



Bedienungsanleitung

GD-RN-BP8616P

GD-RN-BP8632N

GD-RN-DT8864N

Inhalt

1 Einleitung	5
1.1 Modellübersicht	5
2 Aktivieren über das lokale Menü	6
3 Melden Sie sich an Ihrem Gerät an	8
4 Netzwerkeinstellungen	9
4.1 Netzwerk-Parametereinstellungen	9
4.1.1 TCP/IP konfigurieren	9
4.1.2 DDNS konfigurieren	10
4.1.3 PPPoE konfigurieren	11
4.1.4 Multicast konfigurieren	12
4.2 Einstellungen für den Plattformzugang	12
4.2.1 SCMS konfigurieren	12
4.2.2 ISUP konfigurieren	13
4.2.3 SDK-Dienst konfigurieren	14
4.2.4 ISAPI einschalten	15
4.2.5 ONVIF konfigurieren	15
4.2.6 Log-Server konfigurieren	16
4.3 Netzwerkdienst-Einstellungen	17
4.3.1 HTTP(S) konfigurieren	17
4.3.2 RTSP konfigurieren	18
4.3.3 WebSocket(s) konfigurieren	19
4.3.4 Port-Zuordnung konfigurieren (NAT)	19
5 Benutzerverwaltung	21
6 Gerätezugriff	22
6.1 Zugang zum Videogerät	22
6.1.1 Automatisch gesuchte Online-Netzwerkamera hinzufügen	22
6.1.2 Netzwerkamera manuell hinzufügen	23
6.1.3 Netzwerkamera über benutzerdefiniertes Protokoll hinzufügen	24
6.1.4 Hinzufügen einer Netzwerkamera über die Kamerakonfigurationsdatei	25

6.2 Zugangskontrollgerät hinzufügen	25
6.3 Audiogerät hinzufügen.....	26
6.4 POS-Gerät hinzufügen.....	26
7 Kameraeinstellungen	28
7.1 Aktivieren des H.265-Stream-Zugriffs.....	28
7.2 Batch-Konfiguration	28
7.3 Anzeigeeinstellungen	28
7.4 Konfigurieren der Videoparameter.....	29
7.5 Privatzone konfigurieren.....	30
8 Gerätegruppierung.....	32
9 Speicherverwaltung	33
9.1 HDD verwalten	33
9.2 RAID-Konfiguration	34
9.2.1 Festplatten-Array erstellen	35
9.2.2 Array wiederherstellen	36
9.2.3 Array löschen	37
9.2.4 Firmware-Informationen anzeigen	37
9.3 Speichermodus konfigurieren.....	37
9.4 Andere Speicherparameter konfigurieren.....	38
10 Zeitplan Konfiguration	39
10.1 Zeitplanvorlage konfigurieren.....	39
10.2 Aufzeichnungszeitplan konfigurieren	40
10.3 Zeitplan für die Bildaufnahme konfigurieren.....	43
10.4 Konfigurieren der Audioaufzeichnung.....	44
11 Live-Ansicht	46
11.1 Layout der Live-Ansicht konfigurieren	46
11.2 GUI-Einführung	46
11.3 PTZ-Steuerung.....	47
12 Wiedergabe	49
12.1 GUI-Einführung	49
12.2 Normale Wiedergabe.....	50

12.3 Wiedergabe von Ereignissen.....	51
12.4 Wiedergabe von Teilperioden	51
13 Ereigniszentrum	53
13.1 Ereigniseinstellungen	53
13.1.1 Grundlegendes/allgemeines Ereignis	53
13.1.2 Perimeterschutz	56
13.1.3 Ereignis mit abnormalem Verhalten	66
13.1.4 Zielereignis	69
13.1.5 Wärmebildkamera-Erkennung.....	72
13.1.6 Alarmeingang Ereignis	74
13.1.7 Ereignis Audioanalyse	76
13.2 Konfiguration des Gestänges	77
13.3 Ereignissuche	79
13.4 Alarme anzeigen.....	79
14 Suche und Sicherung.....	80
15 Intelligente Einstellungen	82
15.1 Algorithmus-Verwaltung.....	82
15.2 Verwaltung der Listenbibliothek.....	82
15.2.1 Hinzufügen einer Listenbibliothek	82
15.2.2 Hochladen von Gesichtsbildern in die Bibliothek	82
16 Anwendungszentrum	84
16.1 Erkennung von Personen und Fahrzeugen	84
16.2 Personen-Check-In	84
16.2.1 Check-In Aufgabe	85
16.2.2 Check-In-Datensätze suchen.....	85
16.3 Statistischer Bericht	86
17 Systemparametereinstellungen.....	87
18 Hot Spare-Gerätesicherung	88
18.1 Arbeitsgerät einstellen.....	88
18.2 Hot Spare Gerät einstellen.....	88

19 Systemereignis konfigurieren	90
20 Systeminformationen anzeigen	92
21 Wartung des Systems.....	93
21.1 Neustart einplanen	93
21.2 Gerät aufrüsten	93
21.3 Sicherung und Wiederherstellung	93
21.4 Protokollinformationen	94
21.5 Log-Server konfigurieren	94
21.6 Wartungswerkzeuge	94
22 Sicherheitsmanagement	96
22.1 Adressfilter	96
22.2 Stream-Verschlüsselung.....	96
22.3 TLS-Version auswählen	96
23 Anhang	97
23.1 Liste der verwendbaren Netzteile.....	97
23.2 Glossar.....	98
23.3 Häufig gestellte Fragen	99

1 Einleitung

Vielen Dank, dass Sie sich für ein Grundig-Produkt entschieden haben. Bevor Sie das Produkt installieren oder anschließen, sollten Sie lesen Sie zuerst die folgenden Dokumente:

- Rechtlicher Hinweis
- Sicherheitshinweise
- Installationshandbuch und/oder Kurzanleitung für das jeweilige Produktmodell

Weitere Informationen über das Produkt wie Datenblätter, CE-Dokumente usw. finden Sie auch unter

unsere Webseite www.grundig-security.com.

Dieses Benutzerhandbuch ist ein Handbuch für Netzwerk-Videorekorder. Bitte beachten Sie die Liste der 1.1 Modelle

Übersicht der anwendbaren Modelle.

Bitte lesen Sie dieses Benutzerhandbuch sorgfältig durch und bewahren Sie es zur späteren Verwendung auf.

1.1 Modellübersicht

Dieses Benutzerhandbuch gilt für die folgenden Produkte:

- GD-RN-BP8616P
- GD-RN-BP8632N
- GD-RN-DT8864N

2 Aktivieren über das lokale Menü

Für den erstmaligen Zugang müssen Sie ein Admin-Passwort festlegen, um Ihr Gerät zu aktivieren. Vor der Aktivierung ist keine Bedienung möglich. Sie können das Gerät auch über einen Webbrowser, SADP oder eine Client-Software aktivieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihr Gerät mit einem Monitor und einer Maus verbunden ist.

Schritte

1. Schalten Sie Ihr Gerät ein.
2. Wählen Sie eine Systemsprache.
3. Geben Sie das Admin-Passwort zweimal ein.

Vorsicht

Wir empfehlen Ihnen dringend, ein sicheres Passwort Ihrer Wahl zu erstellen (mit mindestens 8 Zeichen, darunter mindestens drei Arten der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zu ändern, vor allem im Hochsicherheitssystem kann eine monatliche oder wöchentliche Änderung des Passworts Ihr Produkt besser schützen.

The screenshot shows the 'Activation' screen of a Grundig device. It has a dark header with the word 'Activation' in white. Below the header, there are several input fields and checkboxes. The first field is labeled 'admin' and contains the text 'admin'. Below it is a field labeled 'Create New Password' with a strength indicator bar. Then there is a field labeled 'Confirm New Password'. Below that is a checkbox labeled 'Export GUID' with a question mark icon to its right. At the bottom of the form is a field labeled 'Create Channel Default Password'. Below the form, there is a note: 'Note: Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.' At the very bottom is an 'OK' button and a small line of text: 'Please respect other people's privacy and rights when using product.'

Abbildung 2-1 Aktivieren über das lokale Menü

4. Optional: Geben Sie einen Passwort-Hinweis ein. Er hilft Ihnen, sich an Ihr Passwort zu erinnern, wenn Sie es vergessen haben.
5. Klicken Sie auf **Aktivieren**.

Hinweis

Nach der Aktivierung des Geräts sollten Sie das Passwort sorgfältig aufbewahren.

6. Optional: Zeichnen Sie ein Entsperrmuster.
7. Konfigurieren Sie mindestens eine Methode zur Wiederherstellung des Passworts.

Was ist als nächstes zu tun?

Folgen Sie dem Assistenten, um die grundlegenden Parameter einzustellen.

3 Melden Sie sich an Ihrem Gerät an

Sie müssen sich bei Ihrem Gerät anmelden, bevor Sie das Menü und andere Funktionen nutzen können.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihr Gerät aktiviert ist.

Schritte

1. Schalten Sie Ihr Gerät ein. Sie gelangen dann automatisch in die Anmeldemaske.

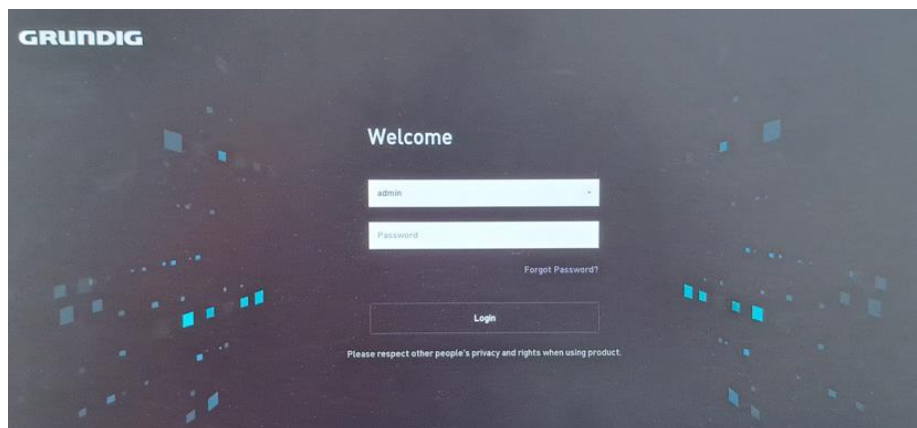


Abbildung 3-1 Anmeldung

2. Verwenden Sie das Entsperrmuster, um sich anzumelden, oder klicken Sie auf **Kennwortanmeldung**, um sich mit Benutzernamen und Kennwort anzumelden.

Hinweis

- Das Entsperrmuster ist nur für Admin-Benutzer verfügbar.
 - Wenn Sie Ihr Entsperrmuster oder Ihr Anmeldekennwort vergessen haben, klicken Sie auf **Kennwort vergessen** auf der Benutzeroberfläche für die Kennwortanmeldung, um Ihr Kennwort zurückzusetzen, oder verwenden Sie den Kennwothinweis zur Erinnerung.
-

4 Netzwerkeinstellungen

Netzwerkparameter, Einstellungen für den Plattformzugang und Netzwerkdienste sind konfigurierbar.

4.1 Netzwerk-Parametereinstellungen

Sie müssen die Netzwerkparameter konfigurieren, bevor Sie Funktionen nutzen, die einen Netzwerkzugang erfordern.

4.1.1 TCP/IP konfigurieren

TCP/IP muss richtig konfiguriert sein, bevor Sie den Videorecorder über das Netzwerk betreiben oder auf Netzwerkgeräte zugreifen.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **Netzwerk** → **TCP/IP**.

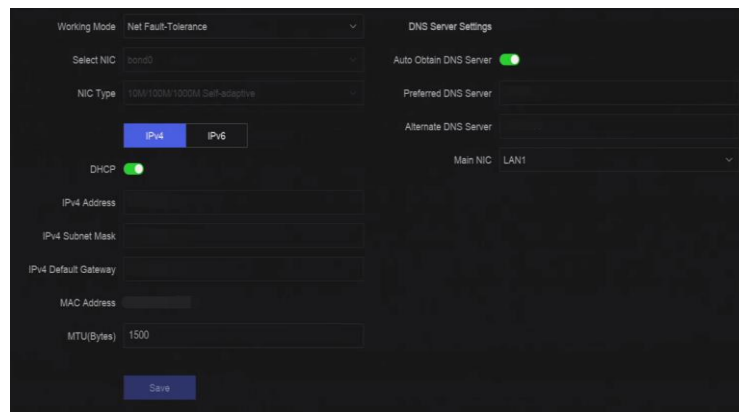


Abbildung 4-1 TCP/IP-Einstellungen

2. **Arbeitsmodus** einstellen und **NIC** auswählen.

Mehrfachadressen

Die Parameter der beiden NIC-Karten können unabhängig voneinander konfiguriert werden. Sie können **LAN1** oder **LAN2** im Feld NIC-Typ für die Parametereinstellungen auswählen. Sie können eine NIC-Karte als Standardroute auswählen. Dann verbindet sich das System mit dem Extranet und die Daten werden über die Standardroute weitergeleitet.

Netzfehlertoleranz

Die beiden NIC-Karten verwenden dieselbe IP-Adresse, und Sie können **Main NIC** auf **LAN1** oder **LAN2** einstellen. Auf diese Weise aktiviert der Videorecorder im Falle eines Ausfalls einer NIC-Karte automatisch die andere Standby-NIC-Karte, um den normalen Betrieb des gesamten Systems zu gewährleisten.

Hinweis

Der Arbeitsmodus ist nur bei bestimmten Modellen verfügbar.

3. Konfigurieren Sie die Netzwerkparameter.

IPv4**DHCP**

Wenn der DHCP-Server verfügbar ist, können Sie **DHCP** aktivieren, um automatisch eine IP-Adresse und andere Netzwerkeinstellungen von diesem Server zu beziehen.

MTU

Die maximale Übertragungseinheit (MTU) ist die Größe der größten Dateneinheit des Netzschichtprotokolls, die in einer einzigen Netztransaktion übertragen werden kann.

DNS-Server automatisch abrufen

Wenn **DHCP** aktiviert ist, Sie können die Option **Auto Obtain DNS Server** aktivieren, um den **bevorzugten DNS-Server** und den **alternativen DNS-Server** zu beziehen.

IPv6**Router-Anzeige**

Wenn der Router im Netzwerk IPv6 unterstützt, ist es empfehlenswert, diesen Modus als Standard zu verwenden.

Auto

Wenn ein DHCPv6-Gerät im Netzwerk vorhanden ist, wird empfohlen, diesen Modus zu verwenden

Manuelle Konfiguration

Diesen Modus sollten Sie verwenden, wenn Sie IPv6-Parameter manuell eingeben wollen.

4. Klicken Sie auf **Speichern**.

4.1.2 DDNS konfigurieren

Dynamische Domain-Name-Server (DDNS) ordnen dynamische Benutzer-IP-Adressen einem festen Domain-Name-Server zu.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie DynDNS-, PeanutHull- und NO-IP-Dienste bei Ihrem ISP registriert haben.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **Netzwerk** → **DDNS**.

Enable ☒

DDNS Type: DynDNS

Server Address:

Device Domain Name:

User Name:

Password:

Status: DDNS is disabled.

Save

Abbildung 4-2 DDNS

2. Schalten Sie **Enable** ein.
3. Wählen Sie einen DDNS-Typ.
4. Legen Sie die Parameter fest, einschließlich Dienstadresse, Domänenname usw.
5. Klicken Sie auf **Speichern**.

4.1.3 PPPoE konfigurieren

Wenn das Gerät über PPPoE mit dem Internet verbunden ist, müssen Sie den Benutzernamen und das Passwort entsprechend konfigurieren. Wenden Sie sich an Ihren Internetdienstanbieter, um Einzelheiten über den PPPoE-Dienst zu erfahren.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **Netzwerk** → **PPPoE**.

Enable ☒

User Name:

Password:

Save

Abbildung 4-3 PPPoE

2. Schalten Sie **Enable** ein.
3. Geben Sie den Benutzernamen und das Passwort ein.
4. Klicken Sie auf **Speichern**.

Was ist als nächstes zu tun?

Gehen Sie zu **System** → **Systemwartung** → **Laufende Info** → **Netzwerkstatus**, um den PPPoE-Status anzuzeigen.

4.1.4 Multicast konfigurieren

Multicast kann so konfiguriert werden, dass die Live-Ansicht für Kameras aktiviert wird, die die maximal zulässige Anzahl im Netzwerk überschreiten.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **Netzwerk** → **Andere**.
2. Stellen Sie die Multicast-Parameter ein.

Hinweis

- Wenn Sie ein Gerät über den Netzwerk-Video-Sicherheits-Client hinzufügen, sollte die IP-Adresse der Multicast-Gruppe mit der Multicast-IP-Adresse des Geräts übereinstimmen.
 - Für IPv4 deckt sie die IP-Klasse D von 224.0.0.0 bis 239.255.255.255 ab, und es wird empfohlen, eine IP-Adresse im Bereich von 239.252.0.0 bis 239.255.255.255 zu verwenden. Wenn Sie ein Gerät zur CMS-Software hinzufügen, muss die Multicast-Adresse mit der des Geräts übereinstimmen.
-

3. Klicken Sie auf **Speichern**.

4.2 Einstellungen für den Plattformzugang

4.2.1 SCMS konfigurieren

SCMS bietet eine Mobiltelefonanwendung und einen Plattformdienst für den Zugriff und die Verwaltung Ihres Videorekorders, der Ihnen einen bequemen Fernzugriff auf das Videosicherheitssystem ermöglicht.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **SCMS**.
2. Schalten Sie **"Aktivieren"** ein und die Servicebedingungen werden angezeigt.
3. Akzeptieren Sie die Servicebedingungen.
4. Klicken Sie auf  , um den Verifizierungscode festzulegen.
5. Optional: Aktivieren Sie **Stream Encryption**, **Sub-Stream Self-Adaptive Bitrate**, **Time Sync**, oder bearbeiten Sie die Server-IP-Adresse.

Stream-Verschlüsselung

Nachdem diese Funktion aktiviert wurde, ist die Eingabe eines Verifizierungscode im Fernzugriff und in der Live-Ansicht erforderlich.

Sub-Stream Selbstanpassende Bitrate

Wenn die Netzwerkumgebung schlecht ist, passt das Gerät die Videobitrate automatisch an, um eine flüssige Wiedergabe zu gewährleisten.

Zeitsynchronisation

Das Gerät synchronisiert die Zeit mit SCMS statt mit dem NTP-Server.

6. SCMS-App herunterladen. Sie können mit einem Smartphone den QR-Code scannen, um die SCMS-App herunterzuladen.
7. Verwenden Sie die SCMS-App, um den Geräte-QR zu scannen und das Gerät mit Ihrem SCMS-Konto zu verbinden.

Hinweis

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

8. Klicken Sie auf **Speichern**.

Ergebnis

- Wenn Ihr Gerät mit SCMS verbunden ist, lautet der **Verbindungsstatus Online**.
- Wenn Ihr Gerät mit einem SCMS-Konto verknüpft ist, wird der **Kontostatus "Verknüpft"** angezeigt.

Was ist als nächstes zu tun?

Sie können über SCMS auf Ihren Videorekorder zugreifen.

4.2.2 ISUP konfigurieren

ISUP (Intelligent Security Uplink Protocol) bietet APIs, Bibliotheksdateien und Befehle für die Plattform von Drittanbietern zum Zugriff auf Geräte wie NVRs, Speed Domes, DVRs, Netzwerkkameras, mobile NVRs, mobile Geräte, Dekodiergeräte usw. Mit diesem Protokoll kann die Drittanbieterplattform Funktionen wie Live-Ansicht, Wiedergabe, Zwei-Wege-Audio, PTZ-Steuerung usw. realisieren.

Schritte

1. Gehen Sie zu **System → CX → Systemeinstellungen → Netzwerk → Plattformzugang → ISUP**.

E-Mail	Plattformzugriff	Weitere Einstellungen	Protokollserver-Einstellungen
Zutrittstyp	ISUP		
Aktivieren	☒		
Serveradresse			
Serverport	7660		
Registrierungsstatus	Offline		
Geräte-ID	FA6699881		
Version	ISUP		
Verschlüsselungspasswort	*****		

Abbildung 4-5 ISUP

2. Schalten **Sie Aktivieren** ein.

Hinweis

Wenn ISUP aktiviert ist, wird der SCMS-Zugang automatisch deaktiviert.

3. Stellen Sie die entsprechenden Parameter ein.

Server-Adresse

Die IP-Adresse des Plattformservers.

Zugangsserver-Anschluss

Der Port des Plattformservers reicht von 1024 bis 65535. Der tatsächliche Port wird von der Plattform zur Verfügung gestellt.

Geräte-ID

Die Geräte-ID wird von der Plattform bereitgestellt.

Protokoll Version

ISUP-Protokollversion, nur ISUP 5.0 ist verfügbar.

Verschlüsselungsschlüssel

Das Verschlüsselungspasswort ist erforderlich, wenn Sie die Version ISUP V5.0 verwenden, da es eine sicherere Kommunikation zwischen dem Gerät und der Plattform ermöglicht. Geben Sie es zur Überprüfung ein, nachdem das Gerät bei der ISUP-Plattform registriert wurde. Es darf nicht leer oder "ABCDEF" sein.

4. Klicken Sie auf **Speichern**.

Sie können den Registrierungsstatus (online oder offline) nach dem Neustart des Geräts sehen.

4.2.3 SDK-Dienst konfigurieren

Der SDK-Dienst (Software Development Kit) wird von Drittanbietern zur Integration verschiedener Funktionen genutzt. Der erweiterte SDK-Dienst verwendet das TLS-Protokoll für den SDK-Dienst, das eine sicherere Datenübertragung ermöglicht.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **Plattformzugang** → **SDK**.

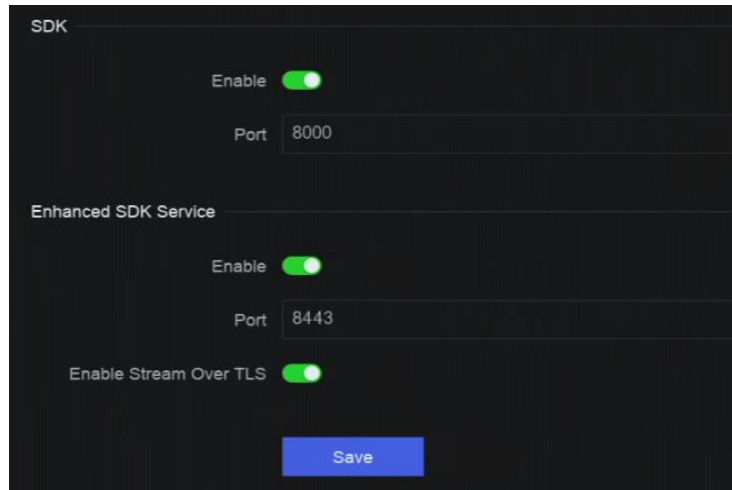


Abbildung 4-6 SDK-Dienst

2. Konfigurieren Sie **SDK** und **Enhanced SDK Service** entsprechend Ihren Anforderungen.

Hinweis

Der Port für den **Enhanced SDK Service** ist standardmäßig 8443.

3. Optional: Aktivieren Sie **Stream Over TLS**. Die Stream-over-TLS-Verschlüsselungstechnologie bietet einen sichereren Stream-Übertragungsdienst.
4. Klicken Sie auf **Speichern**.

4.2.4 ISAPI einschalten

ISAPI (Internet Server Application Programming Interface) ist ein offenes, auf HTTP basierendes Protokoll, das die Kommunikation zwischen den Systemgeräten (z.B. Netzwerkkamera, NVR, etc.) realisieren kann.

Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **Plattformzugriff** → **ISAPI**, um die Funktion zu aktivieren.

4.2.5 ONVIF konfigurieren

Das ONVIF-Protokoll ermöglicht die Verbindung mit Kameras von Drittanbietern. Die hinzugefügten Benutzerkonten haben die Berechtigung, andere Geräte über das ONVIF-Protokoll zu verbinden.

