



Netzwerk-Kamera Web 5.0

Bedienungsanleitung







Vorwort

Allgemein

Dieses Benutzerhandbuch stellt die Funktionen, die Konfiguration, die allgemeine Bedienung und die Systemwartung der Netzwerkkamera vor.

Sicherheitshinweise

Die folgenden kategorisierten Signalwörter mit definierter Bedeutung können im Handbuch auftauchen.

Signalwörter	Bedeutung
 WARNUNG	Weist auf eine mittlere bis geringe Gefahr hin, die zu leichten oder mittelschweren Verletzungen führen kann, wenn sie nicht vermieden wird.
 VORSICHT	Weist auf eine potenziell gefährliche Situation hin, die, wenn sie nicht vermieden wird, zu Schäden am Gerät, Datenverlust, Leistungsminderung oder unerwarteten Ergebnissen führen kann.
 TIPPS	Bietet Methoden, die helfen können, ein Problem zu lösen oder Zeit zu sparen.
 HINWEIS	Bietet zusätzliche Informationen als Hervorhebung oder Ergänzung zum Text.

Änderungsverlauf

Version	Inhaltliche Überarbeitung	Veröffentlichungsdatum
V1.0.0	Erste Veröffentlichung.	Oktober 2020

Über das Handbuch

- Das Handbuch dient nur der Veranschaulichung. Bei Unstimmigkeiten zwischen Handbuch und dem jeweiligen Produkt hat das jeweilige Produkt Vorrang.
- Wir haften nicht für Verluste durch den Betrieb verursacht werden, der nicht den Anweisungen im Handbuch entspricht.
- Das Handbuch wird gemäß den neuesten Gesetzen und Vorschriften des jeweiligen Landes aktualisiert. Ausführliche Informationen finden Sie in der gedruckten Anleitung, auf der beiliegenden CD-ROM, über den QR-Code oder auf unserer offiziellen Website. Bei Widersprüchen zwischen dem gedruckten Handbuch und der elektronischen Version hat die elektronische Version Vorrang.
- Änderungen des Designs und der Software vorbehalten. Produktaktualisierungen können zu Abweichungen zwischen dem jeweiligen Produkt selbst und dem Handbuch führen. Wenden Sie sich für neueste Programm und zusätzliche Unterlagen und den Kundendienst.
- Es können immer noch Abweichungen in den technischen Daten, Funktionen und der Beschreibung der Inbetriebnahme oder Druckfehler vorhanden sein. Bei Unklarheiten oder Widersprüchen behalten wir uns das Recht einer endgültigen Erläuterung vor.

- Aktualisieren Sie die Reader-Software oder probieren Sie eine andere Mainstream-Readersoftware aus, wenn das Handbuch (im PDF-Format) nicht geöffnet werden kann.
- Alle eingetragenen Warenzeichen und Firmennamen im Handbuch sind Eigentum ihrer jeweiligen Besitzer.
- Wenn beim Einsatz des Geräts Probleme aufgetreten, besuchen Sie unsere Website oder wenden Sie sich an den Lieferanten bzw. Kundendienst.
- Bei Unklarheiten oder Widersprüchen behalten wir uns das Recht einer endgültigen Erläuterung vor.

Wichtige Sicherheits- und Warnhinweise

Elektrische Sicherheit

- Alle Installationen und der Betrieb müssen den örtlichen Vorschriften für elektrische Sicherheit entsprechen.
- Die Spannungsversorgung muss den Anforderungen von SELV (Sicherheitskleinspannung) und der Nennspannungsversorgung der Stromquelle mit begrenzter Leistung gemäß IEC60950-1 entsprechen. Beachten Sie, dass die Spannungsversorgung den Angaben auf dem Typenschild des Geräts entsprechen muss.
- Vergewissern Sie sich, dass die Stromversorgung korrekt ist, bevor Sie das Gerät in Betrieb nehmen.
- Eine leicht zugängliche Trennvorrichtung muss in die Verkabelung der Gebäudeinstallation integriert werden.
- Achten Sie darauf, dass niemand auf das Netzkabel treten kann und es nicht eingeklemmt wird, insbesondere am Stecker und am Austritt aus dem Gerät.

Umgebung

- Richten Sie das Gerät nicht auf starke Lichtquellen, wie beispielsweise Lampen oder Sonnenlicht. Andernfalls kann es zu Überbelichtung oder hellen Flecken kommen, die keine Fehlfunktion des Gerätes darstellen und die sich auf die Lebensdauer des CMOS auswirken können.
- Installieren Sie das Gerät nicht in einer feuchten, staubigen, extrem heißen oder kalten Umgebung oder an Orten mit starker elektromagnetischer Strahlung oder instabiler Beleuchtung.
- Schützen Sie das Gerät vor jeglichen Flüssigkeiten, um Schäden an den internen Komponenten zu vermeiden.
- Schützen Sie Geräte zur Innenmontage vor Regen oder Feuchtigkeit, um Schäden durch Feuer oder Blitzeinschlag zu vermeiden.
- Achten Sie auf gute Belüftung, um Wärmestau zu vermeiden.
- Transportieren, verwenden und lagern Sie das Gerät innerhalb der zulässigen Grenzwerte für Luftfeuchtigkeit und Temperatur.
- Während des Transports, der Lagerung und Installation sind starke Belastungen, heftige Erschütterungen und Feuchtigkeit zu vermeiden.
- Verpacken Sie das Gerät während des Transports mit der werksseitigen Standardverpackung oder gleichwertigem Material.
- Montieren Sie das Gerät an einer Stelle, zu der nur Fachpersonal mit einschlägigen Kenntnissen über die Schutzvorrichtungen und Warnhinweise Zugang hat. Bei Laien kann es zu unbeabsichtigten Verletzungen kommen, wenn diese den Montageort bei normalem Betrieb des Geräts betreten.

Betrieb und tägliche Wartung

- Berühren Sie nicht die Komponenten des Geräts zur Wärmeableitung, um Verbrennungen zu vermeiden.
- Befolgen Sie bei einem Auseinanderbauen sorgfältig die Anweisungen im Handbuch des Geräts. Andernfalls kann es zu Wassereintritt oder zu schlechter Bildqualität durch

unprofessionelles Auseinanderbauen kommen. Wenn sich nach dem Auspacken Kondenswasser auf dem Objektiv befindet oder wenn sich das Trockenmittel grün verfärbt hat, wenden Sie sich zum Austausch des Trockenmittels an die Kundendienstabteilung. (Ein Trockenmittel wurde nicht bei allen Modellen beigelegt).

- Zur Verbesserung des Blitzschutzes empfehlen wir, das Gerät mit einem Blitzableiter zu verwenden.
- Es wird empfohlen, um das Gerät zu Erden, um die Zuverlässigkeit zu verbessern.
- Den Bildsensor (CMOS) nicht direkt mit den Fingern berühren. Staub und Schmutz können mit einem Luftgebläse entfernt werden oder Sie können das Objektiv mit einem weichen Tuch, das mit Alkohol angefeuchtet wurde, vorsichtig abwischen.
- Sie können das Gerätegehäuse mit einem weichen, trockenen Tuch reinigen; bei hartnäckigen Flecken verwenden Sie das Tuch mit einem milden Reinigungsmittel. Um mögliche Schäden an der Beschichtung des Gerätegehäuses zu vermeiden, die zu Leistungsabfall führen können, verwenden Sie weder flüchtige Lösungsmittel wie Alkohol, Benzin, Verdünner usw. zur Reinigung des Gerätegehäuses, noch starke, scheuernde Reinigungsmittel.
- Die Kuppelabdeckung ist eine optische Komponente. Berühren Sie die Abdeckung während der Installation oder des Betriebs nicht direkt mit den Händen und wischen Sie nicht darüber. Zum Entfernen von Staub, Fett oder Fingerabdrücken vorsichtig mit einem mit Alkohol angefeuchteten und fettfreien Baumwolltuch oder einem angefeuchteten weichen Tuch sauber wischen. Sie können Staub auch mit einem Luftgebläse entfernen.

**WARNUNG**

- Verstärken Sie den Schutz des Netzwerks, der Gerätedaten und der personenbezogenen Daten unter anderem durch die Verwendung eines sicheren Passworts, regelmäßige Änderung des Passworts, Aktualisieren der Firmware auf die neueste Version und Verwehren des Zugriffs auf das Computer-Netzwerk. Bei einigen Geräten mit alten Firmware-Versionen wird das ONVIF-Passwort nicht automatisch mit der Änderung des System-Passworts geändert und Sie müssen die Firmware oder das ONVIF-Passwort manuell aktualisieren.
- Verwenden Sie Standardkomponenten oder vom Hersteller geliefertes Zubehör und achten Sie darauf, dass das Gerät von professionellen Errichtern installiert und gewartet wird.
- Die Oberfläche des Bildsensors darf nicht Laserstrahlung ausgesetzt werden.
- Schließen Sie nicht zwei oder mehrere Stromquellen an das Gerät an, außer es wurde etwas anders angegeben. Eine Nichtbeachtung dieser Anweisung kann zu Schäden am Gerät führen.

Inhaltsverzeichnis

Vorwort	I
Wichtige Sicherheits- und Warnhinweise.....	III
1 Überblick	1
1.1 Beschreibung	1
1.2 Netzwerkverbindung	1
1.3 Konfigurationsablauf	1
2 Initialisierung des Geräts	3
3 Anmelden	7
3.1 Anmeldung am Gerät	7
3.2 Passwort zurücksetzen	8
4 Live	10
4.1 Live-Menü.....	10
4.2 Kodierung einstellen.....	11
5 Einstellungen.....	12
5.1 Netzwerk.....	12
5.1.1 TCP/IP.....	12
5.1.2 Port	15
5.1.3 E-Mail.....	17
5.1.4 Grundlegende Dienste.....	19
5.2 Ereignis	20
5.2.1 Alarmeingang einstellen	21
5.2.2 Alarmverknüpfung einstellen	22
5.2.2.1 Zeitplan hinzufügen	23
5.2.2.2 Verknüpfung aufnehmen	24
5.2.2.3 Fotoverknüpfung	25
5.2.2.4 Alarmausgangsverknüpfung.....	25
5.2.2.5 E-Mail-Verknüpfung.....	26
5.3 System.....	26
5.3.1 Allgemein	26
5.3.1.1 Allgemein	26
5.3.1.2 Datum und Zeit.....	27
5.3.2 Konto	28
5.3.2.1 Benutzer	28
5.3.2.1.1 Benutzer hinzufügen	28
5.3.2.1.2 Passwort zurücksetzen	32
5.3.2.2 ONVIF-Benutzer	32
5.3.3 Manager.....	33

5.3.3.1 Anforderungen	33
5.3.3.2 Wartung.....	34
5.3.3.3 Importieren/Exportieren	35
5.3.3.4 Rücksetzung zu den Werkseinstellungen.....	35
5.3.4 Aktualisieren.....	36
Anhang 1 Empfehlungen zur Cybersicherheit.....	37

1 Überblick

1.1 Beschreibung

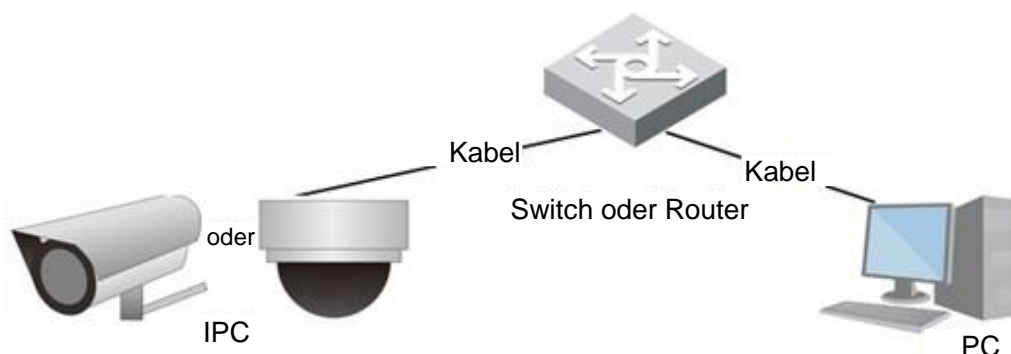
Eine IP-Kamera (Internet-Protokoll-Kamera) ist eine digitale Videokamera, die Steuerdaten empfängt und Bilddaten über das Internet sendet. Diese Kameras werden häufig zur Überwachung eingesetzt und erfordern kein lokales Aufnahmegerät, sondern nur ein lokales Netzwerk.

IP-Kameras werden entsprechend der Kanalanzahl in Einkanal- und Mehrkanal-Kameras unterteilt. Bei Mehrkanal-Kameras können Sie die Parameter für jeden Kanal einstellen.

1.2 Netzwerkverbindung

In der allgemeinen IPC-Netzwerktopologie ist die IPC über einen Netzwerk-Switch oder Router mit dem PC verbunden.

Abbildung 1–1 Generelles IPC-Netzwerk



Erhalten Sie die IP-Adresse, indem Sie im Konfigurations-Tool suchen, dann können Sie mit dem Zugriff auf die IP-Kamera über das Netzwerk beginnen.

1.3 Konfigurationsablauf

Hinweise zum Gerätekonfigurationsablauf, siehe Abbildung 1–2. Details siehe Tabelle 1–1. Konfigurieren Sie das Gerät entsprechend der aktuellen Situation.

