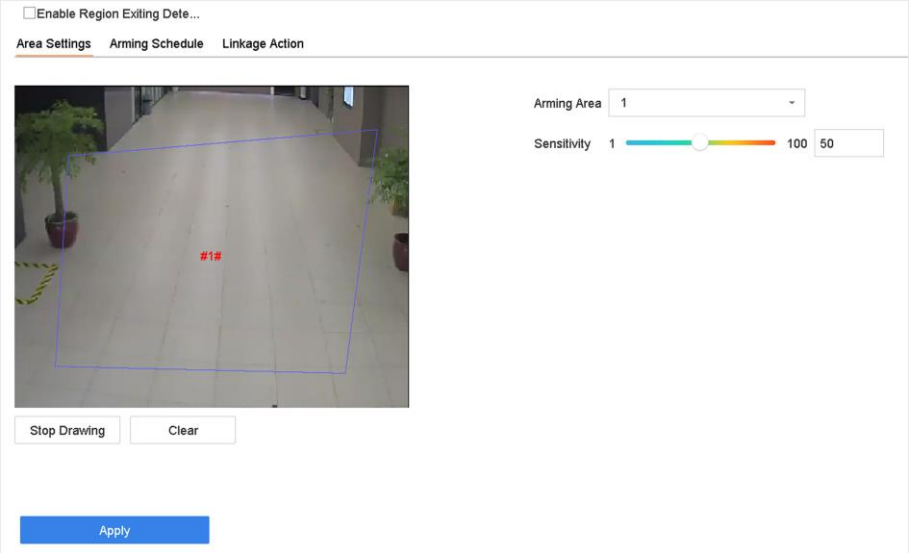


Abbildung 6-10 Austrittsüberwachung

3. Wählen Sie eine Kamera aus.
4. Aktivieren Sie das Kontrollkästchen **Enable Region Exiting Detection**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Austrittsüberwachung zu speichern.
6. Führen Sie die folgenden Schritte aus, um die Erkennungsregeln und Erkennungsbereiche festzulegen.
   1) Wählen Sie **Arming Region**. Bis zu 4 Regionen sind wählbar.
   2) Legen Sie den Wert für **Sensitivity** fest. Je höher der Wert, desto leichter wird der Erkennungsalarm ausgelöst. Der Bereich ist [0 - 100].
   3) Klicken Sie auf **Draw Region** und zeichnen Sie ein Viereck im Vorschaufenster.
7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
8. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
9. Klicken Sie auf **Apply**.

6.2.8 Verweilerkennung

Mithilfe der Verweilerkennung wird ermittelt, ob das Ziel die maximale Aufenthaltszeit innerhalb eines bestimmten Bereichs überschreitet, und es wird ein Alarm für Verknüpfungsaktionen ausgelöst.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Wählen Sie die zu konfigurierende Kamera aus.
3. Klicken Sie auf **Loitering Detection**.

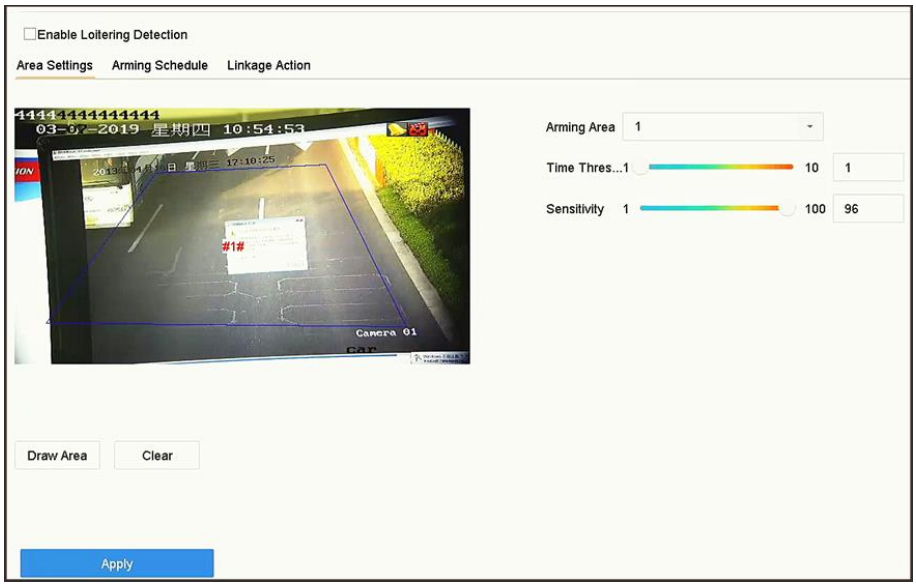


Abbildung 6-11 Verweilerkennung

4. Aktivieren Sie das Kontrollkästchen **Enable Loitering Detection**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die von der Verweilerkennung erfassten Bilder zu speichern.
6. Stellen Sie die Parameter für die Verweilerkennung ein.
   1) Wählen Sie **Arming Region**. Bis zu 4 Regionen sind wählbar.
   2) Legen Sie den Wert für **Time Threshold** fest.

      Time Threshold

      Die Zeit, über die sich das Fahrzeug in der Region aufhält. Liegt der Wert bei 10, wird ein Alarm ausgelöst, nachdem das Fahrzeug länger als 10 Sekunden in der Region verblieben ist. Der Bereich ist [1s - 10s].
   3) Legen Sie den Wert für **Sensitivity** fest.

      Sensitivity

      Ähnlichkeit mit dem Hintergrundbild des Objekts. Je höher der Wert, desto leichter wird der Erkennungsalarm ausgelöst.
7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***
8. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***

9. Klicken Sie auf **Apply**.

6.2.9 Versammlungserkennung

Die Versammlungserkennung wird verwendet, um zu erkennen, ob die Personendichte in einem bestimmten Bereich den eingestellten Wert überschreitet. Sie löst einen Alarm für Verknüpfungsaktionen aus.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Wählen Sie die zu konfigurierende Kamera aus.
3. Klicken Sie auf **People Gathering**.

Abbildung 6-12 Versammlungserkennung

4. Aktivieren Sie das Kontrollkästchen **Enable People Gathering Detection**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Versammlungserkennung zu speichern.
6. Legen Sie die Parameter der Versammlungserkennung fest.
   1) Wählen Sie **Arming Region**. Bis zu 4 Regionen sind wählbar.
   2) Klicken Sie auf **Draw Region** und zeichnen Sie im Vorschaufenster ein Viereck, indem Sie die vier Ecken des Erkennungsbereichs angeben.
   3) Legen Sie den Wert für **Percentage** fest.

   Percentage

   Bezieht sich auf die Personendichte innerhalb des Bereichs. Wenn der Schwellenwert überschritten wird, löst das Gerät einen Alarm aus.
7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***
8. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***
9. Klicken Sie auf **Apply**.

6.2.10 Schnellbewegungserkennung

Die Schnellbewegungserkennung erkennt verdächtiges Laufen und Verfolgen, Geschwindigkeitsüberschreitungen und schnelle Bewegungen. Sie löst einen Alarm aus, wenn sich ein Objekt schnell bewegt, und sendet eine Benachrichtigung an den Scharfschalte-Host, damit die erforderlichen Maßnahmen im Voraus ergriffen werden können.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Wählen Sie die zu konfigurierende Kamera aus.
3. Klicken Sie auf **Fast Moving**.

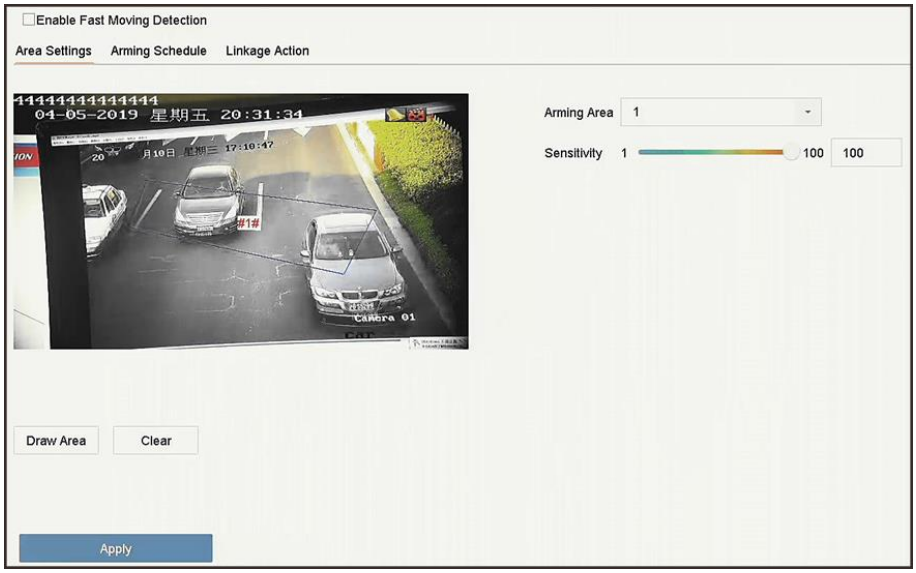


Abbildung 6-13 Schnellbewegungserkennung

4. Aktivieren Sie die Option **Enable Fast Moving**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Schnellbewegungserkennung zu speichern.
6. Legen Sie die Parameter für die Schnellbewegungserkennung fest.
   1) Wählen Sie **Arming Region**. Bis zu 4 Regionen sind wählbar.
   2) Klicken Sie auf **Draw Region** und zeichnen Sie im Vorschaufenster ein Viereck, indem Sie die vier Ecken des Erkennungsbereichs angeben.
   3) Legen Sie den Wert für **Sensitivity** fest.

   Hinweis

   Empfindlichkeit: Ähnlichkeit mit dem Hintergrundbild des Objekts. Je höher der Wert, desto leichter wird der Erkennungsalarm ausgelöst.

7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***
8. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***
9. Klicken Sie auf **Apply**.

6.2.11 Parkerkennung

Die Parkerkennung erkennt Parkverstöße im festgelegten Bereich auf Schnellstraßen und in Einbahnstraßen.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Wählen Sie die zu konfigurierende Kamera aus.
3. Klicken Sie auf **Parking**.

Abbildung 6-14 Parkerkennung

4. Aktivieren Sie die Option **Enable Parking Detection**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die von der Parkerkennung erfassten Bilder zu speichern.
6. Stellen Sie die Parameter für die Parkerkennung ein.
   1) Wählen Sie **Arming Region**. Bis zu 4 Regionen sind wählbar.
   2) Legen Sie den Wert für **Time Threshold** fest.

      Time Threshold

      Die Zeit, über die sich das Fahrzeug in der Region aufhält. Liegt der Wert bei 10, wird ein Alarm ausgelöst, nachdem das Fahrzeug länger als 10 Sekunden in der Region verblieben ist. Der Bereich ist [5s - 20s].
   3) Legen Sie den Wert für **Sensitivity** fest.

      Sensitivity

      Ähnlichkeit mit dem Hintergrundbild des Objekts. Je höher der Wert, desto leichter wird der Erkennungsalarm ausgelöst.
7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***
8. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***
9. Klicken Sie auf **Apply**.

6.2.12 Unbeaufsichtigtes-Gepäck-Erkennung

Die Unbeaufsichtigtes-Gepäck-Erkennung erkennt Objekte, die in einer vordefinierten Region zurückgelassen wurden, wie z. B. Gepäck, Handtaschen, gefährliche Materialien usw., und kann bei Auslösung des Alarms verschiedene Maßnahmen einleiten.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Klicken Sie auf **Unattended Baggage**.

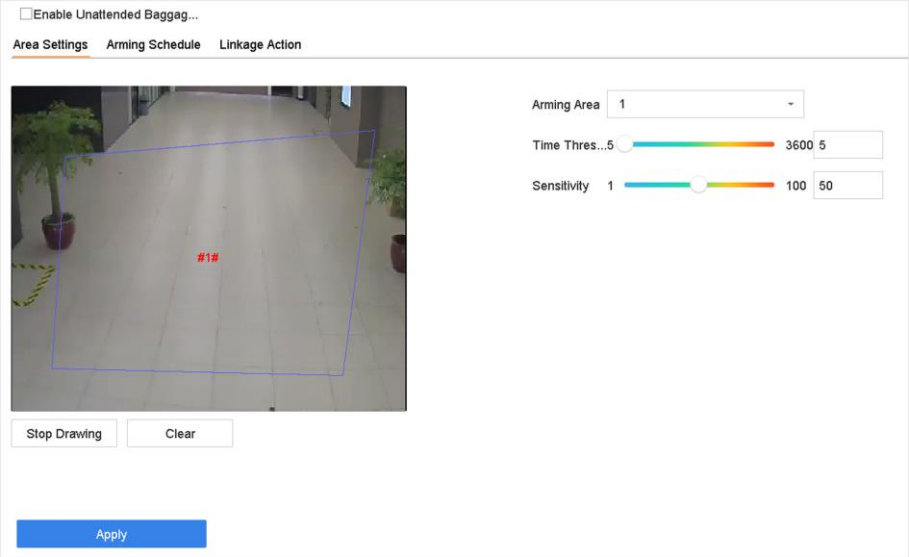


Abbildung 6-15 Unbeaufsichtigtes-Gepäck-Erkennung

3. Wählen Sie eine Kamera aus.
4. Aktivieren Sie die Option **Enable Unattended Baggage Detection**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Unbeaufsichtigtes-Gepäck-Erkennung zu speichern.
6. Legen Sie die Erkennungsregeln und Erkennungsbereiche fest.
   1) Wählen Sie **Arming Region**. Bis zu 4 Regionen sind wählbar.
   2) Verschieben Sie die Schieberegler, um die Werte für **Time Threshold** und **Sensitivity** festzulegen.

      Time Threshold

      Die Zeit, die Objekte in dem Bereich belassen werden. Ist der Wert 10, wird ein Alarm ausgelöst, nachdem das Objekt zurückgelassen wurde und im Bereich für 10 Sekunden verblieben ist. Der Bereich ist [5s - 20s].

      Sensitivity

      Ähnlichkeit mit dem Hintergrundbild des Objekts. Je höher der Wert, desto leichter wird der Erkennungsalarm ausgelöst.
   3) Klicken Sie auf **Draw Region** und zeichnen Sie ein Viereck im Vorschaufenster.
7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
8. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.

9. Klicken Sie auf **Apply**.

6.2.13 Objektentfernungserkennung

Die Objektentfernungserkennung erkennt die aus einem vordefinierten Bereich entfernten Objekte, z. B. ausgestellte Exponate, und kann verschiedene Aktionen einleiten, wenn der Alarm ausgelöst wird.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Klicken Sie auf **Object Removable**.

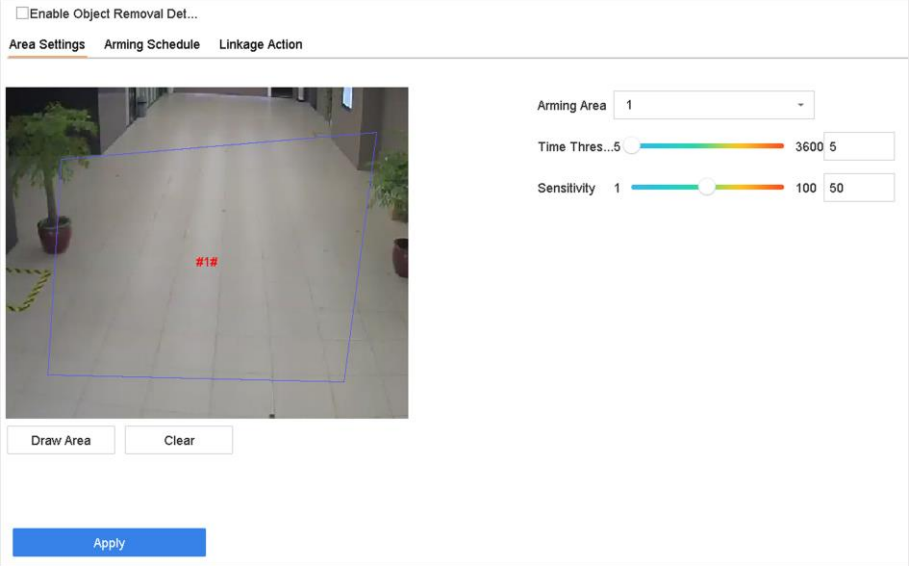


Abbildung 6-16 Objektentfernungserkennung

3. Wählen Sie die zu konfigurierende Kamera aus.
4. Aktivieren Sie die Option **Enable Object Removable Detection**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Objektentfernungserkennung zu speichern.
6. Führen Sie die folgenden Schritte aus, um die Erkennungsregeln und Erkennungsbereiche festzulegen.
   1) Wählen Sie „Arming Region“ aus. Bis zu 4 Regionen sind wählbar.
   2) Verschieben Sie die Schieberegler, um die Werte für **Time Threshold** und **Sensitivity** festzulegen.

Time Threshold

Die Zeitdauer, für die Objekte aus dem Bereich entfernt wurden. Ist der Wert 10, wird ein Alarm ausgelöst, nachdem das Objekt für 10 Sekunden aus dem Bereich verschwunden ist. Der Bereich ist [5s - 20s].

Sensitivity

Ähnlichkeit mit dem Hintergrundbild des Objekts. Ist die Empfindlichkeit hoch, löst ein sehr

kleines aus dem Bereich entferntes Objekt den Alarm aus.

3) Klicken Sie auf **Draw Region** und zeichnen Sie im Vorschaufenster ein Viereck, indem Sie die vier Ecken des Erkennungsbereichs angeben.

7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
8. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
9. Klicken Sie auf **Apply**.

6.2.14 Audioausnahmeerkennung

Die Audioausnahmeerkennung erkennt anormale Geräusche im Überwachungsbereich, wie eine plötzliche Zunahme oder Abnahme der Geräuschintensität.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Klicken Sie auf **Audio Exception**.

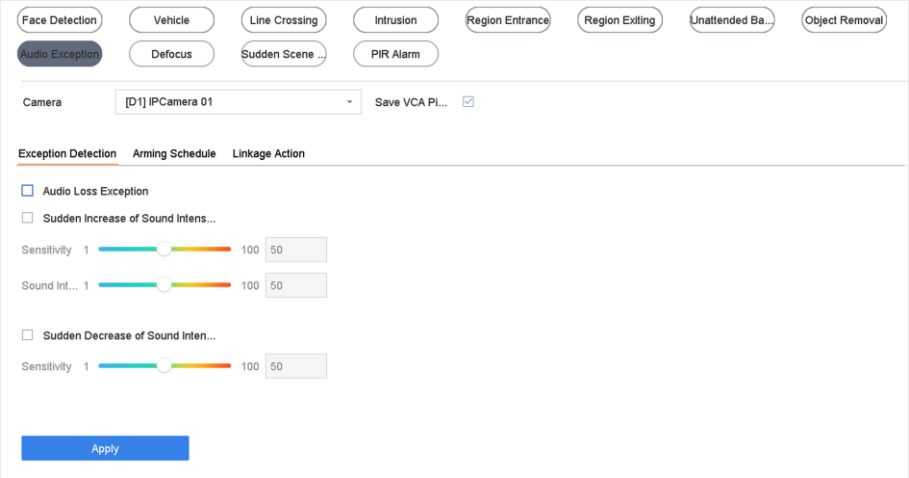


Abbildung 6-17 Audioausnahmeerkennung

3. Wählen Sie die zu konfigurierende Kamera aus.
4. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Audioausnahmeerkennung zu speichern.
5. Erkennungsregeln einstellen:
   1) Wählen Sie **Exception Detection**.
   2) Aktivieren Sie das Kontrollkästchen **Audio Loss Exception**, **Sudden Increase of Sound Intensity Detection** und/oder **Sudden Decrease of Sound Intensity Detection**.

Audio Loss Exception

Erkennt einen steilen Geräuschanstieg in der Überwachungsszene. Sie können die Erkennungsempfindlichkeit und die Schwelle für den steilen Geräuschanstieg einstellen, indem Sie **Sensitivity** und **Sound Intensity Threshold** konfigurieren.

Sensitivity

Je kleiner der Wert, desto stärker muss die Änderung sein, um die Erkennung auszulösen.

Der Bereich ist [1 - 100].

Sound Intensity Threshold

Das Umgebungsgeräusch kann gefiltert werden. Je lauter das Umgebungsgeräusch, desto höher muss der Wert sein. Passen Sie ihn der Umgebung an. Der Bereich ist [1 - 100].

Sudden Decrease of Sound Intensity Detection

Erkennt einen steilen Geräuschabfall in der Überwachungsszene. Sie müssen die Erkennungsempfindlichkeit einstellen [1 - 100].

6. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
7. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
8. Klicken Sie auf **Apply**.

6.2.15 Defokussierungserkennung

Eine Bildunschärfe durch Defokussierung des Objektivs kann erkannt werden.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Klicken Sie auf **Defocus**.

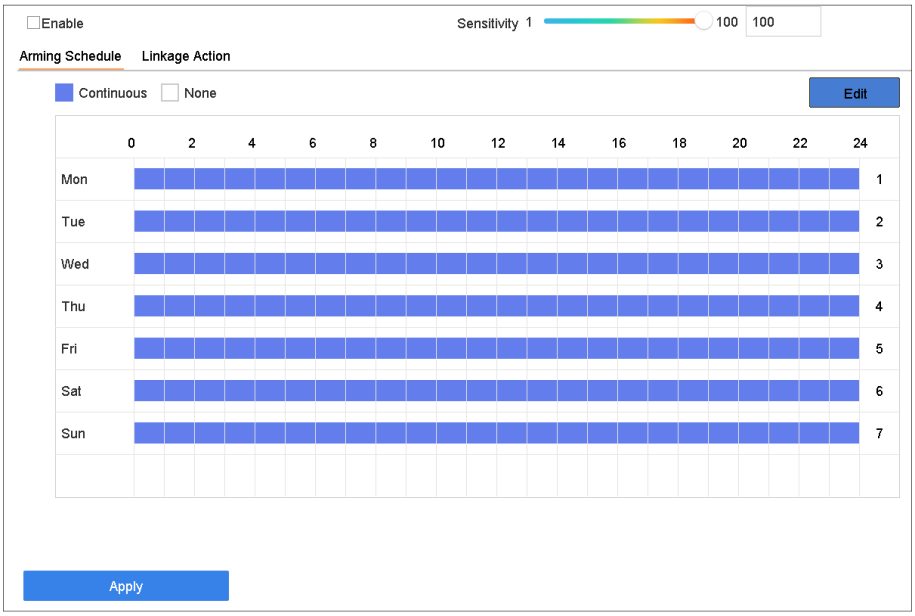


Abbildung 6-18 Defokussierungserkennung

3. Wählen Sie die zu konfigurierende Kamera aus.
4. Aktivieren Sie das Kontrollkästchen **Enable**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die von der Defokussierungserkennung erfassten Bilder zu speichern.
6. Verschieben Sie den Schieberegler **Sensitivity**, um die Erkennungsempfindlichkeit einzustellen.

Hinweis

Empfindlichkeitsbereich: [1 - 100]. Je höher der Wert, desto leichter wird das Defokussierungsbild erkannt.

7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
8. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
9. Klicken Sie auf **Apply**.

6.2.16 Szenenwechselerkennung

Die Szenenwechselerkennung erkennt eine Veränderung der Überwachungsumgebung, die durch externe Faktoren, wie die absichtliche Drehung der Kamera, beeinflusst wird.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Klicken Sie auf **Sudden Scene Change**.

Abbildung 6-19 Szenenwechsel

3. Wählen Sie die zu konfigurierende Kamera aus.
4. Aktivieren Sie das Kontrollkästchen **Enable**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Szenenwechselerkennung zu speichern.
6. Verschieben Sie den Schieberegler **Sensitivity**, um die Erkennungsempfindlichkeit einzustellen.

Hinweis

Empfindlichkeitsbereich: [1 - 100]. Je höher der Wert, desto leichter kann der Szenenwechsel den Alarm auslösen.

7. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
8. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
9. Klicken Sie auf **Apply**.

6.2.17 PIR-Alarm

Ein PIR-Alarm (Passiv-Infrarot-Alarm) wird ausgelöst, wenn sich ein Eindringling im Erfassungsbereich des Melders bewegt. Die durch eine Person oder warmblütige Tiere wie Hunde, Katzen usw. abgestrahlte Wärme wird erkannt.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Klicken Sie auf **PIR Alarm**.

Abbildung 6-20 PIR-Alarm

3. Wählen Sie die zu konfigurierende Kamera aus.
4. Aktivieren Sie das Kontrollkästchen **PIR Alarm**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die aufgenommenen Bilder des PIR-Alarms zu speichern.
6. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
7. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
8. Klicken Sie auf **Apply**.

6.2.18 Wärmebildkameraerkennung

Der NVR unterstützt die Ereigniserkennungsmodi der Wärmebild-Netzwerkkameras: Brand- und Raucherkennung, Temperaturerkennung, Temperaturdifferenzerkennung usw.

Bevor Sie beginnen

Fügen Sie Ihrem Gerät die Wärmebild-Netzwerkkamera hinzu und vergewissern Sie sich, dass die Kamera aktiviert ist.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Wählen Sie eine Wärmebildkamera aus der Kameraliste aus.
3. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Erkennung zu speichern.
4. Wählen Sie eine Ereigniserkennung aus (Temperatur usw.).
5. Legen Sie den Scharfschaltplan fest. Siehe ***Scharfschaltplan konfigurieren***.
6. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
7. Klicken Sie auf **Apply**.

6.2.19 Warteschlangenverwaltung konfigurieren

Nachdem Sie die Verbindung zur Kamera für die Warteschlangenverwaltung hergestellt haben, können Sie den Scharfschaltplan und die Verknüpfungsaktion der Warteschlangenverwaltung festlegen.

Bevor Sie beginnen

Stellen Sie sicher, dass der Rekorder mit der Kamera für die Warteschlangenverwaltung verbunden ist.

Schritte

1. Gehen Sie zu **System** → **Event** → **Smart Event**.
2. Wählen Sie eine Kamera für die Warteschlangenverwaltung aus der Kameraliste aus.
3. Optional: Aktivieren Sie das Kontrollkästchen **Save VCA Picture**, um die erfassten Bilder der Erkennung zu speichern.
4. Legen Sie den Scharfschaltplan fest. Weitere Informationen finden Sie im Kapitel ***Scharfschaltplan konfigurieren***.
5. Legen Sie die Verknüpfungsaktionen fest. Weitere Informationen finden Sie im Kapitel ***Verknüpfungsaktionen konfigurieren***.
6. Klicken Sie auf **Apply**.

