safire
SMART

NETZWERK KAMERA

Benutzerhandbuch

Bitte lesen Sie diese Anleitung sorgfältig durch, bevor Sie das Gerät in Betrieb nehmen, und bewahren Sie sie zum weiteren Nachschlagen auf

Die folgenden Symbole oder Wörter finden Sie in diesem Handbuch.

Symbols/Words	Beschreibung
⚠ Warnung	Weist auf eine mittlere oder geringe potenzielle Gefahrensituation hin, die, wenn sie nicht vermieden wird, zu leichten oder mittelschweren Verletzungen führen kann oder kann.
⚠ Vorsicht	Weist auf ein potenzielles Risiko hin, das, wenn es nicht vermieden wird, zu Geräteschäden, Datenverlust, geringerer Leistung oder unerwarteten Ergebnissen führt oder führen könnte
☞ Anmerkung	Stellt zusätzliche Informationen bereit, um wichtige Punkte des Textes hervorzuheben oder zu ergänzen.

Über das Handbuch

- Dieses Handbuch ist für viele Modelle geeignet. Alle Beispiele, Screenshots, Abbildungen, Diagramme und Illustrationen, die im Handbuch verwendet werden, dienen zu Referenzzwecken, und die tatsächlichen Produkte können von diesem Handbuch abweichen.
- Bitte lesen Sie diese Bedienungsanleitung sorgfältig durch, um sicherzustellen, dass Sie das Gerät korrekt und sicher verwenden können.
- Innerhalb des gesetzlich zulässigen Höchstmaßes werden die in diesem Handbuch beschriebenen Produkte (einschließlich Hardware, Software, Firmware usw.) "WIE BESEHEN" bereitgestellt. Die Informationen in diesem Dokument (einschließlich URL und anderer Referenzdaten auf Internetseiten) können ohne vorherige Ankündigung geändert werden. Dieses Handbuch kann technische Fehlstellen oder Druckfehler enthalten. Diese Informationen werden regelmäßig aktualisiert, und diese Änderungen werden ohne vorherige Ankündigung in die neueste Version dieses Handbuchs aufgenommen.

Verwendung des Produkts

- Dieses Produkt sollte nicht für illegale Zwecke verwendet werden.
- Das Unternehmen gestattet niemandem, die Produkte des Unternehmens zu verwenden, um die Privatsphäre, die persönlichen Daten und die Bildrechte anderer zu verletzen. Der Benutzer darf dieses Produkt nicht für illegale oder verbotene Zwecke gemäß diesen Bedingungen und Erklärungen verwenden. Bei der Verwendung dieses Produkts darf der

Benutzer die Hardware dieses Produkts in keiner Weise beschädigen, deaktivieren, überlasten oder behindern oder die Verwendung dieses Produkts durch andere Benutzer beeinträchtigen. Außerdem sollte der Benutzer nicht versuchen, das Produkt oder die Software durch Hacken, Stehlen des Passworts oder auf andere Weise zu verwenden.

Elektrische Sicherheit

- Dieses Produkt ist für die Stromversorgung durch ein gelistetes Netzteil vorgesehen, das mit "Limited Power Source", "LPS" am Gerät, einem Nennausgang von mindestens 12 V/2 A oder POE 48 V/ 350 mA oder AC24 V (je nach Modell), nicht mehr als 2000 m Betriebshöhe und Tma = 60 °C gekennzeichnet ist.
- Was die Modi mit PoE-Funktion betrifft, so wird davon ausgegangen, dass die Funktion des ITE, die nach der Norm IEC 60950-1 untersucht wird, wahrscheinlich keine Verbindung zu einem Ethernet-Netzwerk mit externem Anlagen-Routing, einschließlich Campus-Umgebung, erfordert, und das ITE darf nur mit PoE-Netzwerken ohne Routing zur externen Anlage verbunden werden.
- Bei unsachgemäßer Handhabung und/oder Installation besteht die Gefahr eines Brandes oder Stromschlags.
- Das Produkt muss geerdet sein, um das Risiko eines Stromschlags zu verringern.
- ⚠ Warnung: Tragen Sie antistatische Handschuhe oder leiten Sie statische Elektrizität ab, bevor Sie die Blase oder Abdeckung der Kamera entfernen.
- ⚠ Achtung: Stellen Sie nicht zwei Stromversorgungsquellen gleichzeitig für das Gerät bereit, sofern nicht anders angegeben, da dies zu Geräteschäden führen kann!

Umwelt

- Starke Beanspruchung, heftige Vibrationen oder Wassereinwirkung sind während des Transports, der Lagerung und der Installation nicht zulässig.
- Vermeiden Sie es, die Kamera direkt auf extrem helle Objekte, wie z. B. Sonne, zu richten, da dies den Bildsensor beschädigen kann.
- Von Wärmequellen wie Heizkörpern, Heizregistern, Ofen usw. fernhalten.
- Setzen Sie das Produkt nicht dem direkten Luftstrom einer Klimaanlage aus.
- Stellen Sie das Gerät nicht in einer feuchten, staubigen, extrem heißen oder kalten Umgebung oder an Orten mit starker elektromagnetischer Strahlung oder instabiler Beleuchtung auf.
- Achten Sie darauf, dass keine reflektierende Fläche zu nah am Kameraobjektiv ist. Das IR-Licht der Kamera kann zurück in das Objektiv reflektiert werden, was zu Bildunschärfe führt.

Betrieb und tägliche Wartung

- Im Inneren befinden sich keine Teile, die vom Benutzer gewartet werden können. Bitte wenden Sie sich an das nächstgelegene Servicecenter, wenn das Produkt nicht richtig funktioniert.
- Bitte schalten Sie das Gerät aus und ziehen Sie dann das Netzkabel ab, bevor Sie mit Wartungsarbeiten beginnen.

- ⚠ Warnung: Alle Inspektions- und Reparaturarbeiten sollten von qualifiziertem Personal durchgeführt werden.
- Berühren Sie nicht die optische Komponente des CMOS-Sensors. Sie können ein Blasebalg verwenden, um den Staub auf der Linsenoberfläche zu entfernen.
- Verwenden Sie immer das trockene, weiche Tuch, um das Gerät zu reinigen. Wenn zu viel Staub vorhanden ist, verwenden Sie eine Tuchreinigung (z. B. mit einem Tuch), was zu einer schlechten IR-Funktionalität und/oder IR-Reflexion führen kann.
- Die Kuppelabdeckung ist ein optisches Gerät, bitte berühren oder wischen Sie die Abdeckungsoberfläche während der Installation und Verwendung nicht direkt ab. Verwenden Sie bei Staub eine ölfreie, weiche Bürste oder einen Haartrockner, um ihn vorsichtig zu entfernen. Verwenden Sie für Fett oder Fingerabdrücke ein ölfreies Baumwolltuch oder Papier, das mit Reinigungsmittel getränkt ist, um von der Linsenmitte nach außen zu wischen. Wechseln Sie das Tuch und wischen Sie es mehrmals ab, wenn es nicht sauber genug ist.

Datenschutz

- Bei der Installation von Kameras in öffentlichen Bereichen ist in angemessener und wirksamer Weise ein Warnhinweis zu geben und den Überwachungsbereich zu verdeutlichen.
- • Als Gerätenutzer oder Datenverantwortlicher können Sie personenbezogene Daten anderer erfassen, wie z. B. Gesicht, Kfz-Kennzeichen usw. Infolgedessen müssen Sie angemessene und notwendige Maßnahmen ergreifen, um die legitimen Rechte und Interessen anderer Personen zu schützen, Datenlecks und missbräuchliche Verwendung zu vermeiden, einschließlich, aber nicht beschränkt auf die Einrichtung einer Zugangskontrolle, die Bereitstellung eines klaren und sichtbaren Hinweises, um Personen über die Existenz des Überwachungsbereichs zu informieren, die Bereitstellung der erforderlichen Kontaktinformationen und so weiter.

Haftungsausschluss

- In Bezug auf das Produkt mit Internetzugang erfolgt die Verwendung des Produkts ausschließlich auf eigene Gefahr. Unser Unternehmen ist nicht verantwortlich für anormalen Betrieb, Datenschutzlecks oder andere Schäden, die sich aus Cyberangriffen, Hackerangriffen, Vireninspektionen oder anderen Internet-Sicherheitsrisiken ergeben; Unser Unternehmen wird jedoch bei Bedarf zeitnahe technische Unterstützung leisten.
- Die Überwachungsgesetze variieren von Land zu Land. Überprüfen Sie alle Gesetze in Ihrer Region, bevor Sie dieses Produkt zu Überwachungszwecken verwenden. Wir übernehmen keine Verantwortung für Folgen, die sich aus illegalen Vorgängen ergeben.

Empfehlungen zur Cybersicherheit

- Verwenden Sie ein sicheres Passwort. Ihr Passwort sollte mindestens 8 Zeichen oder eine

Kombination aus Zeichen, Zahlen sowie Groß- und Kleinbuchstaben enthalten.

- Ändern Sie regelmäßig die Passwörter Ihrer Geräte, um sicherzustellen, dass nur autorisierte Benutzer auf das System zugreifen können (empfohlene Zeit beträgt 90 Tage).
- Es wird empfohlen, die Standard-Ports des Dienstes (wie HTTP-80, HTTPS-443 usw.) zu ändern, um das Risiko zu verringern, dass Außenstehende darauf zugreifen können.
- Es wird empfohlen, die Firewall Ihres Routers einzustellen. Beachten Sie jedoch, dass einige wichtige Ports nicht geschlossen werden können (z. B. HTTP-Port, HTTPS-Port, Daten Port).
- Es wird nicht empfohlen, das Gerät für das öffentliche Netzwerk verfügbar zu machen. Wenn es notwendig ist, dem öffentlichen Netzwerk ausgesetzt zu sein, legen Sie bitte die externe Hardware-Firewall und die entsprechende Firewall-Richtlinie fest.
- Es wird nicht empfohlen, die v1- und v2-Funktionen von SNMP zu verwenden.
- Um die Sicherheit des WEB-Client-Zugriffs zu erhöhen, erstellen Sie bitte ein TLS-Zertifikat, um HTTPS zu aktivieren.
- Verwenden Sie die Black- und Whitelist, um die IP-Adresse zu filtern. Dadurch wird verhindert, dass jeder, mit Ausnahme der angegebenen IP-Adressen, auf das System zugreift.
- Wenn Sie mehrere Benutzer hinzufügen, schränken Sie bitte die Funktionen von Gastkonten ein.
- Wenn Sie UPnP aktivieren, wird automatisch versucht, Ports in Ihrem Router oder Modem weiterzuleiten. Es ist wirklich sehr praktisch für Benutzer, aber dies erhöht das Risiko von Datenlecks, wenn das System Ports automatisch weiterleitet. Das Deaktivieren von UPnP wird empfohlen, wenn die Funktion nicht in realen Anwendungen verwendet wird.
- Überprüfen Sie das Protokoll. Wenn Sie wissen möchten, ob auf Ihr Gerät von nicht autorisierten Benutzern zugegriffen wurde oder nicht, können Sie das Protokoll überprüfen. Das Systemprotokoll zeigt Ihnen, mit welchen IP-Adressen Sie sich in Ihrem System angemeldet haben und worauf zugegriffen wurde.

Regulatorische Informationen

FCC-Informationen

Bitte beachten Sie, dass Änderungen oder Modifikationen, die nicht ausdrücklich von der für die Konformität verantwortlichen Partei genehmigt wurden, die Berechtigung des Benutzers zum Betrieb des Geräts erlöschen lassen können.

1. FCC-konformität

Dieses Gerät wurde getestet und entspricht den Grenzwerten für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Diese Grenzwerte sind so konzipiert, dass sie einen angemessenen Schutz vor schädlichen Interferenzen bei einer Installation in Wohngebieten bieten. Dieses Gerät erzeugt, verwendet und kann Hochfrequenzenergie ausstrahlen und kann, wenn es nicht gemäß den Anweisungen installiert und verwendet wird, schädliche Interferenzen bei der Funkkommunikation verursachen. Es gibt jedoch keine Garantie dafür, dass bei einer bestimmten Installation keine Interferenzen auftreten. Wenn dieses Gerät schädliche Interferenzen beim Radio- oder Fernsehempfang verursacht, was durch Aus- und Einschalten des Geräts festgestellt werden kann, wird dem Benutzer empfohlen, zu versuchen, die

Interferenz durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne neu aus oder versetzen Sie sie an einen anderen Ort.
- Vergrößern Sie den Abstand zwischen Gerät und Empfänger.
- Schließen Sie das Gerät an eine Steckdose an, die sich von dem Stromkreis unterscheidet, an den der Empfänger angeschlossen ist.
- Wenden Sie sich an den Händler oder einen erfahrenen Radio-/TV-Techniker, um Hilfe zu erhalten.

2. FCC-Bedingungen:

- Dieses Gerät entspricht Teil 15 der FCC-Bestimmungen. Der Betrieb dieses Produkts unterliegt den folgenden zwei Bedingungen:
- Dieses Gerät darf keine schädliche Schnittstelle verursachen.
- Dieses Gerät muss alle empfangenen Interferenzen akzeptieren, einschließlich Interferenzen, die einen unerwünschten Betrieb verursachen können.

RoHS

Die Produkte wurden in Übereinstimmung mit der EU-RoHS-Richtlinie 2011/65/EU und ihrer Änderungsrichtlinie EU 2015/863 zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten entwickelt und hergestellt.



