



Bedienungsanleitung

GD-RN-AP8616P

GD-RN-CT8832N

GD-RN-AP8632P

GD-RN-AT8864N

GD-RN-AP8632N

GD-RN-CT8864N

DE

Inhalt

1 Einleitung	1
1.1 Modellübersicht	1
2 Grundlegende Bedienung.....	2
2.1 Aktivieren Sie Ihr Gerät	2
2.1.1 Standardbenutzer und IP-Adresse	2
2.1.2 Aktivieren über das lokale Menü	2
2.1.3 Freischaltung über Grundig IP-Finder Tool	3
2.1.4 Aktivieren über Webbrowser	4
2.2 Konfigurieren der TCP/IP-Einstellungen.....	5
2.3 Festplatteneinstellungen.....	6
2.4 Netzwerkkamera hinzufügen	6
2.4.1 Automatisch gesuchte Online-Netzwerkkamera hinzufügen	7
2.4.2 Netzwerkkamera manuell hinzufügen	8
2.4.3 Hinzufügen einer Netzwerkkamera über PoE	9
2.4.4 Benutzerdefiniertes Protokoll konfigurieren	12
2.5 Zugang zur Plattform	13
2.5.1 EHome konfigurieren	13
2.5.2 SCMS konfigurieren	14
3 IoT.....	16
3.1 Hinzufügen eines IoT-Geräts	16
3.1.1 Hinzufügen eines Zugangskontrollgeräts	16
3.1.2 Hinzufügen eines Alarmgeräts	18
3.2 Konfigurieren Sie die Verknüpfungsaktion und den Scharfschaltplan.....	19
3.3 OSD konfigurieren	20
3.4 Suche im IoT-Datensatz	21
3.5 IoT Video/Bild	22
3.5.1 Konfigurieren der Ereignisaufzeichnung/-erfassung.....	23

3.5.2 Suche im IoT-Video/Bild	24
4 Live-Ansicht	26
4.1 Live-Ansicht starten	26
4.1.1 Konfigurieren der Live-View-Einstellungen	26
4.1.2 Layout der Live-Ansicht konfigurieren	27
4.1.3 Schalter Haupt-/Hilfsanschluss.....	29
4.2 Digitaler Zoom	29
4.3 Fisheye-Ansicht.....	30
4.4 3D-Positionierung.....	31
4.5 Konfigurieren der Kanal-Null-Kodierung	31
4.6 PTZ-Steuerung	32
4.6.1 PTZ-Parameter konfigurieren	32
4.6.2 Eine Voreinstellung festlegen.....	33
4.6.3 Aufrufen einer Voreinstellung.....	33
4.6.4 Eine Patrouille einstellen	34
4.6.5 Eine Patrouille rufen	36
4.6.6 Ein Muster festlegen	36
4.6.7 Aufruf eines Musters	37
4.6.8 Lineare Scangrenze einstellen	37
4.6.9 Parken mit einem Tastendruck	38
5 Aufnahme und Wiedergabe	40
5.1 Aufzeichnung	40
5.1.1 Konfigurieren der Aufzeichnungsparameter	40
5.1.2 Aktivieren des H.265-Stream-Zugriffs	42
5.1.3 ANR	42
5.1.4 Manuelle Aufzeichnung.....	43
5.1.5 Planaufzeichnung konfigurieren.....	43
5.1.6 Urlaubsaufzeichnung konfigurieren	44
5.2 Wiedergabe	45

5.2.1 Sofortige Wiedergabe.....	45
5.2.2 Normales Video abspielen.....	46
5.2.3 Smart Searched Video abspielen.....	46
5.2.4 Benutzerdefinierte gesuchte Dateien abspielen.....	47
5.2.5 Tag-Dateien abspielen.....	48
5.2.6 Spiel nach Teilperioden.....	50
5.2.7 Externe Dateien abspielen.....	50
5.3 Wiedergabemodus.....	51
5.3.1 Videoclips bearbeiten.....	51
5.3.2 Thumbnails-Ansicht.....	51
6 Bildeinzug.....	52
6.1 Parameter konfigurieren.....	52
6.2 Erfassungszeitplan konfigurieren.....	52
6.3 Zeitplan für die Urlaubserfassung konfigurieren.....	52
7 Ereignis.....	54
7.1 Normaler Ereignisalarm.....	54
7.1.1 Konfigurieren von Bewegungserkennungsalarmen.....	54
7.1.2 Konfigurieren von Videoverlustalarmen.....	54
7.1.3 Konfigurieren von Video-Manipulationsalarmen.....	55
7.1.4 Konfigurieren von Sensor-Alarmen.....	55
7.1.5 Ausnahmen konfigurieren Alarme.....	55
7.1.6 Kombinierten Alarm konfigurieren.....	56
7.2 VCA-Ereignis-Alarm.....	57
7.2.1 Erkennung von Gesichtern.....	58
7.2.2 Temperatur-Screening.....	59
7.2.3 Fahrzeug-Erkennung konfigurieren.....	60
7.2.4 Erkennung von Linienkreuzungen.....	61
7.2.5 Intrusion Detection.....	63
7.2.6 Erkennung von Regionseingängen.....	64

7.2.7	Erkennung des Verlassens einer Region.....	65
7.2.8	Erkennung von Herumlungern	66
7.2.9	Erkennung von Menschenansammlungen	67
7.2.10	Erkennung schneller Bewegungen	69
7.2.11	Parkdetektion	70
7.2.12	Erkennung unbeaufsichtigten Gepäcks.....	71
7.2.13	Erkennung der Objektentfernung	72
7.2.14	Erkennung von Audioausnahmen	74
7.2.15	Defokus-Erkennung	75
7.2.16	Erkennung von plötzlichen Szenenwechseln	76
7.2.17	PIR-Alarm.....	77
7.2.18	Wärmebildkamera-Erkennung	78
7.2.19	Warteschlangenverwaltung konfigurieren	78
7.3	Zeitplan für die Scharfschaltung konfigurieren.....	79
7.4	Verknüpfungsaktionen konfigurieren	80
7.4.1	Konfigurieren der Auto-Switch-Vollbildüberwachung.....	80
7.4.2	Audiowarnung konfigurieren	81
7.4.3	Überwachungszentrale benachrichtigen	81
7.4.4	E-Mail-Verknüpfung konfigurieren.....	82
7.4.5	Ausgelöster Alarmausgang.....	82
7.4.6	Audio- und Lichtalarmverknüpfung konfigurieren.....	82
7.4.7	PTZ-Kopplung konfigurieren.....	83
8	Intelligente Analyse	84
8.1	Personenzählung	84
8.2	Wärmebildkarte.....	84
9	POS-Konfiguration	86
9.1	POS-Verbindung konfigurieren.....	86
9.2	POS-Text-Overlay konfigurieren.....	89
9.3	POS-Alarm konfigurieren.....	90

10 Kameraeinstellungen	92
10.1 Bildparameter konfigurieren	92
10.2 Konfigurieren der OSD-Einstellungen.....	92
10.3 Datenschutzmaske konfigurieren.....	93
10.4 Import/Export von IP-Kamera-Konfigurationsdateien	94
10.5 IP-Kameras aufrüsten	95
11 Speicher.....	96
11.1 Verwaltung von Speichergeräten	96
11.1.1 Lokales Festplattenlaufwerk verwalten	96
11.1.2 Hinzufügen einer Netzwerkfestplatte	98
11.1.3 Verwalten von eSATA	99
11.2 Festplatten-Array.....	101
11.2.1 Erstellen eines Plattenarrays.....	101
11.2.2 Ein Array wiederherstellen	104
12 Hot Spare Rekorder Backup.....	107
12.1 Hot Spare Gerät einstellen	107
12.2 Arbeitsschreiber einstellen.....	108
12.3 Verwalten des Hot-Spare-Systems	108
13 Netzwerkeinstellungen	110
13.1 DDNS konfigurieren	110
13.2 PPPoE konfigurieren	110
13.3 SNMP konfigurieren	111
13.4 E-Mail konfigurieren	112
13.5 Port-Zuordnung konfigurieren (NAT)	114
13.6 Anschluss konfigurieren	116
13.7 ONVIF konfigurieren	117
14 Dateiverwaltung	119
14.1 Dateien suchen	119
14.2 Suchverlaufsoperation	119

14.3 Dateien exportieren	120
15 Benutzerverwaltung und Sicherheit.....	121
15.1 Verwalten von Benutzerkonten	121
15.1.1 Einen Benutzer hinzufügen	121
15.1.2 Admin-Benutzer bearbeiten.....	122
15.1.3 Bearbeiten eines Betreibers/Gastbenutzers.....	123
15.2 Benutzerberechtigungen verwalten.....	124
15.2.1 Benutzerberechtigungen festlegen.....	124
15.2.2 Live-Ansichtsberechtigung auf dem Sperrbildschirm festlegen.....	126
15.2.3 Berechtigung zur doppelten Überprüfung für Nicht-Admin-Benutzer festlegen	127
15.3 Konfigurieren der Passwortsicherheit.....	128
15.3.1 Sicherheitsfragen konfigurieren.....	128
15.3.2 Reservierte E-Mail konfigurieren	129
15.3.3 GUID-Datei exportieren.....	130
15.4 Passwort zurücksetzen	131
15.4.1 Passwort über GUID zurücksetzen	131
15.4.2 Passwort mit Sicherheitsfragen zurücksetzen	132
15.4.3 Passwort zurücksetzen durch reservierte E-Mail.....	132
15.4.4 Passwort zurücksetzen durch SCMS.....	133
16 Systemverwaltung	134
16.1 Gerät konfigurieren	134
16.2 Zeit konfigurieren	134
16.2.1 Manuelle Zeitsynchronisation	134
16.2.2 NTP-Synchronisierung	135
16.2.3 Sommerzeit-Synchronisation	135
16.2.4 IP-Kamera Zeitsynchronisation	136
16.3 Netzdetektion.....	136
16.3.1 Überwachung des Netzwerkverkehrs	136
16.3.2 Testnetzverzögerung und Paketverlust.....	137

16.3.3 Netzwerk-Paket exportieren	138
16.3.4 Netzwerk-Ressourcenstatistik	138
16.4 Wartung von Speichergeräten	139
16.4.1 Erkennung von fehlerhaften Sektoren	139
16.4.2 S.M.A.R.T.-Detektion	140
16.4.3 Erkennung des Festplattenzustands	141
16.4.4 Festplattenklon konfigurieren	141
16.4.5 Datenbank reparieren	142
16.5 Upgrade-System	143
16.5.1 Gerät aktualisieren	143
16.5.2 IP-Kameras aufrüsten	144
16.6 Import/Export von IP-Kamera-Konfigurationsdateien	144
16.7 Import/Export von Gerätekonfigurationsdateien	145
16.8 Protokollverwaltung	146
16.8.1 Protokollspeicherung	146
16.8.2 Logdateien suchen und exportieren	147
16.8.3 Protokoll auf den Server hochladen	148
16.8.4 Einweg-Authentifizierung	148
16.8.5 Zwei-Wege-Authentifizierung	149
16.9 Standardeinstellungen wiederherstellen	150
16.10 Sicherheitsmanagement	151
16.10.1 IP/MAC-Adressfilter	151
16.10.2 RTSP-Authentifizierung	152
16.10.3 RTSP-Verschlüsselungsalgorithmus	152
16.10.4 ISAPI-Dienst	153
16.10.5 HTTP-Authentifizierung	153
16.10.6 HTTP/Web-Digest-Algorithmus	153
16.10.7 Bild-URL-Digest-Authentifizierung	154
16.10.8 Dienst zur Authentifizierung der seriellen Schnittstelle	154

17 Anhang	155
17.1 Glossar	155
17.2 Häufig gestellte Fragen.....	156

1 Einleitung

Vielen Dank, dass Sie sich für ein Grundig-Produkt entschieden haben. Bevor Sie das Produkt installieren oder anschließen, lesen Sie bitte zuerst die folgenden Dokumente, die Sie auf der CD-ROM in der Produktverpackung oder in gedruckter Form in der Produktverpackung finden:

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

Weitere Informationen über das Produkt wie Datenblätter, CE-Dokumente usw. finden Sie auch auf der CD-ROM in der Produktverpackung.

Dieses Benutzerhandbuch ist ein Handbuch für Netzwerk-Videorecorder. In der Liste unter 1.1 Modellübersicht finden Sie die entsprechenden 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-AP8616P
- GD-RN-AP8632P
- GD-RN-AP8632N
- GD-RN-CT8832N
- GD-RN-AT8864N
- GD-RN-CT8864N

2 Grundlegende Bedienung

2.1 Aktivieren Sie Ihr Gerät

2.1.1 Standardbenutzer und IP-Adresse

- Standard-Administratorkonto: admin.
- Standard-IPv4-Adresse: 192.168.1.100.

2.1.2 Aktivieren über das lokale Menü

Für den erstmaligen Zugriff müssen Sie das Gerät durch Eingabe eines Admin-Passworts aktivieren. Vor der Aktivierung ist keine Bedienung möglich. Sie können das Gerät auch über einen Webbrowser, SADP oder eine Client-Software aktivieren.

Schritte

1. Geben Sie das Admin-Passwort zweimal ein.

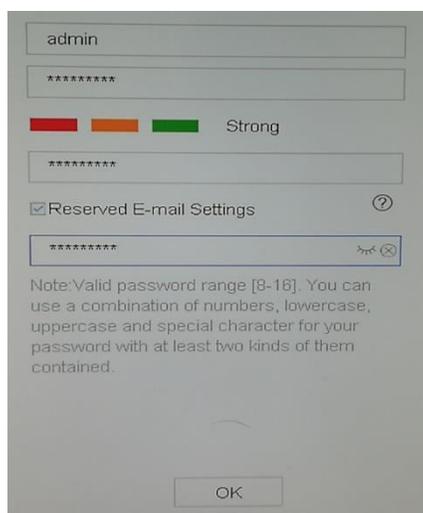
The image shows a screenshot of a device's configuration menu. At the top, there is a text input field containing 'admin'. Below it is a password input field with a masked password '*****'. A strength indicator shows three colored bars (red, orange, green) and the word 'Strong'. Below that is another masked password field '*****'. There is a checked checkbox for 'Reserved E-mail Settings' with a help icon. Below this is a third masked password field '*****' with a clear icon. A note at the bottom states: '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.

Abbildung 2-1 Aktivieren über das lokale Menü

Warnung

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 zurückzusetzen, vor allem im Hochsicherheitssystem kann das monatliche oder wöchentliche Zurücksetzen des Passworts Ihr Produkt besser schützen.

-
2. Geben Sie das Passwort ein, um die IP-Kameras zu aktivieren.
 3. **Optional:** Prüfen Sie **Reservierte E-Mail-Einstellungen**, um das Passwort in Zukunft zurückzusetzen.
 4. Klicken Sie auf **OK**.
-

Hinwe

Nach das Gerät ist aktiviert, sollten Sie das Kennwort ordnungsgemäß

Was ist als nächstes zu tun?

Wenn Sie die **Einstellungen für die reservierte E-Mail** aktiviert haben, können Sie die reservierte E-Mail für das Zurücksetzen des Kennworts auch in Zukunft festlegen.

2.1.3 Freischaltung über Grundig IP-Finder Tool

Die Software GRUNDIG IP-FINDER dient dazu, das Online-Gerät zu erkennen, den Rekorder zu aktivieren und das Passwort zurückzusetzen.

Holen Sie sich die GRUNDIG IP-FINDER Software von der mitgelieferten Diskette oder von unserer Website www.grundig-security.com und installieren Sie den GRUNDIG IP-FINDER entsprechend den Anweisungen. Folgen Sie den Schritten zur Aktivierung des Geräts.

Schritte

1. Schließen Sie das Netzteil Ihres Videorekorders an eine Steckdose an und schalten Sie es ein.
2. Führen Sie die Software IP-Finder aus, um die Online-Recorder zu durchsuchen.
3. Überprüfen Sie den Rekorderstatus in der Geräteliste und wählen Sie den inaktiven Rekorder aus.

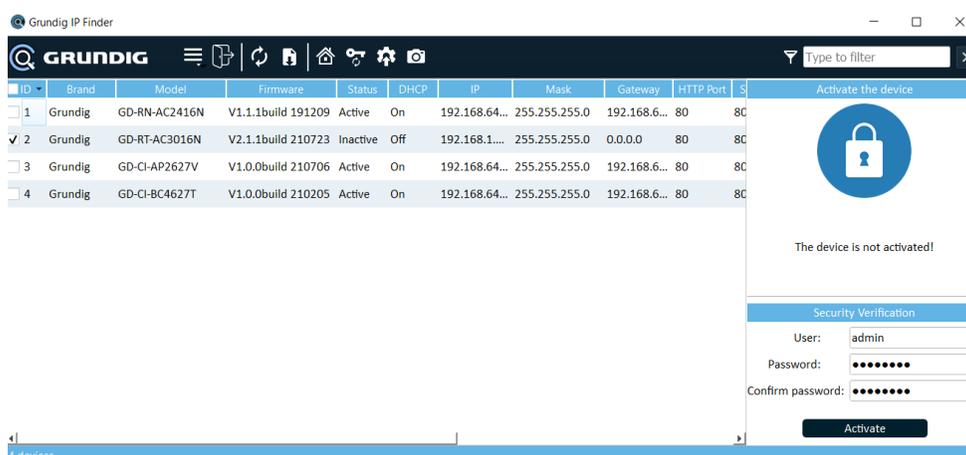


Abbildung 2-2 Aktivieren über Grundig IP-Finder Tool

4. Erstellen Sie das neue Kennwort, geben Sie es in das Kennwortfeld ein und bestätigen Sie das Kennwort.

Hinwe

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 zurückzusetzen, vor allem im Hochsicherheitssystem kann das monatliche oder wöchentliche Zurücksetzen des Passworts Ihr Produkt besser schützen.

5. Klicken Sie auf **Aktivieren**.

2.1.4 Aktivieren über Webbrowser

Sie können über einen Webbrowser auf den Rekorder zugreifen. Sie können einen der nachfolgend aufgeführten Webbrowser verwenden: Internet Explorer 6.0 und höher, Apple Safari, Mozilla Firefox und Google Chrome. Die unterstützten Auflösungen umfassen 1024*768 und höher.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie sich im gleichen Netzwerksegment wie Ihr Gerät befinden.

Schritte

1. Geben Sie die IP-Adresse in den Webbrowser ein und drücken Sie dann die **Eingabetaste**.

Activation

User Name admin

Password Strong

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.

Confirm

OK

Abbildung 2-3 Webbrowser-Aktivierung

2. Legen Sie das Passwort für das Benutzerkonto admin fest.

Hinweis

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 zurückzusetzen, vor allem im Hochsicherheitssystem kann das monatliche oder wöchentliche Zurücksetzen des Passworts Ihr Produkt besser schützen.

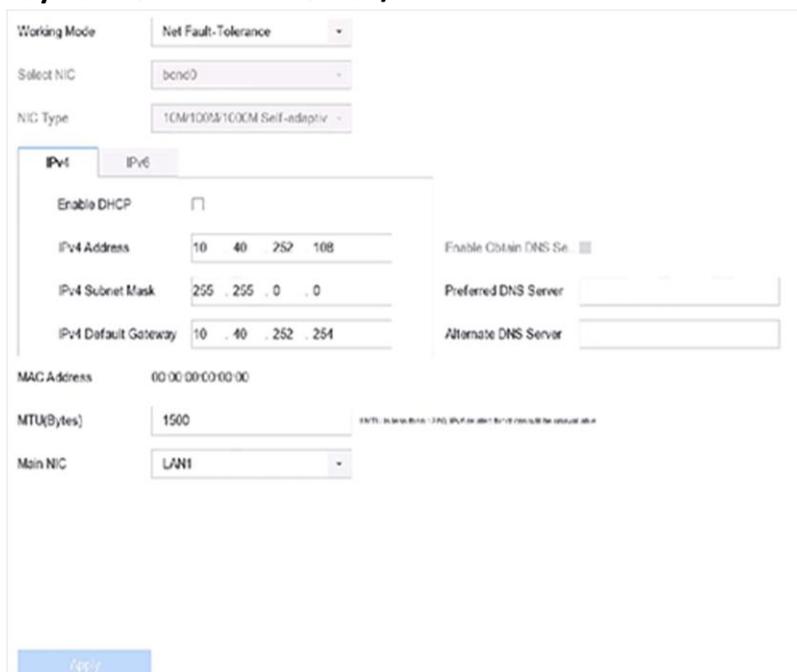
3. Klicken Sie auf **OK**.
4. **Optional:** Legen Sie die Sicherheitsfragen, die E-Mail für die Passwortwiederherstellung oder die Export-GUID-Datei für die zukünftige Passworücksetzung fest.
5. Klicken Sie auf **OK**.
6. Installieren Sie das Plug-in, bevor Sie das Live-Video ansehen und das Gerät verwalten. Möglicherweise müssen Sie den Webbrowser schließen, um die Installation des Plug-ins abzuschließen.

2.2 Konfigurieren der TCP/IP-Einstellungen

Die TCP/IP-Einstellungen müssen ordnungsgemäß konfiguriert werden, bevor Sie Ihr Gerät in einem Netzwerk betreiben. Es sind sowohl IPv4 als auch IPv6 verfügbar.

Schritte

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



The screenshot displays the network configuration interface. At the top, 'Working Mode' is set to 'Net Fault-Tolerance', 'Select NIC' is 'bnc0', and 'NIC Type' is '10M/100M/1000M Self-adaptiv'. Below this, there are tabs for 'IPv4' and 'IPv6', with 'IPv4' currently selected. Under the 'IPv4' tab, there are several settings: 'Enable DHCP' is unchecked; 'IPv4 Address' is '10.40.252.108'; 'IPv4 Subnet Mask' is '255.255.0.0'; 'IPv4 Default Gateway' is '10.40.252.254'; 'MAC Address' is '00:00:00:00:00:00'; 'MTU(Bytes)' is '1500'; and 'Main NIC' is 'LAN1'. To the right of the IPv4 settings, there are options for 'Enable Obtain DNS Se.' (checked), 'Preferred DNS Server', and 'Alternate DNS Server'. A blue 'Apply' button is located at the bottom left of the configuration area.

Abbildung 2-4 TCP/IP-Einstellungen

2. Wählen Sie als **Arbeitsmodus Netzfehlertoleranz** oder **Multiadressmodus**.

Netz-Fehlertoleranz

Die beiden NIC-Karten verwenden dieselbe IP-Adresse, und Sie können die Haupt-NIC-Karte als LAN1 oder LAN2 auswählen. Auf diese Weise aktiviert das Gerät im Falle eines Ausfalls einer NIC-Karte automatisch die andere Standby-NIC-Karte, um den normalen Betrieb des Systems zu gewährleisten.

Multi-Adress-Modus

Die Parameter der beiden NIC-Karten können unabhängig voneinander konfiguriert werden. Sie können LAN1 oder LAN2 unter NIC auswählen für die Parametereinstellungen auswählen. Wählen Sie eine NIC-Karte als Standardroute aus. Wenn das System eine Verbindung mit dem Extranet herstellt, werden die Daten über die Standardroute weitergeleitet.

3. Klicken Sie je nach Bedarf auf **IPv4** oder **IPv6**.
4. Stellen Sie die entsprechenden Parameter ein.
5. Klicken Sie auf **Anwenden**.

Hinwe

- Aktivieren Sie **DHCP**, um IP-Einstellungen automatisch zu beziehen, wenn ein DHCP-Server im Netzwerk verfügbar ist.
 - Der gültige MTU-Wert liegt zwischen 500 und 9676.
-

2.3 Festplatteneinstellungen

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

2.4 Netzwerkkamera hinzufügen

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

Bevor Sie beginnen

Stellen Sie sicher, dass die Netzwerkverbindung gültig und korrekt ist und dass die hinzuzufügende IP-Kamera aktiviert wurde.

Schritte

1. Klicken Sie in der Hauptmenüleiste auf .
2. Klicken Sie in der Titelleiste auf die Registerkarte **Benutzerdefiniert hinzufügen**.

Add IP Camera (Custom)
✕

IP Camera Address

Protocol

Management Port

Transfer Protocol

User Name

Password

Continue to Add
Add

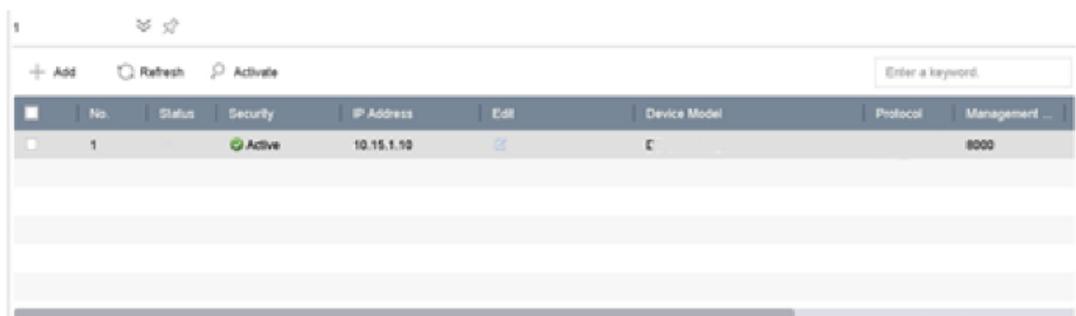
Abbildung 2-5 IP-Kamera hinzufügen

3. Geben Sie die IP-Adresse, das Protokoll, den Verwaltungsport und andere IP-Kamerainformationen ein, die Sie hinzufügen möchten.
4. Geben Sie den Login-Benutzernamen und das Passwort der IP-Kamera ein.
5. Klicken Sie auf **Hinzufügen**, um das Hinzufügen der IP-Kamera abzuschließen.
6. **Optional:** Klicken Sie auf **Weiter zum Hinzufügen**, um weitere IP-Kameras hinzuzufügen.

2.4.1 Automatisch gesuchte Online-Netzwerkamera hinzufügen

Schritte

1. Klicken Sie im Hauptmenü auf .
2. Klicken Sie unten auf **Anzahl der nicht hinzugefügten Online-Geräte**.
3. Wählen Sie die automatisch gesuchten Online-Netzwerk-Kameras aus.
4. Klicken Sie auf **Hinzufügen**, um die Kamera hinzuzufügen, die das gleiche Anmeldekennwort wie der Videorecorder hat.



No.	Status	Security	IP Address	Edit	Device Model	Protocol	Management ...
1	Active		10.15.1.10		E		8000

Abbildung 2-6 Automatisch gesuchte Online-Netzwerkamera hinzufügen

Hinweis

Wenn die hinzuzufügende Netzwerkkamera noch nicht aktiviert ist, können Sie sie in der Netzwerkkameraliste der Kameraverwaltungsoberfläche aktivieren.

2.4.2 Netzwerkkamera manuell hinzufügen

Bevor Sie Live-Videos anzeigen oder Videodateien aufzeichnen können, müssen Sie dem Gerät Netzwerkkameras hinzufügen.

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im Hauptmenü auf .
2. Klicken Sie auf **Benutzerdefiniertes Hinzufügen**.
3. Stellen Sie **IP-Kamera-Adresse**, **Protokoll**, **Verwaltungsport**, **Übertragungsprotokoll**, **Benutzername** und **Passwort** ein. Der Verwaltungsport reicht von 1 bis 65535.

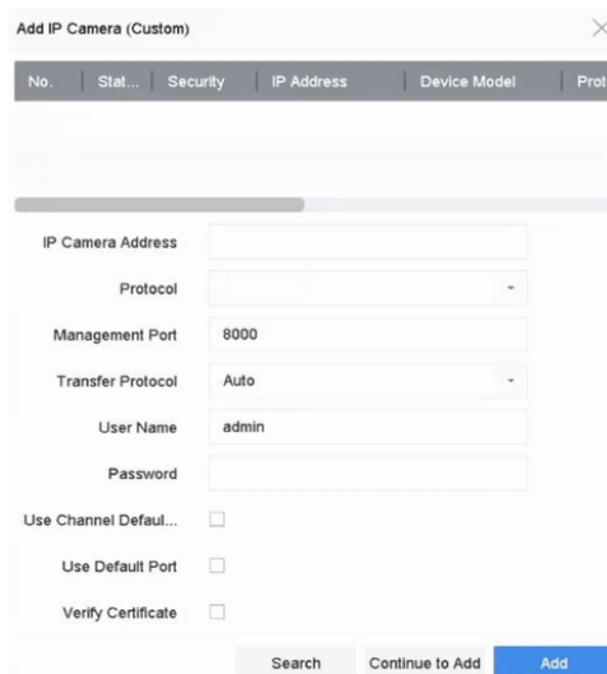


Abbildung 2-7 Netzwerkkamera hinzufügen

-
4. **Optional:** Aktivieren Sie das Kontrollkästchen **Standardpasswort für den Kanal verwenden**, um das Standardpasswort zum Hinzufügen der Kamera zu verwenden.
 5. **Optional:** Aktivieren Sie das Kontrollkästchen **Standardport verwenden**, um den Standardverwaltungsport zum Hinzufügen der Kamera zu verwenden. Für den SDK-Dienst ist der Standardportwert 8000. Für den erweiterten SDK-Dienst ist der Standardwert 8443.

Hinweis

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

6. **Optional:** Aktivieren Sie das Kontrollkästchen **Zertifikat überprüfen**, um die Kamera mit einem Zertifikat zu verifizieren. Das Zertifikat ist eine Form der Identifikation für die Kamera, die eine sicherere Kameraauthentifizierung ermöglicht. Wenn Sie diese Funktion verwenden, müssen Sie zuerst das Zertifikat der Netzwerkkamera in das Gerät importieren. Einzelheiten dazu finden Sie unter.

Hinweis

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

7. Klicken Sie auf **Hinzufügen**.
8. **Optional:** Markieren Sie **Weiter zum Hinzufügen**, um weitere Netzwerkkameras hinzuzufügen.

2.4.3 Hinzufügen einer Netzwerkkamera über PoE

Die PoE-Schnittstellen ermöglichen es dem Gerätesystem, elektrische Energie zusammen mit Daten sicher über Ethernet-Kabel an die angeschlossenen PoE-Kameras weiterzuleiten. Die Anzahl der unterstützten PoE-Kameras variiert je nach Gerätemodul. Wenn Sie die PoE-Schnittstelle deaktivieren, können Sie auch eine Verbindung zu den Online-Netzwerkkameras herstellen. Und die PoE-Schnittstelle unterstützt die Plug-and-Play-Funktion.

PoE-Kamera hinzufügen

Schritte

1. Gehen Sie zu **Kamera → Kamera → PoE-Einstellungen**.
2. Aktivieren oder deaktivieren Sie den Modus für lange Netzwerkkabel, indem Sie **Langstrecke** oder **Kurzstrecke** wählen.
Langstrecke

Netzwerkübertragungen über große Entfernungen (100 bis 300 Meter) über die PoE-Schnittstelle.

Kurzstrecke

Netzwerkübertragung über kurze Distanzen (< 100 Meter) über die PoE-Schnittstelle.

Hinweis

- Die PoE-Ports sind standardmäßig mit dem Kurzstreckenmodus aktiviert.
 - Die Bandbreite der IP-Kamera, die über ein langes Netzkabel (100 bis 300 Meter) mit dem PoE verbunden ist, darf 6 MP nicht überschreiten.
 - Die maximal zulässige Länge des Netzkabels kann je nach IP-Kameramodell und Kabelmaterial weniger als 300 Meter betragen.
 - Wenn die Übertragungsentfernung 100 bis 250 Meter beträgt, müssen Sie ein CAT5E- oder CAT6-Netzkabel für die Verbindung mit der PoE-Schnittstelle verwenden.
 - Wenn die Übertragungsdistanz 250 bis 300 Meter beträgt, müssen Sie ein CAT6-Netzkabel für die Verbindung mit der PoE-Schnittstelle verwenden.
 - Eine Liste der IP-Kameras, die über ein langes Netzkabel (100-300 m) mit PoE verbunden sind, finden Sie im Anhang 20.3.
-

Actual power: 0.0W. Remaining power: 200.0W. 0%

Channel	Long Distance	Short Distance	Channel Status	Actual Power
D1	<input checked="" type="radio"/>	<input type="radio"/>	Disconnected	0.0W
D2	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D5	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D6	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D7	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D8	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D9	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D10	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D11	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D12	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D13	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D14	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D15	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W
D16	<input type="radio"/>	<input checked="" type="radio"/>	Disconnected	0.0W

Apply

Abbildung 2-8 PoE-Kamera hinzufügen

3. Klicken Sie auf **Anwenden**.
4. Schließen Sie PoE-Kameras mit Netzkabeln an die PoE-Ports des Geräts an.
5. Gehen Sie zu **Kamera** → **Kamera** → **IP-Kamera**, um Kamerabilder und -informationen anzuzeigen.

Nicht-PoE-Netzwerkamera hinzufügen

Sie können die PoE-Schnittstelle deaktivieren, indem Sie die manuelle Einstellung wählen, während der aktuelle Kanal als normaler Kanal verwendet werden kann und die Parameter ebenfalls bearbeitet werden können.

Schritte

1. Gehen Sie zu **Kamera → Kamera → IP-Kamera**.
2. Positionieren Sie den Cursor auf ein Fenster ohne verknüpfte Netzwerkamera und klicken Sie auf  .

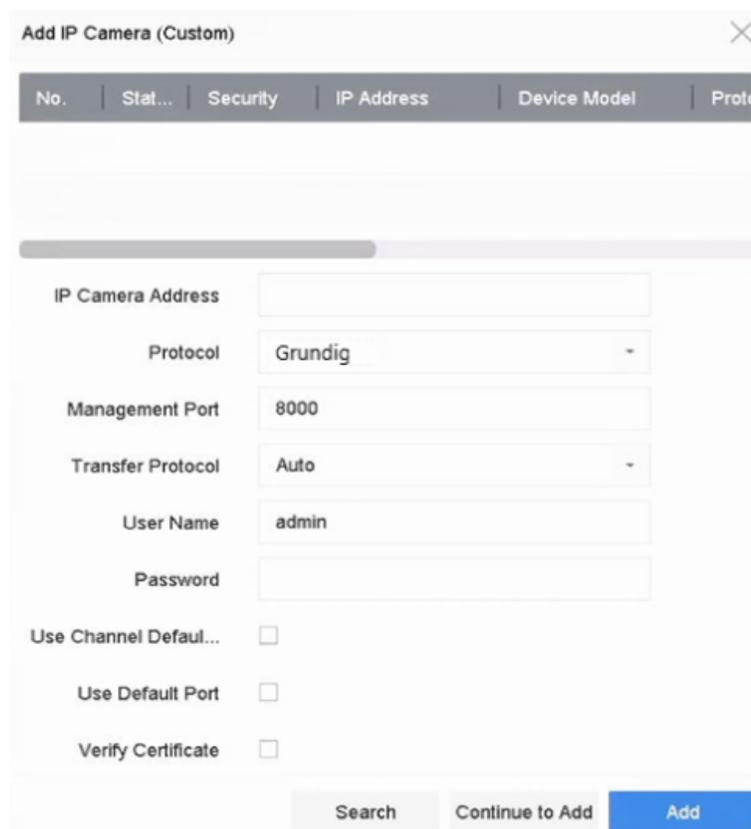


Abbildung 2-9 Netzwerkamera bearbeiten

3. Wählen Sie als **Hinzufügemethode Manuell**.

Plug-and-Play

Die Kamera ist physisch mit der PoE-Schnittstelle verbunden. Ihre Parameter können nicht bearbeitet werden. Sie können zu **System → Netzwerk → TCP/IP** gehen, um die IP-Adresse des PoE-Anschlusses zu ändern. **Manuell**

Hinzufügen einer IP-Kamera ohne physische Verbindung über das Netzwerk.

-
- Geben Sie die **IP-Adresse**, den **Benutzernamen** und das **Passwort** ein.
 - Klicken Sie auf **OK**.

2.4.4 Benutzerdefiniertes Protokoll konfigurieren

Um Netzwerkkameras anzuschließen, die nicht mit den Standardprotokollen konfiguriert sind, können Sie die benutzerdefinierten Protokolle für sie konfigurieren. Das System bietet 16 benutzerdefinierte Protokolle.

Schritte

- Gehen Sie zu **Weitere Einstellungen → Protokoll**.

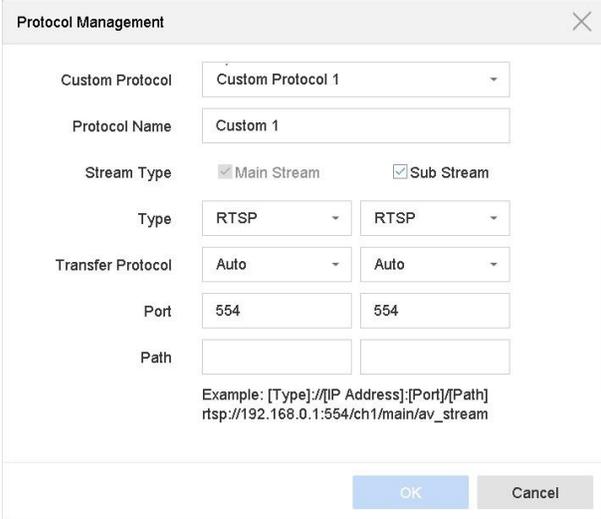


Abbildung 2-10 Protokollverwaltung

- Protokollparameter einstellen.