6.2.20 Zielerkennung

In der Live-Ansicht kann die Zielerkennung verwendet werden, um menschliche Bewegungen/Gesichter/Fahrzeuge/Personen während der letzten 5 Sekunden und den folgenden

10 Sekunden zu erkennen.

Schritte

1. Klicken Sie im Live-Ansichtsmodus auf **Target Detection**, um das Zielerkennungsmenü aufzurufen.
2. Wählen Sie verschiedene Erkennungstypen aus: Smart Detection ( ), Fahrzeugerkennung ( ), Gesichtserkennung ( ) und Personenerkennung ( ).

Hinweis

Bei Wärmebildkameras findet die Temperaturmessung per Smart Detection ( ) und die Gesichtserfassung und Gesichtstemperaturmessung per Gesichtserkennung ( ) statt.

3. Wählen Sie die Verlaufsanalyse ( ) oder die Echtzeitanalyse ( ) aus, um die Ergebnisse zu erhalten.

Hinweis

Die intelligenten Analyseergebnisse der Erkennung werden in der Liste angezeigt. Klicken Sie auf ein Ergebnis in der Liste, um das zugehörige Video wiederzugeben.

4. Optional: Sie können Kanäle auswählen, die eine Bildaufnahme erfordern. Die nicht ausgewählten Kanäle erfassen kein Bild.
   1) Klicken Sie links unten in der Live-Ansicht auf .
   2) Wählen Sie die Kanäle aus. Die ausgewählten Kanäle erfassen ein Bild. Standardmäßig sind alle Kanäle ausgewählt.
   3) Klicken Sie auf **Finish**.

6.3 Scharfschaltplan konfigurieren

Schritte

1. Klicken Sie auf **Arming Schedule**.
2. Klicken Sie auf **Edit**.
3. Wählen Sie einen Wochentag aus und stellen Sie den Zeitraum ein. Es können bis zu acht Zeiträume pro Tag eingestellt werden.

Hinweis

Die Zeiträume dürfen sich nicht wiederholen oder überschneiden.

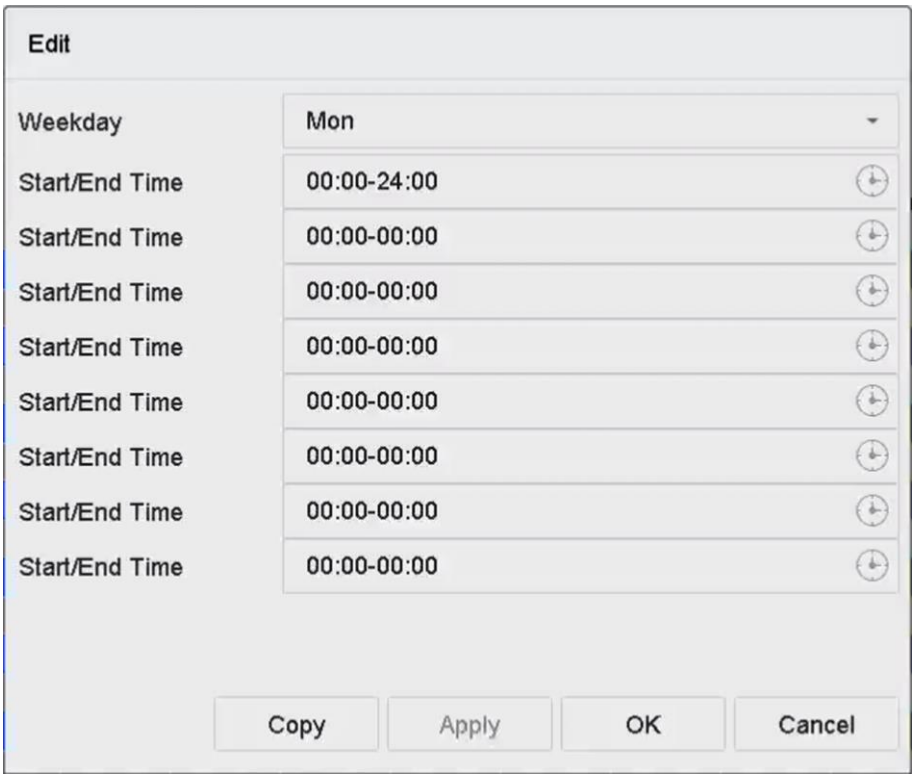


Abbildung 6-21 Scharfschaltplan festlegen

4. Sie können auf **Copy** klicken, um die Einstellungen des Scharfschaltplans auf andere Tage zu kopieren.
5. Klicken Sie auf **Apply**, um die Einstellungen zu speichern.

6.4 Verknüpfungsaktionen konfigurieren

Alarmverknüpfungsaktionen werden aktiviert, wenn ein Alarm oder eine Ausnahme eintritt, einschließlich Ereignishinweisanzeige, Vollbildüberwachung, akustische Warnung (Summer), Überwachungszentrale benachrichtigen, Alarmausgang auslösen und E-Mail senden.

6.4.1 Automatische Umschaltung der Vollbildüberwachung konfigurieren

Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor im Vollbildmodus das Videobild des konfigurierten Alarmierungskanals für die Vollbildüberwachung an. Wenn der Alarm in mehreren Kanälen gleichzeitig ausgelöst wird, müssen Sie die automatische Umschaltung der Verweilzeit

konfigurieren.

Hinweis

Die automatische Umschaltung wird beendet, sobald der Alarm endet und in das Livebildmenü zurückkehrt.

Schritte

1. Gehen Sie zu **System** → **Live View** → **General**.
2. Stellen Sie den Ereignisausgang und die Verweilzeit ein.

   Event Output

   Wählen Sie den Ausgang für die Anzeige des Ereignis-Video aus.

   Full Screen Monitoring Dwell Time

   Stellen Sie die Zeit für die Anzeige des Alarmereignisbildschirms in Sekunden ein. Werden Alarme gleichzeitig auf mehreren Kanälen ausgelöst, so werden deren Vollbilder im Abstand von 10 Sekunden umgeschaltet (Standard-Verweilzeit).
3. Gehen Sie in das Menü **Linkage Action** der Alarmerkennung (z. B. Bewegungserkennung, Videomanipulation, Gesichtserkennung usw.).
4. Wählen Sie die Alarmverknüpfungsaktion **Full Screen Monitoring**.
5. Wählen Sie die Kanäle in **Trigger Channel**, um die Vollbildüberwachung auszulösen.

6.4.2 Akustische Warnung konfigurieren

Die akustische Warnung lässt das System einen Signalton auslösen, wenn ein Alarm erkannt wird.

Schritte

1. Gehen Sie zu **System** → **View** → **General**.
2. Aktivieren Sie den Audioausgang und stellen Sie die Lautstärke ein.
3. Gehen Sie in das Menü **Linkage Action** der Alarmerkennung (z. B. Bewegungserkennung, Videomanipulation, Gesichtserkennung usw.).
4. Wählen Sie die Alarmverknüpfungsaktion **Audio Warning**.

6.4.3 Überwachungszentrale benachrichtigen

Das Gerät kann beim Eintreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den Remote-Alarm-Host senden. Der Alarm-Host bezieht sich auf den mit der Client-Software installierten PC (z. B. iVMS-4200, iVMS-5200).

Schritte

1. Gehen Sie zu **System** → **Network** → **Advanced** → **More Settings**.
2. Stellen Sie die Alarm-Host-IP und den Alarm-Host-Port ein.
3. Gehen Sie in das Menü **Linkage Action** der Alarmerkennung (z. B. Bewegungserkennung, Videomanipulation, Gesichtserkennung usw.).

4. Wählen Sie **Notify Surveillance Center**.

6.4.4 E-Mail-Verknüpfung konfigurieren

Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.

Schritte

1. Gehen Sie zu **System** → **Network** → **Advanced** → **Email**.
2. Legen Sie die E-Mail-Parameter fest.
3. Klicken Sie auf **Apply**.
4. Gehen Sie in das Menü **Linkage Action** der Alarmerkennung (z. B. Bewegungserkennung, Videomanipulation, Gesichtserkennung usw.).
5. Wählen Sie die Alarmverknüpfungsaktion **Send Email**.

6.4.5 Alarmausgang auslösen

Der Alarmausgang kann durch Alarmeingang, Bewegungserkennung, Videomanipulationsüberwachung, Gesichtserkennung, Linienüberschreitungserkennung und alle anderen Ereignisse ausgelöst werden.

Schritte

1. Gehen Sie in das Menü **Linkage Action** der Alarmerkennung (z. B. Bewegungserkennung, Gesichtserkennung, Linienüberschreitungserkennung, Eindringungserkennung usw.).
2. Wählen Sie im Bereich **Trigger Alarm Outputs** aus, welche Alarmausgabe(n) ausgelöst werden soll(en).
3. Gehen Sie zu **System** → **Event** → **Normal Event** → **Alarm Output**.
4. Wählen Sie ein Alarmausgabeelement aus der Liste aus.

Hinweis

Wenn das Gerät 8 Alarmausgänge hat, wird die 12-V-Steuerspannung durch den Alarmausgang 9 gesteuert. Schließen Sie den Pluspol an A der 12-V-Steuerung und den Minuspol an B der 12-V-Steuerung an. Die Stromversorgung wird eingeschaltet, wenn der Alarmausgang ausgelöst wird.

6.4.6 Verknüpfung von Audio- und Lichtalarm konfigurieren

Bei bestimmten Netzwerkkameras können Sie die Alarmverknüpfungsaktion als Audio- oder Lichtalarm einstellen.

Bevor Sie beginnen

- Stellen Sie sicher, dass Ihre Kamera die Audio- und Lichtalarmverknüpfung unterstützt.
- Stellen Sie sicher, dass Audioausgang und Lautstärke korrekt konfiguriert sind.

Schritte

1. Gehen Sie zum Menü mit der Verknüpfungsaktion der Alarmerkennung (z. B. Bewegungserkennung).
2. Stellen Sie **Audio and Light Alarm Linkage** wie gewünscht ein.
3. Klicken Sie auf **Apply**.

6.4.7 PTZ-Verknüpfung konfigurieren

Das System kann die PTZ-Aktionen (z. B. Voreinstellung/Tour/Muster) auslösen, wenn das Alarmereignis oder die VCA-Erkennung eintritt.

Bevor Sie beginnen

Vergewissern Sie sich, dass die angeschlossene PTZ- oder Hochgeschwindigkeits-Kuppelkamera die PTZ-Verknüpfung unterstützt.

Schritte

1. Gehen Sie in das Menü **Linkage Action** des Alarmeingangs oder der VCA-Erkennung (z. B. Gesichtserkennung, Linienüberschreitungserkennung, Eindringungserkennung).
2. Wählen Sie **PTZ Linkage**.
3. Wählen Sie die Kamera für Durchführung der PTZ-Aktionen aus.
4. Wählen Sie die Voreinstellungs-/Tour-/Musternummer, die beim Eintreten der Alarmereignisse aufgerufen werden soll.

Hinweis

Sie können jeweils nur einen PTZ-Typ für die Verknüpfungsaktion einstellen.

Kapitel 7 Intelligente Analyse

7.1 Personenzählung

Die Zählung berechnet die Anzahl der Personen, die einen konfigurierten Bereich betreten oder verlassen, und erstellt Tages-/Wochen-/Monats-/Jahresberichte zur Analyse.

Schritte

1. Gehen Sie zu **Smart Analysis** → **Counting**.
2. Wählen Sie die Kamera(s) aus.
3. Wählen Sie den Berichtstyp aus.
4. Stellen Sie **Date** zur Analyse ein. Die Personenzählgrafik wird angezeigt.

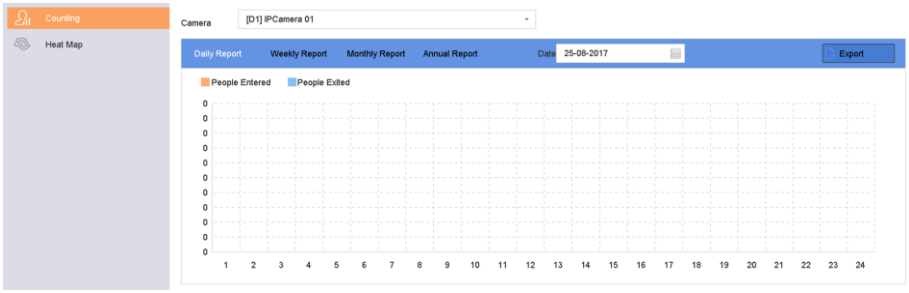


Abbildung 7-1 Menü für die Personenzählung

5. Optional: Klicken Sie auf **Export**, um den Bericht im Microsoft Excel-Format zu exportieren.

7.2 Wärmebildkarte

Die Wärmebildkarte ist eine grafische Darstellung der Daten. Die Wärmebildkarte wird verwendet, um zu analysieren, wie viele Personen einem bestimmten Bereich besucht und darin verweilt haben.

Bevor Sie beginnen

Die Wärmebildkarte muss durch die angeschlossene IP-Kamera unterstützt werden, und die entsprechende Konfiguration muss eingestellt sein.

Schritte

1. Gehen Sie zu **Smart Analysis** → **Heat Map**.
2. Wählen Sie eine Kamera aus.
3. Wählen Sie den Berichtstyp aus.
4. Stellen Sie **Date** zur Analyse ein.

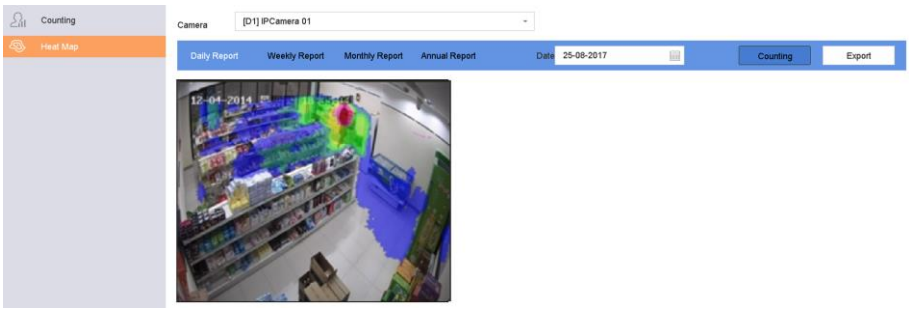


Abbildung 7-2 Menü zur Wärmebildkarte

5. Klicken Sie auf **Counting**. Die Ergebnisse werden in Grafiken mit verschiedenen Farben angezeigt.

Hinweis

Wie in der Abbildung oben dargestellt, zeigt der rote Farbblock (255, 0, 0) den verkehrsreichsten Bereich und der blaue Farbblock (0, 0, 255) den verkehrsärmeren Bereich an.

6. Optional: Klicken Sie auf **Export**, um den Statistikbericht im Microsoft Excel-Format zu exportieren.

Kapitel 8 POS-Konfiguration

Das Gerät kann an eine POS-Maschine oder einen POS-Server angeschlossen werden und erhält während der Live-Ansicht oder Wiedergabe eine Transaktionsmeldung zum Einblenden des Bilds sowie einen POS-Ereignisalarm.

8.1 POS-Verbindung konfigurieren

Schritte

1. Gehen Sie zu **System** → **POS**.
2. Klicken Sie auf **Add**.

Abbildung 8-1 POS-Einstellungen

3. Wählen Sie ein POS-Gerät aus der Dropdown-Liste aus.
4. Aktivieren Sie das Kontrollkästchen **Enable**.

Hinweis

Die Anzahl der POS-Geräte, die von jedem Gerät unterstützt werden, entspricht der Hälfte der jeweiligen Kanalanzahl. Beispiel: 8 POS-Geräte werden vom Modell DS-9616NI-I8 unterstützt.

5. Wählen Sie **POS Protocol**.

Hinweis

Wenn ein neues Protokoll ausgewählt wird, starten Sie das Gerät neu, um die neuen Einstellungen zu aktivieren.

Universal Protocol

Klicken Sie auf **Advanced**, um weitere Einstellungen bei Auswahl des Universalprotokolls anzuzeigen. Sie können die Start-Zeilen-Kennung, das Zeilenumbruch-Tag und das Zeilenende-Tag für die POS-Overlay-Zeichen und die Groß-/Kleinschreibung der Zeichen festlegen. Optional können Sie die Kontrollkästchen „Filtering Identifier“ und „XML Protocol“ aktivieren.

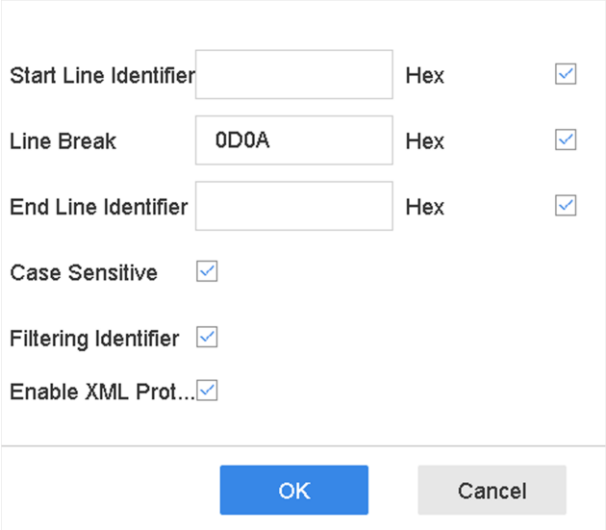


Abbildung 8-2 Einstellungen des Universalprotokolls

EPSON

Für das EPSON-Protokoll werden feststehende Start- und Endzeilen-Tags verwendet.

AVE

Für das AVE-Protokoll werden feststehende Start- und Endzeilen-Tags verwendet. Serielle Schnittstelle und virtuelle serielle Schnittstelle werden unterstützt.
Klicken Sie auf **Custom**, um die AVE-Einstellungen zu konfigurieren. Wählen Sie für **Rule** die Option **VSI-ADD** oder **VNET**. Stellen Sie das Adress-Bit der zu sendenden POS-Mitteilung ein.
Klicken Sie auf **OK**, um die Einstellungen zu speichern.

NUCLEUS

Klicken Sie auf **Custom**, um die NUCLEUS-Einstellungen zu konfigurieren.
Geben Sie Mitarbeiternummer, Schichtnummer und Terminalnummer ein. Die entsprechende vom POS-Gerät gesendete Mitteilung wird als gültiger POS-Datensatz verwendet.

Hinweis

Das NUCLEUS-Protokoll muss bei Kommunikation über RS-232 verwendet werden.

6. Wählen Sie **Connection Mode** und klicken Sie auf **Parameters**, um die Parameter für jeden Verbindungsmodus zu konfigurieren.

TCP Connection

Wenn Sie den TCP-Anschluss verwenden, muss der Port zwischen 1 und 65535 eingestellt sein. Der Port für jedes POS-Gerät muss eindeutig sein.
Stellen Sie den Wert für **Allowed Remote IP-Adresse** des Geräts ein, das die POS-Mitteilung sendet.

UDP Connection

Wenn Sie den UDP-Anschluss verwenden, muss der Port zwischen 1 und 65535 eingestellt sein. Der Port für jedes POS-Gerät muss eindeutig sein.

Stellen Sie den Wert für **Allowed Remote IP-Adresse** des Geräts ein, das die POS-Mitteilung sendet.

USB-to-RS-232 Connection

Konfigurieren Sie die Port-Parameter des USB-zu-RS-232-Konverters, einschließlich Seriennummer, Baudrate, Datenbit, Stoppbit, Parität und Flusssteuerung des Ports.

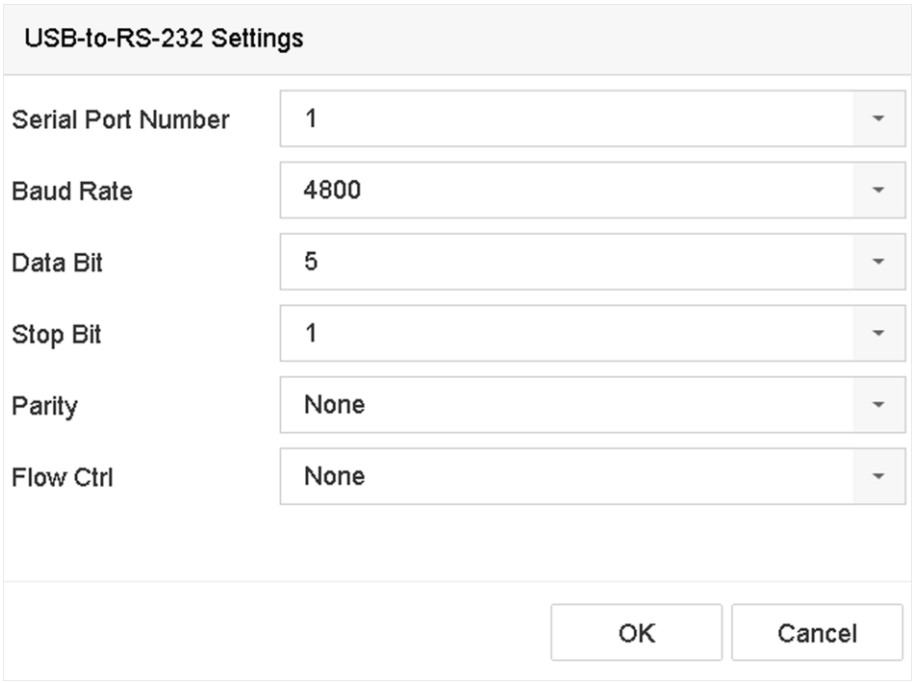


Abbildung 8-3 USB-to-RS-232-Einstellungen

RS-232 Connection

Schließen Sie das Gerät und das Kassensystem über RS-232 an. Die RS-232-Einstellungen können in **Menu** → **Configuration** → **RS-232** konfiguriert werden. „Usage“ muss auf „Transparent Channel“ eingestellt werden.

Multicast Connection

Beim Anschluss des Geräts und des Kassensystems über Multicast-Protokoll stellen Sie die Multicast-Adresse und den Port ein.

Sniff Connection

Schließen Sie das Gerät und das Kassensystem über Sniff an. Konfigurieren Sie die Quell- und Zieladresse.

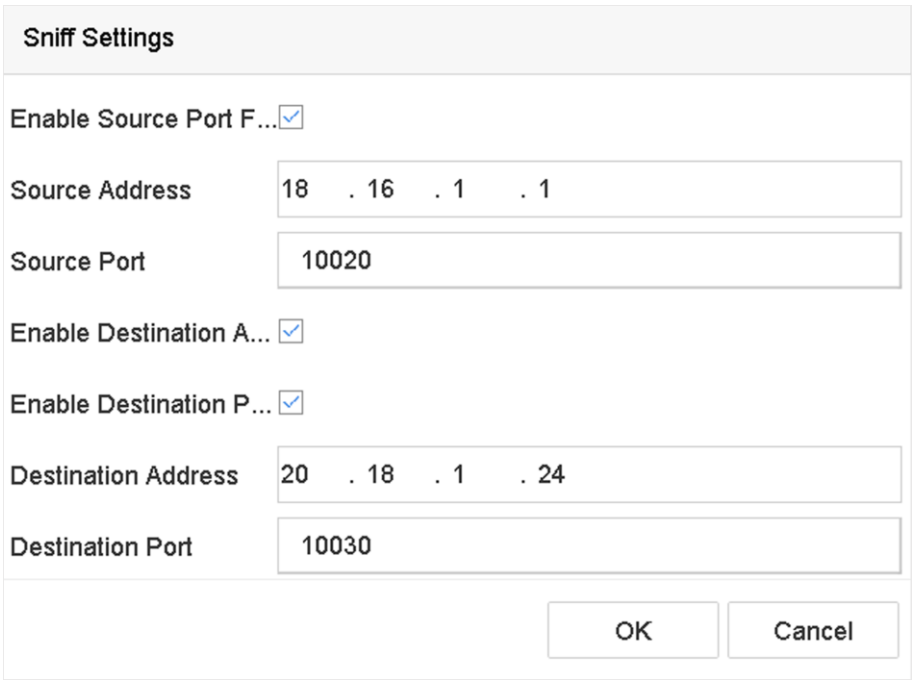


Abbildung 8-4 Sniff-Einstellungen

8.2 POS-Texteinblendung konfigurieren

Schritte

1. Gehen Sie zu **System** → **POS**.
2. Klicken Sie auf **Channel Linkage and Display**.

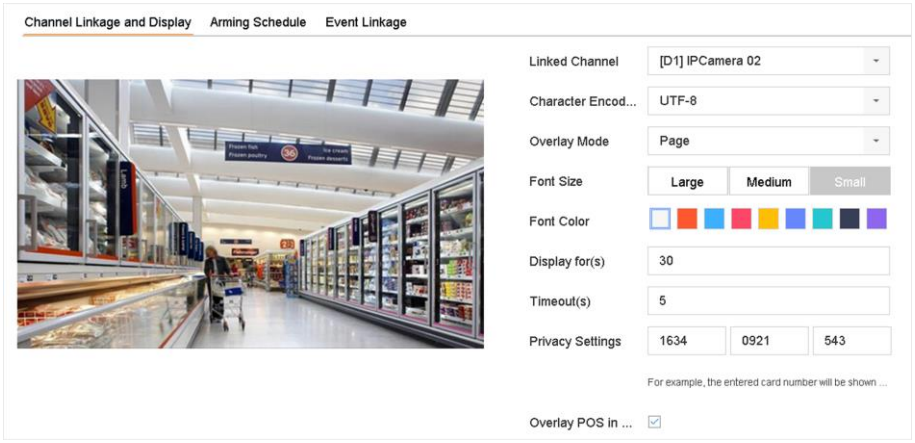


Abbildung 8-5 Einstellungen für Overlay-Zeichen

3. Wählen Sie **linked channel**, um die POS-Zeichen einzublenden.
4. Stellen Sie die Einblendung der Zeichen für die aktivierte Kasse ein.
   - Zeichencodierformat: Derzeit ist das Latin-1-Format verfügbar
   - Einblendmodus der anzuzeigenden Zeichen als Laufschrift oder Seite

- Schriftgröße und -farbe
- Anzeigedauer (Sekunden) der Zeichen. Der Wert reicht von 5 - 3600 Sekunden.
- Zeitüberschreitung des POS-Ereignisses. Der Wert reicht von 5 - 3600 Sekunden. Wenn das Gerät die POS-Meldung nicht innerhalb der definierten Zeit erhalten hat, wird die Transaktion beendet.