2012/19/EU (WEEE-Richtlinie): Die Richtlinie über Elektro- und Elektronik-Altgeräte (WEEE-Richtlinie). Um das Umweltmanagement von Elektro- und Elektronik-Altgeräten zu verbessern, ist die Verbesserung der Sammlung, Behandlung und des Recyclings von Elektronik am Ende ihrer Lebensdauer von entscheidender Bedeutung. Daher muss das mit diesem Symbol gekennzeichnete Produkt auf verantwortungsvolle Weise entsorgt werden.

Richtlinie 94/62/EG: Die Richtlinie zielt auf die Bewirtschaftung von Verpackungen und Verpackungsabfällen sowie auf den Umweltschutz ab. Die Verpackungen und Verpackungsabfälle des Produkts, auf die sich dieses Handbuch bezieht, müssen an ausgewiesenen Sammelstellen entsorgt werden, um ein ordnungsgemäßes Recycling und den Umweltschutz zu gewährleisten.

REACH(EG1907/2006): REACH betrifft die Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe, die darauf abzielt, ein hohes Schutzniveau für die menschliche Gesundheit und die Umwelt durch eine bessere und frühere Identifizierung der inhärenten Eigenschaften chemischer Stoffe zu gewährleisten. Das Produkt in diesem Handbuch entspricht den Regeln und Vorschriften von REACH. Weitere Informationen zu REACH finden Sie auf den Websites der GD WACHSTUM oder der ECHA.

Inhaltsverzeichnis

1 Einleitung ..... ¡Error! Marcador no definido.
2 Netzwerkverbindung ..... ¡Error! Marcador no definido.
2.1 LAN 2
2.1.1 Zugriff über IP-Tool 2
2.1.2 Direkter Zugriff über IE 4
2.2 WAN 6
3 Live-Ansicht ..... ¡Error! Marcador no definido.
4 Konfiguration der Netzwerk-Kamera ..... ¡Error! Marcador no definido.
4.1 Systemkonfiguration 11
4.1.1 Grundlegende Informationen ..... **¡Error! Marcador no definido.**
4.1.2 Datum und Uhrzeit 11
4.1.3 Lokale Konfiguration 12
4.2 Image-Konfiguration 13
4.2.1 Display-Konfiguration 13
4.2.2 Video-/Audio-Konfiguration 15
4.2.3 OSD-Konfiguration 16
4.2.4 Videomaske 16
4.2.5 ROI-Konfiguration 17
4.3 Alarmkonfiguration 18
4.3.1 Bewegungserkennung 18
4.3.2 Alarm-Server 20
4.4 Ereigniskonfiguration 21
4.4.1 Objekt verlassen/fehlt ..... **¡Error! Marcador no definido.**
4.4.2 Video-Ausnahme 22
4.4.3 Linienkreuzung 24
4.4.4 Eindringen in die Region 25
4.5 Netzwerkkonfiguration 26
4.5.1 TCP/IP 26
4.5.2 Anschluss ..... **¡Error! Marcador no definido.**
4.5.3 Serverkonfiguration 28
4.5.4 Onvif 29
4.5.5 DDNS 29
4.5.6 SNMP 30
4.5.7 802.1x 31
4.5.8 RTSP 32
4.5.9 UPNP 33
4.5.10 E-Mail 33
4.5.11 FTP 34
4.5.12 HTTPS 36
4.5.13 QoS 37

4.6 Sicherheitskonfiguration 38
4.6.1 Benutzerkonfiguration 38
4.6.2 Online-Benutzer..... **¡Error! Marcador no definido.**
4.6.3 Sperr- und Zulassungslisten..... **¡Error! Marcador no definido.**
4.6.4 Sicherheitsmanagement 40
4.7 Wartungskonfiguration..... 41
4.7.1 Sichern und Wiederherstellen ..... **¡Error! Marcador no definido.**
4.7.2 Neustart 42
4.7.3 Upgrade 42
4.7.4 Betriebsprotokoll 42
5 Suchen..... ¡Error! Marcador no definido.
5.1 Bildersuche 43
5.2 Video-Suche..... 44
Anlage ..... ¡Error! Marcador no definido.
Anhang 1 Fehlerbehebung **46**

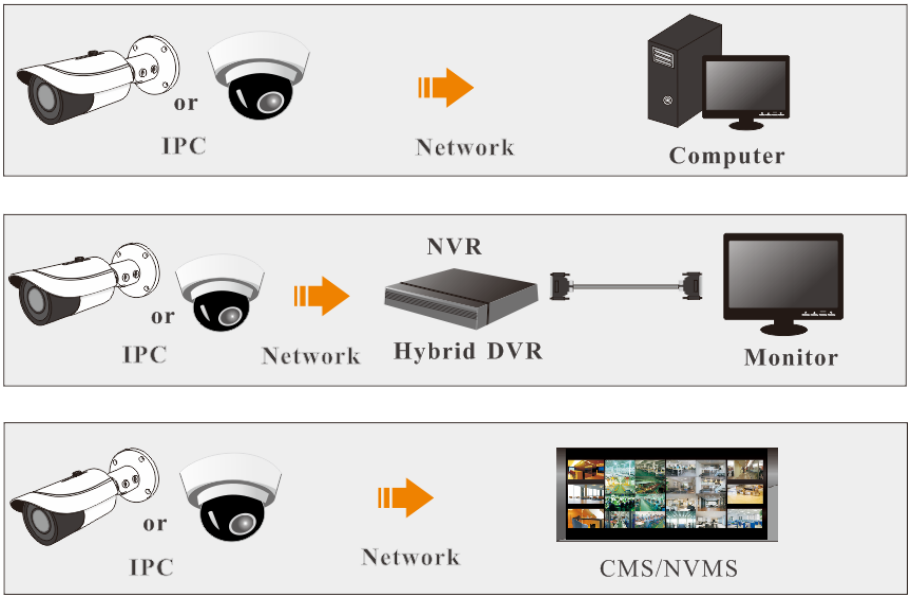
1 Einleitung

Haupteigenschaften

1. ICR-Auto-Umschaltung, Tag / Nacht.
2. Digitaler NR, Digitaler WDR.
3. BLC, HLC, Anti-Flicker, Smart IR, Korridormuster usw.
4. ROI-Codierung.
5. Unterstützt die mobile Überwachung durch Smartphones mit iOS- und Android-Betriebssystem.

- Intelligente Ereignisse: Videoausnahme, Erkennung von Eindringlingen, Erkennung von Linienüberquerungen, Erkennung verlassener/vermisster Objekte.

Überwachungs-Anwendung



2 Netzwerkverbindung

System-Anforderung

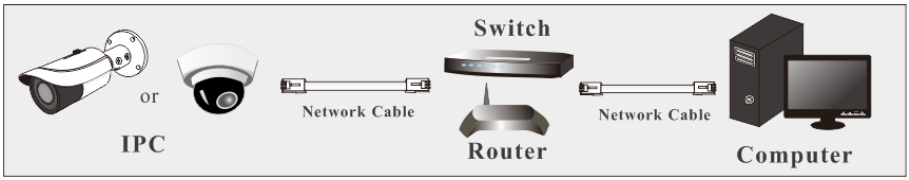
Für den ordnungsgemäßen Betrieb des Produkts sollten die folgenden Anforderungen für Ihren Computer erfüllt sein.
Betriebssystem: Windows 7 Home Basic oder höher.
CPU: 2,0 GHz oder höher.
RAM: 1G oder höher.
Anzeige: Auflösung 1920*1080 oder höher (empfohlen).
Webbrowser: IE (Plug-in erforderlich) / Firefox/Edge/Safari/Google Chrome.
Es wird empfohlen, die neueste Version dieser Webbrowser zu verwenden.
Die Menüanzeige und die Bedienung der Kamera können bei Verwendung des Browsers mit Plug-in oder ohne Plug-in leicht abweichen. Durch die Installation des Plug-Ins werden weitere Funktionen der Kamera angezeigt.
Verbinden Sie die IP-Cam über LAN oder WAN. Nehmen Sie hier zum Beispiel nur den IE-Browser. Die Details lauten wie folgt:

2.1 LAN

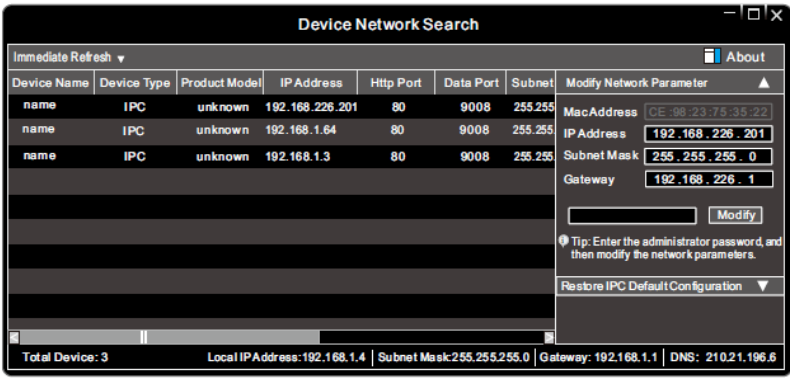
Im LAN gibt es zwei Möglichkeiten, auf die IP-Cam zuzugreifen: 1. Zugriff über IP-Tool; 2. Direkter Zugriff über den IE-Browser.

2.1.1 Zugang über IP-Tool

Netzwerkverbindung:

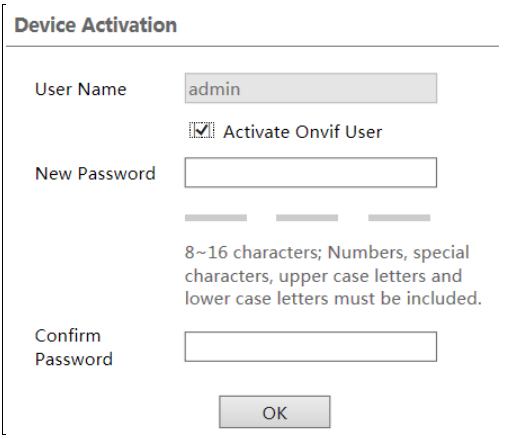


① Setzen Sie sicher, dass der PC und die IP-Cam mit dem LAN verbunden sind und das IP-Tool im PC installiert ist.
② Doppelklicken Sie auf das IP-Tool-Symbol auf dem Desktop, um diese Software wie unten gezeigt auszuführen:

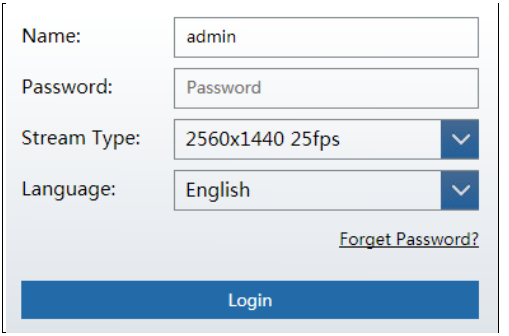


Die Standard-IP-Adresse der Kamera ist: ***192.168.1.64.***

③ Doppelklicken Sie auf die IP-Adresse und das System öffnet den IE-Browser, um IP-CAM zu verbinden. Nachdem Sie die Datenschutzerklärung gelesen haben, überprüfen Sie sie und klicken Sie auf "Bereits gelesen". Aktivieren Sie dann das Gerät.

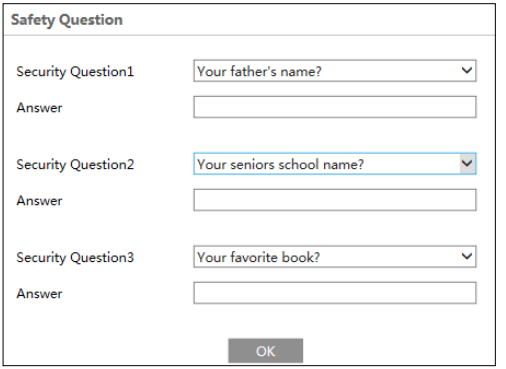


Bitte setzen Sie das Passwort des Admins gemäß Tipp selbst fest.
Wenn "Onvif-Benutzer aktivieren" aktiviert ist, kann der ONVIF-Benutzer gleichzeitig aktiviert werden. Wenn Sie die Kamera über das ONVIF-Protokoll auf der Plattform des Drittanbieters verbinden, können Sie den oben festgelegten Standardbenutzernamen und das oben festgelegte Passwort verwenden, um eine Verbindung herzustellen.
Befolgen Sie danach die Anweisungen zum Herunterladen, Installieren und Ausführen des Aktive X-Steuerelements, wenn Sie dazu aufgefordert werden.
Schließen Sie Ihre Kamera über den IE-Browser erneut an und es erscheint ein Anmeldefeld.



Bitte geben Sie den Benutzernamen (admin) und das Passwort ein. Wählen Sie dann den Stream-Typ und die Sprache nach Bedarf aus.
Stream-Typ: Die Plug-in-freie Live-Ansicht unterstützt nur eine Auflösung von 1080P oder niedriger.

Die Sicherheitsfragen müssen eingestellt werden, nachdem Sie auf die Taste "Anmelden" geklickt haben. Es ist sehr wichtig, dass Sie Ihr Passwort zurücksetzen. Bitte merken Sie sich diese Antworten.