Typ

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

Pfad

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

Hinweis

Der Protokolltyp und das Übertragungsprotokoll müssen von der hinzuzufügenden Netzwerkkamera unterstützt werden.

- Klicken Sie auf **OK**.

Nachdem Sie das benutzerdefinierte Protokoll hinzugefügt haben, können Sie es unter **Protokoll** sehen.

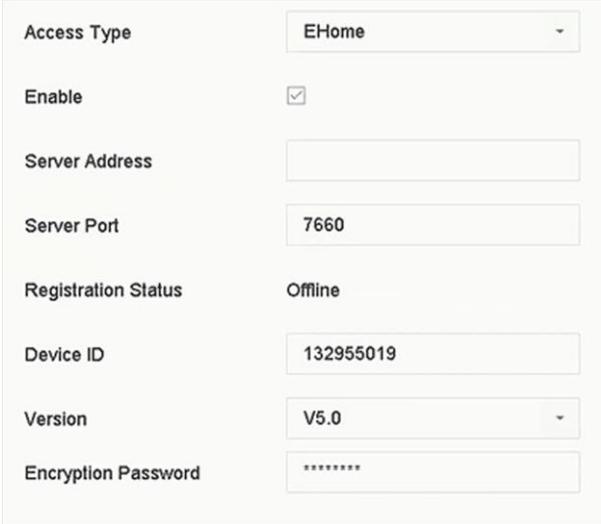
2.5 Zugang zur Plattform

2.5.1 EHome konfigurieren

Das EHome-Protokoll ist ein nicht-offenes und auf TCP/UDP basierendes Push-Modus-Protokoll, das die Kommunikation zwischen dem System und mobilen Geräten (z.B. Körperkamera, MNVR, etc.) realisieren kann. Das System fungiert als Server und Sie können das Gerät im System registrieren. Das Protokoll ist für den Einsatz von dynamischen Geräte-IP-Adressen geeignet.

Schritte

1. Gehen Sie zu **System** → **Netzwerk** → **Erweitert** → **Plattformzugriff**.



The screenshot shows a configuration panel for EHome with the following fields and values:

Access Type	EHome
Enable	<input checked="" type="checkbox"/>
Server Address	
Server Port	7660
Registration Status	Offline
Device ID	132955019
Version	V5.0
Encryption Password	*****

Abbildung 2-11 EHome-Einstellungen

2. Wählen Sie als **Zugriffsart EHome**.

3. **Aktivieren** Sie die Funktion.

Hinwe

Wenn Sie EHome aktivieren, wird der Zugang zu anderen Plattformen deaktiviert.

4. Stellen Sie die entsprechenden Parameter ein.

Server-Adresse

Die IP-Adresse des Plattformservers.

Server-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.

Version

EHome-Protokollversion, nur V5.0 ist verfügbar.

Verschlüsselungs-Passwort

Das Verschlüsselungspasswort ist erforderlich, wenn Sie die EHome V5.0 Version verwenden. Es bietet eine sicherere Kommunikation zwischen dem Gerät und der Plattform. Geben Sie es zur Überprüfung ein, nachdem das Gerät bei der EHome-Plattform registriert wurde.

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

Was ist als nächstes zu tun?

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

2.5.2 SCMS konfigurieren

SCMS bietet eine Mobiltelefonanwendung und einen Plattfordienst für den Zugriff und die Verwaltung Ihres Videorekorders, was Ihnen einen bequemen Fernzugriff auf das Überwachungssystem ermöglicht.

Schritte

1. Gehen Sie zu **System → Netzwerk → Erweitert → Plattformzugriff**.
2. Markieren Sie **Aktivieren**, um die Funktion zu aktivieren. Dann werden die Servicebedingungen angezeigt.
 - 1) Geben Sie den **Verifizierungscode** ein.
 - 2) Scannen Sie den QR-Code, um die Servicebedingungen und die Datenschutzerklärung zu lesen.
 - 3) Prüfen **Der SCMS-Dienst erfordert einen Internetzugang. Bitte lesen Sie die Servicebedingungen und die Datenschutzerklärung, bevor Sie den Dienst aktivieren.**
Wenn Sie mit den Servicebedingungen und der Datenschutzerklärung einverstanden sind.
 - 4) Klicken Sie auf **OK**.

Hinweis

- SCMS ist standardmäßig deaktiviert.
- Der Prüfcode ist standardmäßig leer. Er muss 6 bis 12 Buchstaben oder Zahlen enthalten und es wird zwischen Groß- und Kleinschreibung unterschieden.

3. Optional: Konfigurieren Sie die folgenden Parameter.

- Markieren Sie **Benutzerdefiniert** und geben Sie die gewünschte **Serveradresse** ein.
- Aktivieren Sie die Option **Stream-Verschlüsselung aktivieren**, dann ist ein Verifizierungscode für den Fernzugriff und die Live-Ansicht erforderlich.

4. Binden Sie Ihr Gerät mit einem SCMS-Konto.

- 1) Verwenden Sie ein Smartphone, um den QR-Code zu scannen und die SCMS-App herunterzuladen. Sie können sie auch für Android von <https://play.google.com/store/apps/details?id=com.grundig.scms> oder für iOS von <https://apps.apple.com/us/app/id1442059754> oder über den QR-Code unten herunterladen. Weitere Informationen finden Sie im *SCMS Mobile Client User Manual*.

Android



iOS



Abbildung 2-12 SCMS herunterladen

- 2) Verwenden Sie die SCMS-App, um den Geräte-QR zu scannen und das Gerät zu binden.

Hinweis

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

5. Klicken Sie auf **Anwenden**.

Was ist als nächstes zu tun?

Sie können über die SCMS-App auf Ihren Videorekorder zugreifen.

3 IoT

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

3.1 Hinzufügen eines IoT-Geräts

Hinwe

Die maximale Anzahl der IoT-Kanäle entspricht der Hälfte der maximalen Anzahl der Netzwerkkameras Ihres Videorecorders.

3.1.1 Hinzufügen eines Zugangskontrollgeräts

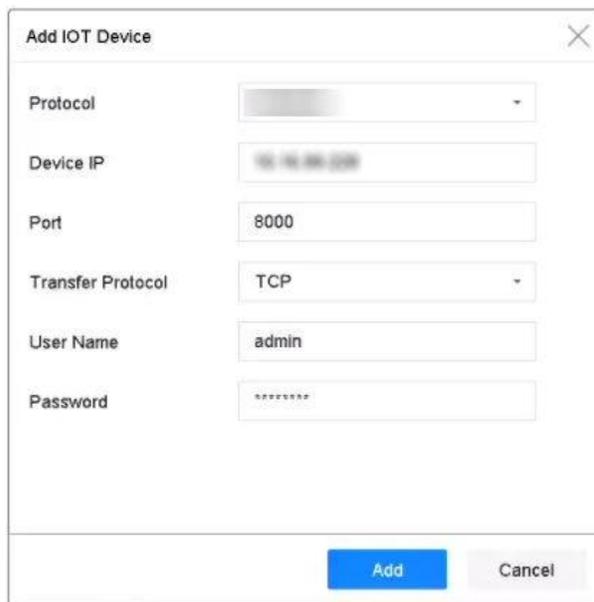
Fügen Sie Alarm-Host- und Video-Gegensprechanlagen hinzu, um deren Alarmer zu empfangen. Sie können Verknüpfungsaktionen konfigurieren, wie z. B. das Auslösen von Aufzeichnungen und Vollbildüberwachung, wenn ein Alarm auftritt.

Bevor Sie beginnen

Installieren Sie Zugangskontrollgeräte. Stellen Sie sicher, dass die Netzwerkkommunikation zwischen den Zugangskontrollgeräten und dem Videorecorder gut funktioniert.

Schritte

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



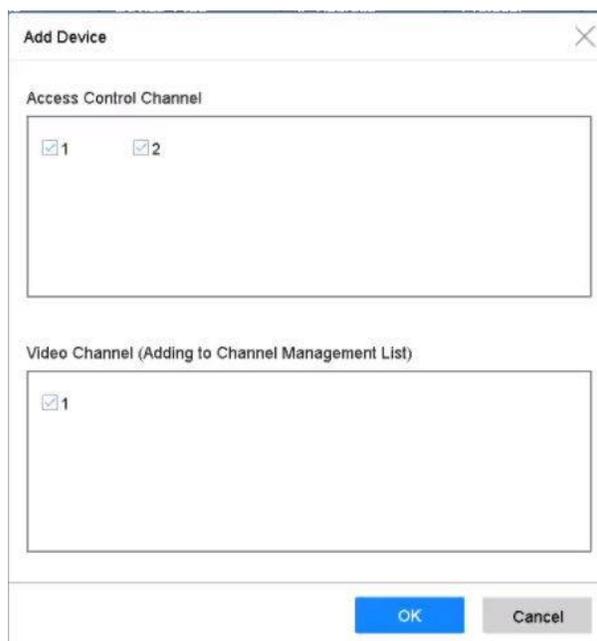
The screenshot shows a dialog box titled "Add IOT Device" with a close button (X) in the top right corner. The dialog contains the following fields and values:

- Protocol: [Dropdown menu]
- Device IP: [Text input field]
- Port: 8000
- Transfer Protocol: TCP
- User Name: admin
- Password: [Masked with asterisks]

At the bottom of the dialog, there are two buttons: "Add" (highlighted in blue) and "Cancel" (disabled).

Abbildung 3-1 Zugangskontrolle

3. Geben Sie die Informationen zum Zugangskontrollgerät ein. **Geräte-IP**, **Port**, **Benutzername** und **Passwort** müssen mit dem Zugangskontrollgerät übereinstimmen.
4. **Optional:** Bei Geräten mit mehreren Zugangskontrollkanälen oder Videokanälen wählen Sie den gewünschten Zugangskontrollkanal und Videokanal aus.



The screenshot shows a dialog box titled "Add Device" with a close button (X) in the top right corner. The dialog contains two sections:

- Access Control Channel:** A list box containing two items, each with a checked checkbox: 1 and 2.
- Video Channel (Adding to Channel Management List):** A list box containing one item with a checked checkbox: 1.

At the bottom of the dialog, there are two buttons: "OK" (highlighted in blue) and "Cancel" (disabled).

Abbildung 3-2 Gerät hinzufügen

5. Klicken Sie auf **Hinzufügen**.

Was ist als nächstes zu tun?

- Klicken Sie auf , um das Live-Video des entsprechenden Kanals zu sehen.

Hinwe

Für Zutrittskontrollgeräte ohne Videokanal. Sie müssen zuerst den Auslösekanal in der Konfiguration der Verknüpfungsaktion auswählen. Einzelheiten finden Sie unter ***Konfigurieren von Verknüpfungsaktionen***.

Klicken Sie  um hinzugefügte Zugangskontrollgeräte zu bearbeiten

3.1.2 Hinzufügen eines Alarmgeräts

Fügen Sie Alarmgeräte der Hersteller Luminite, GJD, Hikvision oder OPTEX hinzu, um deren Alarme zu empfangen. Sie können Verknüpfungsaktionen konfigurieren, wie z. B. das Auslösen von Aufzeichnungen und Vollbildüberwachung, wenn ein Alarm auftritt.

Bevor Sie beginnen

Installieren Sie die Alarmanlagen. Stellen Sie sicher, dass die Netzwerkkommunikation zwischen den Alarmgeräten und dem Videorecorder gut funktioniert.

Schritte

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

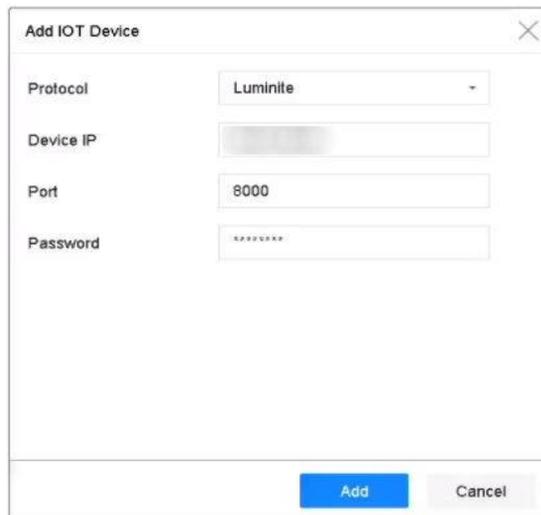


Abbildung 3-3 Alarmvorrichtung

3. Geben Sie die Informationen zum Zugangskontrollgerät ein. Die Informationen müssen mit dem hinzuzufügenden Alarmgerät übereinstimmen.

4. Klicken Sie auf **Hinzufügen**.

Was ist als nächstes zu tun?

- Klicken Sie auf , um das Live-Video des entsprechenden Kanals anzuzeigen.

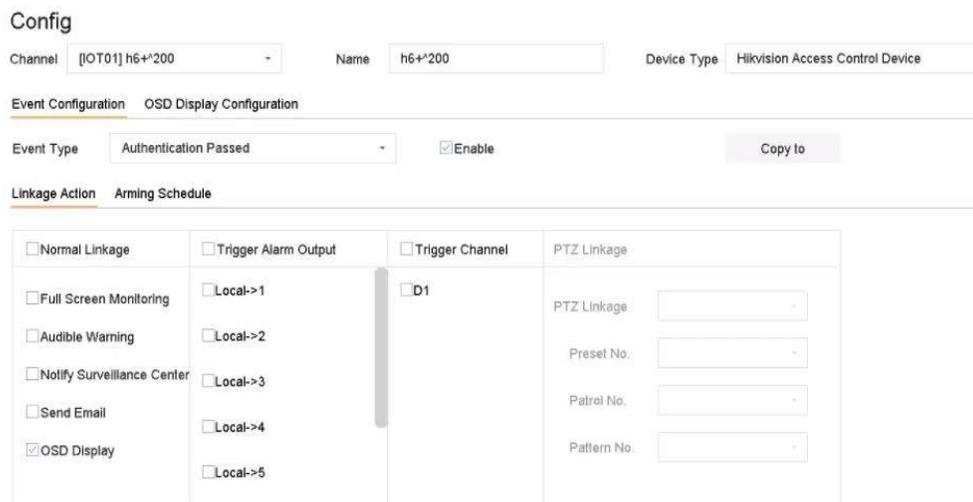
Hinwe

Für Zutrittskontrollgeräte ohne Videokanal. Sie müssen zuerst den Auslösekanal in der Konfiguration der Verknüpfungsaktion auswählen. Einzelheiten finden Sie unter **Konfigurieren von Verknüpfungsaktionen**.

-Klicken Sie  um hinzugefügte Alarmgeräte zu bearbeiten

3.2 Konfigurieren Sie die Verknüpfungsaktion und den Zeitplan für die Scharfschaltung

Konfigurieren Sie die Verknüpfungsaktionen und den Aktivierungszeitplan für Zugangskontroll- oder Alarmgeräte. Die Verknüpfungsaktionen werden ausgelöst, wenn der angegebene Alarm auftritt.



The screenshot shows a configuration window titled "Config". At the top, there are fields for "Channel" (set to "[IOT01] h6+*200"), "Name" (set to "h6+*200"), and "Device Type" (set to "Hikvision Access Control Device"). Below this, there are two tabs: "Event Configuration" and "OSD Display Configuration". Under "Event Configuration", the "Event Type" is set to "Authentication Passed", and the "Enable" checkbox is checked. A "Copy to" button is visible. The "Linkage Action" tab is active, showing a grid of options. On the left, there are checkboxes for "Normal Linkage", "Full Screen Monitoring", "Audible Warning", "Notify Surveillance Center", "Send Email", and "OSD Display" (which is checked). In the middle, there are checkboxes for "Trigger Alarm Output" and "Trigger Channel". Under "Trigger Alarm Output", there are five "Local->" options (1-5), all unchecked. Under "Trigger Channel", there is a "D1" checkbox, which is unchecked. On the right, there is a "PTZ Linkage" section with four dropdown menus for "PTZ Linkage", "Preset No.", "Patrol No.", and "Pattern No.", all currently empty.

Abbildung 3-4 IoT konfigurieren

Schritte

1. Klicken Sie auf  für ein hinzugefügtes IoT-Gerät.

-
- Wählen Sie den **Ereignistyp**. Die folgende Konfiguration ist nur für den ausgewählten Ereignistyp gültig.
 - Aktivieren** Sie.
 - Überprüfen Sie die Verknüpfungsaktionen nach Ihren Wünschen. Detaillierte Schritte finden Sie unter ***Verknüpfungsaktionen konfigurieren***.
-

Hinweis

Vollbild-Überwachung und **OSD-Anzeige** gelten nur für den ausgewählten **Auslösender Kanal**

- Klicken Sie auf **Zeitplan für die Scharfschaltung**.
- Konfigurieren Sie den Scharfschaltplan. Detaillierte Schritte finden Sie unter ***Scharfschaltungszeitplan konfigurieren***. Die Verknüpfungsaktion ist nur während des eingestellten Zeitplans gültig.
- Klicken Sie auf **Anwenden**.

3.3 OSD konfigurieren

Sie können von IoT-Geräten empfangene Alarminformationen in der Live-Ansicht anzeigen.

Schritte

- Klicken Sie auf  für ein hinzugefügtes IoT-Gerät.
- Prüfen Sie die **OSD-Anzeige** auf der Ereignis-Konfigurationsoberfläche.
- Wählen Sie den **Triggerkanal**.
- Klicken Sie auf **OSD-Anzeige Konfiguration**.

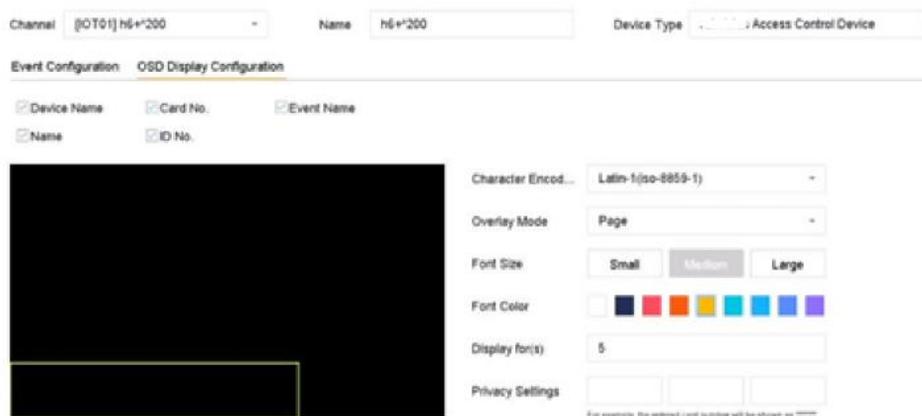


Abbildung 3-5 OSD-Konfiguration

- Wählen Sie die Elemente, einschließlich **Gerätename**, **Kartenummer**, **Ereignisname**, **Name** und **ID-Nummer**, die in der Live-Ansicht angezeigt werden sollen. Die Elemente gelten nur für Zugangskontrollgeräte.

6. Konfigurieren Sie die OSD-Eigenschaften.

Überlagerungsmodus - Blättern

Das OSD zeigt automatisch die neuen Alarminformationen an.

Überlagerungsmodus - Seite

Wenn das aktuelle OSD keine weiteren Alarminformationen mehr anzeigen kann, wird es automatisch auf eine neue Seite umgeschaltet.

Datenschutz-Einstellungen

Geben Sie die Datenschutzinformationen ein, die Sie maskieren möchten. Maskierte Datenschutzinformationen werden durch * ersetzt. Zu den Datenschutzinformationen gehören **Ereignis, Gerät, Karte, Name** und **ID**.

7. Passen Sie das Viereck des gelben Rahmens im Vorschaufenster an, um die Größe und Position des Bildschirmmenüs einzustellen.

8. Klicken Sie auf **Anwenden**.

3.4 Suche im IoT-Datensatz

Suchen Sie Alarme nach Zeit, nach Ereignistyp oder nach Kanal.

Schritte

1. Gehen Sie zur Schnittstelle für Ereignisaufzeichnungen.

- Zugangskontrolle: Gehen Sie zu **Business Application** → **IoT** → **Access Control** → **Card Swiping Record**.
- Alarmgerät: Gehen Sie zu **Business Application** → **IoT** → **Alarm** → **Search Data**.

The screenshot shows a search form with the following fields: 'Time' with a dropdown set to 'Custom' and two date pickers (2019-05-18 00:00:00 and 2019-05-18 23:59:59); 'Channel' with a dropdown set to '[All] IOT Channel'; 'Event Type' with a dropdown set to 'All'; 'Event Subtype' with a dropdown set to 'All'; 'Name' and 'Card No.' with text input fields. A blue 'Search' button is located below the form.

Abbildung 3-6 Ereignisaufzeichnung suchen (Zugriffskontrolle)

The screenshot shows a search form with the following fields: 'Time' with a dropdown set to 'Custom' and two date pickers (2019-05-19 00:00:00 and 2019-05-19 23:59:59); 'Channel' with a dropdown set to '[All] IOT Channel'; 'Main Type' with a dropdown set to 'GJD Alarm Event'; 'Sub Type' with a dropdown set to 'All'. A blue 'Search' button is located below the form.

Abbildung 3-7 Ereignisaufzeichnung suchen (Alarmgerät)

2. Geben Sie die Suchbedingungen an.

Hinweis

Name/Kartennummer: Wenn ein Ereignis beim Durchziehen der Karte eintritt, lädt das Zutrittskontrollgerät den Kartennamen und die Kartennummer in die Videoaufzeichnung. Sie können das Ereignis nach Kartennamen oder Kartennummer suchen.

3. Klicken Sie auf **Suchen**.

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

Total: 22 P: 1/1

Navigation icons: Home, Back, Forward, Refresh, Search, Go

Abbildung 3-8 Suchergebnis (Zugriffskontrolle)

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

Abbildung 3-9 Suchergebnis (Alarmgerät)

3.5 IoT Video/Bild

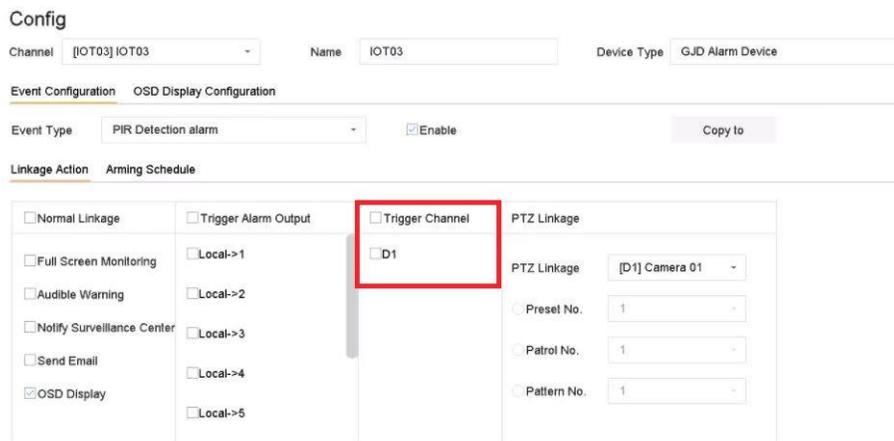
Konfigurieren Sie den Zeitplan für die Ereignisaufzeichnung oder -erfassung für den ausgewählten Auslösekanal. Der Kanal zeichnet automatisch Videos auf oder nimmt Bilder auf, wenn ein IoT-Alarm auftritt.

3.5.1 Konfigurieren der Ereignisaufzeichnung/-erfassung

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

Schritte

1. Klicken Sie auf  für ein hinzugefügtes IoT-Gerät.
2. Wählen Sie den gewünschten **Ereignistyp**.
3. **Aktivieren** Sie.
4. Aktivieren Sie die Option **Auslösekanal**, wenn Sie bei einem Alarm Ereignisvideos oder Bilder aufnehmen möchten.



Config

Channel [IOT03] IOT03 Name IOT03 Device Type GJD Alarm Device

Event Configuration OSD Display Configuration

Event Type PIR Detection alarm Enable Copy to

Linkage Action Arming Schedule

Normal Linkage Trigger Alarm Output Trigger Channel PTZ Linkage

Full Screen Monitoring Local->1

Audible Warning Local->2

Notify Surveillance Center Local->3

Send Email Local->4

OSD Display Local->5

PTZ Linkage [D1] Camera 01

Presel No. 1

Patrol No. 1

Pattern No. 1

Abbildung 3-10 Triggerkanal

5. Klicken Sie auf **Anwenden**.
6. Konfigurieren Sie den Zeitplan für die Ereignisaufzeichnung oder -erfassung. Im Folgenden werden die Schritte am Beispiel der Konfiguration der Ereignisaufzeichnung beschrieben. 1) Gehen Sie zu **Speicherung → Zeitplan → Aufzeichnung**. 2) Wählen Sie **Kameranummer** und markieren Sie **Zeitplan aktivieren**. Die Kamera sollte die Kamera sein, die Sie in Schritt 4 ausgewählt haben. 3) Wählen Sie als Aufzeichnungstyp "**Ereignis**". 4) Ziehen Sie die Maus auf der Zeitleiste, um den Zeitplan für die Aufzeichnung der Ereigniserkennung festzulegen. Weitere Informationen finden Sie unter **Konfigurieren der Planaufzeichnung**. 5) Klicken Sie auf **OK**.

Camera No. [D1] Camera 01

Enable Schedule

Advanced

■ Continuous
 ■ Event
 ■ Motion
 ■ Alarm
 ■ M | A
 ■ M & A
 ■ None

Edit

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon	1												
Tue	2												
Wed	3												
Thu	4												
Fri	5												
Sat	6												
Sun	7												

Apply
Copy to

Abbildung 3-11 Ereignisaufzeichnung

Ergebnis

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

3.5.2 Suche im IoT-Video/Bild

Durch IoT-Ereignisse ausgelöste Videos oder Bilder suchen.

Schritte

1. Gehen Sie zu **Dateiverwaltung** → **Alle Dateien**.

Time	Custom	2019-05-19 00:00:00	2019-05-19 23:59:59
Camera	[All] Camera		
File Type	Video		
Tag		File Status	All
Event Type	None		
Plate No.		Area/Country	None

Abbildung 3-12 Ereignis Video/Bild suchen

2. Suchbedingungen festlegen.

Kamera

Wählen Sie ihn als ausgewählten Auslösekanal in der Konfiguration der IoT-Verknüpfungsaktion aus.

Veranstaltungstyp

Wählen Sie das gewünschte IoT-Ereignis aus.

Datei Typ

Sie können das IoT-Video oder -Bild durchsuchen.

3. Klicken Sie auf **Suchen**.

4 Live-Ansicht

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

4.1 Live-Ansicht starten

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

- Wählen Sie ein Fenster aus und doppelklicken Sie auf eine Kamera in der Liste, um das Video von der Kamera im ausgewählten Fenster abzuspielen.
- Verwenden Sie die Symbolleiste am unteren Rand des Wiedergabefensters, um die Aufnahme, die sofortige Wiedergabe, das Ein- und Ausschalten des Tons, den digitalen Zoom, die Live-Ansichtsstrategie, die Anzeige von Informationen und den Start/Stop der Aufnahme usw. zu realisieren.

4.1.1 Konfigurieren der Live-View-Einstellungen

Die Einstellungen der Live-Ansicht können angepasst werden. Sie können die Ausgabeschnittstelle, die Verweilzeit für die Anzeige des Bildschirms, die Stummschaltung oder das Einschalten des Tons, die Bildnummer für jeden Kanal usw. konfigurieren.

Schritte

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



The screenshot shows a configuration panel for Live View settings. It includes the following elements:

- Video Output Interface:** A dropdown menu set to 'VGA/HDMI'.
- Event Output:** A dropdown menu set to 'VGA/HDMI'.
- Live View Mode:** A dropdown menu set to '2 * 2'.
- Dwell Time:** A dropdown menu set to '5s'.
- Enable Audio Output:** A checked checkbox.
- Volume:** A slider control ranging from 1 to 5, with a colored bar and a white knob.
- Full Screen Monitoring Dwell Time:** A dropdown menu set to '10s'.
- Apply:** A blue button at the bottom.

Abbildung 4-1 Live-Ansicht - Allgemein

2. Konfigurieren Sie die Parameter der Live-Ansicht.

Video Output Interface

Wählen Sie den zu konfigurierenden Videoausgang.

Live-View-Modus

Wählen Sie den Anzeigemodus für Live View, z.B. 2*2, 1*5, usw.

Verweilzeit

Die Zeit in Sekunden, die zwischen dem Umschalten der Kameras gewartet wird, wenn die automatische Umschaltung in der Live-Ansicht verwendet wird.

Aktivieren der Audioausgabe

Aktiviert/deaktiviert die Audioausgabe für den ausgewählten Videoausgang.

Band

Passen Sie die Lautstärke der Live-Ansicht, der Wiedergabe und des Zwei-Wege-Audios für die ausgewählte Ausgangsschnittstelle an.

Ereignis-Ausgang

Wählen Sie den Ausgang für die Anzeige des Ereignisvideos.

Vollbildüberwachung Verweilzeit

Stellen Sie die Zeit in Sekunden ein, nach der das Alarmereignis angezeigt werden soll.

3. Klicken Sie auf **OK**.

4.1.2 Layout der Live-Ansicht konfigurieren

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

Benutzerdefiniertes Layout der Live-Ansicht konfigurieren

Schritte

1. Gehen Sie zu **System → Live-Ansicht → Ansicht**.
2. Klicken Sie auf **Benutzerdefiniertes Layout festlegen**.
3. Klicken Sie auf der Benutzeroberfläche für die Layoutkonfiguration auf .
4. Bearbeiten Sie den Layoutnamen.
5. Wählen Sie in der Symbolleiste einen Fensterteilungsmodus aus.

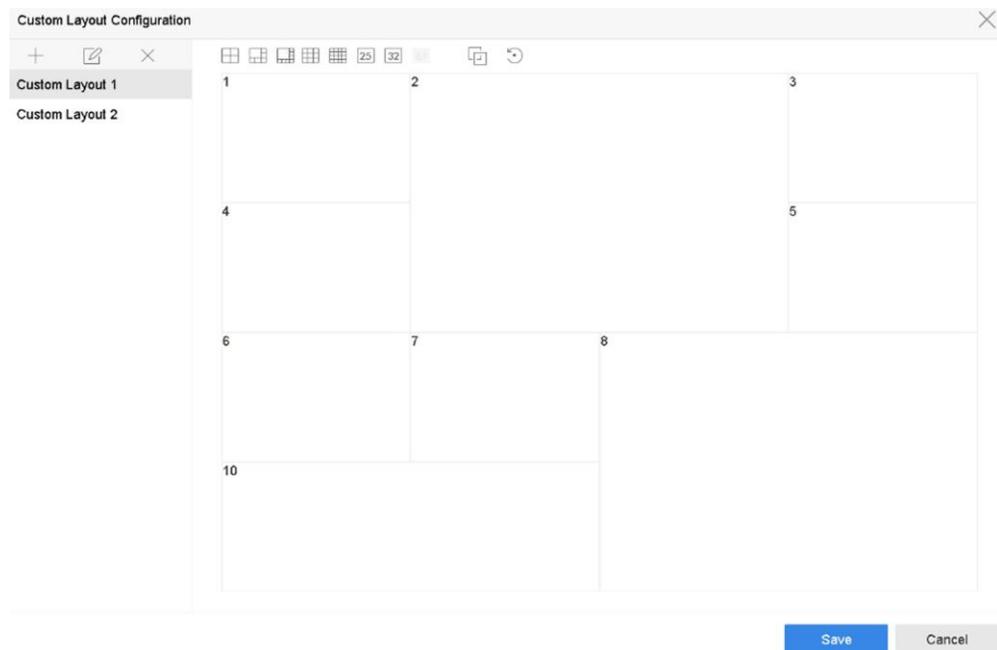


Abbildung 4-2 Layout der Live-Ansicht konfigurieren

6. Wählen Sie mehrere Fenster aus und klicken Sie auf , um die Fenster zu verbinden. Die ausgewählten Fenster müssen in einem rechteckigen Bereich liegen.
7. Klicken Sie auf **Speichern**.
Das erfolgreich konfigurierte Layout wird in der Liste angezeigt.
8. **Optional:** Wählen Sie ein Live-Ansicht-Layout aus der Liste und klicken Sie auf , um den Namen zu bearbeiten, oder klicken Sie auf , um den Namen zu löschen.

Konfigurieren des Live-Ansichtsmodus

Schritte

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

Hinweis

- Sie können die Kamera auch durch Klicken und Ziehen in das gewünschte Fenster der Live-Ansicht-Oberfläche bewegen, um die Reihenfolge der Kameras festzulegen.
- Sie können die Nummer in das Textfeld eingeben, um die Kamera schnell in der Liste zu suchen.

5. Klicken Sie auf **Anwenden**.

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

4.1.3 Haupt-/Hilfsanschluss umschalten

Nur das am Hauptanschluss angezeigte Bild kann das Hauptmenü aufrufen und das Gerät bedienen.

Sie können im Live-View-Modus auf  klicken oder zu **System** → **Live View** → **Allgemein** gehen, um den Haupt-/Hilfsanschluss umzuschalten.

Wenn Ihr Gerät über 2 HDMI-Schnittstellen und 2 VGA-Schnittstellen verfügt. HDMI1 und VGA1 sind die Hauptanschlüsse, und die Videoausgabe erfolgt gleichzeitig. HDMI2 und VGA2 sind Hilfsanschlüsse, und die Videoausgabe erfolgt gleichzeitig.

4.2 Digitaler Zoom

Der Digitalzoom vergrößert das Livebild in verschiedenen Vergrößerungen (1x bis 16x).

Schritte

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



Abbildung 4-3 Digitaler Zoom

4.3 Fisheye-Ansicht

Das Gerät unterstützt die Erweiterung der Fisheye-Kamera im Live-View- oder Wiedergabemodus.

Bevor Sie beginnen

- Die Funktion der Fisheye-Erweiterungsansicht wird nur von der
- Die angeschlossene Kamera muss die Fisheye-Ansicht unterstützen.

Schritte

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

180° Panorama ()	Schalten Sie das Live-View-Bild auf die 180°-Panorama-Ansicht um.	360° Panorama ()	Wechseln Sie in der Live-Ansicht zur 360°-Panorama-Ansicht.
PTZ- Erweiterung ()	Das PTZ Erweiterung ist die Nahaufnahme eines bestimmten Bereichs in der Fischaugenansicht oder im Panorama	Radiale Ausdehnung ()	In radialer Erweiterungsmodus wird die gesamte Weitwinkelansicht der Fischaugenkamera angezeigt. Dieser Ansichtsmodus ist

	<p>Erweiterung. Sie unterstützt die elektronische PTZ-Funktion, auch e-PTZ genannt.</p>		<p>Fisheye View genannt, weil es eine Annäherung an die die Sicht des konvexen Auges eines Fisches. Die Linse erzeugt gekrümmte Bilder eines großen Bereichs und verzerrt dabei die Perspektive und die Winkel der Objekte im Bild.</p>
--	---	--	---

4.4 3D-Positionierung

Die 3D-Positionierung vergrößert/verkleinert einen bestimmten Live-Bild-Bereich.

Schritte

1. Starten Sie die Live-Ansicht, und klicken Sie auf .
2. Vergrößern/Verkleinern des Bildes.
 - Vergrößern: Klicken Sie auf die gewünschte Position im Videobild und ziehen Sie einen rechteckigen Bereich in Richtung unten rechts, um hineinzuzoomen.
 - Herauszoomen: Ziehen Sie einen rechteckigen Bereich in die obere linke Richtung, um die Position in die Mitte zu verschieben und den rechteckigen Bereich zum Herauszoomen zu aktivieren.

4.5 Konfigurieren der Kanal-Null-Kodierung

Aktivieren Sie die Channel-Zero-Codierung, wenn Sie viele Kanäle in Echtzeit über einen Webbrowser oder eine CMS-Software (Client Management System) anzeigen möchten, um den Bandbreitenbedarf zu verringern, ohne die Bildqualität zu beeinträchtigen.

Schritte

1. Gehen Sie zu **System → Live-Ansicht → Kanal-Null**.
2. Aktivieren Sie **Kanal-Null-Kodierung aktivieren**.

Enable Channel-Zero Encoding

Frame Rate

Max. Bitrate Mode

Max. Bitrate(Kbps)

Abbildung 4-4 Kanal-Null-Codierung

3. Konfigurieren Sie **Bildrate**, **Max. Bitrate Modus** und **Max. Bitrate**. Eine höhere Bildrate und Bitrate erfordern eine höhere Bandbreite.
4. Klicken Sie auf **Anwenden**.
 Sie können alle Kanäle über das CMS oder den Webbrowser auf einem Bildschirm anzeigen.