5. Stellen Sie unter **Privacy Settings** die POS-Datenschutzinformationen so ein, dass sie nicht auf dem Bild angezeigt werden, z. B. Kartennummer, Benutzername.
   Die definierten Datenschutzinformationen werden stattdessen mit *** im Bild angezeigt.
6. Aktivieren Sie das Kontrollkästchen **Overlay POS in Live View**. Wenn diese Funktion aktiviert ist, werden die POS-Informationen im Livebild eingeblendet.

Hinweis

Ziehen Sie den Rahmen, um die Größe und Position des Textfelds im Vorschaubild der POS-Einstellungen anzupassen.

7. Klicken Sie auf **Apply**, um die Einstellungen zu übernehmen.

8.3 POS-Alarm konfigurieren

Ein POS-Ereignis kann Kanäle auslösen, um die Aufzeichnung zu starten, oder eine Vollbildüberwachung oder akustische Warnung auslösen, das Überwachungszentrum benachrichtigen, E-Mails senden usw.

Schritte

1. Gehen Sie zu **Storage** → **Recording Schedule**.
2. Stellen Sie den Scharfschaltplan des POS-Ereignisses ein.
3. Gehen Sie zu **System** → **POS**.
4. Klicken Sie im Menü „Add POS“ oder „Edit POS“ auf **Event Linkage**.

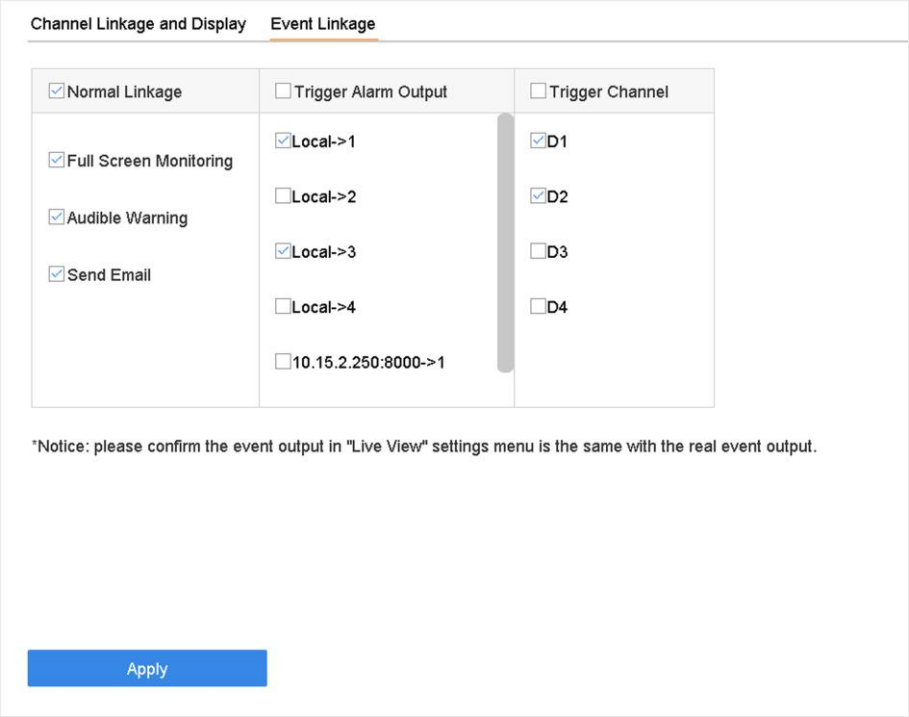


Abbildung 8-6 Auslösekanäle der POS-Kameras einstellen

5. Wählen Sie die normalen Verknüpfungsfunktionen aus.
6. Wählen Sie einen oder mehrere Alarmausgänge zum Auslösen aus.
7. Wählen Sie einen oder mehrere Kanäle zur Aufzeichnung oder zur Vollbildüberwachung aus, wenn ein POS-Alarm ausgelöst wird.
8. Klicken Sie auf **Apply**, um die Einstellungen zu speichern.

Kapitel 9 Kameraeinstellungen

9.1 Bildparameter konfigurieren

Sie können Bildparameter wie Tag/Nacht-Umschaltung, Hintergrundbeleuchtung, Kontrast oder Sättigung in **Camera** → **Display** anpassen.

Bildeinstellungen

Passt Bildparameter wie Helligkeit, Kontrast und Sättigung an.

Exposure

Hier stellen Sie die Belichtungszeit der Kamera ein (1/10000 bis 1 Sekunde). Ein größerer Belichtungswert führt zu einem helleren Bild.

Day/Night Switch

Stellen Sie die Kamera je nach Umgebungsausleuchtung auf Tag-, Nacht- oder Automatikbetrieb ein. Bei abnehmender Helligkeit bei Nacht wechselt die Kamera in den Nachtbetrieb und liefert Schwarzweiß-Bilder hoher Qualität.

Backlight

Hier stellen Sie den breiten Dynamikbereich der Kamera ein (0 bis 100). Wenn die Umgebungsbeleuchtung und das Objekt große Helligkeitsunterschiede aufweisen, können Sie den breiten Dynamikbereich so einstellen, dass die Helligkeit des gesamten Bilds ausgeglichen wird.

Image Enhancement

Für eine optimierte Kontrastverstärkung, die das Rauschen im Videostream reduziert.

9.2 OSD-Einstellungen konfigurieren

Sie können die OSD-Einstellungen (On-Screen-Display) der Kamera konfigurieren, einschließlich Datum/Uhrzeit, Kameraname usw.

Schritte

1. Gehen Sie zu **Camera** → **Display**.
2. Wählen Sie die gewünschte Kamera aus.
3. Bearbeiten Sie den Namen in **Camera Name**.
4. Aktivieren Sie **Display Name**, **Display Date** und **Display Week**, um die Informationen im Bild anzuzeigen.
5. Stellen Sie Datumsformat, Zeitformat und Anzeigemodus ein.

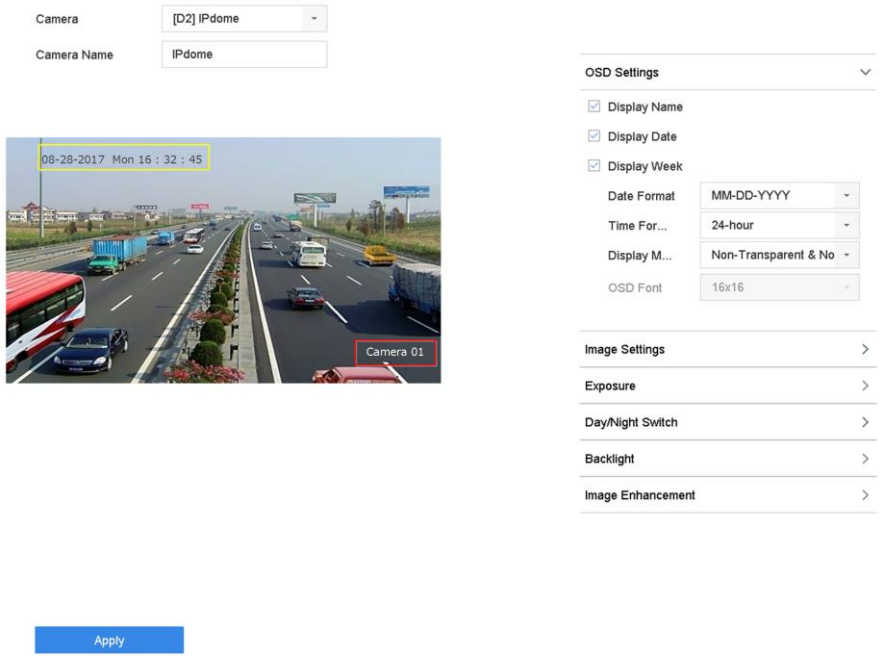


Abbildung 9-1 OSD-Konfigurationsmenü

6. Ziehen Sie den Textrahmen im Vorschaufenster der Live-Ansicht, um die Lage der OSD-Einblendung korrigieren.
7. Klicken Sie auf **Apply**.

9.3 Datenschutzabdeckung konfigurieren

Die Datenschutzabdeckung schützt die Privatsphäre, indem Teile des Bildes gegen Anzeige oder Aufnahme mit einem maskierten Bereich geschützt werden.

Schritte

1. Gehen Sie zu **Camera** → **Privacy Mask**.
2. Wählen Sie die Kamera zur Einstellung der Datenschutzabdeckung aus.
3. Aktivieren Sie das Kontrollkästchen **Enable**.
4. Zeichnen Sie eine Zone in das Fenster. Die Zone ist durch unterschiedliche Rahmenfarben gekennzeichnet.

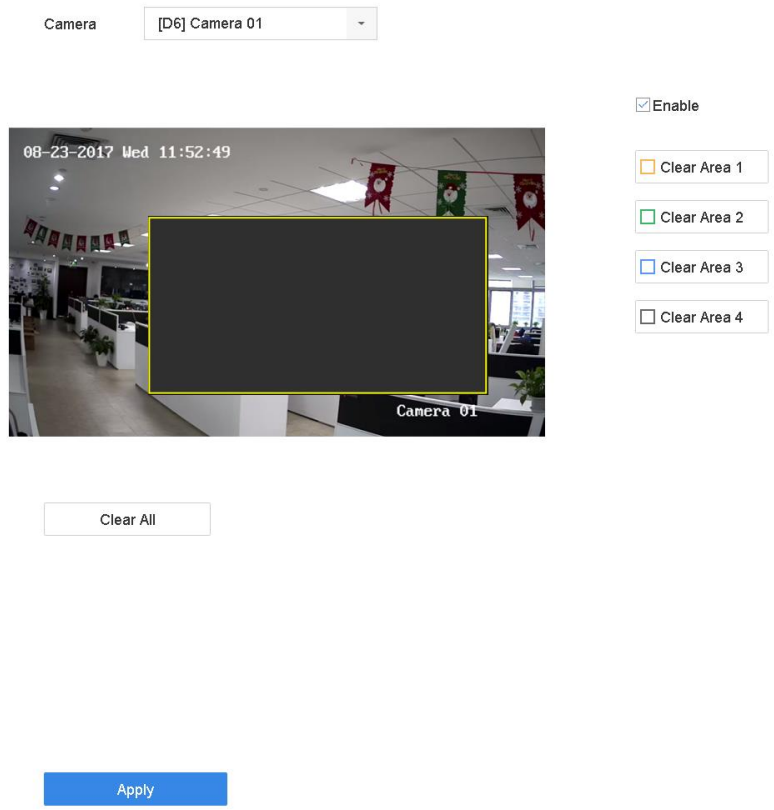


Abbildung 9-2 Einstellmenü der Datenschutzabdeckung

Hinweis

- Bis zu 4 Datenschutzabdeckungszonen können konfiguriert werden. Die Größe der Bereiche kann eingestellt werden.
- Löschen Sie die konfigurierten Datenschutzabdeckungszonen im Fenster, indem Sie auf die entsprechenden Symbole zum Löschen der Zone 1-4 rechts im Fenster klicken, oder klicken Sie auf **Clear All**, um alle Zonen zu löschen.

5. Klicken Sie auf **Apply**.

9.4 IP-Kamera-Konfigurationsdateien importieren/exportieren

Die IP-Kameradaten, einschließlich IP-Adresse, Verwaltungsport, Passwort des Administrators usw. können im Microsoft Excel-Format gespeichert und auf dem lokalen Gerät gesichert werden. Die exportierte Datei kann auf einem PC bearbeitet werden, einschließlich Hinzufügen oder Löschen des Inhalts und Kopieren der Einstellung auf andere Geräte durch Importieren der Excel-Datei.

Bevor Sie beginnen

Beim Import der Konfigurationsdatei schließen Sie das Speichergerät, das die Konfigurationsdatei enthält, an das Gerät an.

Schritte

1. Gehen Sie zu **Camera** → **IP Camera Import/Export**.
2. Klicken Sie auf **IP Camera Import/Export**. Damit werden die Inhalte des erkannten externen Geräts angezeigt.
3. Exportieren oder importieren Sie die IP-Kamera-Konfigurationsdateien.
   – Klicken Sie auf **Export**, um die Konfigurationsdateien auf das ausgewählte lokale Sicherungsgerät zu exportieren.
   – Um eine Konfigurationsdatei zu importieren, wählen Sie die Datei auf dem ausgewählten Sicherungsgerät aus und klicken auf **Import**.

Hinweis

Nach Abschluss des Imports müssen Sie das Gerät neu starten, um die Einstellungen zu aktivieren.

9.5 IP-Kameras aktualisieren

Die IP-Kamera kann per Fernzugriff über das Gerät aktualisiert werden.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie den USB-Stick an das Gerät angeschlossen haben und der Stick die Firmware für die IP-Kamera-Aktualisierung enthält.

Schritte

1. Wählen Sie eine Kamera im Kameraverwaltungsmenü aus.
2. Gehen Sie zu **More Settings** → **Upgrade**.
3. Wählen Sie die Firmware-Aktualisierungsdatei auf dem USB-Stick aus.
4. Klicken Sie auf **Upgrade**.
   Die IP-Kamera wird nach Abschluss der Aktualisierung automatisch neu gestartet.

Kapitel 10 Lagerung

10.1 Verwaltung von Speichergeräten

10.1.1 Lokale Festplatte verwalten

Festplattengruppe konfigurieren

Mehrere Festplatten können als Gruppen verwaltet werden. Videos von spezifizierten Kanälen können über die Festplatteneinstellungen auf einer bestimmte Festplattengruppe aufgenommen werden.

Schritte

1. Gehen Sie zu **Storage** → **Storage Mode**.
2. Wählen Sie für **Mode** die Option **Group**.
3. Klicken Sie auf **Apply**.
4. Gehen Sie zu **Storage** → **Storage Device**.
5. Wählen Sie eine Festplatte aus.

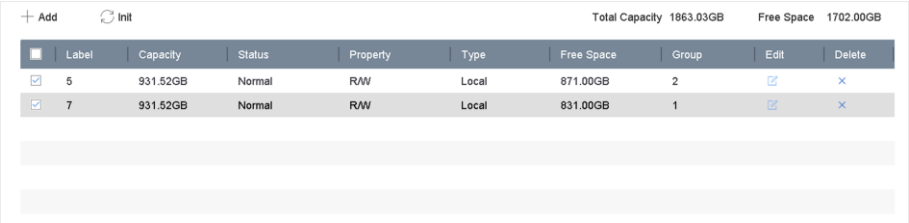


Abbildung 10-1 Speichergerät

6. Klicken Sie auf , um das Menü mit den lokalen Festplatteneinstellungen aufzurufen.

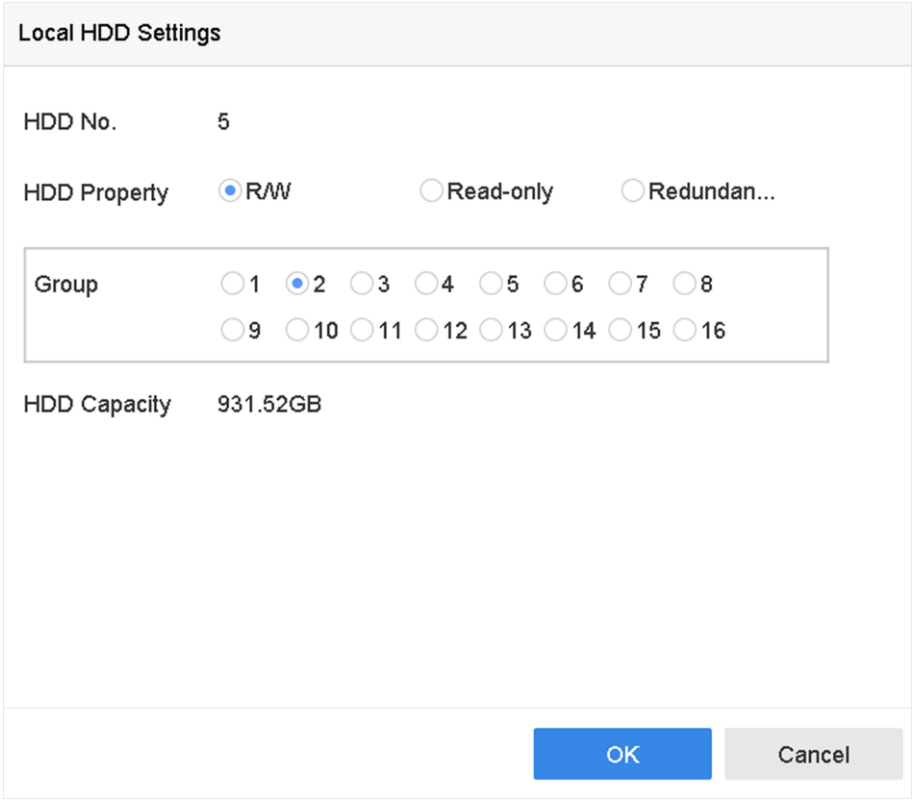


Abbildung 10-2 Lokale Festplatteneinstellungen

7. Wählen Sie eine Gruppennummer für die Festplatte aus.
8. Klicken Sie auf **OK**.

Hinweis

Gruppieren Sie die Kameras für die Festplatte neu, wenn die Nummer der Festplattengruppe geändert wird.

9. Gehen Sie zu **Storage** → **Storage Mode**.
10. Wählen Sie die Gruppennummer aus der Liste aus.
11. Wählen Sie die entsprechende(n) Kamera(s) aus, um Videos und Bilder auf der Festplattengruppe zu speichern.
12. Klicken Sie auf **Apply**.

Festplattenparameter konfigurieren

Die Festplatteneigenschaft kann als „R/W“, „Read-Only“ oder „Redundant“ festgelegt werden.

Bevor Sie beginnen

Stellen Sie den Speichermodus auf „Group“ ein. Detaillierte Schritte finden Sie unter ***Festplattengruppe konfigurieren***

Schritte

1. Gehen Sie zu **Storage** → **Storage Device**.

2. Klicken Sie auf der gewünschten Festplatte.
3. Wählen Sie die Festplatteneigenschaft **Property** aus.

R/W

Die Festplatte kann gelesen und beschrieben werden.

Read-only

Die Dateien auf einer schreibgeschützten Festplatte werden nicht überschrieben.

Redundant

Speichert die Videodateien nicht nur auf der R/W-Festplatte, sondern auch auf einer redundanten Festplatte. Dies verbessert effektiv die Datensicherheit und -zuverlässigkeit. Es muss wenigstens eine weitere Festplatte geben, die sich im R/W-Status befindet.

4. Klicken Sie auf **OK**.

Festplattenquote konfigurieren

Jede Kamera kann mit einer zugeordneten Quote zum Speichern von Videos oder Bildern konfiguriert werden.

Schritte

1. Gehen Sie zu **Storage** → **Storage Mode**.
2. Wählen Sie für **Mode** die Option **Quota**.
3. Wählen Sie eine Kamera zum Einstellen der Quote.
4. Geben Sie die Speicherkapazität in den Textfeldern **Max. Record Capacity (GB)** und **Max. Picture Capacity (GB)** ein.
5. Klicken Sie auf **Copy**, um die Quoteneinstellungen der aktuellen Kamera auf andere Kameras zu übertragen.
6. Klicken Sie auf **Apply**.

Hinweis

- Ist die Quotenkapazität auf 0 eingestellt, so verwenden alle Kameras die Gesamtkapazität der Festplatte für Aufnahmen und Bilderfassung.
- Starten Sie den Videorekorder neu, um die neuen Einstellungen zu aktivieren.

10.1.2 Netzwerkfestplatte hinzufügen

Sie können dem Gerät die zugeordnete NAS- oder IP-SAN-Festplatte hinzufügen und diese als Netzwerkfestplatte verwenden. Bis zu 8 Netzwerkfestplatten können hinzugefügt werden.

Schritte

1. Gehen Sie zu **Storage** → **Storage Device**.
2. Klicken Sie auf **Add**.

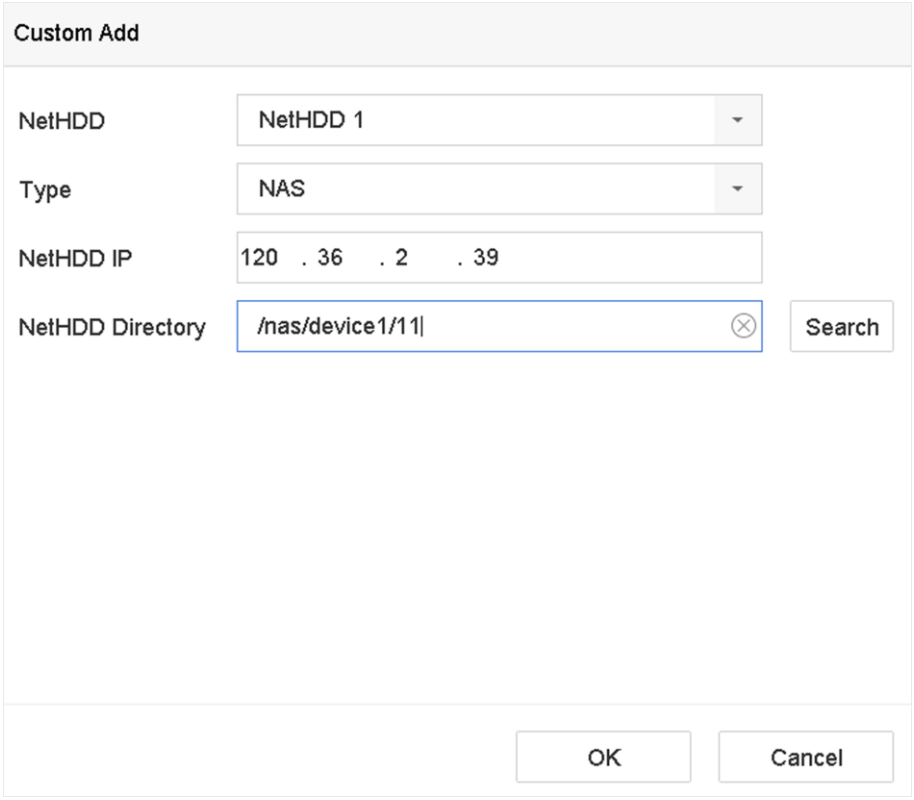


Abbildung 10-3 Netzwerkfestplatte hinzufügen

3. Wählen Sie den Typ unter **NetHDD** aus.
4. Geben Sie die Adresse unter **NetHDD IP** ein und klicken Sie auf **Search**, um nach der verfügbaren Netzwerkfestplatte zu suchen.
5. Wählen Sie die gewünschte Netzwerkfestplatte aus.
6. Klicken Sie auf **OK**.
7. Die hinzugefügte Netzwerkfestplatte wird in der Festplattenliste angezeigt. Wählen Sie die neu hinzugefügte Netzwerkfestplatte aus und klicken Sie auf **Init**.

10.1.3 Cloud-Speicher

Die Cloud-Speicherfunktion ermöglicht es dem Gerät, Videos auf einen Cloud-Server hochzuladen. Dadurch wird nicht nur Speicherplatz auf der lokalen Festplatte gespart, sondern auch der Zugriff auf Videos vereinfacht. Sie können den Cloud-Speicher über einen Webbrowser aktivieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihr Gerät ordnungsgemäß mit dem Internet verbunden ist und Sie über die richtigen Cloud-Speicherdaten verfügen.

Schritte

1. Gehen Sie zu **Configuration** → **Storage** → **Storage Management** → **Cloud Storage**.

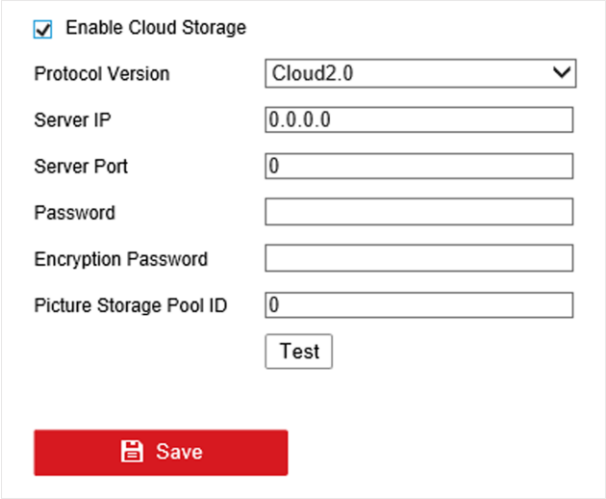


Abbildung 10-4 Cloud-Speicher

2. Aktivieren Sie das Kontrollkästchen **Enable Cloud Storage**.
3. Legen Sie die Serverparameter für den Cloud-Speicher fest.

Hinweis

In einem Cloud-Speicherserver sind mehrere Pools vorhanden. Ein Pool agiert wie eine Festplatte und wird zum Speichern von Dateien verwendet. Jeder Pool hat eine ID, daher müssen Sie die Pool-ID vom Speicherserver abrufen.

4. Klicken Sie auf **Test**, um zu testen, ob die Parameter gültig sind.
5. Klicken Sie auf **Save**.

10.1.4 eSATA verwalten

eSATA für Datenspeicherung konfigurieren

Wenn ein externes eSATA-Gerät an Ihren Videorekorder angeschlossen ist, können Sie eSATA für die Datenspeicherung konfigurieren und eSATA im Gerät verwalten.

Schritte

1. Gehen Sie zu **Storage** → **Advanced**.
2. Wählen Sie für eSATA unter **Usage** die Option **Export** oder **Record/Capture**.

Export

Sie verwenden das eSATA-Gerät als Backup.

Record/Capture

Sie verwenden das eSATA-Gerät zur Aufnahme/Fotoaufnahme. Siehe nachstehende Schritte zur Bedienung.