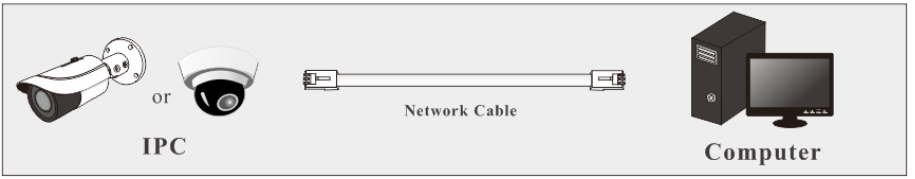
Wenn Sie das Administratorpasswort vergessen haben, können Sie das Passwort zurücksetzen, indem Sie auf **Passwort vergessen** auf der Anmeldeseite. Anschließend können Sie das Passwort zurücksetzen, indem Sie die von Ihnen festgelegten Sicherheitsfragen und -antworten stellen.
Sie können die Frage zur Kontosicherheit während der Aktivierung festlegen oder zu Config→Security→User, klicken Sie **Sicherheitsfrage**, Wählen Sie die Sicherheitsfragen aus und geben Sie Ihre Antworten ein.

2.1.2 Direkter Zugang über IE

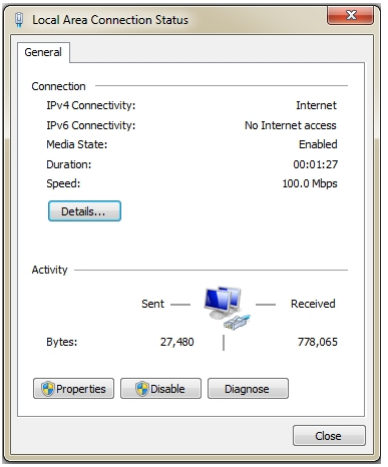
Die Standard-Netzwerkeinstellungen lauten wie folgt:

IP-Adresse: **192.168.226.201**
Subnetzmaske: **255.255.255.0**
Gateway: **192.168.226.1**
HTTP: **80**
Daten-Port: **9008**

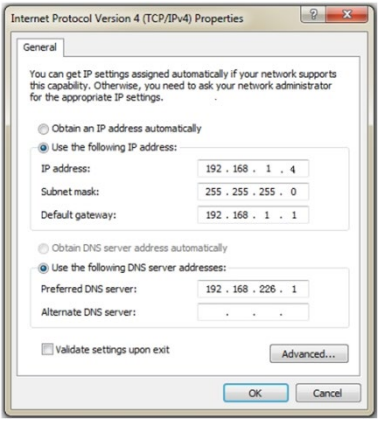
Benutzen Sie die oben genannten Standardeinstellungen, wenn Sie sich zum ersten Mal an der Kamera anmelden. Schließen Sie die Kamera über ein Netzwerkkabel direkt an den Computer an.



① Setzen Sie die IP-Adresse des PCs manuell ein und das Netzwerksegment sollte mit den Standardeinstellungen der IP-Kamera übereinstimmen. Öffnen Sie das Netzwerk- und Freigabecenter. Klicken Sie auf "LAN-Verbindung", um das folgende Fenster zu öffnen.



Wählen Sie "Eigenschaften" und wählen Sie dann je nach tatsächlicher Situation das Internetprotokoll aus (z.B. IPv4). Klicken Sie anschließend auf die Taste "Eigenschaften", um das Netzwerk des PCs festzulegen.



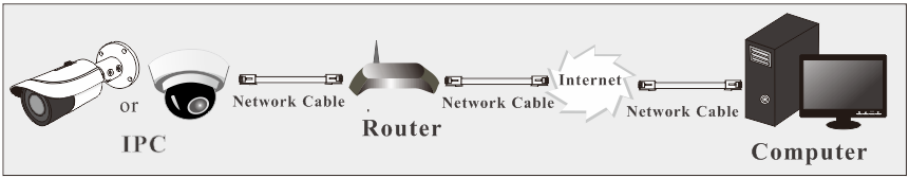
② Öffnen Sie den IE-Browser, geben Sie die Standardadresse von IP-CAM ein und bestätigen Sie.

③ Befolgen Sie die Anweisungen, um das Aktive X-Steuerelement herunterzuladen und zu installieren.

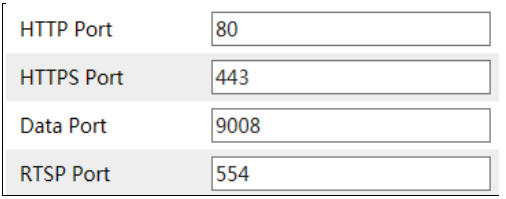
④ Geben Sie den Standardbenutzernamen und das Standardpasswort in das Anmeldefenster ein und geben Sie dann ein, um sie anzuzeigen.

2.2 WAN

➢ **Zugang über den Router oder virtuellen Server**

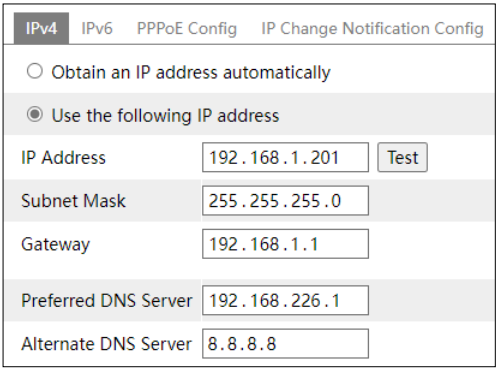


① Stellen Sie sicher, dass die Kamera mit dem lokalen Netzwerk verbunden ist, melden Sie sich dann über LAN bei der Kamera an und gehen Sie zu Config→Network→Port Menü zum Festlegen der Portnummer.



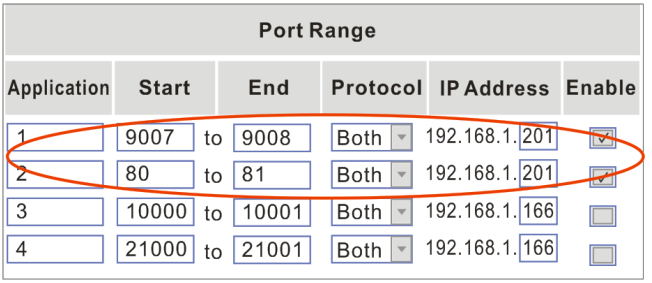
Einrichtung des Ports

② Gehen Sie zu Config →Network→TCP/IP Menü, um die IP-Adresse zu ändern.



IP-Setup

③ Gehen Sie die Verwaltungsschnittstelle des Routers über den IE-Browser auf, um die IP-Adresse und den Port der Kamera auf dem "Virtuellen Server" weiterzuleiten.

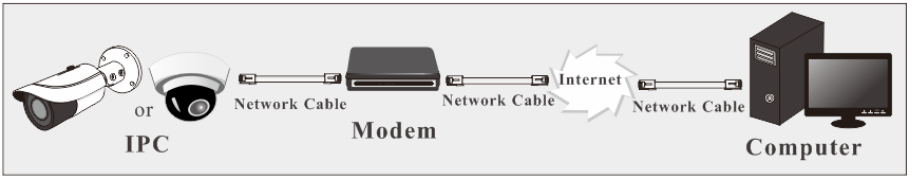


Router-Einrichtung

④ Öffnen Sie den IE-Browser und geben Sie die WAN-IP und den HTTP-Port ein, auf den Sie zugreifen möchten. (Wenn beispielsweise der HTTP-Port auf 81 geändert wird, geben Sie bitte "192.198.1.201:81" in die Adressleiste des Webbrowsers ein, um darauf zuzugreifen.).

➢ **Zugang über PPPoE-Einwahl**

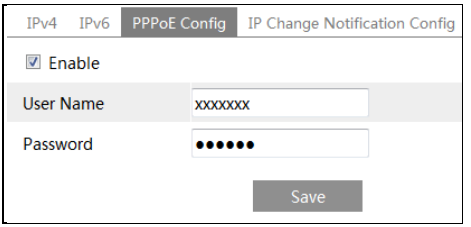
Netzwerkverbindung



Greifen Sie über die automatische PPPoE-Einwahl auf die Kamera zu. Die Einrichtungsschritte sind wie folgt:

① Gehen Sie zu Config→Network→Port Menü zum Festlegen der Portnummer.

② Gehen Sie zu Config →Network→TCP/IP→PPPoE Config Menü. Aktivieren Sie PPPoE und geben Sie dann den Benutzernamen und das Passwort Ihres Internetdienstanbieters ein.

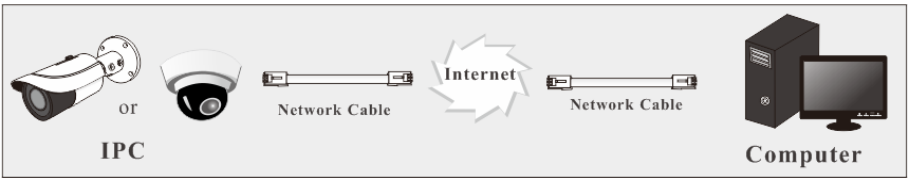


③ Gehen Sie zu Config →Network→DDNS-Menü. Bevor Sie das DDNS konfigurieren, beantragen Sie bitte zunächst einen Domainnamen. Detaillierte Informationen finden Sie in der DDNS-Konfiguration.

④ Öffnen Sie den IE-Browser und geben Sie den Domänennamen und den HTTP-Port ein, auf den Sie zugreifen möchten.

- **Zugang über statische IP**

Netzwerkverbindung



Die Einrichtungsschritte sind wie folgt:

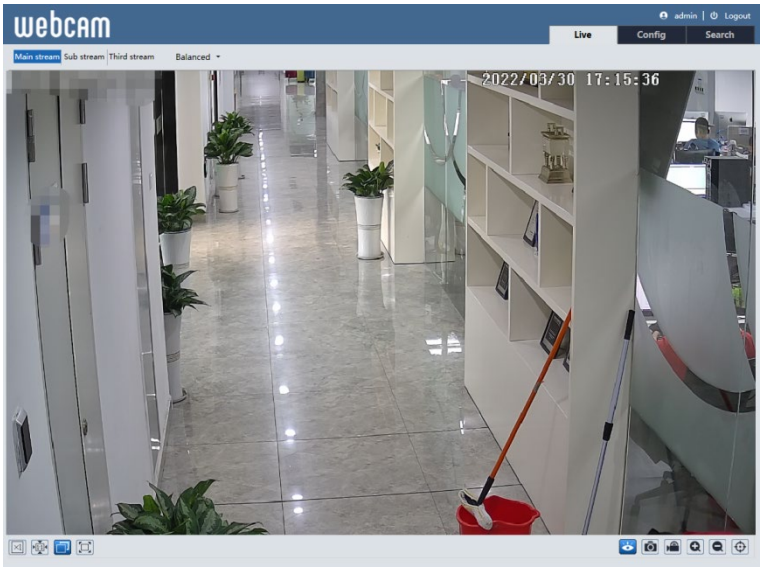
① Gehen Sie zu Config→Network→Port-Menü zum Festlegen der Portnummer.

② Gehen Sie zu Config →Network→TCP/IP Menü zum Festlegen der IP-Adresse. Setzen Sie ein Häkchen bei "Folgende IP-Adresse verwenden" und geben Sie dann die statische IP-Adresse und weitere Parameter ein.

③ Öffnen Sie den IE-Browser und geben Sie die WAN-IP und den HTTP-Port ein, um darauf zuzugreifen.

3 Live-Ansicht

Nach dem Einloggen wird folgendes Fenster angezeigt.



The following table is the instructions of the icons on the live view interface.

Icon	Description	Icon	Description
	Originalgröße		Zoom Aus
	Passen Sie die richtige Skala an		Anzeige von Regelinformationen
	Auto (Fenster füllen)		Bewegungsalarm-Anzeige
	Vollbild		Anzeige für den Szenenwechsel
	Live-Ansicht Start/Stopp		Abnormaler Farbeindikator
	Audio aktiv-/deaktivieren (nur einige Modelle unterstützt)		Anzeige für abnormale Klarheit

Icon	Description	Icon	Description
	Snapshot		Indikator für das Überschreiten der Linie
	Lokale Aufzeichnung Start/Stopp		Intrusion Indikator (Einbruchmelde)
	Zoom Ein		Objekterkennungsanzeige (Objekt verlassen/fehlend)

*Diese intelligenten Alarmanzeigen blinken nur, wenn die Kamera diese Funktionen unterstützt und die entsprechenden Ereignisse aktiviert sind.
*Plug-in-freie Live-Ansicht: Die lokale Aufnahme wird nicht unterstützt und der Schalter für den Vorschaumodus (Echtzeit-/Balanced-/Fluent-Modus) ist ebenfalls nicht verfügbar.
Doppelklicken Sie im Vollbildmodus auf die Maus, um den Vorgang zu beenden, oder drücken Sie die ESC-Taste auf der Tastatur.

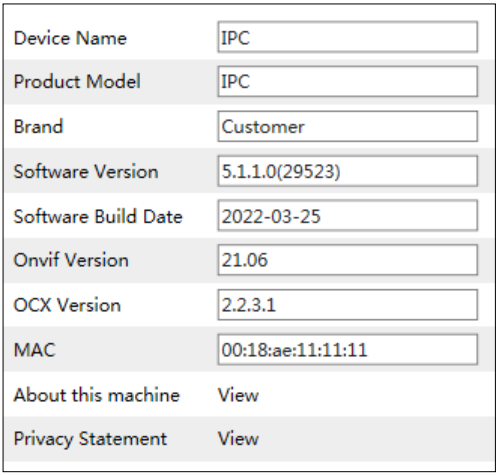
4 Netzwerkkamera-Konfiguration

Wählen Sie im Webcam-Client "Config", um zur Konfigurationsoberfläche zu gelangen.
Hinweis: Klicken Sie ggf. auf die Taste "Speichern", um die Einstellungen zu speichern.