Schritte

1. Gehen Sie zu **Wartung** → **Systemwartung** → **ONVIF**.

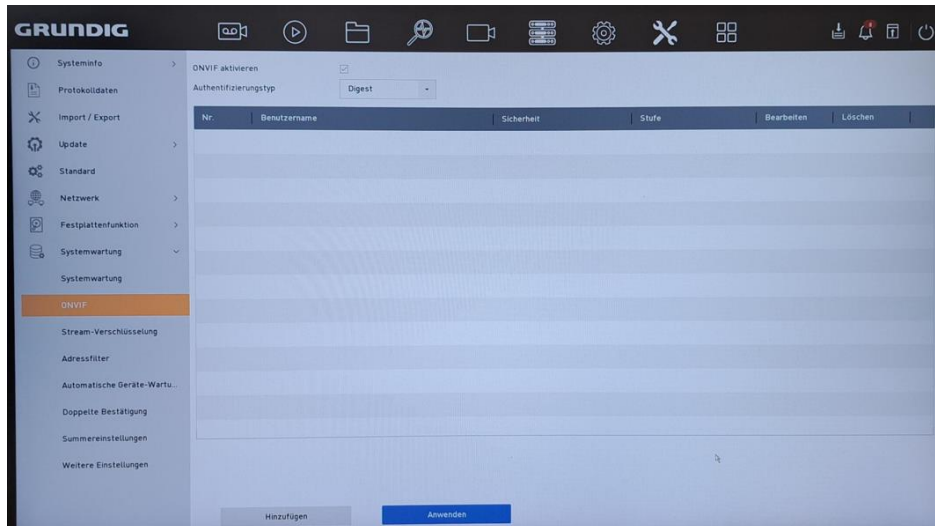


Abbildung 4-7 ONVIF

2. Schalten Sie **Enable** ein.
3. Wählen Sie eine Authentifizierungsart.
4. Klicken Sie auf **Hinzufügen**, um einen Benutzer hinzuzufügen.
5. Legen Sie den Benutzernamen und das Passwort fest.

Vorsicht

Wir empfehlen Ihnen dringend, ein sicheres Passwort Ihrer Wahl zu erstellen (mit mindestens 8 Zeichen, darunter mindestens drei der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zurückzusetzen, vor allem im Hochsicherheitssystem kann das monatliche oder wöchentliche Zurücksetzen des Passworts Ihr Produkt besser schützen.

6. Klicken Sie auf **Speichern**.

4.2.6 Log-Server konfigurieren

Die Protokolle können zur Sicherung auf den Protokollserver hochgeladen werden.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **Plattformzugriff** → **Protokollserver**.

Abbildung 4-8 Protokollserver

2. Klicken Sie **auf Anwenden**.
3. Legen Sie das **Zeitintervall für den Upload**, die **IP-Adresse des Servers** und den **Port** fest.
4. Optional: Klicken Sie auf **Test**, um zu prüfen, ob die Parameter gültig sind.
5. Klicken Sie auf **Speichern**.

4.3 Netzwerkdienst-Einstellungen

4.3.1 HTTP(S) konfigurieren

HTTP- ((Hyper Text Transfer Protocol) und HTTPS- (Hypertext Transfer Protocol Secure) Ports werden für den Fernzugriff über den Webbrowser verwendet. Das HTTPS-Protokoll ermöglicht eine verschlüsselte Übertragung und Identitätsauthentifizierung, was die Sicherheit des Fernzugriffs verbessert.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **Netzwerkdienst** → **HTTP(S)**.

Abbildung 4-9 HTTP(S)

2. Optional: Aktivieren Sie HTTP oder HTTPS.
3. **Port** von HTTP oder HTTPS anzeigen oder bearbeiten.
4. **HTTP/HTTPS-Authentifizierung** einstellen.

Art der Authentifizierung

Es stehen zwei Authentifizierungsarten zur Auswahl. Aus Sicherheitsgründen wird empfohlen, **Digest** als Authentifizierungsart zu wählen.

Verdauungsalgorithmus

Digest-Algorithmen basieren auf HTTP/HTTPS und werden hauptsächlich für die Digest-Authentifizierung der Benutzerauthentifizierung verwendet.

5. Klicken Sie auf **Speichern**.

4.3.2 RTSP konfigurieren

RTSP (Real Time Streaming Protocol) ist ein Netzwerksteuerungsprotokoll, das für die Steuerung von Streaming-Medienservern entwickelt wurde. Sie können die Streaming-Daten der Live-Ansicht besonders schützen, indem Sie die RTSP-Authentifizierung einstellen.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **Netzwerkdienst** → **RTSP**.

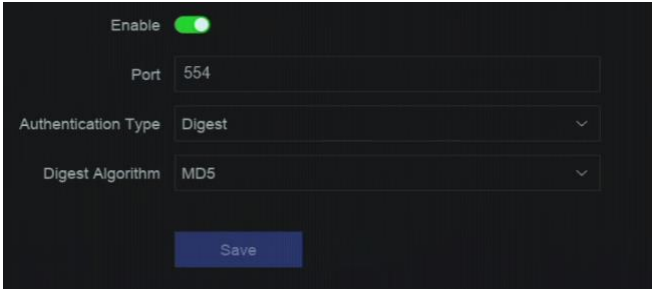


Abbildung 4-10 RTSP

2. Parameter einstellen.

Hafen

Der Port ist standardmäßig 554.

Art der Authentifizierung

Wenn Sie **Digest** auswählen, kann nur die Anfrage mit Digest-Authentifizierung über die IP-Adresse auf den Videostream per RTSP zugreifen. Aus Sicherheitsgründen wird empfohlen, **Digest** als Authentifizierungsart zu wählen.

RTSP-Verschlüsselungsalgorithmus

Der RTSP-Digest-Algorithmus basiert auf RTSP, es handelt sich um einen Algorithmus zur Digest-Authentifizierung der Benutzerauthentifizierung.

3. Klicken Sie auf **Speichern**.

4.3.3 WebSocket(s) konfigurieren

Das auf TCP basierende WebSocket-Protokoll zielt darauf ab, eine Vollduplex-Kommunikation zwischen Webbrowsern und Servern zu ermöglichen. Es ermöglicht die Eröffnung einer interaktiven Zwei-Wege-Kommunikationssitzung.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Netzwerk** → **Netzwerkdienst** → **WebSocket(s)**.
2. Schalten Sie **Enable** ein.
3. **Anschluss** einstellen.
4. Klicken Sie auf **Speichern**.

4.3.4 Port-Zuordnung konfigurieren (NAT)

Für das Port-Mapping stehen zwei Möglichkeiten zur Verfügung, um den Fernzugriff über das segmentübergreifende Netzwerk zu realisieren: UPnP™ (Universal Plug and Play) und manuelles Mapping. Mit UPnP™ kann das Gerät nahtlos die Anwesenheit anderer Netzwerkgeräte im Netzwerk erkennen und funktionale Netzwerkdienste für die gemeinsame Nutzung von Daten, Kommunikation usw. einrichten. Sie können die UPnP™-Funktion verwenden, um eine schnelle Verbindung des Geräts mit dem WAN über einen Router ohne Port-Zuordnung zu ermöglichen.

Bevor Sie beginnen

Wenn Sie die UPnP™-Funktion des Geräts aktivieren möchten, müssen Sie die UPnP™-Funktion des Routers, an den Ihr Gerät angeschlossen ist, aktivieren. Wenn der Netzwerkarbeitsmodus des Geräts auf mehrere Adressen eingestellt ist, sollte sich die Standardroute des Geräts im selben Netzwerksegment befinden wie die LAN-IP-Adresse des Routers.

Schritte

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

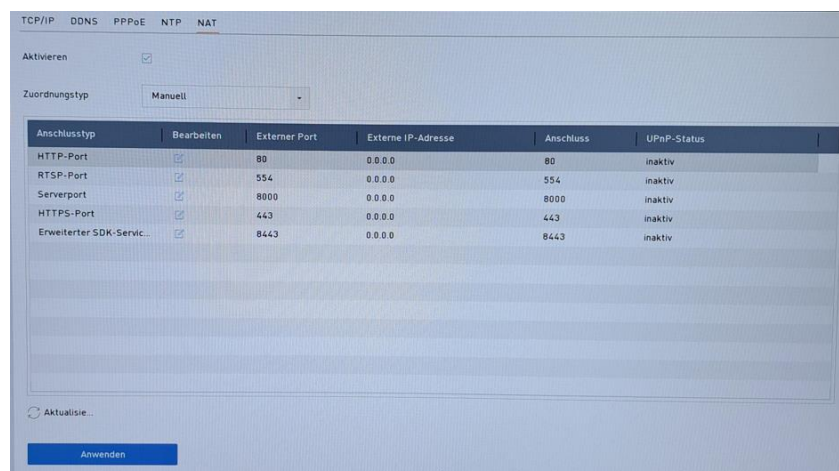


Abbildung 4-11 Port-Zuordnung (NAT)

2. Schalten Sie **Enable** ein.
3. **Mapping-Modus** einstellen.

Auto

Die Portzuordnungselemente sind schreibgeschützt, und die externen Ports werden vom Router automatisch eingestellt.

Manuell

Sie können den externen Anschluss manuell bearbeiten.

4. Wenn **der Zuordnungsmodus** auf **Manuell** eingestellt ist, klicken Sie auf  , um die entsprechenden Anschlüsse zu bearbeiten.
-

Hinweis

- Der Wert der RTSP-Portnummer sollte 554 oder zwischen 1024 und 65535 liegen, während der Wert der anderen Ports zwischen 1 und 65535 liegen sollte und sich voneinander unterscheiden muss. Wenn mehrere Geräte für die UPnP™-Einstellungen unter demselben Router konfiguriert sind, sollte der Wert der Portnummer für jedes Gerät eindeutig sein.
 - **Externer Port** gibt die interne Portnummer für die Portzuordnung im Router an.
-

5. Klicken Sie auf **Speichern**.

Rufen Sie die Seite mit den Einstellungen für den virtuellen Server des Routers auf, und geben Sie den Wert für den internen/externen Quellport und andere erforderliche Inhalte ein.

5 Benutzerverwaltung

Es gibt ein Standardkonto für den Administrator. Der Administrator-Benutzername lautet **admin**. Der Administrator hat die Berechtigung, Benutzer hinzuzufügen, zu löschen und zu bearbeiten. Gast- und Operator-Benutzer haben nur eingeschränkte Berechtigungen. Gehen Sie zu **System** → **Systemeinstellungen** → **Benutzerverwaltung**.

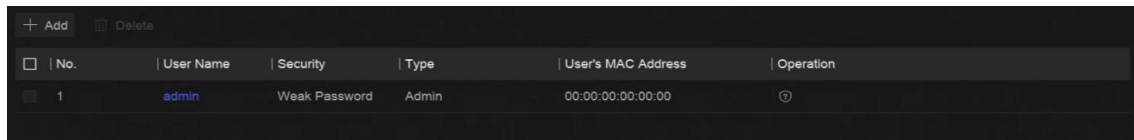


Abbildung 5-1 Benutzerverwaltung

Tabelle 5-1 Symbol/Taste Beschreibung

Ikone/Schaltfläche	Beschreibung
	Kontosicherheit einstellen.
hinzufügen	Fügen Sie einen neuen Gast- oder Betreiberbenutzer hinzu.
	Löscht den ausgewählten Benutzer.

Hinweis

Vor der Inbetriebnahme müssen Sie das Admin-Passwort bestätigen.

6 Gerätezugriff

Der Videorecorder kann möglicherweise auf mehrere Gerätetypen zugreifen, z. B. auf eine Netzwerkkamera, ein Zugangskontrollgerät und ein Alarmgerät. Die Zugriffsmöglichkeiten Ihres Videorekorders entnehmen Sie bitte dem jeweiligen Gerät.

6.1 Zugang zum Videogerät

Es gibt mehrere Möglichkeiten, auf ein Videogerät zuzugreifen.

6.1.1 Automatisch gesuchte Online-Netzwerkkamera hinzufügen

Netzwerkkameras im selben Netzwerksegment können automatisch gesucht und dem Gerät hinzugefügt werden.

Schritte

1. Gehen Sie zu **System** → **Gerätezugriff** → **Gerät** → **Videogerät** → **Online-Geräteliste**.
2. Wählen Sie das/die Gerät(e) aus der Liste aus.

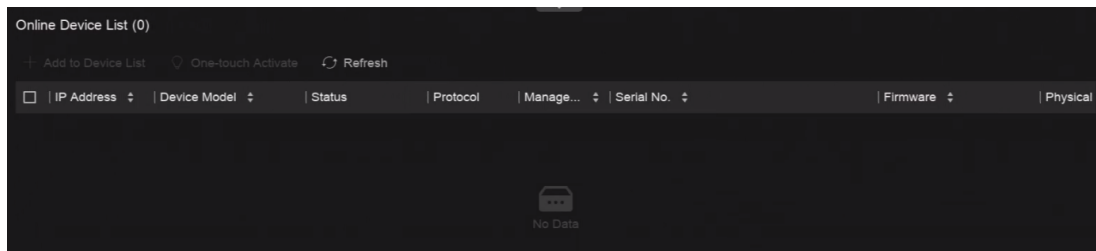


Abbildung 6-1 Automatisch gesuchte Online-Netzwerkkamera hinzufügen

3. Klicken Sie auf **Zur Geräteliste hinzufügen**.

Hinweis

- Das Gerät verwendet ein Standardkennwort, um Netzwerkkameras hinzuzufügen. Stellen Sie sicher, dass das Kamerakennwort mit dem Standardkennwort übereinstimmt.
- Wenn die hinzuzufügende Netzwerkkamera noch nicht aktiviert ist, können Sie sie in der Netzwerkkameraliste der Kameraverwaltungsoberfläche aktivieren.
- Wenn eine Netzwerkkamera erfolgreich hinzugefügt wurde, lautet ihr Status **Online**.
- Sie können auf den Gerätenamen klicken, um seine Parameter hinzuzufügen.

6.1.2 Netzwerkkamera manuell hinzufügen

Fügen Sie die Netzwerkkameras manuell zu Ihrem Videorecorder hinzu.

Bevor Sie beginnen

- Vergewissern Sie sich, dass sich Ihre Netzwerkkamera im selben Netzwerksegment befindet wie Ihr Videorecorder.
 - Stellen Sie sicher, dass die Netzwerkverbindung gültig und korrekt ist.
- Stellen Sie sicher, dass die Netzwerkkamera aktiviert ist.

Schritte

1. Gehen Sie zu **System → Gerätezugriff → Gerät → Videogerät**.

Abbildung 6-2 Manuelles Hinzufügen einer Netzwerkkamera

2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie die Parameter der Netzwerkkamera ein.

Kanal-Standardpasswort verwenden

Wenn sie aktiviert ist, fügt der Videorecorder die Kamera mit dem eingestellten Standardpasswort des Kanals hinzu.

Mehr Einstellungen

Sie können die Option **Zertifikat verifizieren** aktivieren, um die Kamera mit einem Zertifikat zu verifizieren. Das Zertifikat ist eine Form der Identifizierung für die Kamera, die eine sicherere Kameraauthentifizierung ermöglicht. Wenn Sie diese Funktion verwenden, müssen Sie zunächst das Zertifikat der Netzwerkkamera in das Gerät importieren.

4. Optional: Klicken Sie auf **Weiter zum Hinzufügen**, um weitere Netzwerkkameras hinzuzufügen.
5. Klicken Sie auf **Hinzufügen**.

6.1.3 Netzwerkkamera über benutzerdefiniertes Protokoll hinzufügen

Für Netzwerk-Kameras, die keine Standardprotokolle verwenden, können Sie benutzerdefinierte Protokolle konfigurieren, um sie hinzuzufügen. Das System bietet 8 benutzerdefinierte Protokolle.

Bevor Sie beginnen

- Stellen Sie sicher, dass die Netzwerkkamera RTSP-Streaming unterstützt.
- Bereiten Sie die URL (Uniform Resource Locator) für den Abruf des Haupt- oder Substreams der Netzwerkkameras vor.

Schritte

1. Gehen Sie zu **System** → **Gerätezugriff** → **Gerät** → **Videogerät**.
2. Klicken Sie auf **Mehr** → **Benutzerdefinierte Protokollverwaltung**, oder auf **Hinzufügen** → **Protokollverwaltung**.

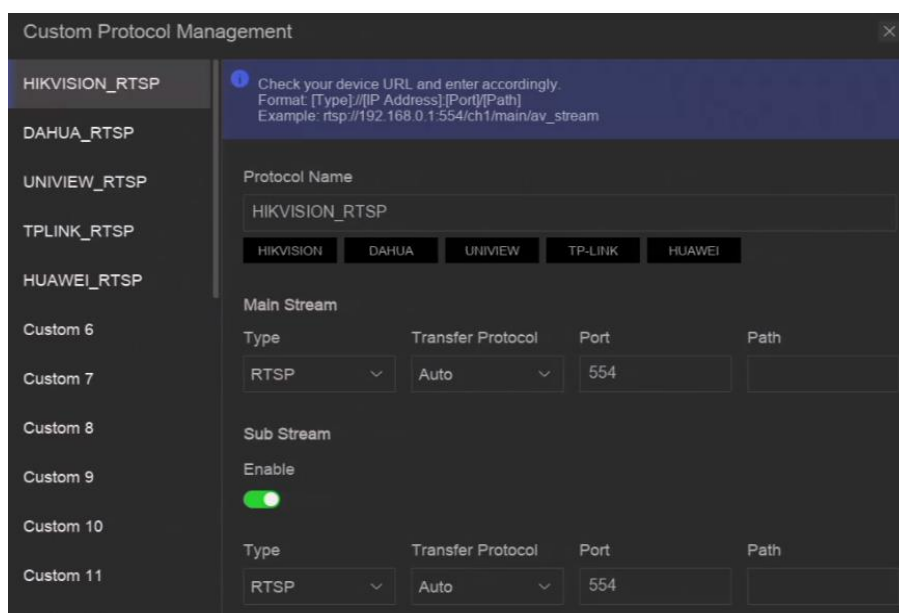


Abbildung 6-3 Netzwerkkamera über benutzerdefiniertes Protokoll hinzufügen

3. Wählen Sie auf der linken Seite einen Protokolltyp aus.
4. Protokollparameter einstellen.

Typ

Die Netzwerk-Kamera, die das benutzerdefinierte Protokoll verwendet, muss die Übertragung von Streams über den Standard RTSP unterstützen.

Übertragungsprotokoll

Es stehen 3 Typen zur Auswahl, darunter **Auto**, **UDP** und **RTP über RTSP**.

Port

Der Port für das RTSP-Streaming. Der Standardwert ist 554.

Pfad

Wenden Sie sich an den Hersteller der Netzwerkkamera, um die URL für den Abruf von Main Stream und Sub-Stream zu erfahren. Das allgemeine Format ist *[Typ]://[IP-Adresse]:[Port]/[Ressourcenpfad]*, zum Beispiel *rtsp://192.168.0.1:554/ch1/main/av_stream*.

Hinweis

- **Protokollname** und **Pfad** können automatisch generiert werden, wenn Sie auf einen Markennamen unter **Protokollname** klicken.

Sie können Sub-Stream deaktivieren, wenn die Kamera Sub-Stream nicht unterstützt oder den Sub-Stream nicht verwenden muss.

5. Klicken Sie auf **OK**.

6. Klicken Sie unter **System** → **Gerätezugriff** → **Gerät** → **Videogerät** auf **Hinzufügen**, um eine Netzwerkkamera manuell hinzuzufügen.

6.1.4 Hinzufügen einer Netzwerkkamera über die Kamerakonfigurationsdatei

Die Informationen der hinzugefügten Netzwerkkameras können exportiert werden, einschließlich der IP-Adresse, des Ports, des Passworts des Administrators usw. Und der Inhalt der exportierten Kamerakonfigurationsdatei kann auf Ihrem Computer bearbeitet werden. Nach der Bearbeitung kann die Datei auch in andere Geräte importiert werden, um die Kameras in der Datei hinzuzufügen.

Bevor Sie beginnen

Schließen Sie Ihren Videorekorder an ein USB-Flash-Laufwerk an, auf dem sich die Konfigurationsdatei der Kamera befindet.

Schritte

1. Gehen Sie zu **System** → **Gerätezugriff** → **Gerät** → **Videogerät**.
2. Klicken Sie auf **Importieren**, um die Konfigurationsdatei auf dem USB-Stick zu importieren.
3. Legen Sie den Ordnerpfad fest.
4. Klicken Sie auf **Bestätigen**.

6.2 Zugangskontrollgerät hinzufügen

Zugangskontrollgeräte können zu Ihrem Videorekorder hinzugefügt werden. Der Vorgang des Hinzufügens ist bei **Access Video Device** ähnlich.

6.3 Audiogerät hinzufügen

Audiogeräte können zu Ihrem Videorekorder hinzugefügt werden. Der Vorgang des Hinzufügens ist bei **Access Video Device** ähnlich.

6.4 POS-Gerät hinzufügen

Bei bestimmten Gerätemodellen kann ein POS-Gerät/Server angeschlossen werden. Das Gerät kann Transaktionsmeldungen von der POS-Maschine/vom POS-Server empfangen, Transaktionsmeldungen auf dem Videobild einblenden und POS-Ereignisalarme auslösen.

Schritte

1. Gehen Sie zu **System** → **Gerätezugriff** → **Gerät** → **POS**.
2. Klicken Sie auf **Hinzufügen**, um ein POS-Gerät hinzuzufügen.

Abbildung 6-4 POS-Gerät hinzufügen

3. Stellen Sie die Parameter des POS-Geräts ein.

POS-Protokoll

Universelles Protokoll

Sie können die Startzeilenkennung, die Zeilenumbruchskennung und die Endzeilenkennung für die POS-Overlay-Zeichen sowie die Groß- und Kleinschreibung der Zeichen festlegen. Optional können Sie auch den Filterbezeichner und das XML-Protokoll überprüfen.

EPSON

Für das EPSON-Protokoll werden die festen Anfangs- und Endzeilenkennzeichnungen verwendet.

AVE

Für das AVE-Protokoll werden die festen Anfangs- und Endzeilen verwendet. Es werden die Verbindungsarten serieller Anschluss und virtueller serieller Anschluss unterstützt.

NUCLEUS

Für das AVE-Protokoll werden die festen Anfangs- und Endzeilen verwendet. Es werden die Verbindungsarten serieller Anschluss und virtueller serieller Anschluss unterstützt. Für die RS-232-Verbindungskommunikation muss das NUCLEUS-Protokoll verwendet werden.

Verbindungsmodus

TCP-Verbindung

Bei Verwendung einer TCP-Verbindung muss der Port zwischen 1 und 65535 eingestellt werden, und der Port muss für jedes POS-Gerät eindeutig sein.

UDP-Verbindung

Bei Verwendung einer UDP-Verbindung muss der Port zwischen 1 und 65535 eingestellt werden, und der Port muss für jedes POS-Gerät eindeutig sein.

USB-zu-RS-232-Verbindung

Konfigurieren Sie die Anschlussparameter des USB-zu-RS-232-Konverters, einschließlich der seriellen Anschlussnummer, der Baudrate, des Datenbits, des Stopbits und der Parität.

RS-232-Anschluss

Verbinden Sie das Gerät und das Kassensystem über RS-232.

Multicast-Verbindung

Wenn Sie das Gerät und das Kassensystem über das Multicast-Protokoll verbinden, stellen Sie die Multicast-Adresse und den Port ein.

Sniff-Verbindung

Verbinden Sie das Gerät und das Kassensystem über Sniff. Konfigurieren Sie die Einstellungen für die Quell- und Zieladresse.

4. Klicken Sie auf **Hinzufügen.**

Hinweis

Nachdem ein POS-Gerät hinzugefügt wurde, können Sie auf  klicken, um das POS-Text-Overlay zu konfigurieren.

7 Kameraeinstellungen

Sie können die hinzugefügte Kamera konfigurieren, z. B. Datenschutzmaske, Bildparameter usw.

7.1 Aktivieren des H.265-Stream-Zugriffs

Das Gerät kann beim ersten Zugriff automatisch auf den H.265-Stream der IP-Kamera (die das H.265-Videoformat unterstützt) umschalten.

Schritte

1. Gehen Sie zu **System** → **Gerätezugriff** → **Gerät** → **Videogerät**.
2. Klicken Sie auf **Mehr** → **Automatischer Wechsel zu H.265**.
3. Aktivieren Sie diese Funktion.
4. Klicken Sie auf **Speichern**.

7.2 Batch-Konfiguration

Kameras können in einem Stapel konfiguriert werden.

Schritte

1. Gehen Sie zu **System** → **Gerätezugriff** → **Gerätekonfiguration** → **Batch-Konfiguration**.

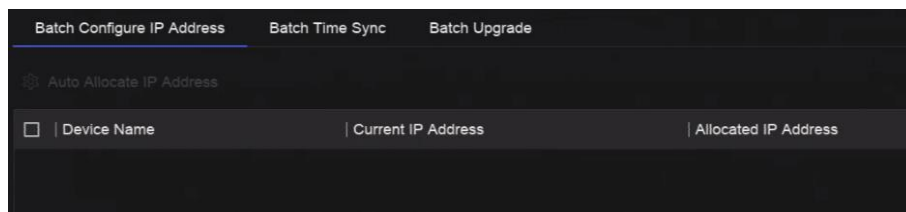


Abbildung 7-1 Batch-Konfiguration

2. Konfigurieren Sie die IP-Adresse, synchronisieren Sie die Zeit, oder aktualisieren Sie die Firmware nach Wunsch.
3. Klicken Sie für die Konfiguration der IP-Adresse und die Zeitsynchronisation auf **Speichern**.