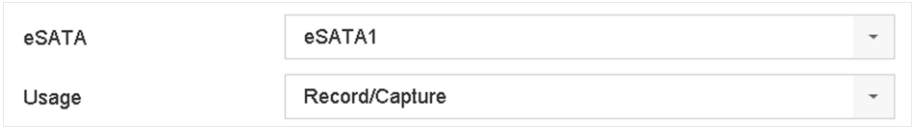


Abbildung 10-5 eSATA-Modus

Was folgt als Nächstes

Wenn die eSATA-Nutzung auf **Record/Capture** eingestellt ist, öffnen Sie das Menü des Speichergeräts, um dessen Eigenschaft zu bearbeiten oder es zu initialisieren.

eSATA für automatische Sicherung konfigurieren

Wenn Sie einen automatischen Sicherungsplan erstellt haben, sichert der Videorekorder die lokalen Videos 24 Stunden vor der Sicherungsstartzeit auf eSATA.

Bevor Sie beginnen

Stellen Sie sicher, dass das Gerät ordnungsgemäß mit einer externen eSATA-Festplatte verbunden ist und dass der Verwendungstyp auf **Export** eingestellt ist. Weitere Informationen finden Sie unter ***eSATA verwalten***.

Schritte

1. Gehen Sie zu **Storage** → **Auto Backup**.
2. Aktivieren Sie die Option **Auto Backup**.
3. Legen Sie die Startzeit für die Sicherung unter **Start Backup at** fest.

Hinweis

Wenn an einem Tag eine Sicherung fehlgeschlagen ist, sichert der Videorekorder die Videos 48 Stunden vor der Startzeit der Sicherung am Folgetag.

4. Wählen Sie die Kanäle für die Sicherung.
5. Wählen Sie **Backup Stream Type**, wenn gewünscht.
6. Wählen Sie den Typ **Overwrite**.
   - **Disable**: Wenn die Festplatte voll ist, wird der Schreibvorgang beendet.
   - **Enable**: Wenn die Festplatte voll ist, werden die ältesten Dateien gelöscht, um neue Dateien schreiben zu können.
7. Klicken Sie auf **Apply**.

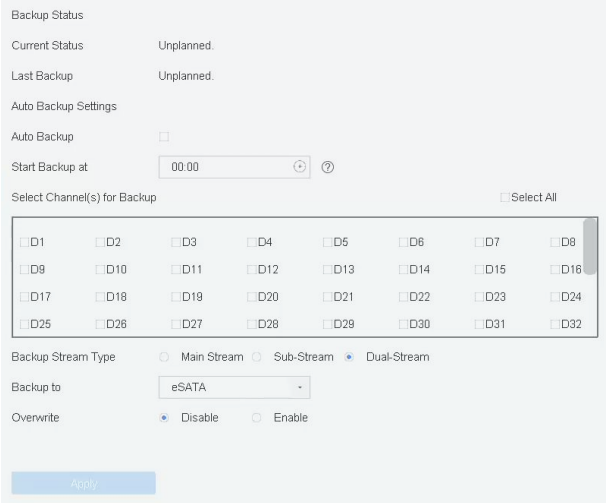


Abbildung 10-6 eSATA für automatische Sicherung konfigurieren

10.2 Festplatten-Array

Ein Festplatten-Array ist eine Datenspeicher-Virtualisierung, die mehrere physische Laufwerke zu einer einzigen logischen Einheit kombiniert. Auch bekannt als „RAID“, speichert ein Array Daten über mehrere Festplatten, um genügend Redundanz zu bieten, sodass Daten wiederhergestellt werden können, wenn eine Festplatte ausfällt. Die Verteilung der Daten auf die Festplatten erfolgt auf eine von mehreren Arten, die als „RAID-Level“ bezeichnet werden, basierend auf der erforderlichen Redundanz und Leistung.

10.2.1 Festplatten-Array erstellen

Der Videorekorder unterstützt softwarebasierte Festplatten-Arrays. Aktivieren Sie die RAID-Funktion nach Bedarf. Für die Erstellung eines Arrays gibt es zwei Möglichkeiten: One-Touch-Konfiguration und manuelle Konfiguration.

One-Touch-Erstellung

Die One-Touch-Konfiguration erstellt das Disk-Array. Standardmäßig ist der durch die One-Touch-Konfiguration erzeugte Array-Typ RAID 5.

Bevor Sie beginnen

Installieren Sie mindestens 3 Festplatten. Wenn mehr als 10 Festplatten installiert sind, werden 2 Arrays erstellt. Um die Zuverlässigkeit und Stabilität der Festplatten zu erhalten, wird empfohlen, Enterprise-Level-Festplatten des gleichen Modells und der gleichen Kapazität zu verwenden.

Schritte

1. Gehen Sie zu **Storage** → **Advanced**.
2. Aktivieren Sie das Kontrollkästchen **Enable RAID**.

3. Klicken Sie auf **Apply** und starten Sie das Gerät neu, um die neuen Einstellungen zu übernehmen.
4. Gehen Sie nach dem Neustart zu **Storage** → **RAID Setup** → **Physical Disk**.
5. Klicken Sie auf **One-touch Config**.
6. Bearbeiten Sie den Eintrag **Array Name** und klicken Sie auf **OK**, um die Konfiguration zu starten.

Hinweis

Wenn Sie 4 oder mehr Festplatten installieren, wird eine Hot-Spare-Festplatte für den Array-Wiederaufbau erstellt.

7. Optional: Der Videorekorder initialisiert das erzeugte Array automatisch. Gehen Sie zu **Storage** → **RAID Setup** → **Array**, um die Daten des erstellten Arrays anzuzeigen.

Manual Creation

Manuell können Sie ein RAID 0-, RAID 1-, RAID 5-, RAID 6- oder RAID 10-Array erstellen.

Schritte

1. Gehen Sie zu **Storage** → **Advanced**.
2. Aktivieren Sie das Kontrollkästchen **Enable RAID**.
3. Klicken Sie auf **Apply** und starten Sie das Gerät neu, um die neuen Einstellungen zu übernehmen.
4. Gehen Sie nach dem Neustart zu **Storage** → **RAID Setup** → **Physical Disk**.
5. Klicken Sie auf **Create**.

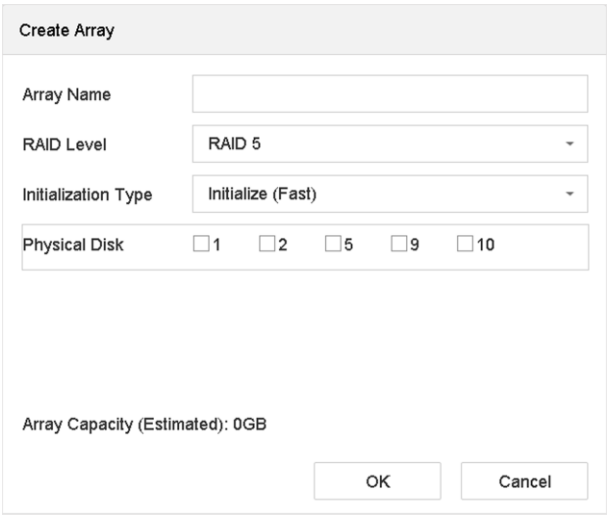


Abbildung 10-7 Array erstellen

6. Geben Sie den Namen unter **Array Name** ein.
7. Wählen Sie das **RAID Level** nach Bedarf aus.
8. Wählen Sie die physischen Festplatten aus, um das Array zu bilden.

Tabelle 10-1 Erforderliche Anzahl Festplatten

RAID-Stufe	Erforderliche Anzahl Festplatten
RAID 0	Mindestens 2 Festplatten.
RAID 1	Mindestens 2 Festplatten.
RAID 5	Mindestens 3 Festplatten.
RAID 6	Mindestens 4 Festplatten.
RAID 10	Die Anzahl der Festplatten muss gerade sein und zwischen 4 und 16 liegen.

9. Klicken Sie auf **OK**.
10. Optional: Der Videorekorder initialisiert das erzeugte Array automatisch. Gehen Sie zu **Storage** → **RAID Setup** → **Array**, um die Daten des erstellten Arrays anzuzeigen.

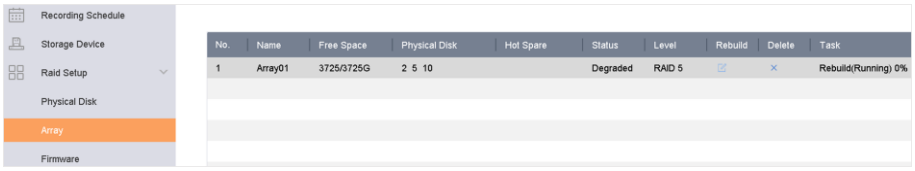


Abbildung 10-8 Array-Liste

10.2.2 Array wiederaufbauen

Der Array-Status umfasst „Functional“, „Degraded“ und „Offline“. Um die hohe Sicherheit und Zuverlässigkeit der in einem Array gespeicherten Daten zu gewährleisten, ist eine sofortige und ordnungsgemäße Pflege der Arrays entsprechend seinem Status erforderlich.

Functional

Kein Festplattenverlust im Array.

Offline

Die Anzahl der verlorenen Festplatten hat das Limit überschritten.

Degraded

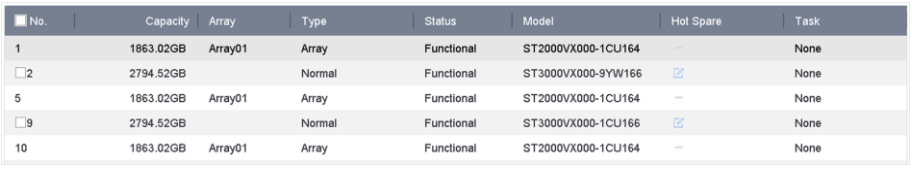
Wenn eine Festplatte im Array ausfällt, wird das Array beeinträchtigt. Setzen Sie das Array auf den Status „Functional“ zurück, indem Sie es neu aufbauen.

Hot-Spare-Festplatte konfigurieren

Hot-Spare-Festplatten werden für die automatische Wiederherstellung des Festplatten-Arrays benötigt.

Schritte

1. Gehen Sie zu **Storage** → **RAID Setup** → **Physical Disk**.



No.	Capacity	Array	Type	Status	Model	Hot Spare	Task
1	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	–	None
2	2794.52GB		Normal	Functional	ST3000VX000-9YW166		None
5	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	–	None
9	2794.52GB		Normal	Functional	ST3000VX000-1CU166		None
10	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	–	None

Abbildung 10-9 Physische Festplatte

2. Klicken Sie auf einer verfügbaren Festplatte, um sie als Hot-Spare-Festplatte einzustellen.

Array automatisch wiederaufbauen

Der Videorekorder kann automatisch beschädigte Arrays mit den Hot-Spare-Festplatten wiederherstellen.

Bevor Sie beginnen

Erstellen Sie Hot-Spare-Festplatten. Weitere Informationen finden Sie unter ***Hot-Spare-Festplatte konfigurieren***.

Schritte

1. Gehen Sie zu **Storage** → **RAID Setup** → **Array**.

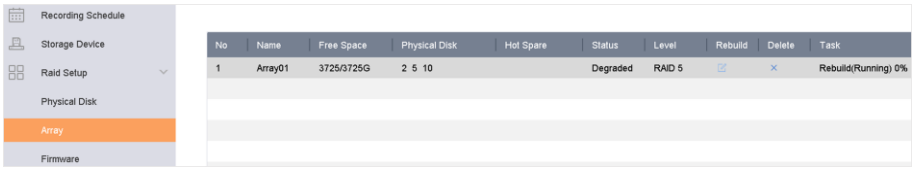


Abbildung 10-10 Array-Liste

Array manuell wiederaufbauen

Wenn keine Hot-Spare-Festplatten konfiguriert sind, bauen Sie ein beschädigtes Array manuell wieder auf.

Bevor Sie beginnen

Es muss mindestens eine physische Festplatte vorhanden sein, um ein Array neu zu erstellen.

Schritte

1. Gehen Sie zu **Storage** → **RAID Setup** → **Array**.
2. Klicken Sie auf des beschädigten Arrays.

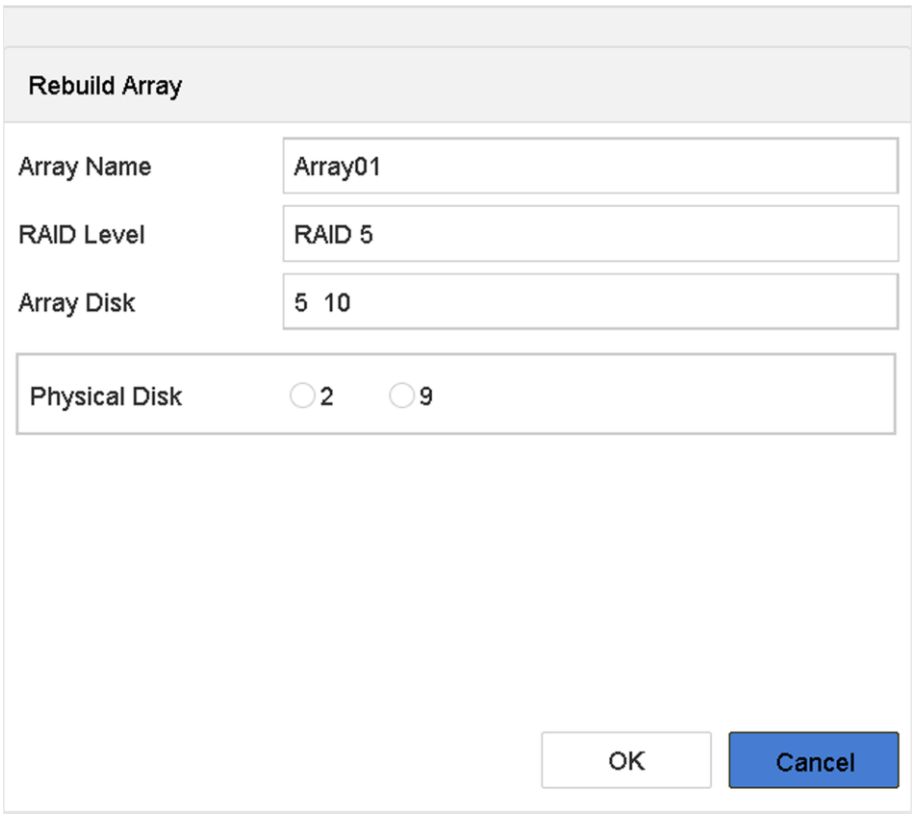


Abbildung 10-11 Array wiederaufbauen

3. Wählen Sie die verfügbare physische Festplatte.
4. Klicken Sie auf **OK**.
5. Klicken Sie im Dialogfenster „Do not unplug the physical disk when it is under rebuilding“ auf **OK**.

Kapitel 11 Hot-Spare-Rekorder sichern

Der Videorekorder kann ein N+1 Hot-Spare-System bilden. Das System besteht aus mehreren funktionierenden Videorekordern und einem Hot-Spare-Videorekorder. Fällt der funktionierende Videorekorder aus, geht der Hot-Spare-Videorekorder in Betrieb und steigert damit die Ausfallsicherheit des Systems. Wenden Sie sich an Ihren Fachhändler, um Informationen über Modelle zu erhalten, die die Hot-Spare-Funktion unterstützen.
Eine bidirektionale Verbindung wie in der nachstehenden Abbildung muss zwischen dem Hot-Spare-Videorekorder und jedem funktionierenden Videorekorder aufgebaut werden.

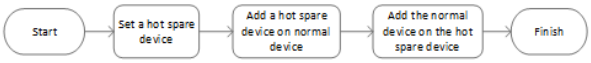


Abbildung 11-1 Aufbau eines Hot-Spare-Systems

11.1 Hot-Spare-Gerät einstellen

Hot-Spare-Geräte übernehmen die Aufgaben des funktionierenden Geräts, wenn das funktionierende Gerät ausfällt.

Schritte

1. Gehen Sie zu **System** → **Hot Spare**.
2. Wählen Sie als **Work Mode** die Option **Hot Spare Mode**.

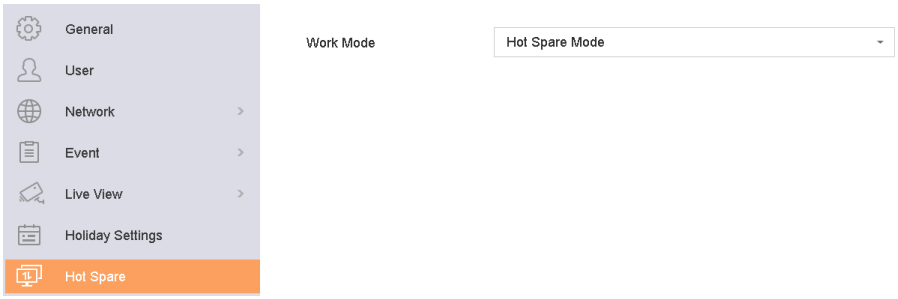


Abbildung 11-2 Hot Spare

3. Klicken Sie auf **Apply**.
4. Klicken Sie im Popup-Fenster auf **Yes**, um das Gerät neu zu starten.

Hinweis

- Die Kameraverbindung wird deaktiviert, wenn das Gerät im Hot-Spare-Modus arbeitet.
- Es wird dringend empfohlen, die Standardeinstellungen des Geräts nach dem Umschalten des Betriebsmodus des Hot-Spare-Geräts auf Normalbetrieb wiederherzustellen, um den Normalbetrieb zu gewährleisten.

11.2 Funktionierenden Rekorder festlegen

Schritte

1. Gehen Sie zu **System** → **Hot Spare**.
2. Wählen Sie als **Work Mode** die Option **Normal Mode**.
3. Aktivieren Sie das Kontrollkästchen **Enable**.
4. Geben Sie IP-Adresse, Benutzername und Admin-Passwort des Hot-Spare-Rekorders ein.

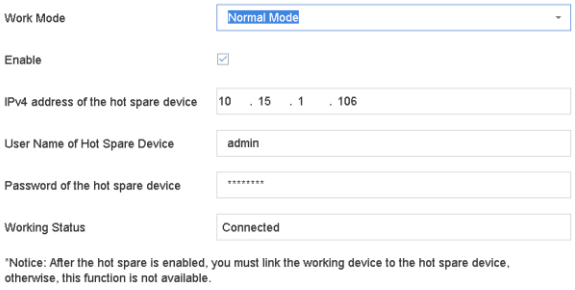


Abbildung 11-3 Hot Spare

5. Klicken Sie auf **Apply**.

11.3 Hot-Spare-System verwalten

Schritte

Hinweis

Nur die 96 I-Serie unterstützt Hot-Spare.

1. Gehen Sie im Hot-Spare-Rekorder zu **System** → **Hot Spare**.
2. Aktivieren Sie das Kontrollkästchen „Working Devices“ in der Geräteliste und klicken Sie auf **Add**, um das funktionierende Gerät mit dem Hot-Spare-Gerät zu verknüpfen. Die Beschreibung des Arbeitsstatus des funktionierenden Rekorders lautet wie folgt:

No record

Der funktionierende Rekorder arbeitet einwandfrei.

Backing up

Wenn der funktionierende Rekorder offline geht, zeichnet der Hot-Spare-Rekorder das Video der mit dem funktionierenden Rekorder verbundenen IP-Kamera auf. Die Videosicherung ist derzeit für einen funktionierenden Rekorder verfügbar.

Synchronizing

Wenn der funktionierende Rekorder wieder online ist, werden die verlorenen Videodateien durch die Videosynchronisation wiederhergestellt. Die Videosynchronisation kann immer nur

für jeweils einen funktionierenden Rekorder aktiviert werden.

Hinweis

Ein Hot-Spare-Rekorder kann an bis zu 32 funktionierende Rekorder angeschlossen werden.

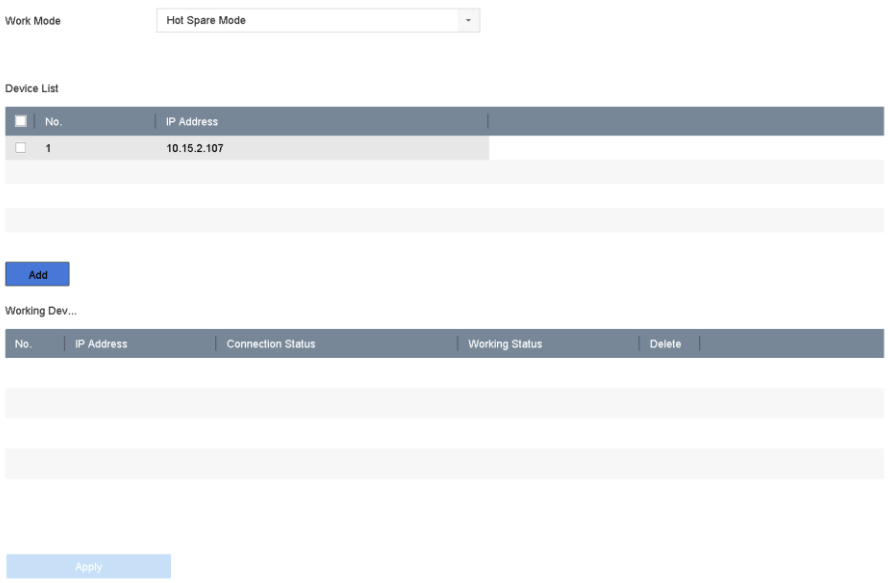


Abbildung 11-4 Funktionierenden Rekorder hinzufügen

Kapitel 12 Netzwerkeinstellungen

12.1 DDNS konfigurieren

Sie können den dynamischen DNS-Dienst für den Netzwerkzugriff einstellen. Es stehen verschiedene DDNS-Modi zur Verfügung: DynDNS, PeanutHull und NO-IP.

Bevor Sie beginnen

Sie müssen DynDNS-, PeanutHull- oder NO-IP-Dienste bei Ihrem Internetdienstanbieter registrieren, bevor Sie DDNS-Einstellungen vornehmen können.

Schritte

1. Gehen Sie zu **System** → **Network** → **TCP/IP** → **DDNS.**

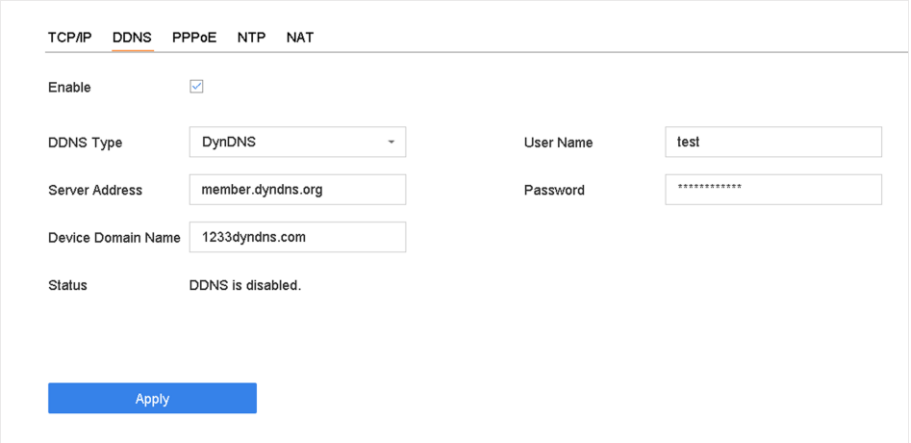


Abbildung 12-1 DDNS-Einstellungen

2. Aktivieren Sie das Kontrollkästchen **Enable**.
3. Wählen Sie als **DDNS Type** die Option „DynDNS“.
4. Geben Sie die Serveradresse für DynDNS ein (z. B. members.dyndns.org).
5. Geben Sie unter „Device Domain Name“ den von der DynDNS-Website erhaltenen Domainnamen ein.
6. Geben Sie **User Name** und **Password** so ein, wie sie auf der DynDNS-Website registriert sind.
7. Klicken Sie auf **Apply**.

12.2 17.3 PPPoE konfigurieren

Wenn das Gerät über PPPoE mit dem Internet verbunden ist, müssen Sie Benutzername und Passwort entsprechend unter **System** → **Network** → **TCP/IP** → **PPPoE** konfigurieren.
Wenden Sie sich an Ihren Internetdienstanbieter für weitere Informationen über den PPPoE-Dienst.

12.3 SNMP konfigurieren

Sie können SNMP-Einstellungen (SNMP v2 und SNMP v3) konfigurieren, um Gerätestatus- und Parameterinformationen über einen Webbrowser abzurufen. SNMP v3 erweitert SNMP v2 um kryptografische Sicherheit und bietet Sicherheit durch Authentifizierung und Datenschutz.

Bevor Sie beginnen

Laden Sie die SNMP-Software herunter, um Geräteinformationen über den SNMP-Port zu empfangen. Durch die Einstellung von Trap-Adresse und Port kann das Gerät Alarmereignisse und Ausnahmemeldungen an die Überwachungszentrale senden.

Schritte

1. Gehen Sie über einen Webbrowser zu **Configuration** → **Network** → **Advanced Settings** → **SNMP**.

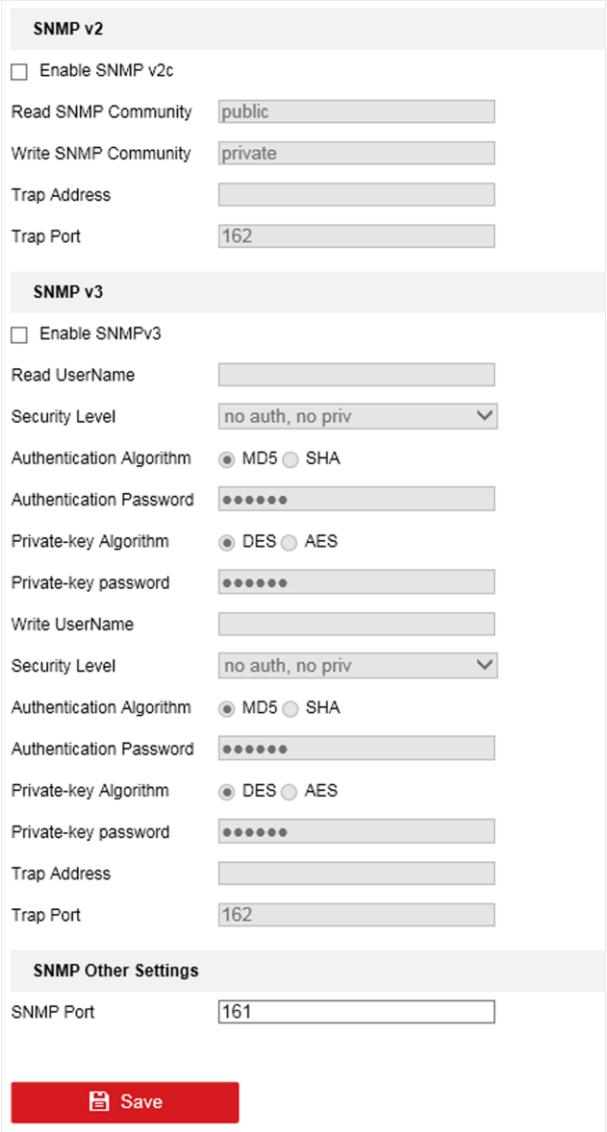


Abbildung 12-2 SNMP-Einstellungen

2. Aktivieren Sie SNMP v2 oder SNMP v3 nach Bedarf.
3. Legen Sie die entsprechenden Parameter fest.
4. Legen Sie den **SNMP Port** fest.
5. Klicken Sie auf **Save**.