4.1 Systemkonfiguration

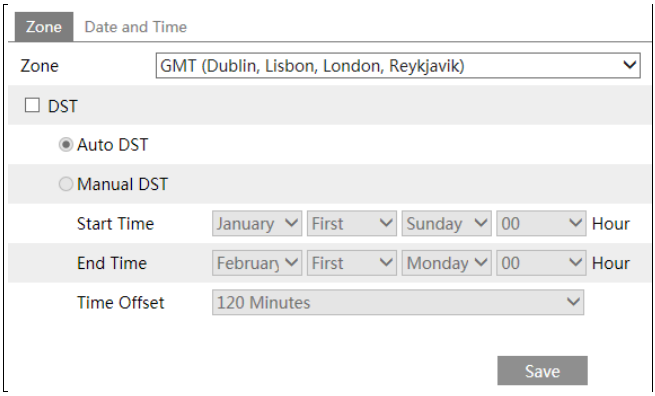
4.1.1 Basisinformation

In der Oberfläche "Basisinformationen" werden die Systeminformationen des Gerätes aufgelistet.



4.1.2 Datum und Uhrzeit

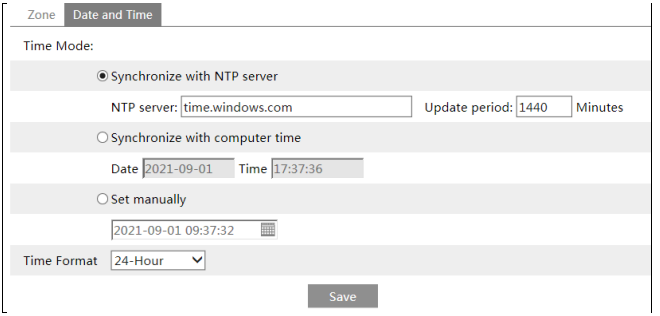
Gehen Sie zu Config→System→Datum und Uhrzeit. Bitte beachten Sie die folgende Schnittstelle.



Wählen Sie die Zeitzone und die Sommerzeit nach Bedarf aus.

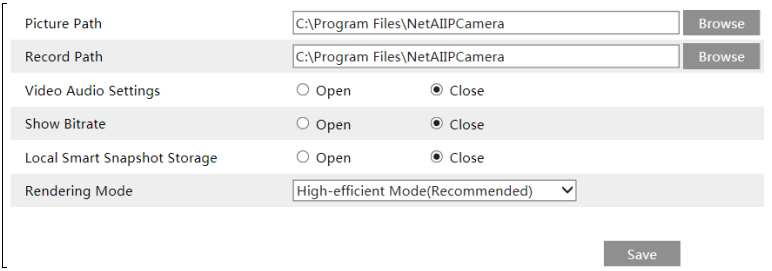
Notiz: Die Zeitzone der Kamera und des Computers muss identisch sein. Es wird empfohlen, die Zeitzone der Kamera entsprechend der Zeitzone des Computers zu ändern. Wenn die Zeitzone des Computers geändert wird, muss der aktuelle Webclient geschlossen werden. Öffnen Sie es dann erneut und melden Sie sich erneut an.

Klicken Sie auf die Registerkarte "Datum und Uhrzeit", um den Zeitmodus und das Zeitformat festzulegen.



4.1.3 Lokale Konfiguration

Gehen Sie zu Config→System→Lokal-Config zum Einrichten des Speicherpfads von aufgenommenen Bildern und aufgezeichneten Videos auf dem lokalen PC. Es gibt auch eine Option zum Aktivieren oder Deaktivieren der Bitratenanzeige in den aufgezeichneten Dateien.



Video-Audio-Einstellungen: Nur einige Modelle unterstützen diese Funktion.

Zusätzlich kann hier "Local Smart Snapshot Storage" aktiviert oder deaktiviert werden. Wenn diese Option aktiviert ist, werden die aufgenommenen Bilder, die durch intelligente Ereignisse ausgelöst werden, auf dem lokalen PC gespeichert.

Rendering-Modus: Der hocheffiziente Modus, der kompatible Modus oder der Modus mit niedriger Effizienz können optional sein.

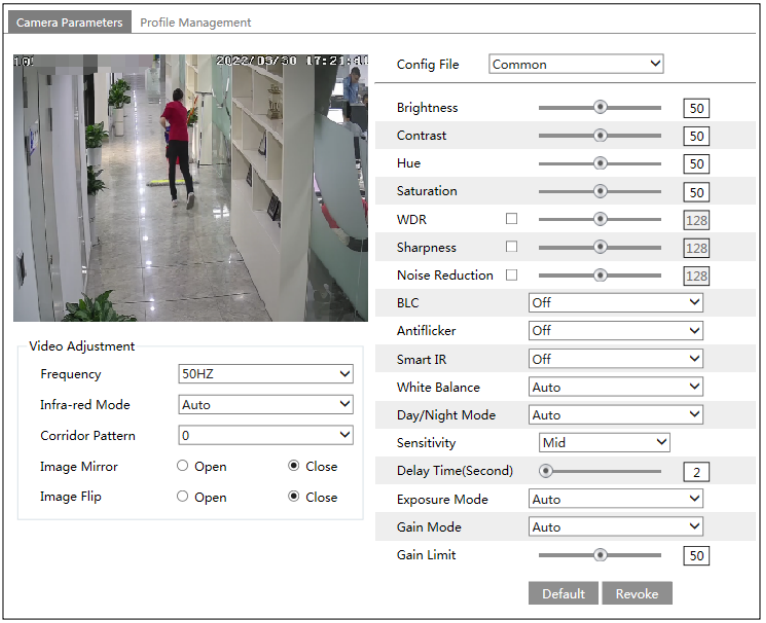
Wenn die Leistung Ihres Computers nicht mit dem IE-Client kompatibel ist oder Ihr Computer keine Grafikkarte hat, wird der Modus mit niedriger Effizienz empfohlen.

Notiz: Wenn Sie über den Webbrowser ohne Plug-in auf Ihre Kamera zugreifen, kann in der obigen Benutzeroberfläche nur Bitrate anzeigen eingestellt werden.

4.2 Image-Konfiguration

4.2.1 Display-Konfiguration

Gehen Sie zu Image→ Display-Oberfläche wie unten gezeigt. Helligkeit, Kontrast, Farbton und Sättigung des Bildes usw. für den gemeinsamen Tag- und Nachtmodus können separat eingestellt werden. Der Bildeffekt ist schnell zu erkennen, wenn die Konfigurationsdatei umgeschaltet wird.



Helligkeit: Setzen Sie die Helligkeitsstufe des Kamerabildes fest.
Kontrast: Setzen Sie den Farbunterschied zwischen den hellsten und dunkelsten Teilen fest.
Farbton: Setzen Sie den Gesamtfarbgrad des Bildes fest.
Sättigung: Setzen Sie den Grad der Farbreinheit fest. Je reiner die Farbe, desto heller das Bild.
WDR: WDR kann die Kamera so einstellen, dass sie ein besseres Bild liefert, wenn sich gleichzeitig sehr helle und sehr dunkle Bereiche im Sichtfeld befinden, indem die Helligkeit des hellen Bereichs verringert und die Helligkeit des dunklen Bereichs erhöht wird.
Die Aufnahme wird für einige Sekunden gestoppt, während der Modus vom Nicht-WDR- in den WDR-Modus wechselt.
Schärfe: Legen Sie die Auflösungsstufe der Bildebene und die Schärfestufe des Bildrandes fest.
Rauschunterdrückung: Verringern Sie das Rauschen und machen Sie das Bild gründlicher. Wenn Sie den Wert erhöhen, wird der Rauschunterdrückungseffekt verbessert, aber die Bildauflösung verringert.
Kompensation der Hintergrundbeleuchtung (BLC):

- Aus: Deaktiviert die Kompensationsfunktion für die Hintergrundbeleuchtung. Das ist der Standardmodus.
- HLC: verringert die Helligkeit des gesamten Bildes, indem die Helligkeit des hellen Bereichs des Bildes unterdrückt und die Größe des Halo-Bereichs verringert wird.

- BLC: Wenn diese Option aktiviert ist, wird die automatische Belichtung entsprechend der Szene aktiviert, so dass das Objekt des Bildes im dunkelsten Bereich deutlich zu sehen ist.

Antiflimmern:

- Aus: Deaktiviert die Anti-Flimmer-Funktion. Dies wird hauptsächlich bei Installationen im Freien verwendet.
- 50 Hz: reduziert Flimmern bei 50 Hz Lichtverhältnissen.
- 60 Hz: reduziert Flimmern bei 60 Hz Lichtverhältnissen.

Smart-IR: Wählen Sie "EIN" oder "AUS". Diese Funktion kann eine Überbelichtung des Bildes effektiv vermeiden, um das Bild realistischer zu machen. Je höher der Pegel ist, desto mehr Überbelichtungskorrektur wird gegeben.

Weißabgleich: Passen Sie die Farbtemperatur automatisch an die Umgebung an.

Tag/Nacht-Modus: Wählen Sie "Auto", "Tag", "Nacht" oder "Timing".

Belichtungsmodus: Wählen Sie "Auto" oder "Manuell". Wenn manuell gewählt wird, kann die digitale Verschlusszeit angepasst werden.

Gain-Modus: Wählen Sie "Auto" oder "Manuell". Wenn "Auto" ausgewählt ist, wird der Verstärkungswert automatisch (innerhalb des eingestellten Verstärkungsgrenzwerts) an die aktuelle Situation angepasst. Wenn "Manuell" ausgewählt ist, muss der Verstärkungswert manuell eingestellt werden. Je höher der Wert, desto heller ist das Bild.

Frequenz: 50 Hz und 60 Hz können optional sein.

Infrarot-Modus: Wählen Sie "Auto", "ON" oder "OFF".

Korridormuster: Korridoransichtsmodi können für Situationen wie lange Flure verwendet werden. 0, 90, 180 und 270 stehen zur Verfügung. Der Standardwert ist 0.

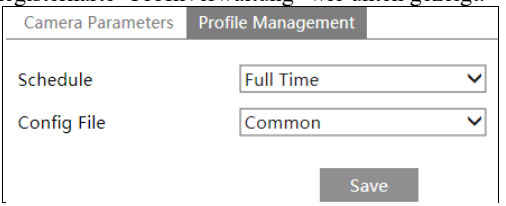
Bildspiegelung: Drehen Sie das aktuelle Videobild horizontal.

Bild spiegeln: Drehen Sie das aktuelle Videobild vertikal.

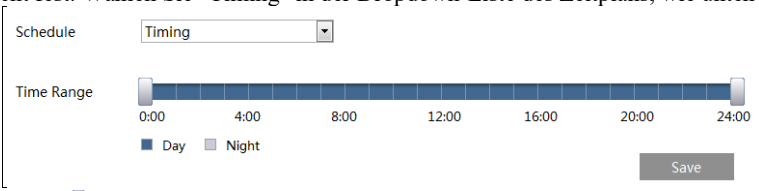
Notiz: Bei einigen Elementen wird die Kamera automatisch neu gestartet, wenn sie ausgewählt/aktiviert ist. Danach wird das Klicken auf die Taste "Standard" nicht wirksam.

Zeitplaneinstellungen von Bildparametern:

Klicken Sie auf die Registerkarte "Profilverwaltung" wie unten gezeigt.



Setzen Sie den vollständigen Zeitplan für den gemeinsamen Tag-, Nacht- und Zeitplan für Tag und Nacht fest. Wählen Sie "Timing" in der Dropdown-Liste des Zeitplans, wie unten gezeigt.

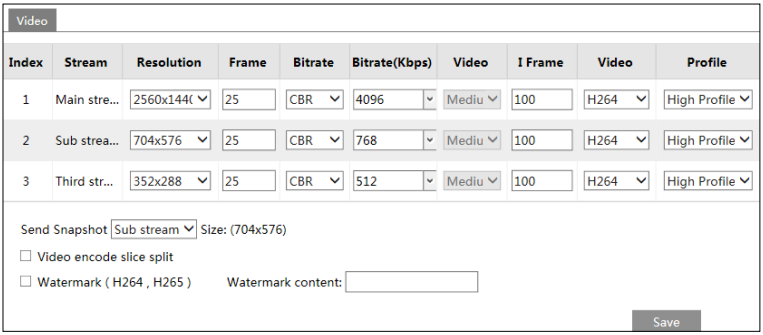


Drücken Sie “ ” Ikon, um die Tages- und Nachtzeit einzustellen. Blau bedeutet Tagzeit und

Leerzeichen bedeutet Nachtzeit. Wenn der aktuelle Modus der Kameraparameter auf Zeitplan eingestellt ist, wechselt der Bildkonfigurationsmodus automatisch zwischen Tag und Nacht gemäß dem Zeitplan.

4.2.2 Video-/Audio-Konfiguration

Gehen Sie zu Image→Video / Audio-Schnittstelle wie unten gezeigt. Stellen Sie in dieser Schnittstelle die Auflösung, die Bildrate, den Bitratentyp, die Videoqualität usw. je nach tatsächlichem Netzwerkzustand ein.