Abbildung 1–2 Konfigurationsablauf

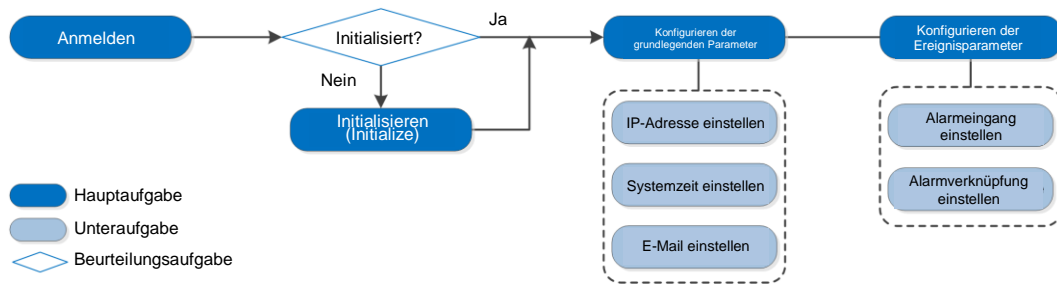


Tabelle 1–1 Beschreibung des Ablaufs

Konfiguration		Beschreibung	Referenz
Anmelden		Öffnen Sie den IE-Browser und geben Sie die IP-Adresse ein, um sich bei der Web-Oberfläche anzumelden. Die Kamera-IP-Adresse lautet standardmäßig 192.168.1.108.	„3 Anmelden“.
Initialisierung		Initialisieren Sie die Kamera, wenn Sie sie das erste Mal verwenden.	„2 Initialisierung des Geräts“
Grundlegende Parameter	IP-Adresse	Ändern Sie die IP-Adresse bei der ersten Verwendung oder während der Netzwerkanpassung entsprechend der Netzwerkplanung.	„5.1.1 TCP/IP“
	Datum und Zeit	Stellen Sie Datum und Uhrzeit ein, um zu gewährleisten, dass die Aufnahmezeit korrekt ist.	„5.3.1.2 Datum und Zeit“

2 Initialisierung des Geräts

Für die erstmalige Verwendung ist eine Geräteinitialisierung erforderlich. Dieses Handbuch basiert auf dem Betrieb über die Weboberfläche. Sie können das Gerät auch über Konfigurations-Tool oder NVR initialisieren.



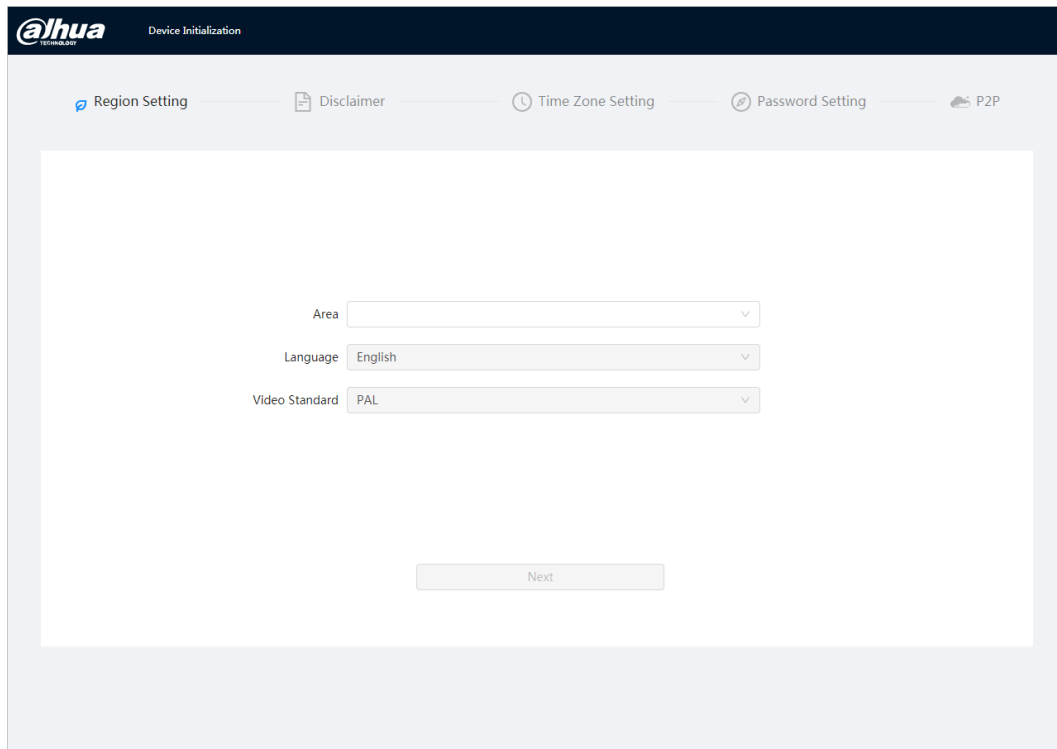
- Um die Sicherheit des Geräts zu gewährleisten, bewahren Sie das Passwort nach der Initialisierung ordnungsgemäß auf und ändern Sie es regelmäßig.
- Halten Sie bei der Initialisierung des Geräts die PC-IP und die Geräte-IP im selben Netzwerk.

Schritt 1: Öffnen Sie den Chrome-Browser, geben Sie die IP-Adresse des Geräts in die Adressleiste ein und drücken Sie dann die Eingabetaste.



Die IP lautet standardmäßig 192.168.1.108.

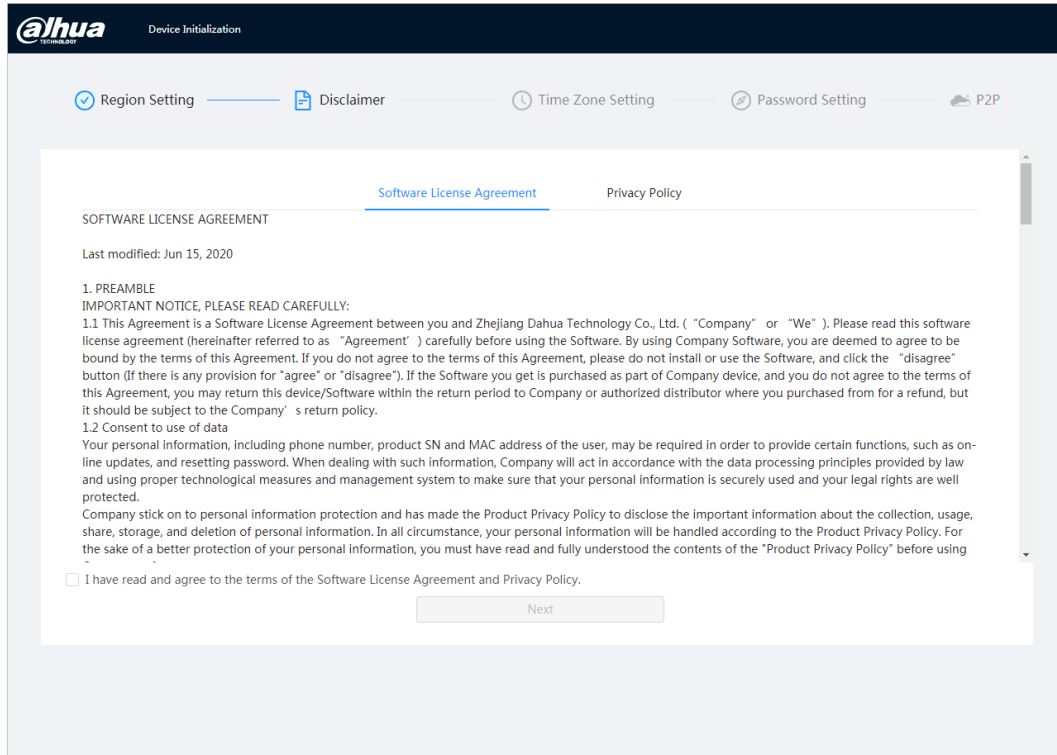
Abbildung 2–1 Regionseinstellung



The screenshot shows the 'Device Initialization' web interface. At the top, there is a progress bar with five steps: 'Region Setting' (active), 'Disclaimer', 'Time Zone Setting', 'Password Setting', and 'P2P'. Below the progress bar, there are three dropdown menus for configuration: 'Area' (empty), 'Language' (set to 'English'), and 'Video Standard' (set to 'PAL'). At the bottom of the configuration area, there is a 'Next' button.

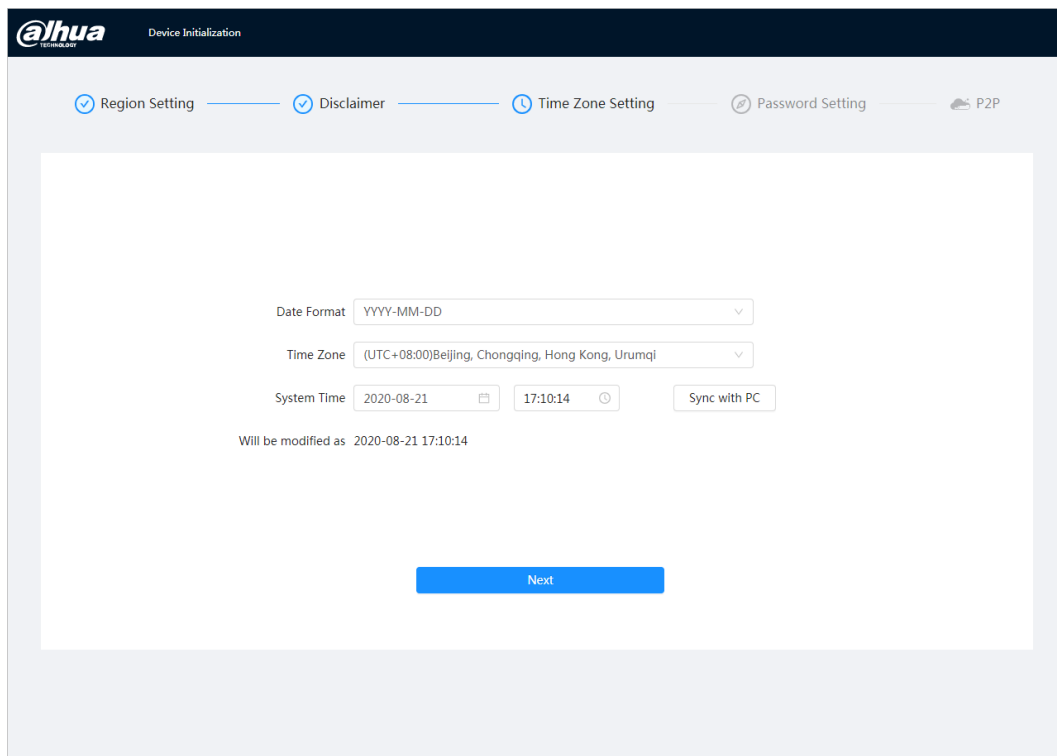
Schritt 2: Wählen Sie den Bereich, die Sprache und den Videostandard entsprechend der aktuellen Situation und klicken Sie dann auf **Weiter** (Next).

Abbildung 2–2 Haftungsausschluss



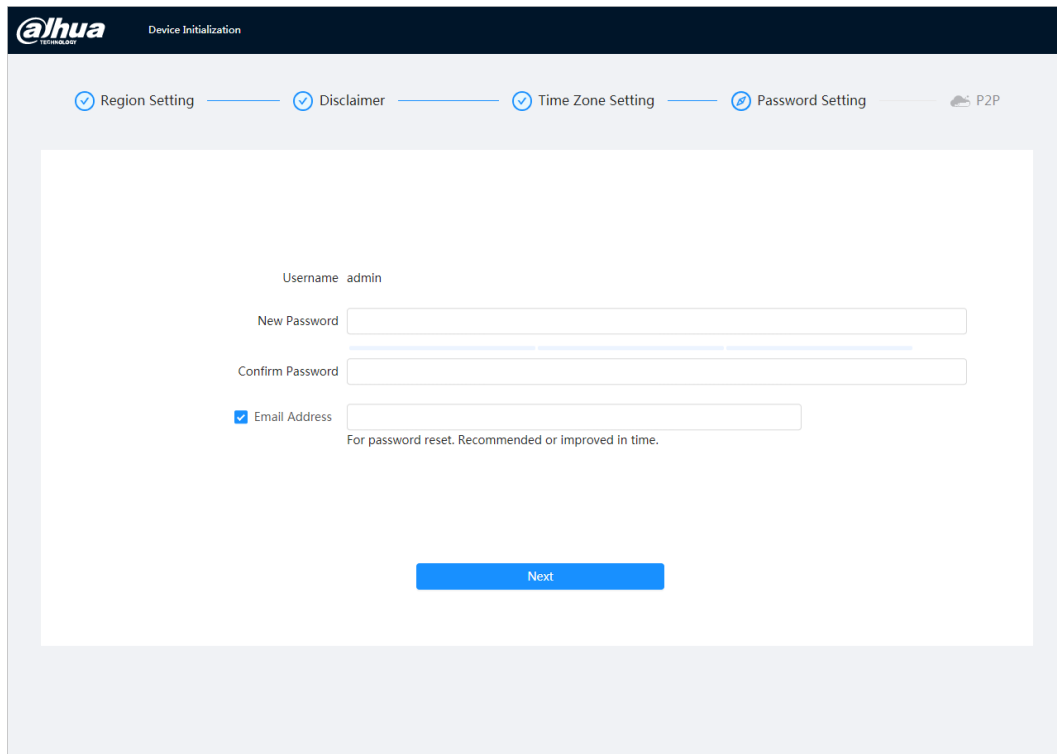
Schritt 3: Markieren Sie das Kontrollkästchen **Ich habe die Bedingungen der Software-Lizenzvereinbarung und der Datenschutzerklärung gelesen und akzeptiere sie** (I have read and agree to the terms of the Software License Agreement and Privacy Policy). Klicken Sie dann auf **Weiter** (Next).