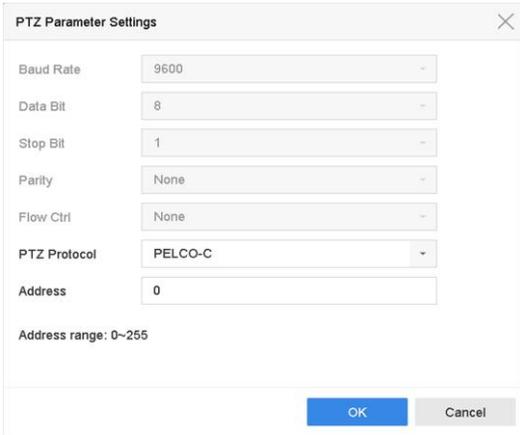
4.6 PTZ-Steuerung

4.6.1 PTZ-Parameter konfigurieren

Gehen Sie wie folgt vor, um die PTZ-Parameter einzustellen. Die PTZ-Parameter müssen konfiguriert werden, bevor Sie die PTZ-Kamera steuern können.

Schritte

1. Klicken Sie auf  in der Symbolleiste für die Schnelleinstellungen in der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf **PTZ-Parameter-Einstellungen**, um die PTZ-Parameter einzustellen.



PTZ Parameter Settings

Baud Rate

Data Bit

Stop Bit

Parity

Flow Ctrl

PTZ Protocol

Address

Address range: 0~255

Abbildung 4-5 PTZ-Parametereinstellungen

3. Bearbeiten Sie die PTZ-Parameter.

Hinweis

Alle Parameter sollten genau mit den Parametern der PTZ-Kamera übereinstimmen.

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

4.6.2 Eine Voreinstellung festlegen

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.

Schritte

1. Klicken Sie auf  in der Symbolleiste für die Schnelleinstellungen in der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf die Richtungstasten, um die Kamera an eine bestimmte Stelle zu bewegen.
3. Stellen Sie den Status von Zoom, Fokus und Blende ein.
4. Klicken Sie in die untere rechte Ecke der Live-Ansicht, um die Voreinstellung festzulegen.



Abbildung 4-6 Voreinstellung einstellen

5. Wählen Sie die voreingestellte Nr. (1 bis 255) aus der Dropdown-Liste.
6. Geben Sie den Namen der Voreinstellung ein.
7. Klicken Sie auf **Übernehmen**, um die Voreinstellung zu speichern.
8. **Optional:** Klicken Sie auf **Abbrechen**, um die Standortinformationen der Voreinstellung zu löschen.
9. **Optional:** Klicken Sie  in der unteren rechten Ecke der Live-Ansicht, um die konfigurierten Voreinstellungen anzuzeigen.



Abbildung 4-7 Ansicht der konfigurierten Voreinstellungen

4.6.3 Aufrufen einer Voreinstellung

Mit einer Voreinstellung kann die Kamera auf eine bestimmte Position, z. B. ein Fenster, zeigen, wenn ein Ereignis eintritt.

Schritte

1. Klicken Sie auf  in der Symbolleiste für die Schnelleinstellungen in der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf  die untere rechte Ecke der Live-Ansicht, um die Voreinstellung festzulegen.
3. Wählen Sie die voreingestellte Nr. aus der Dropdown-Liste.
4. Klicken Sie auf **Aufrufen**, um sie aufzurufen, oder klicken Sie auf  in der unteren rechten Ecke der Live-Ansicht, und klicken Sie auf die konfigurierte Voreinstellung, um sie aufzurufen.



Abbildung 4-8 Voreinstellung aufrufen (1)



Abbildung 4-9 Voreinstellung aufrufen (2)

4.6.4 Eine Patrouille festlegen

Patrouillen können so eingestellt werden, dass die PTZ zu Schlüsselpunkten bewegt wird und dort für eine bestimmte Dauer verbleibt, bevor sie zum nächsten Schlüsselpunkt weitergeht. Die Schlüsselpunkte entsprechen den Voreinstellungen.

Schritte

1. Klicken Sie auf  in der Symbolleiste für die Schnelleinstellungen in der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf **Patrouille**, um die Patrouille zu konfigurieren.

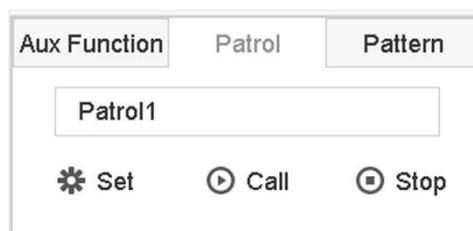


Abbildung 4-10 Konfiguration der Patrouille

3. Wählen Sie die Streifennummer.
4. Klicken Sie auf **Setzen**.

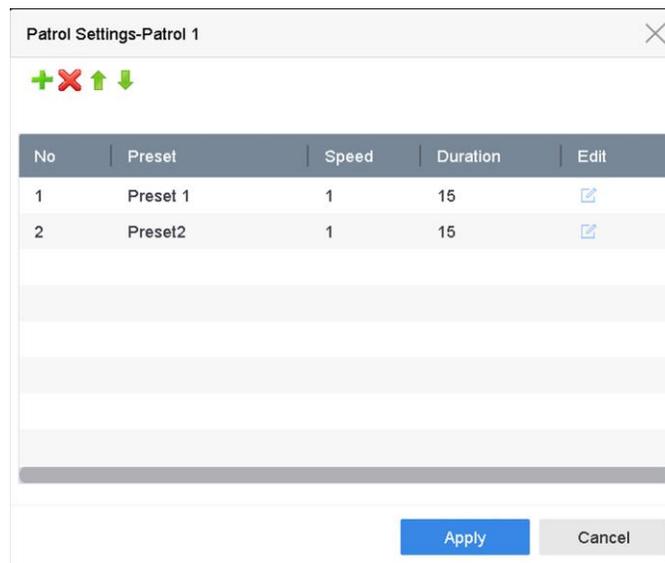


Abbildung 4-11 Patrouilleneinstellungen

5. Klicken Sie auf **+**, um der Patrouille einen Schlüsselpunkt hinzuzufügen.

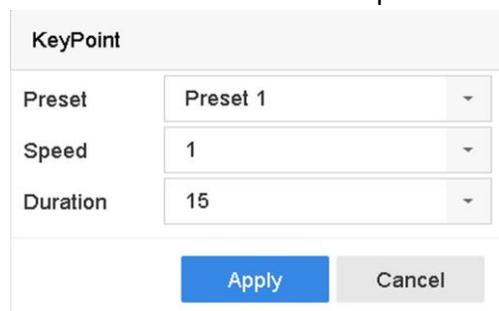


Abbildung 4-12 Schlüsselpunktkonfiguration

1) Konfigurieren Sie die Parameter der Schlüsselstelle.

Voreinstellung

Legt die Reihenfolge fest, in der die PTZ die Patrouille durchlaufen soll.

Geschwindigkeit

Legt die Geschwindigkeit fest, mit der sich die PTZ von einem Haltepunkt zum nächsten bewegt.

Dauer

Bezieht sich auf die Dauer des Aufenthalts am entsprechenden Schlüsselpunkt. 2) Klicken Sie auf **Übernehmen**, um die Schlüsselpunkte in der Patrouille zu speichern.

6. Andere Operationen sind wie folgt.

Operation	Beschreibung	Operation	Beschreibung
✘	Wählen Sie einen zu löschenden Schlüsselpunkt aus.	✍	Bearbeiten Sie den hinzugefügten Stichpunkt.
↑	Anpassen der Reihenfolge der Eckpunkte	↓	Anpassen der Reihenfolge der Eckpunkte

7. Klicken Sie auf **Übernehmen**, um die Patrouilleneinstellungen zu speichern.

4.6.5 Eine Patrouille rufen

Wenn Sie eine Patrouille aufrufen, bewegt sich die PTZ entsprechend dem vordefinierten Patrouillenweg.

Schritte

1. Klicken Sie auf  in der Symbolleiste für die Schnelleinstellungen in der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie im PTZ-Bedienfeld auf **Patrouille**.

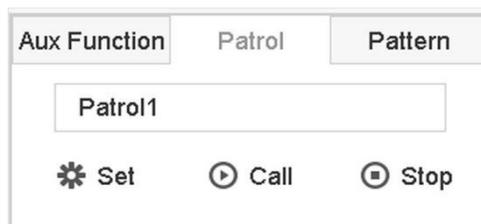


Abbildung 4-13 Konfiguration der Patrouille

3. Wählen Sie eine Patrouille.
4. Klicken Sie auf **Anrufen**, um die Patrouille zu starten.
5. **Optional:** Klicken Sie auf **Stopp**, um die Patrouille zu beenden.

4.6.6 Ein Muster festlegen

Muster können durch Aufzeichnung der PTZ-Bewegung festgelegt werden. Sie können das Muster aufrufen, damit sich die PTZ entsprechend dem vordefinierten Pfad bewegt.

Schritte

1. Klicken Sie auf  in der Symbolleiste für die Schnelleinstellungen in der Live-Ansicht der PTZ-Kamera.

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

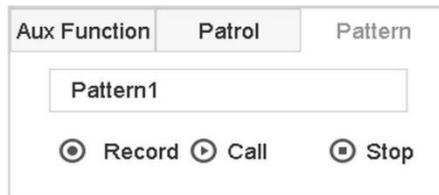


Abbildung 3-14 Musterkonfiguration

3. Wählen Sie die Musternummer.

4. Legen Sie das Muster fest.

- 1) Klicken Sie auf **Aufnahme**, um die Aufzeichnung zu starten.
- 2) Klicken Sie auf die entsprechenden Schaltflächen auf dem Bedienfeld, um die PTZ-Kamera zu bewegen.
- 3) Klicken Sie auf **Stopp**, um die Aufzeichnung zu beenden. Die PTZ-Bewegung wird als Muster aufgezeichnet.

4.6.7 Aufruf eines Musters

Gehen Sie wie folgt vor, um die PTZ-Kamera gemäß den vordefinierten Mustern zu bewegen.

Schritte

1. Klicken Sie auf  in der Symbolleiste für die Schnelleinstellungen in der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf "**Muster**", um das Muster zu konfigurieren.



Abbildung 4-15 Musterkonfiguration

3. Wählen Sie ein Muster aus.

4. Klicken Sie auf **Aufruf**, um das Muster zu starten.

5. **Optional:** Klicken Sie auf **Stopp**, um das Muster anzuhalten.

4.6.8 Lineare Scangrenze einstellen

Linear Scan löst einen Scan in horizontaler Richtung im vordefinierten Bereich aus.

Bevor Sie beginnen

Stellen Sie sicher, dass die angeschlossene IP-Kamera die PTZ-Funktion unterstützt und richtig angeschlossen ist.

Hinweis

Diese Funktion wird nur von einigen bestimmten Modellen unterstützt.

Schritt

1. Klicken Sie  in der Symbolleiste für die Schnelleinstellungen in der Live-Ansicht der PTZ-Kamera.
 2. Klicken Sie auf die Richtungsschaltflächen, um die Kamera an eine bestimmte Stelle zu bewegen, und klicken Sie auf **Linke Grenze** oder **Rechte Grenze**, um die Stelle mit der entsprechenden Grenze zu verknüpfen.
-

Hinweis

Die Speed Dome-Kuppel tastet linear von der linken Grenze zur rechten Grenze, und Sie müssen die linke Grenze auf der linken Seite der rechten Grenze einstellen. Außerdem darf der Winkel zwischen dem linken und dem rechten Grenzwert nicht größer als 180° sein.

4.6.9 Parken mit einem Tastendruck

Bestimmte Speed Dome-Modelle können so konfiguriert werden, dass sie nach einer gewissen Zeit der Inaktivität (Parkzeit) automatisch eine vordefinierte Parkaktion (Scan, Voreinstellung, Patrouille usw.) starten.

Bevor Sie beginnen

Vergewissern Sie sich vor der Verwendung dieser Funktion, dass die angeschlossene Kamera Zeilenscan unterstützt und das Grundig-1-Protokoll verwendet.

Schritte

1. Klicken Sie auf  in der Symbolleiste für die Schnelleinstellungen in der Live-Ansicht der PTZ-Kamera.
2. Klicken Sie auf **Parken (Schnellpatrouille)**, **Parken (Patrouille 1)** oder **Parken (Voreinstellung 1)**, um die Parkaktion zu aktivieren.

Parken (Schnellpatrouille)

Die Kuppel startet den Rundgang von Voreinstellung 1 bis Voreinstellung 32 in der Reihenfolge nach der Parkzeit. Nicht definierte Voreinstellungen werden übersprungen.

Parken (Patrouille 1)

Nach der Parkzeit beginnt die Kuppel, sich entsprechend dem vordefinierten Patrouillenweg 1 zu bewegen.

Parken (Voreinstellung 1)

Die Kuppel bewegt sich nach der Parkzeit zu der vordefinierten Position 1.

Hinweis

Die Parkzeit kann nur über die Konfigurationsoberfläche der Speed Dome-Kamera eingestellt werden. Der Standardwert ist standardmäßig 5s.

- 3. Wahlweise:** Klicken Sie auf **Parken stoppen (Schnellpatrouille)**, **Parken stoppen (Patrouille 1)** oder **Parken stoppen (Voreinstellung 1)**, um die Funktion zu deaktivieren.

5 Aufnahme und Wiedergabe

5.1 Aufzeichnung

5.1.1 Konfigurieren der Aufzeichnungsparameter

Gehen Sie zu **Kamera** → **Videoparameter**.

Hauptstrom

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

Bildfrequenz (FPS - Frames Per Second)

Sie gibt an, wie viele Bilder pro Sekunde aufgezeichnet werden. Eine höhere Bildrate ist vorteilhaft, wenn der Videostrom in Bewegung ist, da so die Bildqualität durchgehend erhalten bleibt.

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

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.

H.264+ aktivieren

H.264+ kombiniert intelligente Analysetechnologie mit prädiktiver Kodierung, Rauschunterdrückung und langfristiger Bitratenkontrolle, um eine niedrigere Bitrate zu realisieren, was eine wichtige Rolle bei der Senkung der Speicherkosten spielt und einen höheren Investitionsertrag ermöglicht.

H.265+ aktivieren

H.265+ ist eine optimierte Kodierungstechnologie, die auf dem Standard H.265/HEVC-Kompression basiert. Mit H.265+ ist die Videoqualität fast die gleiche wie die von H.265/HEVC, jedoch mit weniger benötigter Übertragungsbandbreite und Speicherkapazität.

Hinweis

- Eine höhere Auflösung, Bildrate und Bitrate bieten eine bessere Videoqualität, erfordern aber auch mehr Internet-Bandbreite und benötigen mehr Speicherplatz auf der Festplatte.
- Die H.264+ oder H.265+ Codierungstechnologie ist für alle Grundig-Modelle verfügbar.

Sub-Stream

Sub-Stream ist ein zweiter Codec, der neben dem Haupt-Stream läuft. Er ermöglicht es Ihnen, die ausgehende Internet-Bandbreite zu reduzieren, ohne die Qualität der direkten Aufnahme zu beeinträchtigen.

Der Sub-Stream wird häufig ausschließlich von Anwendungen zur Anzeige von Live-Videos verwendet. Benutzer mit begrenzten Internetgeschwindigkeiten können von dieser Einstellung am meisten profitieren.

Bild

Das Bild bezieht sich auf die Livebild-Aufnahme im Dauer- oder Ereignisaufnahmetyp.
(Speicherung → Aufnahmezeitplan → Erweitert)

Bildqualität

Stellen Sie die Bildqualität auf niedrig, mittel oder hoch ein. Je höher die Bildqualität, desto mehr Speicherplatz wird benötigt.

Intervall

Das Intervall für die Aufnahme von Livebildern.

Erfassungsverzögerungszeit

Die Dauer der Aufnahme von Bildern.

Konfigurieren der erweiterten Aufnahmeparameter

Schritte

1. Gehen Sie zu **Speicherung → Zeitplan → Aufnahme**.
2. Markieren Sie **Zeitplan aktivieren**, um die geplante Aufnahme zu aktivieren.
3. Klicken Sie auf **Erweitert**, um die erweiterten Parameter einzustellen.

The screenshot shows a dialog box titled "Advanced Parameters" with the following settings:

- Record Audio:
- Pre-Record: 5s (dropdown menu)
- Post-Record: 5s (dropdown menu)
- Stream Type: Main Stream (dropdown menu)
- Expired Time (day): 5 (text input)
- Redundant Record/Capture

At the bottom, there are two buttons: "OK" (blue) and "Cancel" (grey).

Abbildung 5-1 Erweiterte Aufnahmeeinstellungen

Audio aufzeichnen

Aktivieren oder deaktivieren Sie die Audioaufnahme.

Voraufzeichnung

Die Zeit, die Sie für die Aufzeichnung vor der geplanten Zeit oder dem Ereignis festlegen.

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

Für die Aufzeichnung können Sie zwischen Hauptstream und Substream wählen. Wenn Sie Sub-Stream wählen, können Sie bei gleichem Speicherplatz eine längere Zeit aufnehmen.

Abgelaufene Zeit

Die abgelaufene Zeit ist der Zeitraum, in dem eine aufgezeichnete 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.

Redundanter Datensatz/Erfassung

Wenn Sie die redundante Aufzeichnung oder Aufnahme aktivieren, speichern Sie die Aufzeichnung und das aufgenommene Bild auf der redundanten Festplatte.

5.1.2 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.

Gehen Sie zu **Kamera → Weitere Einstellungen → H.265 Auto Switch Configuration**, um die Funktion zu aktivieren.

5.1.3 ANR

Mit der Funktion ANR (Automatic Network Replenishment) speichert die IP-Kamera die Aufnahmedateien im lokalen Speicher, wenn die Netzwerkverbindung unterbrochen wird, und lädt die Dateien auf das Gerät hoch, wenn die Netzwerkverbindung wiederhergestellt wird.

Schritte

1. Melden Sie sich über einen Webbrowser an Ihrem Gerät an und gehen Sie zu **Konfiguration → Speicher → Zeitplaneinstellungen → Erweitert**.

2. Aktivieren Sie **ANR aktivieren**.

3. Klicken Sie auf **OK**.

5.1.4 Manuelle Aufzeichnung

Sie können auf  klicken, um die Aufnahme von Videos in der Live-Ansicht manuell zu starten/stoppen.

5.1.5 Planaufzeichnung konfigurieren

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

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie die Festplatten im Gerät installiert oder die Netzwerkfestplatten hinzugefügt haben, bevor Sie die Videodateien, Bilder und Protokolldateien speichern.
- Bevor Sie **Bewegung, Alarm, M | A** (Bewegung oder Alarm), **M & A** (Bewegung und Alarm) und ereignisgesteuerte Aufzeichnung und Erfassung aktivieren, müssen Sie die Einstellungen für die Bewegungserkennung, die Alarmeingänge und andere Ereignisse konfigurieren. Einzelheiten finden Sie unter.

Schritte

1. Gehen Sie zu **Speicherung → Zeitplan → Aufnahme**.
2. Wählen Sie eine Kamera aus.
3. Aktivieren Sie **Zeitplan aktivieren**.
4. Wählen Sie eine Aufnahmeart aus.

Kontinuierlich

Geplante Aufnahme.

Veranstaltung

Aufzeichnung ausgelöst durch alle ereignisgesteuerten Alarme.

Antrag

Aufzeichnung ausgelöst durch Bewegungserkennung.

Alarm

Aufzeichnung ausgelöst durch Alarm.

M/A

Die Aufzeichnung wird entweder durch Bewegungserkennung oder Alarm ausgelöst.

FUSIONEN UND ÜBERNAHMEN

Aufzeichnung ausgelöst durch Bewegungserkennung und Alarm.

POS

Aufzeichnung ausgelöst durch POS und Alarm.

5. Ziehen Sie den Cursor auf die Zeitleiste, um den Aufzeichnungszeitplan festzulegen.

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon	1	1	1	1	1	1	1	1	1	1	1	1	1
Tue	2	2	2	2	2	2	2	2	2	2	2	2	2
Wed	3	3	3	3	3	3	3	3	3	3	3	3	3
Thu	4	4	4	4	4	4	4	4	4	4	4	4	4
Fri	5	5	5	5	5	5	5	5	5	5	5	5	5
Sat	6	6	6	6	6	6	6	6	6	6	6	6	6
Sun	7	7	7	7	7	7	7	7	7	7	7	7	7

Abbildung 5-2 Zeitplan für die Aufzeichnung

Hinweis

- Sie können die obigen Schritte wiederholen, um für jeden Tag der Woche eine Zeitplanaufnahme oder -erfassung einzustellen.
- Die kontinuierliche Aufzeichnung wird standardmäßig auf jeden Tag angewendet.

6. **Optional:** Kopieren Sie den Aufnahmeplan auf andere Kameras.

1) Klicken Sie auf **Kopieren nach**.

2) Wählen Sie die zu duplizierende(n) Kamera(s) mit denselben Zeitplaneinstellungen aus. 3) Klicken Sie auf **OK**.

7. Klicken Sie auf **Anwenden**.

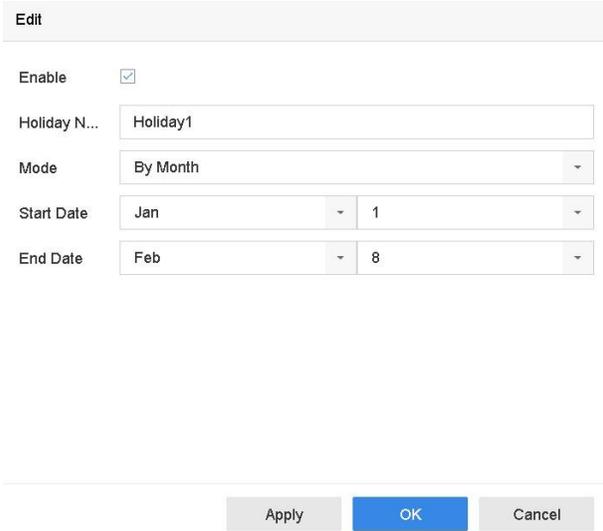
5.1.6 Urlaubsaufzeichnung konfigurieren

Wenn Sie einen anderen Plan für die Aufzeichnung im Urlaub haben möchten, können Sie mit dieser Funktion den Zeitplan für die Aufzeichnung im Urlaub für das ganze Jahr festlegen.

Schritte

1. Gehen Sie zu **System → Urlaub**.

-
2. Wählen Sie einen Urlaubsartikel aus der Liste aus.
 3. Klicken Sie auf , um den ausgewählten Feiertag zu bearbeiten.
 4. **Aktivieren Sie.**



Edit	
Enable	<input checked="" type="checkbox"/>
Holiday N...	Holiday1
Mode	By Month
Start Date	Jan 1
End Date	Feb 8
Apply OK Cancel	

Abbildung 5-3 Feiertageinstellungen bearbeiten

5. Legen Sie **Urlaubsname**, **Modus**, **Start-** und **Enddatum** fest.
6. Klicken Sie auf **OK**.
7. Legen Sie den Zeitplan für die Urlaubsaufzeichnung fest. Weitere Informationen finden Sie unter **Planaufzeichnung konfigurieren**.

5.2 Wiedergabe

5.2.1 Sofortige Wiedergabe

Mit der Sofortwiedergabe kann das Gerät die in den letzten fünf Minuten aufgezeichneten Videodateien wiedergeben. Wenn kein Video gefunden wird, bedeutet dies, dass in den letzten fünf Minuten keine Aufzeichnung stattgefunden hat.

Nachdem Sie die Kamera in der **Live-Ansicht** ausgewählt haben, können Sie den Cursor zum unteren Rand des Fensters bewegen, um auf die Symbolleiste zuzugreifen, und auf  klicken, um die Sofortwiedergabe zu starten.



Abbildung 4-4 Wiedergabebeschnittstelle

5.2.2 Normales Video abspielen

Gehen Sie zu **Wiedergabe**, wählen Sie Datum und Kamera(s) aus und verwenden Sie die Symbolleiste am unteren Rand, um die Wiedergabe durchzuführen. Siehe **Wiedergabeoperationen**. Sie können auf Kamera(s) klicken, um die gleichzeitige Wiedergabe mehrerer Kameras durchzuführen.

Note

256

x playing speed is supported.



Abbildung 4-5 Wiedergabebeschnittstelle

5.2.3 Smart Searched Video abspielen

Im intelligenten Wiedergabemodus kann das Gerät Videos analysieren, die Bewegungs-, Linien- oder Einbruchserkennungsinformationen enthalten, und diese rot markieren.

Gehen Sie zu **Wiedergabe**, klicken Sie auf **Smart** und dann auf Bewegungserkennung (👤), Linienkreuzungserkennung (🔗) oder Eindringlingserkennung (🚪) in der unteren Symbolleiste,



um das Video nach Ihren Wünschen zu durchsuchen und abzuspielen. Bei bestimmten Kameramodellen, die Personen und Fahrzeuge erkennen können, können Sie auf klicken , um nach Personen und Fahrzeugen zu suchen.

Bei der Wiedergabe von Personen- und Fahrzeugvideos kann nicht nach Videos zur Erkennung von Linienkreuzungen () und zur Erkennung von Eindringlingen () gesucht werden, die auf den Personen- und Fahrzeugvideos basieren.



Abbildung 5-6 Amortisation durch intelligente Suche

5.2.4 Benutzerdefinierte gesuchte Dateien abspielen

Sie können Videos nach benutzerdefinierten Suchbedingungen abspielen.

Schritte

1. Gehen Sie zu **Wiedergabe**.
2. Wählen Sie die Kamera(s) aus der Liste aus.
3. Klicken Sie links unten auf **Benutzerdefinierte Suche**.
4. Geben Sie die Suchbedingungen ein, einschließlich **Zeit**, **Dateistatus**, **Ereignistyp** usw.

Abbildung 5-7
Benutzerdefinierte Suche

5. Klicken Sie auf **Suchen**.

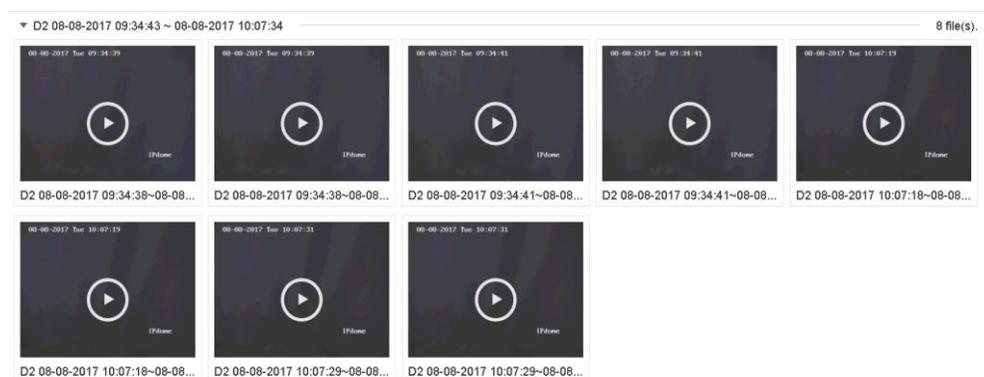


Abbildung 5-8 Benutzerdefinierte gesuchte Videodateien

6. Wählen Sie eine Datei aus und starten Sie die Wiedergabe des Videos auf der Suchergebnisoberfläche.

5.2.5 Tag-Dateien abspielen

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

Tag-Dateien hinzufügen

Schritte

1. Gehen Sie zu **Wiedergabe**.
2. Suchen und Abspielen der Videodatei(en).
3. Klicken Sie auf , um die Markierung hinzuzufügen.
4. Bearbeiten Sie die Tag-Informationen.
5. Klicken Sie auf **OK**.

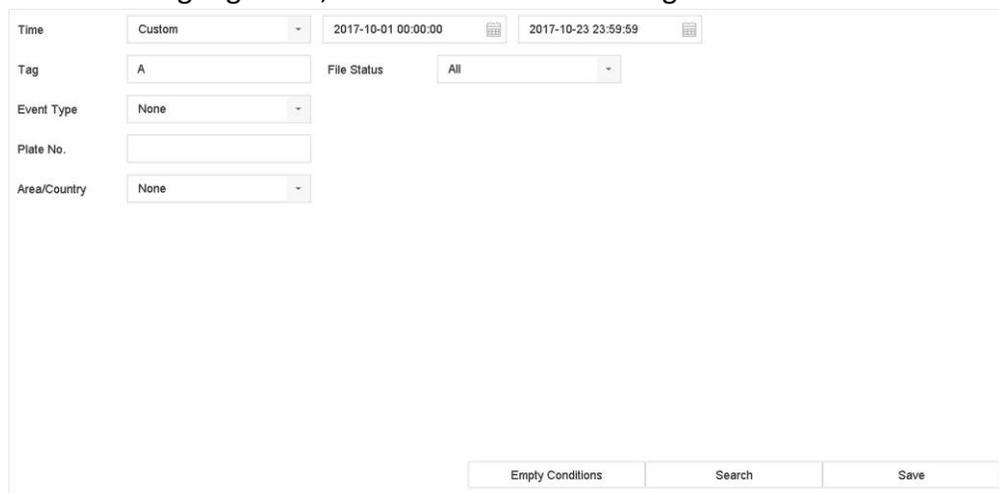
Hinweis

Max. 64 Tags können zu einem einzelnen Video

Tag-Dateien abspielen

Schritte

1. Gehen Sie zu **Wiedergabe**.
2. Klicken Sie links unten auf **Benutzerdefinierte Suche**.
3. Geben Sie die Suchbedingungen ein, einschließlich Zeit und Tag-Schlüsselwort.



Time	Custom	2017-10-01 00:00:00	2017-10-23 23:59:59
Tag	A	File Status	All
Event Type	None		
Plate No.			
Area/Country	None		

Empty Conditions Search Save

Abbildung 5-9 Tag-Suche

4. Klicken Sie auf **Suchen**.

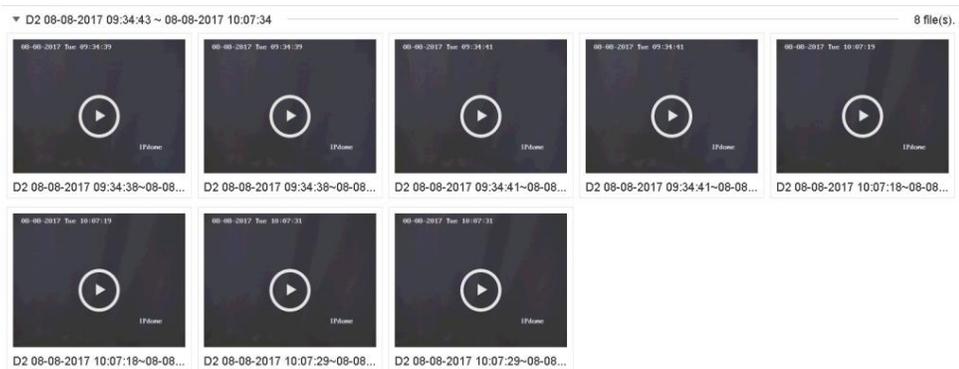


Abbildung 5-10 Durchsuchte Tag-Dateien

5. Wählen Sie eine Tag-Datei aus, und spielen Sie das Video auf der Suchergebnisoberfläche ab.

5.2.6 Abspielen von Subperioden

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

Schritte

1. Gehen Sie zu **Wiedergabe**.
2. Klicken Sie in der linken unteren Ecke auf **HH**.
3. Wählen Sie eine Kamera aus.
4. Legen Sie die Start- und Endzeit für die Videosuche fest.
5. Wählen Sie in der rechten unteren Ecke eine andere Multi-Periode aus, z. B. 4-Perioden.

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.

5.2.7 Externe Dateien abspielen

Sie können Dateien von externen Speichergeräten wiedergeben.

Bevor Sie beginnen

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

Schritte

-
1. Gehen Sie zu **Wiedergabe**.
 2. Klicken Sie in die untere linke Ecke.
 3. Klicken Sie auf , oder doppelklicken Sie auf die Datei, um sie abzuspielen.

5.3 Abspielvorgänge

5.3.1 Videoclips bearbeiten

Sie können Videoclips während der Wiedergabe schneiden und exportieren.

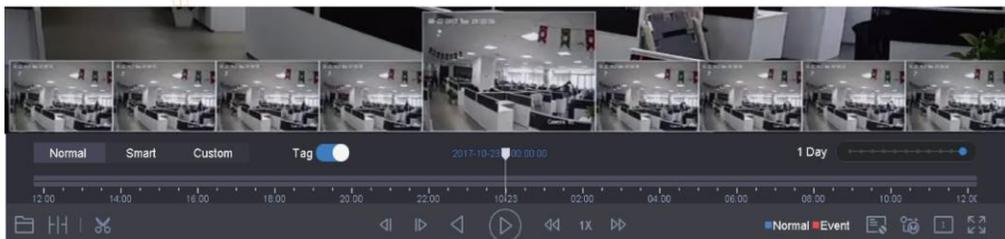
Schritte

1. **Zur Wiedergabe** gehen
2. Klicken Sie in der unteren Symbolleiste auf .
3. Legen Sie die Start- und Endzeit fest. Sie können auf  klicken, um den Zeitraum einzustellen, oder ein Zeitsegment auf der Zeitleiste festlegen.
4. Klicken Sie auf , um den Videoclip auf einem Speichermedium zu speichern.

5.3.2 Thumbnails-Ansicht

Mit der Miniaturansicht auf der Wiedergabeschnittstelle können Sie die gewünschten Videodateien bequem in der Zeitleiste finden.

Positionieren Sie den Cursor im Wiedergabemodus auf der Zeitleiste, um eine Vorschau der Miniaturbilder zu erhalten.



**Abbildung 5-11 Ansicht der
Miniaturansichten**

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

6 Bildaufzeichnung

6.1 Parameter konfigurieren

Das Bild bezieht sich auf das Live-Bild, das bei der Dauer- oder Ereignisaufzeichnung aufgenommen wird.

Sie können die Bildparameter unter **Storage** → **Capture Schedule** → **Advanced** bearbeiten.

Auflösung

Stellen Sie die Bildauflösung ein.

Bildqualität

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

Intervall

Das Intervall für die Livebildaufnahme.

Erfassungsverzögerungszeit

Die Dauer der Aufnahme von Bildern.

6.2 Erfassungszeitplan konfigurieren

Das Gerät nimmt die Bilder automatisch nach dem festgelegten Zeitplan auf.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie Festplatten installiert oder Netzwerkfestplatten zur Speicherung hinzugefügt haben.

Schritte

1. Gehen Sie zu **Speicher** → **Erfassungszeitplan**.
2. Wählen Sie eine Kamera aus.
3. Legen Sie den Zeitplan für die Bildaufnahme fest. Einzelheiten zu den Zeitplaneinstellungen finden Sie unter **Planaufzeichnung konfigurieren**.

6.3 Zeitplan für die Urlaubserfassung konfigurieren

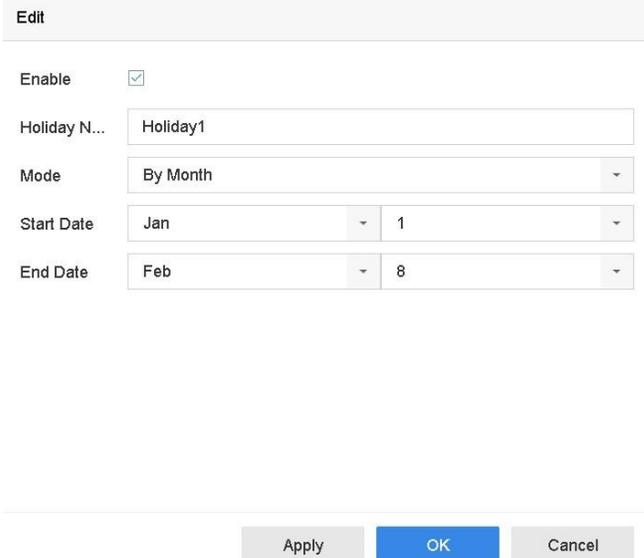
Sie können den Aufnahmeplan für die Feiertage des Jahres festlegen. Der Rekorder folgt dem Ferien-Aufnahmeplan als Aufnahmepriorität während der Ferien.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie Festplatten installiert oder Netzwerkfestplatten zur Speicherung hinzugefügt haben.

Schritte

1. Gehen Sie zu **System → Urlaub**.
2. Wählen Sie einen Urlaubsartikel aus der Liste und klicken Sie auf  .
3. **Aktivieren Sie.**
4. Bearbeiten Sie die Urlaubsparameter, einschließlich Name, Modus und Datum.



Edit	
Enable	<input checked="" type="checkbox"/>
Holiday N...	Holiday1
Mode	By Month
Start Date	Jan 1
End Date	Feb 8

Apply OK Cancel

Abbildung 6-1 Feiertageinstellungen bearbeiten

5. Klicken Sie auf **OK**.
6. Legen Sie den Zeitplan für die Urlaubsaufzeichnung fest. Einzelheiten zu den Zeitplaneinstellungen finden Sie im Kapitel **Planaufzeichnung konfigurieren**.