7.3 Anzeigeeinstellungen

Konfigurieren Sie das OSD (On-Screen-Display), die Bildeinstellungen, die Belichtungseinstellungen, die Einstellungen für den Tag/Nacht-Schalter usw.

Gehen Sie zu **System** → **Gerätezugriff** → **Gerätekonfiguration** → **Geräteparameter** → **Anzeigeeinstellungen**. Wählen Sie eine Kamera aus, und konfigurieren Sie die Parameter nach Ihren Wünschen.

OSD-Einstellungen

Konfigurieren Sie die OSD-Einstellungen (On-Screen-Display) für die Kamera, einschließlich Datum/Uhrzeit, Kameraname usw.

Bildeinstellungen

Passen Sie die Bildparameter wie Helligkeit, Kontrast und Sättigung für die Live-Ansicht und den Aufnahmeeffekt an.

Exposition

Stellen Sie die Belichtungszeit der Kamera ein (1/10000 bis 1 Sekunde). Ein größerer Belichtungswert ergibt ein helleres Bild.

Tag/Nacht-Schalter

Die Kamera kann je nach Beleuchtungsbedingungen auf Tag-, Nacht- oder Automatikmodus eingestellt werden.

Hintergrundbeleuchtung

Stellen Sie den großen Dynamikbereich der Kamera ein (0 bis 100). Wenn die Umgebungsbeleuchtung und das Objekt große Helligkeitsunterschiede aufweisen, sollten Sie den WDR-Wert einstellen.

Bildverbesserung

Für eine optimierte Bildkontrastverbesserung.

7.4 Konfigurieren der Videoparameter

Die Videoparameter wirken sich auf das Livebild und die Aufzeichnungsdatei aus.

Gehen Sie zu **System** → **Gerätezugriff** → **Gerätekonfiguration** → **Geräteparameter** → **Videoparameter**. Wählen Sie eine Kamera aus, und konfigurieren Sie die Parameter nach Ihren Wünschen.

Hauptstrom

Der Hauptstrom ist der primäre Strom, der die auf der Festplatte aufgezeichneten Daten beeinflusst und direkt die Videoqualität und Bildgröße bestimmt. Im Vergleich zum Sub-Stream bietet der Haupt-Stream eine höhere Videoqualität mit höherer Auflösung und Bildrate.

Sub-Stream

Sub-Stream ist ein zweiter Codec, der neben dem Mainstream läuft. Er ermöglicht es Ihnen, die ausgehende Internet-Bandbreite zu reduzieren, ohne die Qualität der direkten Aufnahme zu beeinträchtigen. Sub-Stream wird oft ausschließlich von Smartphone-Anwendungen verwendet, um Live-Videos anzuzeigen. Benutzer mit begrenzten Internetgeschwindigkeiten profitieren am meisten von dieser Einstellung.

Auflösung

Die Bildauflösung ist ein Maß dafür, wie viele Details ein digitales Bild enthalten kann. Je höher die Auflösung, desto größer ist die Detailtreue. Die Auflösung kann als die Anzahl der

Pixelspalten (Breite) mal die Anzahl der Pixelzeilen (Höhe) angegeben werden, z. B. 1024 × 768.

Bitrate Typ

Die Bitrate (in kbit/s oder Mbit/s) wird oft als Geschwindigkeit bezeichnet, definiert aber eigentlich die Anzahl der Bits/Zeiteinheit und nicht die Entfernung/Zeiteinheit. Es stehen zwei Typen zur Verfügung: variabel und konstant.

Bildfrequenz

Sie bezieht sich auf die Anzahl der Bilder, die pro Sekunde aufgenommen werden. Eine höhere Bildrate ist vorteilhaft, wenn der Videostrom in Bewegung ist, da so die Bildqualität durchgehend erhalten bleibt.

I-Frame Intervall

I-Frame wird auch als Intra-Bild bezeichnet und ist das erste Bild jeder GOP (eine Videokomprimierungstechnologie von MPEG). Es kann nach der Komprimierung als Bild betrachtet werden. Das I-Frame-Intervall ist die Anzahl der Bilder zwischen zwei aufeinanderfolgenden I-Frames.

7.5 Privatzone konfigurieren

Die Privatsphärenmaske schützt die persönliche Privatsphäre, indem sie Teile des Bildes vor der Live-Ansicht oder der Aufzeichnung mit einem maskierten Bereich verdeckt.

Schritte

1. Gehen Sie zu **Kamera → Kamera → Privatzone**.

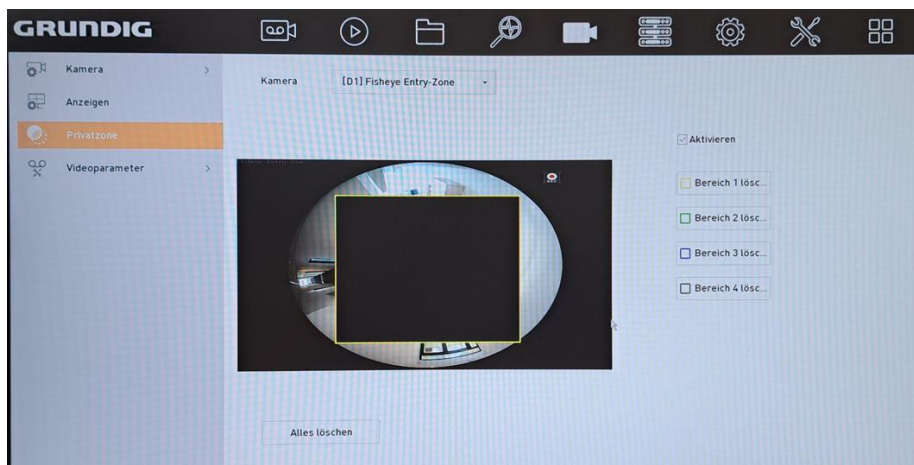


Abbildung 7-2 Privatzone

2. Wählen Sie eine Kamera aus.
3. Klicken Sie auf **Aktivieren**.
4. Zeichnen Sie Maskenbereiche im Vorschaufenster. Die Bereiche werden mit verschiedenen Rahmenfarben markiert.

Hinweis

Es können bis zu 4 Sichtschutzbereiche konfiguriert werden und die Größe jedes Bereichs kann angepasst werden.

5. Klicken Sie auf **Anwenden**.

8 Gerätegruppierung

Die hinzugefügten Geräte können in verschiedene kundenspezifische Gruppen eingeteilt werden.

Schritte

1. Gehen Sie zu **System** → **Gerätezugriff** → **Gerätegruppierung**.

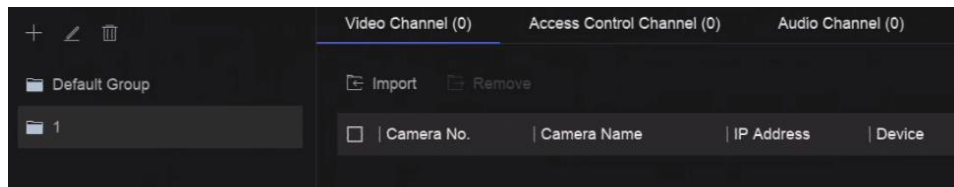


Abbildung 8-1 Gerätegruppierung

2. Klicken Sie auf **+** , um eine Gruppe hinzuzufügen.

Hinweis

Nachdem eine Gruppe hinzugefügt wurde, können Sie auf **/** **✎** **🗑** klicken, um sie zu bearbeiten/löschen.

3. Klicken Sie auf **Importieren**, um der ausgewählten Gruppe einen oder mehrere Kanäle hinzuzufügen.

9 Speicherverwaltung

9.1 HDD verwalten

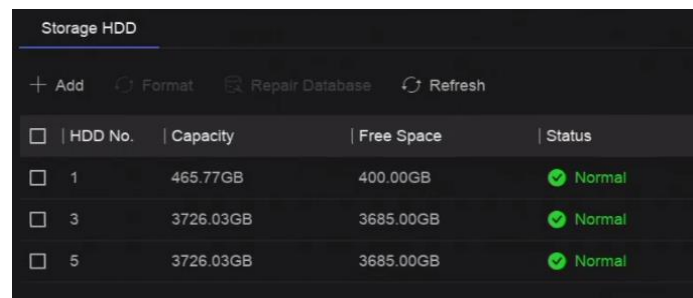
Ein neu installiertes Festplattenlaufwerk (HDD) muss vor der Verwendung initialisiert werden. Sie können die Festplatte formatieren, die Datenbank reparieren und den Festplattenstatus über die Festplattenverwaltungsschnittstelle anzeigen.

Bevor Sie beginnen

Vergewissern Sie sich, dass die Festplatte ordnungsgemäß in Ihrem Gerät installiert ist.

Schritte

1. Gehen Sie zu **System** → **Speicherverwaltung** → **Speicherfestplatte** → **Speicherfestplatte**.



Storage HDD				
+ Add Format Repair Database Refresh				
☐	HDD No.	Capacity	Free Space	Status
☐	1	465.77GB	400.00GB	✓ Normal
☐	3	3726.03GB	3685.00GB	✓ Normal
☐	5	3726.03GB	3685.00GB	✓ Normal

Abbildung 9-1 HDD verwalten

2. Optional: Führen Sie die folgenden Vorgänge nach Belieben aus.

hinzufügen

Fügen Sie eine Netzwerkfestplatte hinzu.

Format

Formatieren Sie die ausgewählte HDD.

Datenbank reparieren

Beim Reparieren der Datenbank werden alle Datenbanken wiederhergestellt. Dies kann helfen, die Systemgeschwindigkeit nach dem Upgrade zu verbessern.

Hinweis

- Bei der Reparatur der Datenbank werden alle Datenbanken neu erstellt. Vorhandene Daten werden nicht beeinträchtigt, aber die lokalen Such- und Wiedergabefunktionen sind während des Prozesses nicht verfügbar. Sie können jedoch weiterhin Such- und Wiedergabefunktionen aus der Ferne über einen Webbrowser, eine Client-Software usw. erreichen.
 - Ziehen Sie das Laufwerk nicht heraus, und schalten Sie das Gerät während des Vorgangs nicht aus.
-



HDD entfernen/einlegen.

9.2 RAID-Konfiguration

Ein Festplatten-Array ist eine Technologie zur Virtualisierung der Datenspeicherung, bei der mehrere physische Festplatten zu einer einzigen logischen Einheit zusammengefasst werden. Ein Array wird auch als "RAID" bezeichnet und speichert Daten auf mehreren Festplatten, um eine ausreichende Redundanz zu gewährleisten, so dass Daten wiederhergestellt werden können, wenn eine Festplatte ausfällt. Die Daten werden je nach der erforderlichen Redundanz und Leistung auf verschiedene Arten auf die Laufwerke verteilt, die als "RAID-Level" bezeichnet werden.

Vorsicht

RAID erfordert Festplatten der Enterprise-Klasse.

Die Funktionen in diesem Abschnitt sind nur für GD-RN-DT8864N verfügbar. Es wird empfohlen, Festplatten desselben Modells und derselben Kapazität zu verwenden.

Es gibt zwei Möglichkeiten, RAID zu erstellen. Bei der Erstellung per Knopfdruck ist der Standard-RAID-Typ RAID5. Für die manuelle Erstellung können RAID0, RAID1, RAID5, RAID6 und RAID10 konfiguriert werden.

Tabelle 9-1 Festplattenanforderung für jeden RAID-Typ

RAID-Typ	Erforderliche Anzahl von HDDs
RAID0	≥ 2
RAID1	2
RAID5	≥ 3
RAID6	≥ 4
RAID10	4 oder 8

Hinweis

- Die Funktion ist nur bei bestimmten Modellen verfügbar.
- Wenn ein Array-Ausnahmeereignis auftritt, können die entsprechenden Verknüpfungsaktionen unter **System** → **Systemeinstellungen** → **Ausnahme** konfiguriert werden.

9.2.1 Festplatten-Array erstellen

Ein Festplatten-Array kann nach Aktivierung des Array-Modus erstellt werden.

Bevor Sie beginnen

- Der **Speichermodus** ist unter **System** → **Speicherverwaltung** → **Speichermodus** auf **Kontingent** eingestellt.
- Genügend Festplatten sind korrekt im Gerät installiert. Und die Festplatten für die Array-Erstellung sind AI- oder Enterprise-Level.

Schritte

1. Gehen Sie zu **System** → **Speicherverwaltung** → **Speicherfestplatte** → **Array-Verwaltung**.
2. Klicken Sie auf **Array-Modus aktivieren**, oder aktivieren Sie den **Array-Modus**.

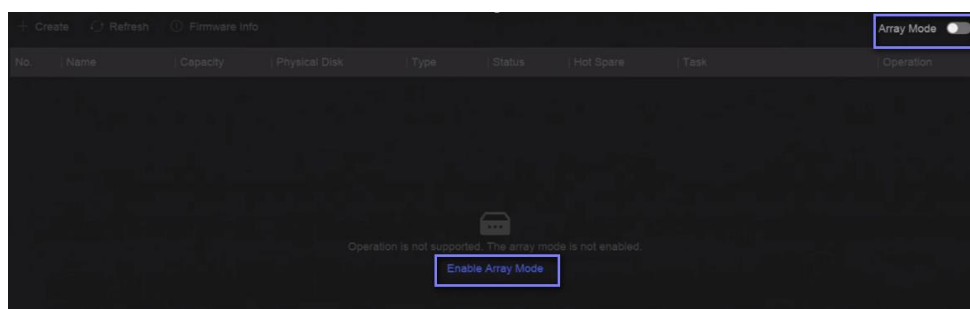


Abbildung 9-2 RAID aktivieren

3. Warten Sie auf den Neustart des Geräts.
4. Gehen Sie erneut zu **System** → **Speicherverwaltung** → **Speicherfestplatte** → **Array-Verwaltung**.

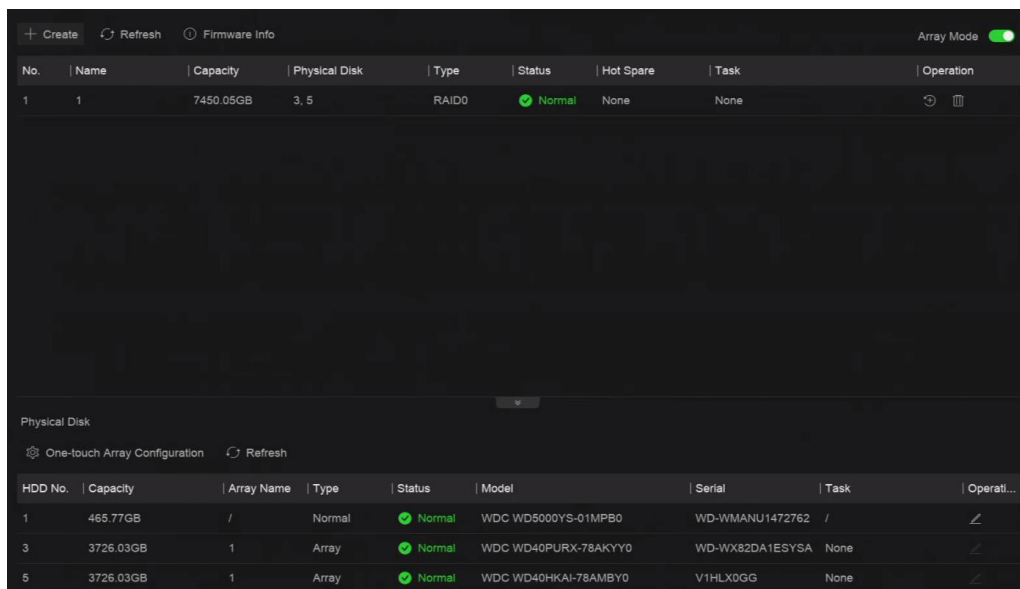


Abbildung 9-3 Array-Verwaltung

5. Erstellen Sie ein Array.

Erstellungsmethode **Beschreibung**

Array-Konfiguration mit einem Tastendruck	Klicken Sie auf One-Touch-Array-Konfiguration. Hinweis Standardmäßig ist der durch die One-Touch-Konfiguration erstellte Array-Typ RAID 5.
Manuelle Erstellung	Klicken Sie auf Erstellen, um manuell ein RAID 0-, RAID 1-, RAID 5-, RAID 6- oder RAID 10-Array zu erstellen.

9.2.2 Array wiederherstellen

Der Array-Status umfasst **Functional**, **Degraded** und **Offline**. Um die hohe Sicherheit und Zuverlässigkeit der in einem Array gespeicherten Daten zu gewährleisten, sollten Sie die Arrays entsprechend ihrem Status sofort und ordnungsgemäß warten.

Schritte

1. Gehen Sie zu **System** → **Speicherverwaltung** → **Speicherfestplatte** → **Array-Verwaltung**.
2. Bauen Sie ein Array neu auf.

Tabelle 9-2 Wiederherstellungsmethode

Wiederherstellungsmethode	Beschreibung
Autoumatische Wiederherstellung	Es sollte eine Hot-Spare-Platte im Array vorhanden sein, und die Kapazität der Hot-Spare-Platte darf nicht geringer sein als die der Platte mit der Mindestkapazität im Array. Klicken Sie auf  in der Spalte "Operation" unter "Physikalische Festplatte", um eine Hot-Spare-Festplatte festzulegen. Wenn eine Festplatte im Array nicht funktioniert, wird die Hot-Spare-Platte aktiviert und das Array automatisch wiederhergestellt. Hinweis Nachdem die automatische Wiederherstellung abgeschlossen ist, wird empfohlen, eine andere Festplatte zu installieren und diese als Hot-Spare-Festplatte zu konfigurieren.

Wiederherstellungsmethode	Beschreibung
Manuelle Wiederherstellung	Wenn keine Hot-Spare-Platten im Array vorhanden sind, müssen Sie das Array manuell neu aufbauen. Gehen Sie zu System → Speicherverwaltung → Speicherfestplatte → Array-Verwaltung und wählen Sie die Hot-Spare-Platte in der Liste aus, die Sie wiederherstellen möchten.

9.2.3 Array löschen

Gehen Sie zu **System** → **Storage Management** → **Storage HDD** und klicken Sie auf , um das ausgewählte Array zu löschen.

9.2.4 Firmware-Informationen anzeigen

Sie können Array-Firmware-Informationen anzeigen und die Geschwindigkeit der Hintergrundaufgaben einstellen.

Bevor Sie beginnen

Stellen Sie sicher, dass das Disk-Array aktiviert ist.

Schritte

1. Gehen Sie zu **System** → **Speicherverwaltung** → **Speicherfestplatte** → **Array-Verwaltung**.
2. Klicken Sie auf **Firmware-Info**.
3. Optional: **Zurücksetzen der Grundgeschwindigkeit der Aufgabe**.

9.3 Speichermodus konfigurieren

Schritte

1. Gehen Sie zu **System** → **Speicherverwaltung** → **Speichermodus**.

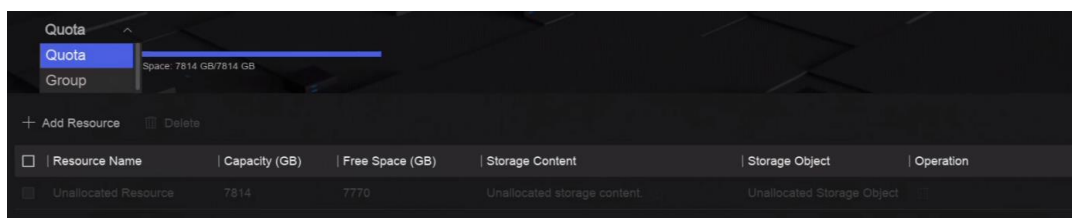


Abbildung 9-4 Speichermodus

2. Wählen Sie **Kontingent** oder **Gruppe**.

Kontingent

Jede Kamera oder jedes Audiogerät kann mit einem zugewiesenen Kontingent für die Speicherung von Videos, Bildern oder Audios konfiguriert werden.

Gruppe

Mehrere HDDs können in Gruppen verwaltet werden. Über die Festplatteneinstellungen können Videos von bestimmten Kanälen auf einer bestimmten Festplattengruppe aufgezeichnet werden.

3. Stellen Sie die entsprechenden Parameter ein.

- **Kontingent:** Zuweisung von Speicherplatz für Speicherobjekte.
- **Gruppe:** Verknüpfen Sie Kanäle mit HDD-Gruppen.

9.4 Andere Speicherparameter konfigurieren

Gehen Sie zu **System** → **Speicherverwaltung** → **Erweiterte Einstellungen**.

Tabelle 9-3 Parameterbeschreibung

Parameter Name	Beschreibung
Festplattenschlaf	Wenn die Festplatte eine Zeit lang nicht benutzt wird, wird sie in den Ruhezustand versetzt.
Überschreiben	Wenn die Festplatte voll ist, werden neue Dateien geschrieben, während die ältesten Dateien gelöscht werden.
Kamera-VCA-Daten speichern	Nachdem Sie die VCA-Daten der Kamera auf Ihrem Gerät gespeichert haben, können Sie sie im Event Center suchen.
Max. Zeit für Clip-Export	Wenn Videos vom Gerät exportiert werden, bedeutet Paketzeit die Videodauer jeder Videopaketei.
eSATA	Für Geräte mit eSATA-Schnittstelle auf der Rückseite.
Verwendung	Legen Sie die Verwendung für eSATA fest.
Tag Video Post-Record	Nach dem Hinzufügen eines Tags zu einem Video ist dies die Zeit, die Sie für die Aufnahme nach der geplanten Zeit festgelegt haben. Hinweis • Sie können während der Live-Ansicht oder der Wiedergabe auf  klicken, um einen Tag hinzuzufügen. • Um Videos mit Tags zu suchen, gehen Sie zu  → Sicherung → Nach Tag.

10 Zeitplan Konfiguration

Das Gerät folgt dem Zeitplan, um Dateien auf der Festplatte zu speichern.

10.1 Zeitplanvorlage konfigurieren

Nachdem eine Zeitplanvorlage konfiguriert wurde, können Sie die Vorlage als Aufzeichnungszeitplan verwenden.

Schritte

1. Gehen Sie zu **System** → **Systemeinstellungen** → **Vorlagenkonfiguration** → **Urlaubsplan**.
2. Klicken Sie auf **Hinzufügen**.

Abbildung 10-1 Feiertag hinzufügen

3. Schalten Sie **Enable** ein.
4. Konfigurieren Sie den Urlaub.

Hinweis

Nachdem die Feiertage konfiguriert sind, können Sie den Feiertagszeitplan unabhängig einstellen. Der Feiertagsplan hat eine höhere Priorität als der normale Zeitplan (von Mo bis So).

5. **Speicherzeitplan** festlegen.
 - 1) Klicken Sie auf **Speicherzeitplan**.
 - 2) Wählen Sie einen Vorlagennamen.

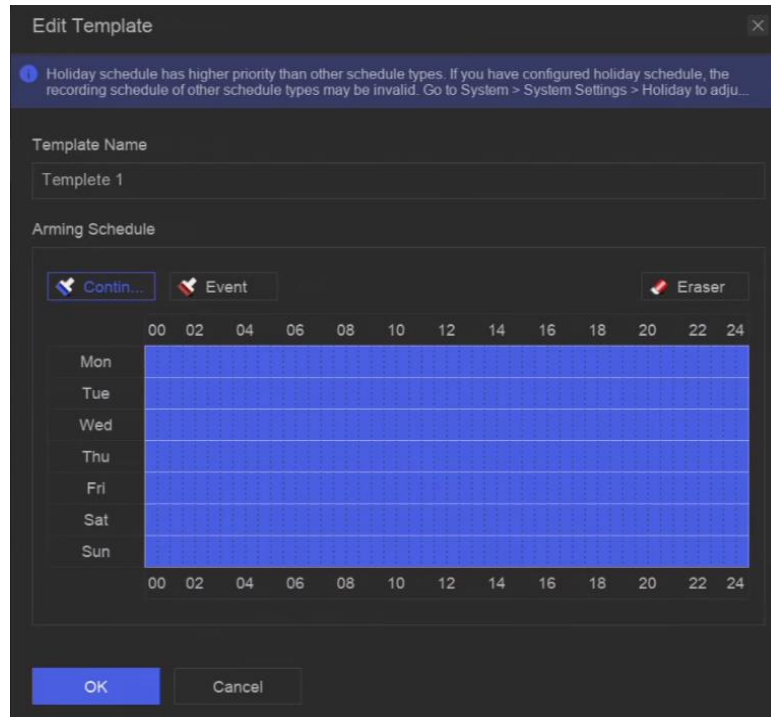


Abbildung 10-2 Vorlage bearbeiten

- 3) Wählen Sie einen Aufzeichnungstyp. Zum Beispiel "Ereignis".
- 4) Ziehen Sie den Cursor auf die Zeitleiste, um den Zeitplan zu zeichnen.