12.4 E-Mail konfigurieren

Das System kann so konfiguriert werden, dass es eine E-Mail-Benachrichtigung an alle festgelegten Benutzer sendet, wenn ein bestimmtes Ereignis eintritt, z. B. wenn ein Alarm- oder ein Bewegungsereignis erkannt wird, das Administrator-Passwort geändert wird usw.

Bevor Sie beginnen

Das Gerät muss an ein lokales Netzwerk (LAN) angeschlossen sein, das einen SMTP-Mailserver

enthält. Das Netzwerk muss ebenfalls mit einem Intranet oder dem Internet verbunden sein, abhängig von der Speicherstelle des E-Mail-Kontos, an das die Benachrichtigung gesendet werden soll.

Schritte

1. Gehen Sie zu **System** → **Network** → **Advanced** → **Email**.

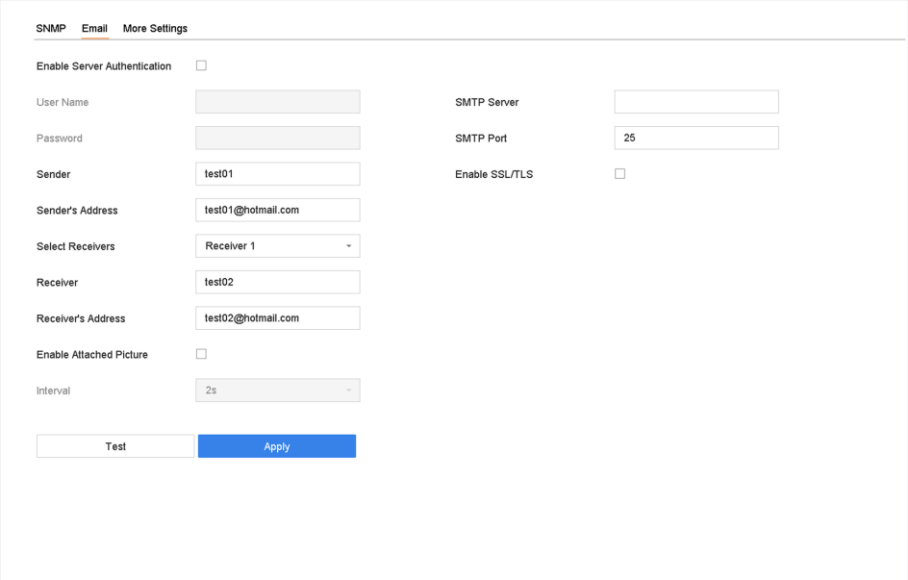


Abbildung 12-3 E-Mail-Einstellungen

2. Konfigurieren Sie die E-Mail-Einstellungen.

Enable Server Authentication

Aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren, wenn der SMTP-Server eine Benutzerauthentifizierung erfordert, und geben Sie Benutzername und Passwort entsprechend ein.

SMTP Server

IP-Adresse des SMTP-Servers oder des Host-Namens (z. B. smtp.263xmail.com).

SMTP Port

Der SMTP-Port. Der Standard-TCP/IP-Port für SMTP ist 25.

Enable SSL/TLS

Aktivieren Sie das Kontrollkästchen, um SSL/TLS zu aktivieren, falls vom SMTP-Server benötigt.

Sender

Der Name des Absenders.

Sender's Address

Die Adresse des Absenders.

Select Receivers

Hier wählen Sie die Empfänger. Bis zu 3 Empfänger können konfiguriert werden.

Receiver

Der Name des Empfängers.

Receiver's Address

E-Mail-Adresse des zu benachrichtigenden Benutzers.

Enable Attached Picture

Aktivieren Sie das Kontrollkästchen, um E-Mails mit angehängten Alarmbildern zu senden. Das Intervall ist die Zeit zwischen dem Senden von zwei aufeinanderfolgenden Alarmbildern.

3. Klicken Sie auf **Apply**.
4. Optional: Klicken Sie auf **Test**, um eine Test-E-Mail zu senden.

12.5 Portzuordnung (NAT) konfigurieren

Es gibt zwei Methoden der Portzuordnung zur Durchführung des Remote-Zugriffs: über segmentübergreifendes Netzwerk-UPnP™ und manuelles Mapping.

Bevor Sie beginnen

Zur Aktivierung der UPnP™-Funktion des Geräts müssen Sie die UPnP™-Funktion des Routers aktivieren, mit dem Ihr Gerät verbunden ist. Wenn der Netzwerk-Arbeitsmodus des Geräts als Mehrfachadresse eingestellt ist, muss sich die Standardroute des Geräts im gleichen Netzwerksegment befinden, wie jene der LAN-IP-Adresse des Routers.

Universal Plug und Play (UPnP™) kann dem Gerät die nahtlose Erkennung des Vorhandenseins anderer Netzwerkgeräte auf dem Netzwerk ermöglichen und funktionale Netzwerkdienste für Datenfreigabe, Kommunikation usw. aufbauen. Sie können die UPnP™-Funktion zur Aktivierung der schnellen Verbindung des Geräts mit dem WAN über einen Router ohne Portzuordnung verwenden.

Schritte

1. Gehen Sie zu **System** → **Network** → **TCP/IP** → **NAT**.

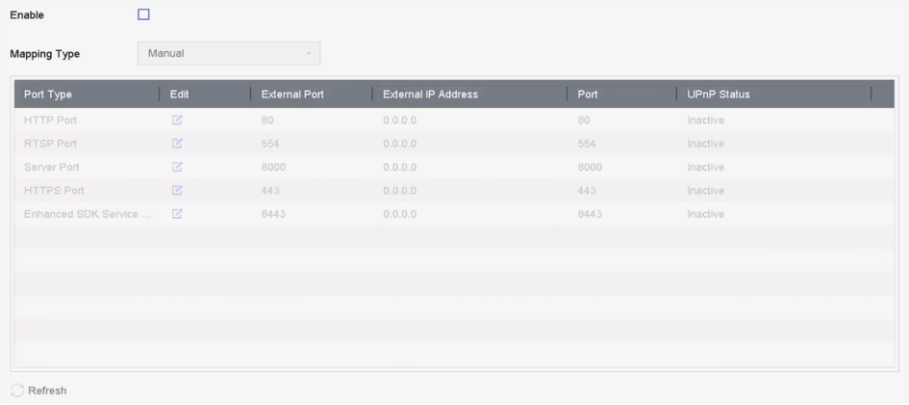


Abbildung 12-4 Einstellung der Portzuordnung

2. Aktivieren Sie das Kontrollkästchen **Enable**.
3. Wählen Sie als **Mapping Type** die Option **Manual** oder **Auto**.

Auto: Wenn Sie **Auto** auswählen, sind die Portzuordnungselemente schreibgeschützt, und die externen Ports werden vom Router automatisch eingestellt.Manuell: Wenn Sie **Manual** auswählen, können Sie den externen Port nach Bedarf bearbeiten, indem Sie ihn anklicken und die Einstellungen für den externen Port aktivieren

.

Hinweis

- Sie können die Standard-Portnummer verwenden oder sie gemäß tatsächlicher Anforderungen ändern.
- „External Port“ zeigt die Portnummer für die Portzuordnung im Router an.
- Der Wert der RTSP-Portnummer muss 554 oder zwischen 1024 und 65535 sein, während der Wert der anderen Ports zwischen 1 und 65535 und eindeutig sein muss. Werden mehrere Geräte für die UPnP™-Einstellungen unter dem gleichen Router konfiguriert, dann muss der Wert der Portnummer für jedes Gerät eindeutig sein.

4. Rufen Sie das virtuelle Servereinstellungsmenü des Routers auf und füllen Sie die leeren Felder von **Internal Source Port** mit dem internen Portwert und die leeren Felder von **External Source Port** mit dem externen Portwert sowie die anderen erforderlichen Inhalte aus.

Hinweis

- Jedes Element muss dem Geräte-Port entsprechen, einschließlich Server-Port, HTTP-Port, RTSP-Port und HTTPS-Port.
- Das virtuelle Servereinstellungsmenü unten dient nur als Referenz, es kann je nach Router anders gestaltet sein. Wenden Sie sich mit Fragen zur virtuellen Servereinstellung an den Hersteller des Routers.

Delete	External Source Port	Protocol	Internal Source IP	Internal Source Port	Application
☐	81	TCP	192.168.251.101	80	HTTP

Abbildung 12-5 Virtuelles Serverelement einstellen

12.6 Port konfigurieren

Sie können verschiedene Typen von Ports konfigurieren, um entsprechende Funktionen zu

aktivieren.

Schritte

1. Gehen Sie zu **System** → **Network** → **Advanced** → **More Settings**.

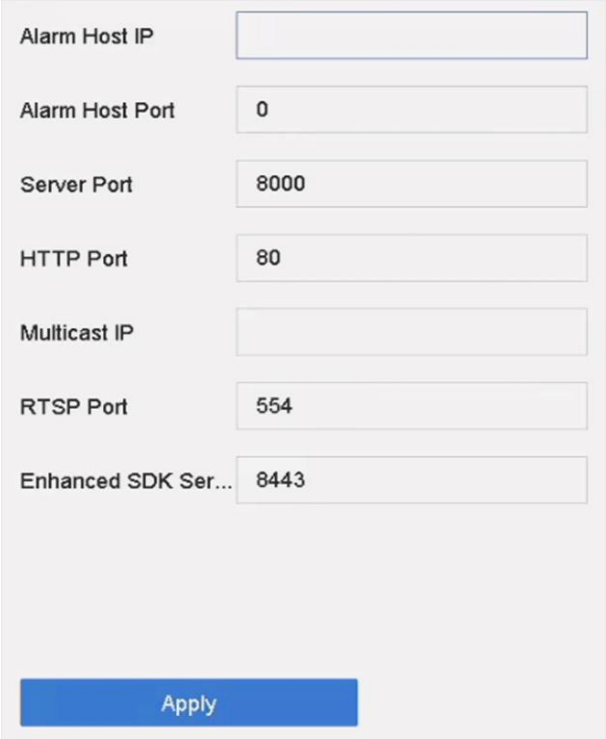


Abbildung 12-6 Port-Einstellungen

2. Konfigurieren Sie die Porteinstellungen nach Bedarf.

Alarm Host IP/Port

Mit einem Remote-Alarm-Host konfiguriert, sendet das Gerät das Alarmereignis oder die Ausnahmemeldung an den Host, wenn ein Alarm ausgelöst wurde. Für den Remote-Alarmhost muss die CMS-Software installiert sein. „Alarm Host IP“ bezieht sich auf die IP-Adresse des Remote-PC, auf dem die CMS-Software (z. B. iVMS-4200) installiert ist, und „Alarm Host Port“(standardmäßig 7200) muss mit dem in der Software konfigurierten Alarmüberwachungsport übereinstimmen.

Server Port

Der Server-Port (standardmäßig 8000) muss für Remote-Client-Softwarezugriff konfiguriert werden, und sein gültiger Bereich ist 2000 bis 65535.

HTTP Port

Der HTTP-Port (standardmäßig 80) muss für den Remote-Zugriff auf den Webbrowser konfiguriert werden.

Multicast IP

Multicast kann konfiguriert werden, um eine Live-Ansicht für Kameras zu ermöglichen, die die maximal zulässige Anzahl über das Netzwerk überschreiten. Sowohl IPv4 als auch IPv6 sind

für Multicast-IP-Adressen verfügbar. Bei IPv4 deckt eine Multicast-IP-Adresse den IP-Bereich von 224.0.0.0 bis 239.255.255.255 ab, und es wird empfohlen, eine IP-Adresse von 239.252.0.0 bis 239.255.255.255 zu verwenden. Beim Hinzufügen eines Geräts zur CMS-Software muss die Multicast-Adresse mit der des Geräts übereinstimmen.

RTSP Port

RTSP (Real-Time Streaming Protocol) ist ein Netzwerkprotokoll zur Steuerung des Streamings von Medien-Servern. Der Port ist standardmäßig 554.

Enhanced SDK Service Port

Der erweiterte SDK-Service verwendet das TLS-Protokoll über den SDK-Service, der eine sichere Datenübertragung bietet. Der Port ist standardmäßig 8443.

3. Klicken Sie auf **Apply**.

12.7 ONVIF konfigurieren

Das ONVIF-Protokoll ermöglicht die Verbindung zu Kameras von Drittanbietern. Die hinzugefügten Benutzerkonten haben die Berechtigung, über das ONVIF-Protokoll eine Verbindung zu anderen Geräten herzustellen.

Schritte

1. Gehen Sie zu **System** → **System Service** → **ONVIF**.
2. Aktivieren Sie das Kontrollkästchen **Enable ONVIF**, um das ONVIF-Zugangsmanagement zu aktivieren.

Hinweis

Das ONVIF-Protokoll ist standardmäßig deaktiviert.

3. Klicken Sie auf **Add**.
4. Geben Sie **User Name** und **Password** ein.

Achtung

Legen Sie unbedingt ein eigenes sicheres Passwort mit mindestens 8 Zeichen aus mindestens drei der Kategorien „Groß- und Kleinbuchstaben“, „Ziffern“ und „Sonderzeichen“ fest, um die Produktsicherheit zu erhöhen. Wir empfehlen weiterhin, dass Sie Ihr Passwort regelmäßig monatlich oder wöchentlich zurücksetzen, insbesondere im Hochsicherheitssystem, um die Sicherheit Ihres Produkts zu erhöhen.

5. Wählen Sie als **Level** die Option **Media User**, **Operator** oder **Admin**.
6. Klicken Sie auf **OK**.

Kapitel 13 Dateiverwaltung

13.1 Dateien suchen

Spezifizieren Sie detaillierte Bedingungen für die Suche nach Videos und Bildern.

Schritte

1. Gehen Sie zu **File Management** → **Video** oder **File Management** → **Picture**.
2. Wählen Sie eine Suchmethode aus. Beispiel: **Search by Appearance** oder **Search by Event**.
3. Spezifizieren Sie detaillierte Bedingungen wie Zeit, Kamera usw.
4. Klicken Sie auf **Start Search**.
5. Klicken Sie auf **Channel**, um den gewünschten Kanal auszuwählen. Es werden die Suchergebnisse für den ausgewählten Kanal angezeigt.
6. Optional: Klicken Sie auf oder , um den Ansichtsmodus zu wechseln.
7. Optional: Klicken Sie bei Videos auf oder in einem anderen Ansichtsmodus, um ein Video zu sperren. Das gesperrte Video wird nicht überschrieben.
8. Optional: Exportieren Sie die Suchergebnisse.
   1) Wählen Sie Ergebnisdatei(en) aus der Suchergebnisschnittstelle aus, oder aktivieren Sie die Option **Select All**, um alle Dateien auszuwählen.
   2) Klicken Sie auf **Export** , um die ausgewählte(n) Datei(en) auf ein Sicherungsgerät zu exportieren.

Hinweis

- Sie können auf klicken, um den Exportfortschritt anzuzeigen.
- Sie können auf klicken, um zum Suchmenü zurückzukehren.

13.2 Suchverlauf

Sie können die Suchbedingungen für später oder für die Schnellsuche speichern.

Schritte

1. Gehen Sie zu **File Management** → **All Files/Human Files/Vehicle Files**.
2. Stellen Sie die Suchbedingungen ein.
3. Klicken Sie auf **Save**.
4. Geben Sie im Textfeld einen Namen ein und klicken Sie auf **Finished**. Die gespeicherten Suchbedingungen werden unter **Search Condition** angezeigt.

Hinweis

Sie können Dateien schnell durchsuchen, indem Sie auf eine Suchbedingung klicken.

13.3 Dateien exportieren

Exportieren Sie Dateien zu Sicherungszwecken auf ein USB-Gerät oder eine eSATA-Festplatte.

Schritte

1. Suchen Sie die Dateien. Weitere Informationen finden Sie unter ***Dateien suchen***.
2. Wählen Sie die Dateien aus.
3. Klicken Sie auf **Export**.
4. Optional: Aktivieren Sie bei Fahrzeugdateien die Option **Backup License Plate Statistics Info**, um später die Kennzeichenstatistik exportieren zu können.
5. Wählen Sie die zu exportierende Datei als **Video and Log** aus und klicken Sie auf **OK**.
6. Wählen Sie das Sicherungsgerät und den Ordnerpfad aus.
7. Klicken Sie auf **OK**.

Kapitel 14 Benutzerverwaltung und Sicherheit

14.1 Benutzerkonten verwalten

Der Administrator-Benutzername ist „admin“, und das Passwort wird festgelegt, wenn Sie das Gerät das erste Mal einschalten. Der Administrator hat die Berechtigung, Benutzer hinzuzufügen und zu löschen sowie Benutzerparameter zu konfigurieren.

14.1.1 Einen Benutzer hinzufügen

Schritte

1. Gehen Sie zu **System** → **User**.
2. Klicken Sie auf **Add**, um das Betriebserlaubnismenü aufzurufen.
3. Geben Sie das Admin-Passwort ein und klicken Sie auf **OK**.
4. Geben Sie im Menü „Add User“ die Informationen für den neuen Benutzer ein.

Achtung

Starkes Passwort empfohlen – Wir empfehlen dringen, ein starkes Passwort Ihrer Wahl zu erstellen (mindestens 8 Schriftzeichen, einschließlich mindestens drei der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Wir empfehlen ebenfalls, dass Sie Ihr Passwort regelmäßig zurücksetzen. Besonders in den Hochsicherheitssystemen kann ein monatliches oder wöchentliches Zurücksetzen des Passwortes Ihr Produkt besser schützen.

Benutzerebene

Stellen Sie die Benutzerebene auf „Operator“ oder „Guest“ ein. Unterschiedliche Benutzerebenen haben unterschiedliche Betriebsberechtigungen.

- Operator: Die Benutzerebene „Operator“ hat Gegensprechberechtigung in der Fernkonfiguration und standardmäßig alle Betriebsberechtigungen in der Kamerakonfiguration.
- Guest: Standardmäßig hat ein Gast in der Remote-Konfiguration keine Befugnis für die Gegensprechfunktion, sondern nur für die lokale/entfernte Wiedergabe in der Kamerakonfiguration.

User’s MAC Address

Die MAC-Adresse des Remote-PCs, der sich am Gerät anmeldet. Ist sie konfiguriert und aktiviert, erlaubt sie nur dem Remote-Benutzer mit dieser MAC-Adresse den Zugriff auf das Gerät.

5. Klicken Sie auf **OK**.
   Im Menü „User Management“ wird der neue Benutzer in der Liste angezeigt.

14.1.2 Admin-Benutzer bearbeiten

Für das Admin-Benutzerkonto können Sie Ihr Passwort und das Entsperrmuster ändern.

Schritte

1. Gehen Sie zu **System** → **User**.
2. Wählen Sie den Admin-Benutzer aus der Liste aus.
3. Klicken Sie auf **Modify**.

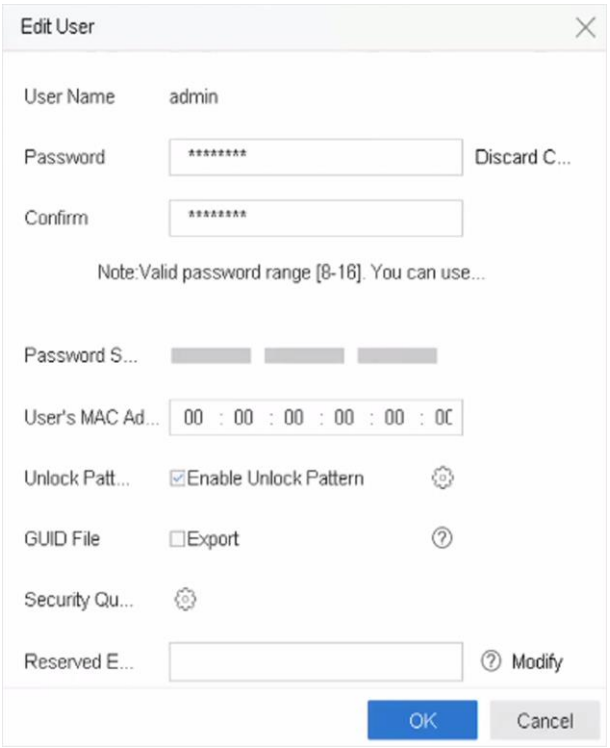


Abbildung 14-1 Benutzer bearbeiten (Admin)

4. Bearbeiten Sie die Admin-Benutzerdaten, einschließlich eines neuen Admin-Passworts (starkes Passwort erforderlich) und der MAC-Adresse.
5. Bearbeiten Sie das Entsperrmuster für das Admin-Benutzerkonto.
   1) Aktivieren Sie das Kontrollkästchen **Enable Unlock Pattern**, um die Verwendung eines Entsperrmusters bei der Anmeldung am Gerät zu ermöglichen.
   2) Zeichnen Sie mit der Maus ein Muster zwischen den 9 Punkten auf dem Bildschirm und lassen Sie die Maus los, wenn das Muster fertig ist.
6. Aktivieren Sie das Kontrollkästchen **Export** für **GUID File**, um die GUID-Datei für das Admin-Benutzerkonto zu exportieren.

Hinweis

Wenn das Admin-Passwort geändert wird, exportieren Sie die neue GUID für zukünftiges Zurücksetzen des Passworts auf den angeschlossenen USB-Stick im Import/Export-Menü.

7. Konfigurieren Sie die Sicherheitsfrage für das Zurücksetzen des Passworts.
8. Konfigurieren Sie reservierte E-Mails für das Zurücksetzen des Passworts.
9. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

14.1.3 Benutzer als Operator/Gast bearbeiten

Sie können die Benutzerdaten bearbeiten, einschließlich Benutzername, Passwort, Berechtigungsebene und MAC-Adresse.

Schritte

1. Gehen Sie zu **System** → **User**.
2. Wählen Sie einen Benutzer aus der Liste aus und klicken Sie auf **Modify**.

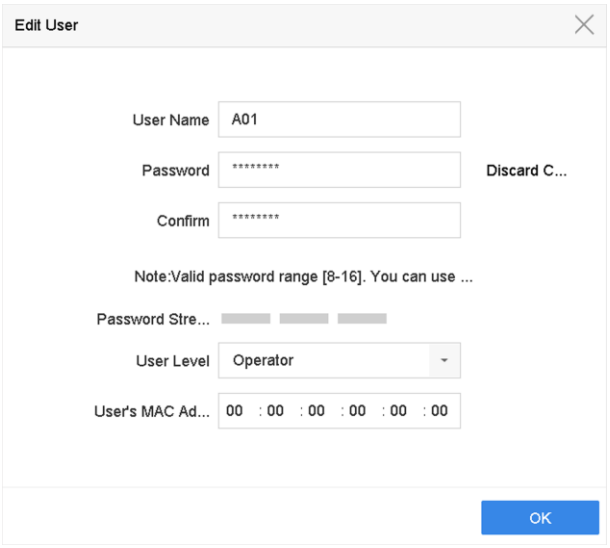


Abbildung 14-2 Benutzer bearbeiten (Operator/Gast)

3. Bearbeiten Sie die Benutzerinformationen wie gewünscht, einschließlich des neuen Passworts (starkes Passwort erforderlich) und der MAC-Adresse.
4. Klicken Sie auf **OK**.

14.2 Benutzerberechtigungen verwalten

14.2.1 Benutzerberechtigungen festlegen

Für einen hinzugefügten Benutzer können Sie verschiedene Berechtigungen zuweisen,

einschließlich der lokalen und externen Bedienung des Geräts.

Schritte

1. Gehen Sie zu **System** → **User**.
2. Wählen Sie einen Benutzer aus der Liste aus und klicken Sie dann auf , um das Menü mit den Berechtigungseinstellungen aufzurufen.

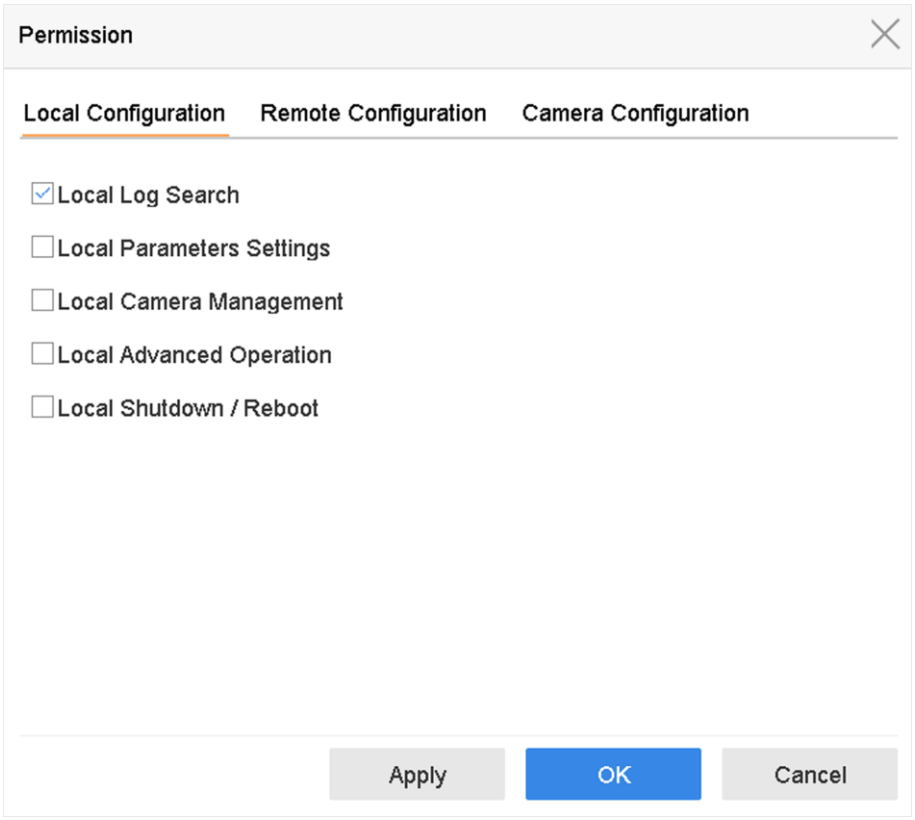


Abbildung 14-3 Menü mit Berechtigungseinstellungen

3. Legen Sie die Betriebsberechtigungen des Benutzers für **Local Configuration**, **Remote Configuration** und **Camera Configuration** fest.
   1) Legen Sie die lokale Konfiguration fest.