7 Ereignis

7.1 Normaler Ereignisalarm

7.1.1 Konfigurieren von Bewegungserkennungsalarmen

Die Bewegungserkennung ermöglicht es dem Gerät, sich bewegende Objekte im überwachten Bereich zu erkennen und Alarme auszulösen.

Schritte

1. Gehen Sie zu **System → Ereignis → Normales Ereignis → Bewegungserkennung**.
2. Wählen Sie eine Kamera aus.
3. **Aktivieren** Sie.
4. Legen Sie die Bewegungserkennungsregel fest.

Denn die Kameras verfügen über eine Personen- und Fahrzeugerkennung.	Klicken Sie auf Bereich zeichnen , um den/die Erkennungsbereich(e) auf dem Vorschaubildschirm zu zeichnen. Stellen Sie die Zielerkennung auf " Menschlicher Körper " oder " Fahrzeug " ein, um Alarme zu verwerfen, die nicht durch einen menschlichen Körper oder ein Fahrzeug ausgelöst werden.
Denn die Kameras haben keine Funktion zur Erkennung von Personen und Fahrzeugen.	Klicken Sie auf Vollbild , um den gesamten Bildschirm als Erkennungsbereich festzulegen, oder ziehen Sie auf dem Vorschaubildschirm, um den benutzerdefinierten Erkennungsbereich zu zeichnen.

5. **Empfindlichkeit** einstellen (0-100). Mit der Empfindlichkeit können Sie kalibrieren, wie schnell Bewegungen den Alarm auslösen. Ein höherer Wert führt dazu, dass die Bewegungserkennung leichter ausgelöst wird.
6. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
7. Legen Sie Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.

7.1.2 Konfigurieren von Videoverlustalarmen

Die Videoverlusterkennung erkennt den Videoverlust eines Kanals und leitet Alarmmaßnahmen ein.

Schritte

1. Gehen Sie zu **System → Ereignis → Normales Ereignis → Videoverlust**.
2. Wählen Sie eine Kamera aus.
3. **Aktivieren** Sie.

-
4. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
 5. Legen Sie Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.

7.1.3 Konfigurieren von Video-Manipulationsalarmen

Die Video-Manipulationserkennung löst einen Alarm aus, wenn das Kameraobjektiv verdeckt ist, und leitet Alarmmaßnahmen ein.

Schritte

1. Gehen Sie zu **System → Ereignis → Normales Ereignis → Video-Manipulation**.
2. Wählen Sie eine Kamera aus.
3. **Aktivieren** Sie.
4. Legen Sie den Bereich für die Video-Manipulation fest. Ziehen Sie auf dem Vorschaubildschirm, um den benutzerdefinierten Bereich für die Video-Manipulation zu zeichnen.
5. **Empfindlichkeit** einstellen (0-2). Es sind 3 Stufen verfügbar. Die Empfindlichkeit legt fest, wie schnell Bewegungen den Alarm auslösen. Ein höherer Wert löst die Erkennung von Videomanipulationen leichter aus.
6. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
7. Legen Sie Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.

7.1.4 Konfigurieren von Sensor-Alarmen

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

Schritte

1. Gehen Sie zu **System → Ereignis → Normales Ereignis → Alarmeingang**.
2. Wählen Sie ein Alarmeingangselement aus der Liste aus und klicken Sie auf .
3. Wählen Sie den Alarmeingangstyp.
4. Bearbeiten Sie den Alarmnamen.
5. **Eingabe** prüfen.
6. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
7. Legen Sie Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.

7.1.5 Ereignisalarme konfigurieren

Systemereignisse können so konfiguriert werden, dass sie den Ereignishinweis im Live-Ansichtsfenster übernehmen und Alarmausgabe- und Verknüpfungsaktionen auslösen.

Schritte

1. Gehen Sie zu **System → Ereignis → Normales Ereignis → Systemereignis**.
2. **Optional:** Aktivieren Sie den Ereignishinweis, um ihn im Fenster der Live-Ansicht anzuzeigen.

1) Aktivieren Sie **Ereignis-Hinweis aktivieren**.

2) Klicken Sie auf , um den/die Ereignistyp(en) auszuwählen, die den Ereignishinweis aufnehmen sollen.

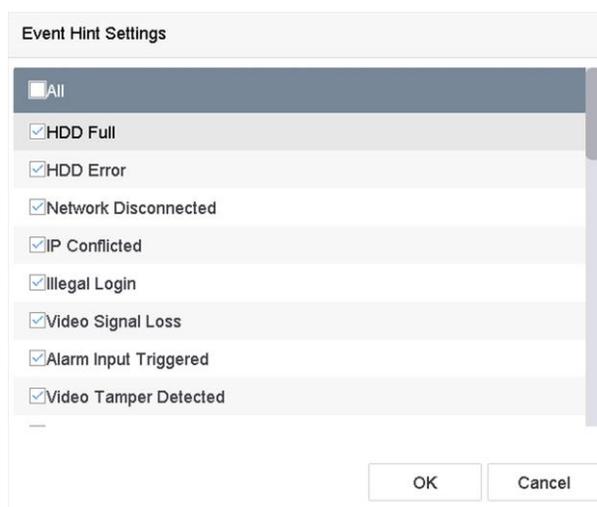


Abbildung 7-1 Ereignishinweis-Einstellungen 3.

Wählen Sie eine Ereignisart aus.

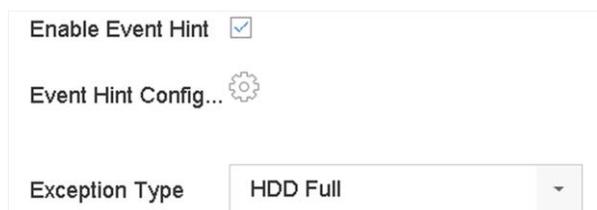


Abbildung 7-2 Behandlung von Ereignissen

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

7.1.6 Kombinierten Alarm konfigurieren

Kombinierter Alarm kombiniert Ereignisse mit Alarmeingängen. Der kombinierte Alarm wird ausgelöst, wenn er Alarme sowohl vom Alarmeingang als auch von Ereignissen empfängt. Zu den Ereignistypen gehören die Bewegungserkennung, die Erkennung von Videomanipulationen und andere intelligente Ereignisse wie die Erkennung von Leitungsüberschreitungen, die Erkennung von Eindringlingen usw.

Bevor Sie beginnen

Vergewissern Sie sich, dass dem Kanal der gewünschte Ereignisalarm zugewiesen wurde und dass der Alarmeingang konfiguriert wurde (siehe ***Konfigurieren von Sensoralarmen***).

Schritte

1. Gehen Sie zu **System → Ereignis → Normales Ereignis → Alarmeingang**.
2. Wählen Sie ein Alarmeingangselement aus der Liste aus und klicken Sie auf .
3. Wählen Sie **Einstellungen als Eingabe**.
4. Klicken Sie auf **Kombinierter Alarm**.
5. Wählen Sie einen Kanal nach Ihren Wünschen.
6. Wählen Sie **Kombiniertes Alarmereignis**.
7. Klicken Sie auf **Anwenden**.

Hinweis

Der kombinierte Alarmplan und die Verknüpfungsaktion sind mit dem ausgewählten Ereignis identisch.

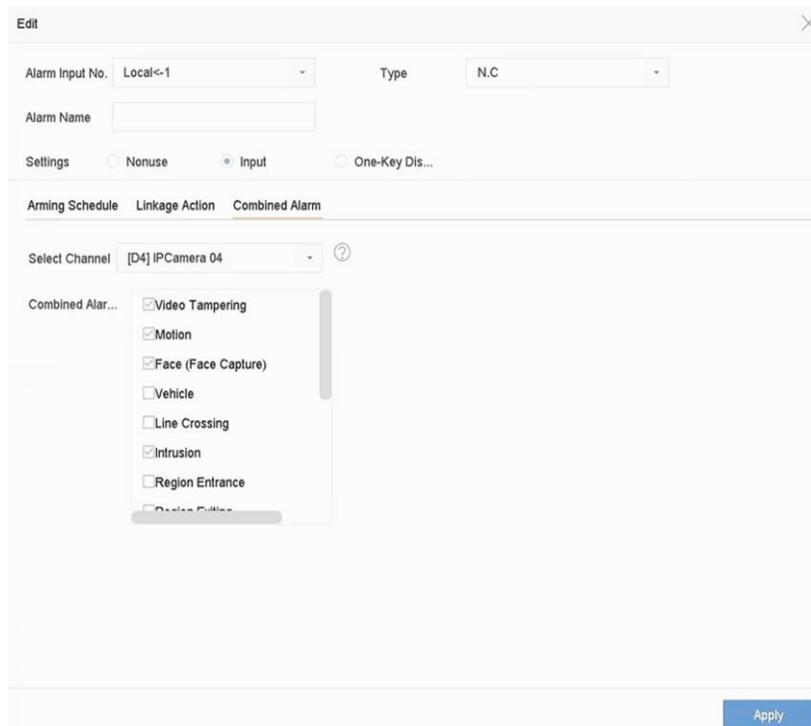


Abbildung 7-3 Kombiniertes Alarm

7.2 VCA-Ereignis-Alarm

Das Gerät unterstützt den Empfang von VCA-Erkennungen, die von angeschlossenen IP-Kameras gesendet werden. Aktivieren und konfigurieren Sie zunächst die VCA-Erkennung auf der Schnittstelle für die IP-Kameraeinstellungen.

Hinweis

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

7.2.1 Erkennung von Gesichtern

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

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Klicken Sie auf "**Gesichtserkennung**".

The screenshot shows a configuration window for 'Arming Schedule' with a 'Linkage Action' tab. At the top, there is a checkbox for 'Enable Face...' and a 'Sensitivity 1' slider set to 3. Below the tabs, there are radio buttons for 'Continuous' (selected) and 'None', and an 'Edit' button. The main area is a grid with days of the week (Mon-Sun) on the y-axis and hours (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24) on the x-axis. All cells in the grid are filled with blue, indicating a continuous schedule. An 'Apply' button is located at the bottom left of the grid area.

Abbildung 7-4 Gesichtserkennung

3. Wählen Sie eine zu konfigurierende Kamera aus.
4. Aktivieren Sie die Option **Gesichtserkennung aktivieren**.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen Bilder der Gesichtserkennung zu speichern.
6. Stellen Sie die Erkennungsempfindlichkeit ein. Empfindlichkeitsbereich: [1-5]. Je höher der Wert ist, desto leichter wird das Gesicht erkannt.
7. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltplan konfigurieren** 8. Legen Sie Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**

9. Klicken Sie auf **Anwenden**.

7.2.2 Temperatur-Screening

Nach der Verbindung mit bestimmten Thermalkameras kann das Gerät die Ergebnisse der Temperaturmessung anzeigen und Sie mit einem akustischen Signal benachrichtigen, wenn eine normale oder abnormale Temperatur festgestellt wird.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihre Thermalkameras diese Funktion unterstützt und richtig konfiguriert ist.

Schritte

1. Gehen Sie zu **System** → **Ereignis** → **Intelligentes Ereignis**.
2. Wählen Sie den optischen Kanal der Thermalkameras.
3. Klicken Sie auf **Gesichtserfassung**.
4. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen Bilder der Gesichtserkennung zu speichern.
5. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
6. Legen Sie Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**. Wenn Sie nur Verknüpfungsaktionen durchführen möchten, wenn die Thermalkameras eine abnormale Temperatur feststellt, gehen Sie zu **Mehr** und aktivieren Sie **Abnormale Körpertemperatur**.

Hinwe

Die abnormale Temperatur wird von der Thermalkameras erkannt und definiert.

7. Gehen Sie zu **Audiowarnung** und wählen Sie je nach Wunsch **Normale Temperatur** oder **Abnormale Temperatur**. Sie werden mit einem akustischen Signal benachrichtigt, wenn die Kamera eine normale oder abnormale Temperatur erkennt.

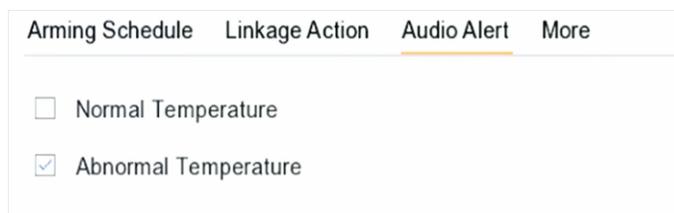


Abbildung 7-5 Audiowarnung

8. Klicken Sie auf **Anwenden**.

Was ist als nächstes zu tun?

- Sie können  der **Zielerfassung** in der Live-Ansicht aufrufen, um die Erfassungsergebnisse zu sehen.

-
- Sie können zu **Dateiverwaltung** → **Intelligente Suche** → **Suche nach Erscheinungsbild** gehen, um nach Erkennungsergebnissen zu suchen.

7.2.3 Fahrzeug-Erkennung konfigurieren

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

Schritte

1. Gehen Sie zu **System** → **Ereignis** → **Intelligentes Ereignis**.
2. Wählen Sie eine zu konfigurierende Kamera aus.
3. Klicken Sie auf **Fahrzeug**.

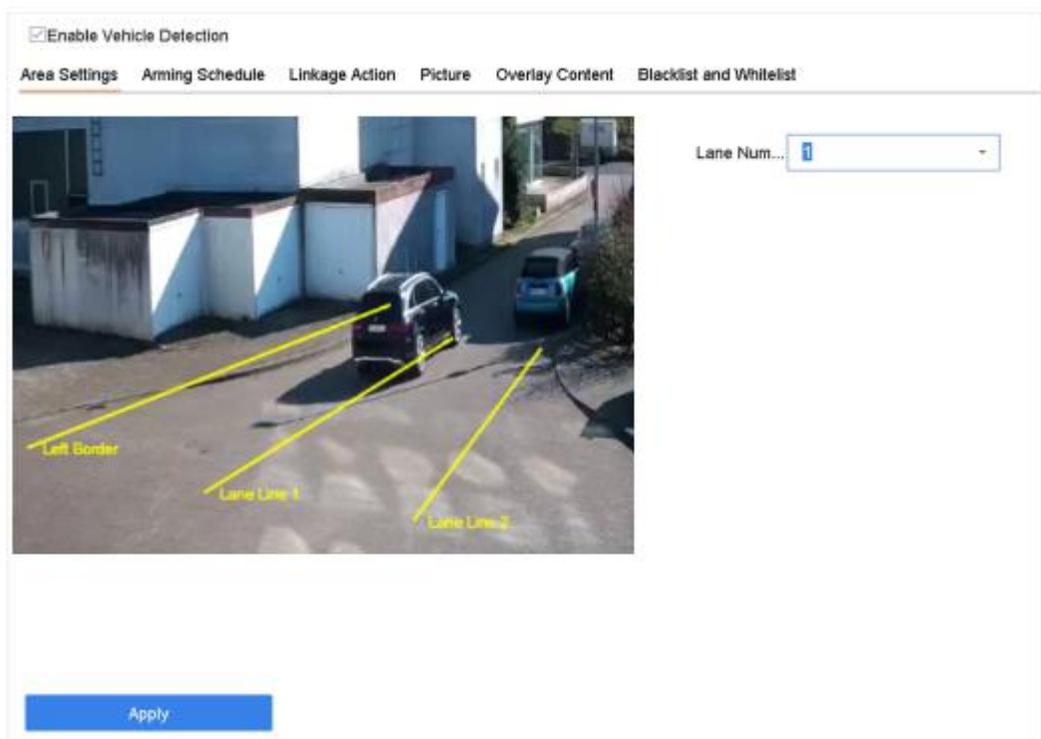


Abbildung 7-6 Fahrzeugdetektion

4. Aktivieren Sie die Option **Fahrzeugerkennung aktivieren**.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die erfassten Fahrzeugerkennungsbilder zu speichern.
6. Legen Sie den Scharfschaltplan fest. Siehe **Scharfschaltungszeitplan konfigurieren**
7. Legen Sie die Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**

8. Konfigurieren Sie Regeln, einschließlich **Bereichseinstellungen, Bild, Overlay-Inhalt** sowie **Blacklist und Whitelist**.

Bereich Einstellungen

Bis zu 4 Fahrspuren sind wählbar.

Schwarze Liste und Whitelist

Sie können die Datei zunächst exportieren, um ihr Format zu sehen, und sie dann bearbeiten und in das Gerät importieren.

9. Klicken Sie auf **Anwenden**.

Hinweis

Detaillierte Anweisungen zur Fahrzeugerkennung finden Sie im Benutzerhandbuch der Netzwerkkamera.

7.2.4 Erkennung von Linienkreuzungen

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.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Klicken Sie auf **Line Crossing**.

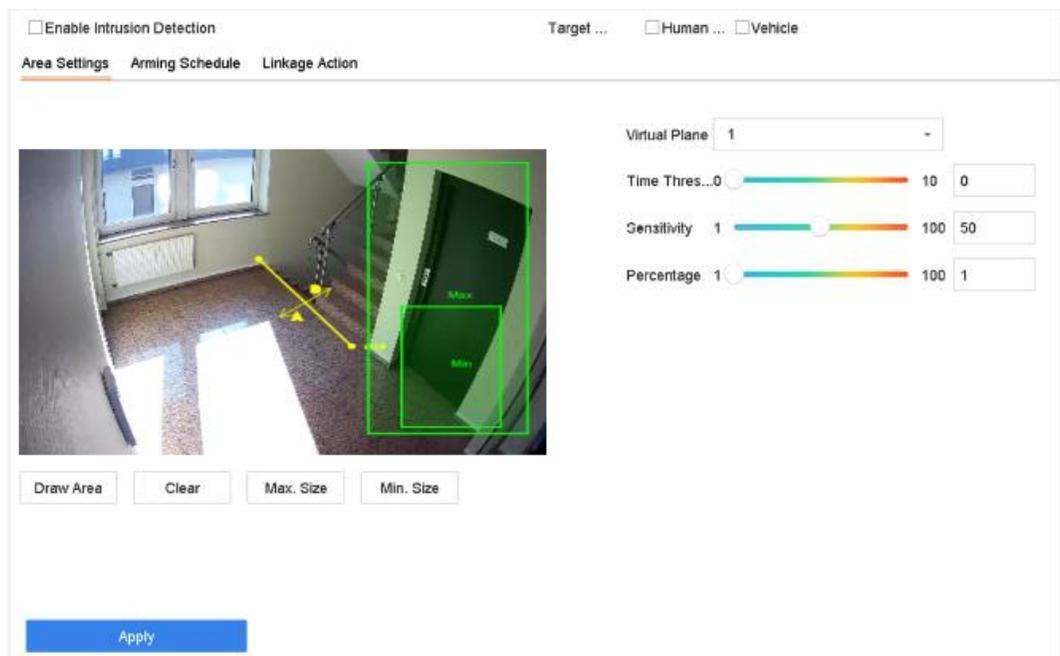


Abbildung 7-7 Erkennung von Linienkreuzungen

3. Wählen Sie eine Kamera aus.
4. Aktivieren Sie die Option **Erkennung von Linienkreuzungen aktivieren**.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen Bilder der Linienkreuzungserkennung zu speichern.
6. Legen Sie die Regeln für die Erkennung von Linienkreuzungen und die Erkennungsbereiche fest. 1) Wählen Sie einen Scharfschaltbereich.

2) Wählen Sie **Richtung** als **A<->B**, **A->B** oder **A<-B**.

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- zur B-Seite kreuzt, kann erkannt werden.

B->A

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

- 3) Stellen Sie die Erkennungsempfindlichkeit ein. Je höher der Wert ist, desto leichter kann der Erkennungsalarm ausgelöst werden.
- 4) Klicken Sie auf **Region zeichnen**.
- 5) Zeichnen Sie eine virtuelle Linie im Vorschaufenster.

-
7. **Optional:** Zeichnen Sie die Maximal-/Minimalgröße für Ziele. Nur die Ziele im Größenbereich zwischen Maximalgröße und Minimalgröße lösen die Erkennung von Linienkreuzungen aus.
 - 1) Klicken Sie auf **Max. Größe/Min. Größe**.
 - 2) Zeichnen Sie einen Bereich im Vorschaufenster.
 - 3) Klicken Sie auf **Zeichnung stoppen**.
 8. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
 9. Legen Sie Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.
 10. Klicken Sie auf **Anwenden**.

7.2.5 Einbrucherkennung

Die Funktion "Einbrucherkennung" 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.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Klicken Sie auf **Eindringen**.

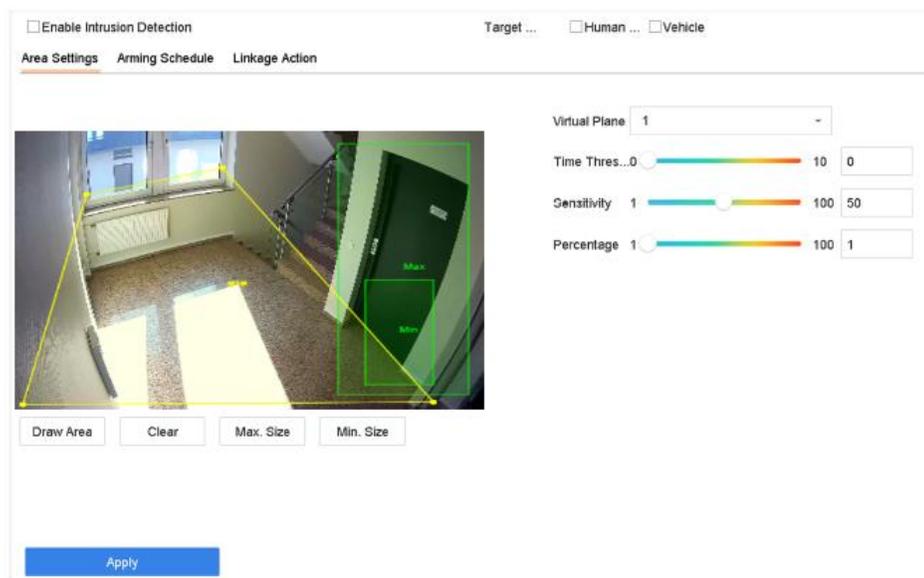


Abbildung 7-8 Einbrucherkennung

3. Aktivieren Sie die Option **Einbrucherkennung aktivieren**.
4. **Optional:** Markieren Sie **VCA-Bild speichern**, um die erfassten Bilder der Einbruchmeldung zu speichern.
5. Legen Sie die Erkennungsregeln und Erkennungsbereiche fest.

1) Wählen Sie ein virtuelles Bedienfeld. Es können bis zu 4 virtuelle Bedienfelder ausgewählt werden.

2) Stellen Sie den **Zeitschwellenwert** und die **Empfindlichkeit** 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

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

3) Klicken Sie auf **Bereich zeichnen**.

4) Zeichnen Sie ein Viereck im Vorschaufenster.

6. Optional: Zeichnen Sie die Maximal-/Minimalgröße für Ziele. Nur die Ziele im Größenbereich zwischen Maximalgröße und Minimalgröße lösen die Erkennung von Linienkreuzungen aus.

1) Klicken Sie auf **Max. Größe/Min. Größe**.

2) Zeichnen Sie einen Bereich im Vorschaufenster.

3) Klicken Sie auf **Zeichnung stoppen**.

7. Stellen Sie den Scharfschaltplan ein. Siehe ***Scharfschaltungszeitplan konfigurieren***.

8. Legen Sie Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.

9. Klicken Sie auf **Anwenden**.

7.2.6 Erkennung von Regionseintritten

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

Schritte

1. Gehen Sie zu **Systemverwaltung** → **Ereigniseinstellungen** → **Intelligentes Ereignis**.

2. Klicken Sie auf **Regionale Eingangsdetektion**.

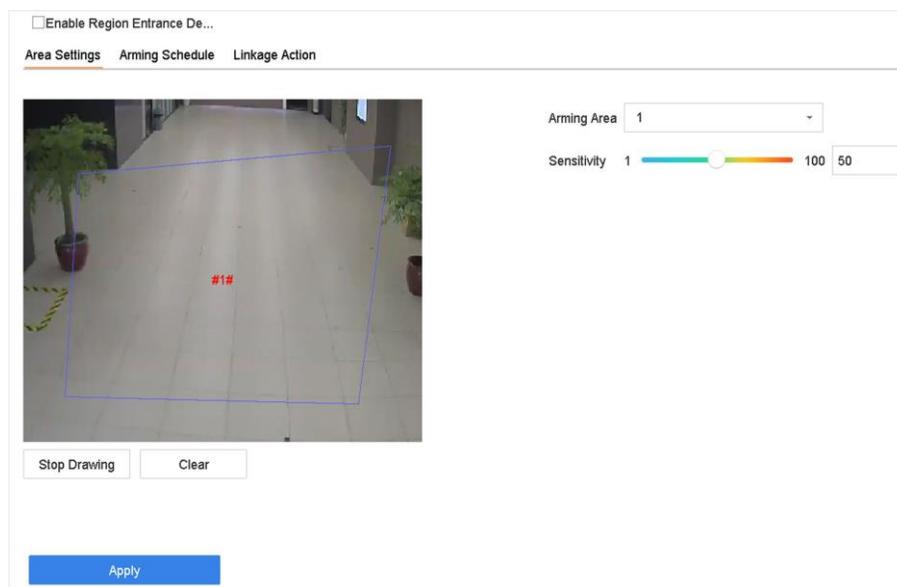


Abbildung 7-9 Erkennung von Regionseintritten

3. Wählen Sie eine Kamera aus.
4. Aktivieren Sie die Option **Erkennung von Regionseintritten aktivieren**.
5. **Optional:** Aktivieren Sie die Option **VCA-Bild speichern**, um die aufgenommenen Bilder der Erkennung des Eingangsbereichs zu speichern.
6. Legen Sie Erkennungsregeln und Erkennungsbereiche fest.
 - 1) Wählen Sie die **Aktivierungsregion**. Es können bis zu 4 Regionen ausgewählt werden.
 - 2) **Empfindlichkeit** einstellen. Je höher der Wert ist, desto leichter wird der Erkennungsalarm ausgelöst. Der Bereich ist [0-100].
 - 3) Klicken Sie auf **Bereich zeichnen** und zeichnen Sie ein Viereck im Vorschaufenster.
7. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
8. Legen Sie Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.
9. Klicken Sie auf **Anwenden**.

7.2.7 Erkennung des Verlassens einer Region

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

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Klicken Sie auf **Region Verlassen**.

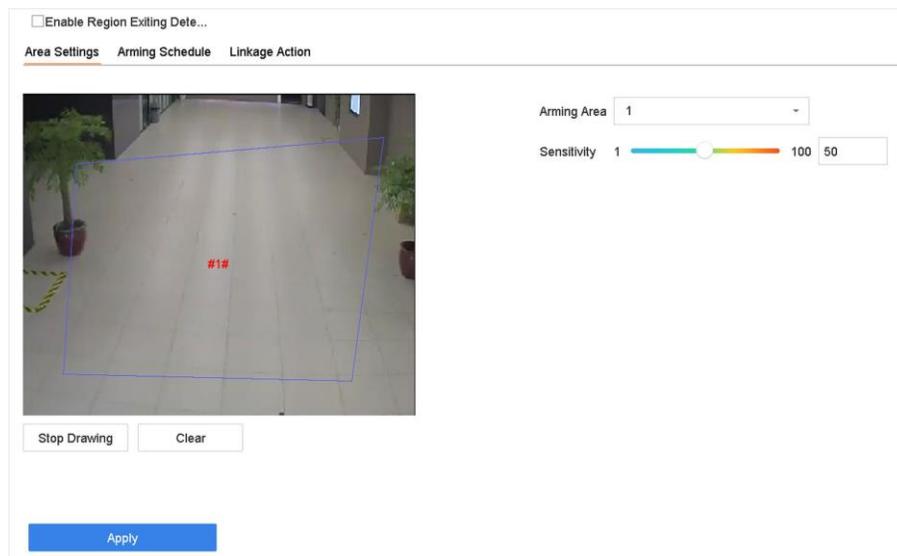


Abbildung 7-10 Erkennung des Verlassens einer Region

3. Wählen Sie eine Kamera aus.
4. Aktivieren Sie die Option **Erkennung des Verlassens einer Region aktivieren**.
5. **Optional:** Aktivieren Sie das Kontrollkästchen **VCA-Bild speichern**, um die Bilder von der Erkennung der erfassten Region zu speichern.
6. Gehen Sie wie folgt vor, um die Erkennungsregeln und Erkennungsbereiche festzulegen.
 - 1) Wählen Sie die **Aktivierungsregion**. Es können bis zu 4 Regionen ausgewählt werden.
 - 2) **Empfindlichkeit** einstellen. Je höher der Wert ist, desto leichter wird der Erkennungsalarm ausgelöst. Der Bereich ist [0-100].
 - 3) Klicken Sie auf **Bereich zeichnen** und zeichnen Sie ein Viereck im Vorschaufenster.
7. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
8. Legen Sie Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.
9. Klicken Sie auf **Anwenden**.

7.2.8 Erkennung von Herumlungern

Die Herumlunger-Erkennung wird 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.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Wählen Sie eine zu konfigurierende Kamera aus.
3. Klicken Sie auf **Erkennung Herumlungern**.

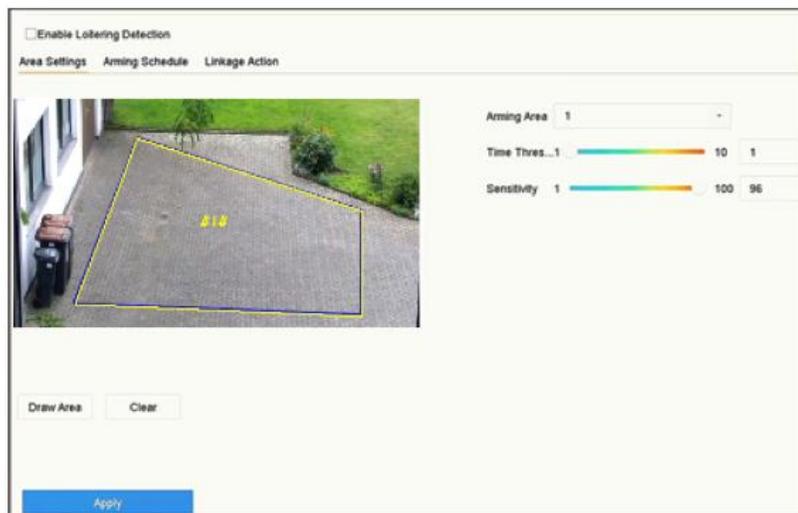


Abbildung 7-11 Erkennung von Herumlungern

4. Aktivieren Sie die Option **Herumlungern-Erkennung aktivieren**.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen Bilder der Herumlungererkennung zu speichern.
6. Parameter für die Erkennung von Herumlungern einstellen.
 - 1) Wählen Sie die **Aktivierungsregion**. Es können bis zu 4 Regionen ausgewählt werden.
 - 2) Stellen Sie den **Zeitschwellenwert ein**.

Zeitschwelle

Die Zeit, die das Fahrzeug in der Region verweilt. Bei einem Wert von 10 wird ein Alarm ausgelöst, wenn sich der Fahrkorb 10s lang in der Region aufgehalten hat. Der Bereich ist [1s-10s].

- 3) **Empfindlichkeit** einstellen.

Empfindlichkeit

Ähnlichkeit des Hintergrundbildes mit dem Objekt. Je höher der Wert, desto eher wird ein Erkennungsalarm ausgelöst.

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

7.2.9 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.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Wählen Sie eine zu konfigurierende Kamera aus.
3. Klicken Sie auf **Menschen versammeln**.

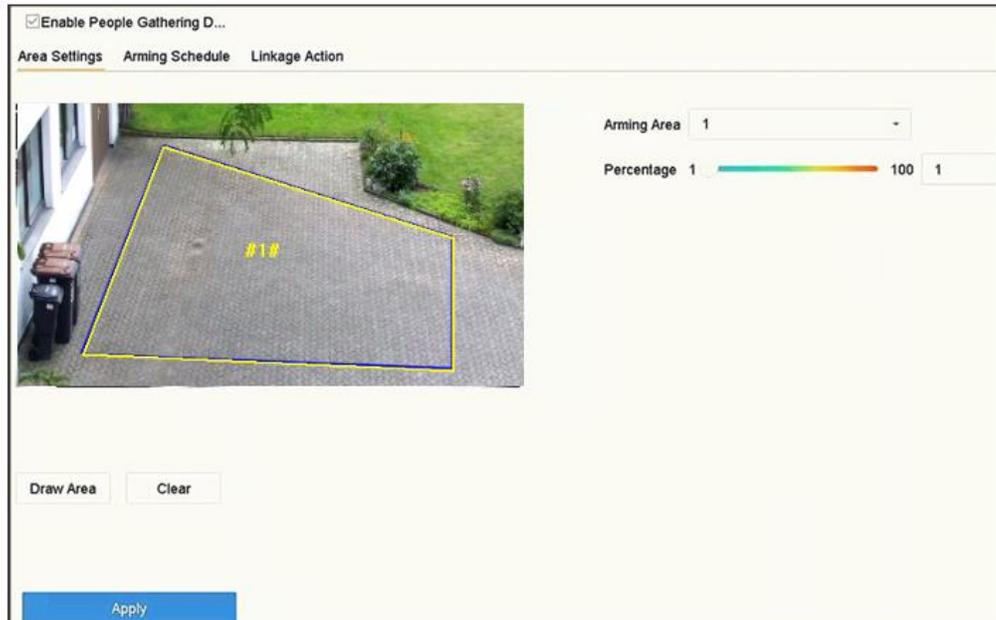


Abbildung 7-12 Erkennung von Personenansammlungen

4. Aktivieren Sie die Option **Erkennung von Personenansammlungen aktivieren**.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die erfassten Bilder der Personensammlungserkennung zu speichern.
6. Legen Sie die Parameter für die Personensammlungserkennung fest.
 - 1) Wählen Sie die **Aktivierungsregion**. Es können bis zu 4 Regionen ausgewählt werden.
 - 2) Klicken Sie auf **Fläche zeichnen**, um ein Viereck im Vorschaufenster zu zeichnen, indem Sie vier Eckpunkte der Fläche angeben.
 - 3) **Prozentsatz** einstellen.

Prozentsatz

Der Prozentsatz bezieht sich auf die Dichte der menschlichen Körper in dem Gebiet. Wenn sie den Schwellenwert überschreitet, löst das Gerät Alarm aus.

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

7.2.10 Erkennung von schnellen Bewegungen

Diese Funktion dient zur Erkennung von verdächtigem Laufen und Rennen, überhöhter Geschwindigkeit und schneller Bewegung. Sie löst einen Alarm aus, wenn sich ein Objekt schnell bewegt, und sendet eine Benachrichtigung an die Alarmzentrale, damit die erforderlichen Maßnahmen im Voraus ergriffen werden können.

Schritte

1. Gehen Sie zu **System** → **Ereignis** → **Intelligentes Ereignis**.
2. Wählen Sie eine zu konfigurierende Kamera aus.
3. Klicken Sie auf **Schnelle Bewegung**.

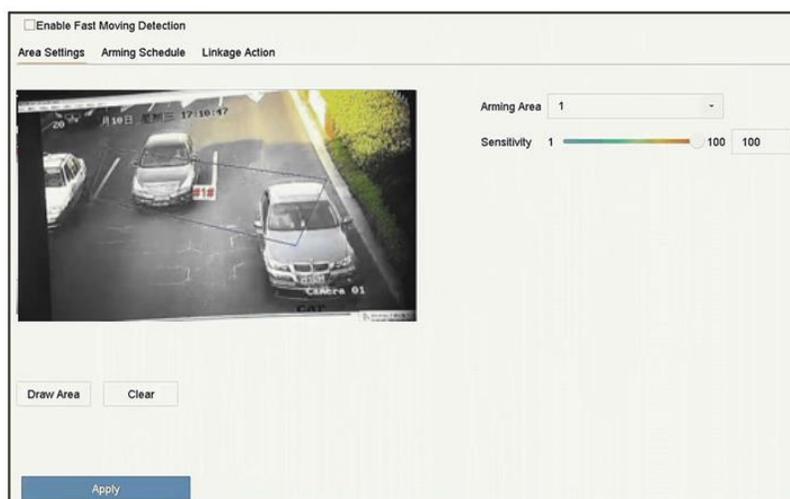


Abbildung 7-13 Erkennung schneller Bewegungen

4. Aktivieren Sie **Schnelle Bewegung**.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen Bilder der Schnellbewegungserkennung zu speichern.
6. Stellen Sie die Parameter für die Erkennung schneller Bewegungen ein.
 - 1) Wählen Sie die **Aktivierungsregion**. Es können bis zu 4 Regionen ausgewählt werden.
 - 2) Klicken Sie auf **Fläche zeichnen**, um ein Viereck im Vorschaufenster zu zeichnen, indem Sie vier Eckpunkte der Fläche angeben.
 - 3) **Empfindlichkeit** einstellen.