Hinweis

- Nachdem Sie den Cursor auf die Zeitleiste bewegt haben, können Sie auch auf **00:00-24:00** klicken, um einen bestimmten Zeitplan festzulegen.
 - Sie können auf **Radiergummi** klicken, um den Zeitplan zu löschen.
-

Hinweis

Sie können auch auf **Vorlage konfigurieren** klicken, um die Vorlage unter **System** → **Speicherverwaltung** → **Speicherplan** → **Videoaufzeichnung** / **Bildaufzeichnung** / **Audioaufzeichnung** zu konfigurieren.

6. Klicken Sie auf **OK**.

10.2 Aufzeichnungszeitplan konfigurieren

Die Kamera startet/stoppt die Aufzeichnung automatisch gemäß dem konfigurierten Aufzeichnungsplan.

Schritte

1. Gehen Sie zu **System** → **Speicherverwaltung** → **Speicherplan** → **Videoaufzeichnung**.

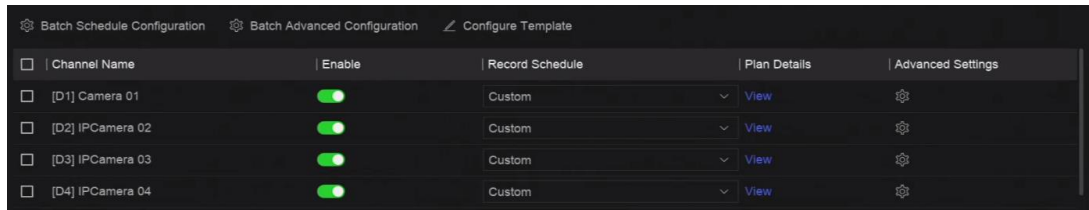


Abbildung 10-3 Konfiguration der Videoaufzeichnung

- Schalten Sie die Option **Aktivieren** für eine Kamera ein.
- Wählen Sie einen Zeitplantyp.

Hinweis

Wenn Sie "**Aufnahmezeitplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf die Zeitleiste ziehen, um einen benutzerdefinierten Aufnahmezeitplan einzustellen, oder Sie bewegen den Cursor auf die Zeitleiste und klicken auf **00:00-24:00** , um einen bestimmten Zeitplan einzustellen.

- Klicken Sie auf **Ansicht**, um den Zeitplan zu sehen.



Abbildung 10-4 Zeitplan anzeigen

- Optional: Klicken Sie unter **Erweiterte Einstellungen** auf , um weitere erweiterte Parameter einzustellen.

Tabelle 10-1 Erweiterte Parameterbeschreibung

Parameter	Beschreibung
Audio aufzeichnen	Aktivieren oder deaktivieren Sie die Audioaufnahme. Hinweis Der Kanal muss über eine Audiofunktion verfügen oder ein Audiogerät angeschlossen haben.
ANR	ANR (Automatic Network Replenishment) kann automatisch die SD-Karte der Netzwerkkamera aktivieren, um das Video im Falle einer Netzwerkunterbrechung zu speichern, und kann Daten synchronisieren, nachdem das Netzwerk wiederhergestellt wurde.
Pre-Record	Die Zeit, die Sie für die Aufzeichnung vor der geplanten Zeit oder dem Ereignis festgelegt haben. Wenn z. B. ein Alarm die Aufnahme um 10:00 Uhr auslöst und Sie die Voraufnahmezeit auf 5 Sekunden einstellen, nimmt die Kamera um 9:59:55 Uhr auf.
Post-Record	Die Zeit, die Sie für die Aufzeichnung nach dem Ereignis oder der geplanten Zeit eingestellt haben. Wenn z. B. eine durch einen Alarm ausgelöste Aufzeichnung um 11:00 Uhr endet und Sie die Zeit nach der Aufzeichnung auf 5 Sekunden einstellen, wird bis 11:00:05 Uhr aufgezeichnet.
Strom-Typ	Bei Main Stream ist die Auflösung in der Regel höher. Bei Sub-Stream können Sie bei gleichem Speicherplatz länger aufnehmen, aber die Auflösung ist geringer. Bei Dual Stream zeichnet das Gerät sowohl Main Stream als auch Sub-Stream auf.
Video/Bild Abgelaufene Zeit	Die abgelaufene Zeit ist der Zeitraum, in dem eine Datei auf der Festplatte aufbewahrt werden soll. Wenn die Frist erreicht ist, wird die Datei gelöscht. Wenn Sie die abgelaufene Zeit auf 0 setzen, wird die Datei nicht gelöscht. Die tatsächliche Aufbewahrungszeit für die Datei sollte sich nach der Kapazität der Festplatte richten.

6. Optional: Wählen Sie Kanäle in der Liste aus, und verwenden Sie **Stapelkonfiguration** und **erweiterte Stapeleinstellungen**, um Kanäle in einem Stapel zu konfigurieren.

7. Klicken Sie auf **Speichern**.

10.3 Zeitplan für die Bildaufnahme konfigurieren

Das Gerät würde automatisch Live-Bilder nach einem bestimmten Zeitplan aufnehmen.

Schritte

1. Gehen Sie zu **System** → **Speicherverwaltung** → **Speicherplan** → **Bilderfassung**.

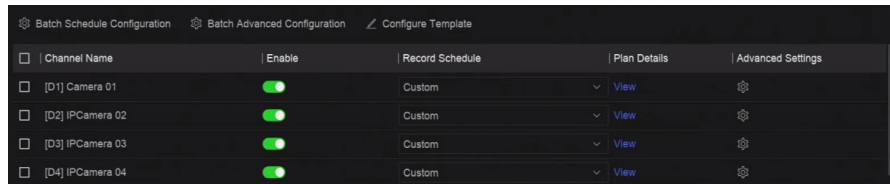


Abbildung 10-5 Picture Capture Konfiguration

2. Schalten Sie die Option **Aktivieren** für eine Kamera ein.
3. Wählen Sie einen Zeitplantyp.

Hinweis

Wenn Sie "**Aufnahmezeitplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf die Zeitleiste ziehen, um einen benutzerdefinierten Aufnahmezeitplan einzustellen, oder Sie bewegen den Cursor auf die Zeitleiste und klicken auf **00:00-24:00** , um einen bestimmten Zeitplan einzustellen.

4. Klicken Sie auf **Ansicht**, um den Zeitplan anzuzeigen.



Abbildung 10-6 Ansicht Zeitplan

5. Klicken Sie unter **Erweiterte Einstellungen** auf, um erweiterte Bildparameter einzustellen.

Tabelle 10-2 Erweiterte Parameterbeschreibung

Parameter	Beschreibung
Erfassungsverzögerung	Die Dauer der Bildaufnahme.
Auflösung	Legen Sie die Auflösung des aufzunehmenden Bildes fest.
Bildqualität	Stellen Sie die Bildqualität auf niedrig, mittel oder hoch ein. Eine hohe Bildqualität erfordert mehr Speicherplatz.
Intervall	Das Zeitintervall, in dem jedes Livebild aufgenommen wird.

6. Optional: Wählen Sie Kanäle in der Liste aus, und verwenden Sie **Stapelkonfiguration** und **erweiterte StapelEinstellungen**, um Kanäle in einem Stapel zu konfigurieren.
7. Klicken Sie auf **Speichern**.

10.4 Konfigurieren der Audioaufzeichnung

Das Gerät nimmt automatisch Audios gemäß dem konfigurierten Aufnahmeplan auf.

Schritte

- Gehen Sie zu **System** → **Speicherverwaltung** → **Speicherplan** → **Audioaufzeichnung**.
- Schalten Sie die Option **Aktivieren** für einen Kanal ein.
- Wählen Sie einen Zeitplantyp.

Hinweis

Wenn Sie "**Aufnahmezeitplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf die Zeitleiste ziehen, um einen benutzerdefinierten Aufnahmezeitplan einzustellen, oder den Cursor auf die Zeitleiste bewegen und auf **00:00-24:00** klicken, um einen bestimmten Zeitplan einzustellen.

- Klicken Sie auf **Ansicht**, um den Zeitplan anzuzeigen.
- Optional: Klicken Sie unter **Erweiterte Einstellungen** auf, um weitere erweiterte Parameter einzustellen.

Tabelle 10-3 Erweiterte Parameterbeschreibung

Parameter	Beschreibung
Pre-Record	Die Zeit, die Sie für die Aufnahme vor der geplanten Zeit oder dem Ereignis festgelegt haben. Wenn z. B. ein Alarm die Aufnahme um 10:00 Uhr auslöst und Sie die Voraufnahmezeit auf 5 Sekunden einstellen, nimmt der Kanal um 9:59:55 Uhr auf.
Post-Record	Die Zeit, die Sie für die Aufzeichnung nach dem Ereignis oder der

Parameter	Beschreibung
	geplanten Zeit eingestellt haben. Wenn z. B. eine durch einen Alarm ausgelöste Aufzeichnung um 11:00 Uhr endet und Sie die Zeit nach der Aufzeichnung auf 5 Sekunden einstellen, wird bis 11:00:05 Uhr aufgezeichnet.

6. Optional: Wählen Sie Kanäle in der Liste aus, und verwenden Sie **Stapelkonfiguration** und **erweiterte Stapeleinstellungen**, um Kanäle in einem Stapel zu konfigurieren.
7. Klicken Sie auf **Speichern**.

11 Live-Ansicht

11.1 Layout der Live-Ansicht konfigurieren

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

Schritte

1. Gehen Sie zur **Live-Ansicht**.
2. Klicken Sie in der rechten unteren Ecke auf .
3. Wählen Sie einen Fenstertyp, oder klicken Sie auf **Benutzerdefiniert**, um einen neuen Typ nach Ihren Wünschen zu erstellen.
4. Bewegen Sie den Cursor auf **Standardansicht** in **Ansicht**.
5. Klicken Sie auf .
6. Legen Sie die Schnittstelle für die Bildausgabe in der Live-Ansicht fest. Sie können einen Kanal aus der Kanalliste in ein Fenster ziehen oder einen Kanal von einem Fenster in ein anderes ziehen.
7. Klicken Sie auf .

11.2 GUI-Einführung

Sie können Live-Bilder anzeigen, Live-Audio wiedergeben, Bilder aufnehmen, sofortige Wiedergabe durchführen usw.

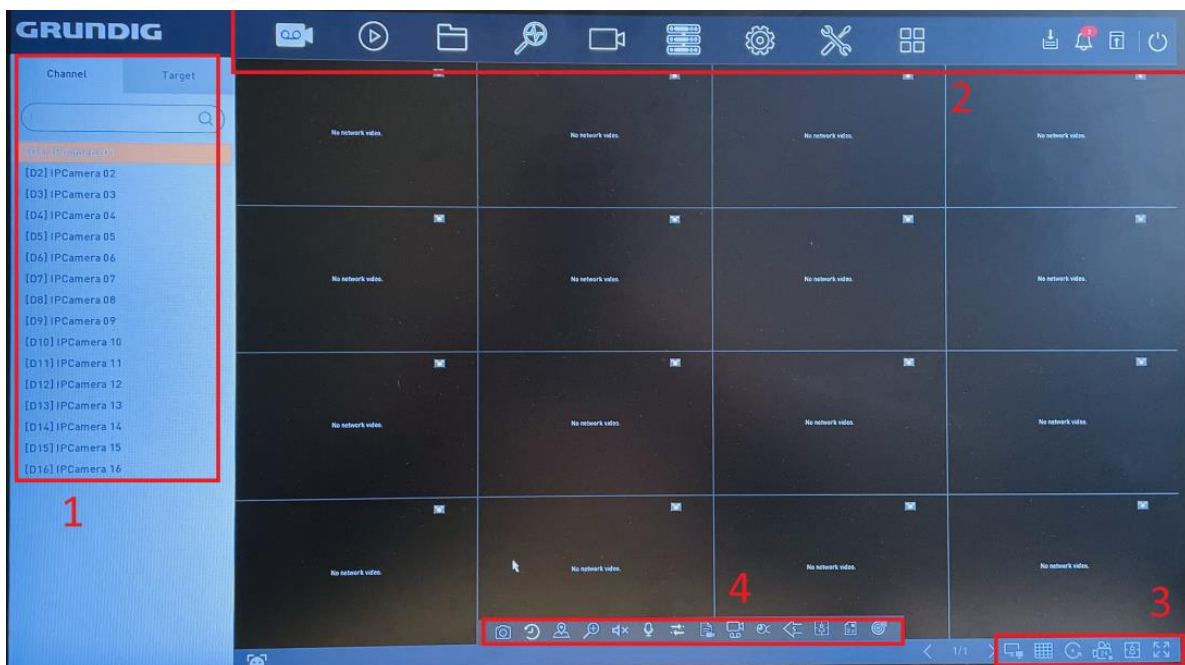


Abbildung 11-1 Live-Ansicht

Tabelle 11-1 Schnittstellenbeschreibung

Nr.	Beschreibung
1	Kanalliste und Zielerkennungsliste. Wenn Sie einen Kanal aus der Kanalliste auswählen, wird das Gerät zum entsprechenden Fenster weitergeleitet.
2	Kontextmenü. Es wird angezeigt, wenn Sie mit dem Cursor auf den Bildbereich klicken.
3	Kanal-Symbolleiste. • Klicken Sie auf , um ein Tag zum Kanal hinzuzufügen. Nach dem Hinzufügen können Sie auf  → Sicherung → Nach Tag gehen, um Videos nach Tag zu suchen. • Sie können  → VCA-Info anzeigen wählen, um die Regelrahmen anzuzeigen.
4	Symbolleiste für die Live-Ansicht.

11.3 PTZ-Steuerung

PTZ ist die Abkürzung für Schwenken, Neigen und Zoomen. Nachdem eine PTZ-Kamera zu Ihrem Gerät hinzugefügt wurde, kann das Gerät nach links und rechts schwenken, nach oben und unten neigen und hinein- und herauszoomen.

Wählen Sie eine PTZ-Kamera aus, und erweitern Sie das PTZ-Steuerungsmenü in der unteren linken Ecke.

Tabelle 11-2 PTZ-Betrieb

Bezeichnung	Beschreibung	Operation
Voreinstellung	Voreinstellungen speichern die PTZ-Position und den Status von Zoom, Fokus, Blende usw. Sie können eine Voreinstellung aufrufen, um die Kamera schnell an die vordefinierte Position zu bewegen.	Stellen Sie eine Voreinstellung ein: 1. Wählen Sie eine Voreinstellung. 2. Verwenden Sie die Richtungstasten, um das Bild einzustellen. 3. Klicken Sie auf .
		Rufen Sie eine Voreinstellung auf: Klicken Sie auf  .
Patrouille	Patrouillen können so eingestellt werden, dass die PTZ zu Schlüsselpunkten fährt und dort für eine bestimmte Dauer verweilt, bevor sie zum nächsten Schlüsselpunkt	Setzen Sie eine Patrouille: 1. Wählen Sie eine Patrouille. 2. Klicken Sie auf . 3. Fügen Sie Voreinstellungen für die Patrouille hinzu. 4. Klicken Sie auf OK.

Bezeichnung	Beschreibung	Operation
	weiterfährt. Die Schlüsselpunkte sind mit den Voreinstellungen verknüpft.	Rufen Sie eine Streife: Klicken Sie auf  .
Muster	Muster können durch Aufzeichnung der PTZ-Bewegung festgelegt werden. Sie können das Muster aufrufen, damit sich die PTZ entsprechend dem vordefinierten Pfad bewegt.	Legen Sie ein Muster fest: 1. Klicken Sie auf  2. Benutzen Sie die Richtungstasten, um das Bild einzustellen, das Gerät wird die Bewegung aufzeichnen. 3. Aufnahme beenden.
		Rufen Sie ein Muster auf: Klicken Sie auf  .

Hinweis

Wenn das PTZ-Panel nicht verwendet werden kann, klicken Sie bitte auf  , um die Einstellungen zu überprüfen.

12 Wiedergabe

12.1 GUI-Einführung

Sie können Video- oder Audiodateien wiedergeben.

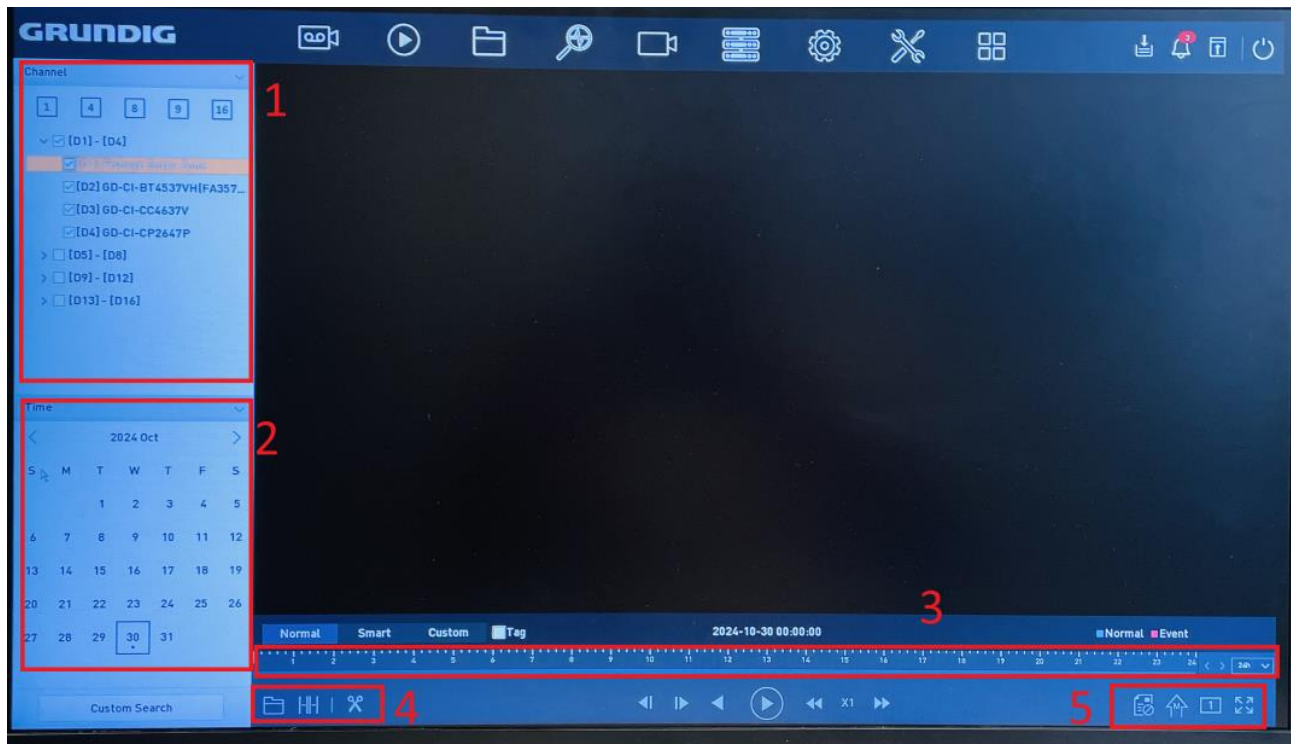


Abbildung 12-1 Wiedergabe

Tabelle 12-1 Schnittstellenbeschreibung

Nr.	Beschreibung
1	Senderliste.
2	Kalender für die Zeitauswahl.
3	Zeitleiste für die Wiedergabe. - Positionieren Sie den Cursor auf der Zeitleiste und ziehen Sie die Zeitleiste, um sie an einen bestimmten Zeitpunkt zu positionieren. - Der mit einem blauen Balken markierte Zeitraum enthält Video. Der rote Balken zeigt an, dass es sich bei dem Video in diesem Zeitraum um ein Ereignisvideo handelt. - Scrollen Sie nach oben/unten, um die Zeitleiste zu vergrößern/verkleinern.
4	Kanal-Symboleiste. Klicken Sie auf , um ein Tag zum Kanal hinzuzufügen. Nach dem Hinzufügen

Nr.	Beschreibung
	können Sie auf  → Sicherung → Nach Tag gehen, um Videos nach Tag zu suchen. • Klicken Sie auf  , um das Video zu sperren. Nachdem ein Video gesperrt wurde, kann es nicht mehr überschrieben werden. Nach dem Sperren können Sie  → Sicherung → Nach Tag aufrufen, um Videos nach Sperre zu suchen. • Wählen Sie  → Dual-VCA, um Videos zu suchen, die die entsprechende Ereignisregel auslösen können. Einzelheiten zu den einzelnen Ereignistypen finden Sie in den Schritten zur Ereigniskonfiguration. Hinweis Um diese Funktion zu nutzen, gehen Sie zu Konfiguration → Gerätezugriff → Gerätekonfiguration → Geräteparameter → Display Info. on Scream, um die Option Enable Dual-VCA zu aktivieren. über den Webbrowser, und gehen Sie zu System → Speicherverwaltung → Erweiterte Einstellungen, um die Option Kamera-VCA-Daten über die lokale GUI-Schnittstelle speichern zu aktivieren. • Sie können  → VCA-Info anzeigen wählen, um die Regelrahmen anzuzeigen.
5	• Strategie für die Wiedergabe

12.2 Normale Wiedergabe

Wiedergabe von Videos für einen Kanal. Bei bestimmten Geräten kann eine synchrone Wiedergabe für mehrere Kanäle möglich sein.

Schritte

1. Gehen Sie zu **Wiedergabe** .
2. Wählen Sie den/die Kanal/Kanäle in der Liste oben aus.

Hinweis

Gruppenwiedergabe: Wählen Sie eine Gruppe in der Liste aus, und die Kanäle in der Gruppe können wiedergegeben werden.

3. Wählen Sie ein Datum im Kalender aus.

Hinweis

Das blaue Dreieck in der Ecke des Kalenderdatums zeigt an, dass Videos verfügbar sind.

4. Optional: Geben Sie Videos wieder, die Menschen oder Fahrzeuge als Ziele enthalten.
 - : Videos, die Menschen enthalten, werden rot markiert.
 - : Videos, die ein Fahrzeug enthalten, werden rot markiert.

12.3 Wiedergabe von Ereignissen

Wenn Sie den Ereigniswiedergabemodus auswählen, analysiert und markiert das System Videos, die Informationen zur Bewegungserkennung, Linienüberquerungserkennung oder Einbruchserkennung enthalten

Bevor Sie beginnen

- Stellen Sie sicher, dass die Kamera **Dual-VCA** aktiviert hat. Sie können es über die Webbrowser-Oberfläche der Kamera unter **Konfiguration** → **Video/Audio** → **Display Info. auf Stream** aktivieren.
- Vergewissern Sie sich, dass Ihr Videorecorder die Option **Kamera-VCA-Daten speichern** unter **Speicherverwaltung** → **Erweiterte Einstellungen** aktiviert hat.

Schritte

1. Wählen Sie **Wiedergabe** → .
2. Wählen Sie ein Datum im Kalender aus.

Hinweis

Das blaue Dreieck in der Ecke des Kalenderdatums zeigt an, dass Videos verfügbar sind.

3. Klicken Sie auf  → **Dual-VCA** in der unteren rechten Ecke des Wiedergabebildes, um einen Ereignistyp auszuwählen. Einzelheiten zu den einzelnen Ereignistypen finden Sie in den Schritten zur Ereigniskonfiguration.
4. Klicken Sie auf **Suchen**.
Videos, die die Anforderungen der Erkennungsregeln erfüllen, werden rot markiert.
5. Klicken Sie auf , um die Wiedergabestrategie für normales Video und Smart Video (das Video, das Smart Data enthält) einzustellen.

Hinweis

Wenn **Dual-VCA** nicht verwendet wird, bedeuten rote Segmente in der Fortschrittsleiste, dass die intelligenten Videos durch das ursprüngliche Ereignis erzeugt werden.

12.4 Wiedergabe von Teilperioden

Die Videodateien können in mehreren Unterabschnitten gleichzeitig auf dem Bildschirm wiedergegeben werden.

Schritte

1. Gehen Sie zu **Wiedergabe**.
2. Wählen Sie eine Kamera aus.
3. Stellen Sie die Start- und Endzeit ein.
4. Klicken Sie auf **Suchen**.