Local Log Search

Durchsuchen und Anzeigen von Protokollen und Systeminformationen des Geräts.

Local Parameters Settings

Konfigurieren von Parametern, Wiederherstellen der werkseitigen Standardparameter und Import/Export von Konfigurationsdateien.

Local Camera Management

Hinzufügen, Löschen und Bearbeiten von IP-Kameras.

Local Advanced Operation

Festplattenverwaltung (Initialisierung, Einstellung der Eigenschaften), Firmware-Aktualisierung, Löschen der E/A-Alarmausgabe.

Local Shutdown Reboot

Herunterfahren und Neustarten des Geräts.

2) Fernkonfiguration einstellen

Remote Log Search

Remote-Anzeige von Protokollen, die auf dem Gerät gespeichert sind.

Remote Parameters Settings

Remote-Konfiguration von Parametern, Wiederherstellen der Werkseinstellungen und Import/Export von Konfigurationsdateien.

Remote Camera Management

Externes Hinzufügen, Löschen und Bearbeiten der IP-Kameras.

Remote Serial Port Control

Konfiguration der Einstellungen für RS-232- und RS-485-Ports.

Remote Video Output Control

Senden von Fernbedienungssignalen.

Two-Way Audio

Betrieb des Gegensprechens zwischen dem Remote-Client und dem Gerät.

Remote Alarm Control

Externe Scharfschaltung (Benachrichtigung Alarm- und Ausnahmemeldungen an Remote-Client) und Steuerung des Alarmausgangs.

Remote Advanced Operation

Remote-Festplattenverwaltung (Initialisierung der Festplatten, Einstellen der Festplatteneigenschaften), Aktualisierung der System-Firmware, Löschen des I/O-Alarmausgangs.

Remote Shutdown/Reboot

Fernabschaltung oder Neustart des Geräts.

3) Kamerakonfiguration einstellen

Remote Live View

Live-Video-Betrachtung der gewählten Kamera(s) über Fernzugriff.

Local Manual Operation

Lokales Starten/Beenden der manuellen Aufzeichnung und Alarmausgabe der ausgewählten Kamera(s).

Remote Manual Operation

Externes Starten/Beenden der manuellen Aufzeichnung und Alarmausgabe der ausgewählten Kamera(s).

Local Playback

Lokale Wiedergabe der aufgenommenen Dateien der ausgewählten Kamera(s).

Remote Playback

Externe Wiedergabe der aufgenommenen Dateien der ausgewählten Kamera(s).

Local PTZ Control

Lokale Steuerung von PTZ-Bewegungen der gewählten Kamera(s).

Remote PTZ Control

Steuerung von PTZ-Bewegungen der gewählten Kamera(s) über Fernzugriff.

Local Video Export

Lokales Exportieren der aufgezeichneten Dateien der ausgewählten Kamera(s).

Local Live View

Lokale Anzeige eines Live-Videos der ausgewählten Kamera(s).

4. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

14.2.2 Live-Ansicht-Berechtigung auf dem Sperrbildschirm einstellen

Der Admin-Benutzer kann die Live-Ansicht-Berechtigung für bestimmte Kameras im Bildschirmsperrstatus des Geräts einstellen.

- Der Admin-Benutzer kann diese Berechtigung für Benutzerkonten einstellen.
- Wenn der normale Benutzer (Operator oder Gast) keine lokale Live-Ansicht-Berechtigung für bestimmte Kamera(s) hat, kann die Live-Ansicht-Berechtigung für solche Kamera(s) auf dem Sperrbildschirm nicht konfiguriert werden (Live-Ansicht standardmäßig nicht erlaubt).

Schritte

1. Gehen Sie zu **System** → **User**.
2. Klicken Sie auf **Live View Permission on Lock Screen**.
3. Geben Sie das Admin-Passwort ein und klicken Sie auf **Next**.

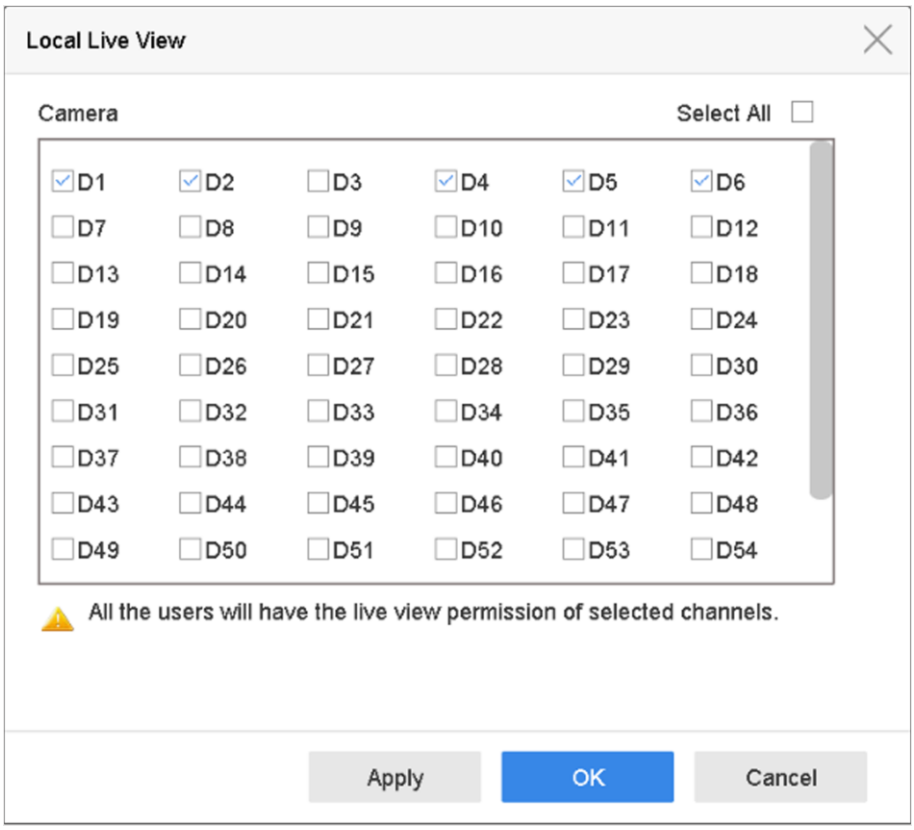


Abbildung 14-4 Live-Ansicht-Berechtigung auf Sperrbildschirm einstellen

4. Legen Sie die Berechtigungen fest. Wählen Sie die Kamera(s) aus, für die die Live-Ansicht erlaubt werden soll, wenn sich das aktuelle Benutzerkonto im Abmeldestatus befindet.
5. Klicken Sie auf **OK**.

14.2.3 Doppelte Verifizierung für Nicht-Admins festlegen

Nachdem die doppelte Überprüfung am Kanal aktiviert wurde, muss ein Benutzer ohne Administratorberechtigung von einem autorisierten Benutzer überprüft werden, um die Genehmigung zu erhalten. Nur der Administrator hat die Berechtigung, die doppelte Verifizierung festzulegen.

Schritte

1. Gehen Sie zu **Maintenance** → **System Service** → **Double Verification Settings**.

Abbildung 14-5 Benutzer für doppelte Verifizierung festlegen

2. Aktivieren Sie das Kontrollkästchen **Enable Double Verification**.
3. Legen Sie die doppelte Benutzer-Überprüfung fest. Die doppelte Verifizierung unterscheidet sich vom Verfahren beim Systembenutzer. Sie können bis zu 8 Benutzer mit doppelter Verifizierung hinzufügen.
   1) Klicken Sie auf **Add**, um einen Benutzer mit doppelter Verifizierung hinzuzufügen.
   2) Geben Sie das Admin-Passwort ein.
   3) Stellen Sie die Benutzerparameter ein, **user name**, **password**, **camera permission** usw.
   4) Klicken Sie auf **OK**.
4. Klicken Sie auf **Apply**.
5. Legen Sie die Berechtigung für Nicht-Admin-Benutzer fest.
   1) Gehen Sie zu **System** → **User**.
   2) Klicken Sie auf , um die Benutzerberechtigungen zu bearbeiten.
   3) Wählen Sie **Camera Permission**. Nur **Local Playback**, **Remote Playback/Download** und **Local Video Export** stehen für die doppelte Verifizierung zur Verfügung.
   4) Wählen Sie die Kanäle aus, für die eine doppelte Verifizierung erforderlich ist.
   5) Klicken Sie auf **OK**.

14.3 Passwortsicherheit konfigurieren

14.3.1 Sicherheitsfragen konfigurieren

Die Sicherheitsfragen helfen Ihnen, das Passwort zurückzusetzen, wenn Sie es vergessen haben oder wenn Sicherheitsprobleme aufgetreten sind. Sie können Sicherheitsfragen über einen Webbrowser konfigurieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie sich im selben Netzwerksegment wie Ihr Gerät befinden.

Schritte

1. Gehen Sie zu **Configuration** → **System** → **User Management** → **User Management**.
2. Wählen Sie den Admin-Benutzer aus.
3. Klicken Sie auf **Account Security Settings**.
4. Klicken Sie auf **Modify**.

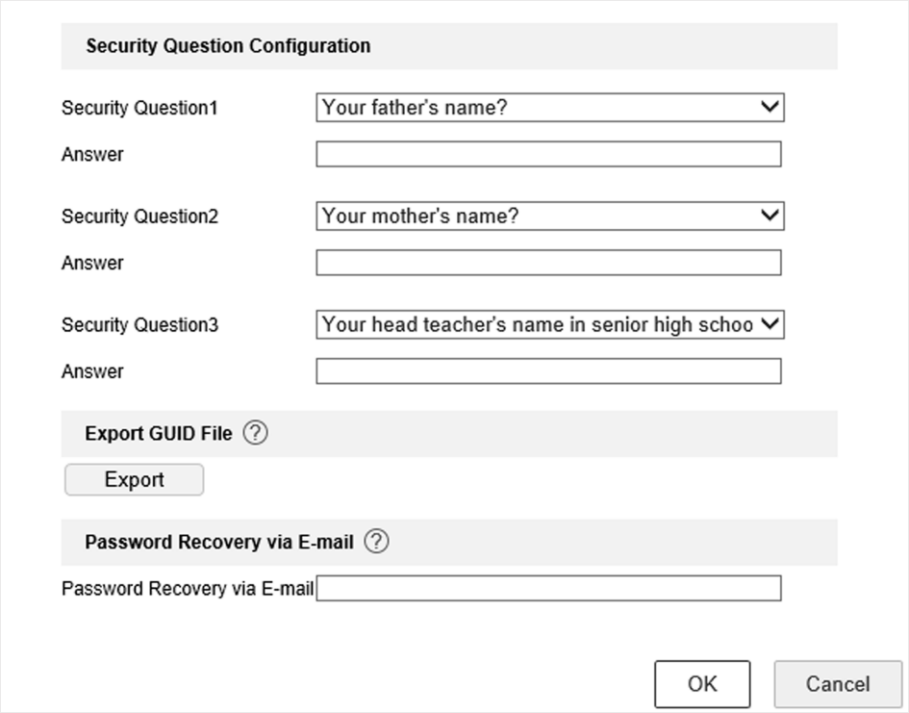


Abbildung 14-6 Sicherheitsfragen konfigurieren

5. Legen Sie die Sicherheitsfragen fest.
6. Klicken Sie auf **OK**.
7. Geben Sie das Administrator-Passwort ein.
8. Klicken Sie auf **OK**.

14.3.2 Reservierte E-Mail konfigurieren

Die reservierte E-Mail hilft Ihnen beim Zurücksetzen des Passworts, wenn Sie Ihr Passwort vergessen haben.

Schritte

1. Aktivieren Sie das Kontrollkästchen **Reserved E-mail**, wenn Sie das Gerät aktivieren, oder klicken Sie auf **Modify**, wenn Sie das Admin-Benutzerkonto bearbeiten.
2. Geben Sie die reservierte E-Mail-Adresse ein.

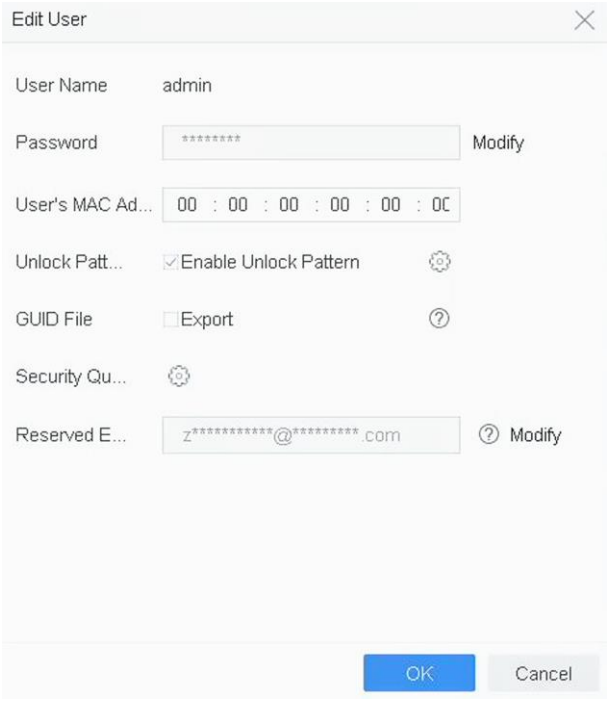


Abbildung 14-7 Reservierte E-Mail konfigurieren

3. Klicken Sie auf **OK**.

14.3.3 GUID-Datei exportieren

Die GUID-Datei hilft Ihnen, das Passwort zurückzusetzen, wenn Sie es vergessen haben. Sie können die GUID-Datei über einen Webbrowser exportieren. Bewahren Sie die GUID-Datei sorgfältig auf.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie sich im selben Netzwerksegment wie Ihr Gerät befinden.

Schritte

1. Gehen Sie zu **Configuration** → **System** → **User Management** → **User Management**.
2. Wählen Sie den Admin-Benutzer aus.
3. Klicken Sie auf **Account Security Settings**.
4. Klicken Sie auf **Modify**.

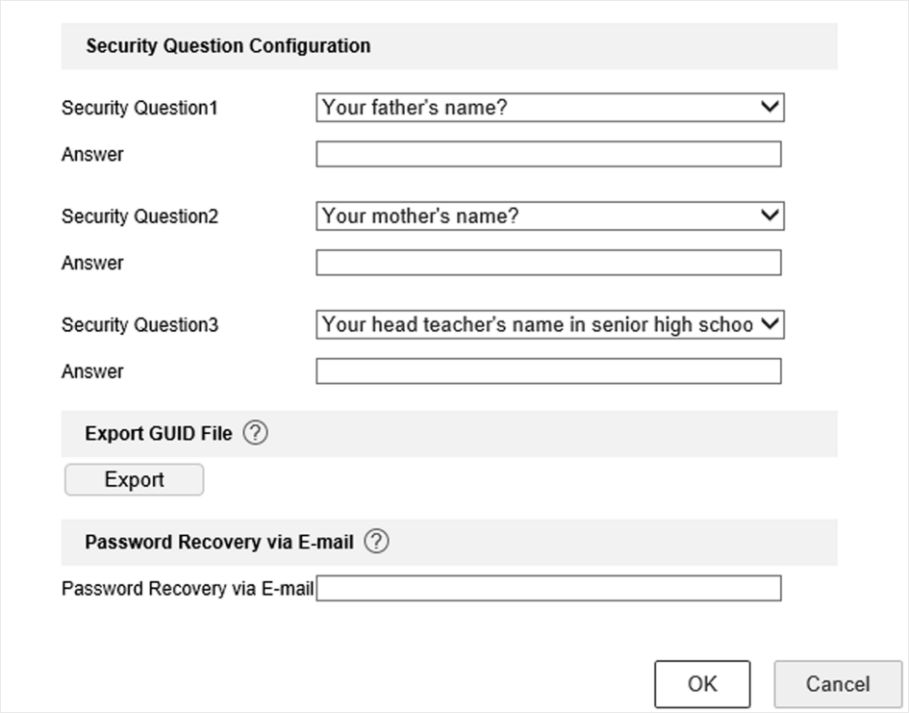


Abbildung 14-8 GUID-Datei exportieren

5. Klicken Sie unter **Export GUID File** auf **Export**.
6. Geben Sie das Administrator-Passwort ein.
7. Speichern Sie die GUID-Datei in dem gewünschten Verzeichnis.

14.4 Passwort zurücksetzen

Wenn Sie das Admin-Passwort vergessen haben, können Sie es zurücksetzen, indem Sie die GUID-Datei importieren, Sicherheitsfragen beantworten oder den Verifizierungscode aus Ihrer reservierten E-Mail eingeben.

14.4.1 Passwort mit GUID zurücksetzen

Sie können das Passwort per GUID über den Webbrowser zurücksetzen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie über die richtige GUID-Datei verfügen.

Schritte

1. Klicken Sie im Benutzeranmeldemenü auf **Forgot Password?**.
2. Wählen Sie als **Verification Mode** die Option **GUID File Verification**.
3. Klicken Sie auf **Browse**, um die GUID-Datei zu suchen.
4. Klicken Sie auf **Next**.
5. Geben Sie ein neues Passwort ein.

Warnung

Wir empfehlen dringend, dass Sie ein starkes Passwort eigener Wahl erstellen (mindestens 8 Zeichen, einschließlich mindestens drei der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Wir empfehlen weiterhin, dass Sie Ihr Passwort regelmäßig monatlich oder wöchentlich zurücksetzen, insbesondere im Hochsicherheitssystem, um die Sicherheit Ihres Produkts zu erhöhen.

6. Bestätigen Sie das neue Passwort.
7. Klicken Sie auf **Next**.

14.4.2 Passwort mit Sicherheitsfragen zurücksetzen

Sie können das Passwort durch Sicherheitsfragen über einen Webbrowser zurücksetzen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die Sicherheitsfragen konfiguriert haben, wenn Sie das Gerät aktivieren oder das Admin-Benutzerkonto bearbeiten.

Schritte

1. Klicken Sie im Benutzeranmeldemenü auf **Forgot Password?**.
2. Wählen Sie als **Verification Mode** die Option **Security Question Verification**.
3. Geben Sie die Antworten auf jede Frage ein.
4. Klicken Sie auf **Next**.
5. Geben Sie das neue Passwort zweimal ein.

Warnung

Wir empfehlen dringend, dass Sie ein starkes Passwort eigener Wahl erstellen (mindestens 8 Zeichen, einschließlich mindestens drei der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Wir empfehlen weiterhin, dass Sie Ihr Passwort regelmäßig monatlich oder wöchentlich zurücksetzen, insbesondere im Hochsicherheitssystem, um die Sicherheit Ihres Produkts zu erhöhen.

6. Klicken Sie auf **Next**.

14.4.3 Passwort mit reservierter E-Mail zurücksetzen

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die Sicherheitsfragen konfiguriert haben, wenn Sie das Gerät aktivieren oder das Admin-Benutzerkonto bearbeiten. (Siehe ***Reservierte E-Mail konfigurieren***)

Schritte

1. Klicken Sie im Benutzeranmeldemenü auf **Forgot Password**.
2. Wählen Sie im Menü mit der Art der Passwortzurücksetzung die Option **Verify by Reserved Email**.
3. Klicken Sie auf **OK**.
4. Klicken Sie auf **Next**, wenn Sie den Haftungsausschluss akzeptieren. Sie können den QR-Code mit einem Smartphone scannen und den Haftungsausschluss lesen.
5. Beschaffen Sie den Verifizierungscode. Es gibt zwei Möglichkeiten, den Verifizierungscode abzurufen.
   – Scannen Sie den QR-Code mit der Hik-Connect-App.
   – Senden Sie den QR-Code an den E-Mail-Server.
      1. Schließen Sie einen USB-Stick an das Gerät an.
      2. Klicken Sie auf **Export**, um den QR-Code auf den USB-Stick zu exportieren.
      3. Senden Sie den QR-Code als Anhang an ***pw_recovery@hikvision.com***.
6. Rufen Sie Ihre reservierte E-Mail ab. Sie erhalten innerhalb von 5 Minuten einen Verifizierungscode.
7. Geben Sie den Verifizierungscode ein.
8. Klicken Sie auf **OK**, um das neue Passwort zu bestätigen.

14.4.4 Passwort mit Hik-Connect zurücksetzen

Bevor Sie beginnen

Stellen Sie sicher, dass auf Ihrem Gerät die Funktion „Hik-Connect“ aktiviert und mit einem registrierten Hik-Connect-Konto gekoppelt ist.

Schritte

1. Klicken Sie im Benutzeranmeldemenü auf **Forgot Password**.
2. Wählen Sie im Menü mit der Art der Passwortzurücksetzung die Option **Verify by Hik-Connect**.
3. Melden Sie sich mit dem Konto, das mit Ihrem Gerät gekoppelt ist, bei der Hik-Connect-App an.
4. Verwenden Sie Hik-Connect, um den QR-Code zu scannen. Anschließend erhalten Sie einen Verifizierungscode von Hik-Connect.
5. Geben Sie den Verifizierungscode ein.
6. Klicken Sie auf **OK**.

Kapitel 15 Systemverwaltung

15.1 Gerät konfigurieren

Schritte

1. Gehen Sie zu **System** → **General**.
2. Konfigurieren Sie die folgenden Einstellungen.

Language

Die Standardsprache ist Englisch.

Output Standard

Stellen Sie den Ausgabestandard auf „NTSC“ oder „PAL“ ein. Dies muss dem Videoeingangsstandard entsprechen.

Resolution

Konfigurieren Sie die Videoausgangsauflösung.

Device Name

Bearbeiten Sie den Gerätenamen.

Device No.

Bearbeiten Sie die Seriennummer des Geräts. Die Gerätenummer kann im Bereich von 1 bis 255 eingestellt werden, die Standardnummer ist 255. Diese Nummer wird für die Fern- und Tastatursteuerung verwendet.

Auto Logout

Stellen Sie das Zeitlimit für die Inaktivität des Menüs ein. Wenn die Timeout-Zeit beispielsweise auf 5 Minuten eingestellt ist, kehrt das System nach 5 Minuten Inaktivität des Menüs aus dem aktuellen Betriebsmenü in die Live-Ansicht zurück.

Mouse Pointer Speed

Stellen Sie die Geschwindigkeit des Mauszeigers ein; 4 Stufen sind konfigurierbar.

Enable Wizard

Aktivieren/deaktivieren Sie den Assistenten, wenn das Gerät hochfährt.

Enable Password

Aktivieren/deaktivieren Sie die Verwendung des Anmeldepassworts.

3. Klicken Sie auf **Apply**, um die Einstellungen zu speichern.

15.2 Uhrzeit konfigurieren

15.2.1 Manuelle Zeitsynchronisation

Schritte

1. Gehen Sie zu **System** → **General**.
2. Konfigurieren Sie das Datum und die Uhrzeit.
3. Klicken Sie auf **Apply**, um die Einstellungen zu speichern.

15.2.2 NTP-Synchronisierung

Die Verbindung zu einem NTP-Server (Network Time Protocol) kann auf Ihrem Gerät konfiguriert werden, um die Datums- und Zeitgenauigkeit des Systems zu gewährleisten.

Schritte

1. Gehen Sie zu **System** → **Network** → **TCP/IP** → **NTP**.
2. Aktivieren Sie das Kontrollkästchen **Enable**.
3. Konfigurieren Sie die NTP-Einstellungen.

   Interval (min)

   Das Zeitintervall zwischen zwei Zeitsynchronisationen mit dem NTP-Server

   NTP Server

   IP-Adresse des NTP-Servers

   NTP Port

   Port des NTP-Servers
4. Klicken Sie auf **Apply**.

15.2.3 DST-Synchronisation

DST (Sommerzeit) bezieht sich auf den Zeitraum des Jahres, in dem die Uhren um eine Stunde vorgestellt werden. In einigen Gebieten hat dies den Effekt, dass in den Monaten, in denen das Wetter am wärmsten ist, mehr Sonnenstunden am Abend entstehen.

Wir stellen unsere Uhren zu Beginn der Sommerzeit um eine Stunde vor (abhängig von der eingestellten Sommerzeit) und stellen sie um eine Stunde zurück, wenn wir zur Standardzeit zurückkehren.

Schritte

1. Gehen Sie zu **System** → **General**.
2. Aktivieren Sie das Kontrollkästchen **Enable DST**.
3. Wählen Sie als **DST mode** die Option **Auto** oder **Manual**.

Auto

Aktiviert automatisch die Sommerzeit gemäß den entsprechenden lokalen Regeln.

Manuell

Erfordert manuell das Einstellen von Beginn und Ende der Sommerzeit sowie des Zeitversatzes.

4. Legen Sie „DST Bias“ fest. Stellen Sie den Zeitversatz (30/60/90/120 Minuten) gegenüber der Standardzeit ein.
5. Klicken Sie auf **Apply**, um die Einstellungen zu speichern.

15.2.4 IP-Kamera-Zeitsynchronisation

Das Gerät kann die Uhrzeit der verbundenen IP-Kamera automatisch synchronisieren, nachdem diese Funktion aktiviert wurde.

Schritte

1. Gehen Sie zu **Camera** → **Camera** → **IP Camera**.
2. Führen Sie den Mauszeiger auf das Fenster der IP-Kamera und klicken Sie auf .
3. Aktivieren Sie das Kontrollkästchen **Enable IP Camera Time Sync**.
4. Klicken Sie auf **OK**.