Drei Videostreams einstellbar.

Auflösung: Die Größe des Bildes.

Bildrate: Je höher die Bildrate, desto flüssiger ist das Video.

Bitratentyp: CBR und VBR sind optional. Die Bitrate hängt mit der Bildqualität zusammen. CBR bedeutet, dass unabhängig davon, wie viel Änderung in der Videoszene zu sehen ist, die Komprimierungsbitrate konstant bleibt. VBR bedeutet, dass die Komprimierungsbitrate entsprechend den Szenenänderungen angepasst wird. Bei Szenen, die nicht viel Bewegung aufweisen, wird die Bitrate beispielsweise auf einem niedrigeren Wert gehalten. Dies kann dazu beitragen, die Nutzung der Netzwerkbandbreite zu optimieren.

Bitrate: Sie kann angepasst werden, wenn der Modus auf CBR eingestellt ist. Je höher die Bitrate, desto besser ist die Bildqualität.

Videoqualität: Sie kann angepasst werden, wenn der Modus auf VBR eingestellt ist. Je höher die Bildqualität, desto mehr Bitrate wird benötigt.

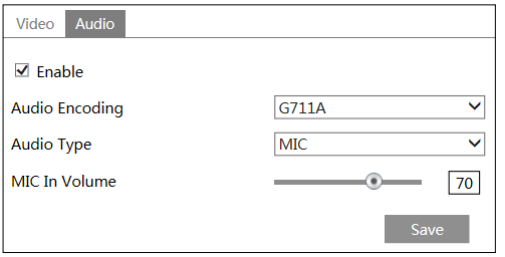
I Frame-Intervall: Legt fest, wie viele Frames zwischen "einer Gruppe von Bildern" zulässig sind. Wenn eine neue Szene in einem Video beginnt, kann bis zum Ende dieser Szene die gesamte Gruppe von Frames (oder Bildern) als eine Gruppe von Bildern betrachtet werden. Wenn sich in der Szene nicht viel bewegt, ist es in Ordnung, den Wert höher als die Bildrate einzustellen, was möglicherweise zu einer geringeren Bandbreitennutzung führt. Wenn der Wert jedoch zu hoch eingestellt ist und das Video eine hohe Bewegungsfrequenz aufweist, besteht die Gefahr, dass Frames übersprungen werden.

Videokomprimierung: MJPEG, H264 oder H265 können optional sein. MJPEG ist für den Haupt Stream nicht verfügbar. Wenn H.265 ausgewählt ist, stellen Sie sicher, dass das Clientsystem H.265 dekodieren kann. Im Vergleich zu H.264 reduziert H.265 die Übertragungsbitrate bei gleicher Auflösung, Bildrate und Bildqualität.

Profil: Für H.264. Basis-, Haupt- und Hochprofile sind wählbar.

Snapshot senden: Legen Sie den Snapshot-Stream fest.
Videokodierungs-Slice-Split: Wenn diese Funktion aktiviert ist, kann auch bei Verwendung des leistungsschwachen PCs ein flüssiges Bild erzielt werden.
Wasserzeichen: Bei der Wiedergabe des lokal aufgenommenen Videos in der Suchoberfläche kann das Wasserzeichen angezeigt werden. Um es zu aktivieren, aktivieren Sie das Wasserzeichenfeld und geben Sie den Wasserzeichentext ein.

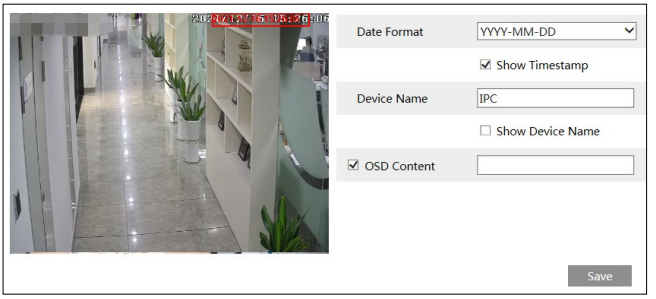
Klicken Sie auf die Taste "Audio", um zur unten gezeigten Benutzeroberfläche zu gelangen. Nur die Modelle mit dem eingebauten MIC unterstützen diese Funktion.



Audiokodierung: G711A und G711U sind wählbar.
Audio-Typ: MIC.
MIC IN-Lautstärke: Wenn MIC ausgewählt ist, kann die MIC IN-Lautstärke eingestellt werden.

4.2.3 OSD-Konfiguration

Gehen Sie zu Image→OSD-Schnittstelle wie unten gezeigt.

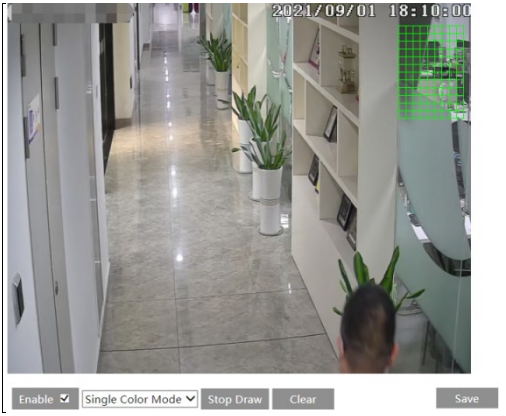


Setzen Sie hier Zeitstempel, Gerätename und OSD-Inhalt fest. Nachdem Sie die entsprechende Anzeige aktiviert und den Inhalt eingegeben haben, ziehen Sie sie, um ihre Position zu ändern. Klicken Sie dann auf die Taste "Speichern", um die Einstellungen zu speichern.

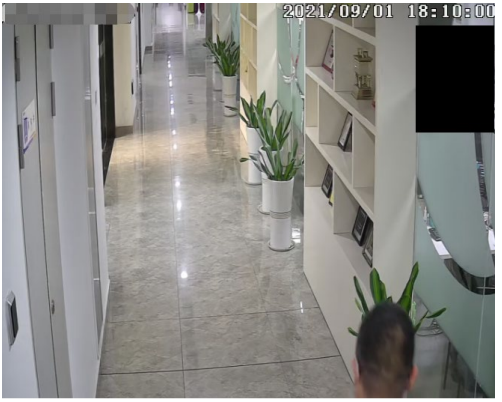
4.2.4 Video-Maske

Gehen Sie zu Image→ Video-Maske-Schnittstelle wie unten gezeigt. Es können maximal 4

Zonen eingerichtet werden.



So richten Sie die Video-Maske ein:
1. Aktivieren Sie die Video-Maske.
2. Klicken Sie auf die Taste "Bereich zeichnen" und ziehen Sie dann die Maus, um den Videomaskenbereich zu zeichnen.
3. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.
4. Kehren Sie zum Live-Modus zurück, um zu überprüfen, ob der Bereich so gezeichnet wurde, wie er im Bild als blockiert angezeigt wird.

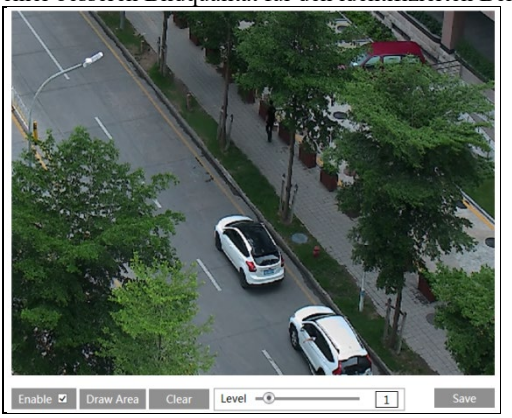


So löschen Sie die Video-Maske:
Klicken Sie auf die Taste "Löschen", um den aktuellen Videomaskenbereich zu löschen.

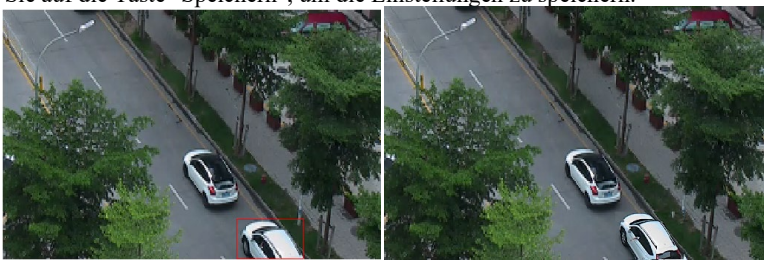
4.2.5 ROI-Konfiguration

Gehen Sie zu Image→ROI-Konfigurationsschnittstelle wie unten gezeigt. Ein Bereich im Bild kann als Interessenbereich festgelegt werden. Dieser Bereich hat eine höhere Bitrate als der

Rest des Bildes, was zu einer besseren Bildqualität für den identifizierten Bereich führt.



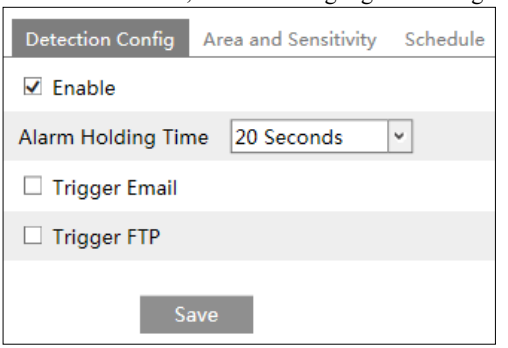
1. Markieren Sie "Aktivieren" und klicken Sie dann auf die Taste "Bereich zeichnen".
2. Ziehen Sie die Maus, um den ROI-Bereich festzulegen.
3. Stellen Sie den Pegel ein.
4. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.



4.3 Alarm-Konfiguration

4.3.1 Bewegungserkennung

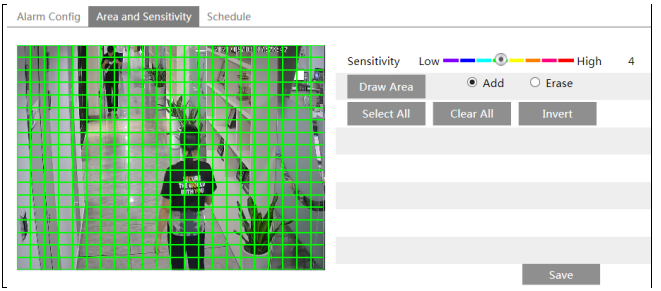
Gehen Sie zu Alarm→Motion Detektion, um die Bewegungserkennungsalarm einzustellen.



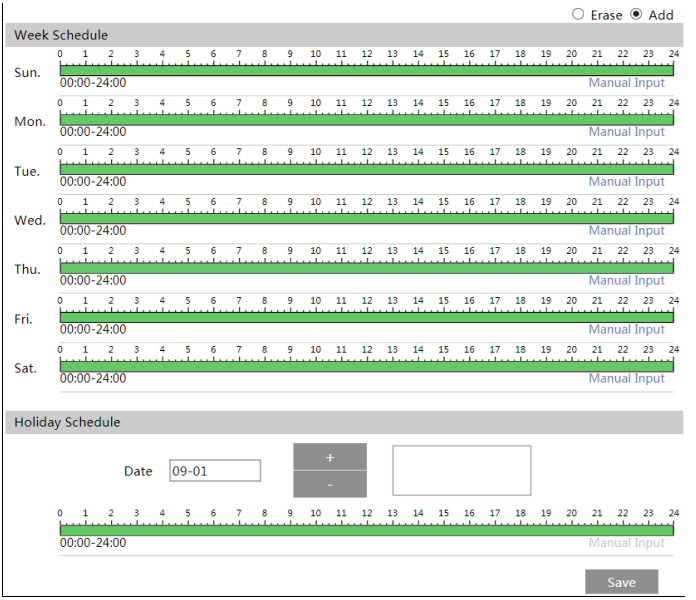
1. Markieren Sie das Feld "Aktivieren", um bewegungsbasierte Alarme zu aktivieren. Wenn das Kontrollkästchen nicht aktiviert ist, sendet die Kamera keine Signale zur Auslösung der bewegungsbasierten Aufzeichnung an den NVR oder das CMS, selbst wenn eine Bewegung

im Video zu sehen ist.
Alarmhaltezeit: Sie bezieht sich auf die Intervallzeit zwischen den benachbarten Bewegungserkennungen. Wenn beispielsweise die Haltezeit des Alarms auf 20 Sekunden eingestellt ist, geht die Kamera, sobald sie eine Bewegung erkennt, in den Alarm und erkennt innerhalb von 20 Sekunden keine andere Bewegung. Wenn während dieses Zeitraums eine andere Bewegung erkannt wird, wird dies als kontinuierliche Bewegung betrachtet. Andernfalls wird es als eine einzelne Bewegung betrachtet.
Trigger-E-Mail: Wenn "Trigger-E-Mail" und "Bild anhängen" aktiviert sind (E-Mail-Adresse muss zuerst in der E-Mail-Konfiguration Schnittstelle), werden die aufgenommenen Bilder und das ausgelöste Ereignis an diese Adressen gesendet.
FTP auslösen: Wenn "FTP auslösen" und "Bild anhängen" aktiviert sind, werden die aufgenommenen Bilder an die FTP-Serveradresse gesendet. Weitere Informationen finden Sie unter FTP-Konfiguration Kapitel für weitere Details.

2. Setzen Sie den Bewegungs-Erkennungsbereich und die Empfindlichkeit ein. Klicken Sie auf die Registerkarte "Bereich und Empfindlichkeit", um zur unten gezeigten Benutzeroberfläche zu gelangen.