Hinweis

Empfindlichkeit: Ähnlichkeit des Hintergrundbildes mit dem Objekt. Je höher der Wert, desto eher wird ein Erkennungsalarm ausgelöst.

-
7. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltplan konfigurieren**
 8. Legen Sie die Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**
 9. Klicken Sie auf **Anwenden**.

7.2.11 Parkdetektion

Die Parkerkennung dient zur Erkennung von Parkverstößen in einem bestimmten Bereich und wird auf Schnellstraßen und Einbahnstraßen eingesetzt.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Wählen Sie eine zu konfigurierende Kamera aus.
3. Klicken Sie auf **Parken**.



Abbildung 7-14 Parkdetektion

4. Aktivieren Sie **Einparkhilfe aktivieren**.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen Bilder der Parkerkennung zu speichern.
6. Stellen Sie die Parameter für die Parkerkennung ein.
 - 1) Wählen Sie die **Aktivierungsregion**. Es können bis zu 4 Regionen ausgewählt werden.
 - 2) Stellen Sie den **Zeitschwellenwert** ein.

Zeitschwelle

Die Zeit, die das Fahrzeug in der Region verweilt. Bei einem Wert von 10 wird ein Alarm ausgelöst, wenn sich das Fahrzeug 10s lang in der Region aufgehalten hat. Der Bereich ist [5s-20s].

3) **Empfindlichkeit** einstellen.

Empfindlichkeit

Ähnlichkeit des Hintergrundbildes mit dem Objekt. Je höher der Wert, desto eher wird ein Erkennungsalarm ausgelöst.

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

7.2.12 Erkennung unbeaufsichtigtes Gepäck

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.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Klicken Sie auf **Unbeaufsichtigtes Gepäck**.

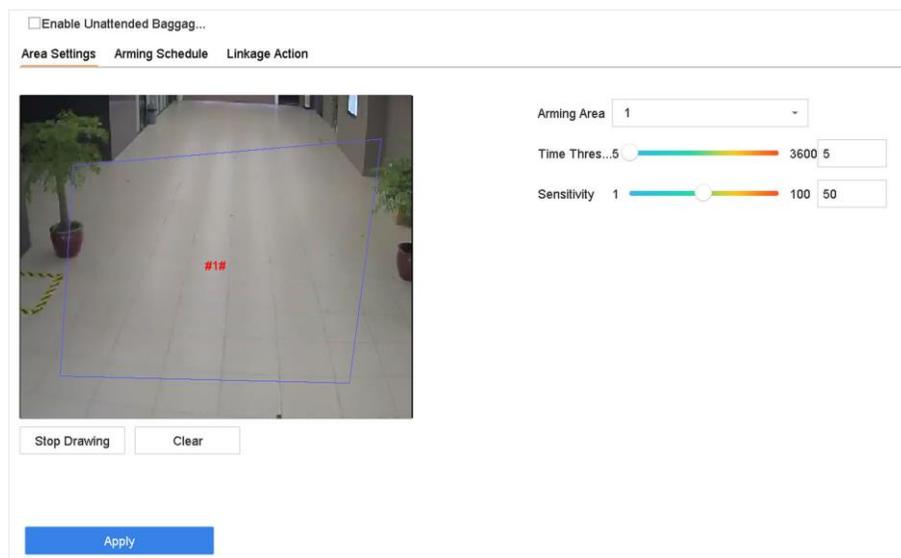


Abbildung 7-15 Erkennung unbeaufsichtigtes Gepäck

3. Wählen Sie eine Kamera aus.
4. Aktivieren Sie die Option **Erkennung von unbeaufsichtigtem Gepäck**.

-
- 5. Optional:** Aktivieren Sie das Kontrollkästchen **VCA-Bild speichern**, um die erfassten Bilder der Erkennung unbeaufsichtigter Gepäckstücke zu speichern.
- 6.** Legen Sie die Erkennungsregeln und Erkennungsbereiche fest.
- 1) Wählen Sie die **Aktivierungsregion**. Es können bis zu 4 Regionen ausgewählt werden.
 - 2) Ziehen Sie die Schieberegler, um den **Zeitschwellenwert** und die **Empfindlichkeit** einzustellen.
- Zeitschwelle**
- Die Zeit, die die Objekte in der Region verbleiben. Wenn der Wert 10 ist, wird ein Alarm ausgelöst, nachdem das Objekt verlassen wurde und 10s lang in der Region geblieben ist. Der Bereich ist [5s-20s].
- Empfindlichkeit**
- Ähnlichkeit des Hintergrundbildes mit dem Objekt. Je höher der Wert, desto eher wird ein Erkennungsalarm ausgelöst.
- 3) Klicken Sie auf **Bereich zeichnen** und zeichnen Sie ein Viereck im Vorschaufenster.
- 7.** Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
- 8.** Legen Sie Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.
- 9.** Klicken Sie auf **Anwenden**.

7.2.13 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.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Klicken Sie auf **Objekt entfernt**.

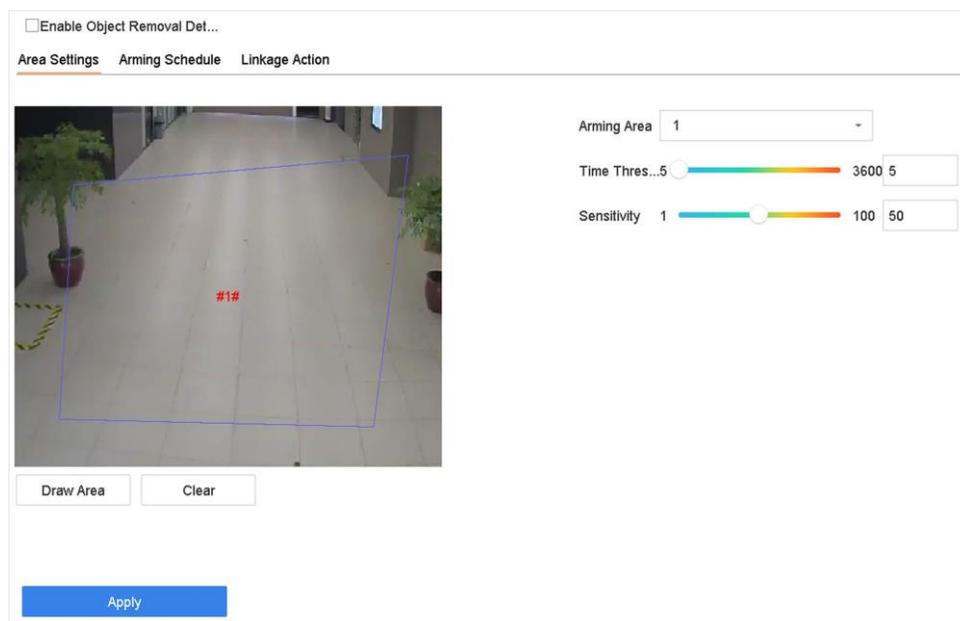


Abbildung 7-16 Erkennung der Objektentfernung

3. Wählen Sie eine zu konfigurierende Kamera aus.
4. Aktivieren Sie die Option **Erkennung von entfernbaren Objekten aktivieren**.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die erfassten Bilder der abnehmbaren Objekte zu speichern.
6. Gehen Sie wie folgt vor, um die Erkennungsregeln und Erkennungsbereiche festzulegen.
 - 1) Wählen Sie die Aktivierungsregion. Es können bis zu 4 Regionen ausgewählt werden.
 - 2) Ziehen Sie die Schieberegler, um den **Zeitschwellenwert** und die **Empfindlichkeit** einzustellen.

Zeitschwelle

Die Zeit, in der die Objekte aus dem Bereich entfernt werden. Bei einem Wert von 10 wird der Alarm ausgelöst, nachdem das Objekt 10s lang aus dem Bereich verschwunden ist. Der Bereich ist [5s-20s].

Empfindlichkeit

Der Ähnlichkeitsgrad des Hintergrundbildes. Wenn die Empfindlichkeit hoch ist, wird ein sehr kleines Objekt aus der Region den Alarm auslösen.

- 3) Klicken Sie auf **Bereich zeichnen** und zeichnen Sie im Vorschaufenster ein Viereck, indem Sie vier Eckpunkte des Erkennungsbereichs angeben.
7. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
8. Legen Sie die Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.
9. Klicken Sie auf **Anwenden**.

7.2.14 Erkennung von Audioereignissen

Die Audio-Ereigniserkennung erkennt abnormale Geräusche in der Überwachungsszene, wie z. B. eine plötzliche Zunahme/Abnahme der Geräuschintensität.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Klicken Sie auf **Audio-Ereignis**.

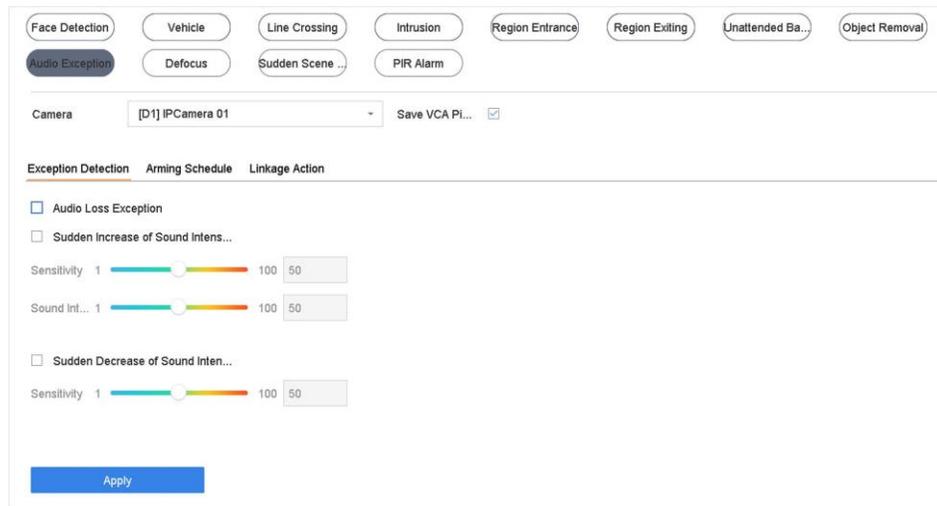


Abbildung 7-17 Erkennung von Audioereignissen

3. Wählen Sie eine zu konfigurierende Kamera aus.
4. **Optional:** Markieren Sie **VCA-Bild speichern**, um die erfassten Bilder der Audioereigniserkennung zu speichern.
5. Legen Sie die Erkennungsregeln fest:
 - 1) Wählen Sie **Ereigniserfassung**.
 - 2) Prüfen Sie die **Ereignisse Audioverlust, plötzliche Erhöhung der Schallintensität und/oder plötzliche Verringerung der Schallintensität**.

Audioverlust-Ereignis

Erkennt einen steilen Tonanstieg in der Überwachungsszene. Sie können die Erkennungsempfindlichkeit und den Schwellenwert für einen steilen Schallanstieg einstellen, indem Sie die **Empfindlichkeit** und den **Schwellenwert für die Schallintensität** konfigurieren **Empfindlichkeit**

Je kleiner der Wert, desto gravierender muss die Änderung sein, damit die Erkennung ausgelöst wird. Bereich [1-100].

Schwellenwert für die Schallintensität

Er 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. Bereich [1-100].

Erkennung einer plötzlichen Verringerung der Schallintensität

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

6. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
7. Legen Sie die Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.
8. Klicken Sie auf **Anwenden**.

7.2.15 Defokus-Erkennung

Durch Objektivdefokussierung verursachte Bildunschärfe kann erkannt werden.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Klicken Sie auf **Defokussieren**.

The screenshot shows a configuration window for 'Defocus Detection'. At the top, there is an 'Enable' checkbox and a 'Sensitivity 1' slider set to 100. Below this, there are two tabs: 'Arming Schedule' (selected) and 'Linkage Action'. Under 'Arming Schedule', there are radio buttons for 'Continuous' (selected) and 'None', and an 'Edit' button. The main area is a grid with columns for hours (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24) and rows for days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun). Each cell in the grid contains a blue bar, indicating that the event is armed continuously for all days. At the bottom, there is an 'Apply' button.

Abbildung 7-18 Defokus-Erkennung

3. Wählen Sie eine zu konfigurierende Kamera aus.
4. **Aktivieren** Sie.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen Bilder der Defokussierung zu speichern.
6. Ziehen Sie den Schieberegler **Empfindlichkeit**, um die Erkennungsempfindlichkeit einzustellen.

Hinweis

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

7. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
8. Legen Sie die Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.
9. Klicken Sie auf **Anwenden**.

7.2.16 Erkennung plötzlicher Szenenwechsel

Die Erkennung von Szenenveränderungen erkennt die Veränderung der Überwachungsumgebung durch externe Faktoren, wie z. B. die absichtliche Drehung der Kamera.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Klicken Sie auf **Plötzlicher Szenenwechsel**.

Enable Sensitivity 1 100 50

Arming Schedule Linkage Action

Continuous None Edit

	0	2	4	6	8	10	12	14	16	18	20	22	24	
Mon	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Tue	2	2	2	2	2	2	2	2	2	2	2	2	2	2
Wed	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Thu	4	4	4	4	4	4	4	4	4	4	4	4	4	4
Fri	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Sat	6	6	6	6	6	6	6	6	6	6	6	6	6	6
Sun	7	7	7	7	7	7	7	7	7	7	7	7	7	7

Apply

Abbildung 7-19 Plötzlicher Szenenwechsel

3. Wählen Sie eine zu konfigurierende Kamera aus.
4. **Aktivieren** Sie.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen Bilder der plötzlichen Szenenwechselerkennung zu speichern.
6. Ziehen Sie den Schieberegler **Empfindlichkeit**, um die Erkennungsempfindlichkeit einzustellen.

Hinweis

Empfindlichkeitsbereich: [1-100]. Je höher der Wert, desto eher kann die Änderung der Szene den Alarm auslösen.

7. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.
8. Legen Sie die Verknüpfungsaktionen fest. Siehe **Verknüpfungsaktionen konfigurieren**.
9. Klicken Sie auf **Anwenden**.

7.2.17 PIR-Alarm

Ein PIR-Alarm (Passiv-Infrarot) wird ausgelöst, wenn sich ein Eindringling im Sichtfeld des Melders bewegt. Die von einer Person oder einem anderen warmblütigen Lebewesen wie Hunden, Katzen usw. abgegebene Wärmeenergie kann erkannt werden.

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Klicken Sie auf **PIR-Alarm**.

Enable PIR Alarm

Arming Schedule Linkage Action

Continuous None Edit

	0	2	4	6	8	10	12	14	16	18	20	22	24	
Mon														1
Tue														2
Wed														3
Thu														4
Fri														5
Sat														6
Sun														7

Apply

Abbildung 7-20 PIR-Alarm

3. Wählen Sie eine zu konfigurierende Kamera aus.
4. **PIR-Alarm** prüfen.
5. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen PIR-Alarmbilder zu speichern.
6. Stellen Sie den Scharfschaltplan ein. Siehe **Scharfschaltungszeitplan konfigurieren**.

-
7. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
 8. Klicken Sie auf **Anwenden**.

7.2.18 Wärmebildkamera-Erkennung

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

Bevor Sie beginnen

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

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Wählen Sie eine Wärmebildkamera aus der Kameraliste aus.
3. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen Bilder der Erkennung zu speichern.
4. Wählen Sie eine Ereigniserkennung (Temperatur usw.).
5. Stellen Sie den Scharfschaltplan ein. Siehe ***Scharfschaltungszeitplan konfigurieren***.
6. Legen Sie die Verknüpfungsaktionen fest. Siehe ***Verknüpfungsaktionen konfigurieren***.
7. Klicken Sie auf **Anwenden**.

7.2.19 Warteschlangenverwaltung konfigurieren

Nach der Verbindung mit der Kamera für die Warteschlangenverwaltung können Sie den Aktivierungszeitplan und die Verknüpfungsaktion der Warteschlangenverwaltung festlegen.

Bevor Sie beginnen

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

Schritte

1. Gehen Sie zu **System → Ereignis → Intelligentes Ereignis**.
2. Wählen Sie eine Kamera für die Warteschlangenverwaltung aus der Kameraliste aus.
3. **Optional:** Markieren Sie **VCA-Bild speichern**, um die aufgenommenen Bilder der Erkennung zu speichern.
4. Stellen Sie den Scharfschaltplan ein. Einzelheiten finden Sie im Kapitel ***Scharfschaltplan konfigurieren***.
5. Legen Sie die Verknüpfungsaktionen fest. Weitere Informationen finden Sie im Kapitel ***Verknüpfungsaktionen konfigurieren***.
6. Klicken Sie auf **Anwenden**.

6.2.20 Zielerfassung

Im Live-View-Modus kann die Zielerfassungsfunktion während der letzten 5 Sekunden und der folgenden 10 Sekunden Smart Detection, Gesichtserkennung, Fahrzeugerkennung und Erkennung menschlicher Körper erreichen.

Schritte

1. Klicken Sie im Live-View-Modus auf **Zielerfassung**, um die Zielerfassungsoberfläche aufzurufen.
2. Wählen Sie verschiedene Erkennungsarten aus: Smart Detection (), Fahrzeugerkennung (), Gesichtserkennung () und menschliche Körpererkennung ().

Hinweis

Bei Wärmekameras befindet sich das Ereignis der Temperaturmessung in der intelligenten Erkennung (), die Erfassung des Gesichts und die Messung der Gesichtstemperatur in der Gesichtserkennung ().

3. Wählen Sie die historische Analyse () oder die Echtzeitanalyse (), um die Ergebnisse zu erhalten.

Hinweis

Die Smart-Analyseergebnisse der Erkennung werden in der Liste angezeigt. Klicken Sie auf ein Ergebnis in der Liste, um das entsprechende Video abzuspielen.

4. **Optional:** Sie können Kanäle auswählen, die eine Bildaufnahme erfordern. Die nicht ausgewählten Kanäle werden nicht erfasst.
 - 1) Klicken Sie links unten in der Live-Ansicht auf  .
 - 2) Wählen Sie den/die Kanal/Kanäle, der/die markierte(n) Kanal/Kanäle wird/werden ein Bild aufnehmen. Standardmäßig sind alle Kanäle ausgewählt.
 - 3) Klicken Sie auf **Fertigstellen**.

7.3 Zeitplan für die Scharfschaltung konfigurieren

Schritte

1. Klicken Sie auf **Zeitplan für die Scharfschaltung**.
2. Klicken Sie auf **Bearbeiten**.
3. Wählen Sie einen Wochentag und legen Sie den Zeitraum fest. Pro Tag können bis zu acht Zeiträume eingestellt werden.

Hinweis

Zeiträume können sich nicht wiederholen oder überschneiden.

Edit	
Weekday	Mon
Start/End Time	00:00-24:00
Start/End Time	00:00-00:00

Copy Apply OK Cancel

Abbildung 7-21 Aktivierungszeitplan einstellen

4. Sie können auf **Kopieren** klicken, um die Einstellungen des aktuellen Scharfschaltungsplans auf andere Tage zu übertragen.
5. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

7.4 Verknüpfungsaktionen konfigurieren

Alarmverknüpfungsaktionen werden aktiviert, wenn ein Alarm oder ein Ereignis auftritt, einschließlich Ereignishinweisanzeige, Vollbildüberwachung, akustische Warnung (Summer), Benachrichtigung der Überwachungszentrale, Auslösen des Alarmausgangs und Senden einer E-Mail.

7.4.1 Konfigurieren der Auto-Switch-Vollbildüberwachung

Wenn ein Alarm ausgelöst wird, zeigt der lokale Monitor das Bild des für die Vollbildüberwachung konfigurierten Alarmkanals im Vollbild an. Wenn der Alarm gleichzeitig auf mehreren Kanälen ausgelöst wird, müssen Sie die Verweilzeit für die autom. Umschaltung konfigurieren.

Hinweis

Die autom. Umschaltung ist beendet, sobald der Alarm aufhört und die Live-Ansicht wieder angezeigt wird.

Schritte

1. Gehen Sie zu **System → Live-Ansicht → Allgemein**.
2. Stellen Sie den Ereignisausgang und die Verweilzeit ein.

Ereignis-Ausgang

Wählen Sie den Ausgang für die Anzeige des Ereignisvideos.

Vollbildüberwachung Verweilzeit

Legen Sie die Zeit in Sekunden fest, nach der der Bildschirm für das Alarmereignis angezeigt wird. Wenn Alarme in mehreren Kanälen gleichzeitig ausgelöst werden, werden ihre Vollbildbilder in einem Intervall von 10 Sekunden umgeschaltet (Standardverweilzeit).

3. Wechseln Sie zur Schnittstelle für die **Verknüpfungsaktion** der Alarmerkennung (z. B. Bewegungserkennung, Videomanipulation, Gesichtserkennung usw.).
4. Wählen Sie die Alarmverknüpfungsaktion **Vollbildüberwachung**.
5. Wählen Sie den/die Kanal/Kanäle unter **Triggerkanal** für die Vollbildüberwachung aus.

7.4.2 Audiowarnung konfigurieren

Bei der akustischen Warnung löst das System einen Signalton aus, wenn ein Alarm erkannt wird.

Schritte

1. Gehen Sie zu **System → Ansicht → Allgemein**.
2. Aktivieren Sie die Audioausgabe und stellen Sie die Lautstärke ein.
3. Wechseln Sie zur Schnittstelle für **Verknüpfungsaktionen** der Alarmerkennung (z. B. Bewegungserkennung, Videomanipulation, Gesichtserkennung usw.).
4. Wählen Sie die Alarmverknüpfungsaktion **Audiowarnung**.

7.4.3 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 installiert ist (z. B. iVMS-4200, iVMS-5200).

Schritte

1. Gehen Sie zu **System → Netzwerk → Erweitert → Weitere Einstellungen**.
2. Stellen Sie die IP-Adresse und den Port des Alarm-Hosts ein.
3. Wechseln Sie zur Schnittstelle für **Verknüpfungsaktionen** der Alarmerkennung (z. B. Bewegungserkennung, Videomanipulation, Gesichtserkennung usw.).
4. Wählen Sie **Überwachungszentrale benachrichtigen**.

7.4.4 E-Mail-Verknüpfung konfigurieren

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

Schritte

1. Gehen Sie zu **System → Netzwerk → Erweitert → E-Mail**.
2. Stellen Sie die E-Mail-Parameter ein.
3. Klicken Sie auf **Anwenden**.
4. Wechseln Sie zur Schnittstelle für die **Verknüpfungsaktion** der Alarmerkennung (z. B. Bewegungserkennung, Videomanipulation, Gesichtserkennung usw.).
5. Wählen Sie die Verknüpfungsaktion **E-Mail-Alarm senden**.

7.4.5 Ausgelöster Alarmausgang

Der Alarmausgang kann durch den Alarmeinang, die Bewegungserkennung, die Erkennung von Videomanipulationen, die Gesichtserkennung, die Erkennung von Linienüberquerungen und alle anderen Ereignisse ausgelöst werden.

Schritte

1. Wechseln Sie zur Verknüpfungsschnittstelle der Alarmerkennung (z. B. Bewegungserkennung, Gesichtserkennung, Erkennung von Linienüberquerungen, Eindringlingserkennung usw.).
2. Wählen Sie im Bereich **Alarmausgänge auslösen** den oder die Alarmausgänge aus, die ausgelöst werden sollen.
3. Gehen Sie zu **System → Ereignis → Normales Ereignis → Alarmausgang**.
4. Wählen Sie einen Alarmausgang aus der Liste aus.

Hinweis

Wenn das Gerät 8 Alarmausgänge hat, wird die Stromversorgung von Ctrl 12V durch den Alarmausgang 9 gesteuert. Schließen Sie den positiven Pol an A von Ctrl 12V und den negativen Pol an B von Ctrl 12V an. Der Strom wird eingeschaltet, wenn der Alarmausgang ausgelöst wird.

7.4.6 Audio- und Lichtalarmverknüpfung konfigurieren

Für bestimmte Netzwerk-Kameras können Sie die Alarmverknüpfung als Audio- oder Lichtalarm einstellen.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Ihre Kamera die Verknüpfung von Audio- und Lichtalarm unterstützt.
- Stellen Sie sicher, dass der Audioausgang und die Lautstärke richtig konfiguriert sind.

Schritte

1. Wechseln Sie zur Schnittstelle für die Verknüpfungsaktion der Alarmerkennung (z. B. Bewegungserkennung).
2. Stellen Sie die **Audio- und Lichtalarmverknüpfung** nach Ihren Wünschen ein.
3. Klicken Sie auf **Anwenden**.

7.4.7 Konfigurieren der PTZ-Verknüpfung

Das System kann die PTZ-Aktionen (z. B. Voreinstellung/Patrouille/Pattern) auslösen, wenn ein Alarmereignis oder ein VCA-Erkennungsereignis eintritt.

Bevor Sie beginnen

Vergewissern Sie sich, dass die angeschlossene PTZ- oder Speed Dome-Kamera die PTZ-Kopplung unterstützt.

Schritte

1. Wechseln Sie zur Verknüpfungsschnittstelle des Alarmeingangs oder der VCA-Erkennung (z. B. Gesichtserkennung, Linienüberquerungserkennung, Eindringlingserkennung usw.).
2. Wählen Sie die **PTZ-Kopplung** aus.
3. Wählen Sie die Kamera aus, die die PTZ-Aktionen ausführen soll.
4. Wählen Sie die voreingestellte/patrouillierte/patternierte Nr., die bei Alarmereignissen angerufen werden soll.

Hinweis

Sie können für jede Zeit nur einen PTZ-Typ für die Verknüpfung einstellen.

8 Intelligente Analyse

8.1 Personenzählung

Die Zählung berechnet die Anzahl der Personen, die einen bestimmten konfigurierten Bereich betreten oder verlassen, und erstellt tägliche/wöchentliche/monatliche/jährliche Berichte zur Analyse.

Schritte

1. Gehen Sie zu **Intelligente Analyse** → **Zählen**.
2. Wählen Sie die Kamera(s) aus.
3. Wählen Sie den Berichtstyp aus.
4. Legen Sie das **Datum** für die Analyse fest. Die Grafik zur Personenzählung wird angezeigt.



Abbildung 8-1 Schnittstelle zur Personenzählung

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

8.2 Wärmebildkarte

Die Wärmebildkarte ist eine grafische Darstellung von Daten. Die Funktion wird verwendet, um zu analysieren, wie viele Personen ein bestimmtes Gebiet besucht und sich dort aufgehalten haben.

Bevor Sie beginnen

Die Funktion muss von der angeschlossenen IP-Kamera unterstützt werden und die entsprechende Konfiguration muss eingestellt sein.

Schritte

1. Gehen Sie zu **Intelligente Analyse** → **Wärmebildkarte**.
2. Wählen Sie eine Kamera aus.

-
3. Wählen Sie den Berichtstyp aus.
 4. **Datum** für die Analyse festlegen.

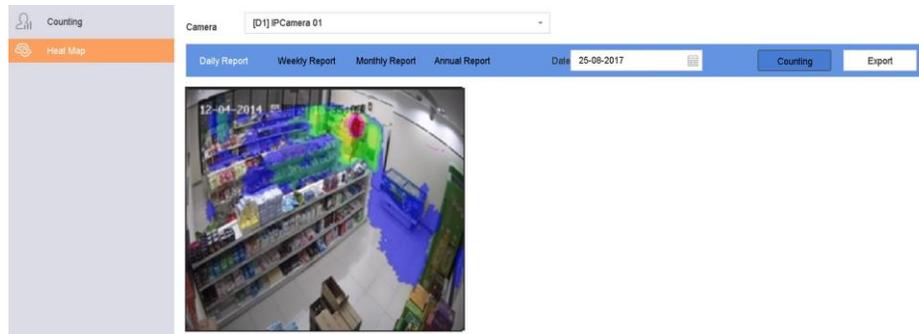


Abbildung 8-2 Heatmap-Schnittstelle

5. Klicken Sie auf **Zählen**. Die Ergebnisse werden in Grafiken angezeigt, die in verschiedenen Farben markiert sind.

Hinwe

Wie in der obigen Abbildung zu sehen ist, kennzeichnet der rote Farblock (255, 0, 0) den am stärksten frequentierten Bereich und der blaue Farblock (0, 0, 255) den weniger stark frequentierten Bereich.

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

9 POS-Konfiguration

Das Gerät kann mit einer POS-Maschine/einem POS-Server verbunden werden und eine Transaktionsnachricht empfangen, die während der Live-Ansicht oder der Wiedergabe in das Bild eingeblendet wird, sowie einen POS-Alarm auslösen.

9.1 POS-Verbindung konfigurieren

Schritte

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



The screenshot shows a web interface for adding a POS device. It features the following elements:

- Add POS** (Section Header)
- Enable** checkbox (unchecked)
- POS Name** dropdown menu (selected: POS 3)
- POS Protocol** dropdown menu (selected: AVE) and a **Custom** button
- Connection Mode** dropdown menu (selected: Sniff)
- Parameters** button

Abbildung 9-1 POS-Einstellungen

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

Hinwe

Die Anzahl der von jedem Gerät unterstützten POS-Geräte entspricht der Hälfte der Kanalanzahl, z. B. werden 8 POS-Geräte für das Modell GD-RN-CT8832N unterstützt.

5. Wähle **POS-Protokoll**

Hinwe

Wenn ein neues Protokoll ausgewählt wurde, starten Sie das Gerät neu.

Universelles Protokoll

Klicken Sie auf **Erweitert**, um bei der Auswahl des Universalprotokolls weitere Einstellungen vorzunehmen. Sie können die Startzeilenkennung, die Zeilenumbruchskennzeichnung und die Endzeilenkennzeichnung für die POS-Overlay-Zeichen sowie die Groß- und Kleinschreibung der Zeichen festlegen. Optional können Sie auch den Filterbezeichner und das XML-Protokoll aktivieren.

Start Line Identifier Hex

Line Break Hex

End Line Identifier Hex

Case Sensitive

Filtering Identifier

Enable XML Prot...

OK Cancel

Abbildung 9-2 Universelle Protokolleinstellungen

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.

Klicken Sie auf **Benutzerdefiniert**, um die AVE-Einstellungen zu konfigurieren. Wählen Sie **Regel** als **VSI-ADD** oder **VNET**. Legen Sie das Adressbit der zu sendenden POS-Nachricht fest. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

NUCLEUS

Klicken Sie auf die Schaltfläche **Benutzerdefiniert**, um die NUCLEUS-Einstellungen zu konfigurieren.

Geben Sie die Mitarbeiternummer, die Schichtnummer und die Terminalnummer in das Feld ein. Die vom POS-Gerät gesendete übereinstimmende Nachricht wird als gültige POS-Daten verwendet.

Hinwe

Für die Kommunikation über die RS-232-Verbindung muss das NUCLEUS-Protokoll verwendet werden.

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

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.

Legen Sie die **zulässige Remote-IP-Adresse** des Geräts fest, das die POS-Nachricht sendet.

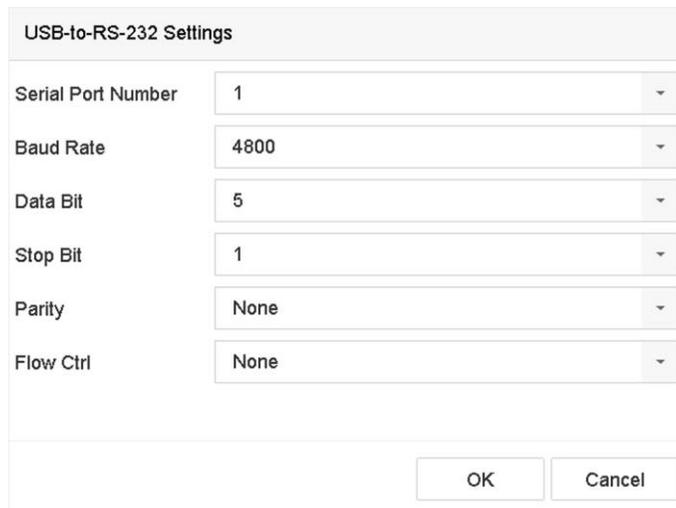
UDP-Verbindung

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

Legen Sie die **zulässige Remote-IP-Adresse** des Geräts fest, das die POS-Nachricht sendet.

USB-zu-RS-232-Verbindung

Konfigurieren Sie die Anschlussparameter des USB-zu-RS-232-Konverters, einschließlich der Seriennummer des Anschlusses, Baudrate, Datenbit, Stoppbit, Parität und Flusststeuerung.



USB-to-RS-232 Settings	
Serial Port Number	1
Baud Rate	4800
Data Bit	5
Stop Bit	1
Parity	None
Flow Ctrl	None

OK Cancel

Abbildung 9-3 USB-zu-RS-232-Einstellungen

RS-232-Anschluss

Verbinden Sie das Gerät und das Kassensystem über RS-232. Die RS-232-Einstellungen können unter **Menü → Konfiguration → RS-232** konfiguriert werden. Die Verwendung muss auf Transparenter Kanal eingestellt sein.

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.

Abbildung 9-4 Sniff-Einstellungen

9.2 POS-Text-Overlay konfigurieren

Schritte

1. Gehen Sie zu **System** → **POS**.
2. Klicken Sie auf **Kanalverknüpfung und Anzeige**.

Abbildung 9-5 Einstellungen für Überlagerungszeichen

3. Wählen Sie den **verknüpften Kanal**, um die POS-Zeichen zu überlagern.
4. Legen Sie das Zeichen-Overlay für die aktivierte Kasse fest.
 - Zeichenkodierungsformat: derzeit ist das Latin-1-Format verfügbar
 - Überlagerungsmodus der Zeichen, die beim Blättern oder im Seitenmodus angezeigt werden sollen

-
- Schriftgröße und Schriftfarbe
 - Anzeigzeit (Sek.) der Zeichen. Der Wert liegt zwischen 5 und 3600 Sekunden.
 - Zeitüberschreitung des POS-Ereignisses. Der Wert liegt zwischen 5 und 3600 Sekunden.
Wenn das Gerät die POS-Nachricht nicht innerhalb der festgelegten Zeit empfangen hat, wird die Transaktion beendet.
5. Legen Sie in den **Datenschutzeinstellungen** fest, dass die Datenschutzinformationen der Kasse nicht auf dem Bild angezeigt werden, z. B. die Kartenummer, der Benutzername usw.
Die festgelegten Datenschutzinformationen werden stattdessen mit *** auf dem Bild angezeigt.
 6. Aktivieren Sie **POS in Live-Ansicht überlagern**. Wenn diese Funktion aktiviert ist, werden die POS-Informationen auf dem Live-View-Bild eingeblendet.

Hinweis

Ziehen Sie den Rahmen, um die Größe und Position des Textfeldes auf dem Vorschaubildschirm der POS-Einstellungsschnittstelle anzupassen.

7. Klicken Sie auf **Übernehmen**, um die Einstellungen zu aktivieren.

9.3 POS-Alarm konfigurieren

Ein POS-Ereignis kann dazu führen, dass Kanäle mit der Aufzeichnung beginnen, eine Vollbildüberwachung oder eine akustische Warnung ausgelöst wird, die Überwachungszentrale benachrichtigt wird, eine E-Mail gesendet wird usw.

Schritte

1. Gehen Sie zu **Speicher → Aufzeichnungszeitplan**.
2. Legen Sie den Zeitplan für das Scharfschalten des POS-Ereignisses fest.
3. Gehen Sie zu **System → POS**.
4. Klicken Sie in der Schnittstelle zum Hinzufügen oder Bearbeiten von POS auf **Ereignisverknüpfung**.

Channel Linkage and Display **Event Linkage**

<input checked="" type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output	<input type="checkbox"/> Trigger Channel
<input checked="" type="checkbox"/> Full Screen Monitoring	<input checked="" type="checkbox"/> Local->1	<input checked="" type="checkbox"/> D1
<input checked="" type="checkbox"/> Audible Warning	<input type="checkbox"/> Local->2	<input checked="" type="checkbox"/> D2
<input checked="" type="checkbox"/> Send Email	<input checked="" type="checkbox"/> Local->3	<input type="checkbox"/> D3
	<input type="checkbox"/> Local->4	<input type="checkbox"/> D4
	<input type="checkbox"/> 10.15.2.250:8000->1	

*Notice: please confirm the event output in "Live View" settings menu is the same with the real event output.

Abbildung 9-6 Auslösekameras des POS einstellen

5. Wählen Sie die normalen Verknüpfungsaktionen aus.
6. Wählen Sie einen oder mehrere Alarmausgänge, die ausgelöst werden sollen.
7. Wählen Sie einen oder mehrere Kanäle für die Aufzeichnung oder Vollbildüberwachung aus, wenn ein POS-Alarm ausgelöst wird.
8. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

10 Kameraeinstellungen

10.1 Bildparameter konfigurieren

Sie können die Bildparameter, einschließlich Tag/Nacht-Schalter, Hintergrundbeleuchtung, Kontrast und Sättigung unter **Kamera → Display** anpassen.