Abbildung 2–3 Zeitzoneneinstellung



Schritt 4: Konfigurieren Sie die Zeitparameter und klicken Sie dann auf **Weiter** (Next).

Abbildung 2–4 Passwordeinstellung



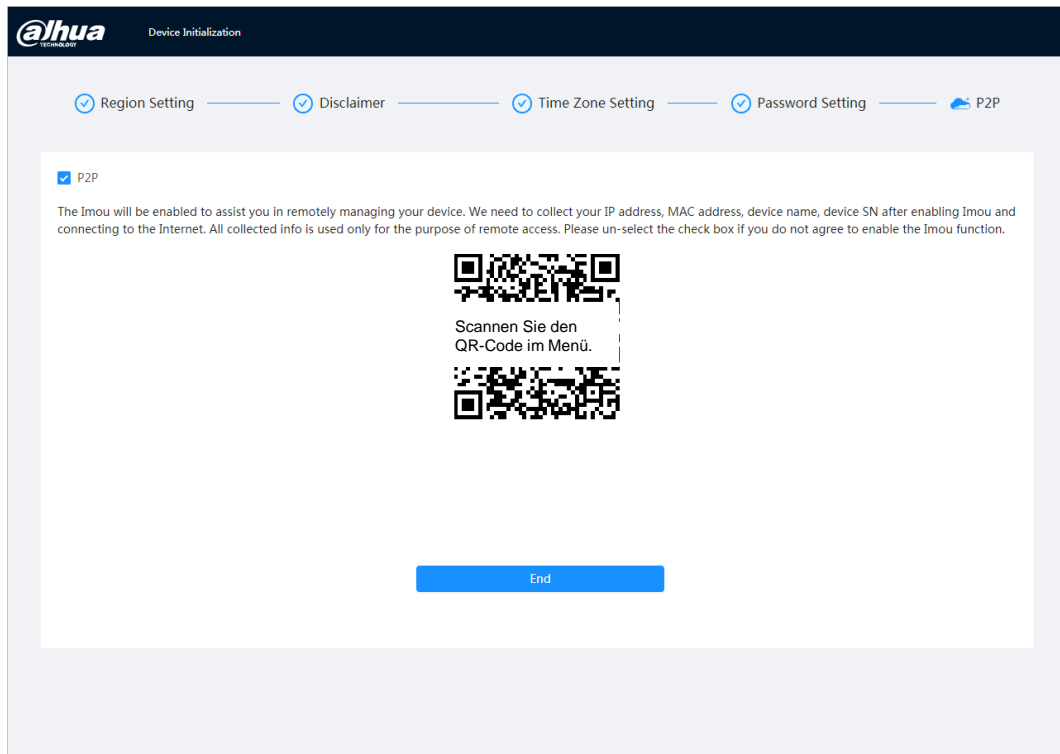
Schritt 5: Stellen Sie das Passwort für das Administratorkonto ein.

Tabelle 2–1 Beschreibung der Passwort-Konfiguration

Parameter	Beschreibung
Benutzername	Der standardmäßige Benutzername lautet admin.
Passwort	Das Passwort muss aus 8 bis 32 nicht leeren Zeichen bestehen und mindestens zwei Arten von Zeichen von Groß- und Kleinschreibung, Ziffer und Sonderzeichen enthalten (außer ' " ; : &). Stellen Sie ein Passwort mit hoher Sicherheitsstufe entsprechend dem Sicherheitshinweis zum Passwort ein.
Passwort bestätigen	
Reservierte E-Mail	Geben Sie eine E-Mail-Adresse zum Zurücksetzen des Passworts ein, sie ist standardmäßig ausgewählt. Wenn Sie das Passwort des Admin-Kontos zurücksetzen müssen, wird ein Sicherheitscode für die Passwortrücksetzung an die reservierte E-Mail-Adresse gesendet.

Schritt 6: Klicken Sie auf **Weiter** (Next). Anschließend wird die **P2P**-Oberfläche angezeigt.

Abbildung 2–5 P2P



3 Anmelden

3.1 Anmeldung am Gerät

In diesem Abschnitt wird erläutert, wie Sie sich an der Weboberfläche an- und abmelden können. In diesem Abschnitt wird Chrome als Beispiel verwendet.



- Sie müssen die Kamera initialisieren, bevor Sie sich bei der Web-Oberfläche anmelden. Einzelheiten siehe „2 Initialisierung des Geräts“.
- Halten Sie bei der Initialisierung der Kamera die PC-IP und die Geräte-IP im gleichen Netzwerk.
- Folgen Sie den Anleitungen zum Herunterladen und Installieren des Plug-ins für die erste Anmeldung.

Schritt 1: Öffnen Sie den Chrome-Browser, geben Sie die IP-Adresse der Kamera (standardmäßig 192.168.1.108) in die Adressleiste ein und drücken Sie die Eingabetaste.

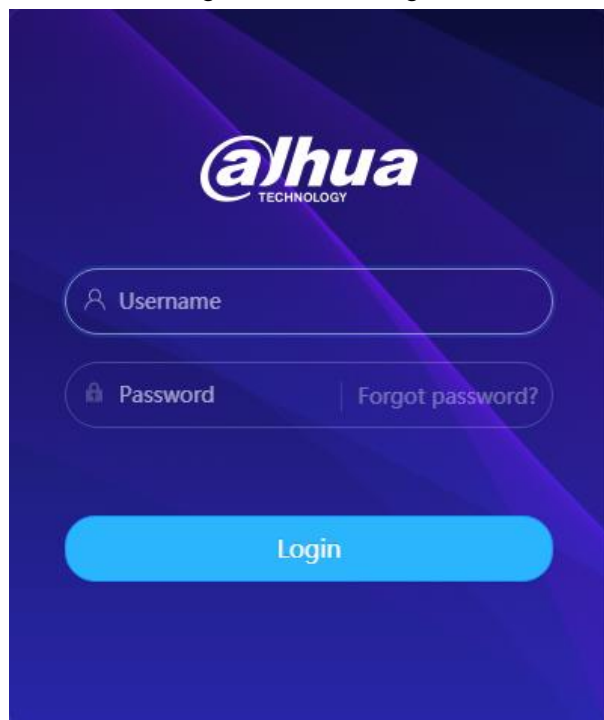
Schritt 2: Geben Sie den Benutzernamen und das Passwort ein.

Der Benutzername ist standardmäßig admin.



Klicken Sie auf **Passwort vergessen?** (Forgot password?), damit können Sie das Passwort über die E-Mail-Adresse zurücksetzen, die bei der Initialisierung festgelegt wurde. Einzelheiten siehe „3.2 Passwort zurücksetzen“.

Abbildung 3–1 Anmeldung



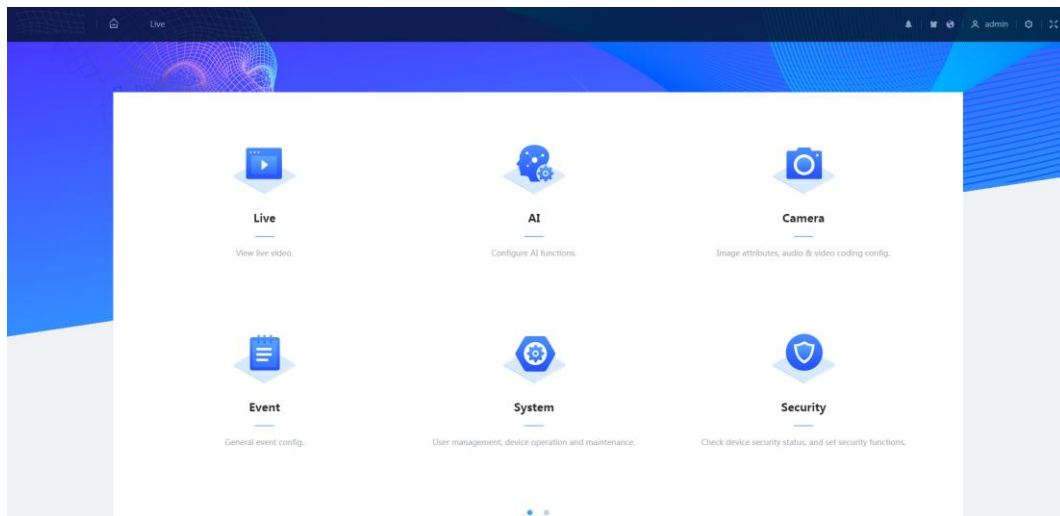
Schritt 3: Klicken Sie auf **Anmelden** (Login).

Das Fenster **Live** wird angezeigt. Klicken Sie auf  in der linken oberen Ecke des Fensters, um das Hauptfenster anzuzeigen.



Installieren Sie bei der erstmaligen Anmeldung das Plug-In gemäß den Bildschirmmanweisungen.

Abbildung 3–2 Hauptfenster




- Live: Anzeige des Echtzeit-Überwachungsbildes.
- KI: Konfiguration der Kameraparameter.
- Kamera: Konfiguration der Kameraparameter, einschließlich Bild-, Encoder- und Audio-Parameter.
- Ereignis: Konfiguration der generellen Ereignisse, einschließlich Alarmverknüpfungsausnahme, Video- und Audioerkennung.
- System: Konfiguration der Systemparameter, einschließlich Generell, Datum und Uhrzeit, Konto, Sicherheit, PTZ-Einstellungen, Standard, Importieren/Exportieren, Fernwartung, automatische Wartung und Upgrade.
- Sicherheit: Überprüfung des Gerätesicherheitsstatus und Einstellen der Sicherheitsfunktionen.
- Aufnahme: Aufgenommene Videos wiedergeben oder herunterladen.
- Bild: Bilddateien wiedergeben oder herunterladen.
- Bericht: KI-Ereignis- und Systembericht suchen.

3.2 Passwort zurücksetzen

Wenn Sie das Passwort für das Admin-Konto zurücksetzen müssen, wird an die eingegebene E-Mail-Adresse ein Sicherheitscode gesendet, mit dem Sie das Passwort zurücksetzen können.

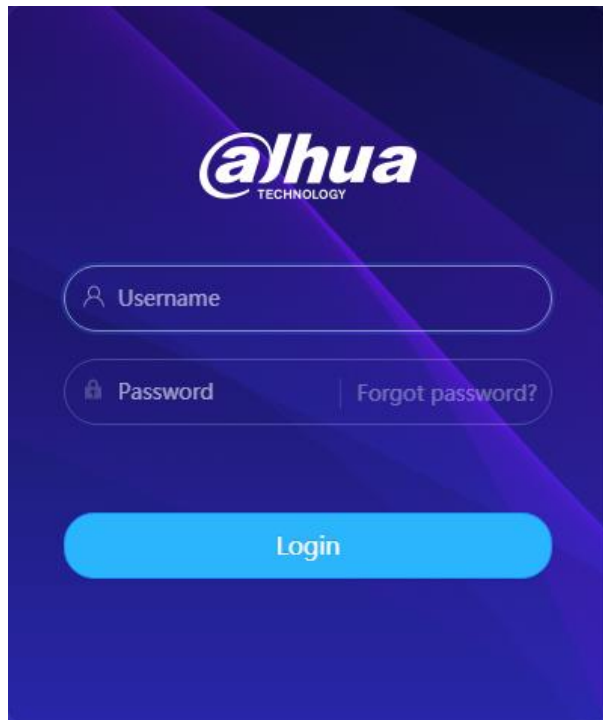
Voraussetzungen

Sie haben den Dienst zum Zurücksetzen des Passworts unter  > **System** > **Konto** (Account) > **Benutzer** (User) aktiviert.

Vorgehensweise

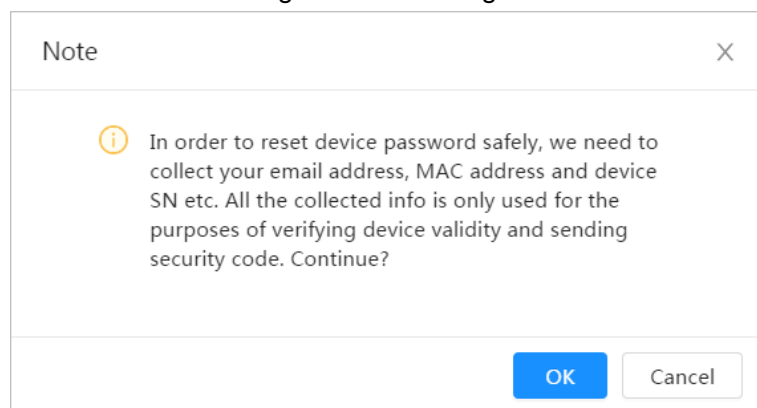
Schritt 1: Öffnen Sie den Chrome-Browser, geben Sie die IP-Adresse des Geräts in die Adressleiste ein und drücken Sie die Eingabetaste.

Abbildung 3–3 Anmeldung



Schritt 2: Klicken Sie auf **Passwort vergessen?** (Forgot password?), damit können Sie das Passwort über die E-Mail-Adresse zurücksetzen, die bei der Initialisierung festgelegt wurde.

Abbildung 3–4 Anmeldung



4 Live

In diesem Abschnitt werden das Layout des Menüs und die Funktionskonfiguration vorgestellt.

4.1 Live-Menü

Melden Sie sich an oder klicken Sie auf die Registerkarte **Live**.