Verschieben Sie die Bildlaufleiste "Empfindlichkeit", um die Empfindlichkeit einzustellen. Ein höherer Empfindlichkeitswert bedeutet, dass Bewegungen leichter ausgelöst werden können.
Wählen Sie "Addieren" und klicken Sie auf "Zeichnen". Ziehen Sie die Maus, um den Bewegungserkennungsbereich zu zeichnen. Wählen Sie "Löschen" und ziehen Sie die Maus, um den Bewegungserkennungsbereich zu löschen.
Klicken Sie anschließend auf "Speichern", um die Einstellungen zu speichern.
3. Setzen des Zeitplans für die Bewegungserkennung.



Wochenplan

Stellen Sie den Alarm von Montag bis Sonntag für eine einzelne Woche ein. Jeder Tag ist in Ein-Stunden-Schritten unterteilt. Grün bedeutet geplant. Leer bedeutet ungeplant.

"Addieren": Fügen Sie den Zeitplan für einen bestimmten Tag hinzu. Ziehen Sie die Maus, um die Uhrzeit auf der Zeitleiste einzustellen.

"Löschen": Löscht den Zeitplan. Ziehen Sie die Maus, um die Zeit auf der Zeitleiste zu löschen.

Manuelle Eingabe: Klicken Sie für einen bestimmten Tag darauf, um bestimmte Start- und Endzeiten einzugeben. Dadurch werden weitere Granularitäten (Minuten) hinzugefügt.

Tagesablauf

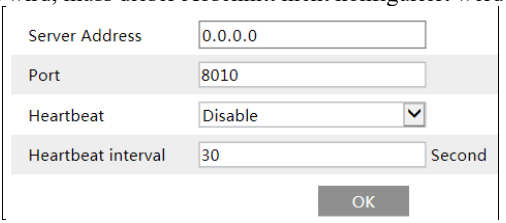
Setzen Sie die Weckzeit für den Alarm an einem bestimmten Tag ein, z. B. an einem Feiertag.

Notiz: Der Feiertagsplan hat Vorrang vor dem Wochenplan**.**

4.3.2 Alarm-Server

Gehen Sie zu Alarm→Alarm-Server-Schnittstelle wie unten gezeigt.

Setzen Sie die Serveradresse, den Port, den Herzschlag und das Herzschlag-Intervall fest. Wenn ein Alarm auftritt, überträgt die Kamera das Alarmereignis an den Alarmserver. Wenn kein Alarmserver benötigt wird, muss dieser Abschnitt nicht konfiguriert werden.



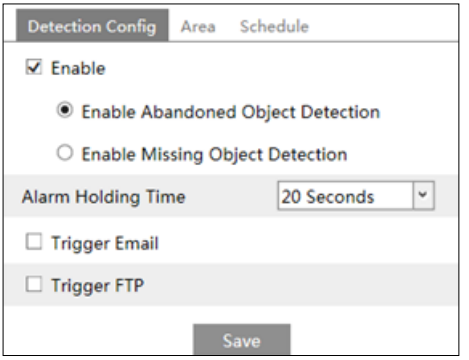
4.4 Ereignis-Konfiguration

Für mehr Genauigkeit finden Sie hier einige Empfehlungen für die Installation.

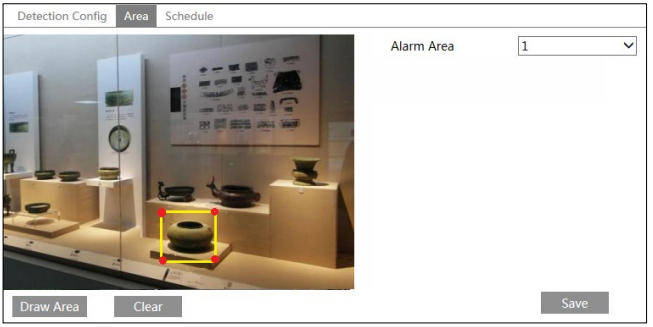
- Kameras sollten auf stabilen Oberflächen installiert werden, da Vibrationen die Erkennungsgenauigkeit beeinträchtigen können.
- Vermeiden Sie es, die Kamera auf reflektierende Oberflächen zu richten (z. B. glänzende Böden, Spiegel, Glas, Seeoberflächen usw.).
- Vermeiden Sie Stellen, die eng sind oder zu viel Schatten haben.
- Vermeiden Sie Szenarien, in denen die Farbe des Objekts der Hintergrundfarbe ähnelt.
- Bitte stellen Sie zu jeder Tages- und Nachtzeit sicher, dass das Bild der Kamera klar und mit ausreichendem und gleichmäßigem Licht ist, um eine Überbelichtung oder zu viel Dunkelheit auf beiden Seiten zu vermeiden.

4.4.1 Verlassenes/vermisstes Objekt

Der Alarm wird aktiviert, wenn die Objekte aus dem vordefinierten Bereich entfernt oder dort zurückgelassen werden.
So setzen Sie die Erkennung verlassener/vermisster Objekte ein:
Gehen Sie zu Config→Event→Object Verlassene/vermisste Schnittstelle wie unten gezeigt.



1. Aktivieren Sie die Erkennung von verlassenen/vermissten Objekten und wählen Sie dann den Erkennungstyp.
Aktivierung der Erkennung verlassener Objekte: Alarme werden ausgelöst, wenn sich noch Gegenstände im vordefinierten Bereich befinden.
Aktivierung der Erkennung fehlender Objekte: Alarme werden ausgelöst, wenn Elemente im vordefinierten Bereich fehlen.
2. Festlegen der Alarmhaltezeit und der Alarmauslöseoptionen. Die Einrichtungsschritte sind die gleichen wie bei der Bewegungserkennung. Weitere Informationen finden Sie unter Bewegungserkennung Kapitel für Details.
3. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.
4. Setzen Sie den Alarmbereich der Erkennung von zurückgelassenen/fehlenden Objekten fest. Klicken Sie auf die Registerkarte "Bereich", um zur unten gezeigten Benutzeroberfläche zu gehen.



Setzen Sie die Nummer des Alarmbereichs ein und geben Sie dann den gewünschten Namen des Alarmbereichs ein. Es kann nur ein Alarmbereich hinzugefügt werden. Klicken Sie auf die Taste "Bereich zeichnen" und klicken Sie dann um den Bereich herum, den Sie als Alarmbereich im Bild festlegen möchten (der Alarmbereich sollte ein geschlossener Bereich sein). Klicken Sie auf die Taste "Zeichnen stoppen", um das Zeichnen zu stoppen. Klicken Sie auf die Taste "Löschen", um den Alarmbereich zu löschen. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.

5. Setzen Sie den Zeitplan für die Erkennung verlassener/vermisster Objekte. Die Einrichtungsschritte für den Zeitplan sind die gleichen wie die Einstellungen für den Bewegungserkennungszeitplan (Sehen Sie Bewegungserkennung Kapitel für Details).

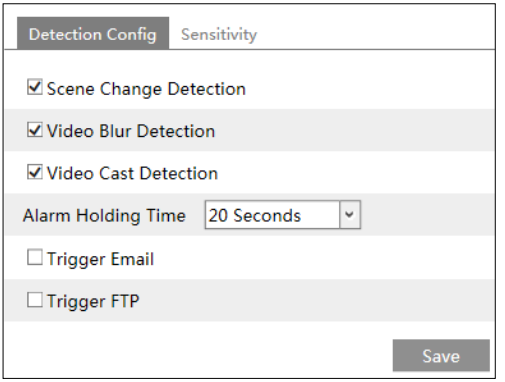
※ Die Konfigurationsanforderungen der Kamera und der Umgebung

1. Der Bereich des Erkennungsobjekts sollte 1/50 bis 1/3 des gesamten Bildes einnehmen.
2. Die Erkennungszeit von Objekten in der Kamera muss 3 bis 5 Sekunden betragen.
3. Der definierte Bereich kann nicht häufig und kontinuierlich abgedeckt werden (wie z.B. Personen- und Verkehrsfluss).
4. Für die Erkennung fehlender Objekte ist es notwendig, dass der gezeichnete Rahmen sehr nahe am Rand des Objekts liegt, um die Empfindlichkeit und Genauigkeit der Erkennung zu erhöhen.
5. Die Erkennung verlassener/vermisster Objekte kann nicht feststellen, wem die Objekte gehören. Zum Beispiel befindet sich ein unbeaufsichtigtes Paket in der Station. Die Erkennung verlassener Objekte kann das Paket selbst erkennen, aber kann nicht feststellen, wem es gehört.
6. Versuchen Sie, die Erkennung von zurückgelassenen/fehlenden Objekten nicht zu aktivieren, wenn sich das Licht in der Szene stark ändert.
7. Versuchen Sie, verlassene/fehlende Objekte nicht zu aktivieren, wenn es komplexe und dynamische Umgebungen in der Szene gibt.
8. Ausreichendes Licht und eine klare Landschaft sind sehr wichtig für die Erkennung von zurückgelassenen/fehlenden Objekten.

4.4.2 Video-Ausnahme

Diese Funktion kann Veränderungen in der Überwachungsumgebung erkennen, die von den externen Faktoren beeinflusst werden.

Setzen Sie die Ausnahmeerkennung fest: Gehen Sie zu Config→Event→Ausnahme-Schnittstelle wie unten gezeigt.



1. Aktivieren Sie die gewünschte Erkennung.

Erkennung von Szenenwechseln: Alarme werden ausgelöst, wenn sich die Szene des Monitorvideos geändert hat.

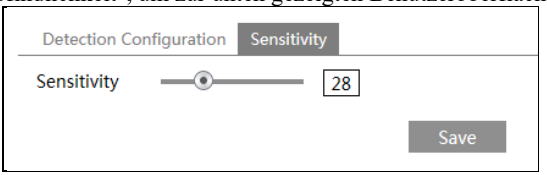
Erkennung von Videounschärfe: Alarme werden aktiviert, wenn das Video unscharf wird.

Erkennung von Videoübertragungen: Alarme werden aktiviert, wenn das Bild aufgrund einer Farbabweichung abnormal ist.

2. Setzen Sie die Haltezeit des Alarms und die Optionen für die Alarmauslösung ein. Die Einrichtungsschritte sind die gleichen wie bei der Bewegungserkennung. Weitere Informationen finden Sie im Kapitel Bewegungserkennung.

3. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.

4. Setzen Sie die Empfindlichkeit der Ausnahmeerkennung fest. Klicken Sie auf die Registerkarte "Empfindlichkeit", um zur unten gezeigten Benutzeroberfläche zu gelangen.



Ziehen Sie den Schieberegler, um den Empfindlichkeitswert festzulegen, oder geben Sie den Empfindlichkeitswert direkt in das Textfeld ein. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.

Der Empfindlichkeitswert der Erkennung von Szenenwechseln: Je höher der Wert ist, desto empfindlicher reagiert das System auf die Amplitude des Szenenwechsels.

Der Empfindlichkeitswert der Videounschärfeerkennung: Je höher der Wert ist, desto empfindlicher reagiert das System auf die Unschärfe des Bildes.

Der Empfindlichkeitswert das Videoübertragung-Erkennung: Je höher der Wert ist, desto empfindlicher reagiert das System auf die Farbverschiebung des Bildes.

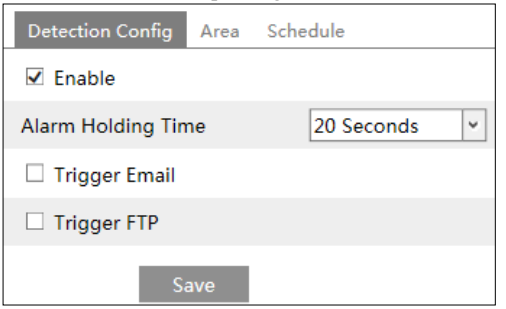
※ Die Anforderungen der Kamera und der Umgebung

1. Die Autofokus-Funktion sollte für die Ausnahmeerkennung nicht aktiviert sein.
2. Versuchen Sie, die Ausnahmeerkennung nicht zu aktivieren, wenn sich das Licht in der Szene stark ändert.
3. Bitte kontaktieren Sie uns für detailliertere Anwendungsszenarien.

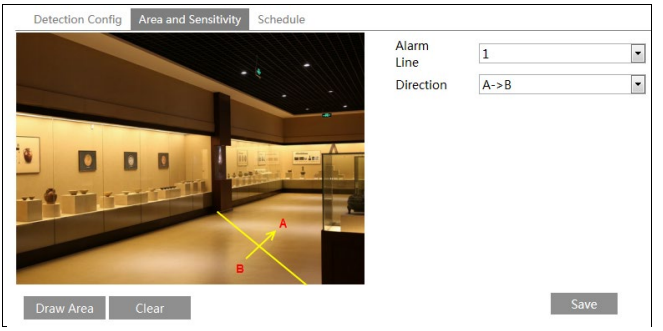
4.4.3 Line Crossing

Linienüberquerung: Alarme werden ausgelöst, wenn jemand oder etwas die vordefinierten Alarmlinien überschreitet.

Gehen Sie zu Config→Event→Linienüberquerung Schnittstelle wie unten gezeigt.