Bildeinstellungen

Passen Sie die Bildparameter wie Helligkeit, Kontrast und Sättigung an.

Exposition

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

Tag/Nacht-Schalter

Stellen Sie die Kamera je nach Zeit oder Umgebungslicht auf den Tag-, Nacht- oder Automatikmodus ein. Wenn das Licht in der Nacht schwächer wird, kann die Kamera in den Nachtmodus mit qualitativ hochwertigen Schwarzweißbildern umschalten.

Hintergrundbeleuchtung

Stellen Sie den großen Dynamikbereich der Kamera ein (0 bis 100). Wenn die Umgebungsbeleuchtung und das Objekt große Helligkeitsunterschiede aufweisen, können Sie den WDR-Wert einstellen, um den Helligkeitspegel des gesamten Bildes auszugleichen.

Bildverbesserung

Für optimierte Bildkontrastverbesserung, die das Rauschen im Videostrom reduziert.

10.2 Konfigurieren der OSD-Einstellungen

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

Schritte

1. Gehen Sie zu **Kamera → Anzeige**.
2. Wählen Sie eine Kamera nach Ihren Wünschen.
3. Name in **Kameraname** bearbeiten.
4. Markieren Sie **Name anzeigen**, **Datum anzeigen** und **Woche anzeigen**, um die Informationen auf dem Bild anzuzeigen.
5. Stellen Sie das Datumsformat, das Zeitformat und den Anzeigemodus ein.

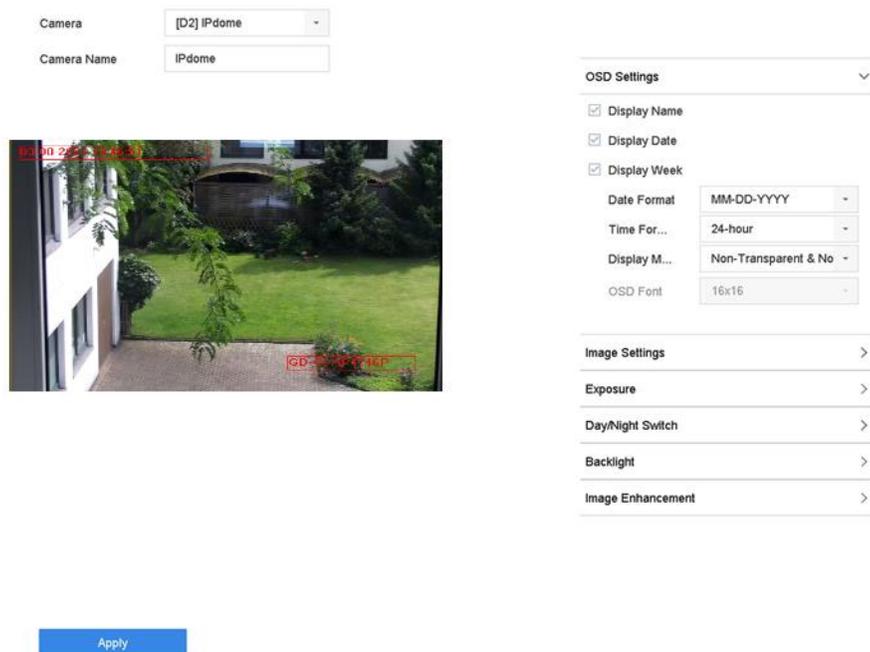


Abbildung 10-1 OSD-Konfigurationsoberfläche

6. Ziehen Sie den Textrahmen im Vorschaufenster, um die OSD-Position anzupassen.
7. Klicken Sie auf **Anwenden**.

10.3 Datenschutzmaske 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** → **Datenschutzmaske**.
2. Wählen Sie eine Kamera aus, für die Sie eine Datenschutzmaske festlegen möchten.
3. **Aktivieren** Sie.
4. Zeichnen Sie einen Bereich auf dem Fenster. Der Bereich wird durch verschiedene Rahmenfarben markiert.

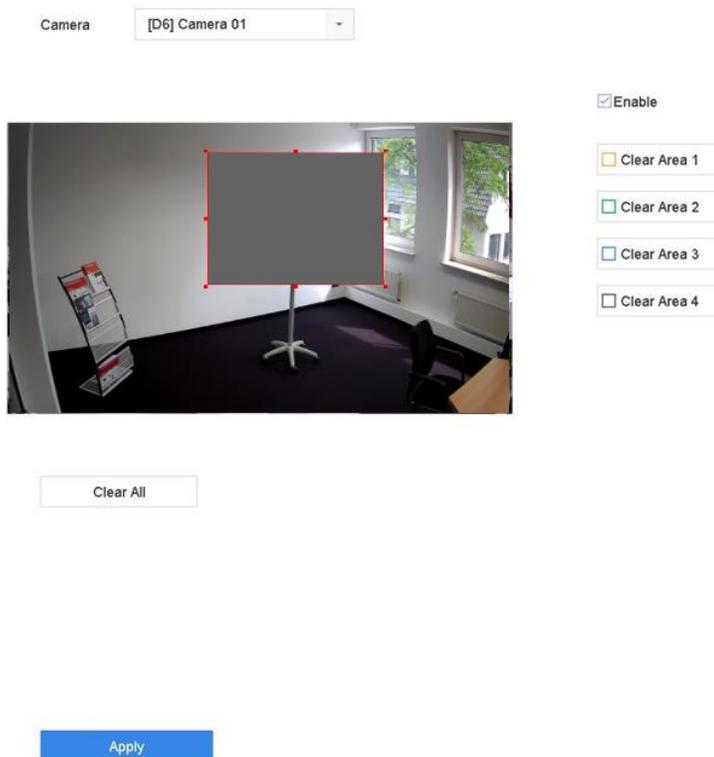


Abbildung 10-2 Schnittstelle für Datenschutzmaskeneinstellungen

Hinwe

- Es können bis zu 4 Sichtschutzzonen konfiguriert und die Größe der einzelnen Bereiche angepasst werden.
- Sie können die konfigurierten Bereiche der Datenschutzmaske im Fenster löschen, indem Sie auf die entsprechenden Symbole für die Bereiche 1 bis 4 auf der rechten Seite des Fensters klicken, oder klicken Sie auf **Alle löschen**, um alle Bereiche zu löschen.

5. Klicken Sie auf **Anwenden**.

10.4 Import/Export von IP-Kamera-Konfigurationsdateien

Die IP-Kamerainformationen, einschließlich der IP-Adresse, des Verwaltungsports, des Admin-Passworts usw., können im Microsoft Excel-Format gespeichert und auf dem lokalen Gerät gesichert werden. Die exportierte Datei kann auf einem PC bearbeitet werden, einschließlich des Hinzufügens oder Löschens von Inhalten und des Kopierens der Einstellungen auf andere Geräte, indem die Excel-Datei dorthin importiert wird.

Bevor Sie beginnen

Wenn Sie die Konfigurationsdatei importieren, schließen Sie das Speichermedium, das die Konfigurationsdatei enthält, an das Gerät an.

Schritte

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

Hinweis

Nachdem der Importvorgang abgeschlossen ist, müssen Sie das Gerät neu starten, um die Einstellungen zu aktivieren.

10.5 IP-Kameras aufrüsten

Die IP-Kamera kann aus der Ferne über das Gerät aufrüstet werden.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie das USB-Flash-Laufwerk an das Gerät angeschlossen haben und dass es die Aktualisierungsfirmware für die IP-Kamera enthält.

Schritte

1. Wählen Sie in der Kameraverwaltungsoberfläche eine Kamera aus.
2. Gehen Sie zu **Weitere Einstellungen → Upgrade**.
3. Wählen Sie die Firmware-Upgrade-Datei vom USB-Flash-Laufwerk aus.
4. Klicken Sie auf **Upgrade**.

Die IP-Kamera wird nach Abschluss der Aktualisierung automatisch neu gestartet.

11 Speicherung

11.1 Verwaltung von Speichergeräten

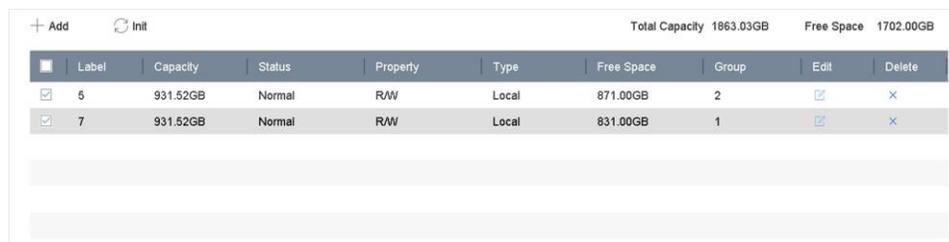
11.1.1 Lokales Festplattenlaufwerk verwalten

Festplattengruppe konfigurieren

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

Schritte

1. Gehen Sie zu **Speicher** → **Speichermodus**.
2. Wählen Sie **Modus** als **Gruppe**.
3. Klicken Sie auf **Anwenden**.
4. Gehen Sie zu **Speicher** → **Speichergerät**.
5. Wählen Sie ein HDD.



	Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
<input checked="" type="checkbox"/>	5	931.52GB	Normal	RAW	Local	871.00GB	2		
<input checked="" type="checkbox"/>	7	931.52GB	Normal	RAW	Local	831.00GB	1		

Abbildung 11-1 Speichergerät

6. Klicken Sie auf , um die Schnittstelle für die lokalen Festplatteneinstellungen zu öffnen.

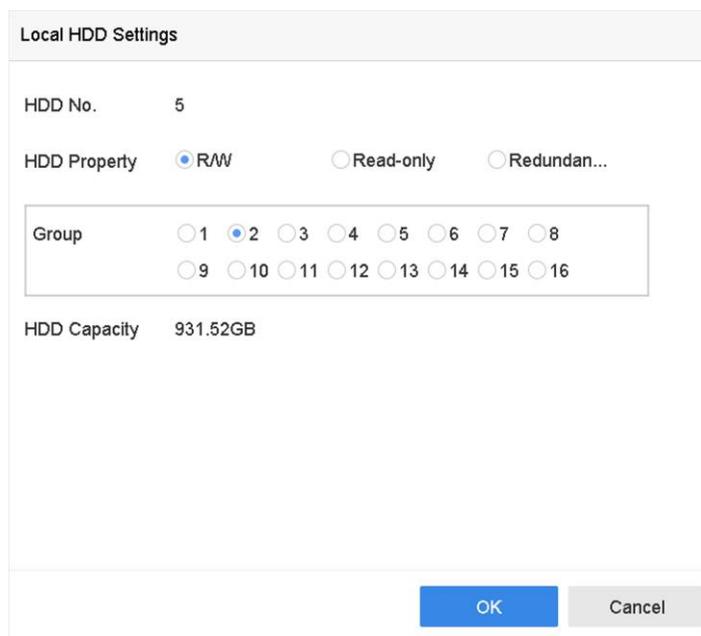


Abbildung 11-2 Lokale Festplatteneinstellungen

7. Wählen Sie eine Gruppennummer für das Festplattenlaufwerk.
8. Klicken Sie auf **OK**.

Hinwe

Gruppieren Sie die Kameras für HDD neu, wenn die HDD-Gruppennummer geändert

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

Konfigurieren Sie die HDD-Eigenschaft

Die HDD-Eigenschaft kann als R/W, schreibgeschützt oder redundant eingestellt werden.

Bevor Sie beginnen

Stellen Sie den Speichermodus auf Gruppe ein. Detaillierte Schritte finden Sie unter **Festplattengruppe konfigurieren**

Schritte

1. Gehen Sie zu **Speicher → Speichergerät**.
2. Klicken Sie auf  der gewünschten HDD.
3. Wählen Sie **HDD-Eigenschaft**.

R/W

Die Festplatte unterstützt sowohl Lese- als auch Schreibvorgänge.

Schreibgeschützt

Dateien auf schreibgeschützten Festplatten werden nicht überschrieben.

Redundant

Speichern Sie die Videos und Bilder nicht nur auf der R/W-Festplatte, sondern auch auf der redundanten Festplatte. Dadurch wird die Datensicherheit und Zuverlässigkeit effektiv erhöht. Stellen Sie sicher, dass mindestens eine weitere Festplatte mit Lese-/Schreibstatus vorhanden ist.

4. Klicken Sie auf **OK**.

Konfigurieren Sie die Festplattenkontingente

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

Schritte

1. Gehen Sie zu **Speicher → Speichermodus**.
2. Wählen Sie **Modus** als **Quote**.
3. Wählen Sie eine Kamera aus, um die Quote festzulegen.
4. Geben Sie die Speicherkapazität in die Textfelder von **Max. Aufnahmekapazität (GB)** und **Max. Bildkapazität (GB)** ein.
5. Klicken Sie auf **Kopieren**, um die Quoteneinstellungen der aktuellen Kamera auf andere Kameras zu kopieren.
6. Klicken Sie auf **Anwenden**.

Hinwe

- Wenn die Quotenkapazität auf 0 gesetzt ist, nutzen alle Kameras die gesamte Kapazität der Festplatte für Videos und Bilder.
 - Starten Sie den Videorecorder neu, um die neuen Einstellungen zu aktivieren.
-

11.1.2 Hinzufügen einer Netzwerkfestplatte

Sie können die zugewiesene NAS- oder IP SAN-Festplatte zum Gerät hinzufügen und als Netzwerkfestplatte verwenden. Es können bis zu 8 Netzwerkfestplatten hinzugefügt werden.

Schritte

1. Gehen Sie zu **Speicher → Speichergerät**.
2. Klicken Sie auf **Hinzufügen**.

Custom Add

NetHDD: NetHDD 1

Type: NAS

NetHDD IP: 120 . 36 . 2 . 39

NetHDD Directory: /nas/device1/11 | Search

OK Cancel

Abbildung 11-3 NetHDD hinzufügen

3. Wählen Sie den NetHDD-Typ.
4. Geben Sie die IP-Adresse des **NetHDD** ein und klicken Sie auf **Suchen**, um das verfügbare NetHDD zu suchen.
5. Wählen Sie das gewünschte NetHDD aus.
6. Klicken Sie auf **OK**.
7. Die hinzugefügte NetHDD wird in der Festplattenliste angezeigt. Wählen Sie die neu hinzugefügte NetHDD aus und klicken Sie auf **Einleitung**.

11.1.3 Verwalten von eSATA

Konfigurieren Sie eSATA für die Datenspeicherung

Wenn ein externes eSATA-Gerät an Ihren Videorecorder angeschlossen ist, können Sie die eSATA-Nutzung als Datenspeicher konfigurieren und das eSATA-Gerät verwalten.

Schritte

1. Gehen Sie zu **Speicher** → **Erweitert**.
2. Wählen Sie **eSATA-Nutzung** als **Export** oder **Aufzeichnen/Erfassen**.

Exportieren

Verwenden Sie den eSATA-Anschluss für die Datensicherung.

Aufzeichnen/Erfassen

Verwenden Sie die eSATA-Schnittstelle für die Aufnahme. Beachten Sie die folgenden Schritte für die Bedienungsanleitung.



The image shows a configuration window with two rows. The first row has 'eSATA' on the left and a dropdown menu showing 'eSATA1'. The second row has 'Usage' on the left and a dropdown menu showing 'Record/Capture'.

Abbildung 11-4 eSATA-Modus

Was ist als nächstes zu tun?

Wenn die eSATA-Nutzung auf **Aufzeichnen/Erfassen** eingestellt ist, geben Sie die Schnittstelle des Speichergeräts ein, um dessen Eigenschaften zu bearbeiten oder es zu initialisieren.

eSATA für die automatische Sicherung konfigurieren

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

Bevor Sie beginnen

Vergewissern Sie sich, dass das Gerät korrekt mit einer externen eSATA-Festplatte verbunden ist und die Verwendungsart auf **Export** eingestellt ist. Weitere Informationen finden Sie unter **eSATA verwalten**.

Schritte

1. Gehen Sie zu **Speicher → Automatische Sicherung**.
2. Aktivieren Sie **Auto-Backup**.
3. Legen Sie die Startzeit für das Backup in **Backup starten um** fest.

Hinwe

Wenn an einem Tag die Sicherung fehlschlägt, sichert der Videorecorder die Videos 48 Stunden vor der Startzeit der Sicherung am nächsten Tag.

-
4. Wählen Sie Kanäle für die Sicherung aus.
 5. Wählen Sie den gewünschten **Backup-Stream-Typ**.
 6. Wählen Sie den Typ "**Überschreiben**".
 - **Deaktivieren**: Wenn die Festplatte voll ist, hört sie auf zu schreiben.
 - **Aktivieren**: Wenn die Festplatte voll ist, werden neue Dateien geschrieben, während die ältesten Dateien gelöscht werden.
 7. Klicken Sie auf **Anwenden**.

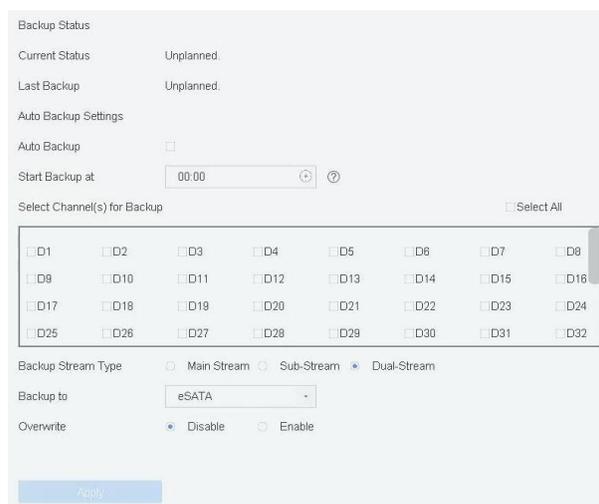


Abbildung 11-5 eSATA für die automatische Sicherung konfigurieren

11.2 Festplatten-Array

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 die 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.

11.2.1 Erstellen eines Festplattenarrays

Die Videorecorder der GD-RN-AT- und GD-RN-CT-Serien unterstützen softwarebasierte Festplatten-Arrays. Aktivieren Sie bei Bedarf die RAID-Funktion. Für die Erstellung eines Arrays gibt es zwei Möglichkeiten: One-Touch-Konfiguration und manuelle Konfiguration.

Erstellung mit einem Tastendruck

Mit der One-Touch-Konfiguration wird das Festplatten-Array erstellt. Standardmäßig ist der durch die One-Touch-Konfiguration erstellte Array-Typ RAID 5.

Bevor Sie beginnen

Installieren Sie mindestens 3 HDDs. Wenn mehr als 10 Festplatten installiert werden, werden 2 Arrays erstellt. Um einen zuverlässigen und stabilen Betrieb der Festplatten zu gewährleisten, wird empfohlen, Festplatten der Enterprise-Klasse mit demselben Modell und derselben Kapazität zu verwenden.

Schritte

1. Gehen Sie zu **Speicher → Erweitert**.
2. Aktivieren Sie **RAID aktivieren**.
3. Klicken Sie auf **Übernehmen** und starten Sie das Gerät neu, damit die Einstellungen wirksam werden.
4. Gehen Sie nach dem Neustart zu **Storage → RAID Setup → Physical Disk**.
5. Klicken Sie auf **One-Touch-Konfiguration**.
6. **Array-Name** bearbeiten und klicken Sie auf **OK**, um mit der Konfiguration zu beginnen.

Hinwe

Wenn Sie 4 oder mehr Festplatten installieren, wird eine Hot-Spare-Platte für den Wiederaufbau des Arrays erstellt.

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

Manuelle Erstellung

Manuelles Erstellen eines RAID 0-, RAID 1-, RAID 5-, RAID 6- oder RAID 10-Arrays.

Schritte

1. Gehen Sie zu **Speicher → Erweitert**.
2. Aktivieren Sie **RAID aktivieren**.
3. Klicken Sie auf **Übernehmen** und starten Sie das Gerät neu, damit die Einstellungen wirksam werden.
4. Gehen Sie nach dem Neustart zu **Storage → RAID Setup → Physical Disk**.
5. Klicken Sie auf **Erstellen**.

The screenshot shows a 'Create Array' dialog box with the following fields and options:

- Array Name:** An empty text input field.
- RAID Level:** A dropdown menu currently showing 'RAID 5'.
- Initialization Type:** A dropdown menu currently showing 'Initialize (Fast)'.
- Physical Disk:** A row of five checkboxes labeled '1', '2', '5', '9', and '10'.
- Array Capacity (Estimated):** 0GB.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Abbildung 11-6 Array erstellen

6. **Array-Name** eingeben.
7. Wählen Sie bei Bedarf den **RAID-Level**.
8. Wählen Sie die physischen Festplatten aus, die das Array bilden sollen.

Tabelle 11-1 Die erforderliche Anzahl von Festplatten

RAID-Stufe	Die erforderliche Anzahl von Festplatten
RAID 0	Mindestens 2 HDDs.
RAID 1	Mindestens 2 HDDs.
RAID-Stufe	Die erforderliche Anzahl von Festplatten
RAID 5	Mindestens 3 HDDs.
RAID 6	Mindestens 4 HDDs.
RAID 10	Die Anzahl der Festplatten muss in einem geraden Bereich von 4 bis 16 liegen.

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

No.	Name	Free Space	Physical Disk	Hot Spare	Status	Level	Rebuild	Delete	Task
1	Array01	3725/3725G	2 5 10		Degraded	RAID 5			Rebuild(Running) 0%

Abbildung 11-7 Array-Liste

11.2.2 Ein 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.

Funktionell

Kein Plattenverlust im Array.

Offline

Die Anzahl der verlorenen Festplatten hat den Grenzwert überschritten.

Abgebaut

Wenn eine Festplatte im Array ausfällt, wird das Array degradiert. Stellen Sie den Funktionsstatus wieder her, indem Sie das Array neu aufbauen.

Konfigurieren einer Hot Spare Disk

Die Hot-Spare-Platte ist für den automatischen Wiederaufbau des Disk-Arrays erforderlich.

Schritte

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

No.	Capacity	Array	Type	Status	Model	Hot Spare	Task
1	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None
<input type="checkbox"/> 2	2794.52GB		Normal	Functional	ST3000VX000-9YW166		None
5	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None
<input type="checkbox"/> 9	2794.52GB		Normal	Functional	ST3000VX000-1CU166		None
10	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None

Abbildung 11-8 Physikalische Festplatte

2. Klicken Sie auf für eine verfügbare Festplatte, um sie als Hot-Spare-Disk festzulegen.

Automatisch ein Array wiederherstellen

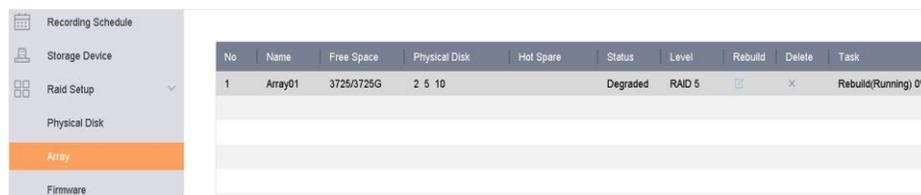
Der Videorekorder kann beschädigte Arrays automatisch mit Hot-Spare-Festplatten wiederherstellen.

Bevor Sie beginnen

Erstellen Sie Hot-Spare-Disks. Einzelheiten hierzu finden Sie unter **Konfigurieren einer Hot Spare Disk**.

Schritte

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



No	Name	Free Space	Physical Disk	Hot Spare	Status	Level	Rebuild	Delete	Task
1	Array01	3725/3725G	2 5 10		Degraded	RAID 5			Rebuild(Running) 0%

Abbildung 11-9 Array-Liste

Manuelles Wiederherstellen eines Arrays

Wenn keine Hot-Spare-Platten konfiguriert sind, müssen Sie ein degradiertes Array manuell wiederherstellen.

Bevor Sie beginnen

Um ein Array wiederherzustellen, muss mindestens eine verfügbare physische Festplatte vorhanden sein.

Schritte

1. Gehen Sie zu **Speicher → RAID-Einrichtung → Array**.
2. Klicken Sie auf  des degradierten Arrays.

Rebuild Array

Array Name

RAID Level

Array Disk

Physical Disk 2 9

Abbildung 11-10 Array wiederherstellen

3. Wählen Sie die verfügbare physische Festplatte aus.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **OK** im Popup-Fenster "Trennen Sie den physischen Datenträger nicht, wenn er gerade neu erstellt wird".

12 Hot Spare Rekorder Backup

Die Videorecorder der GD-RN-AT- und GD-RN-CT-Serie können ein N+1 Hot-Spare-System bilden. Das System besteht aus mehreren Arbeitsvideorecordern und einem Hot-Spare-Videorecorder; wenn der Arbeitsvideorecorder ausfällt, schaltet sich der Hot-Spare-Videorecorder ein und erhöht so die Zuverlässigkeit des Systems. Wenden Sie sich an Ihren Händler, um Einzelheiten zu den Modellen zu erfahren, die die Hot-Spare-Funktion unterstützen.

Zwischen dem Hot Spare-Videorecorder und jedem Arbeitsvideorecorder muss eine bidirektionale Verbindung hergestellt werden, die in der folgenden Abbildung dargestellt ist.

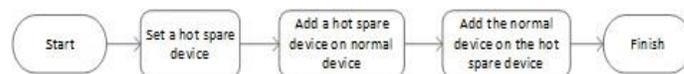


Abbildung 12-1 Aufbau eines Hot-Spare-Systems

12.1 Hot Spare Gerät einstellen

Hot-Spare-Geräte übernehmen die Aufgaben des Arbeitsgeräts, wenn das Arbeitsgerät ausfällt.

Schritte

1. Gehen Sie zu **System → Hot Spare**.
2. Wählen Sie den **Arbeitsmodus** als **Hot Spare Modus**.

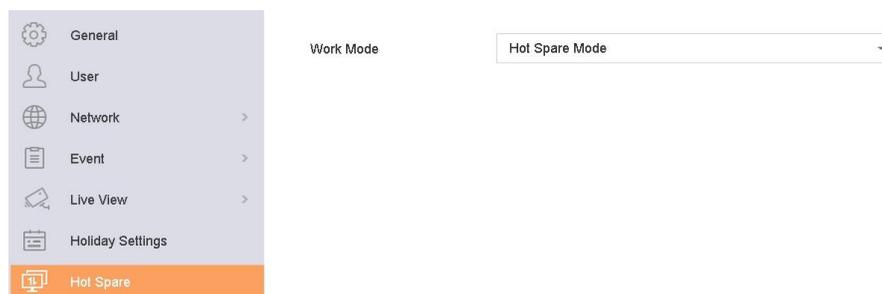


Abbildung 12-2 Hot Spare

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

Hinwe

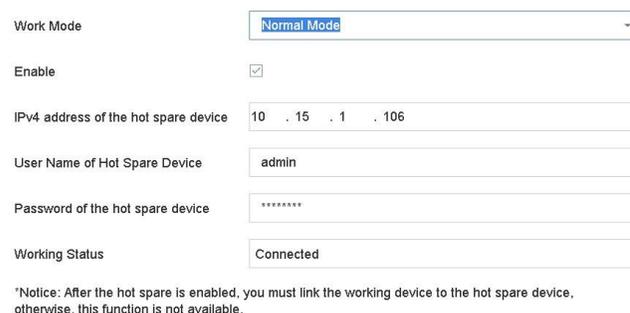
- Die Kameraverbindung wird deaktiviert, wenn das Gerät im Hot-Spare-Modus arbeitet.

-
- Es wird dringend empfohlen, die Standardeinstellungen des Geräts wiederherzustellen, nachdem der Arbeitsmodus des Hot-Spare-Geräts auf den Normalmodus umgestellt wurde, um den normalen Betrieb zu gewährleisten.
-

12.2 Arbeitsschreiber einstellen

Schritte

1. Gehen Sie zu **System → Hot Spare**.
2. Wählen Sie den **Arbeitsmodus** als **Normalmodus**.
3. **Aktivieren** Sie.
4. Geben Sie die IP-Adresse, den Benutzernamen und das Admin-Passwort des Hot-Spare-Recorders ein.



Work Mode	Normal Mode
Enable	<input checked="" type="checkbox"/>
IPv4 address of the hot spare device	10 . 15 . 1 . 106
User Name of Hot Spare Device	admin
Password of the hot spare device	*****
Working Status	Connected

*Notice: After the hot spare is enabled, you must link the working device to the hot spare device, otherwise, this function is not available.

Abbildung 12-3 Hot Spare

5. Klicken Sie auf **Anwenden**.

12.3 Verwalten des Hot-Spare-Systems

Schritte

1. Gehen Sie im Hot-Spare-Recorder auf **System → Hot Spare**.
2. Überprüfen Sie die Arbeitsschreiber in der Geräteliste und klicken Sie auf **Hinzufügen**, um den Arbeitsschreiber mit dem Hot-Spare-Schreiber zu verbinden. Die Beschreibungen des Arbeitsstatus des Arbeitsschreibers lauten wie folgt:

Kein Eintrag

Der Arbeitsschreiber funktioniert einwandfrei.

Sichern von Daten

Wenn der Arbeitsrekorder offline geht, zeichnet der Hot-Spare-Rekorder die Videos der Netzwerkkamera auf, die mit dem Arbeitsgerät verbunden ist. Das Video-Backup funktioniert jeweils für einen Arbeitsrekorder.

Synchronisierung

Wenn der Arbeitsrekorder wieder online ist, werden die verlorenen Videos durch die Videosynchronisierungsfunktion wiederhergestellt. Die Videosynchronisierungsfunktion kann jeweils für einen Arbeitsrekorder aktiviert werden.

Hinwe

An einen Hot-Spare-Rekorder können bis zu 32 Arbeitsrekorder angeschlossen

Work Mode

Device List

No.	IP Address
<input type="checkbox"/> 1	10.15.2.107

Working Dev...

No.	IP Address	Connection Status	Working Status	Delete

Abbildung 12-4 Arbeitsschreiber hinzufügen

13 Netzwerkeinstellungen

13.1 DDNS konfigurieren

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

Bevor Sie beginnen

Sie müssen die DynDNS- oder NO-IP-Dienste bei Ihrem ISP registrieren, bevor Sie die DDNS-Einstellungen konfigurieren.

Schritte

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

TCP/IP **DDNS** PPPoE NTP NAT

Enable

DDNS Type User Name

Server Address Password

Device Domain Name

Status DDNS is disabled.

Abbildung 13-1 DDNS-Einstellungen

2. **Aktivieren** Sie.

3. Wählen Sie als **DDNS-Typ** DynDNS.

4. Geben Sie die Server-Adresse für DynDNS ein (z. B. members.dyndns.org).

5. Geben Sie unter Device Domain Name (Gerätedomänenname) den Domänennamen ein, den Sie von der DynDNS-Website erhalten haben.

6. Geben Sie den **Benutzernamen** und das **Passwort** ein, die auf der DynDNS-Website registriert sind.

7. Klicken Sie auf **Anwenden**.

13.2 PPPoE konfigurieren

Wenn das Gerät über PPPoE mit dem Internet verbunden ist, müssen Sie unter **System → Netzwerk → TCP/IP → PPPoE** den Benutzernamen und das Kennwort entsprechend konfigurieren.

Wenden Sie sich an Ihren Internetdienstanbieter, um Einzelheiten über den PPPoE-Dienst zu erfahren.

13.3 SNMP konfigurieren

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

Bevor Sie beginnen

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

Schritte

1. Gehen Sie über den Webbrowser zu **Konfiguration** → **Netzwerk** → **Erweiterte Einstellungen** → **SNMP**.

SNMP v2

Enable SNMP v2c

Read SNMP Community

Write SNMP Community

Trap Address

Trap Port

SNMP v3

Enable SNMPv3

Read UserName

Security Level

Authentication Algorithm MD5 SHA

Authentication Password

Private-key Algorithm DES AES

Private-key password

Write UserName

Security Level

Authentication Algorithm MD5 SHA

Authentication Password

Private-key Algorithm DES AES

Private-key password

Trap Address

Trap Port

SNMP Other Settings

SNMP Port

Abbildung 13-2 SNMP-Einstellungen

2. Aktivieren Sie je nach Wunsch SNMP v2 oder SNMP v3.
3. Stellen Sie die entsprechenden Parameter ein.
4. **SNMP-Port** einstellen.
5. Klicken Sie auf **Speichern**.

13.4 E-Mail konfigurieren

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

Bevor Sie beginnen

Das Gerät muss mit einem lokalen Netzwerk (LAN) verbunden sein, das einen SMTP-Mailserver enthält. Das Netzwerk muss außerdem entweder mit einem Intranet oder dem Internet verbunden sein, je nachdem, wo sich die E-Mail-Konten befinden, an die Sie Benachrichtigungen senden möchten.

Schritte

1. Gehen Sie zu **System → Netzwerk → Erweitert → E-Mail**.

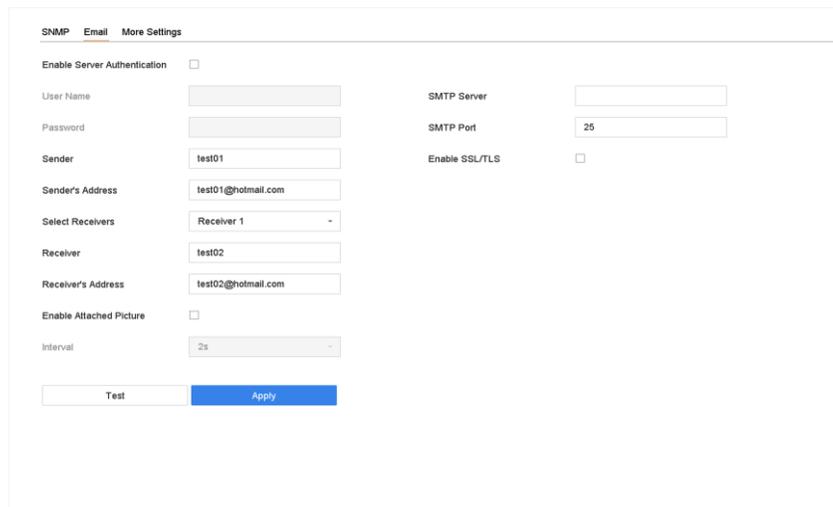


Abbildung 13-3 E-Mail-Einstellungen

2. Konfigurieren Sie die E-Mail-Einstellungen. **Aktivieren Sie die Server-Authentifizierung**

Aktivieren Sie die Funktion, 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 dies erfordert.

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.

Empfänger

Der Name des Empfängers.

Adresse des Empfängers

Die E-Mail-Adresse des Benutzers, der benachrichtigt werden soll.

Angehängtes Bild aktivieren

Aktivieren Sie diese Option, um eine E-Mail mit angehängten Alarmbildern zu versenden. Das Intervall ist die Zeit zwischen dem Versand von zwei aufeinanderfolgenden Alarmbildern.

3. Klicken Sie auf **Anwenden**.

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

13.5 Port-Zuordnung konfigurieren (NAT)

Für die Portzuordnung sind zwei Möglichkeiten vorgesehen, um den Fernzugriff über das segmentübergreifende Netzwerk zu realisieren: UPnP™ und manuelle Zuordnung.

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.

Universal Plug and Play (UPnP™) kann es dem Gerät ermöglichen, nahtlos das Vorhandensein anderer Netzwerkgeräte im Netzwerk zu erkennen und funktionale Netzwerkdienste für die gemeinsame Nutzung von Daten, Kommunikation usw. einzurichten. Sie können die UPnP™-Funktion verwenden, um die schnelle Verbindung des Geräts mit dem WAN über einen Router ohne Portzuordnung zu ermöglichen.

Schritte

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

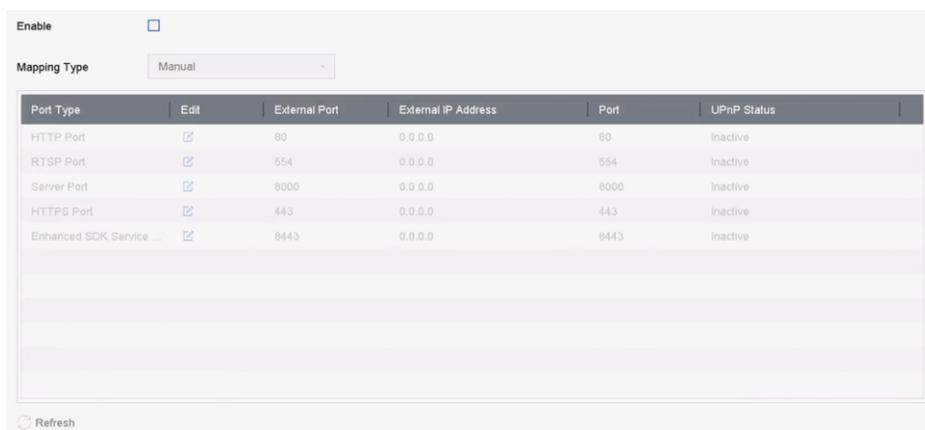


Abbildung 13-4 Port Mapping Einstellung

2. Aktivieren Sie.

3. Wählen Sie als Zuordnungsart **Manuell** oder **Automatisch**.

- Auto: Wenn Sie **Auto** wählen, sind die Portzuordnungselemente schreibgeschützt, und die externen Ports werden vom Router automatisch festgelegt.
- Manuell: Wenn Sie **Manuell** wählen, können Sie den externen Anschluss auf Wunsch bearbeiten, indem Sie auf **Externe Anschlusseinstellungen** klicken.