15.3 Netzwerkerkennung

15.3.1 Netzwerkverkehrsüberwachung

Die Netzwerkverkehrsüberwachung beschreibt die Überprüfung, Analyse und Verwaltung des Netzwerkverkehrs hinsichtlich Anomalien oder Prozessen, die sich auf Netzwerkleistung, Verfügbarkeit und/oder Sicherheit auswirken können.

Schritte

1. Gehen Sie zu **Maintenance** → **Network** → **Traffic**.
2. Sie können den Status des Netzwerkdatenverkehrs, einschließlich MTU (Maximum Transmission Unit) und Netzwerkdurchsatz, in Echtzeit abrufen.

Abbildung 15-1 Netzwerkverkehr

15.3.2 Netzwerkverzögerung und Paketverlust prüfen

Die Netzwerkverzögerung wird durch eine langsame Reaktion des Geräts verursacht, wenn überdimensionierte Dateninformationen während der Übertragung unter bestimmten Netzwerkprotokollen wie TCP/IP nicht begrenzt werden. Der Paketverlusttest überprüft die Häufigkeit von Paketverlusten im Netzwerk und stellt das Verhältnis der verlorenen Datenpakete zur Gesamtzahl der übertragenen Datenpakete dar.

Schritte

1. Gehen Sie zu **Maintenance** → **Network** → **Network Detection**.
2. Wählen Sie unter **Select NIC** eine Netzwerkkarte aus.
3. Geben Sie in **Destination Address** die IP-Zieladresse ein.
4. Klicken Sie auf **Test**.

Abbildung 15-2 Netzwerkverzögerung und Paketverlust prüfen

15.3.3 Netzwerkpaket exportieren

Nachdem der Rekorder auf das Netzwerk zugegriffen hat, kann das Netzwerkpaket mit einem USB-Stick exportiert werden.

Bevor Sie beginnen

Bereiten Sie einen USB-Stick vor, um das Netzwerkpaket zu exportieren.

Schritte

1. Schließen Sie den USB-Stick an.
2. Gehen Sie zu **Maintenance** → **Network** → **Network Detection**.
3. Wählen Sie unter **Select NIC** die Netzwerkkarte aus.
4. Wählen Sie unter **Device Name** den USB-Stick aus. Klicken Sie auf **Refresh**, falls das angeschlossene lokale Speichermedium nicht angezeigt werden kann.

Abbildung 15-3 Netzwerkpaket exportieren

5. Optional: Klicken Sie auf **Status**, um den Netzwerkstatus anzuzeigen.
6. Klicken Sie auf **Export**.

Hinweis

Standardmäßig wird jedes Mal 1 MB Daten exportiert.

15.3.4 Netzwerk-Ressourcen-Statistik

Der Remote-Zugriff, auch auf Webbrowser und Client-Software, verbraucht Ausgabebandbreite. Sie können die Bandbreitenstatistik in Echtzeit anzeigen.

Schritte

1. Gehen Sie zu **Maintenance** → **Network** → **Network Stat**.

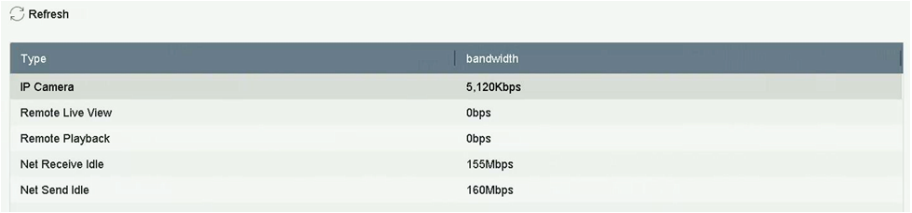


Abbildung 15-4 Netzwerkressourcenstatistik

2. Rufen Sie die Bandbreitenstatistik einschließlich **IP Camera**, **Remote Live View**, **Remote Play**, **Net Total Idle** usw. ab.
3. Optional: Klicken Sie auf **Refresh**, um die aktuellen Daten abzurufen.

15.4 Speichergerätewartung

15.4.1 Erkennung fehlerhafter Sektoren

Schritte

1. Gehen Sie zu **Maintenance** → **HDD Operation** → **Bad Sector Detection**.
2. Wählen Sie die Nummer der zu konfigurierenden Festplatte im Aufklappmenü.
3. Wählen Sie als Erkennungstyp **All Detection** oder **Key Area Detection**.
4. Klicken Sie auf **Self-Test**, um die Erkennung zu starten.

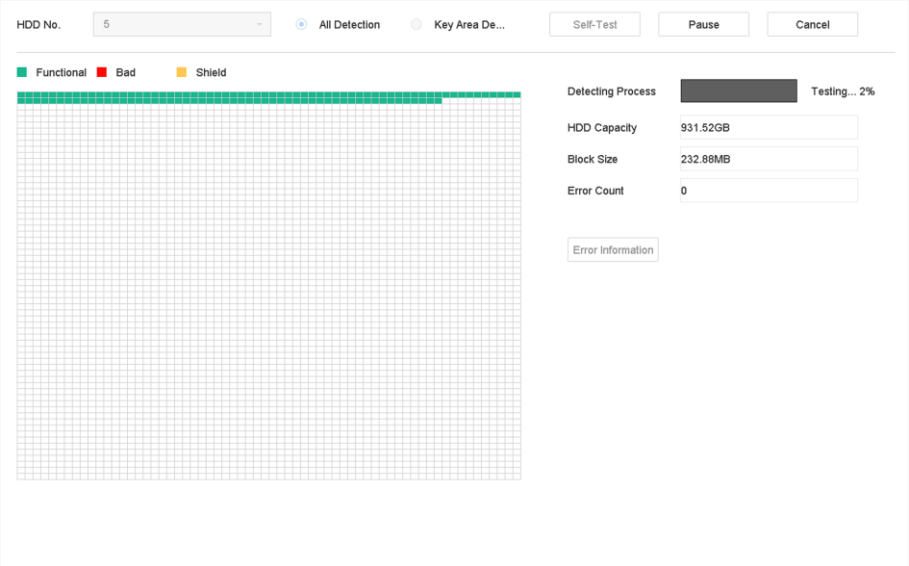


Abbildung 15-5 Fehlerhafte Sektorerkennung

Hinweis

Sie können die Erkennung pausieren und wieder starten. Nach Abschluss des Tests klicken Sie auf **Error information**, um die detaillierten Schadensinformationen anzuzeigen.

15.4.2 S.M.A.R.T. Detection

Festplatten-Erkennungsfunktionen wie die Übernahme der S.M.A.R.T.- und der Bad-Sector-Detection-Techniken. S.M.A.R.T. (Self-Monitoring, Analysis & Reporting Technology) sind Festplatten-Überwachungssysteme zur Erkennung verschiedener Zuverlässigkeitsindikatoren zum Zweck der Fehlererkennung.

Schritte

1. Gehen Sie zu **Maintenance** → **HDD Operation** → **S.M.A.R.T**.
2. Wählen Sie die Festplatte aus, um ihre S.M.A.R.T.-Informationsliste aufzurufen.

3. Legen Sie den Typ unter **Self-Test Type** fest.
4. Klicken Sie auf **Self-Test**, um S.M.A.R.T. zu starten. Festplatten-Selbsttest

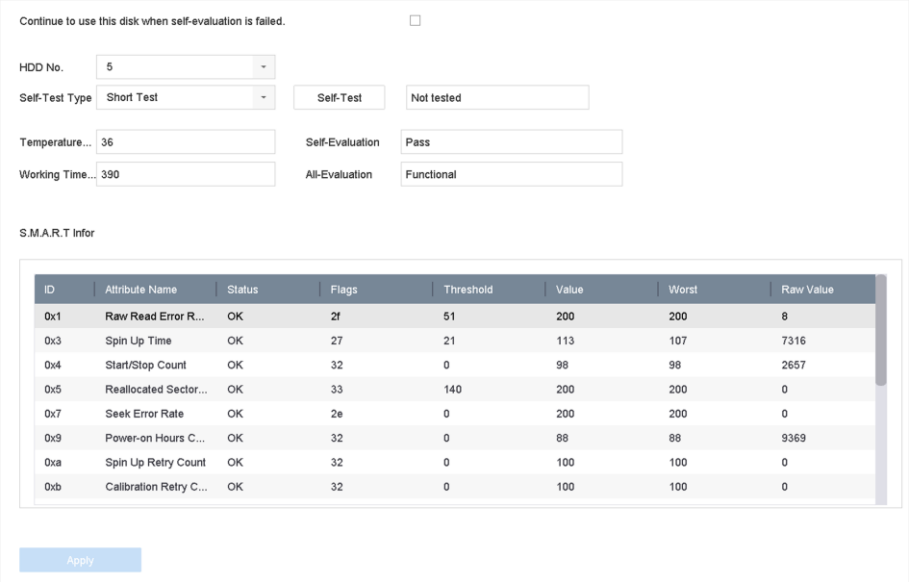


Abbildung 15-6 S.M.A.R.T. Einstellmenü

Hinweis

Um die Festplatte auch dann zu verwenden, wenn der S.M.A.R.T.-Test fehlgeschlagen ist, aktivieren Sie das Kontrollkästchen **Continue to use the disk when self-evaluation is failed**.

Die zugehörigen S.M.A.R.T.-Informationen werden angezeigt, und Sie können den Festplattenstatus überprüfen.

15.4.3 Festplatten-Integritätserkennung

Sie können den Integritätsstatus einer Seagate-Festplatte mit 4 TB bis 8 TB anzeigen, sofern sie nach dem 1. Oktober 2017 erstellt wurde. Verwenden Sie diese Funktion, um Probleme mit der Festplatte zu beheben. „Health Detection“ zeigt einen genaueren Festplattenstatus als die S.M.A.R.T.-Funktion.

Schritte

1. Gehen Sie zu **Maintenance** → **HDD Operation** → **Health Detection**.

Abbildung 15-7 Integritätserkennung

2. Klicken Sie auf eine Festplatte, um die Details anzuzeigen.

15.4.4 Festplattenklon konfigurieren

Wählen Sie die auf die eSATA-Festplatte zu klonenden Festplatten.

Bevor Sie beginnen

Schließen Sie eine eSATA-Festplatte am Gerät an.

Schritte

1. Gehen Sie zu **Maintenance** → **HDD Operation** → **HDD Clone**.

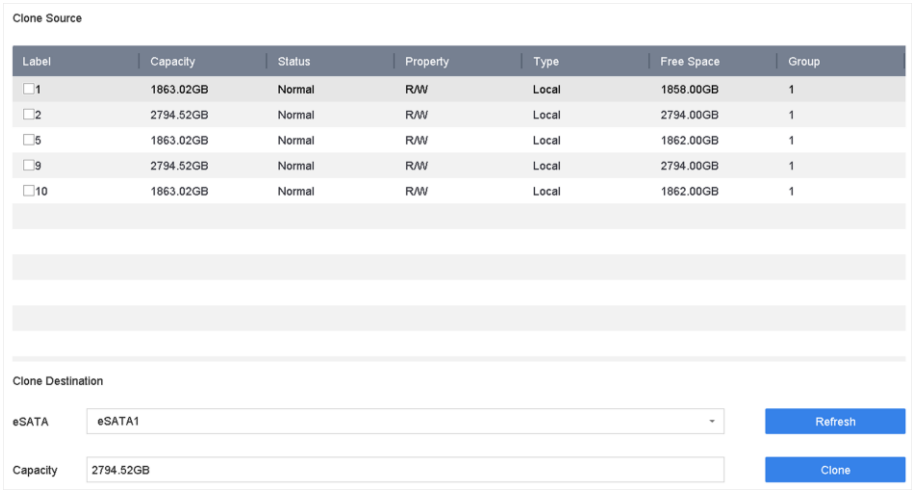


Abbildung 15-8 Festplattenklon

2. Aktivieren Sie das Kontrollkästchen der zu klonenden Festplatte. Die Kapazität der gewählten Festplatte muss mit der Kapazität des Klonziels übereinstimmen.
3. Klicken Sie auf **Clone**.
4. Klicken Sie im Dialogfenster zum Erstellen des Klons auf **Yes**.

15.4.5 Datenbank reparieren

Beim Reparieren der Datenbank werden alle Datenbanken neu aufgebaut. Dies kann dazu beitragen, die Systemgeschwindigkeit nach dem Upgrade zu verbessern.

Schritte

1. Gehen Sie zu **Storage** → **Storage Device**.
2. Wählen Sie das Laufwerk aus.
3. Klicken Sie auf **Repair Database**.
4. Klicken Sie auf **Yes**.

Hinweis

- Beim Reparieren der Datenbank werden alle Datenbanken neu aufgebaut. Die vorhandenen Daten sind nicht betroffen, aber die lokalen Such- und Wiedergabefunktionen sind währenddessen nicht verfügbar. Such- und Wiedergabefunktionen können Sie weiterhin per Fernzugriff über Webbrowser, Client-Software usw. ausführen
- Ziehen Sie das Laufwerk nicht heraus und fahren Sie das Gerät während des Vorgangs nicht herunter.

Sie können den Fortschritt der Reparatur unter **Status** verfolgen.

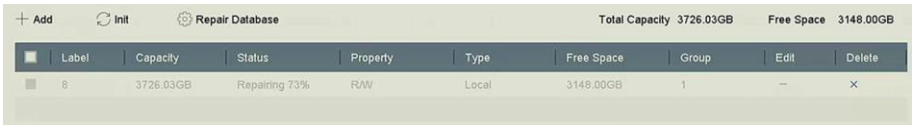


Abbildung 15-9 Datenbank reparieren

15.5 Gerät aktualisieren

Die Geräte-Firmware kann mit einem lokalen Sicherungsgerät oder einem externen FTP-Server aktualisiert werden.

15.5.1 Upgrade mit lokalem Sicherungsgerät

Bevor Sie beginnen

Verbinden Sie das Gerät mit einem lokalen Speichergerät, das die Firmware-Aktualisierungsdatei enthält.

Schritte

1. Gehen Sie zu **Maintenance** → **Upgrade**.
2. Klicken Sie auf **Local Upgrade**, um das Menü für die lokale Aktualisierung aufzurufen.

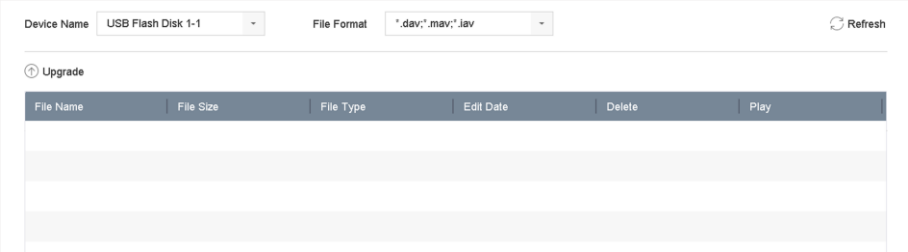


Abbildung 15-10 Menü für die lokale Aktualisierung

3. Wählen Sie die Firmware-Aktualisierungsdatei auf dem Speichergerät aus.
4. Klicken Sie auf **Upgrade**, um die Aktualisierung zu starten.
   Nach Abschluss der Aktualisierung startet das Gerät automatisch neu, um die neue Firmware zu aktivieren.

15.5.2 Upgrade per FTP

Bevor Sie beginnen

Vergewissern Sie sich, dass die Netzwerkverbindung von PC (laufender FTP-Server) und Gerät gültig und korrekt ist. Führen Sie den FTP-Server auf dem PC aus und kopieren Sie die Firmware in das entsprechende Verzeichnis Ihres PC.

Schritte

1. Gehen Sie zu **Maintenance** → **Upgrade**.
2. Klicken Sie auf **FTP**, um das Menü für die lokale Aktualisierung aufzurufen.

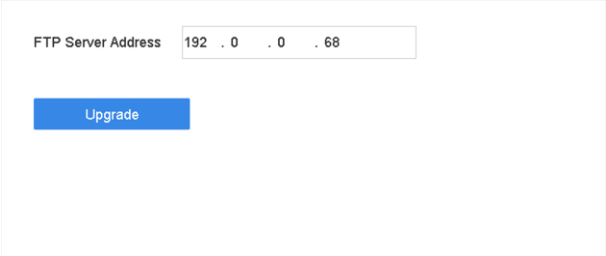


Abbildung 15-11 Menü für die FTP-Aktualisierung

3. Geben Sie die **FTP Server Address** ein.
4. Klicken Sie auf **Upgrade**, um die Aktualisierung zu starten.
5. Nach Abschluss der Aktualisierung starten Sie das Gerät neu, um die neue Firmware zu aktivieren.

15.5.3 Aktualisierung über Hik-Connect

Nachdem das Gerät bei Hik-Connect angemeldet wurde, überprüft es regelmäßig, ob eine neue Firmwareversion von Hik-Connect verfügbar ist. Wenn eine Firmware-Aktualisierung verfügbar ist, werden Sie beim Anmelden vom Gerät benachrichtigt. Sie können auch manuell nach der

neuesten Firmware suchen.

Bevor Sie beginnen

Stellen Sie sicher, dass das Gerät erfolgreich eine Verbindung zu Hik-Connect hergestellt hat. Es muss mindestens eine Lese-/Schreib-Festplatte zum Herunterladen der Firmware installiert sein.

Schritte

1. Gehen Sie zu **Maintenance** → **Upgrade** → **Online Upgrade**.
2. Klicken Sie auf **Check Upgrade**, um die neueste Firmware von Hik-Connect manuell zu überprüfen und herunterzuladen.

Hinweis

Das Gerät prüft alle 24 Stunden automatisch auf neue Firmwareversionen. Wenn es eine verfügbare Firmware-Aktualisierung erkennt, werden Sie bei der Anmeldung vom Gerät benachrichtigt.

3. Optional: Sie können die Option **Download Latest Package Automatically** aktivieren, sodass das aktuelle Firmware-Paket automatisch heruntergeladen wird.
4. Klicken Sie auf **Upgrade Now**.

15.6 IP-Kamera-Konfigurationsdateien importieren/exportieren

Die IP-Kameradaten, einschließlich IP-Adresse, Verwaltungsport, Passwort des Administrators usw. können im Microsoft Excel-Format gespeichert und auf dem lokalen Gerät gesichert werden. Die exportierte Datei kann auf einem PC bearbeitet werden, einschließlich Hinzufügen oder Löschen des Inhalts und Kopieren der Einstellung auf andere Geräte durch Importieren der Excel-Datei.

Bevor Sie beginnen

Beim Import der Konfigurationsdatei schließen Sie das Speichergerät, das die Konfigurationsdatei enthält, an das Gerät an.

Schritte

1. Gehen Sie zu **Camera** → **IP Camera Import/Export**.
2. Klicken Sie auf **IP Camera Import/Export**. Damit werden die Inhalte des erkannten externen Geräts angezeigt.
3. Exportieren oder importieren Sie die IP-Kamera-Konfigurationsdateien.
   - Klicken Sie auf **Export**, um die Konfigurationsdateien auf das ausgewählte lokale Sicherungsgerät zu exportieren.
   - Um eine Konfigurationsdatei zu importieren, wählen Sie die Datei auf dem ausgewählten Sicherungsgerät aus und klicken auf **Import**.

Hinweis

Nach Abschluss des Imports müssen Sie das Gerät neu starten, um die Einstellungen zu aktivieren.

15.7 Geräte-Konfigurationsdateien importieren/exportieren

Die Geräte-Konfigurationsdateien können in ein lokales Gerät zur Sicherung exportiert werden, und die Konfigurationsdateien eines Geräts können in mehrere Geräte importiert werden, wenn sie mit den gleichen Parametern konfiguriert werden sollen.

Bevor Sie beginnen

Schließen Sie ein Speichergerät an Ihr Gerät an. Um die Konfigurationsdatei zu importieren, muss das Speichergerät die Datei enthalten.

Schritte

1. Gehen Sie zu **Maintenance** → **Import/Export**.

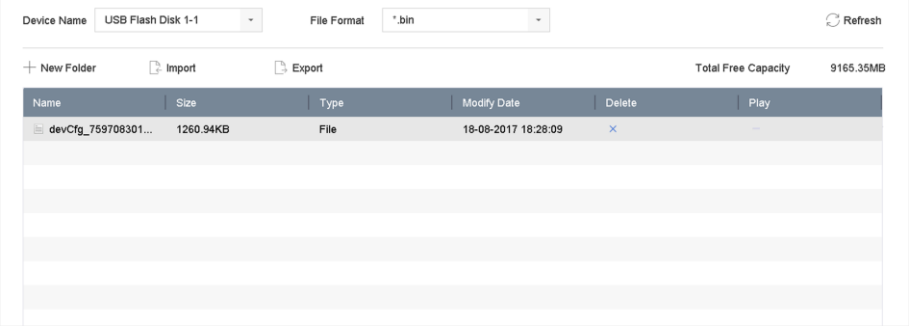


Abbildung 15-12 Konfigurationsdatei importieren/exportieren

2. Exportieren oder importieren Sie die Gerätekonfigurationsdateien.
   - Klicken Sie auf **Export**, um die Konfigurationsdateien auf das ausgewählte lokale Sicherungsgerät zu exportieren.
   - Um eine Konfigurationsdatei zu importieren, wählen Sie die Datei auf dem ausgewählten Sicherungsgerät aus und klicken auf **Import**.

Hinweis

Nach dem Import der Konfigurationsdateien wird das Gerät automatisch neu gestartet.

15.8 Protokollverwaltung

15.8.1 Protokollspeicherung

Sie können die Festplatte für die Protokollspeicherung und deren Dauer individuell festlegen.

Schritte

1. Gehen Sie zu **Storage** → **Advanced**.

Abbildung 15-13 Protokollspeicherung

2. Legen Sie den Modus unter **Log Storage Mode** fest.

System Default	Jede Festplatte weist einen bestimmten Speicherplatz für ca. 400.000 Protokolle zu. Wenn der Speicherplatz voll ist, werden alte Protokolle überschrieben.
Custom	Sie können die Dauer unter **Log Storage Period** festlegen und unter **Log Disk** die Festplatte für die Protokollspeicherung angeben. Wenn die Protokollfestplatte voll ist, werden Protokolle, die den angegebenen Zeitraum überschreiten, überschrieben.

3. Klicken Sie auf **Apply**.

15.8.2 Protokolldateien suchen und exportieren

Gerätebetrieb, Alarm, Ausnahme und Daten können in Protokolldateien gespeichert werden, die jederzeit eingesehen und exportiert werden können.

Schritte

1. Gehen Sie zu **Maintenance** → **Log Information**.

Abbildung 15-14 Menü für die Protokollsuche

2. Legen Sie die Bedingungen für die Protokollsuche fest, einschließlich Zeit, Haupttyp und Nebentyp.

3. Klicken Sie auf **Search**, um die Suche in den Protokolldateien zu starten.
4. Die übereinstimmenden Protokolldateien werden in der Liste angezeigt, wie unten dargestellt.

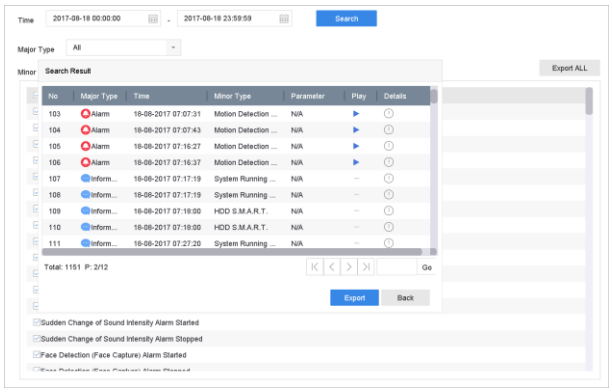


Abbildung 15-15 Protokollsuchergebnisse

Hinweis

Bis zu 2000 Protokolldateien können gleichzeitig angezeigt werden.

5. Related Operation:

ⓘ	Klicken oder doppelklicken Sie darauf, um detaillierte Informationen anzuzeigen.
▶	Klicken Sie darauf, um die zugehörige Videodatei anzuzeigen.
Export/Export ALL	Klicken Sie darauf, um alle Systemprotokolle auf das Speichermedium zu exportieren.

15.8.3 Protokolle auf den Server hochladen

Sie können Systemprotokolle zur Sicherung auf den Server hochladen.

Schritte

1. Gehen Sie zu **System** → **Network** → **Advanced** → **Log Server Settings**.

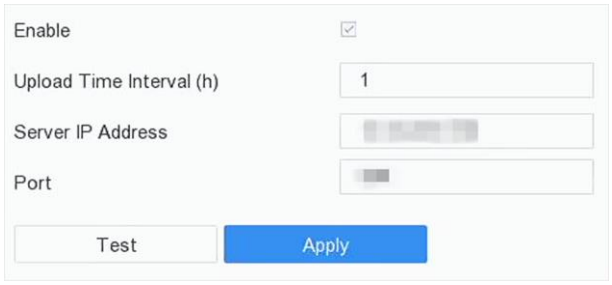


Abbildung 15-16 Einstellungen des Protokollservers

2. Aktivieren Sie das Kontrollkästchen **Enable**.

3. Legen Sie **Upload Time**, **Server IP Address** und **Port** fest.
4. Optional: Klicken Sie auf **Test**, um zu testen, ob die Parameter gültig sind.
5. Klicken Sie auf **Apply**.

15.8.4 Unidirektionale Authentifizierung

Sie können ein CA-Zertifikat (vom Server) auf Ihrem Gerät installieren, um den Server über einen Webbrowser zu autorisieren. Dies verbessert die Sicherheit der Protokollkommunikation.

Bevor Sie beginnen

- Laden Sie das CA-Zertifikat vom Server herunter.
- Stellen Sie sicher, dass die Protokollserver-Parameter gültig sind.