1. Aktivieren Sie den Linienkreuzungsalarm und stellen Sie die Haltezeit des Alarms ein.
2. Setzen Sie die Alarm-Aktivierungsoptionen. Die Einrichtungsschritte sind die gleichen wie bei der Bewegungserkennung. Weitere Informationen finden Sie unter Bewegungserkennung Kapitel für Details.
3. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.
4. Setzen Sie den Bereich und die Empfindlichkeit des Linienkreuzungsalarms ein. Klicken Sie auf die Taste "Bereich und Empfindlichkeit", um zur unten gezeigten Benutzeroberfläche zu gehen.



Setzen Sie die Nummer und Richtung der Alarmlinie fest. Es können vier Zeilen hinzugefügt werden. Es können nicht mehrere Zeilen gleichzeitig hinzugefügt werden.

Richtung: A<->B, A->B und A<-B optional. Dieses gibt die Richtung des Eindringlings an, der die Alarmlinie überquert, die den Alarm aktiviert würde.

A<->B: Der Alarm wird aktiviert, wenn der Eindringling die Alarmlinie von B nach A oder von A nach B überquert.

A->B: Der Alarm wird aktiviert, wenn der Eindringling die Alarmlinie von A nach B quert.

A<-B: Der Alarm wird aktiviert, wenn der Eindringling die Alarmlinie von B nach A quert.

Klicken Sie auf die Taste "Bereich zeichnen" und ziehen Sie dann die Maus, um eine Linie im Bild zu zeichnen. Klicken Sie auf die Taste "Zeichnen stoppen", um das Zeichnen zu beenden. Klicken Sie auf die Taste "Löschen", um die Zeilen zu löschen. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.

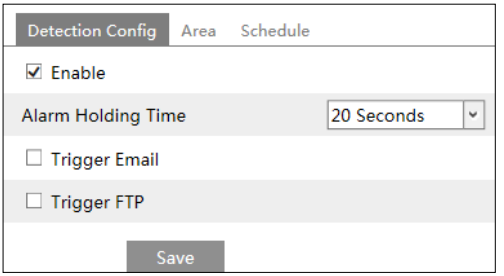
5. Setzen Sie den Zeitplan für den Linienkreuzungsalarm fest. Die Einrichtungsschritte des Zeitplans sind die gleichen wie die Zeitplaneinstellungen für die Bewegungserkennung (Sehen Sie Bewegungserkennung Kapitel für Details).

※ **Konfiguration der Kamera und der Umgebung**

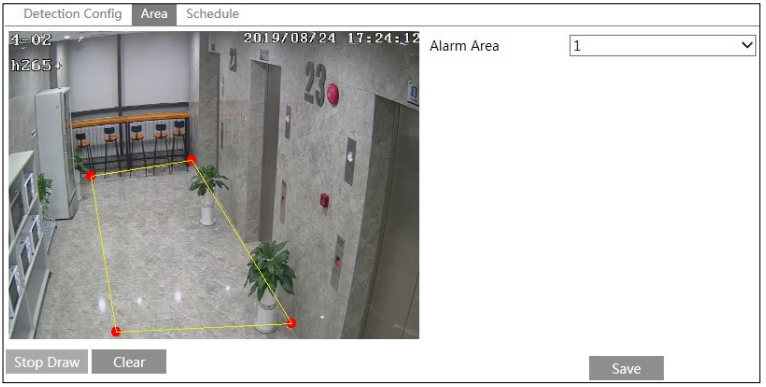
1. Vermeiden Sie die Szenen mit vielen Bäumen oder die Szenen mit verschiedenen Lichtwechseln (z. B. viele blinkende Scheinwerfer). Die Umgebungshelligkeit der Szenen sollte nicht zu niedrig sein.
2. Kameras sollten in einer Höhe von 2,8 Metern oder mehr montiert werden.
3. Halten Sie den Montagewinkel der Kamera bei ca. 45°.
4. Die erkannten Objekte sollten nicht weniger als 1% des gesamten Bildes ausmachen und die größten Größen der erkannten Objekte sollten nicht mehr als 1/8 des gesamten Bildes betragen.
5. Stellen Sie sicher, dass Kameras Objekte im erkannten Bereich mindestens 2 Sekunden lang sehen können, um eine genaue Erkennung zu erzielen.
6. Ausreichendes Licht und eine klare Umgebung sind entscheidend für die Erkennung von Linienüberquerungen.

4.4.4 Region Intrusion

Region Intrusion: Alarme werden aktiviert, wenn jemand oder etwas in die vordefinierten Bereiche eindringt. Diese Funktion kann auf wichtige Überwachungsplätze , Gefahrenbereiche und Sperrgebiete angewendet werden, wie z. B. militärische Verwaltungszonen, Einbrüche, landschaftlich reizvolle Hochgefahrenbereiche, Niemandsbereiche usw.
Gehen Sie zu Config→Event→Intrusion-Schnittstelle wie unten gezeigt.



1. Aktivieren Sie den Alarm zur Erkennung von Eindringlingen in der Region und stellen Sie die Haltezeit des Alarms ein.
2. Legen Sie Alarmaktivierungsoptionen fest. Die Einrichtungsschritte sind die gleichen wie bei der Bewegungserkennung. Weitere Informationen finden Sie unter Bewegungserkennung Kapitel für Details.
3. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.
4. Setzen Sie den Alarmbereich der Einbruchmeldeanlage fest. Klicken Sie auf die Taste "Bereich", um zur unten gezeigten Benutzeroberfläche zu gelangen.



Stellen Sie die Nummer des Alarmbereichs auf der rechten Seite ein. Vier Alarmbereiche können hinzugefügt werden.
Klicken Sie auf die Taste "Bereich zeichnen" und klicken Sie dann um den Bereich herum, den Sie als Alarmbereich im Bild auf der linken Seite festlegen möchten (der Alarmbereich sollte ein geschlossener Bereich sein). Klicken Sie auf die Taste "Zeichnen stoppen", um das Zeichnen zu beenden. Klicken Sie auf die Taste "Löschen", um den Alarmbereich zu löschen. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.
5. Setzen Sie den Zeitplan für die Erkennung von Eindringlingen in der Region fest. Die Einrichtungsschritte des Zeitplans sind die gleichen wie die Zeitplaneinstellungen für die Bewegungserkennung (Sehen Sie Bewegungserkennung Kapitel für Details).

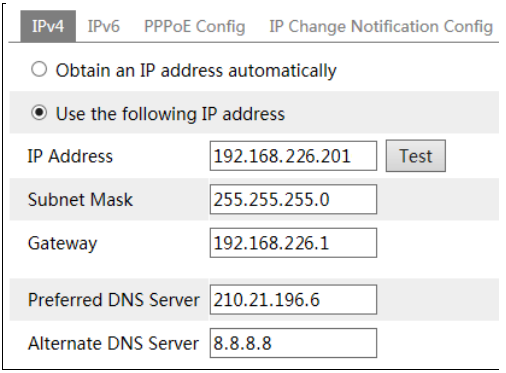
※ **Konfigurationsanforderungen der Kamera und der Umgebung**

1. Vermeiden Sie die Szenen mit vielen Bäumen oder die Szenen mit verschiedenen Lichtwechseln (z. B. viele blinkende Scheinwerfer). Die Umgebungshelligkeit der Szenen sollte nicht zu niedrig sein.
2. Kameras sollten in einer Höhe von 2,8 Metern oder mehr montiert werden.
3. Halten Sie den Montagewinkel der Kamera bei ca. 45°. Legen Sie den Zeitplan für die Erkennung von Eindringlingen in der Region fest. Die Einrichtungsschritte des Zeitplans sind identisch mit den Zeitplaneinstellungen für die Bewegungserkennung
4. Die erkannten Objekte sollten nicht weniger als 1% des gesamten Bildes ausmachen und die größten Größen der erkannten Objekte sollten nicht mehr als 1/8 des gesamten Bildes betragen.
5. Stellen Sie sicher, dass Kameras Objekte im erkannten Bereich mindestens 2 Sekunden lang sehen können, um eine genaue Erkennung zu erzielen.
6. Ausreichendes Licht und eine klare Szenerie sind entscheidend für die Erkennung von Linienüberschreitungen.

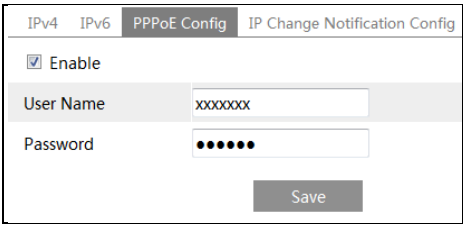
4.5 Netzwerkkonfiguration

4.5.1 TCP/IP

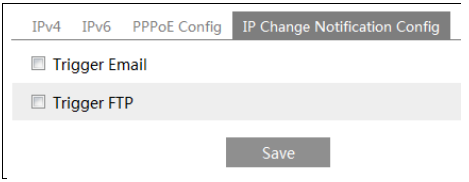
Gehen Sie zu Config→Network→TCP/IP Schnittstelle wie unten gezeigt. Es gibt zwei Möglichkeiten für die Netzwerkverbindung.



Benutzen Sie die IP-Adresse (z. B. IPv4) -Es gibt zwei Möglichkeiten für die IP-Einrichtung: Beziehen Sie automatisch eine IP-Adresse per DHCP und verwenden Sie die folgende IP-Adresse. Bitte wählen Sie bei Bedarf eine der Optionen aus.
Test: Testen Sie die Wirksamkeit der IP-Adresse, indem Sie auf diese Taste klicken.
PPPoE benutzen-Klicken Sie auf die Taste "PPPoE-Konfiguration", um zur unten gezeigten Benutzeroberfläche zu gelangen. Aktivieren Sie PPPoE und geben Sie dann den Benutzernamen und das Passwort Ihres ISP ein.



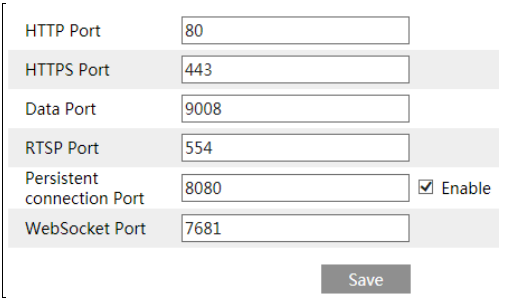
Beide Methoden der Netzwerkverbindung können verwendet werden. Wenn PPPoE für die Internetverbindung verwendet wird, erhält die Kamera eine dynamische WAN-IP-Adresse. Diese IP-Adresse ändert sich häufig. Um benachrichtigt zu werden, kann die IP-Änderungsbenachrichtigungsfunktion verwendet werden.
Klicken Sie auf "IP Change Notifikation Config", um zur unten gezeigten Schnittstelle zu gelangen.



E-Mail aktivieren: Wenn die IP-Adresse des Geräts geändert wird, wird die neue IP-Adresse an die eingerichtete E-Mail-Adresse gesendet.
FTP aktivieren: Wenn die IP-Adresse des Geräts geändert wird, wird die neue IP-Adresse an den eingerichteten FTP-Server gesendet.

4.5.2 Anschluss

Gehen Sie zu Config→Network→ Port-Schnittstelle wie unten gezeigt. HTTP-Port, Daten-Port und RTSP-Port können eingestellt werden.



HTTP-Anschluss: Der Standard-HTTP-Port ist 80. Es kann auf jeden Port geändert werden, der nicht belegt ist.

HTTPS-Anschluss: Der Standard-HTTPS-Port ist 443. Er kann auf jeden Port umgestellt werden, der nicht belegt ist.

Daten-Anschluss: Der Standard-Datenanschluss ist 9008. Bitte ändern Sie es nach Bedarf.

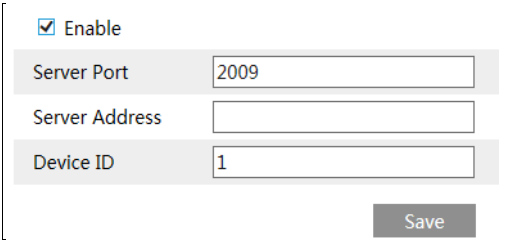
RTSP-Anschluss: Der Standard-Port ist 554. Bitte ändern Sie ihn, wenn nötig.

Persistenter Verbindungsport: Der Port wird für eine dauerhafte Verbindung der Drittanbieterplattform verwendet, um intelligente Daten, wie z. B. Gesichtsbilder, zu übertragen.

WebSocket-Anschluss: Kommunikationsprotokoll-Port für Plug-in-freie Vorschau.

4.5.3 Server-Konfiguration

Diese Funktion wird hauptsächlich zum Anschließen von Netzwerk-Videomanagement-Systemen benutzt.