Hinwe

- Sie können die voreingestellte Anschlussnummer verwenden oder sie entsprechend den tatsächlichen Anforderungen ändern.
- Externer Port gibt die Portnummer für die Portzuordnung im Router an.
- Der Wert der RTSP-Port-Nr. 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 Port-Nr. für jedes Gerät eindeutig sein.

4. Rufen Sie die Einstellungsseite für den virtuellen Server des Routers auf; geben Sie bei **Interner Quellport** den Wert für den internen Port, bei **Externer Quellport** den Wert für den externen Port und andere erforderliche Inhalte ein.

Hinwe

- Jedes Element sollte mit dem Geräteport übereinstimmen, einschließlich Serverport, http-Port, RTSP-Port und https-Port.
- Die unten stehende Schnittstelle für die Einstellung des virtuellen Servers dient nur als Referenz, sie kann je nach Routerhersteller unterschiedlich sein. Bitte wenden Sie sich an den Hersteller des Routers, wenn Sie Probleme mit der Einstellung des virtuellen Servers haben.

Delete	External Source Port	Protocol	Internal Source IP	Internal Source Port	Application
<input type="checkbox"/>	81	TCP	192.168.251.101	80	HTTP

Abbildung 13-5 Einstellung virtueller Server Element

13.6 Anschluss konfigurieren

Sie können verschiedene Arten von Anschlüssen konfigurieren, um die entsprechenden Funktionen zu aktivieren.

Schritte

1. Gehen Sie zu **System** → **Netzwerk** → **Erweitert** → **Weitere Einstellungen**.

Alarm Host IP	<input type="text"/>
Alarm Host Port	<input type="text" value="0"/>
Server Port	<input type="text" value="8000"/>
HTTP Port	<input type="text" value="80"/>
Multicast IP	<input type="text"/>
RTSP Port	<input type="text" value="554"/>
Enhanced SDK Ser...	<input type="text" value="8443"/>

Abbildung 13-6 Anschlusseinstellungen

2. Konfigurieren Sie die Anschlusseinstellungen nach Bedarf.

Alarm Host IP/Port

Wenn ein Fernalarm-Host konfiguriert ist, sendet das Gerät das Alarmereignis oder die Ausnahmemeldung an den Host, wenn ein Alarm ausgelöst wird. Auf dem Remote-Alarm-Host muss die Client-Management-System-Software (CMS) installiert sein. Die IP-Adresse des Alarm-Hosts bezieht sich auf die IP-Adresse des Remote-PCs, auf dem die CMS-Software installiert ist, und der Anschluss des Alarm-Hosts (standardmäßig 7200) muss mit dem in der Software konfigurierten Anschluss für die Alarmüberwachung übereinstimmen.

Server-Anschluss

Der Server-Port (standardmäßig 8000) sollte für den Remote-Zugriff der Client-Software konfiguriert werden. Der gültige Bereich ist 2000 bis 65535.

HTTP-Anschluss

Der HTTP-Port (standardmäßig 80) sollte für den Fernzugriff per Webbrowser konfiguriert werden.

Multicast-IP

Multicast kann konfiguriert werden, um die Live-Ansicht für Kameras zu aktivieren, die die maximal zulässige Anzahl im Netzwerk überschreiten. Sowohl IPv4 als auch IPv6 sind für Multicast-IP-Adressen verfügbar. Für IPv4 wird eine IP-Adresse der Klasse D im Bereich von 224.0.0.0 bis 239.255.255.255 verwendet, 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.

RTSP-Anschluss

RTSP (Real Time Streaming Protocol) ist ein Netzwerksteuerungsprotokoll zur Steuerung von Streaming Media Servern. Der Port ist standardmäßig 554.

Erweiterter SDK-Dienstanschluss

Der erweiterte SDK-Dienst verwendet das TLS-Protokoll für den SDK-Dienst, das eine sicherere Datenübertragung ermöglicht. Der Port ist standardmäßig 8443.

3. Klicken Sie auf **Anwenden**.

13.7 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 **System → Systemdienst → ONVIF**.
2. Markieren Sie **ONVIF aktivieren**, um die ONVIF-Zugangsverwaltung zu aktivieren.

Hinwe

Das ONVIF-Protokoll ist standardmäßig

3. Klicken Sie auf **Hinzufügen**.
 4. **Benutzernamen** und **Passwort** eingeben
-

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, besonders im Hochsicherheitssystem kann das monatliche oder wöchentliche Zurücksetzen des Passworts Ihr Produkt besser schützen.

5. Wählen Sie die **Stufe Medienbenutzer, Bediener** oder **Administrator**.
6. Klicken Sie auf **OK**.

14 Dateiverwaltung

14.1 Dateien suchen

Geben Sie detaillierte Bedingungen für die Suche nach Videos und Bildern an.

Schritte

1. Gehen Sie zu **Dateiverwaltung → Video** oder **Dateiverwaltung → Bild**.
2. Wählen Sie eine Suchmethode. Zum Beispiel: **Suche nach Erscheinungsbild** oder **Suche nach Ereignis**.
3. Geben Sie die genauen Bedingungen an, einschließlich Uhrzeit, Kamera usw.
4. Klicken Sie auf **Suche starten**.
5. Klicken Sie auf **Kanal**, um einen gewünschten Kanal auszuwählen. Es werden die Suchergebnisse des ausgewählten Kanals angezeigt.
6. **Wahlweise:** Klicken Sie auf  oder , um den Ansichtsmodus zu wechseln.
7. **Optional:** Klicken Sie bei Videos auf  oder  in einem anderen Ansichtsmodus, um ein Video zu sperren. Das gesperrte Video wird nicht überschrieben.
8. **Optional:** Exportieren Sie die Suchergebnisse.
 - 1) Wählen Sie die Ergebnisdatei(en) aus der Suchergebnisoberfläche aus, oder markieren Sie **Alle auswählen**, um alle Dateien auszuwählen.
 - 2) Klicken Sie auf **Exportieren**, um die ausgewählte(n) Datei(en) auf ein Sicherungsgerät zu exportieren.

Hinwe

-Sie können  um den Exportfortschritt zu

- Sie können  um zur Suchoberfläche

14.2 Suchverlaufsoperation

Sie können die Suchbedingungen für eine spätere Bezugnahme und schnelle Suche speichern.

Schritte

1. Gehen Sie zu **Dateiverwaltung → Alle Dateien/Menschliche Dateien/Fahrzeugdateien**.
2. Legen Sie die Suchbedingungen fest.
3. Klicken Sie auf **Speichern**.
4. Geben Sie einen Namen in das Textfeld ein und klicken Sie auf **Beendet**. Die gespeicherten Suchbedingungen werden in der Liste der **Suchbedingungen** angezeigt.

Hinwe

Sie können schnell suchen durch Anklicken ein Zustand.

14.3 Dateien exportieren

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

Schritte

1. Dateien suchen. Weitere Informationen finden Sie unter **Dateien suchen**.
2. Dateien auswählen.
3. Klicken Sie auf **Exportieren**.
4. **Optional:** Aktivieren Sie bei Fahrzeugdateien das Kontrollkästchen **Kennzeichenstatistikinformationen sichern**, um die Kennzeichenstatistikinformationen später zu exportieren.
5. Wählen Sie die Datei aus, die als **Video und Protokoll** exportiert werden soll, und klicken Sie auf **OK**.
6. Wählen Sie das Sicherungsgerät und den Ordnerpfad.
7. Klicken Sie auf **OK**.

15 Benutzerverwaltung und Sicherheit

15.1 Verwalten von Benutzerkonten

Der Administrator-Benutzername lautet admin und das Passwort wird beim ersten Start des Geräts festgelegt. Der Administrator hat die Berechtigung, Benutzer hinzuzufügen und zu löschen und Benutzerparameter zu konfigurieren.

15.1.1 Einen Benutzer hinzufügen

Schritte

1. Gehen Sie zu **System** → **Benutzer**.
2. Klicken Sie auf **Hinzufügen**, um die Schnittstelle für Betriebsgenehmigungen zu öffnen.
3. Geben Sie das Admin-Passwort ein und klicken Sie auf **OK**.
4. In der Benutzeroberfläche Benutzer hinzufügen geben Sie die Informationen für einen neuen Benutzer ein.

Vorsicht

Starkes Passwort empfohlen - Wir empfehlen Ihnen dringend, ein starkes 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. Wir empfehlen Ihnen außerdem, Ihr Passwort regelmäßig zu ändern. Insbesondere bei Hochsicherheitssystemen kann ein monatliches oder wöchentliches Zurücksetzen des Passworts Ihr Produkt besser schützen.

Benutzerebene

Setzen Sie die Benutzerebene auf Bediener oder Gast. Verschiedene Benutzerebenen haben unterschiedliche Betriebsrechte.

- Bediener: Die Benutzerebene "Operator" verfügt standardmäßig über die Berechtigung "Zwei-Wege-Audio" in der Fernkonfiguration und alle Betriebsberechtigungen in der Kamerakonfiguration.
- Gast: Der Gast-Benutzer hat keine Berechtigung für Zwei-Wege-Audio in der Fernkonfiguration und verfügt standardmäßig nur über die lokale/ferne Wiedergabe in der Kamerakonfiguration.

MAC-Adresse des Benutzers

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

5. Klicken Sie auf **OK**.

In der Benutzerverwaltungsoberfläche wird der neu hinzugefügte Benutzer in der Liste angezeigt.

15.1.2 Bearbeiten des Admin-Benutzers

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

Schritte

1. Gehen Sie zu **System → Benutzer**.
2. Wählen Sie den Benutzer admin aus der Liste aus.
3. Klicken Sie auf **Ändern**.

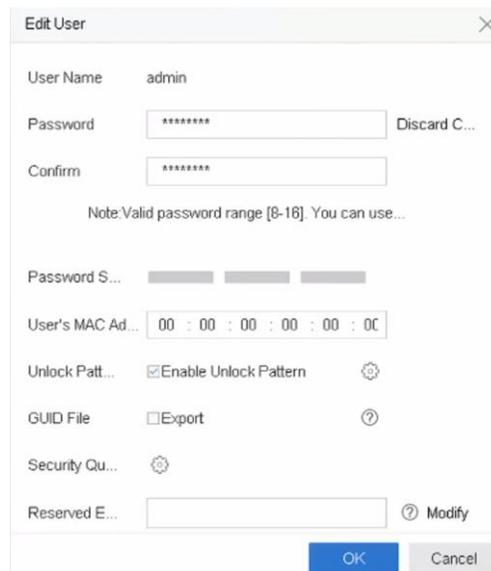


Abbildung 15-1 Benutzer bearbeiten (Admin)

4. Bearbeiten Sie die Admin-Benutzerinformationen wie gewünscht, einschließlich eines neuen Admin-Passworts (ein sicheres Passwort ist erforderlich) und der MAC-Adresse.
5. Bearbeiten Sie das Entsperrmuster für das Admin-Benutzerkonto.
 - 1) Aktivieren Sie **Entsperrmuster aktivieren**, um die Verwendung eines Entsperrmusters bei der Anmeldung am Gerät zu aktivieren.
 - 2) Benutze die Maus, um ein Muster zwischen den 9 Punkten auf dem Bildschirm zu zeichnen, und lass die Maus los, wenn das Muster fertig ist.
6. Markieren Sie **GUID-Datei exportieren**, um die GUID-Datei für das Admin-Benutzerkonto zu exportieren.

Hinwe

Wenn das Administratorkennwort geändert wird, exportieren Sie die neue GUID auf den angeschlossenen USB-Stick in der Import/Export-Schnittstelle, um das Kennwort später zurückzusetzen.

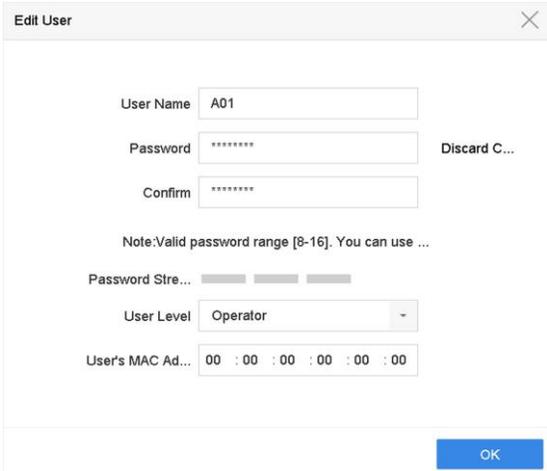
7. Konfigurieren Sie die Sicherheitsfrage zum Zurücksetzen des Passworts.
8. Konfigurieren Sie die reservierte E-Mail für die Passwortrücksetzung.
9. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

15.1.3 Bearbeiten eines Betreibers/Gastbenutzers

Sie können die Benutzerinformationen bearbeiten, einschließlich Benutzername, Passwort, Berechtigungsstufe und MAC-Adresse.

Schritte

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



The screenshot shows a dialog box titled "Edit User" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- User Name: A01
- Password: masked with asterisks
- Confirm: masked with asterisks
- Note: Valid password range [8-16]. You can use ...
- Password Stre...: Password strength indicator (three bars)
- User Level: Operator (dropdown menu)
- User's MAC Ad...: 00 : 00 : 00 : 00 : 00 : 00
- Discard C...: Button next to the password fields
- OK: Button at the bottom right

Abbildung 15-2 Benutzer bearbeiten (Bediener/Gast)

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

15.2 Benutzerberechtigungen verwalten

15.2.1 Benutzerberechtigungen festlegen

Für einen hinzugefügten Benutzer können Sie die verschiedenen Berechtigungen zuweisen, einschließlich der lokalen und entfernten Bedienung des Geräts.

Schritte

1. Gehen Sie zu **System → Benutzer**.
2. Wählen Sie einen Benutzer aus der Liste aus und klicken Sie dann auf , um die Oberfläche für die Berechtigungseinstellungen aufzurufen.

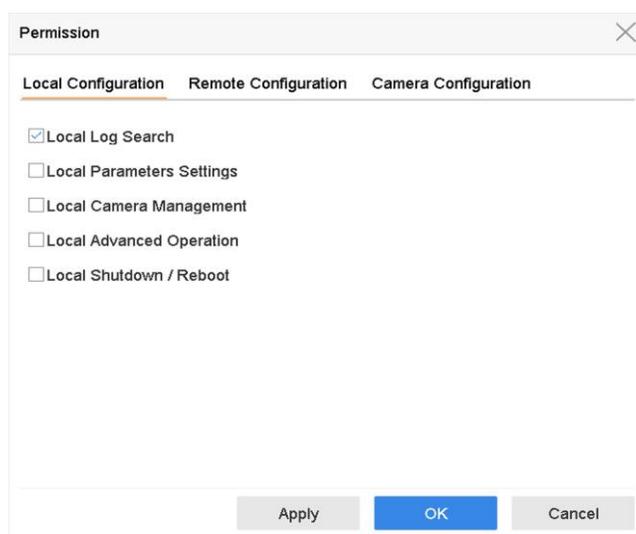


Abbildung 15-3 Schnittstelle für Benutzerberechtigungseinstellungen

3. Legen Sie die Betriebsrechte des Benutzers für die **lokale Konfiguration**, die **Fernkonfiguration** und die **Kamerakonfiguration** für den Benutzer fest.

1) Lokale Konfiguration einstellen

Lokale Logsuche

Durchsuchen und Anzeigen von Protokollen und Systeminformationen des Geräts.

Lokale Parametereinstellungen

Konfigurieren von Parametern, Wiederherstellen der werkseitigen Standardparameter und Importieren/Exportieren von Konfigurationsdateien.

Lokale Kameraverwaltung

Hinzufügen, Löschen und Bearbeiten von IP-Kameras.

Lokaler erweiterter Betrieb

Betrieb der Festplattenverwaltung (Initialisierung der Festplatte, Einstellung der Festplatteneigenschaften), Aktualisierung der Systemfirmware, Löschen der E/A-Alarmausgabe.

Lokale Abschaltung Neustart

Ausschalten oder Neustart des Geräts.

2) Fernkonfiguration einstellen

Remote Log Suche

Fernanzeige von Protokollen, die auf dem Gerät gespeichert sind.

Einstellungen der Remote-Parameter

Fernkonfiguration von Parametern, Wiederherstellung der werkseitigen Standardparameter und Import/Export von Konfigurationsdateien.

Kamera-Fernverwaltung

Ferngesteuertes Hinzufügen, Löschen und Bearbeiten von IP-Kameras.

Fernsteuerung der seriellen Schnittstelle

Konfigurieren der Einstellungen für die RS-232- und RS-485-Anschlüsse.

Fernsteuerung des Videoausgangs

Senden von Fernbedienungs signalen.

Zwei-Wege-Audio

Betrieb des Zwei-Wege-Funks zwischen dem Remote Client und dem Gerät.

Alarm-Fernsteuerung

Scharfschalten aus der Ferne (Alarm- und Ausnahmemeldung an den Remote-Client) und Steuerung des Alarmausgangs.

Erweiterter Fernbetrieb

Fernsteuerung der Festplattenverwaltung (Initialisierung der Festplatte, Einstellung der Festplatteneigenschaften), Aktualisierung der Systemfirmware, Löschen der E/A-Alarmausgabe.

Fernabschaltung/Neustart

Ausschalten oder Neustart des Geräts aus der Ferne.

3) Einstellen der Kamerakonfiguration

Ferngesteuerte Live-Ansicht

Live-Video der ausgewählten Kamera(s) aus der Ferne betrachten.

Lokaler Handbetrieb

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

Ferngesteuerte manuelle Bedienung

Ferngesteuertes Starten/Stoppen der manuellen Aufzeichnung und Alarmausgabe der ausgewählten Kamera(s).

Lokale Wiedergabe

Lokale Wiedergabe von aufgezeichneten Dateien der ausgewählten Kamera(s).

Fernwiedergabe

Ferngesteuerte Wiedergabe von aufgezeichneten Dateien der ausgewählten Kamera(s).

Lokale PTZ-Steuerung

Lokale Steuerung der PTZ-Bewegung der ausgewählten Kamera(s).

PTZ-Fernsteuerung

Ferngesteuerte PTZ-Bewegung der ausgewählten Kamera(s).

Lokaler Videoexport

Lokaler Export von aufgezeichneten Dateien der ausgewählten Kamera(s).

Lokale Live-Ansicht

Zeigen Sie das Live-Video der ausgewählten Kamera(s) in der lokalen Ansicht an.

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

15.2.2 Live-Ansichtsberechtigung auf dem Sperrbildschirm festlegen

Der Administrator kann die Live-Ansichtsberechtigung für bestimmte Kameras im Bildschirmsperrstatus des Geräts festlegen.

- Der Admin-Benutzer kann diese Berechtigung für Benutzerkonten festlegen.
- Wenn der normale Benutzer (Bediener oder Gast) keine lokale Live-Ansichtsberechtigung für bestimmte Kamera(s) hat, kann die Live-Ansichtsberechtigung für diese Kamera(s) im Sperrbildschirmstatus nicht konfiguriert werden (Live-Ansicht standardmäßig nicht zulässig).

Schritte

1. Gehen Sie zu **System → Benutzer**.
2. Klicken Sie auf **Live-Ansichtsberechtigung auf dem Sperrbildschirm**.
3. Geben Sie das Admin-Passwort ein und klicken Sie auf **Weiter**.

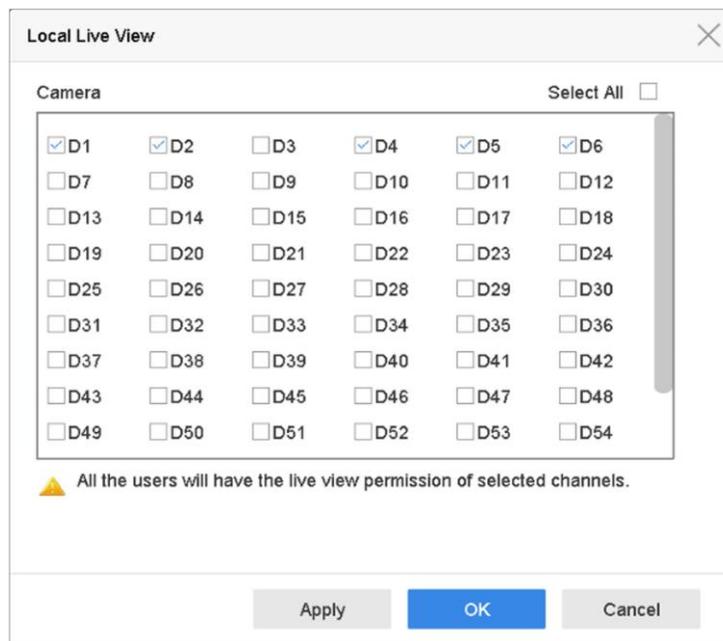


Abbildung 15-4 Berechtigungen für die Live-Ansicht auf dem Sperrbildschirm festlegen

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

15.2.3 Berechtigung zur doppelten Überprüfung für Nicht-Admin-Benutzer festlegen

Nachdem die doppelte Verifizierung im Channel aktiviert wurde, muss ein Nicht-Admin-Benutzer von einem autorisierten Benutzer verifiziert werden, um die Berechtigung zu erhalten. Nur der Administrator hat die Berechtigung, die doppelte Verifizierung einzustellen.

Schritte

1. Gehen Sie zu **Wartung** → **Systemdienst** → **Einstellungen für doppelte Verifizierung**.



Abbildung 15-5 Doppelte Verifizierung einstellen Benutzer

-
2. Aktivieren Sie die Option **Doppelte Verifizierung aktivieren**.
 3. Legen Sie den Benutzer für die Doppelverifizierung fest. Die Doppelverifizierung unterscheidet sich vom Systembenutzer. Sie können bis zu 8 doppelt verifizierte Benutzer hinzufügen.
 - 1) Klicken Sie auf **Hinzufügen**, um einen Benutzer mit doppelter Verifizierung hinzuzufügen.
 - 2) Geben Sie das Admin-Passwort ein.
 - 3) Legen Sie die Benutzerparameter fest, einschließlich **Benutzername, Passwort, Kamerazulassung** usw.
 - 4) Klicken Sie auf **OK**.
 4. Klicken Sie auf **Anwenden**.
 5. Berechtigung für Nicht-Admin-Benutzer festlegen.
 - 1) Gehen Sie zu **System → Benutzer**.
 - 2) Klicken Sie auf , um die Benutzerberechtigung zu bearbeiten.
 - 3) Wählen Sie **Kamerazulassung**. Nur **Lokale Wiedergabe, Fernwiedergabe/Download** und **Lokaler Videoexport** sind für die doppelte Überprüfung verfügbar.
 - 4) Wählen Sie den/die Kanal/Kanäle aus, der/die eine doppelte Überprüfung erfordert/erfordern.
 - 5) Klicken Sie auf **OK**.

15.3 Konfigurieren der Passwortsicherheit

15.3.1 Sicherheitsfragen konfigurieren

Die Sicherheitsfragen können Ihnen helfen, Ihr Passwort zurückzusetzen, wenn Sie Ihr Passwort vergessen haben oder Sicherheitsprobleme auftreten. Sie können die Sicherheitsfragen über den Webbrowser konfigurieren.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie sich im gleichen Netzwerksegment wie Ihr Gerät befinden.

Schritte

1. Gehen Sie zu **Konfiguration → System → Benutzerverwaltung → Benutzerverwaltung**.
2. Wählen Sie den Benutzer admin.
3. Klicken Sie auf **Konto-Sicherheitseinstellungen**.
4. Klicken Sie auf **Ändern**.

The image shows a 'Security Question Configuration' dialog box. It has three sections for security questions. Each section includes a question label, a dropdown menu for the question, and a text input field for the answer. The questions are: 'Your father's name?', 'Your mother's name?', and 'Your head teacher's name in senior high school'. Below these is an 'Export GUID File' section with a question mark icon and an 'Export' button. The next section is 'Password Recovery via E-mail' with a question mark icon and a text input field. At the bottom right are 'OK' and 'Cancel' buttons.

Abbildung 15-6 Sicherheitsfragen konfigurieren

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

15.3.2 Reservierte E-Mail konfigurieren

Die reservierte E-Mail wird Ihnen helfen, Ihr Passwort zurückzusetzen, wenn Sie es vergessen haben.

Schritte

1. Aktivieren Sie **Reservierte E-Mail**, wenn Sie das Gerät aktivieren, oder klicken Sie auf **Ändern**, wenn Sie das Administrator-Benutzerkonto bearbeiten.
2. Geben Sie die reservierte E-Mail Adresse ein.

The image shows a dialog box titled "Edit User" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- User Name: admin
- Password: A text box containing seven asterisks (*****), with a "Modify" button to its right.
- User's MAC Ad...: A text box containing "00 : 00 : 00 : 00 : 00 : 00".
- Unlock Patt...: A checkbox labeled "Enable Unlock Pattern" which is checked, with a gear icon to its right.
- GUID File: A checkbox labeled "Export" which is unchecked, with a question mark icon to its right.
- Security Qu...: A gear icon.
- Reserved E...: A text box containing "z*****@*****.com", with a question mark icon and a "Modify" button to its right.

At the bottom of the dialog, there are two buttons: "OK" (highlighted in blue) and "Cancel".

Abbildung 15-7 Reservierte E-Mail konfigurieren

3. Klicken Sie auf **OK**.

15.3.3 GUID-Datei exportieren

Die GUID-Datei kann Ihnen helfen, Ihr Passwort zurückzusetzen, wenn Sie es vergessen haben. Sie können die GUID-Datei über den Webbrowser exportieren. Bitte bewahren Sie die GUID-Datei ordnungsgemäß auf.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie sich im gleichen Netzwerksegment wie Ihr Gerät befinden.

Schritte

1. Gehen Sie zu **Konfiguration → System → Benutzerverwaltung → Benutzerverwaltung**.
2. Wählen Sie den Benutzer **admin**.
3. Klicken Sie auf **Konto-Sicherheitseinstellungen**.
4. Klicken Sie auf **Ändern**.

The image shows a 'Security Question Configuration' dialog box. It has three sections for security questions. Each section includes a question dropdown menu and an 'Answer' text input field. The questions are: 'Your father's name?', 'Your mother's name?', and 'Your head teacher's name in senior high school'. Below these is an 'Export GUID File' section with a question mark icon and an 'Export' button. Below that is a 'Password Recovery via E-mail' section with a question mark icon and a text input field. At the bottom right are 'OK' and 'Cancel' buttons.

Abbildung 15-8 GUID-Datei exportieren

5. Klicken Sie auf **Exportieren** in **GUID-Datei exportieren**.
6. Geben Sie das Admin-Passwort ein.
7. Speichern Sie die GUID-Datei in einem Verzeichnis Ihrer Wahl.

15.4 Passwort zurücksetzen

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

15.4.1 Passwort nach GUID zurücksetzen

Sie können das Kennwort mit Hilfe der GUID über den Webbrowser zurücksetzen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die richtige GUID-Datei haben.

Schritte

1. Klicken Sie auf der Benutzeranmeldeoberfläche auf **Passwort vergessen?**
2. Wählen Sie als **Verifizierungsmodus GUID-Dateiverifizierung**.
3. Klicken Sie auf **Durchsuchen**, um die GUID-Datei zu finden.
4. Klicken Sie auf **Weiter**.
5. Geben Sie ein neues Passwort ein.

Warnung

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 zurückzusetzen, vor allem im Hochsicherheitssystem kann das monatliche oder wöchentliche Zurücksetzen des Passworts Ihr Produkt besser schützen.

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

15.4.2 Passwort mit Sicherheitsfragen zurücksetzen

Sie können das Passwort mit Hilfe von Sicherheitsfragen über den Webbrowser zurücksetzen.

Bevor Sie beginnen

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

Schritte

1. Klicken Sie auf der Benutzeranmeldeoberfläche auf **Passwort vergessen?**
 2. Wählen Sie als **Überprüfungsmodus** die **Sicherheitsfragenüberprüfung**.
 3. Geben Sie die Antworten auf die einzelnen Fragen ein.
 4. Klicken Sie auf **Weiter**.
 5. Geben Sie das neue Passwort zweimal ein.
-

Warnung

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 zurückzusetzen, vor allem im Hochsicherheitssystem kann das monatliche oder wöchentliche Zurücksetzen des Passworts Ihr Produkt besser schützen.

6. Klicken Sie auf **Weiter**.

15.4.3 Passwort zurücksetzen durch reservierte E-Mail

Bevor Sie beginnen

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

Schritte

1. Klicken Sie auf der Benutzeranmeldeoberfläche auf **Passwort vergessen**.
2. Wählen Sie auf der Schnittstelle für die Art der Kennworrücksetzung die Option **Überprüfen durch Reservierte E-Mail**.
3. Klicken Sie auf **OK**.
4. Holen Sie sich den Verifizierungscode. Schließen Sie ein USB-Flash-Laufwerk an Ihr Gerät an.
5. Klicken Sie auf **Exportieren**, um den QR-Code auf ein USB-Flash-Laufwerk zu exportieren.
6. Senden Sie den QR-Code als Anhang per E-Mail an pw_recovery@device-service.com.
7. Prüfen Sie Ihre reservierte E-Mail, und Sie erhalten innerhalb von 5 Minuten einen Bestätigungscode.
8. Geben Sie den Verifizierungscode ein.
9. Klicken Sie auf **OK**, um das neue Kennwort festzulegen.

15.4.4 Passwort zurücksetzen durch SCMS

Bevor Sie beginnen

Stellen Sie sicher, dass Ihr Gerät SCMS aktiviert hat und mit einem registrierten SCMS-Konto verbunden ist.

Schritte

1. Klicken Sie auf der Benutzeranmeldeoberfläche auf **Passwort vergessen**.
2. Wählen Sie auf der Schnittstelle für die Art der Kennworrücksetzung die Option **Verifizierung durch reservierte E-Mail**.
3. Melden Sie sich bei der SCMS-App mit dem Konto an, das mit Ihrem Gerät verbunden ist.
4. Verwenden Sie die SCMS-App, um den QR-Code zu scannen. Danach erhalten Sie einen Verifizierungscode per Post.
5. Geben Sie den Verifizierungscode ein.
6. Klicken Sie auf **OK**.

16 Systemverwaltung

16.1 Gerät konfigurieren

Schritte

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

Die Standardsprache ist Englisch.

Ausgabe Standard

Stellen Sie den Ausgabestandard auf NTSC oder PAL ein, der mit dem Videoeingangsstandard übereinstimmen muss.

Auflösung

Konfigurieren Sie die Auflösung der Videoausgabe.

Gerät Name

Gerätename bearbeiten.

Gerät Nr.

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

Automatisch abmelden

Legen Sie die Timeout-Zeit für die Inaktivität des Menüs fest. Wenn z. B. die Timeout-Zeit auf 5 Minuten eingestellt ist, wechselt das System nach 5 Minuten Inaktivität vom aktuellen Betriebsmenü zur Live-Ansicht.

Geschwindigkeit des Mauszeigers

Legen Sie die Geschwindigkeit des Mauszeigers fest; 4 Stufen sind konfigurierbar.

Assistent einschalten

Aktivieren/deaktivieren Sie den Assistenten beim Starten des Geräts.

Passwort einschalten

Aktivieren/deaktivieren Sie die Verwendung des Anmeldekennworts.

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

16.2 Zeit konfigurieren

16.2.1 Manuelle Zeitsynchronisation

Schritte

-
1. Gehen Sie zu **System → Allgemein**.
 2. Stellen Sie Datum und Uhrzeit ein.
 3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

16.2.2 NTP-Synchronisierung

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

Schritte

1. Gehen Sie zu **System → Netzwerk → TCP/IP → NTP**.
2. **Aktivieren** Sie.
3. Konfigurieren Sie die NTP-Einstellungen nach Bedarf.

Intervall (min)

Zeitintervall zwischen zwei Zeitsynchronisationen mit dem NTP-Server

NTP-Server

IP-Adresse des NTP-Servers

NTP-Anschluss

Port des NTP-Servers

4. Klicken Sie auf **Anwenden**

16.2.3 Sommerzeit-Synchronisation

Sommerzeit bezeichnet den Zeitraum des Jahres, in dem die Uhren um eine Periode vorgestellt werden. In einigen Regionen der Welt hat dies den Effekt, dass in den Monaten mit dem wärmsten Wetter mehr Sonnenstunden am Abend zur Verfügung stehen.

Zu Beginn der Sommerzeit werden die Uhren um eine bestimmte Zeitspanne vorgestellt (abhängig von der eingestellten Sommerzeit) und bei der Rückkehr zur Standardzeit (ST) um die gleiche Zeit zurückgestellt.

Schritte

1. Gehen Sie zu **System → Allgemein**.
2. Aktivieren Sie **DST aktivieren**.
3. Stellen Sie den **Sommerzeitmodus** auf **Auto** oder **Manuell** ein. **Automatisch**

Aktivieren Sie automatisch die Standardzeit für die Sommerzeit gemäß den lokalen Regeln für die Sommerzeit.

Handbuch

Legen Sie die Start- und Endzeit der Sommerzeit sowie die Sommerzeitverzögerung manuell fest.

-
4. Stellen Sie die Sommerzeitvorwahl ein. Stellen Sie die Zeit (30/60/90/120 Minuten) ein, die von der Standardzeit abweicht.
 5. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

16.2.4 IP-Kamera Zeitsynchronisation

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

Schritte

1. Gehen Sie zu **Kamera → Kamera → IP-Kamera**.
2. Positionieren Sie den Cursor auf das Fenster der IP-Kamera und klicken Sie auf  .
3. Aktivieren Sie **IP-Kamera-Zeitsynchronisation aktivieren**.
4. Klicken Sie auf **OK**.

16.3 Netzdetektion

16.3.1 Überwachung des Netzwerkverkehrs

Die Überwachung des Netzwerkverkehrs ist der Prozess der Überprüfung, Analyse und Verwaltung des Netzwerkverkehrs auf Anomalien oder Prozesse, die die Leistung, Verfügbarkeit und/oder Sicherheit des Netzwerks beeinträchtigen können.

Schritte

1. Gehen Sie zu **Wartung → Netzwerk → Verkehr**.
2. Sie können den Status des Netzwerkverkehrs in Echtzeit anzeigen, einschließlich MTU (Maximum Transmission Unit) und Netzwerkdurchsatz.

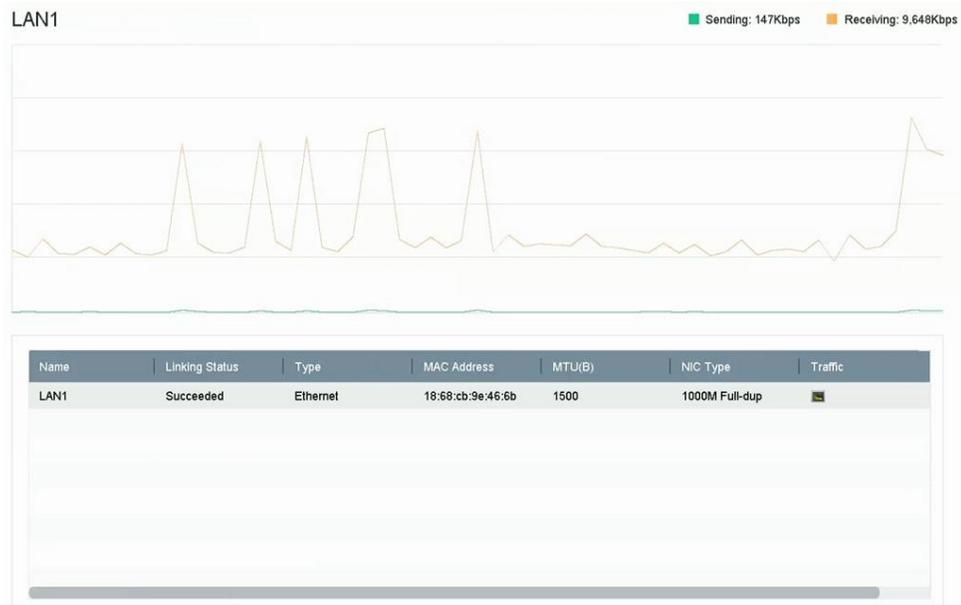


Abbildung 16-1 Netzwerkverkehr

16.3.2 Testnetzverzögerung und Paketverlust

Die Netzwerkverzögerung wird durch eine langsame Reaktion des Geräts verursacht, wenn übergroße Dateninformationen während der Übertragung unter einem bestimmten Netzwerkprotokoll, z. B. TCP/IP, nicht begrenzt werden. Der Paketverlusttest dient zum Testen der Netzwerk-Paketverlustrate, d. h. des Verhältnisses von verlorenen Datenpaketen und der Gesamtzahl der übertragenen Datenpakete.