Das Fenster kann sich bei verschiedenen Modellen unterscheiden und das tatsächliche Fenster ist maßgebend.

Abbildung 4–1 Live (einkanalig)

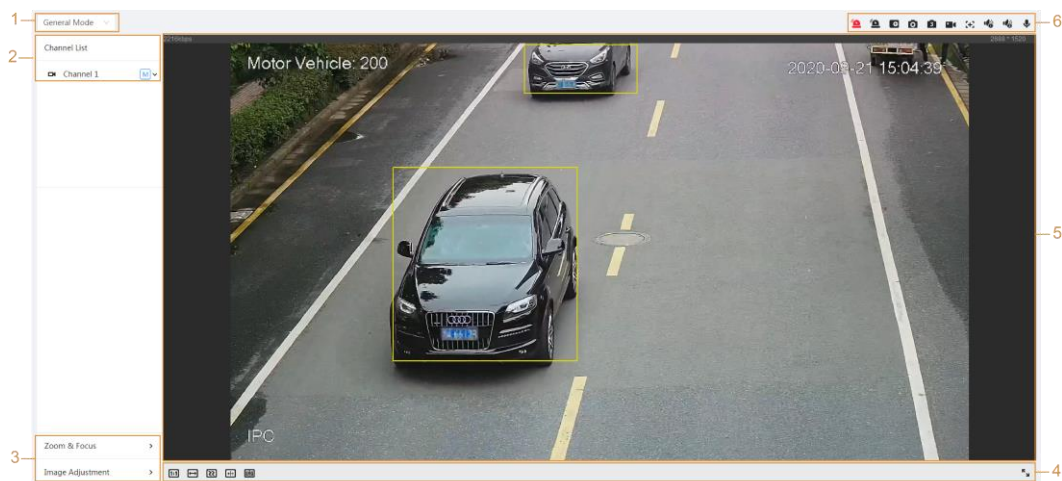


Abbildung 4–2 Live (mehrkanalig)

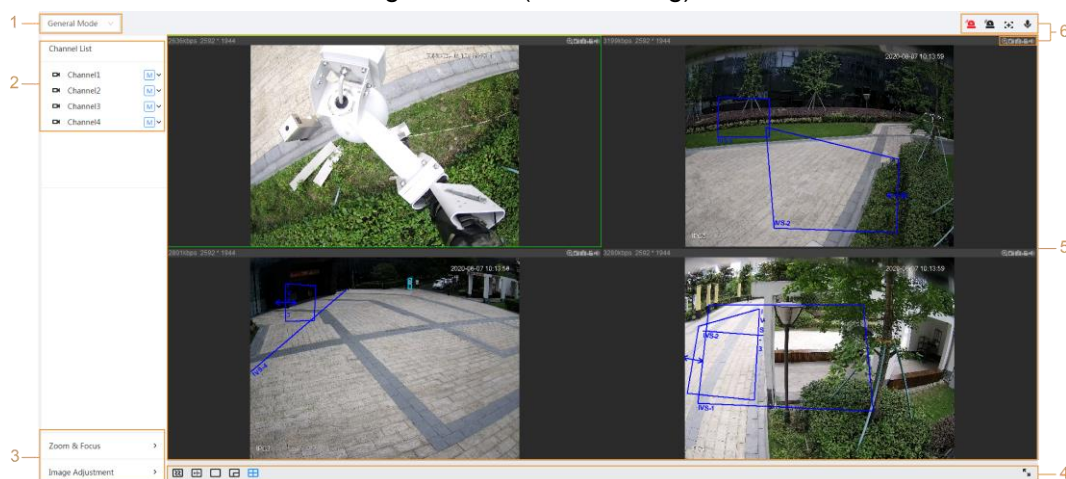


Tabelle 4–1 Beschreibung der Funktionsleiste

Nr.	Funktion	Beschreibung
1	Anzeigemodus	Sie können den Anzeigemodus zwischen Genereller Modus (General Mode) und Gesichtsmodus (Face Mode) auswählen.

Nr.	Funktion	Beschreibung
2	Kanalliste	Zeigt alle Kanäle an. Sie können den Kanal nach Bedarf auswählen und den Streamtyp festlegen.
3	Bildeinstellung	Einstellvorgänge in der Live-Ansicht.
4		
5	Live-Ansicht	Zeigt das Echtzeit-Überwachungsbild an.
6	Funktionsleiste der Live-Ansicht	Funktionen und Operationen in der Live-Ansicht.

4.2 Kodierung einstellen


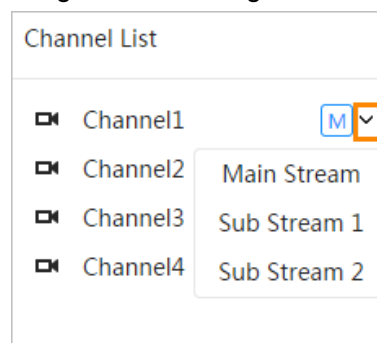



Klicken Sie auf  und wählen Sie dann den Stream nach Bedarf aus.

Abbildung 4–3 Kodierungsleiste



- **Haupt-Stream:** Es hat einen hohen Bitstreamwert und ein Bild mit hoher Auflösung, benötigt aber auch eine große Bandbreite. Diese Option kann zur Speicherung und Überwachung verwendet werden.
- **Sub-Stream:** Hat einen kleinen Bitstreamwert und ein flüssiges Bild und benötigt weniger Bandbreite. Diese Option wird normalerweise verwendet, um den Haupt-Stream zu ersetzen, wenn die Bandbreite nicht ausreicht.
-  bedeutet, dass der aktuelle Stream der Hauptstream ist;  bedeutet, dass der aktuelle Stream der Unterstream 1 ist;  bedeutet, dass der aktuelle Stream der Unterstream 2 ist.

5 Einstellungen

In diesem Abschnitt wird die Grundeinstellung der Kamera beschrieben, einschließlich der Konfiguration von Netzwerk, Ereignis und System.

5.1 Netzwerk

In diesem Abschnitt wird die Netzwerkkonfiguration vorgestellt.

5.1.1 TCP/IP

Sie können IP-Adresse und DNS-Server (Domain Name System) usw. entsprechend der Netzwerkplanung konfigurieren.

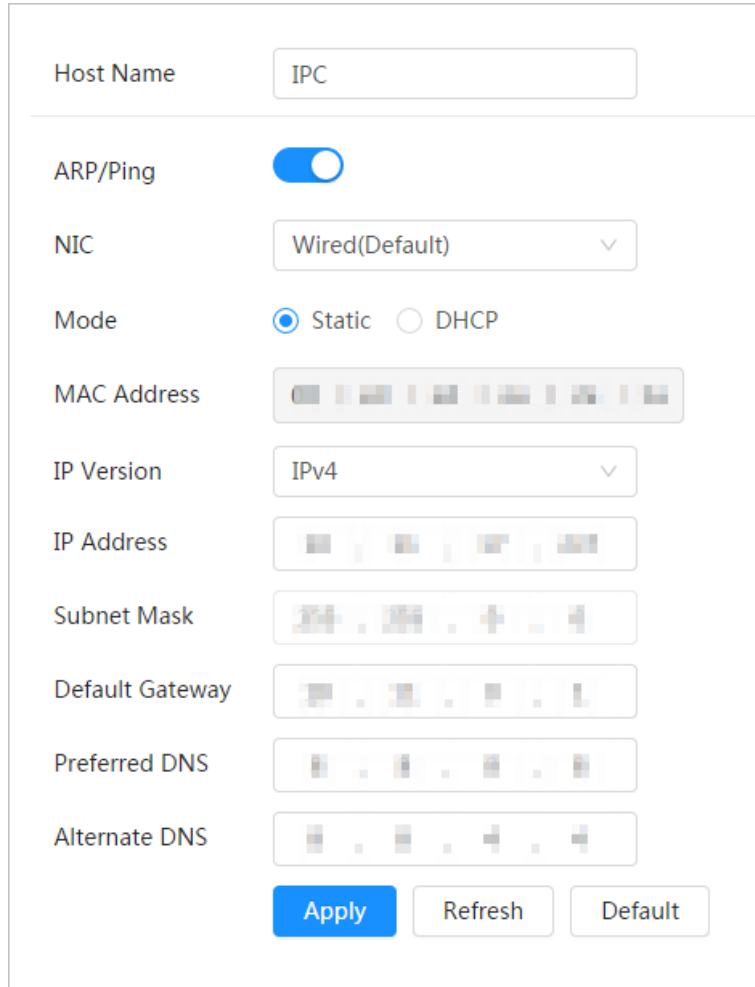
Voraussetzungen

Die Kamera ist mit dem Netzwerk verbunden.

Vorgehensweise

Schritt 1: Wählen Sie  > **Netzwerk** (Network)> **TCP/IP**.


Abbildung 5–1 TCP/IP




Schritt 2: Konfigurieren Sie die TCP/IP-Parameter.

Tabelle 5–1 Beschreibung der TCP/IP-Parameter

Parameter	Beschreibung
Host-Name	Geben Sie den Hostnamen ein. Die maximale Länge beträgt 15 Zeichen.

Parameter	Beschreibung
ARP/Ping	<p>Klicken Sie auf , um ARP/Ping zu aktivieren und den IP Adressdienst einzustellen. Rufen Sie die MAC-Adresse der Kamera ab und dann können Sie die Geräte-IP-Adresse mit dem Befehl ARP/Ping ändern und konfigurieren.</p> <p>Dies ist standardmäßig aktiviert. Während des Neustarts haben Sie nicht mehr als 2 Minuten Zeit, um die Geräte-IP-Adresse durch ein Ping-Paket mit einer bestimmten Länge zu konfigurieren. Der Server wird nach 2 Minuten abgeschaltet oder er wird sofort abgeschaltet, nachdem die IP-Adresse erfolgreich konfiguriert wurde. Wenn dies nicht aktiviert ist, kann die IP-Adresse nicht mit Ping-Paket konfiguriert werden.</p> <p>Beispiel für die Konfiguration der IP-Adresse mit ARP/Ping.</p> <ol style="list-style-type: none"> Halten Sie die zu konfigurierende Kamera und den PC im gleichen lokalen Netzwerk und beziehen Sie eine nutzbare IP-Adresse. Erhalten Sie die MAC-Adresse der Kamera vom Geräte-Label. Öffnen Sie den Befehlseditor auf dem PC und geben Sie folgenden Befehl ein. <div data-bbox="676 938 1351 1505" style="border: 1px solid black; padding: 5px;"> <pre>Windows syntax arp -s <IP Address> <MAC> ping -l 480 -t <IP Address> Windows example arp -s 192.168.0.125 11-40-8c-18-10-11 ping -l 480 -t 192.168.0.125 UNIX/Linux/Mac syntax arp -s <IP Address> <MAC> ping -s 480 <IP Address> UNIX/Linux/Mac example arp -s 192.168.0.125 11-40-8c-18-10-11 ping -s 480 192.168.0.125</pre> </div> <ol style="list-style-type: none"> Starten Sie die Kamera neu. Überprüfen Sie die PC-Befehlszeile, ob Informationen wie Antwort von 192.168.0.125... (Reply from 192.168.0.125...) angezeigt werden. Die Konfiguration ist erfolgreich und Sie können den PC abschalten. Geben Sie zum Anmelden in der Adresszeile des Browsers http://(IP-Adresse) ein.
Netzwerkkarte	Wählen Sie die Ethernet-Karte, die konfiguriert werden soll. Die Standardeinstellung ist Kabelgebunden (Wired).

Parameter	Beschreibung
Modus	<p>Modus, in dem die Kamera die IP erhält:</p> <ul style="list-style-type: none"> Statisch Konfigurieren Sie IP-Adresse (IP Address), Subnetzmaske (Subnet Mask) und Standard-Gateway (Default Gateway) manuell und klicken Sie auf Speichern (Save), damit wird das Anmeldenmenü mit der konfigurierten IP-Adresse angezeigt. DHCP Wenn sich ein DHCP-Server im Netzwerk befindet, wählen Sie DHCP, damit bezieht die Kamera die IP-Adresse automatisch.
MAC-Adresse	Zeigt die Host-MAC-Adresse an.
IP-Version	Wählen Sie IPv4 oder IPv6 .
IP-Adresse	Bei Auswahl von Statisch (Static) in Modus (Mode) geben Sie die IP-Adresse und Subnetzmaske ein, die Sie benötigen.
Subnetzmaske	
Standardgateway	
	 <ul style="list-style-type: none"> IPv6 hat keine Subnetzmaske. Das Standard-Gateway muss sich im gleichen Netzwerksegment wie die IP-Adresse befinden.
Bevorzugtes DNS	IP-Adresse des bevorzugten DNS.
Alternatives DNS	IP-Adresse des alternativen DNS.

Schritt 3: Klicken Sie auf **Anwenden** (Apply).

5.1.2Port

Konfigurieren Sie die Portnummern und die maximale Anzahl der Benutzer (einschließlich Web-, Plattform- und Mobiltelefon-Client), die sich gleichzeitig mit dem Gerät verbinden dürfen.

Schritt 1: Wählen Sie  > **Netzwerk** (Network)> **TCP/IP**.

Abbildung 5–2 Port

Max Connection	<input type="text" value="10"/>	(1-20)
TCP Port	<input type="text" value="37777"/>	(1025-65534)
UDP Port	<input type="text" value="37778"/>	(1025-65534)
HTTP Port	<input type="text" value="80"/>	
RTSP Port	<input type="text" value="554"/>	
RTMP Port	<input type="text" value="1935"/>	(1025-65534)
HTTPS Port	<input type="text" value="443"/>	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		

Schritt 2: Konfigurieren Sie die Port-Parameter.