Schritte

1. Gehen Sie zu **Configuration** → **Network** → **Advanced Settings** → **Log Server Configuration**.

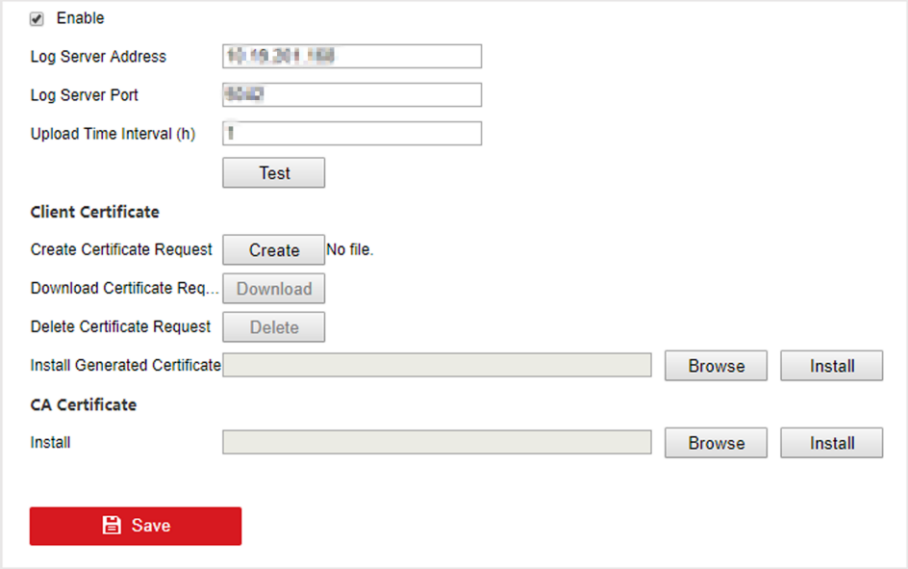


Abbildung 15-17 Unidirektionale Authentifizierung

2. Installieren Sie das CA-Zertifikat unter **CA Certificate**.
3. Optional: Klicken Sie auf **Test**, um zu testen, ob die Verbindung gültig ist.
4. Klicken Sie auf **Save**.

15.8.5 Bidirektionale Authentifizierung

Sie können ein CA-Zertifikat (vom Server) auf dem Gerät installieren, um den Server zu autorisieren, und ein Zertifikat (auf Ihrem Gerät) erstellen, um das Gerät über den Server zu autorisieren. Dies verbessert die Sicherheit der Protokollkommunikation. Die bidirektionale Authentifizierung kann über einen Webbrowser konfiguriert werden.

Bevor Sie beginnen

- Laden Sie das CA-Zertifikat vom Server herunter.

- Stellen Sie sicher, dass die Protokollserver-Parameter gültig sind.

Schritte

1. Gehen Sie zu **Configuration** → **Network** → **Advanced Settings** → **Log Server Configuration**.

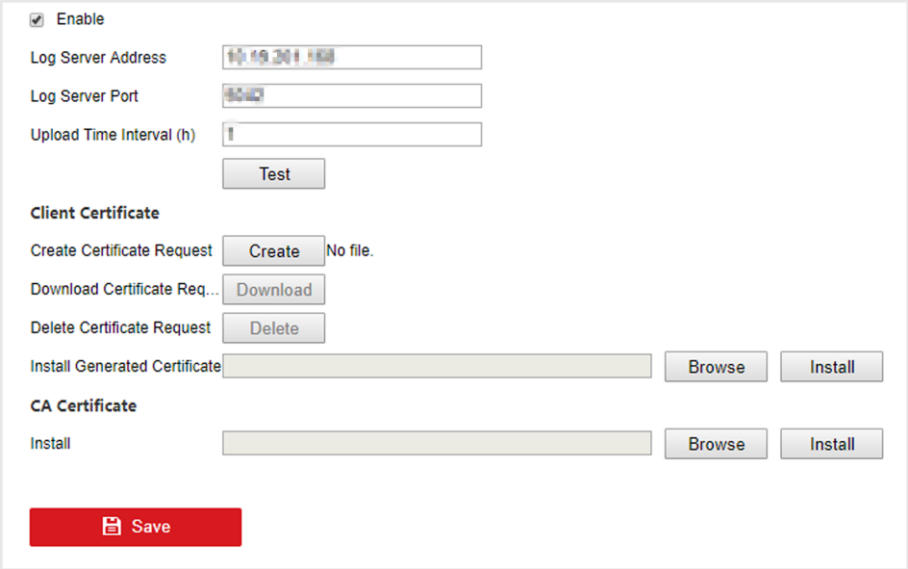


Abbildung 15-18 Bidirektionale Authentifizierung

2. Installieren Sie das CA-Zertifikat unter **CA Certificate**.
3. Klicken Sie unter **Client Certificate** auf **Create** und befolgen Sie die Anweisungen im Popup-Fenster, um das Zertifikat zu erstellen.
4. Klicken Sie auf **Download**, um die Zertifikatsdatei am gewünschten Speicherort herunterzuladen.
5. Laden Sie die heruntergeladene Zertifikatsdatei auf den Server hoch. Der Server gibt dann den Zertifikatschlüssel zurück.
6. Öffnen Sie das Zertifikat als Textdatei und ändern Sie es mithilfe des vom Server zurückgegebenen Zertifikatschlüssels.
7. Installieren Sie das geänderte Zertifikat unter **Client Certificate**.
8. Optional: Klicken Sie auf **Test**, um zu testen, ob die Verbindung gültig ist.
9. Klicken Sie auf **Save**.

15.9 Standardeinstellungen wiederherstellen

Schritte

1. Gehen Sie zu **Maintenance** → **Default**.

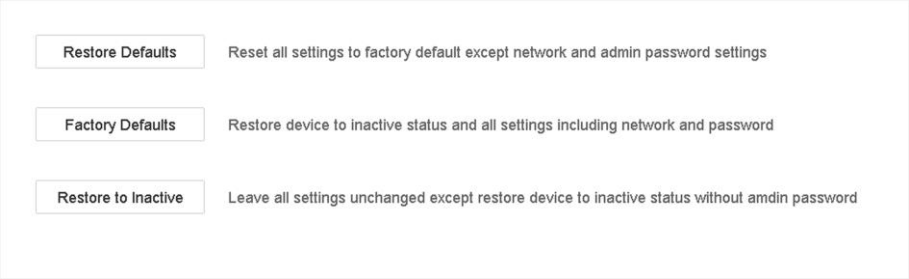


Abbildung 15-19 Standardeinstellungen wiederherstellen

2. Wählen Sie den Wiederherstellungstyp aus den folgenden drei Optionen aus.

Restore Defaults

Setzt alle Parameter außer Netzwerk (IP-Adresse, Subnetzmaske, Gateway, MTU, NIC-Arbeitsmodus, Standardroute, Serverport usw.) und Benutzerkontoparameter auf die Werkseinstellungen zurück.

Factory Defaults

Setzt alle Parameter auf die Werkseinstellungen zurück.

Restore to Inactive

Stellt den Rekorder im inaktiven Status wieder her.

Hinweis

Der Rekorder fährt nach der Rücksetzung auf die Standardeinstellungen automatisch hoch.

15.10 Sicherheitsverwaltung

15.10.1 IP/MAC-Adressfilter

Der Adressfilter entscheidet, ob bestimmte IP/MAC-Adressen für den Zugriff auf Ihr Gerät zugelassen oder abgelehnt werden.

Schritte

1. Gehen Sie zu **Maintenance** → **System Service** → **Address Filter**.

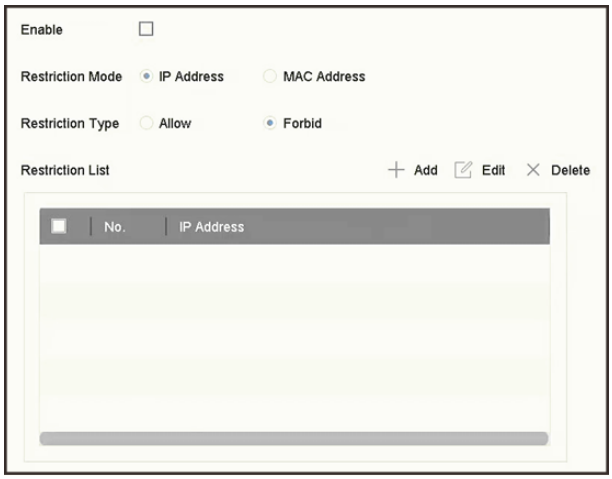


Abbildung 15-20 Adressfilter

2. Aktivieren Sie das Kontrollkästchen **Enable**.
3. Wählen Sie **Restriction Mode**. Wählen Sie diese Option, um nach IP-Adresse oder MAC-Adresse zu filtern.
4. Wählen Sie **Restriction Type**. Der Gerätemechanismus erlaubt oder verbietet spezifischen IP/MAC-Adressen, auf Ihr Gerät zuzugreifen.
5. Optional: Legen Sie die Inhalte der **Restriction List** fest. Sie können Adressen hinzufügen bearbeiten oder löschen.
6. Klicken Sie auf **Apply**, um die Einstellungen zu speichern.

15.10.2 RTSP-Authentifizierung

Sie können die Stream-Daten der Live-Ansicht gezielt sichern, indem Sie die RTSP-Authentifizierung einstellen.

Schritte

1. Gehen Sie zu **System** → **System Service** → **System Service**.

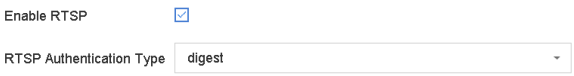


Abbildung 15-21 RTSP-Authentifizierung

2. Wählen Sie **RTSP Authentication Type**.

Hinweis

Es können zwei Authentifizierungstypen gewählt werden. Wenn Sie **digest** wählen, kann nur die Anforderung mit „digest“-Authentifizierung über die IP-Adresse per RTSP-Protokoll auf den Video-Stream zugreifen. Aus Sicherheitsgründen wird empfohlen, **digest** als Authentifizierungstyp zu wählen.

3. Klicken Sie auf **Apply**.
4. Starten Sie das Gerät neu, damit die Einstellungen wirksam werden.

15.10.3 RTSP-Digest-Algorithmus

Der RTSP-Digest-Algorithmus basiert auf dem RTSP-Protokoll und ist ein Algorithmus für die Digest-Authentifizierung der Benutzerauthentifizierung. Sie können den RTSP-Digest-Algorithmus über einen Webbrowser konfigurieren.
Gehen Sie über einen Webbrowser zu **Configuration** → **System** → **Security** → **Authentication**, um den gewünschten RTSP-Digest-Algorithmus zu wählen.

15.10.4 ISAPI-Dienst

ISAPI (Internet Server Application Programming Interface) ist ein offenes Protokoll, das auf HTTP basiert und die Kommunikation zwischen den Systemgeräten (z. B. Netzwerkkamera, NVR) ermöglicht. Das Gerät ist ein Server, der das Gerät finden und verbinden kann.

Schritte

1. Gehen Sie zu **System** → **System Service** → **System Service**.
2. Aktivieren Sie das Kontrollkästchen **Enable ISAPI**.
3. Klicken Sie auf **Apply**.
4. Starten Sie das Gerät neu, damit die Einstellungen wirksam werden.

15.10.5 HTTP-Authentifizierung

Wenn Sie den HTTP-Dienst aktivieren müssen, können Sie die HTTP-Authentifizierung einstellen, um die Zugriffsicherheit zu erhöhen.

Schritte

1. Gehen Sie zu **Maintenance** → **System Service** → **System Service**.

Abbildung 15-22 HTTP-Authentifizierung

2. Aktivieren Sie das Kontrollkästchen **Enable HTTP**.
3. Wählen Sie **HTTP Authentication Type**.

Hinweis

Es können zwei Authentifizierungstypen gewählt werden. Aus Sicherheitsgründen wird empfohlen, **digest** als Authentifizierungstyp zu wählen.

4. Klicken Sie auf **Apply**, um die Einstellungen zu speichern.
5. Starten Sie das Gerät neu, damit die Einstellungen wirksam werden.

15.10.6 HTTP/Web-Digest-Algorithmus

Der HTTP/Web-Digest-Algorithmus basiert auf dem HTTP-Protokoll und ist ein Algorithmus für die Digest-Authentifizierung der Benutzerauthentifizierung. Sie können den HTTP/Web-Digest-Algorithmus über einen Webbrowser konfigurieren.
Gehen Sie über einen Webbrowser zu **Configuration** → **System** → **Security** → **Authentication**, um den gewünschten Digest-Algorithmus zu wählen.

15.10.7 Bild-URL-Digest-Authentifizierung

Wenn Sie das HTTP-Protokoll zum Herunterladen der die von SDK hochgeladenen Bilder verwenden, kann die Digest-Authentifizierung für die Bild-URL kontrollieren, ob das Herunterladen des Bilds eine Digest-Authentifizierung erfordert. Sie können die Bild-URL-Digest-Authentifizierung über einen Webbrowser konfigurieren.
Gehen Sie über einen Webbrowser zu **Configuration** → **System** → **Security** → **Security Service**, um die Bild-URL-Digest-Authentifizierung zu aktivieren/deaktivieren.

15.10.8 Authentifizierungsdienst für serielle Ports

Ein serieller Port kann verwendet werden, um Geräteinformationen zu erfassen und das Gerät zu steuern. Der Authentifizierungsdienst für serielle Ports stellt die Authentifizierung für die Verwendung serieller Ports bereit.
Gehen Sie über einen Webbrowser zu **Configuration** → **System** → **Security** → **Security Service**, um den Authentifizierungsdienst für serielle Ports zu aktivieren/deaktivieren.

Service Close Time

Der Authentifizierungsservice für serielle Ports wird für einen bestimmten Zeitraum geschlossen. Wenn beispielsweise die **Service Close Time** auf **30** gesetzt ist, wird der Authentifizierungsdienst für die serielle Schnittstelle 30 Tage lang geschlossen. Nach 30 Tagen wird der Authentifizierungsdienst für den seriellen Port wieder aktiviert.

Kapitel 16 Anhang

16.1 Glossar

Dual-Stream

Dual-Stream ist eine Technologie, die zur lokalen Aufnahme von HD-Video verwendet wird, während ein Stream mit niedrigerer Auflösung über das Netzwerk übertragen wird. Beide Streams werden vom DVR erzeugt, wobei der Haupt-Stream die maximale Auflösung 1080p und der Sub-Stream die maximale Auflösung CIF hat.

DVR

Akronym für Digitaler Videorekorder. Ein DVR ist ein Gerät, das Videosignale von Analogkameras aufnimmt, das Signal anschließend komprimiert und auf seinen Laufwerken speichert.

HDD

Abkürzung für Hard Disk Drive = Festplatte. Speichermedium für digital codierte Daten auf Platten mit magnetischer Oberfläche.

DHCP

Dynamic Host Configuration Protocol (DHCP) ist ein Netzwerkanwendungsprotokoll, das von Geräten verwendet wird (DHCP-Clients), um Konfigurationsdaten zum Betrieb in einem Internet-Protokoll-Netzwerk zu erhalten.

HTTP

Abkürzung für Hypertext Transfer Protocol. Protokoll zur Übertragung von Hypertextanfragen und Daten zwischen Servern und Browsern über ein Netzwerk.

PPPoE

Akronym für Point-to-Point Protocol over Ethernet. PPPoE ist ein Netzwerkprotokoll, um PPP-(Point-to-Point Protocol-)Bilder in Ethernet-Bilder einzubinden. Es wird hauptsächlich von ADSL-Diensten, bei denen einzelne Benutzer über ein Ethernet mit einem ADSL-Transceiver (Modem) verbunden sind, oder in reinen Metro Ethernet-Netzwerken verwendet.

DDNS

Dynamisches DNS ist eine Methode, ein Protokoll oder ein Netzwerkdienst, womit einem Netzwerkgerät (z. B. Router oder Computersystem) unter Verwendung der Internet Protocol Suite ermöglicht wird, in Echtzeit (ad-hoc) die aktive DNS-Konfiguration seiner konfigurierten Hostnamen, Adressen oder anderen im DNS gespeicherten Informationen zu ändern.

Hybrid-DVR

Ein Hybrid-DVR ist eine Kombination aus DVR und NVR.

NTP

Abkürzung für Network Time Protocol. Ein Protokoll zur Synchronisierung der Uhren von Computern über ein Netzwerk.

NTSC

Abkürzung für National Television System Committee. NTSC ist ein analoger Fernsehstandard, der in Ländern wie den USA und Japan verwendet wird. Jedes Einzelbild eines NTSC-Signals enthält 525 Zeilen bei 60 Hz.

NVR

Abkürzung für Netzwerkvideorekorder. Ein NVR kann ein PC-basiertes oder eingebettetes System sein, das für die zentralisierte Verwaltung und Speicherung für IP-Kameras, IP-Kuppelkameras und andere DVRs verwendet wird.

PAL

Abkürzung für Phase Alternating Line. PAL ist ein weiterer Videostandard, der zur Übertragung von Fernsehsendungen in weiten Teilen der Welt verwendet wird. Das PAL-Signal enthält 625 Zeilen bei 50 Hz.

PTZ

Abkürzung für Pan, Tilt, Zoom. PTZ-Kameras sind Systeme mit Elektromotoren, die der Kamera Schwenks nach links und rechts, Aufwärts- und Abwärtsneigung sowie das Vergrößern und Verkleinern ermöglichen.

USB

Abkürzung für Universal Serial Bus. USB ist ein serieller Plug-&-Play-Busstandard zum Anschluss von Geräten an einen Host-Computer.

16.2 Kommunikationsmatrix

Scannen Sie den QR-Code unten, um das Dokument mit der Kommunikationsmatrix zu öffnen.

Abbildung 16-1 Kommunikationsmatrix

16.3 Gerätebefehl

Scannen Sie den QR-Code unten, um das Dokument mit dem Gerätebefehl zu öffnen.

Abbildung 16-2 Gerätebefehl

16.4 Häufige Fragen

16.4.1 Warum wird in einem Teil der Kanäle „No Resource“ bzw. in der Live-Ansicht auf mehreren Bildschirmen ein schwarzer Bildschirm angezeigt?

Grund

1. Sub-Stream-Auflösung oder Bitraten-Einstellungen sind ungeeignet.
2. Verbindung zum Sub-Stream fehlgeschlagen.

Lösung

1. Gehen Sie zu **Camera** → **Video Parameters** → **Sub-Stream**. Wählen Sie den Kanal aus und verringern Sie die Auflösung und die maximale Bitrate (die Auflösung muss kleiner als 720p sein und die maximale Bitrate weniger als 2048 kBit/s betragen).

Hinweis

Wenn Ihr Videorekorder diese Funktion nicht unterstützt, können Sie sich bei der Kamera anmelden und die Videoparameter über einen Webbrowser anpassen.

2. Stellen Sie die Sub-Stream-Auflösung und die maximale Bitrate ordnungsgemäß ein (die Auflösung muss kleiner als 720p sein und die maximale Bitrate muss kleiner als 2048 kBit/s sein). Löschen Sie den Kanal und fügen Sie ihn erneut hinzu.

16.4.2 Warum unterstützt der Videorekorder den Streamtyp nicht?

Grund

Das Codierungsformat der Kamera stimmt nicht mit dem Videorekorder überein.

Lösung

Wenn die Kamera H.265/MJPEG für die Verschlüsselung verwendet, der Videorekorder aber H.265/MJPEG nicht unterstützt, müssen Sie das Codierungsformat der Kamera in das gleiche Format wie beim Videorekorder ändern.

16.4.3 Warum meldet der Videorekorder nach dem Hinzufügen einer Netzwerkkamera ein riskantes Passwort?

Grund

Das Passwort der Kamera ist zu schwach.

Lösung

Ändern Sie das Passwort der Kamera.

Warnung

Legen Sie unbedingt ein eigenes sicheres Passwort mit mindestens 8 Zeichen aus mindestens drei der Kategorien „Groß- und Kleinbuchstaben“, „Ziffern“ und „Sonderzeichen“ fest, um die Produktsicherheit zu erhöhen. Wir empfehlen weiterhin, dass Sie Ihr Passwort regelmäßig monatlich oder wöchentlich zurücksetzen, insbesondere im Hochsicherheitssystem, um die Sicherheit Ihres Produkts zu erhöhen.

16.4.4 Wie verbessere ich die Wiedergabebildqualität?

Grund

Die Einstellungen für die Aufzeichnungsparameter sind ungeeignet.

Lösung

Gehen Sie zu **Camera** → **Video Parameters**. Erhöhen Sie die Auflösung und die maximale Bitrate und versuchen Sie es erneut.

16.4.5 Wie finde ich heraus, ob der Videorekorder bei der

Videoaufzeichnung H.265 verwendet?

Lösung

Prüfen Sie, ob der Codierungstyp in der Symbolleiste der Live-Ansicht „H.265“ lautet.

16.4.6 Warum ist die Zeitleiste bei der Wiedergabe nicht konstant?

Grund

1. Wenn der Videorekorder die Ereignisaufzeichnung verwendet, wird das Video nur bei einem Ereignis aufgezeichnet. Daher ist das Video möglicherweise nicht fortlaufend.
2. Es kommt zu einer Ausnahme, z. B. Gerät offline, Festplattenfehler, Datensatzausnahme, Netzwerkkamera offline usw.

Lösung

1. Stellen Sie sicher, dass der Aufzeichnungstyp „Continuous Recording“ ist.
2. Gehen Sie zu **Maintenance** → **Log Information**. Suchen Sie die Protokolldatei innerhalb des Videozeitraums. Prüfen Sie, ob unerwartete Ereignisse vorhanden sind, z. B. Festplattenfehler, Datensatzausnahmen usw.

16.4.7 Wenn eine Netzwerkkamera hinzugefügt wird, meldet der Videorekorder, dass das Netzwerk nicht erreichbar ist.

Grund

1. Die IP-Adresse oder der Port der Netzwerkkamera ist falsch.
2. Das Netzwerk zwischen Videorekorder und Kamera ist getrennt.

Lösung

1. Gehen Sie zu **Camera** → **Camera** → **IP Camera**. Klicken Sie auf bei der ausgewählten Kamera und bearbeiten Sie die IP-Adresse und den Port. Stellen Sie sicher, dass der Videorekorder und die Kamera denselben Anschluss verwenden.
2. Gehen Sie zu **Maintenance** → **Network** → **Detection**. Geben Sie die IP-Adresse der Netzwerkkamera in **Destination Address** ein und klicken Sie auf **Test**, um zu prüfen, ob das Netzwerk erreichbar ist.

16.4.8 Warum wird die IP-Adresse der Netzwerkkamera automatisch geändert?

Grund

Wenn Netzwerkkamera und Videorekorder denselben Switch verwenden, sich jedoch in einem

anderen Subnetz befinden, ändert der Videorekorder die IP-Adresse der Netzwerkkamera auf das Subnetz, das er selbst verwendet.

Lösung

Klicken Sie beim Hinzufügen der Kamera auf **Custom Add**, um die Kamera hinzuzufügen.

16.4.9 Warum meldet der Videorekorder einen IP-Konflikt?

Grund

Der Videorekorder verwendet dieselbe IP-Adresse wie andere Geräte.

Lösung

Ändern Sie die IP-Adresse des Videorekorders. Stellen Sie sicher, dass sie nicht mit den IP-Adressen anderer Geräte übereinstimmt.

16.4.10 Warum stockt das Bild bei der Wiedergabe im Einzel- oder Mehrkanalmodus?

Grund

Lese-/Schreibausnahme auf der Festplatte.

Lösung

Exportieren Sie das Video und spielen Sie es mit anderen Geräten ab. Wenn es auf einem anderen Gerät normal wiedergegeben wird, wechseln Sie die Festplatte und versuchen Sie es erneut.

16.4.11 Warum gibt mein Videorekorder nach dem Hochfahren ein akustisches Signal aus?

Grund

1. Die Frontplatte ist nicht befestigt (bei einem Gerät, dessen Frontplatte abgenommen werden kann).
2. Festplattenfehler oder keine Festplatte vorhanden.

Lösung

1. Wenn ein durchgehender Signalton ausgegeben wird und das Gerät eine abnehmbare Frontplatte hat, stellen Sie sicher, dass die Frontplatte befestigt ist.
2. Wenn ein unterbrochener Signalton ausgegeben wird (3x lang, 2x kurz), nehmen Sie einen Festplattenfehler als Beispiel und prüfen Sie, ob das Gerät eine Festplatte hat. Andernfalls können Sie zu **System** → **Event** → **Normal Event** → **Exception** gehen und die Option **Event Hint Configuration** abwählen, um Hinweise auf Festplatten-Fehlerereignisse zu deaktivieren.

Überprüfen Sie, ob die Festplatte initialisiert wurde. Andernfalls gehen Sie zu „Storage“ > „Storage Device“, um die Festplatte zu initialisieren.
Überprüfen Sie, ob die Festplatte beschädigt ist. Sie können sie austauschen und es erneut versuchen.

16.4.12 Warum wird nach dem Einstellen der Bewegungserkennung kein Video aufgezeichnet?

Grund

1. Der Aufnahmeplan ist fehlerhaft.
2. Die Einstellung für das Bewegungserkennungsereignis ist falsch.
3. Ausnahme bei der Festplatte.

Lösung

1. Der Aufnahmeplan wird ordnungsgemäß eingerichtet, indem die Schritte unter „Aufzeichnungs-/Aufnahmeplan konfigurieren“ befolgt werden.
2. Der Bewegungserkennungsbereich wurde korrekt konfiguriert. Die Kanäle für die Bewegungserkennung werden ausgelöst (siehe „Bewegungserkennung konfigurieren“).
3. Überprüfen Sie, ob auf dem Gerät eine Festplatte installiert ist.
   Überprüfen Sie, ob die Festplatte initialisiert wurde. Andernfalls gehen Sie zu „Storage“ > „Storage Device“, um die Festplatte zu initialisieren.
   Überprüfen Sie, ob die Festplatte beschädigt ist. Sie können sie austauschen und es erneut versuchen.

16.4.13 Warum ist die Klangqualität bei der Videoaufzeichnung nicht gut?

Grund

1. Das Audio-Eingabegerät wirkt sich negativ auf die Klangerfassung aus.
2. Störung in der Übertragung.
3. Der Audio-Parameter ist nicht richtig eingestellt.

Lösung

1. Überprüfen Sie, ob das Audio-Eingabegerät ordnungsgemäß funktioniert. Sie können das Audio-Eingabegerät austauschen und es erneut versuchen.
2. Überprüfen Sie die Audio-Übertragungsleitung. Stellen Sie sicher, dass alle Leitungen richtig angeschlossen bzw. verschweißt sind und keine elektromagnetischen Störungen vorliegen.
3. Passen Sie die Lautstärke an Umgebung und Audio-Eingabegerät an.


See Far, Go Further