Schritte

1. Gehen Sie zu **Wartung → Netzwerk → Netzwerkerkennung**.
2. Wählen Sie unter **NIC auswählen** eine Netzwerkkarte aus.
3. Geben Sie die Ziel-IP-Adresse unter **Zieladresse** ein.
4. Klicken Sie auf **Test**.

Network Delay, Packet Loss Test

Select NIC

Destination Address

Abbildung 16-2 Testnetzverzögerung und Paketverlust

16.3.3 Netzwerk-Paket exportieren

Nachdem der Rekorder auf das Netzwerk zugegriffen hat, können Sie ein USB-Flash-Laufwerk verwenden, um Netzwerkpakete zu exportieren.

Bevor Sie beginnen

Bereiten Sie ein USB-Flash-Laufwerk für den Export von Netzwerkpaketen vor.

Schritte

1. Stecken Sie das USB-Flash-Laufwerk ein.
2. Gehen Sie zu **Wartung → Netzwerk → Netzwerkerkennung**.
3. Wählen Sie die Netzwerkkarte unter **NIC auswählen** aus.
4. Wählen Sie das USB-Flash-Laufwerk unter **Gerätename** aus. Sie können auf **Aktualisieren** klicken, wenn das angeschlossene lokale Sicherungsgerät nicht angezeigt werden kann.



Abbildung 16-3 Netzwerk-Paket exportieren

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

Hinwe

Es werden jeweils 1 MB Dateizeit als Standard.

16.3.4 Netzwerk-Ressourcenstatistik

Der Fernzugriff, einschließlich Webbrowser und Client-Software, verbraucht die Ausgangsbandbreite. Sie können die Echtzeit-Bandbreitenstatistiken einsehen.

Schritte

1. Gehen Sie zu **Wartung → Netzwerk → Netzwerkstatus**.

Type	bandwidth
IP Camera	5,120Kbps
Remote Live View	0bps
Remote Playback	0bps
Net Receive Idle	155Mbps
Net Send Idle	160Mbps

Abbildung 16-4 Netzwerk-Ressourcenstatistik

2. Zeigen Sie die Bandbreitenstatistiken an, einschließlich **IP-Kamera**, **Remote Live View**, **Remote Play**, **Net Total Idle** usw.
3. **Optional:** Klicken Sie auf **Aktualisieren**, um die neuesten Daten zu erhalten.

16.4 Wartung von Speichergeräten

Geben Sie hier eine kurze Beschreibung Ihres Konzepts ein (optional).

Dies ist der Anfang Ihres Konzepts.

16.4.1 Erkennung von fehlerhaften Sektoren

Schritte

1. Gehen Sie zu **Wartung** → **Festplattenbetrieb** → **Erkennung von fehlerhaften Sektoren**.
2. Wählen Sie die Festplattennummer, die Sie konfigurieren möchten, in der Dropdown-Liste aus.
3. Wählen Sie als Erkennungsart "**All Detection**" oder "**Key Area Detection**".
4. Klicken Sie auf **Selbsttest**, um die Erkennung zu starten.

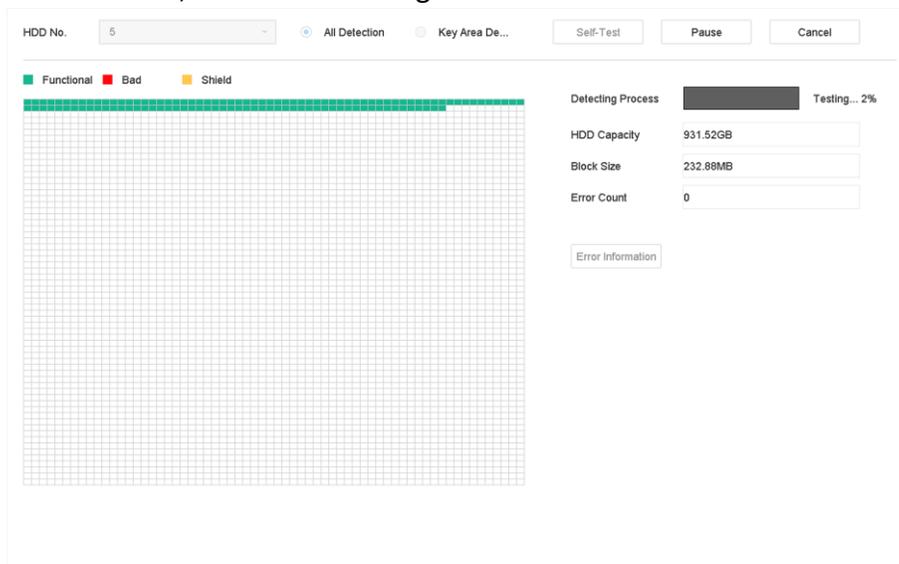


Abbildung 16-5 Erkennung von fehlerhaften Sektoren

Hinwe

- Sie können die Erkennung unterbrechen/fortsetzen oder abbrechen.
- Nach Abschluss der Prüfung können Sie auf **Fehlerinformationen** klicken, um die detaillierten Schadensinformationen anzuzeigen.

16.4.2 S.M.A.R.T.-Detektion

HDD-Erkennungsfunktionen wie die Annahme der S.M.A.R.T.- und der Bad Sector Detection-Techniken. S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) sind HDD-Überwachungssysteme zur Erkennung verschiedener Zuverlässigkeitsindikatoren in der Hoffnung, Ausfälle vorhersehen zu können.

Schritte

1. Gehen Sie zu **Wartung → Festplattenbetrieb → Erkennung von fehlerhaften Sektoren**.
2. Wählen Sie die Festplatte aus, um ihre S.M.A.R.T.-Informationsliste anzuzeigen.
3. Wählen Sie die Selbsttesttypen **Kurztest, Erweiterter Test** oder **Fördertest**.
4. Klicken Sie auf **Selbsttest**, um die S.M.A.R.T.-Festplatten-Selbsteinschätzung zu starten.

Continue to use this disk when self-evaluation is failed.

HDD No.

Self-Test Type Self-Test

Temperature... Self-Evaluation

Working Time... All-Evaluation

S.M.A.R.T Infor

ID	Attribute Name	Status	Flags	Threshold	Value	Worst	Raw Value
0x1	Raw Read Error R...	OK	2f	51	200	200	8
0x3	Spin Up Time	OK	27	21	113	107	7316
0x4	Start/Stop Count	OK	32	0	98	98	2657
0x5	Reallocated Sector...	OK	33	140	200	200	0
0x7	Seek Error Rate	OK	2e	0	200	200	0
0x9	Power-on Hours C...	OK	32	0	88	88	9369
0xa	Spin Up Retry Count	OK	32	0	100	100	0
0xb	Calibration Retry C...	OK	32	0	100	100	0

Abbildung 16-6 S.M.A.R.T.-Einstellungsschnittstelle

Hinwe

Um die Festplatte auch dann zu verwenden, wenn die S.M.A.R.T.-Prüfung fehlgeschlagen ist, markieren Sie **Weiter verwenden, wenn die Selbstausswertung fehlgeschlagen ist**.

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

16.4.3 Erkennung des Festplattenzustands

Sie können den Gesundheitsstatus einer Western Digital- oder Seagate-Festplatte anzeigen, die nach dem 1. Oktober 2017 erstellt wurde. Verwenden Sie diese Funktion, um Probleme mit Festplatten zu beheben. Health Detection zeigt einen detaillierteren Festplattenstatus als die S.M.A.R.T.-Funktion.

Schritte

1. Gehen Sie zu **Wartung → Festplattenbetrieb → Zustandserfassung**.



Abbildung 16-7 Gesundheitszustandserfassung

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

16.4.4 Festplattenklon konfigurieren

Wählen Sie die Festplatten aus, die auf die eSATA-Festplatte geklont werden sollen.

Bevor Sie beginnen

Schließen Sie eine eSATA-Festplatte an das Gerät an.

Schritte

1. Gehen Sie zu **Wartung → Festplattenbetrieb → Festplattenklonen**.

Clone Source

Label	Capacity	Status	Property	Type	Free Space	Group
<input type="checkbox"/> 1	1863.02GB	Normal	R/W	Local	1858.00GB	1
<input type="checkbox"/> 2	2794.52GB	Normal	R/W	Local	2794.00GB	1
<input type="checkbox"/> 5	1863.02GB	Normal	R/W	Local	1862.00GB	1
<input type="checkbox"/> 9	2794.52GB	Normal	R/W	Local	2794.00GB	1
<input type="checkbox"/> 10	1863.02GB	Normal	R/W	Local	1862.00GB	1

Clone Destination

eSATA Refresh

Capacity Clone

Abbildung 16-8 Festplattenklon

2. Wählen Sie die zu klonende Festplatte aus. Die Kapazität der ausgewählten Festplatte muss mit der Kapazität des Klonziels übereinstimmen.
3. Klicken Sie auf **Klonen**.
4. Klicken Sie im Pop-up-Fenster auf **Ja**, um den Klon zu erstellen.

16.4.5 Datenbank reparieren

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

Schritte

1. Gehen Sie zu **Speicher → Speichergerät**.
2. Wählen Sie das Laufwerk aus.
3. Klicken Sie auf **Datenbank reparieren**.
4. Klicken Sie auf **Ja**.

Hinwe

- 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.
- Sie können den Fortschritt der Reparaturen unter **Status** verfolgen.

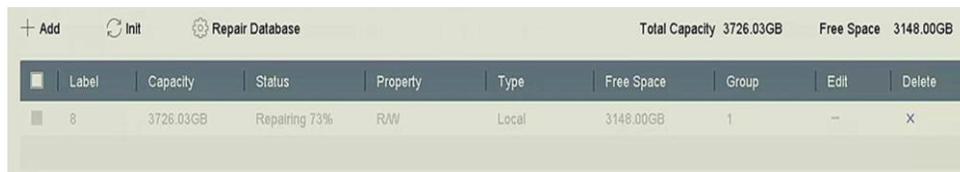


Abbildung 16-9 Datenbank reparieren

16.5 System aufrüsten

16.5.1 Gerät aufrüsten

Die Firmware Ihres Geräts kann mit einem lokalen Sicherungsgerät oder einem entfernten FTP-Server aktualisiert werden.

Upgrade durch lokales Sicherungsgerät

Bevor Sie beginnen

Verbinden Sie Ihr Gerät mit einem lokalen Speichergerät, das die Firmware-Update-Datei enthält.

Schritte

1. Gehen Sie zu **Wartung** → **Upgrade**.
2. Klicken Sie auf **Lokales Upgrade**, um die Schnittstelle für das lokale Upgrade zu öffnen.

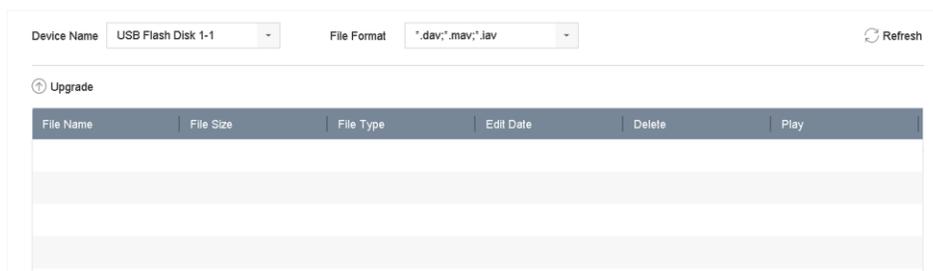


Abbildung 16-10 Lokale Upgrade-Schnittstelle

3. Wählen Sie die Firmware-Update-Datei vom Speichermedium aus.
4. Klicken Sie auf **Upgrade**, um das Upgrade zu starten.

Nach Abschluss der Aktualisierung wird das Gerät automatisch neu gestartet, um die neue Firmware zu aktivieren.

Aktualisierung per FTP

Bevor Sie beginnen

Stellen Sie sicher, dass die Netzwerkverbindung zwischen dem PC (auf dem der FTP-Server läuft) und dem Gerät gültig und korrekt ist. Starten Sie den FTP-Server auf dem PC und kopieren Sie die Firmware in das entsprechende Verzeichnis auf Ihrem PC.

Schritte

1. Gehen Sie zu **Wartung → Upgrade**.
2. Klicken Sie auf **FTP**, um die lokale Upgrade-Schnittstelle zu öffnen.

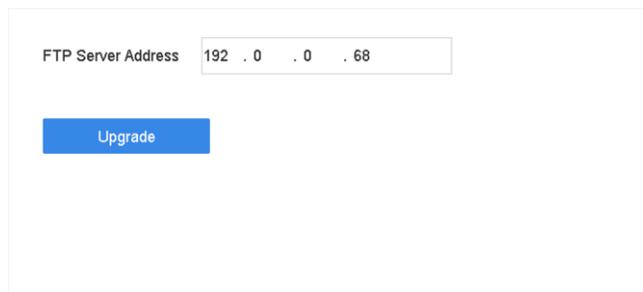


Abbildung 16-11 FTP-Upgrade-Schnittstelle

3. Geben Sie die **Adresse des FTP-Servers** ein.
4. Klicken Sie auf **Upgrade**, um das Upgrade zu starten.
5. Starten Sie das Gerät nach Abschluss des Upgrades neu, um die neue Firmware zu aktivieren.

16.5.2 IP-Kameras aufrüsten

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

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie das USB-Flash-Laufwerk an das Gerät angeschlossen haben und dass es die Aktualisierungsfirmware für die IP-Kamera enthält.

Schritte

1. Wählen Sie in der Kameraverwaltungsoberfläche eine Kamera aus.
2. Gehen Sie zu **Weitere Einstellungen → Upgrade**.
3. Wählen Sie die Firmware-Upgrade-Datei vom USB-Flash-Laufwerk aus.
4. Klicken Sie auf **Upgrade**.

Die IP-Kamera wird nach Abschluss der Aktualisierung automatisch neu gestartet.

16.6 Import/Export von IP-Kamera-Konfigurationsdateien

Die IP-Kamerainformationen, einschließlich der IP-Adresse, des Verwaltungsports, des Admin-Passworts usw., können im Microsoft Excel-Format gespeichert und auf dem lokalen Gerät gesichert werden. Die exportierte Datei kann auf einem PC bearbeitet werden, einschließlich des

Hinzufügen oder Löschen von Inhalten und des Kopierens der Einstellungen auf andere Geräte, indem die Excel-Datei dorthin importiert wird.

Bevor Sie beginnen

Wenn Sie die Konfigurationsdatei importieren, schließen Sie das Speichermedium, das die Konfigurationsdatei enthält, an das Gerät an.

Schritte

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

Hinweis

Nachdem der Importvorgang abgeschlossen ist, müssen Sie das Gerät neu starten, um die Einstellungen zu aktivieren.

16.7 Import/Export von Gerätekonfigurationsdateien

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.

Bevor Sie beginnen

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

Schritte

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

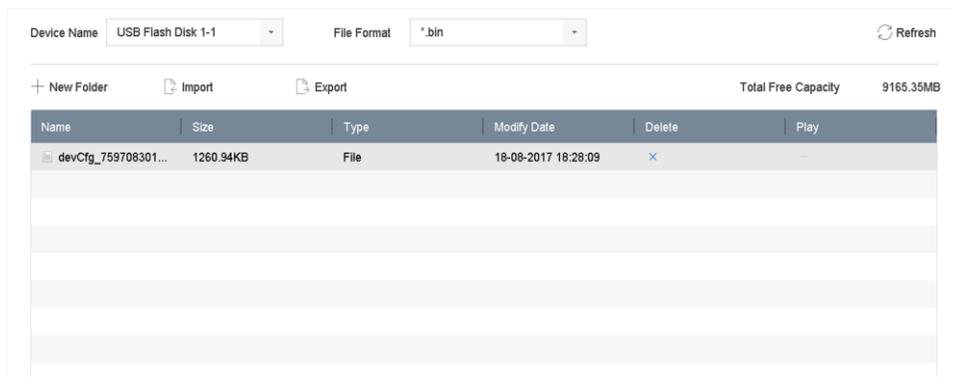


Abbildung 16-12 Import/Export der Konfigurationsdatei

2. Exportieren oder importieren Sie die Gerätekonfigurationsdateien.

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

Hinwe

Nach mit fertig importieren Konfiguration Dateiwird das Gerät neu gestartet.

16.8 Protokollverwaltung

16.8.1 Protokollspeicherung

Sie können die Speicherplatte für die Protokolle und die Speicherdauer der Protokolle anpassen.

Schritte

1. Gehen Sie zu **Speicher** → **Erweitert**.

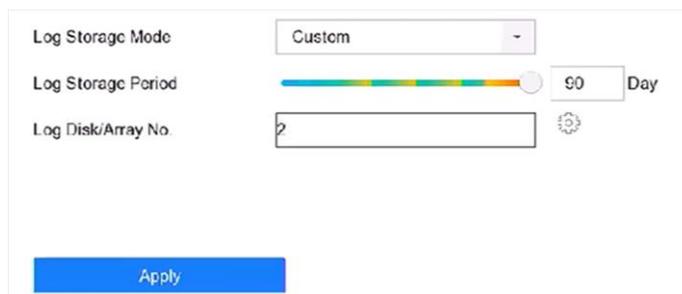


Abbildung 16-13 Protokollspeicherung

2. **Log-Speichermodus** einstellen.

Systemvoreinstellung Jeder Festplatte wird ein bestimmter Speicherplatz zugewiesen, auf dem etwa 400.000 Protokolle gespeichert werden können. Wenn die Protokolle voll sind, werden alte Protokolle überschrieben.

Benutzerdefiniert Sie können den **Zeitraum für die Speicherung von Protokollen** festlegen und die **Festplatte** für die Speicherung von Protokollen zuweisen. Wenn die Protokollplatte voll ist, werden Protokolle, die den Zeitraum überschreiten, überschrieben.

3. Klicken Sie auf **Anwenden**.

16.8.2 Logdateien suchen und exportieren

Der Gerätebetrieb, Alarme, Ausnahmen und Informationen können in Protokolldateien gespeichert werden, die jederzeit eingesehen und exportiert werden können.

Schritte

1. Gehen Sie zu **Wartung** → **Protokollinformationen**.

Time: 2017-08-18 00:00:00 - 2017-08-18 23:59:59 [Search]

Major Type: All

Minor Type: Select All [Export ALL]

Abbildung 16-14 Schnittstelle zur Protokollsuche

2. Legen Sie die Suchbedingungen für das Protokoll fest, einschließlich Zeit, Haupt- und Nebentyp.

3. Klicken Sie auf **Suchen**, um die Suche in den Protokolldateien zu starten.

4. Die übereinstimmenden Protokolldateien werden in der Liste angezeigt, wie unten dargestellt.

Time: 2017-08-18 00:00:00 - 2017-08-18 23:59:59 [Search]

Major Type: All

Minor Search Result

No.	Major Type	Time	Minor Type	Parameter	Play	Details
103	Alarm	18-08-2017 07:07:31	Motion Detection ...	N/A	▶	⊙
104	Alarm	18-08-2017 07:07:43	Motion Detection ...	N/A	▶	⊙
105	Alarm	18-08-2017 07:16:27	Motion Detection ...	N/A	▶	⊙
106	Alarm	18-08-2017 07:16:37	Motion Detection ...	N/A	▶	⊙
107	Inform...	18-08-2017 07:17:19	System Running ...	N/A	▶	⊙
108	Inform...	18-08-2017 07:17:19	System Running ...	N/A	▶	⊙
109	Inform...	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	▶	⊙
110	Inform...	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	▶	⊙
111	Inform...	18-08-2017 07:27:20	System Running ...	N/A	▶	⊙

Total: 1151 P: 2/12 [Navigation] [Export] [Back]

Sudden Change of Sound Intensity Alarm Started
 Sudden Change of Sound Intensity Alarm Stopped
 Face Detection (Face Capture) Alarm Started
 Face Detection (Face Capture) Alarm Stopped

Abbildung 16-15 Log-Suchergebnisse

Hinwe

Bis zu 2.000 LogDateikönnen jeweils angezeigt.

5. Verwandte Operationen:

-  Klicken oder doppelklicken Sie darauf, um detaillierte Informationen anzuzeigen.
-  Klicken Sie darauf, um die entsprechende Videodatei anzuzeigen.

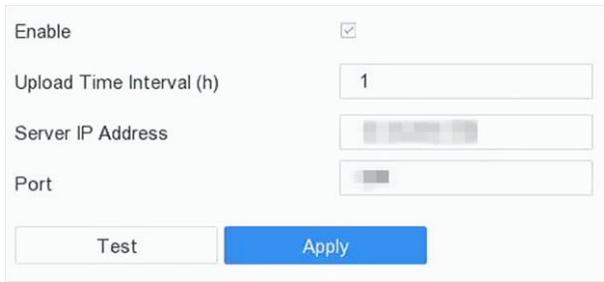
ALLE exportieren/exportieren Klicken Sie darauf, um alle Systemprotokolle auf das Speichermedium zu exportieren.

16.8.3 Protokoll auf den Server hochladen

Sie können Systemprotokolle zur Sicherung auf den Server hochladen.

Schritte

1. Gehen Sie zu **System** → **Netzwerk** → **Erweitert** → **Protokollservereinstellungen**.



Enable	<input checked="" type="checkbox"/>
Upload Time Interval (h)	<input type="text" value="1"/>
Server IP Address	<input type="text"/>
Port	<input type="text"/>
<input type="button" value="Test"/> <input type="button" value="Apply"/>	

Abbildung 16-16 Log-Server-Einstellungen

2. **Aktivieren** prüfen

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 **Anwenden**.

16.8.4 Einweg-Authentifizierung

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

Bevor Sie beginnen

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

Schritte

1. Gehen Sie zu **Konfiguration** → **Netzwerk** → **Erweiterte Einstellungen** → **Protokollserverkonfiguration**.

The screenshot shows a web configuration page for a protocol server. At the top, there is a checkbox labeled 'Enable' which is checked. Below it are three input fields: 'Log Server Address' with the value '10.10.201.168', 'Log Server Port' with the value '8042', and 'Upload Time Interval (h)' with the value '1'. A 'Test' button is located below these fields. The 'Client Certificate' section contains three buttons: 'Create' (with 'No file.' next to it), 'Download', and 'Delete'. Below this is an 'Install Generated Certificate' section with a file selection field, a 'Browse' button, and an 'Install' button. The 'CA Certificate' section has an 'Install' label, a file selection field, a 'Browse' button, and an 'Install' button. At the bottom left of the form is a large blue 'Save' button.

Abbildung 16-17 Einweg-Authentifizierung

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

16.8.5 Zwei-Wege-Authentifizierung

Sie können ein CA-Zertifikat (vom Server) auf Ihrem Gerät installieren, um den Server zu autorisieren, und ein Zertifikat (von Ihrem Gerät) erstellen, um Ihr Gerät durch den Server zu autorisieren. Dies würde die Sicherheit der Protokollkommunikation verbessern. Die Zwei-Wege-Authentifizierung kann über den Webbrowser konfiguriert werden.

Bevor Sie beginnen

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

Schritte

1. Gehen Sie zu **Konfiguration** → **Netzwerk** → **Erweiterte Einstellungen** → **Protokollserverkonfiguration**.

The screenshot shows a configuration interface for two-way authentication. It features several input fields and buttons:

- Enable:** A checked checkbox.
- Log Server Address:** A text field containing '10.10.201.168'.
- Log Server Port:** A text field containing '8042'.
- Upload Time Interval (h):** A text field containing '1'.
- Test:** A button to test the connection.
- Client Certificate:**
 - Create Certificate Request:** A button labeled 'Create' with 'No file.' next to it.
 - Download Certificate Request:** A button labeled 'Download'.
 - Delete Certificate Request:** A button labeled 'Delete'.
 - Install Generated Certificate:** A text field with 'Browse' and 'Install' buttons.
- CA Certificate:**
 - Install:** A text field with 'Browse' and 'Install' buttons.
- Save:** A large blue button at the bottom.

Abbildung 16-18 Zwei-Wege-Authentifizierung

2. Installieren Sie das CA-Zertifikat unter **CA-Zertifikat**.
3. Klicken Sie unter **Client-Zertifikat** auf **Erstellen**, und folgen Sie dem Popup-Fenster, um das Zertifikat zu erstellen.
4. Klicken Sie auf **Download**, um die Zertifikatsdatei an einen gewünschten Ort herunterzuladen.
5. Laden Sie die heruntergeladene Zertifikatsdatei auf den Server hoch, und der Server wird den Zertifikatsschlüssel zurückgeben.
6. Öffnen Sie das Zertifikat als Textdatei, und ändern Sie es mit dem Zertifikatsschlüssel, den der Server zurückgegeben hat.
7. Installieren Sie das geänderte Zertifikat in **Client-Zertifikat**.
8. **Optional:** Klicken Sie auf **Test**, um zu prüfen, ob die Verbindung gültig ist.
9. Klicken Sie auf **Speichern**.

16.9 Standardeinstellungen wiederherstellen

Schritte

1. Gehen Sie zu **Wartung** → **Standard**.

The screenshot shows three options for restoring settings:

- Restore Defaults:** Reset all settings to factory default except network and admin password settings.
- Factory Defaults:** Restore device to inactive status and all settings including network and password.
- Restore to Inactive:** Leave all settings unchanged except restore device to inactive status without admin password.

Abbildung 16-19 Standardeinstellungen wiederherstellen

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

Standardeinstellungen wiederherstellen

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 den Rekorder in den inaktiven Zustand.

Hinwe

Der Rekorder wird neu ~~gestartet~~ automatisch nach Wiederherstellung der Einstellung

16.10 Sicherheitsmanagement

16.10.1 IP/MAC-Adressfilter

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

Schritte

1. Gehen Sie zu **Wartung** → **Systemdienst** → **Adressfilter**.

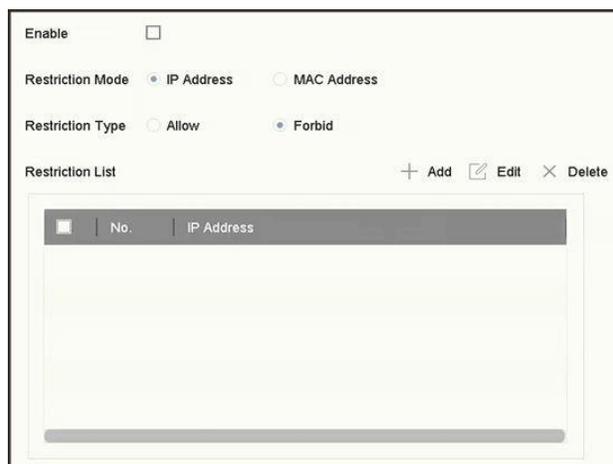


Abbildung 16-20 Adressfilter

2. **Aktivieren** Sie.

3. Wählen Sie den **Einschränkungsmodus**. Wählen Sie, ob Sie nach IP-Adresse oder MAC-Adresse filtern möchten.

-
4. Wählen Sie den **Einschränkungstyp**. Der Gerätemechanismus erlaubt oder verbietet bestimmten IP/MAC-Adressen den Zugang zu Ihrem Gerät.
 5. **Optional: Einschränkungsliste** festlegen. Sie können Adressen hinzufügen, bearbeiten oder löschen.
 6. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

16.10.2 RTSP-Authentifizierung

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

Schritte

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



Enable RTSP

RTSP Authentication Type

Abbildung 16-21 RTSP-Authentifizierung

2. Wählen Sie **RTSP-Authentifizierungstyp**.
-

Hinwe

Wenn Sie **Digest** auswählen, kann nur die Anfrage mit Digest-Authentifizierung über das RTSP-Protokoll über die IP-Adresse auf den Videostream zugreifen. Aus Sicherheitsgründen wird empfohlen, **digest** als Authentifizierungstyp auszuwählen.

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

16.10.3 RTSP-Verschlüsselungsalgorithmus

Der RTSP-Digest-Algorithmus basiert auf dem RTSP-Protokoll und ist ein Algorithmus für die Digest-Authentifizierung der Benutzerauthentifizierung. Sie können den RTSP-Digest-Algorithmus über den Webbrowser konfigurieren.

Gehen Sie zu **Konfiguration** → **System** → **Sicherheit** → **Authentifizierung** über Webbrowser, um den gewünschten RTSP-Digest-Algorithmustyp auszuwählen.

16.10.4 ISAPI-Dienst

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

Schritte

1. Gehen Sie zu **System → Systemdienst → Systemdienst**.
2. Aktivieren Sie **ISAPI aktivieren**.
3. Klicken Sie auf **Anwenden**.
4. Starten Sie das Gerät neu, damit die Einstellungen wirksam werden.

16.10.5 HTTP-Authentifizierung

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

Schritte

1. Gehen Sie zu **Wartung → Systemservice → Systemservice**.



Enable HTTP

HTTP Authentication Type

Abbildung 16-22 HTTP-Authentifizierung

2. Aktivieren Sie die Option **HTTP aktivieren**.
3. Wählen Sie **HTTP-Authentifizierungstyp**.

Hinwe

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

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

16.10.6 HTTP/Web Digest Algorithmus

Der HTTP/Web-Digest-Algorithmus basiert auf dem HTTP-Protokoll und ist ein Algorithmus für die Digest-Authentifizierung der Benutzerauthentifizierung. Sie können den HTTP/Web-Digest-Algorithmus über den Webbrowser konfigurieren.

Gehen Sie zu **Konfiguration → System → Sicherheit → Authentifizierung** über Webbrowser, um den gewünschten Digest-Algorithmus-Typ auszuwählen.

16.10.7 Bild-URL-Digest-Authentifizierung

Wenn Sie das HTTP-Protokoll zum Herunterladen von Bildern verwenden, die vom SDK hochgeladen wurden, können Sie mit der Bild-URL-Digest-Authentifizierung festlegen, ob für den Download von Bildern eine Digest-Authentifizierung erforderlich ist oder nicht. Sie können die Bild-URL-Digest-Authentifizierung über den Webbrowser konfigurieren.

Gehen Sie über den Webbrowser zu **Konfiguration → System → Sicherheit → Sicherheitsdienst**, um die Bild-URL-Digest-Authentifizierung zu aktivieren/deaktivieren.

16.10.8 Dienst zur Authentifizierung der seriellen Schnittstelle

Die serielle Schnittstelle kann zur Erfassung von Geräteinformationen und zur Steuerung des Geräts verwendet werden. Der Authentifizierungsdienst für den seriellen Anschluss bietet die Authentifizierung für die Nutzung des seriellen Anschlusses.

Gehen Sie über den Webbrowser zu **Konfiguration → System → Sicherheit → Sicherheitsdienst**, um den Authentifizierungsdienst für den seriellen Anschluss zu aktivieren/deaktivieren.

Dienstschlusszeit

Der Authentifizierungsdienst für den seriellen Anschluss wird für einen bestimmten Zeitraum geschlossen. Wenn z. B. "**Service Close Time**" auf **30** eingestellt ist, wird der Authentifizierungsdienst für den seriellen Anschluss für 30 Tage geschlossen. Nach 30 Tagen wird der Authentifizierungsdienst für den seriellen Anschluss wieder aktiviert.

17 Anhang

17.1 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.

17.2 Häufig gestellte Fragen

Warum wird bei einem Teil der Kanäle die Meldung "Keine Ressource" angezeigt oder der Bildschirm wird in der Mehrfachansicht der Live-Ansicht 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).

Hinwe

Wenn Ihr Videorekorder 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.

Warum meldet der Videorekorder, dass der Streamtyp nicht unterstützt wird?

Grund

Das Kodierungsformat der Kamera stimmt nicht mit dem des Videorekorders 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.

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

Grund

Das Passwort der Kamera ist zu schwach.

Lösung

Ändern Sie das Passwort der Kamera.

Warnung

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.

Wie lässt sich die Bildqualität bei der Wiedergabe verbessern?

Grund

Die Einstellungen der Aufnahmeparameter sind ungeeignet.

Lösung

Gehen Sie zu **Kamera → Videoparameter**. Erhöhen Sie die Auflösung und die maximale Bitrate, und versuchen Sie es erneut.

Wie kann ich sicherstellen, dass der Videorekorder H.265 für die Videoaufzeichnung verwendet?

Lösung

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

Warum ist die Zeitlinie bei der Wiedergabe nicht konstant?

Grund

1. Wenn der Videorekorder die Ereignisaufzeichnung verwendet, nimmt er nur Videos auf, wenn ein Ereignis eintritt. Daher kann das Video nicht kontinuierlich sein.
2. Eine Ausnahme tritt auf, z. B. wenn das Gerät offline ist, ein Festplattenfehler vorliegt, eine Aufzeichnungsausnahme vorliegt, die Netzwerkkamera offline ist usw.

Lösung

1. Vergewissern Sie sich, dass die Aufzeichnungsart auf Daueraufzeichnung eingestellt ist.
2. Gehen Sie zu **Wartung → Protokollinformationen**. Durchsuchen Sie die Protokolldatei während des Videozeitraums. Prüfen Sie, ob unerwartete Ereignisse wie Festplattenfehler, Aufzeichnungsausnahmen usw. aufgetreten sind.

Wenn Sie eine Netzwerkkamera hinzufügen, meldet der Videorekorder, dass das Netzwerk nicht erreichbar ist.

Grund

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

Lösung

1. Gehen Sie zu **Kamera → Kamera → IP-Kamera**. Klicken Sie auf  der ausgewählten Kamera und bearbeiten Sie ihre IP-Adresse und ihren Port. Vergewissern Sie sich, dass der Videorecorder und die Kamera denselben Port verwenden.

-
2. Gehen Sie zu **Wartung** → **Netzwerk** → **Erkennung**. Geben Sie die IP-Adresse der Netzwerkkamera unter **Zieladresse** ein, und klicken Sie auf **Testen**, um zu sehen, ob das Netzwerk erreichbar ist.

Warum wird die IP-Adresse der Netzwerkkamera automatisch geändert?

Grund

Wenn die Netzwerkkamera und der Videorecorder denselben Switch, aber ein anderes Subnetz verwenden, ändert der Videorecorder die IP-Adresse der Netzwerkkamera in dasselbe Subnetz wie er selbst.

Lösung

Wenn Sie eine Kamera hinzufügen, klicken Sie auf **Benutzerdefiniert hinzufügen**, um die Kamera hinzuzufügen.

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.

Warum bleibt das Bild bei der Wiedergabe von Ein- oder Mehrkanal-Kameras auf dem Videorecorder 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.

Warum gibt mein Videorecorder nach dem Hochfahren einen Piepton von sich?

Grund

1. Die Frontplatte ist nicht befestigt (bei Geräten, deren Frontplatte abnehmbar ist).

2. HDD-Fehler oder keine HDD.

Lösung

1. Wenn das Gerät kontinuierliche Pieptöne von sich gibt und die Frontblende abnehmbar ist, stellen Sie sicher, dass die Frontblende befestigt ist.
2. Wenn es nicht kontinuierlich piept (3 lange, 2 kurze), nehmen Sie den Festplattenfehler als Beispiel und prüfen Sie, ob das Gerät eine Festplatte installiert hat. Ist dies nicht der Fall, können Sie unter **System → Ereignis → Normales Ereignis → Ausnahme** das Kontrollkästchen **Ereignishinweiskonfiguration** deaktivieren, um den Ereignishinweis für Festplattenfehler zu deaktivieren.

Prüfen Sie, ob die Festplatte initialisiert ist. Wenn nicht, gehen Sie zu Speicher > Speichergerät, um die Festplatte zu initialisieren. Prüfen Sie, ob die Festplatte defekt ist. Sie können sie austauschen und erneut versuchen.

Warum gibt es nach der Einstellung der Bewegungserkennung keine Videoaufzeichnung?

Grund

1. Der Aufzeichnungsplan ist nicht korrekt.
2. Die Einstellung für das Bewegungserkennungsereignis ist falsch.
3. HDD-Ausnahme.

Lösung

1. Der Aufzeichnungszeitplan wird korrekt eingerichtet, indem Sie die unter Konfigurieren des Aufzeichnungs-/Aufnahmezeitplans aufgeführten Schritte ausführen.
2. Der Bewegungserkennungsbereich ist korrekt konfiguriert. Die Kanäle werden für die Bewegungserkennung ausgelöst (siehe Bewegungserkennung konfigurieren).
3. Prüfen Sie, ob das Gerät eine Festplatte installiert hat.
Prüfen Sie, ob die Festplatte initialisiert ist. Wenn nicht, gehen Sie zu Speicher > Speichergerät, um die Festplatte zu initialisieren. Prüfen Sie, ob die Festplatte defekt ist. Sie können sie austauschen und erneut versuchen.

Warum ist die Tonqualität bei Videoaufnahmen 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. Prüfen 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.

UG-GD-RN-AP8616P-2022-02-01-V5-DE ©ABETECHS GMBH, DÜSSELDORF, GERMANY

grundig-security.com

GRUNDIG