- 0 - 1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780 - 37880, 39999 und 42323 sind für spezifische Anwendungen belegt.
- Verwenden Sie während der Port-Konfiguration nicht den gleichen Wert eines anderen Ports.

Tabelle 5–2 Beschreibung der Port-Parameter

Parameter	Beschreibung
Höchstzahl der Verbindungen	Höchstzahl von Benutzern (Web-, Plattform- oder Mobiltelefon-Client), die sich gleichzeitig mit dem Gerät verbinden können. Der Wert ist standardmäßig 10.
TCP-Port	Transmission Control Protocol-Port. Der Wert ist standardmäßig 37777.
UDP-Port	Port für das Protokoll des Benutzerdatagramms. Der Wert ist standardmäßig 37778.
HTTP-Port	Hypertextübertragungsprotokollport. Der Wert ist standardmäßig 80.

Parameter	Beschreibung
RTSP-Port	<ul style="list-style-type: none"> Echtzeit-Streaming-Protokollport, der Wert ist standardmäßig 554. Wenn Sie die Live-Ansicht mit QuickTime, VLC oder Blackberry Smartphone abspielen, steht Ihnen das folgende URL-Format zur Verfügung. Wenn das URL-Format RTSP erfordert, müssen Sie in der URL Kanalnummer und Bitstreamtyp sowie ggf. Benutzername und Passwort angeben. <p>Beispiel für ein URL-Format: <code>rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</code> Hierbei ist:</p> <ul style="list-style-type: none"> Benutzername: Der Benutzername, z. B. admin. Passwort: Das Passwort, z.B. admin. IP: Die Geräte-IP, z.B. 192.168.1.112. Port: Belassen, wenn der Wert standardmäßig 554 ist. Kanal: Kanalnummer, beginnend mit 1. Wenn Sie beispielsweise Kanal 2 verwenden, dann ist der Kanal (channel) = 2. subtype: Der Bitstreamtyp; 0 bedeutet Haupt-Stream (Subtyp=0) und 1 bedeutet Sub-Stream (Subtyp=1). <p>Beispiel: Wenn Sie den Sub-Stream von Kanal 2 von einem bestimmten Gerät benötigen, dann muss die URL lauten: <code>rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=21&=1</code> Wenn Benutzername und Passwort nicht erforderlich sind, dann ist die URL folgende: <code>rtsp://ip:port/cam/realmonitor?channel=11&=0</code></p>
RTMP-Port	Echtzeit-Messaging-Protokollport. Der Port, den RTMP als Dienst bereitstellt. Standardmäßig ist es 1935.
HTTPS-Port	HTTPS-Kommunikationsport. Standardmäßig ist es 443.

Schritt 3: Klicken Sie auf **Anwenden** (Apply).



Die Konfiguration von **Höchstzahl der Verbindungen** (Max Connection) wird sofort wirksam, andere werden nach dem Neustart wirksam.

5.1.3E-Mail

Konfigurieren Sie die E-Mail-Parameter und aktivieren Sie die E-Mail-Verknüpfung. Das System sendet eine E-Mail an die angegebene Adresse, wenn der entsprechende Alarm ausgelöst wird.

Schritt 1: Wählen Sie  > **Netzwerk** (Network) > **E-Mail** (Email).


Abbildung 5–3 E-Mail

Schritt 2: Klicken Sie auf , um die Funktion zu aktivieren.

Schritt 3: Konfigurieren Sie die E-Mail-Parameter.


Tabelle 5–3 Beschreibung der E-Mail-Parameter

Parameter	Beschreibung	
SMTP-Server	SMTP-Serveradresse	 Details siehe Tabelle 5–4.
Port	Portnummer des SMTP-Servers.	
Benutzername	Konto des SMTP-Servers.	
Passwort	Passwort des SMTP-Servers.	
Anonym	Klicken Sie auf <input type="checkbox"/> und die Absenderdaten werden nicht in der E-Mail angezeigt.	
Absender	E-Mail-Adresse des Absenders.	
Verschlüsselungstyp	Wählen Sie zwischen Keiner (None), SSL und TLS . Details siehe Tabelle 5–4.	
Betreff	Geben Sie maximal 63 Zeichen in chinesischen, englischen oder arabischen Ziffern ein. Klicken Sie zur Auswahl des Titeltyps auf + , einschließlich Gerätename (Device Name), Geräte-ID (Device ID) und Ereignistyp (Event Type). Sie können maximal 2 Titel festlegen.	
Anhang	Aktivieren Sie das Kontrollkästchen, um einen Anhang in der E-Mail zu unterstützen.	

Parameter	Beschreibung
Empfänger	<ul style="list-style-type: none"> E-Mail-Adresse des Empfängers. Unterstützt maximal 3 Adressen. Nach Eingabe der E-Mail-Adresse des Empfängers wird die Schaltfläche Test angezeigt. Klicken Sie auf Test, um zu testen, ob die E-Mails erfolgreich gesendet und empfangen werden können.
Integritäts-Mail	Das System sendet eine Testmail, um zu überprüfen, ob die Verbindung erfolgreich konfiguriert wurde. Klicken Sie auf  und konfigurieren Sie das Sendeintervall (Sending Interval). Das System sendet dann Testmails gemäß dem eingestellten Intervall.

Zur Konfiguration der wichtigsten Posteingänge siehe Tabelle 5–4.

Tabelle 5–4 Beschreibung der Mailbox-Konfiguration

Posteingang	SMTP-Server	Authentifizierung	Port	Beschreibung
Gmail	smtp.gmail.com	SSL	465	<ul style="list-style-type: none"> Sie müssen den SMTP-Dienst in Ihrer Mailbox aktivieren. Der Authentifizierungscode ist erforderlich, das E-Mail-Passwort ist nicht anwendbar.  Authentifizierungscode: Der Code, den Sie erhalten, wenn Sie den SMTP-Dienst aktivieren.
		TLS	587	

Schritt 4: Klicken Sie auf **Anwenden** (Apply).

5.1.4 Grundlegende Dienste

Konfigurieren Sie die grundlegenden Dienste zur Verbesserung von Netzwerk- und Datensicherheit.

Schritt 1: Wählen Sie  > **Netzwerk** (Network) > **Grundlegende Dienste** (Basic Service).

Abbildung 5–4 Grundlegende Dienste

Schritt 2: Aktivieren Sie die grundlegenden Dienste entsprechend dem tatsächlichen Bedarf.

Tabelle 5–5 Beschreibung der Parameter der grundlegenden Dienste

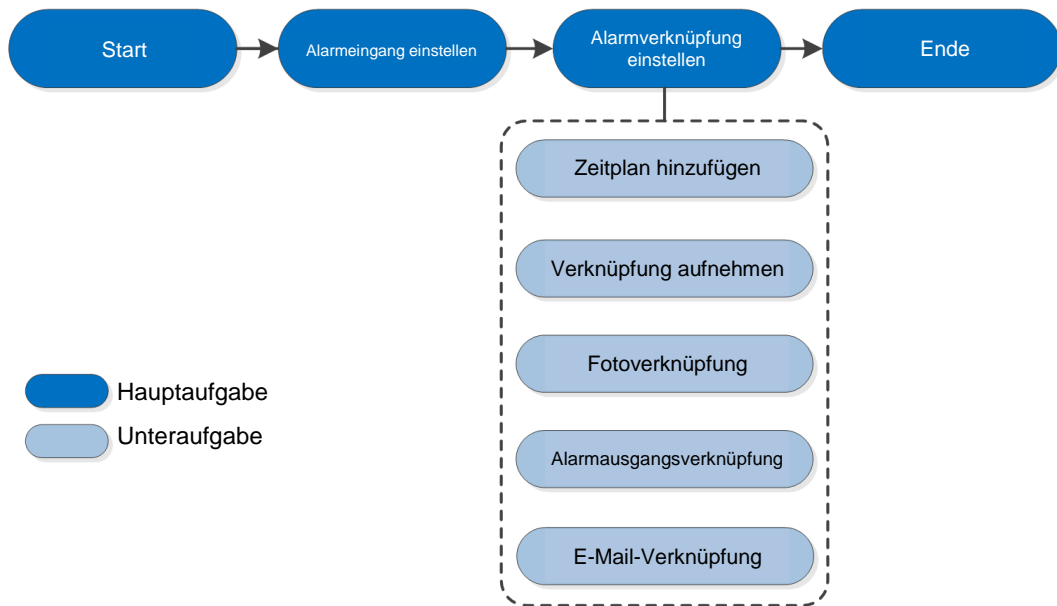
Funktion	Beschreibung
SSH	Sie können die SSH-Authentifizierung aktivieren, um die Sicherheitsverwaltung durchzuführen.
Multicast-/Broadcast-Suche	Aktivieren Sie diese Funktion. Wenn mehrere Benutzer das Videobild des Geräts gleichzeitig über das Netzwerk anzeigen, finden sie Ihr Gerät über das Multicast-/Broadcast-Protokoll.
CGI	Aktivieren Sie diese Funktion, dann können andere Geräte über diesen Dienst darauf zugreifen. Die Funktion ist standardmäßig aktiviert.
Onvif	
Genetec	
Mobiltelefon Push-Benachrichtigung	Aktivieren Sie diese Funktion, dann sendet das System das Foto, das bei Auslösung des Alarms aufgenommen wurde, an Ihr Telefon. Diese Funktion ist standardmäßig aktiviert.
Privater Protokoll-Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus zwischen Sicherheitsmodus (Security Mode) und Kompatibilitätsmodus (Compatible Mode) aus. Sicherheitsmodus ist empfohlen.

Schritt 3: Klicken Sie auf **Anwenden** (Apply).

5.2 Ereignis


Dieser Abschnitt nimmt Alarmeingang als Beispiel, um die Konfiguration der Alarmverknüpfung zu beschreiben.

Abbildung 5–5 Konfigurieren von Alarmereignissen



5.2.1 Alarmeingang einstellen

Wenn vom Gerät ein Alarm am Alarmeingang ausgelöst wird, führt das System die festgelegte Alarmverknüpfung aus.

Schritt 1: Wählen Sie  > **Ereignis** (Event) > **Alarm**.


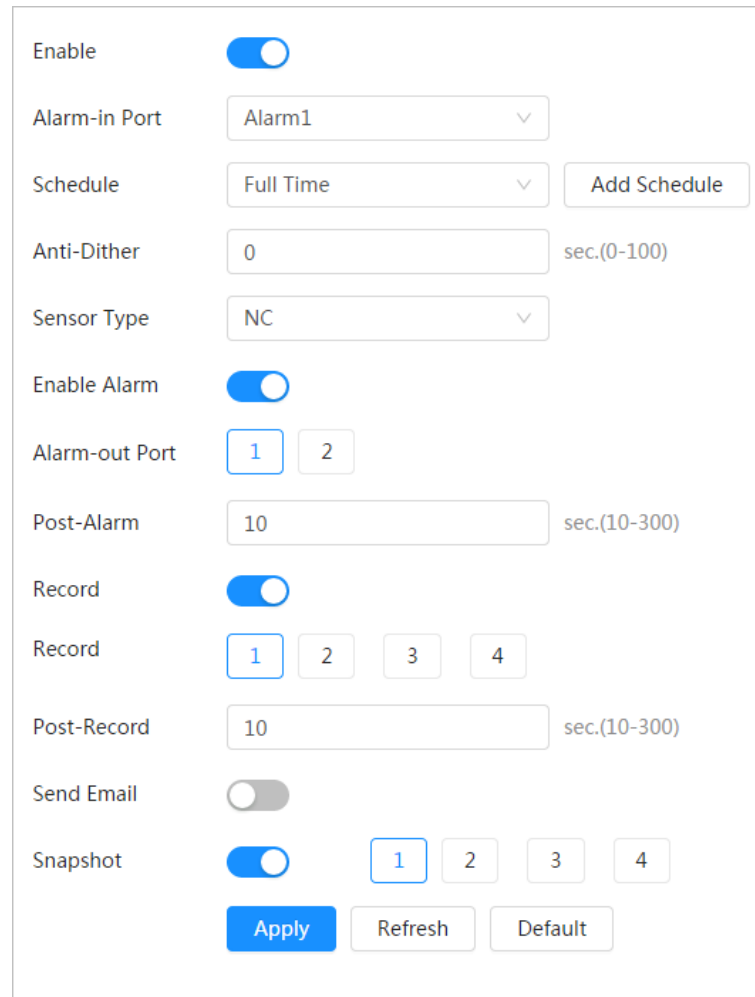
Schritt 2: Klicken Sie neben **Aktivieren** (Enable) auf , um die Alarmverknüpfung zu aktivieren.

Abbildung 5–6 Alarmverknüpfung



Schritt 3: Wählen Sie einen Alarmeingang und einen Sensortyp.

- Sensortyp: NO oder NC.
- Anti-Verwackeln: Nimmt nur einen Alarmereignis während des Anti-Verwackeln-Zeitraums auf.

Schritt 4: Wählen Sie die Zeitplan- und Scharfschaltungszeiträume sowie die Alarmverknüpfungsaktion. Einzelheiten siehe „5.2.2 Alarmverknüpfung einstellen“.

Wenn die vorhandenen Zeitpläne die Szenenanforderung nicht erfüllen, klicken Sie auf **Zeitplan hinzufügen** (Add Schedule), um einen neuen Zeitplan hinzuzufügen. Einzelheiten siehe „5.2.2.1 Zeitplan hinzufügen“.