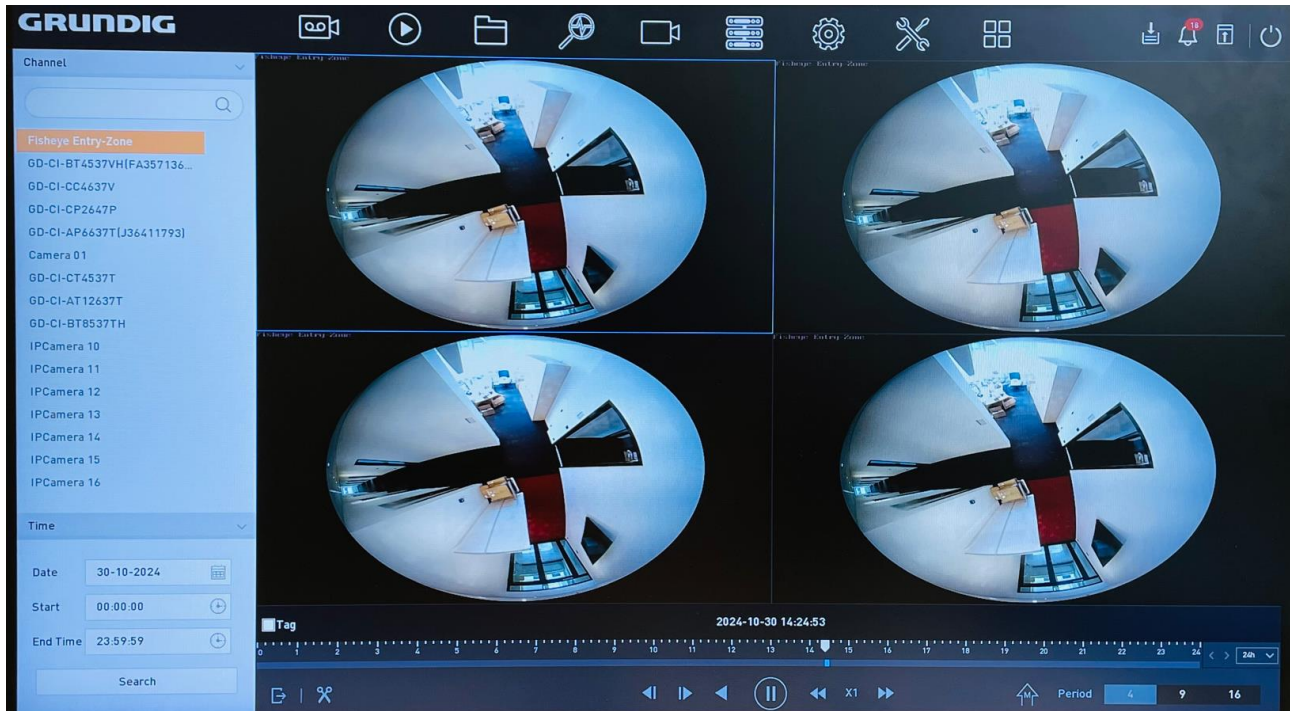


Abbildung 12-2 Sub-Perioden-Wiedergabe

5. Wählen Sie den Punkt in der unteren rechten Ecke, z. B. 4.

Hinweis

Entsprechend der festgelegten Anzahl von geteilten Bildschirmen können die Videodateien am ausgewählten Datum in durchschnittliche Abschnitte für die Wiedergabe unterteilt werden. Wenn z. B. Videodateien zwischen 16:00 und 22:00 Uhr vorhanden sind und der 6-Bildschirm-Anzeigemodus ausgewählt ist, können die Videodateien eine Stunde lang gleichzeitig auf jedem Bildschirm wiedergegeben werden.

13 Ereigniszentrum

13.1 Ereignisseinstellungen

13.1.1 Grundlegendes/allgemeines Ereignis

Schritte

1. Gehen Sie zu **Event Center** →  → **Ereigniskonfiguration** → **Basisereignis / Allgemeines Ereignis**.
2. Wählen Sie einen Kanal.
3. Wählen Sie einen Ereignistyp.
4. Schalten **Sie Enable** ein.
5. Klicken Sie auf **Regeleinstellungen**, um die Regel festzulegen.

Tabelle 13-1 Normales Ereignis

Name des Ereignisses	Ereignis Beschreibung	Regel-Konfiguration	
Bewegungserkennung	Die Bewegungserkennung erkennt die sich bewegendenden Objekte im überwachten Bereich.	Verwenden Sie die Symbolleiste am oberen Bildrand, um den Erkennungsbereich zu zeichnen. AI durch NVR Das Ereignis der Bewegungserkennung wird vom NVR analysiert. Das Gerät kann Videos analysieren, die Menschen und Fahrzeuge enthalten. Nur das Ziel des ausgewählten Typs (Mensch oder Fahrzeug) löst Alarme aus, wodurch Fehlalarme, die durch andere Objekte	Mit der Empfindlichkeit können Sie kalibrieren, wie leicht Bewegungen den Alarm auslösen können. Ein höherer Wert führt dazu, dass die Bewegungserkennung leichter ausgelöst wird.

		verursacht werden, reduziert werden können. AI nach Kamera Das Ereignis der Bewegungserkennung wird von der Kamera analysiert. Erkennung Ziel Menschen und Fahrzeuge sind auswählbar, abgesehen von Fehlalarmen können nur die ausgewählten Ziele Alarme auslösen.	
Erkennung von Video-Manipulationen	Die Video-Manipulationserkennung löst einen Alarm aus, wenn das Kameraobjektiv verdeckt wird, und leitet Alarmmaßnahmen ein.	Verwenden Sie die Symbolleiste am oberen Bildrand, um den Erkennungsbereich zu zeichnen.	
Erkennung von Videoverlusten	Die Videoverlusterkennung erkennt den Videoverlust eines Kanals und leitet Alarmmaßnahmen ein.	-	
Audio-Ausnahme-Erkennung	Die Audio-Ausnahmeerkennung erkennt anormale Geräusche in der Szene, z. B. eine plötzliche Zunahme/Abnahme der Lautstärke.	-	

Defokus-Erkennung	Durch Objektivdefokus verursachte Bildunschärfe kann erkannt werden.	-
Erkennung von plötzlichen Szenenwechseln	Die Erkennung von Szenenveränderungen erkennt die Veränderung der Videoüberwachungsumgebung durch externe Faktoren, wie z. B. die absichtliche Drehung der Kamera.	-

6. Klicken Sie auf **Scharfschaltplan**, um einen Scharfschaltplantyp auszuwählen.

Hinweis

Wenn Sie "**Scharfschaltplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf den Zeitbalken ziehen, um einen benutzerdefinierten Scharfschaltplan einzustellen, oder Sie bewegen den Cursor auf den Zeitbalken und klicken auf  , um einen bestimmten Zeitplan einzustellen.

7. Klicken Sie auf **Verknüpfungsmethode**, um Verknüpfungsmethoden festzulegen.

Tabelle 13-2 Beschreibung der Verknüpfungsmethode

Verknüpfung Methode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Alarm-Pop-up-Fenster	Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Alarm-Pop-up-Fenster an.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarめingang, die Bewegungserkennung, die Erkennung von Videomanipulationen, die Gesichtserkennung, die Erkennung von Linienüberquerungen und andere Ereignisse ausgelöst werden.
Datensatz	Wenn ein Alarm erkannt wird, zeichnet der ausgewählte Kanal Videos auf.

Verknüpfung Methode	Beschreibung
	Hinweis Der Zeitplan für die Videoaufzeichnung muss für den Kanal aktiviert sein, andernfalls wäre diese Verknüpfung ungültig. Sie können zu System → Speicherverwaltung → Speicherplan → Videoaufzeichnung gehen, um den Zeitplan für die Videoaufzeichnung zu konfigurieren.

8. Klicken Sie auf **Speichern**.

13.1.2 Perimeterschutz

Zu den Ereignissen des Perimeterschutzes gehören die Erkennung von Linienüberquerungen, das Erkennen von Eindringlingen, das Erkennen des Eintritts in einen Bereich und das Erkennen des Austritts aus einem Bereich.

Erkennung von Linienkreuzungen konfigurieren

Die Linienüberquerungserkennung erkennt Personen, Fahrzeuge und Objekte, die eine festgelegte virtuelle Linie überqueren. Die Erkennungsrichtung kann als bidirektional, von links nach rechts oder von rechts nach links eingestellt werden.

Bevor Sie beginnen

Bitte gehen Sie zu **System** → **Intelligente Analyse** → **Intelligente Ereigniseinstellungen** → **Perimeterschutz**, um den Algorithmus **für den Perimeterschutz** zu aktivieren .

Schritte

Hinweis

Ein Teil der folgenden Schritte ist nur für bestimmte NVR- oder Kameramodelle verfügbar.

1. Gehen Sie zu **Smart Analysis** → **Smart Event Configuration** → **Perimeter Protection** .
2. Wählen Sie eine Kamera aus.
3. Optional: Aktivieren **Sie AI durch NVR aktivieren**.
Das Gerät analysiert das Video, und die Kameras übertragen nur den Videostrom.
4. Wählen Sie **Linienkreuzung**.
5. Schalten **Sie Enable** ein.

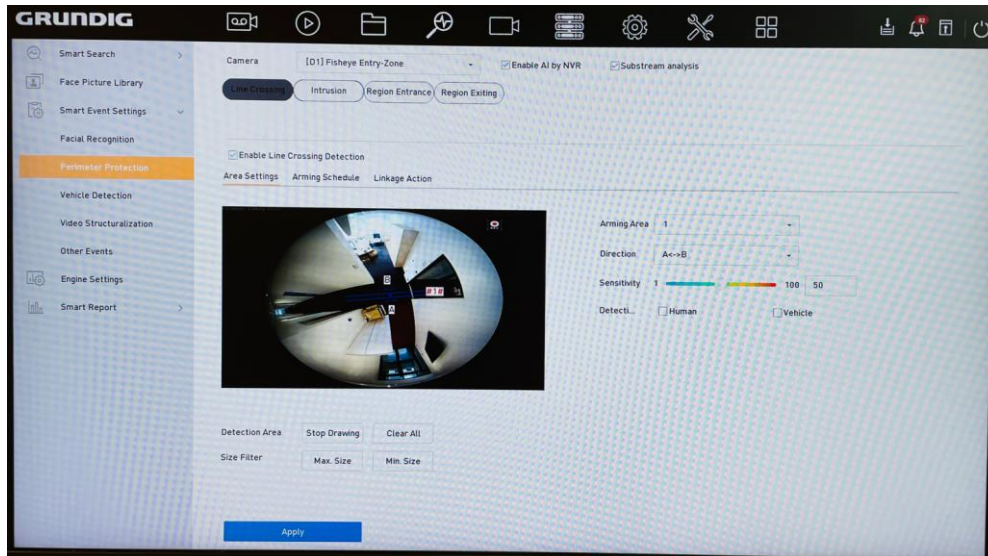


Abbildung 13-1 Erkennung von Linienkreuzungen

6. Klicken Sie auf **Regeleinstellungen**, um Regeln zu erkennen.
 - 1) Wählen Sie eine Regelnummer. Wählen Sie zum Beispiel **1**.
 - 2) Klicken Sie auf , und klicken Sie jeweils zweimal auf das Bild, um den Start- und Endpunkt der Erkennungslinie zu zeichnen.
 - 3) Legen Sie **Richtung**, **Empfindlichkeit** und **Erkennungsziel** fest.

A<->B

Nur der Pfeil auf der B-Seite wird angezeigt. Wenn ein Objekt die konfigurierte Linie in beide Richtungen überquert, kann es erkannt werden und Alarme werden ausgelöst.

A->B

Nur das Objekt, das die konfigurierte Linie von der A-Seite zur B-Seite kreuzt, kann erkannt werden.

B->A

Nur das Objekt, das die konfigurierte Linie von der B-Seite zur A-Seite kreuzt, kann erkannt werden.

Empfindlichkeit

Je höher der Wert ist, desto leichter kann der Detektionsalarm ausgelöst werden.

Erkennung Ziel

Wählen Sie **Erkennungsziel** als **Mensch** oder **Fahrzeug**, um Alarme zu verwerfen, die nicht von Menschen oder Fahrzeugen ausgelöst werden. **Erkennungsziel** ist nur für bestimmte Modelle verfügbar.

- 4) Optional: Klicken Sie auf , um die **Max. Größe** oder **Min. Größe**. Nur Ziele, die die Größenanforderungen erfüllen, können Alarme auslösen.
 - 5) Optional: Wiederholen Sie die obigen Schritte, um weitere Regeln zu zeichnen. Es werden bis zu 4 Regeln unterstützt.
7. Klicken Sie auf **Scharfschaltplan**, um einen Scharfschaltplantyp auszuwählen.

Hinweis

Wenn Sie "**Scharfschaltplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf den Zeitbalken ziehen, um einen benutzerdefinierten Scharfschaltplan einzustellen, oder den Cursor auf den Zeitbalken bewegen und auf **00:00-24:00** klicken, um einen bestimmten Zeitplan einzustellen.

8. Klicken Sie auf **Verknüpfungsmethode**, um Verknüpfungsmethoden festzulegen.

Tabelle 13-3 Beschreibung der Verknüpfungsmethode

Verknüpfungsmethode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Alarm-Pop-up-Fenster	Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Alarm-Pop-up-Fenster an.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarめingang, die Bewegungserkennung, die Videomanipulationserkennung, die Gesichtserkennung, die Linienüberquerungserkennung und alle anderen Ereignisse ausgelöst werden.
Datensatz	Wenn ein Alarm erkannt wird, zeichnet der ausgewählte Kanal Videos auf. Hinweis Der Zeitplan für die Videoaufzeichnung muss für den Kanal aktiviert sein, andernfalls wäre diese Verknüpfung ungültig. Sie können zu System → Speicherverwaltung → Speicherplan → Videoaufzeichnung gehen, um den Zeitplan für die Videoaufzeichnung zu konfigurieren.

9. Optional: Legen Sie einen **Schutzbereich** fest, wenn **AI by NVR** aktiviert ist. Nachdem ein Schutzbereich festgelegt wurde, analysiert das Gerät das Verhalten des Ziels in diesem Bereich nicht, so dass die Perimeterschutz-Ereignisse innerhalb dieses Bereichs nicht ausgelöst werden.
10. Klicken Sie auf **Speichern**.

Was ist als nächstes zu tun?

Sie können die **Live-Ansicht** aufrufen und auf **Ziel** klicken, um Alarmer in Echtzeit anzuzeigen.

Einbrucherkennung konfigurieren

Die Funktion zur Erkennung von Eindringlingen erkennt Personen, Fahrzeuge oder andere Objekte, die in einen vordefinierten virtuellen Bereich eindringen und sich dort aufhalten. Wenn ein Alarm ausgelöst wird, können bestimmte Maßnahmen ergriffen werden.

Bevor Sie beginnen

Bitte gehen Sie zu **System** → **Intelligente Analyse** → **Intelligente Ereigniseinstellungen** → **Perimeterschutz**, um den Algorithmus **für den Perimeterschutz** zu aktivieren.

Schritte

Hinweis

Ein Teil der folgenden Schritte ist nur für bestimmte NVR- oder Kameramodelle verfügbar.

1. Gehen Sie zu **Smart Analysis** → **Smart Event Configuration** → **Perimeter Protection**.
2. Wählen Sie eine Kamera aus.
3. Optional: Aktivieren **Sie AI durch NVR aktivieren**.
Das Gerät analysiert das Video, und die Kameras übertragen nur den Videostrom.
4. Wählen Sie **Aufdringlich**.
5. Schalten **Sie Enable** ein.

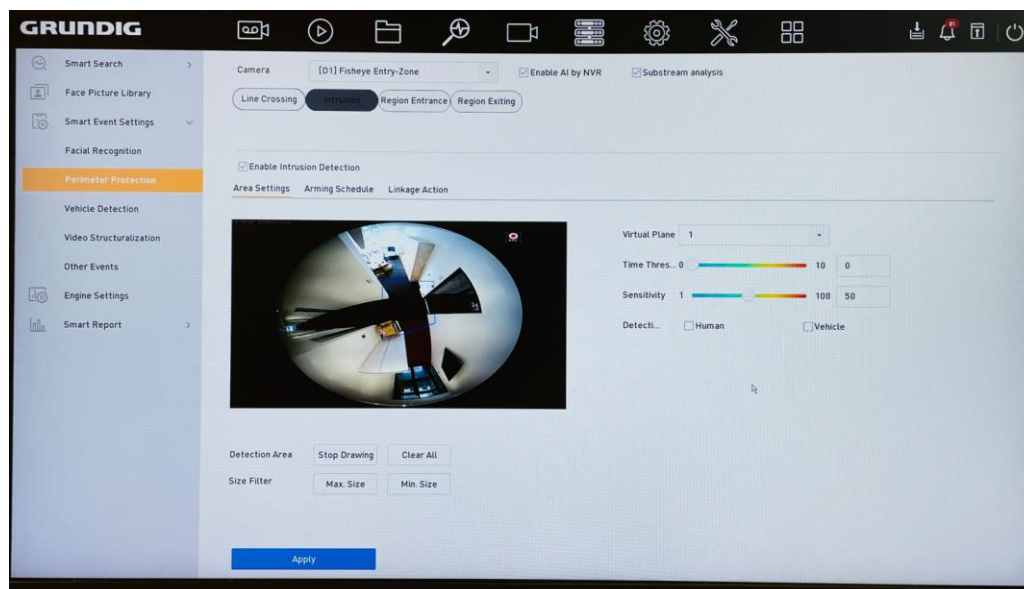


Abbildung 13-2 Einbrucherkennung

6. Klicken Sie auf **Regeleinstellungen**, um Regeln zu erkennen.
1) Wählen Sie eine Regelnummer. Wählen Sie zum Beispiel **1**.

- 2) Klicken Sie auf  , und klicken Sie jeweils 4 Mal auf das Bild, um jeden Punkt einer viereckigen Fläche zu zeichnen.
- 3) Stellen Sie **Zeitschwelle**, **Empfindlichkeit** und **Erkennungsziel** ein.

Zeitschwelle

Die Zeit, die ein Objekt in der Region verweilt. Wenn die Dauer des Objekts im definierten Erfassungsbereich den Schwellenwert überschreitet, löst das Gerät einen Alarm aus.

Empfindlichkeit

Je höher der Wert ist, desto leichter kann der Detektionsalarm ausgelöst werden.

Erkennung Ziel

Wählen Sie **Erkennungsziel** als **Mensch** oder **Fahrzeug**, um Alarmer zu verwerfen, die nicht von Menschen oder Fahrzeugen ausgelöst werden. **Erkennungsziel** ist nur für bestimmte Modelle verfügbar.

- 4) Optional: Klicken Sie auf  , um die **Max. Größe** oder **Min. Größe**. Nur Ziele, die die Größenanforderungen erfüllen, können Alarmer auslösen.
- 5) Optional: Wiederholen Sie die obigen Schritte, um weitere Regeln zu zeichnen. Es werden bis zu 4 Regeln unterstützt.
7. Klicken Sie auf **Scharfschaltplan**, um einen Scharfschaltplantyp auszuwählen.

Hinweis

Wenn Sie "**Scharfschaltplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf den Zeitbalken ziehen, um einen benutzerdefinierten Scharfschaltplan einzustellen, oder den Cursor auf den Zeitbalken bewegen und auf  klicken, um einen bestimmten Zeitplan einzustellen.

8. Klicken Sie auf **Verknüpfungsmethode**, um Verknüpfungsmethoden festzulegen.

Tabelle 13-4 Verknüpfungsmethode Beschreibung

Verknüpfungsmethode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Alarm-Pop-up-Fenster	Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Alarm-Pop-up-Fenster an.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarめingang, die Bewegungserkennung, die Videomanipulationserkennung, die Gesichtserkennung, die Linienüberquerungserkennung und alle

Verknüpfungsmethode	Beschreibung
	anderen Ereignisse ausgelöst werden.
Datensatz	Wenn ein Alarm erkannt wird, zeichnet der ausgewählte Kanal Videos auf. Hinweis Der Zeitplan für die Videoaufzeichnung muss für den Kanal aktiviert sein, andernfalls wäre diese Verknüpfung ungültig. Sie können zu System → Speicherverwaltung → Speicherplan → Videoaufzeichnung gehen, um den Zeitplan für die Videoaufzeichnung zu konfigurieren.

9. Optional: Legen Sie einen **Schutzbereich** fest, wenn **AI by NVR** aktiviert ist. Nachdem ein Schutzbereich festgelegt wurde, analysiert das Gerät das Verhalten des Ziels in diesem Bereich nicht, so dass die Perimeterschutz-Ereignisse innerhalb dieses Bereichs nicht ausgelöst werden.
10. Klicken Sie auf **Speichern**.

Was ist als nächstes zu tun?

Sie können die **Live-Ansicht** aufrufen und auf **Ziel** klicken, um Alarmer in Echtzeit anzuzeigen.

Konfigurieren Sie die Erkennung von Regionseingängen

Die Erkennung des Eintritts in einen Bereich erkennt Objekte, die in einen vordefinierten virtuellen Bereich eintreten.

Bevor Sie beginnen

Bitte gehen Sie zu **System** → **Intelligente Analyse** → **Intelligente Ereigniseinstellungen** → **Perimeterschutz**, um den Algorithmus **für den Perimeterschutz** zu aktivieren.

Schritte

Hinweis

Ein Teil der folgenden Schritte ist nur für bestimmte NVR- oder Kameramodelle verfügbar.

- Gehen Sie zu **Smart Analysis** → **Smart Event Configuration** → **Perimeter Protection**.
- Wählen Sie eine Kamera aus.
- Optional: Aktivieren Sie **AI durch NVR aktivieren**.
Das Gerät analysiert das Video, und die Kameras übertragen nur den Videostrom.
- Wählen Sie **Region Eingang**.
- Schalten Sie **Enable** ein.

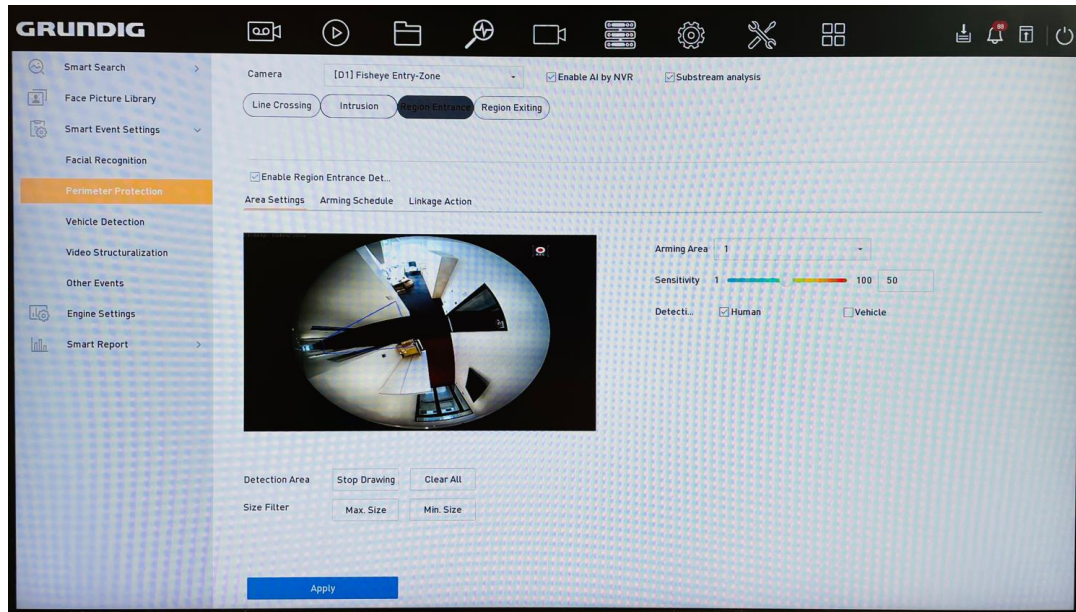


Abbildung 13-3 Erkennung von Regionseingängen

6. Klicken Sie auf **Regeleinstellungen**, um Regeln zu erkennen.
 - 1) Wählen Sie eine Regelnummer. Wählen Sie zum Beispiel **1**.
 - 2) Klicken Sie auf , und klicken Sie jeweils 4 Mal auf das Bild, um jeden Punkt einer viereckigen Fläche zu zeichnen.
 - 3) **Empfindlichkeit** und **Erkennungsziel** einstellen.

Empfindlichkeit

Je höher der Wert ist, desto leichter kann der Detektionsalarm ausgelöst werden.

Erkennung Ziel

Wählen Sie **Erkennungsziel** als **Mensch** oder **Fahrzeug**, um Alarmer zu verwerfen, die nicht von Menschen oder Fahrzeugen ausgelöst werden. **Erkennungsziel** ist nur für bestimmte Modelle verfügbar.

- 4) Optional: Wiederholen Sie die obigen Schritte, um weitere Regeln zu zeichnen. Es werden bis zu 4 Regeln unterstützt.
7. Klicken Sie auf **Scharfschaltplan**, um einen Scharfschaltplantyp auszuwählen.

Hinweis

Wenn Sie "**Scharfschaltplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf den Zeitbalken ziehen, um einen benutzerdefinierten Scharfschaltplan einzustellen, oder den Cursor auf den Zeitbalken bewegen und auf  klicken, um einen bestimmten Zeitplan einzustellen.

8. Klicken Sie auf **Verknüpfungsmethode**, um Verknüpfungsmethoden festzulegen.

Tabelle 13-5 Verknüpfungsmethode Beschreibung

Verknüpfungsmethode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Alarm-Pop-up-Fenster	Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Alarm-Pop-up-Fenster an.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarmeingang, die Bewegungserkennung, die Erkennung von Videomanipulationen, die Gesichtserkennung, die Erkennung von Linienüberquerungen und andere Ereignisse ausgelöst werden.
Datensatz	Wenn ein Alarm erkannt wird, zeichnet der ausgewählte Kanal Videos auf. Hinweis Der Zeitplan für die Videoaufzeichnung muss für den Kanal aktiviert sein, andernfalls wäre diese Verknüpfung ungültig. Sie können zu System → Speicherverwaltung → Speicherplan → Videoaufzeichnung gehen, um den Zeitplan für die Videoaufzeichnung zu konfigurieren.