Schritt 5: Klicken Sie auf **Anwenden** (Apply).

5.2.2 Alarmverknüpfung einstellen

Wählen Sie bei der Konfiguration von Alarmereignissen Alarmverknüpfungen aus (z. B. Aufzeichnung, Momentaufnahme). Das System alarmiert, sobald der entsprechende Alarm in der eingestellten Scharfschaltungsperiode ausgelöst wird.



Wählen Sie  > **Ereignis** (Event) > **Alarm** und klicken Sie dann neben **Aktivieren** (Enable) auf , um die Alarmverknüpfung zu aktivieren.

Abbildung 5–7 Alarmverknüpfung

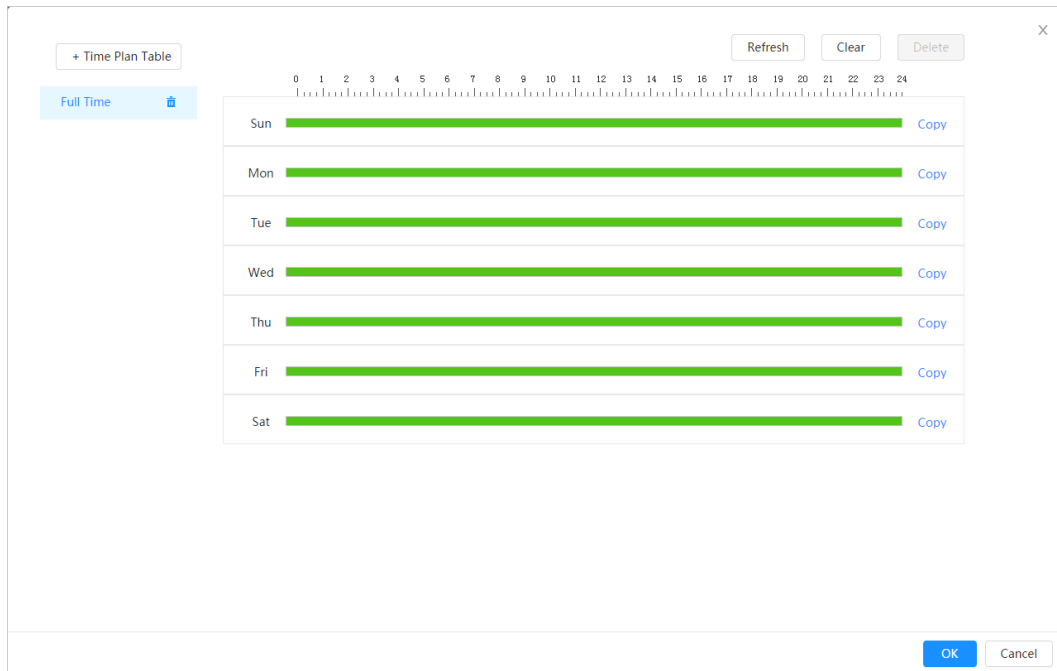
Enable	<input checked="" type="checkbox"/>
Alarm-in Port	Alarm1 <input type="button" value="v"/>
Schedule	Full Time <input type="button" value="v"/> <input type="button" value="Add Schedule"/>
Anti-Dither	0 sec.(0-100)
Sensor Type	NC <input type="button" value="v"/>
Enable Alarm	<input checked="" type="checkbox"/>
Alarm-out Port	<input type="button" value="1"/> <input type="button" value="2"/>
Post-Alarm	10 sec.(10-300)
Record	<input checked="" type="checkbox"/>
Record	<input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/>
Post-Record	10 sec.(10-300)
Send Email	<input type="checkbox"/>
Snapshot	<input checked="" type="checkbox"/> <input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>	

5.2.2.1 Zeitplan hinzufügen

Stellen Sie die Aktivierungszeiträume ein. Das System führt eine entsprechende Verknüpfungsaktion ausschließlich im eingestellten Zeitraum durch.

Schritt 1: Klicken Sie neben **Zeitplan** (Schedule) auf **Zeitplan hinzufügen** (Add Schedule).

Abbildung 5–8 Zeitplan




Schritt 2: Ziehen Sie mit gedrückter linker Maustaste auf der Zeitachse, um Scharfschaltungszeiträume festzulegen. Alarme werden in dem auf der Zeitachse grün markierten Zeitraum ausgelöst.

- Klicken Sie neben einem Tag auf **Kopieren** (Copy) und wählen Sie die Tage aus, die Sie zum Eingabeaufforderungsfenster kopieren möchten. Sie können die Konfiguration zu den ausgewählten Tagen kopieren. Aktivieren Sie das Kontrollkästchen **Alle auswählen** (Select All), um alle Tage zum Kopieren der Konfiguration auszuwählen.
- Sie können 6 Zeiträume pro Tag einstellen.

Schritt 3: Klicken Sie auf **Anwenden** (Apply).

Schritt 4: (Optional) Klicken Sie auf **Zeitplantabelle** (Time Plan Table), um eine neue Zeitplantabelle hinzuzufügen.

Sie können:

- Klicken Sie auf den Gerätenamen doppelt, um ihn zu bearbeiten.
- Klicken Sie auf , um die Tabelle nach Bedarf zu löschen.

5.2.2.2 Verknüpfung aufnehmen

Das System kann den Aufnahmekanal verknüpfen, wenn ein Alarm ausgelöst wird. Nach einem Alarm beendet das System die Aufnahme nach einem längeren Zeitraum entsprechend der **Nachaufnahme** (Post-Record)-Einstellung.

Voraussetzungen

- Nachdem der entsprechende Alarmtyp (**Normal**, **Bewegung** (Motion) oder **Alarm**) aktiviert wurde, wird der Aufnahmekanal mit der Aufnahme verknüpft.
- Wenn Sie den automatischen Aufnahmemodus aktivieren, tritt die Aufnahmeverknüpfung in Kraft.

Aufnahmeverknüpfung einstellen

Klicken Sie im **Alarm**-Fenster auf , um die Aufnahmeverknüpfung zu aktivieren. Wählen Sie den Kanal nach Bedarf aus und stellen Sie die **Nachaufnahme** (Post-Record) ein, um die Alarmverknüpfung und Aufnahmeverzögerung einzustellen.

Nachdem **Nachaufnahme** (Post-Record) konfiguriert wurde, wird die Alarmaufnahme nach dem Alarmende noch für einen längeren Zeitraum fortgesetzt.

Abbildung 5–9 Aufnahmeverknüpfung



5.2.2.3 Fotoverknüpfung

Nachdem die Fotoverknüpfung konfiguriert wurde, alarmiert das System automatisch und erstellt Fotos, wenn ein Alarm ausgelöst wird.

Voraussetzungen

Nachdem der entsprechende Alarmtyp (**Normal**, **Bewegung** (Motion) oder **Alarm**) aktiviert wurde, wird der Fotoaufnahmekanal mit dem aufzunehmenden Bild verknüpft.

Aufnahmeverknüpfung einstellen

Klicken Sie im **Alarm**-Fenster auf , um die Fotoverknüpfung zu aktivieren und wählen Sie den Kanal nach Bedarf aus.

Abbildung 5–10 Fotoverknüpfung



5.2.2.4 Alarmausgangsverknüpfung

Wenn ein Alarm ausgelöst wurde, stellt das System automatisch eine Verknüpfung mit einem Alarmausgabegerät her.

Klicken Sie im **Alarm**-Fenster auf , um die Alarmausgabeverknüpfung zu aktivieren. Wählen Sie bei Bedarf den Kanal aus und konfigurieren Sie dann den **Nachalarm** (Post alarm). Wenn die Alarmverzögerung eingestellt ist, wird der Alarm für einen bestimmten Zeitraum fortgesetzt, nachdem der Alarm beendet wurde.

Abbildung 5–11 Alarm-Ausgabeverknüpfung

Enable Alarm	<input checked="" type="checkbox"/>
Alarm-out Port	<input type="text" value="1"/> <input type="text" value="2"/>
Post-Alarm	<input type="text" value="10"/> sec.(10-300)

5.2.2.5E-Mail-Verknüpfung

Wenn ein Alarm ausgelöst wird, sendet das System automatisch eine E-Mail an Benutzer. Die E-Mail-Verknüpfung wird nur wirksam, wenn SMTP konfiguriert ist. Einzelheiten siehe „5.1.3 E-Mail“.

Abbildung 5–12 E-Mail-Verknüpfung

Send Email	<input type="checkbox"/>
------------	--------------------------

5.3 System

In diesem Abschnitt werden die Systemkonfigurationen vorgestellt, einschließlich Allgemein, Datum und Zeit, Konto, Sicherheit, PTZ-Einstellungen, Rücksetzung, Import/Export, Fernkonfiguration, Automatische Wartung und Upgrade.

5.3.1 Allgemein

5.3.1.1 Allgemein

Sie können Gerätenamen, Sprache und Videostandard konfigurieren.

Schritt 1: Wählen Sie  > **System** > **Generell** (General) > **Allgemein** (Basic).

Abbildung 5–13 Allgemein

Basic	Date & Time
Device Name	<input type="text" value="XXXXXXXXXX"/>
Video Standard	<input type="text" value="PAL"/> ▼
	<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>

Schritt 2: Konfigurieren Sie die allgemeinen Parameter.

Tabelle 5–6 Beschreibung der allgemeinen Parameter

Parameter	Beschreibung
Name	Geben Sie den Gerätenamen ein.
Video-Standard	Wählen Sie den Videostandard als PAL oder NTSC .

Schritt 3: Klicken Sie auf **Anwenden** (Apply).

5.3.1.2 Datum und Zeit

Sie können Datum- und Zeitformat, Zeitzone, Uhrzeit, Sommerzeit und NTP-Server konfigurieren.

Schritt 1: Wählen Sie  > **System** > **Generell** (General) > **Datum & Zeit** (Date & Time).

Abbildung 5–14 Datum und Zeit

Schritt 2: Konfiguriert Datum- und Zeitparameter.

Tabelle 5–7 Beschreibung der Datums- und Zeitparameter

Parameter	Beschreibung
Datumformat	Konfiguriert das Datumformat.
Zeit	<ul style="list-style-type: none"> • Manuelle Einstellung: Konfiguriert die Parameter manuell. • NTP: Wenn Sie NTP wählen, synchronisiert das System dann die Zeit mit dem Internet-Server in Echtzeit. Sie können auch IP-Adresse, Zeitzone, Port und Intervall eines PC eingeben, der den NTP-Server installiert hat, um NTP zu verwenden.

Parameter	Beschreibung
Zeitformat	Konfiguriert das Zeitformat. Wählen Sie 12-Stundenformat (12-Hour) oder 24-Stundenformat (24-Hour).
Zeitzone	Konfiguriert die Zeitzone, in der sich die Kamera befindet.
Uhrzeit	Konfiguriert die Systemzeit. Klicken Sie auf PC synchronisieren , damit ändert sich die Systemzeit zur PC-Zeit.
Sommerzeit	Aktivieren Sie die Sommerzeit nach Bedarf. Klicken Sie auf <input type="checkbox"/> und konfigurieren Sie Startzeit und Endzeit der Sommerzeit mit Datum (Date) oder Woche (Week).

Schritt 3: Klicken Sie auf **Anwenden** (Apply).

5.3.2 Konto

Sie können Benutzer verwalten, z. B. hinzufügen, löschen oder bearbeiten. Zu den Benutzern gehören Admin, hinzugefügte Benutzer und ONVIF-Benutzer.

Die Verwaltung von Benutzern und Gruppen ist nur für Administratoren möglich.

- Die maximale Länge des Benutzer- oder Gruppennamens beträgt 31 Zeichen, der aus Ziffern, Buchstaben, Unterstrichungen, Bindestrichen, Punkten und @ bestehen kann.
- Das Passwort muss aus 8 bis 32 nicht leeren Zeichen bestehen und mindestens zwei Arten von Zeichen von Groß- und Kleinschreibung, Ziffer und Sonderzeichen enthalten (außer ' " ; : &).
- Sie können maximal 18 Benutzer und 8 Gruppen haben.
- Sie können Benutzer über einzelne Benutzer oder Gruppen verwalten. Doppelte Benutzer- oder Gruppennamen sind nicht zulässig. Ein Benutzer kann sich jeweils nur in einer Gruppe befinden und die Gruppenbenutzer können Berechtigungen im Gruppenberechtigungsbereich besitzen.
- Online-Benutzer können ihre eigenen Berechtigungen nicht ändern.
- Es gibt standardmäßig einen Administrator, der die höchste Berechtigung hat.
- Wählen Sie **Anonyme Anmeldung** (Anonymous Login) und melden Sie sich nur mit der IP-Adresse statt mit Benutzername und Passwort an. Anonyme Benutzer haben nur Vorschau-Berechtigungen. Klicken Sie während der anonymen Anmeldung auf **Abmeldung** (Logout), damit können Sie sich mit einem anderen Benutzernamen anmelden.

5.3.2.1 Benutzer

5.3.2.1.1 Benutzer hinzufügen

Standardmäßig sind Sie ein Admin-Benutzer. Sie können Benutzer hinzufügen und verschiedene Berechtigungen konfigurieren.


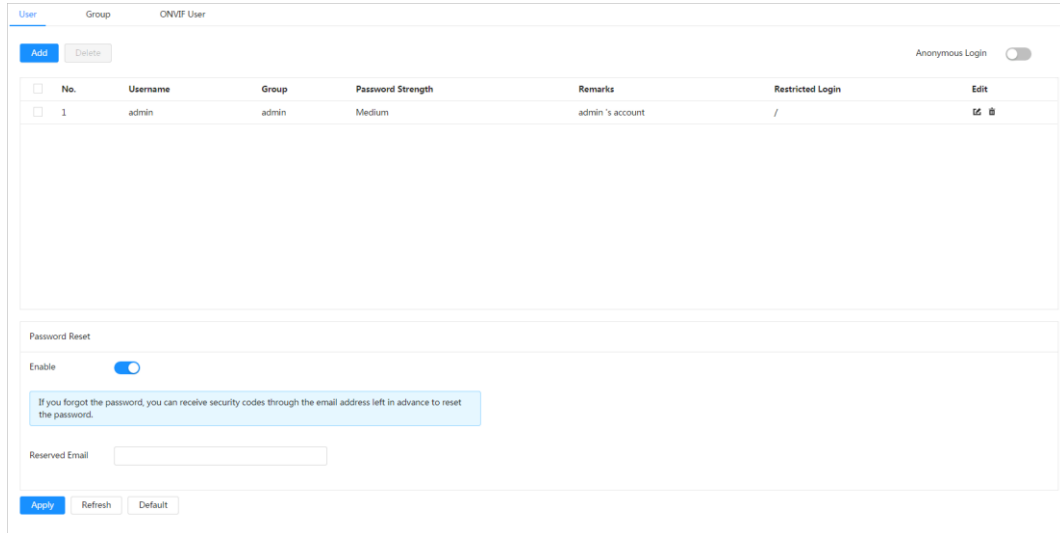


Schritt 1: Wählen Sie  > **System** > **Konto** (Account) > **Benutzer** (User).

Abbildung 5–15 Benutzer



The screenshot displays a user management interface. At the top, there are tabs for 'User', 'Group', and 'ONVIF User'. Below the tabs, there are 'Add' and 'Delete' buttons. On the right side, there is a toggle for 'Anonymous Login'. The main area contains a table with the following data:

No.	Username	Group	Password Strength	Remarks	Restricted Login	Edit
1	admin	admin	Medium	admin's account	/	 

Below the table, there is a 'Password Reset' section. It includes a toggle for 'Enable' which is turned on. A text box explains: 'If you forgot the password, you can receive security codes through the email address left in advance to reset the password.' There is an input field for 'Reserved Email' and buttons for 'Apply', 'Refresh', and 'Default' at the bottom.

Schritt 2: Klicken Sie auf **Hinzufügen** (Add).

Abbildung 5–16 Benutzer hinzufügen (System)

Abbildung 5–17 Benutzer hinzufügen (eingeschränkte Anmeldung)

Schritt 3: Konfigurieren Sie die Benutzerparameter.

Tabelle 5–8 Beschreibung der Benutzerparameter (1)


Parameter	Beschreibung
Benutzername	Eindeutige Identifizierung des Benutzers. Sie dürfen keinen vorhandenen Benutzernamen verwenden.
Passwort	Passwort eingeben und erneut bestätigen.

Parameter	Beschreibung
Passwort bestätigen	Das Passwort muss aus 8 bis 32 nicht leeren Zeichen bestehen und mindestens zwei Arten von Zeichen von Groß- und Kleinschreibung, Ziffer und Sonderzeichen enthalten (außer ' " ; : &).
Gruppe	Gruppe, zu der die Benutzer gehören. Jede Gruppe hat unterschiedliche Berechtigungen.
Anmerkung	Beschreiben Sie den Benutzer.
System	Wählen Sie die Berechtigungen nach Bedarf.  Wir empfehlen, Normalbenutzern weniger Befugnisse zu erteilen als Premiumbenutzern.
Live	Wählt die Live-View-Berechtigung für den hinzuzufügenden Benutzer aus.
Suche	Wählt die Suchberechtigung für den hinzuzufügenden Benutzer aus.
Eingeschränkte Anmeldung	<p>Stellt die PC-Adresse ein, mit der sich der definierte Benutzer an der Kamera anmelden kann, sowie den Gültigkeitszeitraum und den Zeitbereich. Sie können sich mit der festgelegten IP im definierten Zeitraum der Gültigkeitsdauer bei der Weboberfläche anmelden.</p> <ul style="list-style-type: none"> • IP-Adresse: Sie können sich über den PC mit der eingestellten IP im Web anmelden. • Gültigkeitszeitraum: Sie können sich im Web im eingestellten Gültigkeitszeitraum anmelden. • Zeitbereich: Sie können sich im eingestellten Zeitbereich im Web anmelden. <p>Einstellungs-Möglichkeiten</p> <ol style="list-style-type: none"> 1. IP-Adresse: Geben Sie die IP-Adresse des hinzuzufügenden Hosts ein. 2. IP-Segment: Geben Sie die Start- und die Endadresse des hinzuzufügenden Hosts ein.

Schritt 4: Klicken Sie auf **Anwenden** (Apply).


Der neu hinzugefügte Benutzer wird in der Benutzernamenliste angezeigt.

Verwandte Operationen

- Klicken Sie auf , um Passwort, Gruppe, Memo oder Berechtigungen zu bearbeiten.



Beim Admin-Konto können Sie nur das Passwort bearbeiten.

- Klicken Sie auf , um hinzugefügte Benutzer zu löschen. Der Admin-Benutzer kann nicht gelöscht werden.



Das-Admin-Konto kann nicht gelöscht werden.

5.3.2.1.2 Passwort zurücksetzen

Aktivieren Sie die Funktion und Sie können das Passwort zurücksetzen, indem Sie im Anmeldefenster auf **Passwort vergessen?** (Forget password?) klicken. Einzelheiten siehe „3.2 Passwort zurücksetzen“.

Schritt 1: Wählen Sie > **System** > **Konto** (Account) > **Benutzer** (User).

Abbildung 5–18 Benutzer

The screenshot shows the 'User' management page with the 'Password Reset' section. The 'Enable' toggle is currently turned on. Below the toggle, there is a text box for 'Reserved Email' and buttons for 'Apply', 'Refresh', and 'Default'.

No.	Username	Group	Password Strength	Remarks	Restricted Login	Edit
1	admin	admin	Medium	admin's account	/	

Schritt 2: Klicken Sie unter **Passwort zurücksetzen** (Password Reset) neben **Aktivieren** (Enable) auf .

Wenn die Funktion nicht aktiviert wurde, können Sie das Passwort nur durch Zurücksetzen der Kamera zurücksetzen.

Schritt 3: Geben Sie die reservierte E-Mail-Adresse ein.

Schritt 4: Klicken Sie auf **Anwenden** (Apply).

5.3.2.2 ONVIF-Benutzer

Sie können ONVIF-Benutzer hinzufügen, löschen und ihre Passwörter ändern.

Schritt 1: Wählen Sie > **System** > **Konto** (Account) > **ONVIF-Benutzer** (ONVIF User).

Abbildung 5–19 ONVIF-Benutzer

The screenshot shows the 'ONVIF User' management page. It features an 'Add' button and a 'Delete' button. Below them is a table with columns for 'No.', 'Username', 'Group', 'Password Strength', and 'Edit'.

No.	Username	Group	Password Strength	Edit
1	admin	admin	Medium	

Schritt 2: Klicken Sie auf **Hinzufügen** (Add).

Abbildung 5–20 ONVIF-Benutzer hinzufügen

Schritt 3: Konfigurieren Sie die Benutzerparameter.

Tabelle 5–9 Beschreibung der ONVIF-Benutzerparameter

Parameter	Beschreibung
Benutzername	Eindeutige Identifizierung des Benutzers. Sie dürfen keinen vorhandenen Benutzernamen verwenden.
Passwort	Passwort eingeben und erneut bestätigen.
Passwort bestätigen	Das Passwort muss aus 8 bis 32 nicht leeren Zeichen bestehen und mindestens zwei Arten von Zeichen von Groß- und Kleinschreibung, Ziffer und Sonderzeichen enthalten (außer ' " ; : &).
Gruppenname	Gruppe, zu der die Benutzer gehören. Jede Gruppe hat unterschiedliche Berechtigungen.

Schritt 4: Klicken Sie auf **OK**.


Der neu hinzugefügte Benutzer wird in der Benutzernamenliste angezeigt.

Verwandte Operationen

- Klicken Sie auf , um Passwort, Gruppe, Memo oder Berechtigungen zu bearbeiten.



Beim Admin-Konto können Sie nur das Passwort ändern.

- Klicken Sie auf , um hinzugefügte Benutzer zu löschen. Der Admin-Benutzer kann nicht gelöscht werden.



Das-Admin-Konto kann nicht gelöscht werden.

5.3.3 Manager

5.3.3.1 Anforderungen

Um sicherzustellen, dass das System normal läuft, warten Sie es entsprechend den folgenden Anforderungen:

- Überprüfen Sie regelmäßig die Überwachungsbilder.
- Löschen Sie regelmäßig Daten über Benutzer und Benutzergruppen, die nicht häufig verwendet werden.

- Ändern Sie das Passwort alle drei Monate. Einzelheiten siehe „5.3.2 Konto“.
- Zeigen Sie die Systemprotokolle an und analysieren Sie sie. Verarbeiten Sie Abweichungen zeitnah.
- Sichern Sie die Systemkonfiguration regelmäßig.
- Starten Sie das Gerät neu und löschen Sie regelmäßig die alten Dateien.
- Aktualisieren Sie die Firmware zeitnah.

5.3.3.2Wartung

Sie können das System manuell neu starten und den Zeitpunkt für den automatischen Neustart und das automatische Löschen alter Dateien festlegen. Diese Funktion ist standardmäßig deaktiviert.


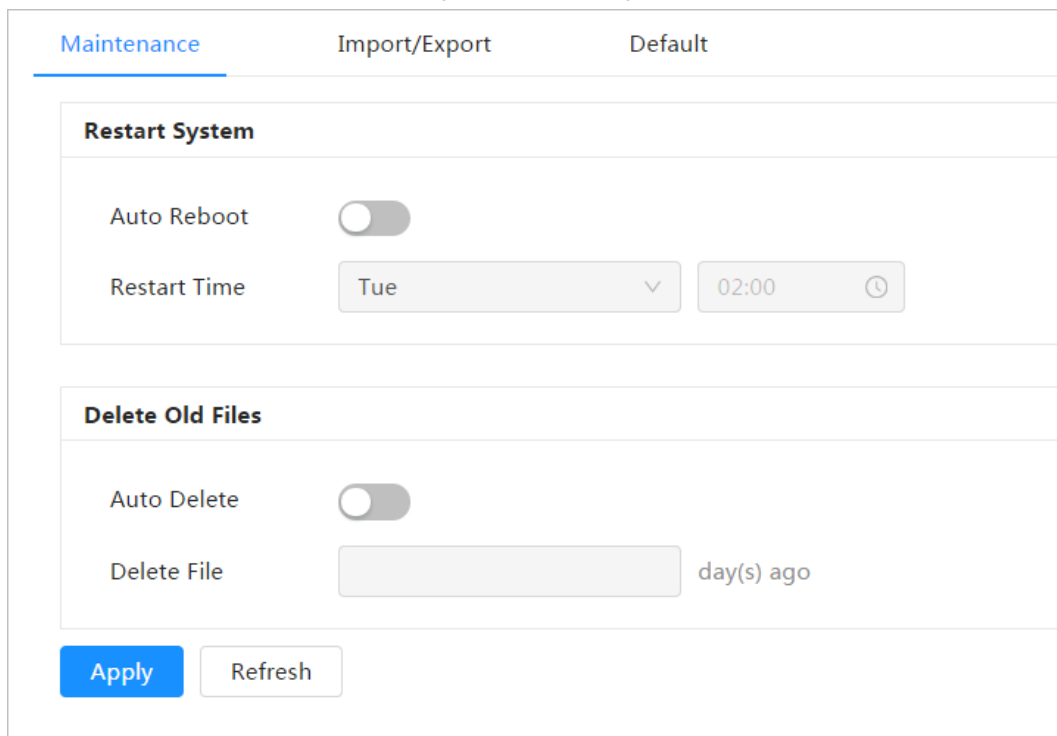


Schritt 1: Wählen Sie  > **System** > **Manager** > **Wartung** (Maintenance).

Abbildung 5–21 Wartung



Schritt 2: Konfigurieren Sie die Parameter für die automatische Wartung.

- Klicken Sie unter **Systemneustart** (Restart System) auf  neben **Automatischer Neustart** (Auto Reboot) und legen Sie den Zeitpunkt für den Neustart fest. Das System führt dann automatisch zum vorgegebenen Zeitpunkt jede Woche einen Neustart durch.
- Klicken Sie unter **Alte Dateien automatisch löschen** (Auto Delete Old Files) auf  neben **Automatisch Löschen** (Auto Delete) und legen Sie den Zeitpunkt fest. Das System löscht dann alte Dateien automatisch zum vorgegebenen Zeitpunkt. Der Zeitrahmen beträgt 1 bis 31 Tage.



Wenn Sie die **Automatisch LösCHFunktion** (Auto Delete) aktivieren und bestätigen, können die gelöschten Dateien nicht wiederhergestellt werden. Verwenden Sie diese Funktion **vorsichtig**.