9. Optional: Legen Sie einen **Schutzbereich** fest, wenn **AI by NVR** aktiviert ist. Nachdem ein Schutzbereich festgelegt wurde, analysiert das Gerät das Verhalten des Ziels in diesem Bereich nicht, so dass die Perimeterschutz-Ereignisse innerhalb dieses Bereichs nicht ausgelöst werden.

10. Klicken Sie auf **Speichern**.

Was ist als nächstes zu tun?

Sie können die **Live-Ansicht** aufrufen und auf **Ziel** klicken, um Alarme in Echtzeit anzuzeigen.

Konfigurieren der Erkennung des Verlassens einer Region

Die Bereichsausgangserkennung erkennt Objekte, die einen vordefinierten virtuellen Bereich verlassen.

Bevor Sie beginnen

Bitte gehen Sie zu **System** → **Intelligente Analyse** → **Intelligente Ereignisseinstellungen** → **Perimeterschutz**, um den Algorithmus für den Perimeterschutz zu aktivieren.

Schritte

Hinweis

Ein Teil der folgenden Schritte ist nur für bestimmte NVR- oder Kameramodelle verfügbar.

1. Gehen Sie zu **Smart Analysis** → **Smart Event Configuration** → **Perimeter Protection**.
2. Wählen Sie eine Kamera aus.
3. Optional: Aktivieren Sie AI durch NVR aktivieren.
Das Gerät analysiert das Video, und die Kameras übertragen nur den Videostrom.
4. Wählen Sie **Region Beenden**.
5. Schalten Sie **Enable** ein.

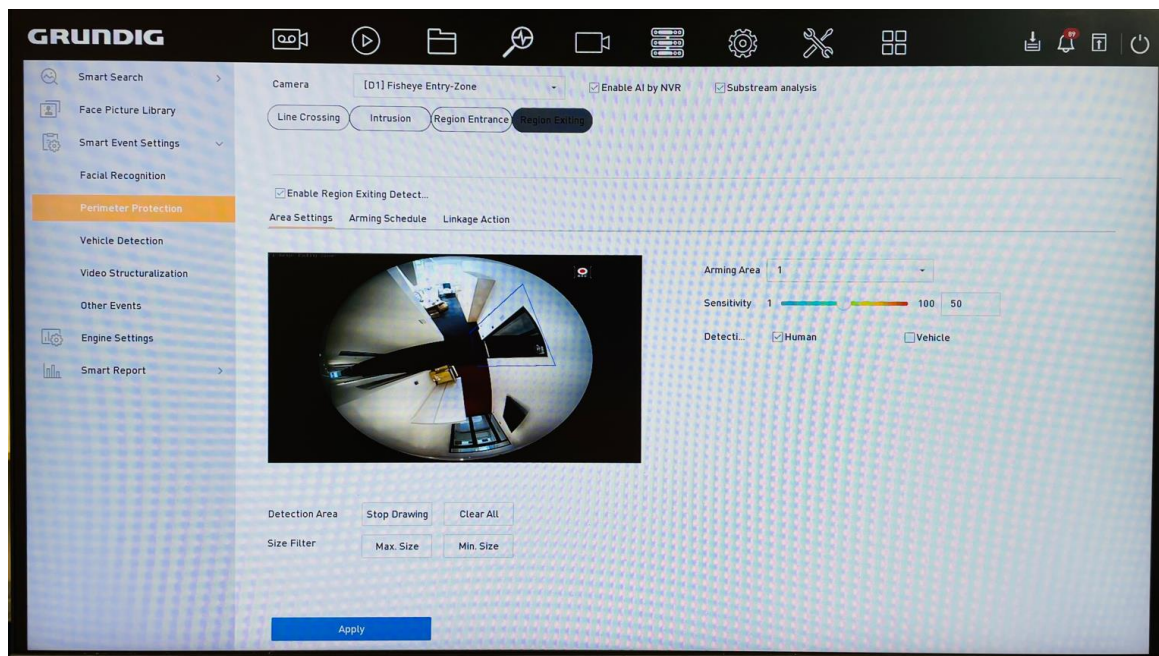


Abbildung 13-4 Erkennung des Verlassens einer Region

6. Klicken Sie auf **Regeleinstellungen**, um Regeln zu erkennen.
 - 1) Wählen Sie eine Regelnummer. Wählen Sie zum Beispiel **1**.
 - 2) Klicken Sie auf , und klicken Sie jeweils 4 Mal auf das Bild, um jeden Punkt einer viereckigen Fläche zu zeichnen.
 - 3) **Empfindlichkeit** und **Erkennungsziel** einstellen.

Empfindlichkeit

Je höher der Wert ist, desto leichter kann der Detektionsalarm ausgelöst werden.

Erkennung Ziel

Wählen Sie **Erkennungsziel** als **Mensch** oder **Fahrzeug**, um Alarme zu verwerfen, die nicht von Menschen oder Fahrzeugen ausgelöst werden. **Erkennungsziel** ist nur für bestimmte Modelle verfügbar.

4) Optional: Wiederholen Sie die obigen Schritte, um weitere Regeln zu zeichnen. Es werden bis zu 4 Regeln unterstützt.

7. Klicken Sie auf **Scharfschaltplan**, um einen Scharfschaltplantyp auszuwählen.

Hinweis

Wenn Sie "**Scharfschaltplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf den Zeitbalken ziehen, um einen benutzerdefinierten Scharfschaltplan einzustellen, oder Sie bewegen den Cursor auf den Zeitbalken und klicken auf **00:00-24:00** , um einen bestimmten Zeitplan einzustellen.

8. Klicken Sie auf **Verknüpfungsmethode**, um Verknüpfungsmethoden festzulegen.

Tabelle 13-6 Verknüpfungsmethode Beschreibung

Verknüpfungsmethode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Alarm-Pop-up-Fenster	Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Alarm-Pop-up-Fenster an.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarmeingang, die Bewegungserkennung, die Videomanipulationserkennung, die Gesichtserkennung, die Linienüberquerungserkennung und alle anderen Ereignisse ausgelöst werden.
Datensatz	Wenn ein Alarm erkannt wird, zeichnet der ausgewählte Kanal Videos auf.

Verknüpfungsmethode	Beschreibung
	Hinweis Der Zeitplan für die Videoaufzeichnung muss für den Kanal aktiviert sein, andernfalls wäre diese Verknüpfung ungültig. Sie können zu System → Speicherverwaltung → Speicherplan → Videoaufzeichnung gehen, um den Zeitplan für die Videoaufzeichnung zu konfigurieren.

9. Optional: Legen Sie einen **Schutzbereich** fest, wenn **AI by NVR** aktiviert ist. Nachdem ein Schutzbereich festgelegt wurde, analysiert das Gerät das Verhalten des Ziels in diesem Bereich nicht, so dass die Perimeterschutz-Ereignisse innerhalb dieses Bereichs nicht ausgelöst werden.
10. Klicken Sie auf **Speichern**.

Was ist als nächstes zu tun?

Sie können die **Live-Ansicht** aufrufen und auf **Ziel** klicken, um Alarme in Echtzeit anzuzeigen.

13.1.3 Ereignis mit abnormalem Verhalten

Bevor Sie beginnen

Stellen Sie sicher, dass die Kamera diese Funktion unterstützt.

Schritte

1. Gehen Sie zu **Smart Analysis** → **Smart Event Settings** → **Other Event**.
2. Wählen Sie eine Kamera
3. Wählen Sie einen Ereignistyp.
4. Schalten Sie **Enable** ein.
5. Klicken Sie auf **Regeleinstellungen**, um die Regel festzulegen.

Tabelle 13-7 Ereignisse mit abnormalem Verhalten

Name des Ereignisses	Ereignis Beschreibung	Regel-Konfiguration
Erkennung von Herumlungen	Die Herumlunger-Erkennung wird	1. Wählen Sie eine Regelnummer aus.

	verwendet, um zu erkennen, ob sich ein Ziel länger als die eingestellte Zeit in einem bestimmten Bereich aufhält, und um einen Alarm für damit verbundene Aktionen auszulösen.	2. Verwenden Sie die Symbolleiste oben im Bild, um die Erkennungslinie zu zeichnen.
Parkdetektion	Die Parkerkennung dient zur Erkennung von Parkverstößen in der Umgebung, die auf Schnellstraßen und Einbahnstraßen anwendbar ist.	4. Zeitschwelle und Empfindlichkeit einstellen. Zeitschwelle Die Zeit, die das Ziel in der Region verweilt. Bei einem Wert von 10 wird ein Alarm ausgelöst, wenn das Ziel 10 s lang in der Region geblieben ist: [1-10]. Sensitivität Ähnlichkeit des Hintergrundbildes mit dem Objekt. Je höher der Wert ist, desto eher wird ein Erkennungsalarm ausgelöst.
Erkennung unbeaufsichtigten Gepäcks	Die Erkennung von unbeaufsichtigtem Gepäck erkennt die in einem vordefinierten Bereich zurückgelassenen Gegenstände wie Gepäck, Geldbörsen, gefährliche Materialien usw., und bei Auslösung des Alarms kann eine Reihe von Maßnahmen ergriffen werden.	4. Optional: Wiederholen Sie die obigen Schritte, um einen weiteren einzustellen.
Erkennung der Objektentfernung	Die Funktion zur Erkennung der Entfernung von Objekten erkennt die Objekte, die aus einem vordefinierten Bereich, z. B. den ausgestellten Exponaten, entfernt wurden, und es können eine Reihe von Maßnahmen ergriffen werden, wenn der Alarm ausgelöst wird.	

Schnelle Erkennung von Bewegungen	Die Schnellbewegungserkennung dient zur Erkennung von verdächtigen Lauf- und Verfolgungsvorgängen, überhöhter Geschwindigkeit und schneller Bewegung. Sie löst einen Alarm aus, wenn sich ein Objekt schnell bewegt, und sendet eine Benachrichtigung an den Scharfschaltungs-Host, damit die erforderlichen Maßnahmen im Voraus ergriffen werden können.	
Erkennung von Menschenansammlungen	Die Erkennung von Menschenansammlungen dient dazu, festzustellen, ob die Dichte menschlicher Körper innerhalb eines bestimmten Bereichs den festgelegten Wert überschreitet, und einen Alarm für entsprechende Maßnahmen auszulösen.	1. Wählen Sie eine Regelnummer aus. 2. Verwenden Sie die Symbolleiste oben im Bild, um die Erkennungslinie zu zeichnen. 3. Prozentsatz festlegen. Der Prozentsatz ist die Dichte der menschlichen Körper innerhalb des Bereichs. Wenn sie den Schwellenwert überschreitet, löst das Gerät einen Alarm aus. 4. Optional: Wiederholen Sie die obigen Schritte, um einen weiteren einzustellen.

6. Klicken Sie auf **Scharfschaltplan**, um einen Scharfschaltplantyp auszuwählen.

Hinweis

Wenn Sie "**Scharfschaltplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf den Zeitbalken ziehen, um einen benutzerdefinierten Scharfschaltplan einzustellen, oder Sie bewegen den Cursor auf den Zeitbalken und klicken auf **00:00-24:00** , um einen bestimmten Zeitplan einzustellen.

7. Klicken Sie auf **Verknüpfungsmethode**, um Verknüpfungsmethoden festzulegen.

Tabelle 13-8 Verknüpfungsmethode Beschreibung

Verknüpfungsmethode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Alarm-Pop-up-Fenster	Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Alarm-Pop-up-Fenster an.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarmeingang, die Bewegungserkennung, die Erkennung von Videomanipulationen, die Gesichtserkennung, die Erkennung von Linienüberquerungen und andere Ereignisse ausgelöst werden.
Datensatz	Wenn ein Alarm erkannt wird, zeichnet der ausgewählte Kanal Videos auf. Hinweis Der Zeitplan für die Videoaufzeichnung muss für den Kanal aktiviert sein, andernfalls wäre diese Verknüpfung ungültig. Sie können zu System → Speicherverwaltung → Speicherplan → Videoaufzeichnung gehen, um den Zeitplan für die Videoaufzeichnung zu konfigurieren.

8. Klicken Sie auf **Speichern**.

13.1.4 Zielereignis

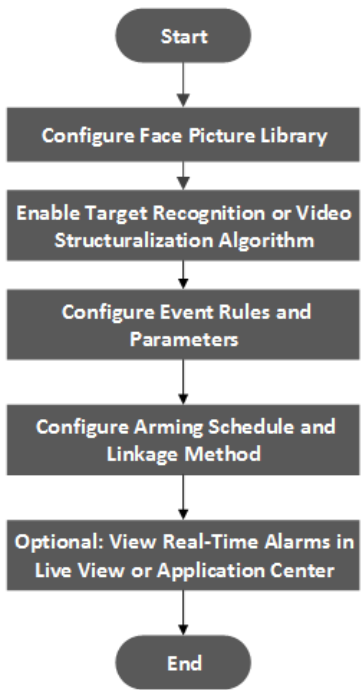
Bevor Sie beginnen

Stellen Sie sicher, dass die angeschlossene Kamera diese Funktion unterstützt oder dass die Geräte-Engine den Algorithmus **für die Zielerkennung** oder die **Videostrukturierung** unter **System** → **Intelligente Einstellungen** → **Algorithmuskonfiguration** → **Algorithmusverwaltung** aktiviert hat.

Schritte

1. Gehen Sie zu **Ereignis-Center** →  → **Ereigniskonfiguration** → **Zielereignis**.

2. Wählen Sie eine Kamera aus.
3. Wählen Sie ein Ereignis aus.
4. Schalten **Sie Enable** ein.
5. Ereignisregeln festlegen.

Name des Ereignisses	Ereignis Beschreibung	Regel-Konfiguration
Gesichtserfassung	Die Gesichtserfassung erkennt und erfasst Gesichter, die in der Szene erscheinen. Wenn ein menschliches Gesicht erkannt wird, können Verknüpfungsaktionen ausgelöst werden.	-
Gesichtsbildvergleich	Die Funktion vergleicht erkannte Gesichtsbilder mit der angegebenen Listenbibliothek. Bei erfolgreichem Vergleich wird ein Alarm ausgelöst.	 <pre> graph TD Start([Start]) --> Step1[Configure Face Picture Library] Step1 --> Step2[Enable Target Recognition or Video Structuralization Algorithm] Step2 --> Step3[Configure Event Rules and Parameters] Step3 --> Step4[Configure Arming Schedule and Linkage Method] Step4 --> Step5[Optional: View Real-Time Alarms in Live View or Application Center] Step5 --> End([End]) </pre> Abbildung 13-5 Flussdiagramm des Gesichtsbildvergleichs

Ziel-Einstufung

Die Gesichtseinstufung wird für die Auswahl von Gesichtsbildern verwendet. Je nach Pupillendistanz, Neigungs- und Schwenkwinkel werden nur Gesichtsbilder für die Analyse verwendet, die die Anforderungen an die Einstufung erfüllen. Je größer der Pupillenabstand und je kleiner der Neigungs- und Schwenkwinkel, desto besser ist es für die Analyse.

Nicht-Echtzeit-Modus

An Orten mit hohem Personenaufkommen kann die Verarbeitungsgeschwindigkeit des Geräts

nicht schnell genug sein. **Der Nicht-Echtzeit-Modus** speichert die Echtzeitbilder im Cache und verarbeitet sie später, wenn die Maschine freie Ressourcen hat. Nach Aktivierung dieser Funktion können alle Kanäle den Gesichtsbildvergleich unterstützen. **Im Nicht-Echtzeitmodus** wird kein Echtzeitalarm ausgelöst, so dass **der Scharfschaltplan** nicht verfügbar ist.

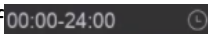
Verknüpfung erfolgreich / Verknüpfung gescheitert

Wenn der Vergleich erfolgreich war oder fehlgeschlagen ist, werden die entsprechenden Verknüpfungsaktionen ausgelöst. Sie können das Ergebnis des Echtzeit-Vergleichs in **Target of Live View** anzeigen.

Multi-Target-Type-Detektion	Die Multi-Target-Type-Erkennung ermöglicht es dem Gerät, Gesichter, menschliche Körper und Fahrzeuge gleichzeitig in einer Szene zu erkennen.	-
-----------------------------	---	---

6. Klicken Sie auf **Scharfschaltplan**, um einen Scharfschaltplantyp auszuwählen.

Hinweis

Wenn Sie "**Scharfschaltplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf den Zeitbalken ziehen, um einen benutzerdefinierten Scharfschaltplan einzustellen, oder Sie bewegen den Cursor auf den Zeitbalken und klicken auf  , um einen bestimmten Zeitplan einzustellen.

7. Klicken Sie auf **Verknüpfungsmethode**, um Verknüpfungsmethoden festzulegen.

Tabelle 13-9 Beschreibung der Verknüpfungsmethode

Verknüpfungsmethode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Alarm-Pop-up-Fenster	Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Alarm-Pop-up-Fenster an.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarmeingang, die Bewegungserkennung, die Erkennung von Videomanipulationen, die Gesichtserkennung, die Erkennung von Linienüberquerungen und andere Ereignisse ausgelöst werden.

Verknüpfungsmethode	Beschreibung
Datensatz	Wenn ein Alarm erkannt wird, zeichnet der ausgewählte Kanal Videos auf. Hinweis Der Zeitplan für die Videoaufzeichnung muss für den Kanal aktiviert sein, andernfalls wäre diese Verknüpfung ungültig. Sie können zu System → Speicherverwaltung → Speicherplan → Videoaufzeichnung gehen, um den Zeitplan für die Videoaufzeichnung zu konfigurieren.

8. Klicken Sie auf **Speichern**.

13.1.5 Wärmebildkamera-Erkennung

Der NVR unterstützt die Ereigniserkennungsmodi der Wärmebild-Netzwerk-Kameras: Feuer- und Rauchererkennung, Temperaturerkennung, Temperaturdifferenzerkennung usw.

Bevor Sie beginnen

Fügen Sie die Wärmebild-Netzwerkkamera zu Ihrem Gerät hinzu und stellen Sie sicher, dass die Kamera aktiviert ist.

Schritte

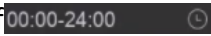
1. Gehen Sie zu **Smart Analysis** → **Smart Event Settings** → **Other Events**.
2. Wählen Sie eine Kamera aus.
3. Wählen Sie einen Ereignistyp.
4. Schalten **Sie Enable** ein.
5. Klicken Sie auf **Regeleinstellungen**, um die Regel festzulegen.

Tabelle 13-10 Thermische Ereignisse

Name der Veranstaltung	Ereignis Beschreibung
Branderkennung	Ein Alarm wird ausgelöst, wenn im Scharfschaltungsbereich ein Feuer entdeckt wird.
Temperatur-Erkennung	Ein Alarm würde ausgelöst werden, wenn die Temperatur den Schwellenwert überschreitet.

6. Klicken Sie auf **Scharfschaltplan**, um einen Scharfschaltplantyp auszuwählen.

Hinweis

Wenn Sie "**Scharfschaltplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf den Zeitbalken ziehen, um einen benutzerdefinierten Scharfschaltplan einzustellen, oder Sie bewegen den Cursor auf den Zeitbalken und klicken auf  , um einen bestimmten Zeitplan einzustellen.

7. Klicken Sie auf **Verknüpfungsmethode**, um Verknüpfungsmethoden festzulegen.

Tabelle 13-11 Verknüpfungsmethode Beschreibung

Verknüpfungsmethode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Alarm-Pop-up-Fenster	Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Alarm-Pop-up-Fenster an.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarmeingang, die Bewegungserkennung, die Erkennung von Videomanipulationen, die Gesichtserkennung, die Erkennung von Linienüberquerungen und andere Ereignisse ausgelöst werden.
Datensatz	Wenn ein Alarm erkannt wird, zeichnet der ausgewählte Kanal Videos auf. Hinweis Der Zeitplan für die Videoaufzeichnung muss für den Kanal aktiviert sein, andernfalls wäre diese Verknüpfung ungültig. Sie können zu System → Speicherverwaltung → Speicherplan → Videoaufzeichnung gehen, um den Zeitplan für die Videoaufzeichnung zu konfigurieren.

8. Klicken Sie auf **Speichern**.

13.1.6 Alarmeingang Ereignis

Legen Sie fest, wie ein Alarm eines externen Sensors behandelt werden soll.

Schritte

1. Gehen Sie zu **Ereigniszentrum** →  → **Normales Ereignis** → **Alarmeingang**.
2. Wählen Sie einen Alarmeingangsnamen.

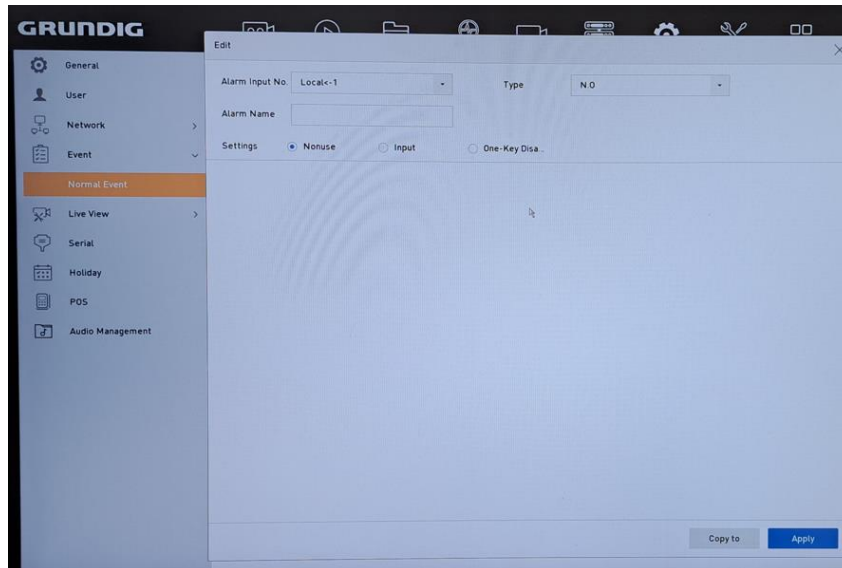


Abbildung 13-6 Alarmeingang konfigurieren

Hinweis

Beispiel: **Lokal<-1** bedeutet, dass die Nummer des Alarmeingangs an der Geräterückseite 1 ist.

3. **Alarmname** bearbeiten.
 4. Schalten **Sie Enable** ein.
 5. **Schnellentschärfung** einstellen. Die Schnellentschärfung kann die ausgewählten Alarmverknüpfungsmethoden in einem Stapel deaktivieren.
 6. **Alarmtyp** einstellen.
-

Hinweis

Beziehen Sie sich auf die Alarmquelle, um den Alarmtyp korrekt zu konfigurieren.

N.O

Wenn sich die Kontakte im stromlosen Zustand befinden und zwei Kontakte ausgeschaltet sind, können sie als normal offen bezeichnet werden.

N.C.

Wenn sich die Kontakte im stromlosen Zustand befinden und zwei Kontakte miteinander verbunden sind, können sie als normal geschlossen bezeichnet werden.

7. Klicken Sie auf **Scharfschaltplan**, um einen Scharfschaltplantyp auszuwählen.

Hinweis

Wenn Sie "**Scharfschaltplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf den Zeitbalken ziehen, um einen benutzerdefinierten Scharfschaltplan einzustellen, oder Sie bewegen den Cursor auf den Zeitbalken und klicken auf **00:00-24:00** , um einen bestimmten Zeitplan einzustellen.

8. Klicken Sie auf **Verknüpfungsmethode**, um Verknüpfungsmethoden festzulegen.

Tabelle 13-12 Verknüpfungsmethode Beschreibung

Verknüpfungsmethode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Alarm-Pop-up-Fenster	Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Alarm-Pop-up-Fenster an.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarmeingang, die Bewegungserkennung, die Erkennung von Videomanipulationen, die Gesichtserkennung, die Erkennung von Linienüberquerungen und andere Ereignisse ausgelöst werden.
Datensatz	Wenn ein Alarm erkannt wird, zeichnet der ausgewählte Kanal Videos auf. Hinweis Der Zeitplan für die Videoaufzeichnung muss für den Kanal aktiviert sein, andernfalls wäre diese Verknüpfung ungültig. Sie können zu System → Speicherverwaltung → Speicherplan → Videoaufzeichnung gehen, um den Zeitplan für die Videoaufzeichnung zu konfigurieren.

9. Klicken Sie auf **Speichern**.

13.1.7 Ereignis Audioanalyse

Schritte

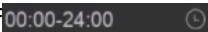
1. Gehen Sie zu **Smart Analysis** → **Smart Event Settings** → **Other Events**.
2. Wählen Sie einen Kanal.
3. Wählen Sie einen Ereignistyp.
4. Schalten Sie **Enable** ein.
5. Klicken Sie auf **Regeleinstellungen**, um die Regel festzulegen.