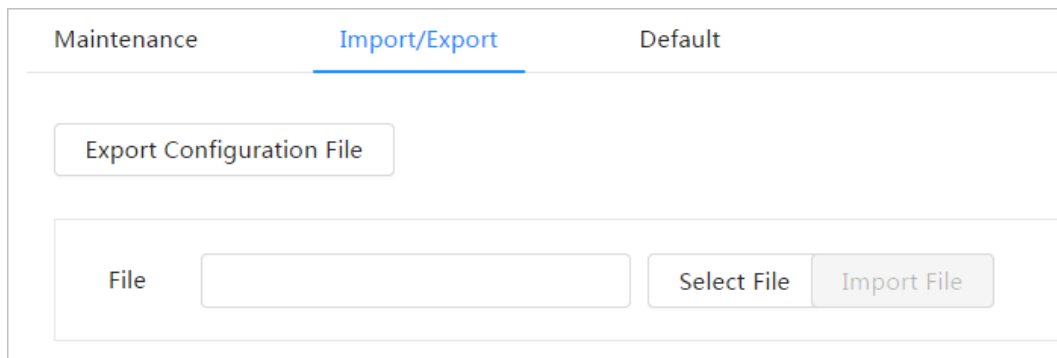
Schritt 3: Klicken Sie auf **Anwenden** (Apply).

5.3.3.3 Importieren/Exportieren

- Exportieren Sie die Systemkonfigurationsdatei, um die Systemkonfiguration zu sichern.
- Importieren Sie die Systemkonfigurationsdatei, um eine schnelle Konfiguration vorzunehmen oder die Systemkonfiguration wiederherzustellen.

Schritt 1: Wählen Sie  > **System** > **Manager** > **Importieren/Exportieren** (Import/Export).

Abbildung 5–22 Importieren/Exportieren



Schritt 2: Importieren und exportieren.

- Importieren: Wählen Sie die lokale Konfigurationsdatei aus und klicken Sie auf **Datei importieren** (Import File), um die lokale Systemkonfigurationsdatei in das System zu importieren.
- Exportieren: Klicken Sie auf **Konfigurationsdatei exportieren** (Export Configuration file), um die Systemkonfigurationsdatei in den lokalen Speicher zu exportieren.

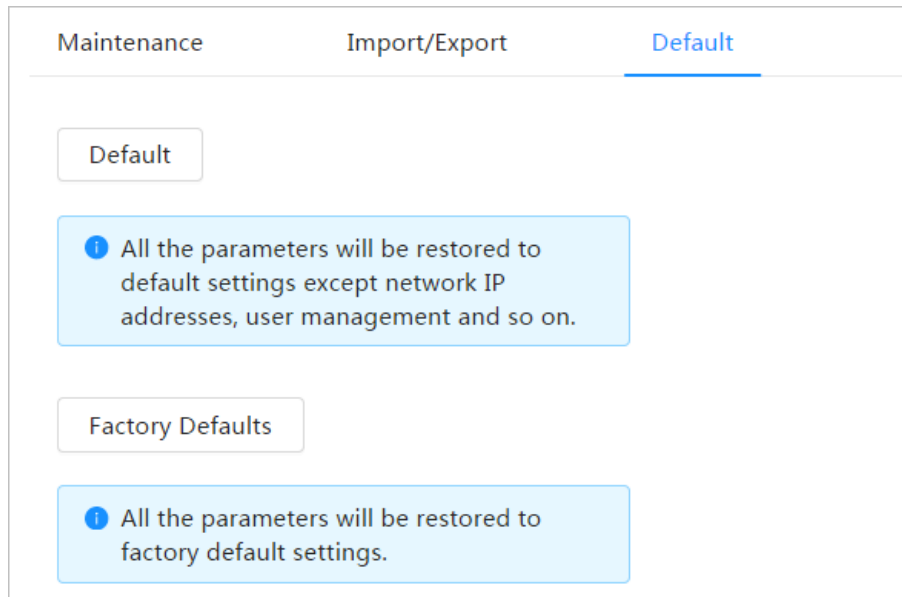
5.3.3.4 Rücksetzung zu den Werkseinstellungen

Stellen Sie das Gerät auf die Standardkonfiguration oder die Werkseinstellungen zurück. Die Funktion setzt das Gerät auf die Standardkonfiguration oder die Werkseinstellungen zurück.

Wählen Sie  > **System** > **Manager** > **Standard** (Default).

- Klicken Sie auf **Standard** (Default), damit werden alle Konfigurationen außer IP-Adresse und Konto zu den Standardeinstellungen zurückgesetzt.
- Klicken Sie auf **Werkseinstellungen** (Factory Default), damit werden alle Konfigurationen zu den Werkseinstellungen zurückgesetzt.

Abbildung 5–23 Standard



5.3.4 Aktualisieren

Mit einem Upgrade auf das neuste System können die Kamerafunktionen optimiert und die Stabilität verbessert werden.

Wenn versehentlich die falsche Upgrade-Datei verwendet wurde, muss das Gerät neu gestartet werden; andernfalls funktionieren bestimmte Funktionen möglicherweise fehlerhaft.

Schritt 1: Wählen Sie  > **System** > **Upgrade**.

Abbildung 5–24 Upgrade



Schritt 2: Klicken Sie auf **Browse** und laden Sie die Upgrade-Datei hoch.

Die Upgrade-Datei muss eine .bin-Datei sein.

Schritt 3: Klicken Sie auf **Upgrade**.

Die Aktualisierung beginnt.

Anhang 1 Empfehlungen zur Cybersicherheit

Cybersicherheit ist mehr als nur ein Schlagwort: Es ist etwas, das sich auf jedes Gerät bezieht, das mit dem Internet verbunden ist. Die IP-Videoüberwachung ist nicht immun gegen Cyberrisiken, aber grundlegende Maßnahmen zum Schutz und zur Stärkung von Netzwerken und vernetzten Geräten machen sie weniger anfällig für Angriffe. Nachstehend finden Sie einige Tipps und Empfehlungen, wie Sie ein sichereres Sicherheitssystem schaffen können.

Verbindliche Maßnahmen, die zur Netzwerksicherheit der Grundausstattung zu ergreifen sind:

1. Verwenden Sie sichere Passwörter

Sehen Sie sich die folgenden Vorschläge an, um Passwörter festzulegen:

- Die Länge darf nicht weniger als 8 Zeichen betragen;
- Schließen Sie mindestens zwei Arten von Zeichen ein: Groß- und Kleinbuchstaben, Zahlen und Symbole;
- Fügen Sie nicht den Kontonamen oder den Kontonamen in umgekehrter Reihenfolge ein;
- Verwenden Sie keine fortlaufenden Zeichen, wie z.B. 123, abc usw.;
- Verwenden Sie keine Mehrfachzeichen, wie z.B. 111, aaa, usw.;

2. Aktualisieren Sie Firmware und Client-Software rechtzeitig

- Gemäß dem in der Tech-Industrie üblichen Verfahren empfehlen wir, die Firmware Ihrer Geräte (wie NVR, DVR, IP-Kamera usw.) auf dem neuesten Stand zu halten, um zu gewährleisten, dass das System mit den neuesten Sicherheitspatches und -fixes ausgestattet ist. Wenn das Gerät an ein öffentliches Netzwerk angeschlossen ist, empfehlen wir, die Funktion „Nach Updates suchen“ zu aktivieren, um rechtzeitig Informationen zu Firmware-Aktualisierungen zu erhalten, die vom Hersteller veröffentlicht wurden.
- Wir empfehlen, die neueste Version der Client-Software herunterzuladen und zu verwenden.

„Nice to have“-Empfehlungen zur Verbesserung der Netzwerksicherheit Ihrer Geräte:

1. Physischer Schutz

Wir empfehlen, dass Sie Geräte, insbesondere Speichergeräte, physisch schützen. Stellen Sie die Geräte beispielsweise in einen speziellen Computerraum und -schrank und implementieren Sie eine gut durchdachte Zutrittskontrollberechtigung und Schlüsselverwaltung, um unbefugte Mitarbeiter davon abzuhalten, physische Kontakte wie beschädigte Hardware, unbefugten Anschluss von Wechseldatenträgern (z.B. USB-Stick, serielle Schnittstelle) usw. durchzuführen.

2. Passwörter regelmäßig ändern

Wir empfehlen, die Passwörter regelmäßig zu ändern, um das Risiko zu verringern, erraten oder geknackt zu werden.

3. Passwörter einstellen und rechtzeitig aktualisieren

Das Gerät unterstützt die Funktion Passwortrücksetzung. Richten Sie rechtzeitig entsprechende Daten für das Zurücksetzen des Passworts ein, einschließlich der Fragen zur Mailbox und zum Passwortschutz des Endbenutzers. Wenn sich die Daten ändern, ändern Sie diese bitte rechtzeitig. Bei der Einstellung von Fragen zum Passwortschutz empfehlen wir, keine Fragen zu verwenden, die leicht zu erraten sind.

4. Kontosperrre aktivieren

Die Kontosperrfunktion ist standardmäßig aktiviert und wir empfehlen, sie eingeschaltet zu lassen, um die Kontosicherheit zu gewährleisten. Versucht sich ein Angreifer mehrmals mit dem falschen Passwort anzumelden, wird das entsprechende Konto und die Quell-IP-Adresse gesperrt.

5. Standard HTTP und andere Dienstports ändern

Wir empfehlen, die Standard-HTTP- und andere Dienstports in einen beliebigen Zahlensatz zwischen 1024 - 65535 zu ändern, um das Risiko zu verringern, dass Außenstehende erraten können, welche Ports Sie verwenden.

6. HTTPS aktivieren

Wir empfehlen, HTTPS zu aktivieren, damit Sie den Webdienst über einen sicheren Kommunikationskanal besuchen können.

7. MAC-Adressenverknüpfung

Wir empfehlen, die IP- und MAC-Adresse des Gateways mit dem Gerät zu verknüpfen, um das Risiko von ARP-Spoofing zu reduzieren.

8. Konten und Privilegien sinnvoll zuordnen

Gemäß den Geschäfts- und Verwaltungsanforderungen sollten Sie Benutzer sinnvoll hinzufügen und ihnen ein Minimum an Berechtigungen zuweisen.

9. Unnötige Dienste deaktivieren und sichere Modi wählen

Falls nicht erforderlich, empfehlen wir, einige Dienste wie SNMP, SMTP, UPnP usw. zu deaktivieren, um Risiken zu reduzieren.

Falls erforderlich, wird dringend empfohlen, dass Sie sichere Modi verwenden, einschließlich, aber nicht darauf beschränkt, die folgenden Dienste:

- SNMP: Wählen Sie SNMP v3 und richten Sie starke Verschlüsselungs- und Authentifizierungspasswörter ein.
- SMTP: Wählen Sie TLS, um auf den Mailbox-Server zuzugreifen.
- FTP: Wählen Sie SFTP, und richten Sie starke Passwörter ein.
- AP-Hotspot: Wählen Sie den Verschlüsselungsmodus WPA2-PSK und richten Sie starke Passwörter ein.

10. Audio- und Video-verschlüsselte Übertragung

Wenn Ihre Audio- und Videodateninhalte sehr wichtig oder sensibel sind, empfehlen wir, eine verschlüsselte Übertragungsfunktion zu verwenden, um das Risiko zu verringern, dass Audio- und Videodaten während der Übertragung gestohlen werden.

Zur Erinnerung: Die verschlüsselte Übertragung führt zu einem Verlust der Übertragungseffizienz.

11. Sichere Auditierung

- Online-Benutzer überprüfen: Wir empfehlen, die Online-Benutzer regelmäßig zu überprüfen, um zu sehen, ob ein Gerät ohne Berechtigung angemeldet ist.
- Geräteprotokoll prüfen: Durch die Anzeige der Protokolle können Sie die IP-Adressen, mit denen Sie sich bei Ihren Geräten angemeldet haben und deren wichtigste Funktionen erkennen.

12. Netzwerkprotokoll

Aufgrund der begrenzten Speicherkapazität der Geräte sind gespeicherte Protokolle begrenzt. Wenn Sie das Protokoll über einen längeren Zeitraum speichern müssen, empfehlen wir, die Netzwerkprotokollfunktion zu aktivieren, um zu gewährleisten, dass die

kritischen Protokolle mit dem Netzwerkprotokollserver für die Rückverfolgung synchronisiert werden.

13. Aufbau einer sicheren Netzwerkkumgebung

Um die Sicherheit der Geräte besser zu gewährleisten und mögliche Cyberrisiken zu reduzieren, empfehlen wir:

- Deaktivieren Sie die Port-Mapping-Funktion des Routers, um einen direkten Zugriff auf die Intranet-Geräte aus dem externen Netzwerk zu vermeiden.
- Das Netzwerk muss entsprechend dem tatsächlichen Netzwerkbedarf partitioniert und isoliert werden. Wenn es keine Kommunikationsanforderungen zwischen zwei Subnetzwerken gibt, empfehlen wir, VLAN, Netzwerk-GAP und andere Technologien zur Partitionierung des Netzwerks zu verwenden, um den Netzwerkisolationseffekt zu erreichen.
- Einrichtung des 802.1x Zugangsauthentifizierungssystems, um das Risiko eines unbefugten Zugriffs auf private Netzwerke zu reduzieren.
- Aktivieren Sie die IP/MAC-Adressfilterfunktion, um den Bereich der Hosts einzuschränken, die auf das Gerät zugreifen dürfen.

EINE SICHERERE GESELLSCHAFT UND EINE INTELLIGENTERE
LEBENSWEISE ERMÖGLICHEN

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Adresse: Nr.1399 Bin'an Road, Binjiang District, Hangzhou, P.R. China | Webseite: www.dahuasecurity.com | Postleitzahl: 310053

E-Mail: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883