Tabelle 13-13 Audioanalyse-Ereignis

Name des Ereignisses	Ereignis Beschreibung	Regel-Konfiguration
Audio-Ausnahme-Erkennung	Die Audio-Ausnahmeerkennung erkennt anormale Geräusche in der Szene, z. B. eine plötzliche Zunahme/Abnahme der Lautstärke.	Erkennung eines plötzlichen Anstiegs der Tonintensität Erkennt einen steilen Tonanstieg in der Szene. Plötzliche Verringerung der Schallintensität Erkennung eines steilen Schallabfalls in der Szene. Empfindlichkeit Je höher der Wert ist, desto leichter kann der Erkennungsalarm ausgelöst werden. Schallintensitätsschwelle Sie kann den Schall in der Umgebung filtern. Je lauter die Umgebungsgeräusche sind, desto höher sollte der Wert sein. Stellen Sie ihn entsprechend der Umgebung ein.

6. Klicken Sie auf **Scharfschaltplan**, um einen Scharfschaltplantyp auszuwählen.

Hinweis

Wenn Sie "**Scharfschaltplan**" als "**Benutzerdefiniert**" eingestellt haben, können Sie den Cursor auf den Zeitbalken ziehen, um einen benutzerdefinierten Scharfschaltplan einzustellen, oder den Cursor auf den Zeitbalken bewegen und auf  klicken, um einen bestimmten Zeitplan einzustellen.

7. Klicken Sie auf **Verknüpfungsmethode**, um Verknüpfungsmethoden festzulegen.

Tabelle 13-14 Verknüpfungsmethode Beschreibung

Verknüpfungsmethode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ausnahme- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host

Verknüpfungsmethode	Beschreibung
	bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Alarm-Pop-up-Fenster	Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Alarm-Pop-up-Fenster an.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarmeingang, die Bewegungserkennung, die Erkennung von Videomanipulationen, die Gesichtserkennung, die Erkennung von Linienüberquerungen und andere Ereignisse ausgelöst werden.
Datensatz	Wenn ein Alarm erkannt wird, zeichnet der ausgewählte Kanal Videos auf. Hinweis Der Zeitplan für die Videoaufzeichnung muss für den Kanal aktiviert sein, andernfalls wäre diese Verknüpfung ungültig. Sie können zu System → Speicherverwaltung → Speicherplan → Videoaufzeichnung gehen, um den Zeitplan für die Videoaufzeichnung zu konfigurieren.

8. Klicken Sie auf **Speichern**.

13.2 Konfiguration des Gestänges

Konfigurieren Sie die Parameter für Ereigniskopplungen.

Schritte

1. Gehen Sie zu **Event Center** →  → **Linkage Configuration**.
2. Klicken Sie auf **E-Mail**, um die E-Mail-Parameter zu konfigurieren.

Tabelle 13-15 E-Mail-Verknüpfung

Bezeichnung	Beschreibung
Server-Authentifizierung	Aktivieren Sie diese Option, wenn der SMTP-Server eine Benutzerauthentifizierung erfordert, und geben Sie den Benutzernamen und das Passwort entsprechend ein.

SMTP-Server	Die IP-Adresse des SMTP-Servers oder der Hostname (z. B. smtp.263xmail.com).
SMTP-Anschluss	Der SMTP-Anschluss. Der Standard-TCP/IP-Port für SMTP ist 25.
SSL/TLS aktivieren	Aktivieren Sie SSL/TLS, wenn der SMTP-Server diese Anforderung erfüllt.
Sender	Der Name des Absenders.
Adresse des Absenders	Die Adresse des Absenders.
Empfänger auswählen	Wählen Sie den Empfänger aus. Es können bis zu 3 Empfänger konfiguriert werden.
Beigefügtes Bild	Senden Sie eine E-Mail mit angehängten Alarmbildern.
Aktivieren Sie 3 angehängte Bilder für den Perimeterschutz	Wenn ein Perimeterschutz-Ereignis ausgelöst wird, sendet das Gerät eine E-Mail mit 3 angehängten Alarmbildern.
Intervall	Das Zeitintervall für die Erfassung der angehängten Bilder.

3. Klicken Sie auf **Audioverwaltung**, um Audiodateien für die Alarmverknüpfung zu verwalten.

Hinweis

Es gibt 3 Standard-Audiodateien in der Liste, die nicht gelöscht werden können. Sie können Audiodateien von einem USB-Stick importieren. Die Dateien müssen im AAC- oder MP3-Format vorliegen, und jede Datei sollte nicht größer als 1 MB sein.

4. Klicken Sie auf **Alarmausgang**, um die Parameter für den Alarmausgang einzustellen.

Hinweis

- Klicken Sie auf den Namen des jeweiligen Alarmausgangs, um ihn zu bearbeiten.
- Die Alarmausgangsnummer ist die gleiche wie die an der Geräterückseite. Zum Beispiel bedeutet "**Lokal->1**" den Alarmausgang Nr. 1 auf der Geräterückseite.

Verzögerung

Die Dauer des Alarmsignals.

Alarm-Status

Klicken Sie auf **Auslösen**, um den Status zu wechseln.

5. Klicken Sie auf **Alarm-Host**, um die Parameter des Sicherheitskontrollfelds einzustellen.

6. Klicken Sie auf **Blinklicht-Alarmausgang**, um das Blinklicht der Kamera einzustellen.

7. Klicken Sie auf **Audio-Alarmausgang**, um den Lautsprecher der Kamera einzustellen.

13.3 Ereignissuche

Sie können Ereignisdateien wie Videos und Bilder entsprechend den Suchbedingungen durchsuchen.

Schritte

1. Gehen Sie zu **Event Center** → 

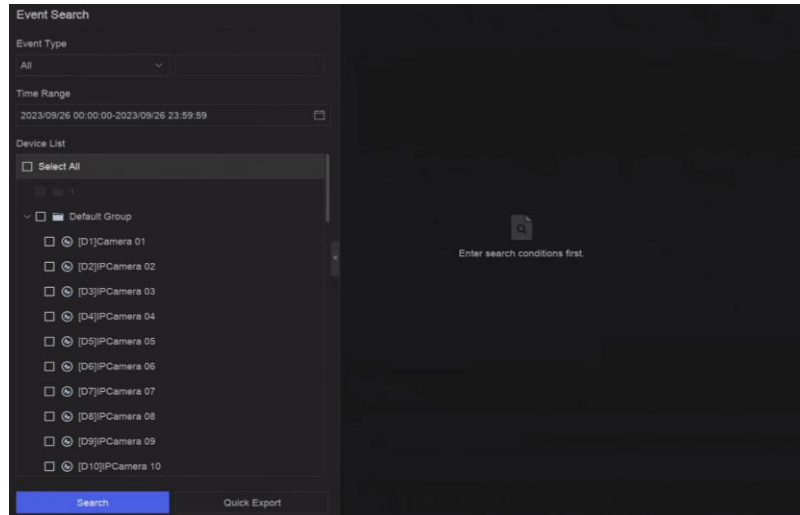


Abbildung 13-7 Ereignissuche

2. Geben Sie detaillierte Bedingungen an, einschließlich Ereignistyp, Zeit, Kanal usw.
3. Klicken Sie auf **Suchen**.

Das Gerät zeigt die Suchergebnisse des/der ausgewählten Kanals/Kanäle an.

Was ist als nächstes zu tun?

Wählen Sie die Elemente aus der Ergebnisliste aus und exportieren Sie sie zur Sicherung.

13.4 Alarme anzeigen

Sie können Alarmvideos und -bilder in Echtzeit ansehen und abspielen.

Schritte

1. Gehen Sie zu **Event Center** → 
2. Klicken Sie auf **Real-Time Alarm**.
3. Wählen Sie den Alarm aus der Liste aus.

Wenn es zu viele Alarme gibt, klicken Sie auf **Filter**, um den Alarm zu suchen und zu finden.

4. Klicken Sie auf **Wiedergabe**, und das Video der Alarmaufnahme wird wiedergegeben.
5. Zeigen Sie das/die Alarmbild(er) auf der rechten Seite an. Die Anzahl der verfügbaren Bilder wird angezeigt.

14 Suche und Sicherung

Sie können Dateien nach verschiedenen Suchbedingungen durchsuchen, z. B. nach Dateityp, Ereignistyp, Zeit, Tag usw. Die Suchergebnisse können auf ein anderes Gerät exportiert werden, z. B. auf einen USB-Stick.

Bevor Sie beginnen

Vergewissern Sie sich, dass die Festplatte korrekt installiert ist und die Aufzeichnungsparameter richtig konfiguriert sind.

Schritte

1. Gehen Sie zu **Backup**.

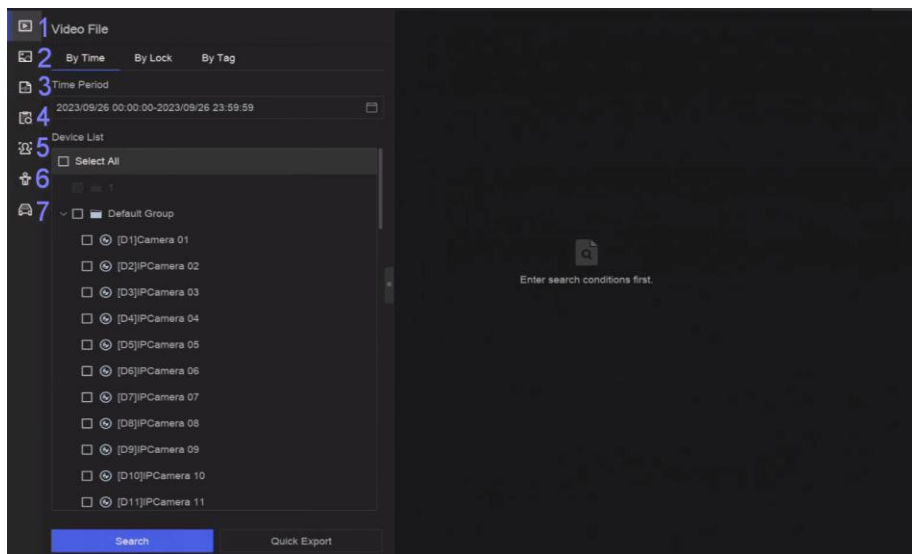


Abbildung 14-1 Suche und Sicherung

2. Wählen Sie auf der linken Seite die gewünschte Suchmethode aus, es werden mehrere Arten unterstützt.

Hinweis

Die Suchbedingungen variieren je nach der gewählten Suchmethode.

3. Legen Sie die Suchbedingungen fest.
4. Klicken Sie auf **Suchen**.

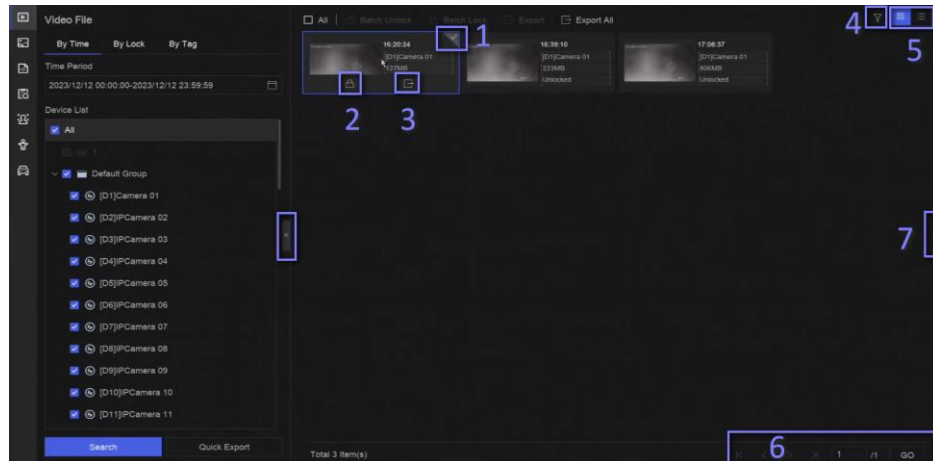


Abbildung 14-2 Suchergebnis

5. Optional: Führen Sie die folgenden Vorgänge durch.

- 1 Klicken Sie auf , um eine Datei auszuwählen.
- 2 Klicken Sie auf , um eine Datei zu sperren. Nachdem eine Datei gesperrt wurde, kann sie nicht mehr überschrieben werden.
- 3 Klicken Sie auf , um eine Datei zu exportieren.
- 4 Verwenden Sie die Symbolleiste am oberen Rand, um die Ergebnisse nach Kanal zu filtern.
- 5 Verwenden Sie die Symbolleiste am oberen Rand, um den Anzeigeeffekt zu ändern.
- 6 Gehen Sie zu verschiedenen Ergebnisseiten.
- 7 Erweitern oder reduzieren Sie die Schnittstelle. Nachdem Sie ein Video aus der Ergebnisliste ausgewählt haben, können Sie es schnell wiedergeben.

6. Schließen Sie ein USB-Flash-Laufwerk zur Sicherung an das Gerät an.

7. Exportieren Sie Dateien auf den USB-Stick.

- Wählen Sie die Dateien in der Ergebnisliste aus und klicken Sie auf **Exportieren**.
- Klicken Sie auf **Alle exportieren**, um alle Dateien zu exportieren.

15 Intelligente Einstellungen

15.1 Algorithmus-Verwaltung

Algorithmen werden für Geräte-Engines verwendet, um verschiedene intelligente Funktionen zu analysieren. Intelligente Funktionen können genutzt werden, nachdem der entsprechende Algorithmus einer Engine zugewiesen wurde.

Gehen Sie zu **Intelligente Analyse** → **Motoreinstellungen**. Die verfügbaren Algorithmen werden aufgelistet, und Sie können auf den gewünschten Algorithmus klicken, um die Engine(s) zu verknüpfen.

15.2 Verwaltung der Listenbibliothek

Die Listenbibliothek wird hauptsächlich für die Speicherung von Zielbildern und den Zielvergleich verwendet. Die Bibliothek "**Fremde**" wird zum Speichern von Bildern für Fremde verwendet und kann nicht gelöscht werden.

15.2.1 Hinzufügen einer Listenbibliothek

Schritte

1. Gehen Sie zu **Intelligente Analyse** → **Gesichtsbildbibliothek**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie den Namen der Bibliothek ein.
4. Klicken Sie auf **Bestätigen**.

Hinweis

- Nach einer Listenbibliothek können Sie den Cursor auf die Bibliothek bewegen, um sie zu bearbeiten oder zu löschen.
 - Sie können auf **Stapelweise löschen** klicken, um ausgewählte Bibliotheken zu löschen, oder alle Bilder in den ausgewählten Bibliotheken löschen.
-

15.2.2 Hochladen von Gesichtsbildern in die Bibliothek

Der Zielbildvergleich basiert auf den Zielbildern in der Bibliothek. Sie können ein einzelnes Zielbild hochladen oder mehrere Zielbilder in die Bibliothek importieren.

Bevor Sie beginnen

- Stellen Sie sicher, dass das Bildformat JPEG oder JPG ist.
- Importieren Sie alle Bilder im Voraus auf ein Sicherungsgerät.

Schritte

1. Doppelklicken Sie auf eine Listenbibliothek.
2. Wahlweise: Klicken Sie auf **Benutzerdefinierte Markierung**, um den Bildern Markierungen hinzuzufügen. Die Markierung kann nach Ihren Wünschen bearbeitet werden, z. B. persönliche Informationen, Organisation, Position usw.
3. Klicken Sie auf **Hinzufügen** oder **Importieren**.
4. Bild(er) importieren.
 - **Hinzufügen:** Klicken Sie auf , um ein Bild nach dem anderen hochzuladen. Wenn das Bild mehrere Ziele hat, müssen Sie eines davon auswählen.
 - **Importieren:** Es können mehrere Bilder auf einmal importiert werden. Das Gerät verwendet den Dateinamen als Bildnamen und lässt andere Attribute leer, oder es importiert Bilddateien nach bestimmten Regeln. Wenn ein Bild mehrere Ziele enthält, wählt das Gerät standardmäßig das Ziel in der Mitte.
5. Optional: Führen Sie die folgenden Vorgänge durch.

Bilder aus der Bibliothek löschen	• Wählen Sie ein Bild aus und löschen Sie es. • Wählen Sie Bilder aus und klicken Sie auf Stapelweise löschen, um die ausgewählten Bilder zu löschen.
--	---

Bilder in der Bibliothek suchen	Klicken Sie in der Symbolleiste auf  , um Bilder zu suchen.
--	--

Bilder in eine andere Bibliothek kopieren	Wählen Sie Bilder aus und klicken Sie auf Kopieren , um die hochgeladenen Bilder der aktuellen Bibliothek in eine andere Bibliothek zu kopieren.
--	---

Bilder bearbeiten	Klicken Sie auf den Namen des Bildes und bearbeiten Sie seine Attribute.
--------------------------	--

Bilder exportieren	Wählen Sie Bilder aus, und klicken Sie auf Exportieren , um sie auf einen USB-Stick zu exportieren.
---------------------------	--

16 Anwendungszentrum

16.1 Erkennung von Personen und Fahrzeugen

Die Personen- und Fahrzeuginformationen werden für den ausgewählten Kanal in Echtzeit angezeigt.

Die Personen- und Fahrzeugerkennung sollte im Voraus konfiguriert werden. Gehen Sie zum Konfigurieren zu **System → Ereignis** .



Abbildung 16-1 Erkennung von Personen und Fahrzeugen

Tabelle 16-1 Personen- und Fahrzeugdetektion Beschreibung

Nr.	Beschreibung
1	Klicken Sie mit der rechten Maustaste, um die Menüleiste anzuzeigen.
2	Einstellungen für die Erkennung von Personen und Fahrzeugen. Sie können das Layout, die Aufforderung zum erfolgreichen Vergleich und die Ressourcenkanäle einstellen.
3	Vollbildmodus aufrufen/verlassen.

16.2 Personen-Check-In

Nach dem Hinzufügen von Check-in-Aufgaben können Sie die Live-Check-in-Informationen anzeigen und Check-in-Ergebnisse suchen.

16.2.1 Check-In Aufgabe

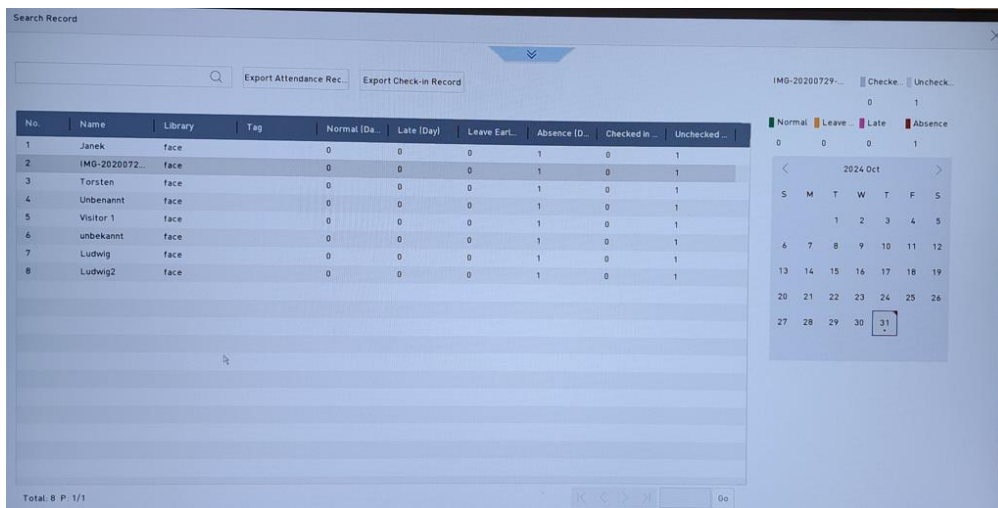
Bevor Sie mit dem Einchecken von Personen beginnen, sollte die entsprechende Aufgabe richtig konfiguriert sein.

Bevor Sie beginnen

- Eine Kamera für die Personenkontrolle ist ordnungsgemäß angeschlossen.
- Gehen Sie zu **Intelligente Analyse** → **Intelligente Ereignisseinstellungen** → **Gesichtserkennung**. Weisen Sie die **Zielerfassung** mindestens einer Engine zu.
- Die Listenbibliothek für den Check-in-Vergleich ist richtig konfiguriert. Einzelheiten finden Sie unter [Hinzufügen einer Listenbibliothek](#).

Schritte

1. Klicken Sie auf **Person Passing**.
2. Klicken Sie auf **Datensatz suchen**.
4. Wählen Sie Kamera und Zeitbereich und klicken Sie auf **Suchen**.



The screenshot shows the 'Search Record' window. It contains a table with columns: No., Name, Library, Tag, Normal (Da...), Late (Day), Leave Eart..., Absence (D...), Checked in..., and Unchecked... The table lists 8 records. To the right of the table is a calendar for October 2024, with the 31st highlighted. Below the calendar are buttons for 'Normal', 'Leave', 'Late', and 'Absence'.

No.	Name	Library	Tag	Normal (Da...)	Late (Day)	Leave Eart...	Absence (D...)	Checked in...	Unchecked...
1	JaneK	face		0	0	0	1	0	1
2	IMG-2020072...	face		0	0	0	1	0	1
3	Torsten	face		0	0	0	1	0	1
4	Unbenannt	face		0	0	0	1	0	1
5	Visitor 1	face		0	0	0	1	0	1
6	unbekannt	face		0	0	0	1	0	1
7	Ludwig	face		0	0	0	1	0	1
8	Ludwig2	face		0	0	0	1	0	1

Abbildung 16-2 Check-In Aufgabe

16.2.2 Check-In-Datensätze suchen

Nachdem die Check-in-Aufgaben konfiguriert sind, können Sie die Datensätze nach Tag oder Monat durchsuchen.

Bevor Sie beginnen

Stellen Sie sicher, dass die Check-in-Aufgaben konfiguriert sind.

Schritte

1. Gehen Sie zu **Person Check-In**.
2. Klicken Sie mit der rechten Maustaste, um das Menü auf der linken Seite anzuzeigen.
3. Klicken Sie auf .

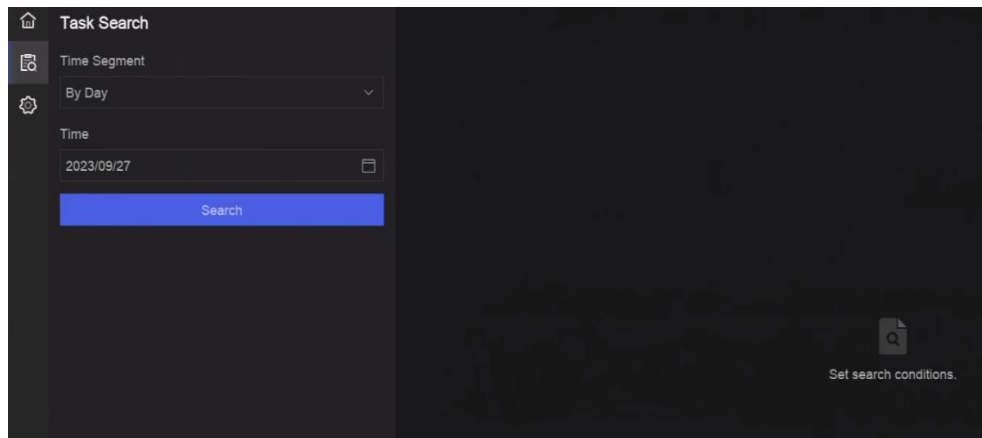


Abbildung 16-3 Suche nach Eincheck-Datensätzen

4. Zeit einstellen.
5. Klicken Sie auf **Suchen**.

16.3 Statistischer Bericht

Sie können Berichte über Personenzählungen und Heatmaps einsehen.

Tabelle 17-2 Einführung in den Statistikbericht

Funktion Name	Symbol	Zustand	Beschreibung
Personenzählung		- Die Funktion muss von der angeschlossenen IP-Kamera unterstützt werden. Zum Beispiel ist eine Personenzählkamera an Ihr Gerät angeschlossen. - Die statistischen Daten der Kamera können auf der Festplatte des Geräts gespeichert werden.	Die Personenzählung berechnet die Anzahl der Personen, die einen bestimmten konfigurierten Bereich betreten oder verlassen, und erstellt tägliche/wöchentliche/monatliche/jährliche Berichte zur Analyse.
Wärmekarte		- Die Funktion muss von der angeschlossenen IP-Kamera unterstützt werden. - Die statistischen Daten der Kamera können auf der Festplatte des Geräts gespeichert werden.	Eine Heatmap ist eine grafische Darstellung von Daten. Die Heatmap-Funktion wird verwendet, um zu analysieren, wie viele Personen ein bestimmtes Gebiet besucht und sich dort aufgehalten haben.

17 Systemparametereinstellungen

Zu den Systemparametern gehören der Gerätename, die Uhrzeit, die Zeit der Bildschirmsperre, die Sprache usw.

Gehen Sie zu **System** → **Systemeinstellungen** → **Systemkonfiguration**, um die Parameter zu konfigurieren.

Tabelle 17-1 Parameterbeschreibung

Typ	Parameter Name	Beschreibung
Grundlegende Informationen	Bildschirm sperren Zeit	Der Bildschirm wird gesperrt, wenn sich der Cursor eine bestimmte Zeit lang nicht bewegt.
	Live-Ansichtsberechtigung auf dem Sperrbildschirm	Nach dem Sperren des Bildschirms gibt das Gerät das Live-Bild der Kameras wieder, die diese Berechtigung haben.
Zeit Konfiguration	Zeitsynchronisationsmodus	NTP-Zeitsynchronisation Ihr Gerät kann eine Verbindung zu einem Netzwerk-Zeitprotokollserver herstellen, um die Genauigkeit der Systemzeit zu gewährleisten. Manuelle Zeitsynchronisation. Manuelles Einstellen der Systemzeit.
Menü Ausgabe	Auto-Switch für Hilfsanschluss	Wenn zwei oder mehr Monitore an der Rückseite angeschlossen sind, kann einer der Monitore zum Hilfsausgang werden, der das Hauptmenü nicht aufrufen kann. Die Bilder in den Fenstern des Hilfsausgangs werden automatisch entsprechend dem Intervall auf die nächsten Bilder umgeschaltet.
Kanal-Null	-	Kanal-Null, bekannt als virtueller Kanal, kann Live-Bilder von allen Kanälen des Geräts zeigen, was Bandbreite für die Übertragung spart.
RS-232	Verwendung	Konsole Nach dem Anschluss an den PC mit einem Konverter kann der PC die Geräteparameter einstellen. Transparenter Kanal Er ist direkt mit einem seriellen Gerät verbunden. Der PC kann aus der Ferne über das Netzwerk auf das serielle Gerät zugreifen.

18 Hot Spare-Gerätesicherung

Der Videorecorder GD-RN-DT8864N kann ein N+M Hot-Spare-System bilden. Das System besteht aus mehreren Arbeitsvideorekordern und mindestens einem Hot Spare-Videorecorder. Wenn ein funktionierender Videorecorder ausfällt, wird der Hot-Spare-Videorecorder in Betrieb genommen, was die Zuverlässigkeit des Systems erhöht. Zwischen dem/den Hot-Spare-Videorecorder(n) und dem Arbeitsvideorecorder muss eine bidirektionale Verbindung hergestellt werden, die in der folgenden Abbildung dargestellt ist.

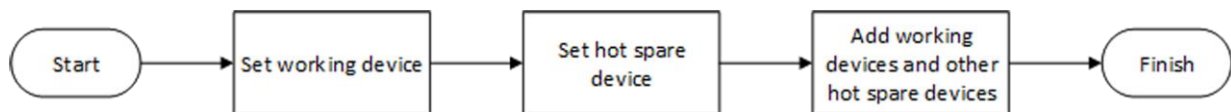


Abbildung 18-1 Aufbau eines Hot-Spare-Systems

Hinweis

- Es sind bis zu 32 Arbeitsgeräte und 32 Hot-Spare-Geräte zulässig.
 - Aus Kompatibilitätsgründen wird empfohlen, alle Geräte desselben Modells zu verwenden. Wenden Sie sich an Ihren Händler, um Einzelheiten zu den Modellen zu erfahren, die die Hot-Spare-Funktion unterstützen.
-

18.1 Arbeitsgerät einstellen

Schritte

1. Gehen Sie zu **System** → **Systemverwaltung** → **N+M Hot Spare**.
2. Stellen Sie den **Arbeitsmodus** als **Normalmodus** ein.
3. Schalten Sie **Enable** ein.
4. Klicken Sie auf **Speichern**.
5. Optional: Anzeigen der **IP-Adresse des Hot-Spare-Geräts** und des **Arbeitsstatus des Hot-Spare-Geräts**.

18.2 Hot Spare Gerät einstellen

Das Hot-Spare-Gerät übernimmt die Aufgaben des Arbeitsgeräts, wenn das Arbeitsgerät ausfällt.

Schritte

1. Gehen Sie zu **System** → **Systemverwaltung** → **N+M Hot Spare**.
2. **Arbeitsmodus** als **Hot Spare Modus** einstellen.

3. Klicken Sie auf **Speichern**. Ihr Gerät wird automatisch neu gestartet.

Hinweis

- Die Kameraverbindung wird deaktiviert, wenn das Gerät im Hot-Spare-Modus arbeitet.
 - Es wird dringend empfohlen, die Standardeinstellungen des Geräts wiederherzustellen, nachdem der Arbeitsmodus von Hot-Spare-Geräten auf den Normalmodus umgestellt wurde, um den normalen Betrieb zu gewährleisten.
-

4. Gehen Sie erneut zu **System** → **Systemverwaltung** → **N+M Hot Spare**.

5. Fügen Sie dem Hot-Spare-System funktionierende Geräte hinzu.

6. Fügen Sie Hot-Spare-Geräte zum Hot-Spare-System hinzu.

7. Klicken Sie auf **Speichern**.

19 Systemereignis konfigurieren

Systemereignisse können so konfiguriert werden, dass sie den Ereignishinweis in der Live-Ansicht übernehmen und Alarmausgaben und Verknüpfungsaktionen auslösen.

Schritte

1. Gehen Sie zu **System → Ereignis → Systemereignis**.

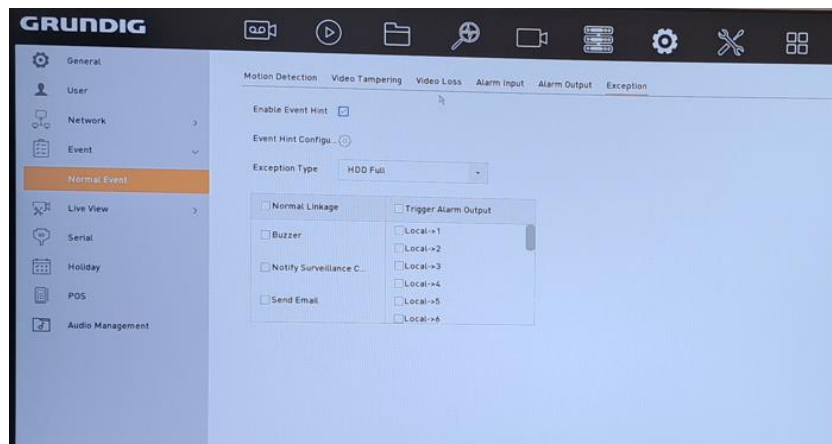


Abbildung 19-1 Konfiguration von Systemereignissen

2. Wählen Sie die Art des Ereignisses.
3. Konfigurieren Sie die Verknüpfungsmethoden.

Tabelle 20-1 Linkage Beschreibung

Verknüpfungsmethode	Beschreibung
Überwachungszentrale benachrichtigen	Das Gerät kann bei Auftreten eines Ereignisses ein Ereignis- oder Alarmsignal an den entfernten Alarm-Host senden. Der Alarm-Host bezieht sich auf den PC, auf dem die Client-Software SCMS installiert ist.
Buzzer	Wenn ein Alarm erkannt wird, gibt der Summer einen Signalton ab.
E-Mail senden	Das System kann eine E-Mail mit Alarminformationen an einen oder mehrere Benutzer senden, wenn ein Alarm erkannt wird.
Alarm Ausgang	Der Alarmausgang kann durch den Alarmeingang, die Bewegungserkennung, die Erkennung von Videomanipulationen, die Gesichtserkennung, die Erkennung von Linienüberquerungen und andere Ereignisse ausgelöst werden.

Hinweis

Wenn Systemereignisse auftreten, wird  in der oberen rechten Ecke angezeigt, und Sie können auf  klicken, um sie anzuzeigen.

4. Klicken Sie auf **Speichern**.

20 Systeminformationen anzeigen

Gehen Sie zu **Wartung** → Systeminfo → **Geräteinfo**, um die Systeminformationen anzuzeigen.



Abbildung 20-1 Systeminformationen

21 Wartung des Systems

Zu den Systemwartungsfunktionen gehören die Suche nach Protokollen, die Planung von Neustarts, Upgrades usw.

21.1 Neustart einplanen

Das Gerät wird automatisch nach dem festgelegten Zeitplan neu gestartet.

Gehen Sie zu **System** → **Systemwartung** → **Wartung** → **Neustart planen**, um die Funktion zu aktivieren und den Zeitplan für den Neustart festzulegen.

21.2 Gerät aufrüsten

Das Gerätesystem kann mit einem lokalen USB-Flash-Laufwerk, einem entfernten FTP-Server usw. aktualisiert werden.

Gehen Sie zu **System** → **Systemwartung** → **Wartung** → **Upgrade**, um Ihr Gerät zu aktualisieren.

21.3 Sicherung und Wiederherstellung

Gehen Sie zu **System** → **Systemwartung** → **Wartung** → **Sichern und Wiederherstellen**, um Systemparameter wiederherzustellen oder zu sichern.

Konfigurationsdatei importieren/exportieren

Die Gerätekonfigurationsdateien können zur Sicherung auf ein lokales Gerät exportiert werden, und die Konfigurationsdateien eines Geräts können in mehrere Geräte importiert werden, wenn diese mit denselben Parametern konfiguriert werden sollen.

Einfache Wiederherstellung

Stellen Sie alle Parameter mit Ausnahme des Netzwerks (einschließlich IP-Adresse, Subnetzmaske, Gateway, MTU, NIC-Arbeitsmodus, Standardroute, Serverport usw.) und der Benutzerkontoparameter auf die Werkseinstellungen zurück.

Werkseinstellungen

Stellen Sie alle Parameter auf die werkseitigen Standardeinstellungen zurück.

Wiederherstellen auf Inaktiv

Versetzen Sie das Gerät in den inaktiven Zustand und lassen Sie alle Einstellungen unverändert, mit Ausnahme der Wiederherstellung der Benutzerkonten.

21.4 Protokollinformationen

Gehen Sie zu **System** → **Systemwartung** → **Wartung** → **Protokoll**, um Protokollinformationen zu suchen und zu exportieren.

Abgelaufene Zeiteinstellungen

Wenn die Protokollplatte voll ist, werden Protokolle, die diesen Zeitraum überschreiten, überschrieben.

21.5 Log-Server konfigurieren

Sie können Systemprotokolle zur Sicherung auf den Server hochladen.

Schritte

1. Gehen Sie zu **System** → **CX** → **Systemeinstellungen** → **Netzwerk** → **Netzwerk** → **Protokollserver**.
2. Schalten **Sie Enable** ein.
3. Legen Sie **Upload-Zeit**, **Server-IP-Adresse** und **Port** fest.
4. Optional: Klicken Sie auf **Test**, um zu prüfen, ob die Parameter gültig sind.
5. Klicken Sie auf **Speichern**.

21.6 Wartungswerkzeuge

Für die Systemwartung stehen mehrere Tools zur Verfügung, z. B. S.M.A.R.T.-Erkennung und Erkennung fehlerhafter Sektoren.

Bevor Sie beginnen

Stellen Sie sicher, dass die Festplatte richtig installiert ist.

Schritte

1. Gehen Sie zu **System** → **Systemwartung** → **Wartung** → **Wartungswerkzeuge**.
2. Wählen Sie die Werkzeuge entsprechend Ihren Anforderungen aus.

Tabelle 21-1 Werkzeugbeschreibung

Name des Werkzeugs	Beschreibung
Überwachung von Netzwerkdaten	Die Überwachung von Netzwerkdaten ist der Prozess der Überprüfung, Analyse und Verwaltung von Netzwerkdaten auf Anomalien oder Prozesse, die die Leistung, Verfügbarkeit oder Sicherheit des Netzwerks beeinträchtigen können.

Netzwerk-Paket-Erfassung	
Erkennung des Festplattenstatus	Sie können den Gesundheitszustand einer 4 TB- bis 8 TB-Festplatte von Seagate anzeigen, die nach dem 1. Oktober 2017 erstellt wurde. Verwenden Sie diese Funktion, um Probleme mit der Festplatte zu beheben. Health Detection zeigt einen detaillierteren Festplattenstatus als die S.M.A.R.T.-Funktion.
S.M.A.R.T.-Detektion	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) sind HDD-Überwachungssysteme, die verschiedene Zuverlässigkeitsindikatoren erkennen und so Ausfälle vorhersehen können.
Erkennung von fehlerhaften Sektoren	Wenn eine Festplatte zu viele fehlerhafte Sektoren enthält, wird empfohlen, die Festplatte auszutauschen, da sonst Dateien auf der Festplatte verloren gehen können.
HDD-Klon	Kopieren Sie die Daten auf der Festplatte auf eine andere Festplatte über die eSATA-Schnittstelle.

Hinweis

Es wird empfohlen, Wartungswerkzeuge mit Hilfe des technischen Supports zu verwenden.

22 Sicherheitsmanagement

22.1 Adressfilter

Der Adressfilter entscheidet, ob der Zugriff auf Ihr Gerät für bestimmte IP-/MAC-Adressen erlaubt oder verboten ist.

Bevor Sie beginnen

Melden Sie sich mit dem Administratorkonto an.

Schritte

1. Gehen Sie zu **System** → **Systemwartung** → **Sicherheitsmanagement** → **Adressfilter**.
2. Schalten Sie **Enable** ein.
3. **Filtertyp** festlegen. Wählen Sie, ob Sie nach IP-Adresse oder MAC-Adresse filtern möchten.
4. **Einschränkungsart** festlegen. Der Gerätemechanismus erlaubt oder verbietet bestimmten IP/MAC-Adressen den Zugriff auf Ihr Gerät.
5. Optional: **Einschränkungsliste** festlegen. Sie können Adressen hinzufügen, bearbeiten oder löschen.
6. Klicken Sie auf **Speichern**.

22.2 Stream-Verschlüsselung

Nach dem Aktivieren der Stream-Verschlüsselung ist ein Verschlüsselungscode für die Remote-Live-Ansicht, die Remote-Wiedergabe und die heruntergeladenen Videos erforderlich.

Schritte

1. Gehen Sie zu **System** → **Systemwartung** → **Sicherheitsmanagement** → **Stream Encryption**.
2. Schalten Sie **Enable** ein.
3. **Verschlüsselungsschlüssel** festlegen.

Hinweis

Der Verschlüsselungscode des Streams wird mit dem Verifizierungscode des SCMS-Dienstes synchronisiert. Nach Aktivierung des Verschlüsselungscodes wird der SCMS-Stream zwangsweise verschlüsselt.

4. Klicken Sie auf **Speichern**.

22.3 TLS-Version auswählen

Die TLS-Einstellungen sind für HTTP(s) und den erweiterten SDK-Dienst wirksam. Es bietet einen sichereren Stream-Übertragungsdienst. Gehen Sie zu **System** → **Systemwartung** → **Sicherheitsmanagement** → **TLS**, um die TLS-Version auszuwählen.

23 Anhang

23.1 Liste der verwendbaren Netzteile

Verwenden Sie nur die unten aufgeführten Netzteile.

Netzadapter Modell	Spezifikationen	Hersteller
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3,33 A	Moso Power Supply Technology Co, Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1,5 A	MOSO Technology Co. Ltd.
ADS-25FSG-12 12018GPG	CE, 100 bis 240 VAC, 12 V, 1,5 A, 18 W, $\Phi 5,5 \times 2,1 \times 10$	Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1,5 A	MOSO Technology Co. Ltd.
TS-A018-120015AD	100 bis 240 VAC, 12 V, 1,5 A, 18 W, $\Phi 5,5 \times 2,1 \times 10$	Shenzhen Transin Technologies Co, Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	MOSO Technology Co. Ltd.
ADS-24S-12 1224GPG	CE, 100 bis 240 VAC, 12 V, 2 A, 24 W, $\Phi 2.1$	Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	MOSO Technology Co. Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3,33 A, 40 W	Channel Well Technology Co, Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3,33 A	MOSO Technology Co. Ltd.
MSP-Z1360IC48.0-65W	48 V, 1,36 A	MOSO Technology Co. Ltd.

Netzadapter Modell	Spezifikationen	Hersteller
KPL-050S-II	48 V, 1,04 A	Channel Well Technology Co, Ltd.

23.2 Glossar

Dual-Stream

Dual-Stream ist eine Technologie zur lokalen Aufzeichnung von hochauflösenden Videos bei gleichzeitiger Übertragung eines Streams mit geringerer Auflösung über das Netzwerk. Die beiden Streams werden vom DVR erzeugt, wobei der Hauptstream eine maximale Auflösung von 1080P und der Substream eine maximale Auflösung von CIF hat.

DVR

Akronym für Digitaler Videorekorder. Ein DVR ist ein Gerät, das in der Lage ist, Videosignale von analogen Kameras zu empfangen, das Signal zu komprimieren und es auf seinen Festplatten zu speichern.

HDD

Akronym für Hard Disk Drive. Ein Speichermedium, das digital kodierte Daten auf Platten mit magnetischer Oberfläche speichert.

DHCP

Dynamic Host Configuration Protocol (DHCP) ist ein Netzwerk-Anwendungsprotokoll, das von Geräten (DHCP-Clients) verwendet wird, um Konfigurationsinformationen für den Betrieb in einem Internet-Protokoll-Netzwerk zu erhalten.

HTTP

Akronym für Hypertext Transfer Protocol. Ein Protokoll zur Übertragung von Hypertext-Anfragen und Informationen zwischen Servern und Browsern über ein Netzwerk.

PPPoE

PPPoE, Point-to-Point Protocol over Ethernet, ist ein Netzwerkprotokoll zur Einkapselung von Point-to-Point Protocol (PPP)-Rahmen in Ethernet-Rahmen. Es wird hauptsächlich bei ADSL-Diensten verwendet, bei denen einzelne Benutzer über Ethernet eine Verbindung zum ADSL-Transceiver (Modem) herstellen, sowie in einfachen Metro-Ethernet-Netzen.

DDNS

Dynamisches DNS ist eine Methode, ein Protokoll oder ein Netzdienst, der es einem vernetzten Gerät, z. B. einem Router oder einem Computersystem, das die Internet Protocol Suite verwendet, ermöglicht, einen Domänennamenserver zu benachrichtigen, um die aktive DNS-Konfiguration seiner konfigurierten Hostnamen, Adressen oder anderen im DNS gespeicherten Informationen in Echtzeit (ad hoc) zu ändern.

Hybrid-DVR

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

NTP

Akronym für Network Time Protocol. Ein Protokoll, mit dem die Uhren von Computern über ein Netzwerk synchronisiert werden.

NTSC

Akronym für National Television System Committee. NTSC ist eine analoge Fernsehnorm, die in Ländern wie den Vereinigten Staaten und Japan verwendet wird. Jedes Bild eines NTSC-Signals enthält 525 Zeilen bei 60 Hz.

NVR

Akronym für Netzwerk-Videorekorder. Ein NVR kann ein PC-basiertes oder eingebettetes System sein, das für die zentrale Verwaltung und Speicherung von IP-Kameras, IP-Domes und anderen DVRs verwendet wird.

PAL

Akronym für Phase Alternating Line. PAL ist ein weiterer Videostandard, der in weiten Teilen der Welt für Fernsehsysteme verwendet wird. Das PAL-Signal enthält 625 Abtastzeilen bei 50 Hz.

PTZ

Akronym für Schwenken, Neigen, Zoomen. PTZ-Kameras sind motorbetriebene Systeme, die es der Kamera ermöglichen, nach links und rechts zu schwenken, nach oben und unten zu neigen und hinein- und herauszuzoomen.

USB

Akronym für Universal Serial Bus. USB ist ein Plug-and-Play-Standard für serielle Busse zum Anschluss von Geräten an einen Host-Computer.

23.3 Häufig gestellte Fragen

23.3.1 Warum wird bei einem Teil der Kanäle in der Live-Ansicht mit mehreren Bildschirmen "Keine Ressource" angezeigt oder der Bildschirm wird schwarz?

Grund

1. Die Einstellungen für die Sub-Stream-Auflösung oder -Bitrate sind ungeeignet.
2. Verbinden des Sub-Streams fehlgeschlagen.

Lösung

1. Gehen Sie zu **Kamera** → **Videoparameter** → **Sub-Stream**. Wählen Sie den Kanal aus, und verringern Sie die Auflösung und die maximale Bitrate (die Auflösung muss weniger als 720p und die maximale Bitrate weniger als 2048 Kbps betragen).

Hinweis

Wenn Ihr Videorecorder diese Funktion nicht unterstützt, können Sie sich bei der Kamera anmelden und die Videoparameter über den Webbrowser einstellen.

2. Legen Sie die Auflösung und die maximale Bitrate des Sub-Streams richtig fest (die Auflösung muss weniger als 720p und die maximale Bitrate weniger als 2048 Kbps betragen), löschen Sie den Kanal und fügen Sie ihn wieder hinzu.

2433.2 Warum meldet der Videorecorder ein riskantes Passwort, nachdem eine Netzwerkkamera hinzugefügt wurde?

Grund

Das Passwort der Kamera ist zu schwach.

Lösung

Ändern Sie das Passwort der Kamera.

Warnung

Wir empfehlen Ihnen dringend, ein sicheres Passwort Ihrer Wahl zu erstellen (mit mindestens 8 Zeichen, darunter mindestens drei der folgenden Kategorien: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen), um die Sicherheit Ihres Produkts zu erhöhen. Und wir empfehlen Ihnen, Ihr Passwort regelmäßig zurückzusetzen, besonders im Hochsicherheitssystem kann das monatliche oder wöchentliche Zurücksetzen des Passworts Ihr Produkt besser schützen.

23.3.3 Warum meldet der Videorecorder, dass der Streamtyp nicht unterstützt wird?

Grund

Das Kodierungsformat der Kamera stimmt nicht mit dem des Videorecorders überein.

Lösung

Wenn die Kamera H.265/MJPEG für die Kodierung verwendet, der Videorecorder aber H.265/MJPEG nicht unterstützt, ändern Sie das Kodierungsformat der Kamera in das gleiche wie das des Videorecorders.

23.3.4 Wie kann ich bestätigen, dass der Videorecorder H.265 für die Videoaufzeichnung verwendet?

Lösung

Prüfen Sie, ob der Codierungstyp in der Symbolleiste der Live-Ansicht H.265 ist.

23.3.5 Warum meldet der Videorecorder einen IP-Konflikt?

Grund

Der Videorecorder verwendet die gleiche IP-Adresse wie andere Geräte.

Lösung

Ändern Sie die IP-Adresse des Videorecorders. Vergewissern Sie sich, dass sie nicht mit anderen Geräten identisch ist.

23.3.6 Warum bleibt das Bild bei der Wiedergabe von Ein- oder Mehrkanalkameras hängen?**Grund**

HDD Lese-/Schreibausnahme.

Lösung

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

23.3.7 Warum kann das Gerät die PTZ-Kamera nicht über Coaxitron steuern?**Grund**

1. Die Kamera unterstützt kein Coaxitron.
2. Das Coaxitron-Protokoll ist falsch.
3. Das Signal wird vom optischen Video-Transceiver beeinflusst.

Lösung

1. Stellen Sie sicher, dass das Videoeingangssignal HDTV I ist und die Kamera Koaxitron unterstützt.
2. Stellen Sie sicher, dass die Coaxitron-Protokollparameter wie Baudrate und Adresse korrekt sind.
3. Entfernen Sie den optischen Video-Transceiver, und versuchen Sie es erneut.

23.3.8 Warum scheint die PTZ über RS-485 nicht zu reagieren?**Grund**

1. Das RS-485-Kabel ist nicht richtig angeschlossen.
2. Die RS-485-Schnittstelle ist defekt.
3. Das Kontrollprotokoll ist nicht korrekt.

Lösung

1. Prüfen Sie, ob das RS-485-Kabel richtig angeschlossen ist.
2. Ändern Sie die RS-485-Schnittstelle, und versuchen Sie es erneut.
3. Stellen Sie sicher, dass das Steuerungsprotokoll Pelco lautet.

23.3.9 Warum ist die Tonqualität des Videos nicht gut?

Grund

1. Das Audio-Eingabegerät hat keine gute Wirkung bei der Tonsammlung.
2. Störung der Übertragung.
3. Der Audioparameter ist nicht richtig eingestellt.

Lösung

1. Überprüfen Sie, ob das Audio-Eingabegerät richtig funktioniert. Sie können ein anderes Audio-Eingabegerät wählen und es erneut versuchen.
2. Überprüfen Sie die Audioübertragungsleitung. Stellen Sie sicher, dass alle Leitungen gut angeschlossen oder verschweißt sind und keine elektromagnetischen Störungen vorliegen.
3. Stellen Sie die Lautstärke entsprechend der Umgebung und dem Audioeingabegerät ein.