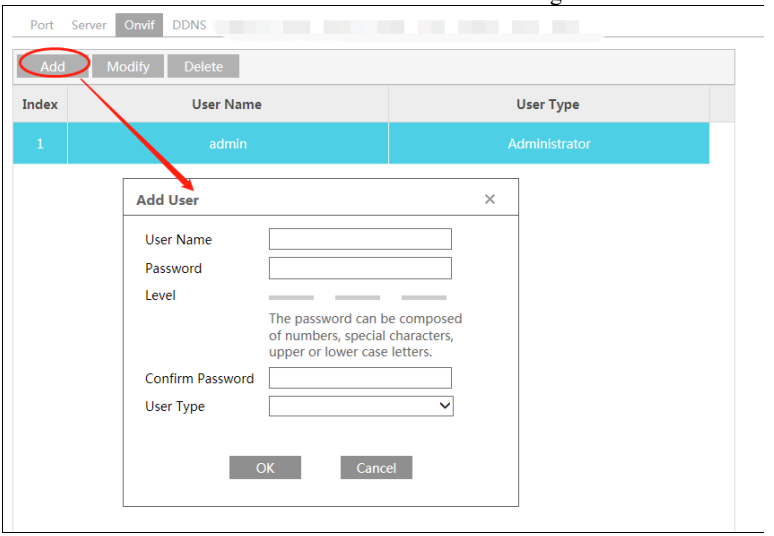
1. Markieren Sie "Aktivieren”.
2. Überprüfen Sie die IP-Adresse und den Port des Übertragungsmedien-Servers im ECMS/NVMS. Aktivieren Sie dann den automatischen Bericht im ECMS/NVMS, wenn Sie ein neues Gerät hinzufügen. Geben Sie als Nächstes die restlichen Informationen des Geräts in das ECMS/NVMS ein. Danach weist das System automatisch eine Geräte-ID zu. Bitte überprüfen Sie es im ECMS/NVMS.
3. Geben Sie die oben genannte Serveradresse, den Serveranschluss und die Geräte-ID in die entsprechenden Felder ein. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.

4.5.4 Onvif

Die Kamera kann über das ONVIF/RTSP-Protokoll gesucht und mit der Plattform des Drittanbieters verbunden werden.

Wenn in der Geräteaktivierungsschnittstelle "Onvif-Benutzer aktivieren" aktiviert ist, kann der ONVIF-Benutzer gleichzeitig aktiviert werden. Wenn Sie die Kamera über das ONVIF-Protokoll auf der Drittanbieterplattform verbinden, können Sie diesen onvif-Benutzer zum Herstellen einer Verbindung verwenden.

Sie können auch neue Benutzer in der Onvif-Oberfläche hinzufügen.

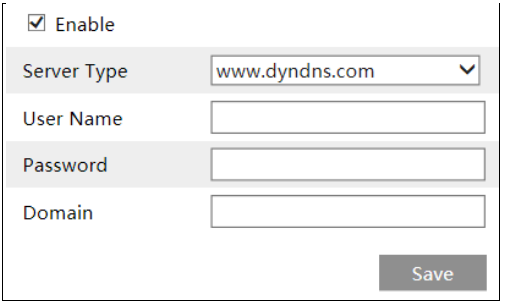


Notiz: Wenn Sie das Gerät zur Drittanbieterplattform mit ONVIF/RTSP-Protokoll hinzufügen, verwenden Sie bitte den Onvif-Benutzer in der obigen Schnittstelle.

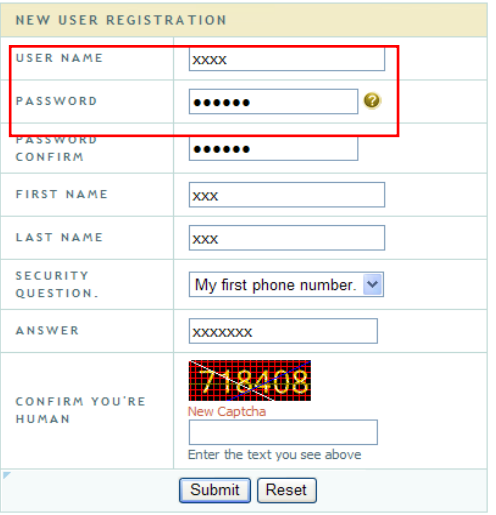
4.5.5 DDNS

Wenn die Kamera mit einer DHCP-Verbindung eingerichtet ist, sollte DDNS für das Internet eingestellt werden.

1. Gehen Sie zu Config→Network→ DDNS.



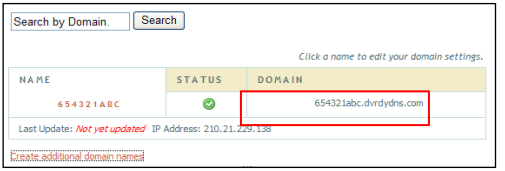
2. Melden Sie sich für einen Domänennamen an. Nehmen Sie zum Beispiel www.dvrdyndns.com.
Geben Sie www.dvrdydns.com in die IE-Adresszeile ein, um die Website zu besuchen. Klicken Sie dann auf die Taste "Registrierung".



Domainnamen erstellen.



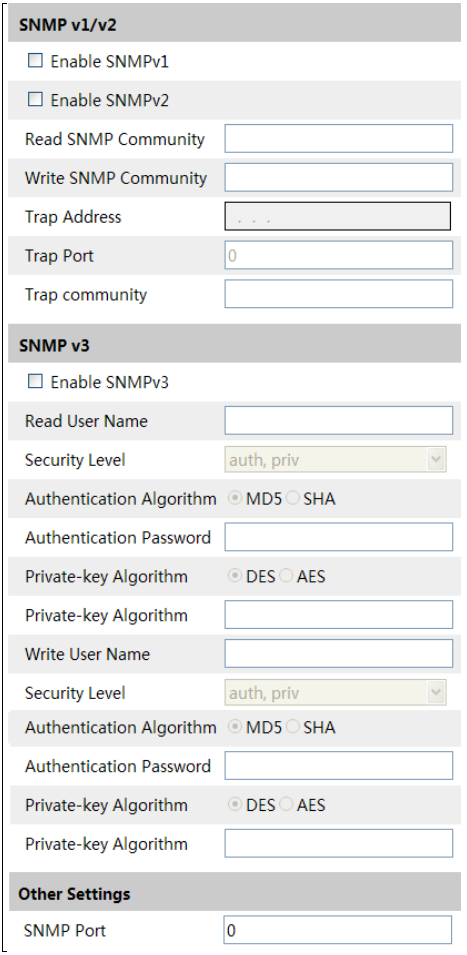
Nachdem der Domainname erfolgreich beantragt wurde, wird der Domainname wie folgt aufgeführt.



3. Geben Sie den Benutzernamen, das Passwort und die Domäne, die Sie beantragen, in der DDNS-Konfigurationsschnittstelle ein.
4. Klicken Sie auf die Taste "Speichern", um die Einstellungen zu speichern.

4.5.6 SNMP

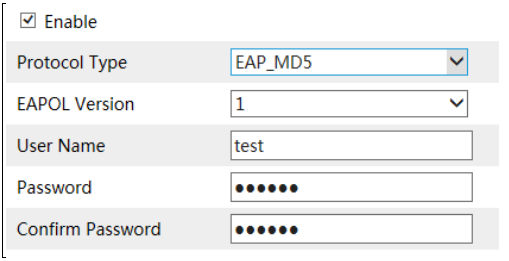
Um den Kamerastatus, Parameter und Alarminformationen abzurufen und die Kamera aus der Ferne zu verwalten, kann die SNMP-Funktion verwendet werden. Bevor Sie SNMP verwenden, installieren Sie bitte ein SNMP-Management-Tool und stellen Sie die Parameter des SNMP ein, z. B. SNMP-Port, Trap-Adresse.
1. Gehen Sie zu Config→Network→SNMP.



2. Aktivieren Sie das entsprechende Kontrollbox für die Version (SNMPv1 aktivieren, SNMPv2 aktivieren, SNMPv3 aktivieren) entsprechend der Version der SNMP-Software, die verwendet werden soll.
3. Setzen Sie die Werte für "SNMP-Community lesen", "SNMP-Community schreiben", "Trap-Adresse", "Trap-Port" usw. fest. Bitte stellen Sie sicher, dass die Einstellungen, mit denen der SNMP-Software übereinstimmen.
Notiz: Bitte benutzen Sie die andere Version entsprechend der von Ihnen gewünschten Sicherheitsstufe. Je höher die Version ist, desto höher ist die Sicherheitsstufe.

4.5.7 802.1x

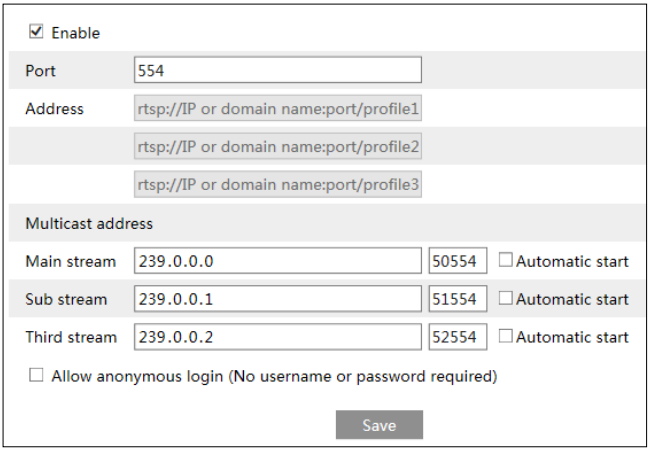
Wenn es aktiviert ist, können die Daten der Kamera geschützt werden. Wenn die Kamera mit dem durch den IEE802.1x geschützten Netzwerk verbunden ist, ist eine Benutzerauthentifizierung notwendig.



Um diese Funktion nutzen zu können, muss die Kamera an einen Switch angeschlossen werden, der das 802.1x-Protokoll unterstützt. Der Switch kann als Authentifizierungssystem zur Identifizierung des Geräts in einem lokalen Netzwerk betrachtet werden. Wenn die mit der Netzwerkschnittstelle des Switches verbundene Kamera die Authentifizierung des Switches bestanden hat, kann über das lokale Netzwerk darauf zugegriffen werden. Protokolltyp und EAPOL-Version: Bitte verwenden Sie die Standardeinstellungen. Benutzername und Passwort: Der Benutzername und das Passwort müssen mit dem Benutzernamen und dem Passwort übereinstimmen, die auf dem Authentifizierungsserver beantragt und registriert wurden.

4.5.8 RTSP

Gehen Sie zu Config→Network→RTSP.



Wählen Sie "Aktivieren", um die RTSP-Funktion zu aktivieren.
Anschluss: Gehen Sie auf den Port des Streaming-Mediums zu. Die Standardnummer ist 554.
RTSP-Adresse: Das RTSP-Adressformat (Unicast), das zum Wiedergeben des Streams in einem Media Player verwendet werden kann.

Multicast-Adresse
Main Stream: Das Adressformat ist
"rtsp://IP Adresse: rtsp port/profile1?transportmode=mcast".
Sub-Stream: Das Adressformat ist
"rtsp://IP Adresse: rtsp port/profile2?transportmode=mcast".
Dritter Stream: Das Adressformat ist
"rtsp://IP Adresse: rtsp port/profile3?transportmode=mcast".
Audio: Nachdem Sie den Haupt-/Sub-Stream in einem VLC-Player eingegeben haben, werden Video und Audio automatisch abgespielt. (Nur das Modell mit dem eingebauten Mikrofon unterstützt diese Funktion)
Wenn "Anonyme Anmeldung zulassen..." aktiviert ist, müssen Sie den Benutzernamen und das Passwort nicht eingeben, um das Video anzuzeigen.
Wenn "Autostart" aktiviert ist, sollten die empfangenen Multicast-Daten in einen VLC-Player eingegeben werden, um das Video abzuspielen.

Notiz:1. Diese Kamera unterstützt die lokale Vorschau über einen VLC-Player. Geben Sie die RTSP-Adresse ein (Unicast oder Multicast, z. B. rtsp://192.168.226.201:554/profile1?transportmode=mcast) in einem VLC-Player, um die gleichzeitige Vorschau mit dem Webclient zu realisieren.

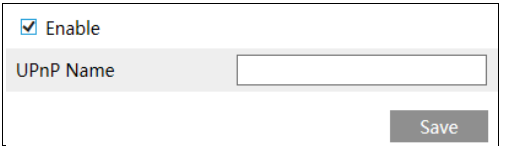
2. Die oben genannte IP-Adresse darf nicht die Adresse von IPv6 sein.

3. Vermeiden Sie die Verwendung derselben Multicastadresse im selben lokalen Netzwerk.

4. Wenn Sie das Video über die Multicast-Streams in einem VLC-Player abspielen, achten Sie bitte auf den Modus des VLC-Players. Wenn es auf den TCP-Modus eingestellt ist, kann das Video nicht abgespielt werden.

4.5.9 UPNP

Wenn diese Funktion aktiviert ist, kann über das LAN schnell auf die Kamera zugegriffen werden.
Gehen Sie zu Config→Network→UPnP. Aktivieren Sie UPNP, und geben Sie dann den UPnP-Namen ein.



4.5.10 E-Mail

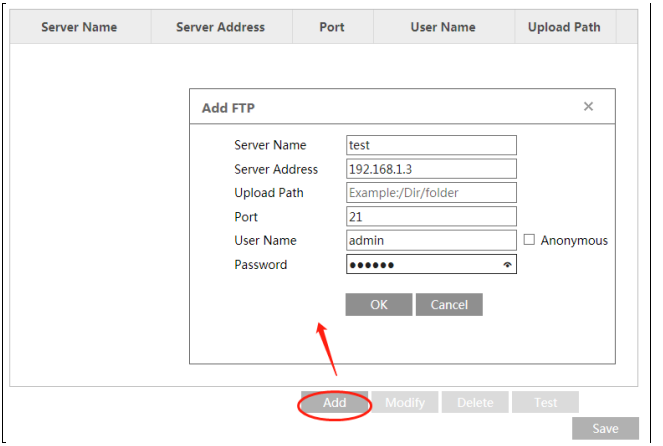
Wenn Sie E-Mail aktivieren müssen, wenn ein Alarm auftritt oder die IP-Adresse geändert wird, stellen Sie bitte zuerst die E-Mail-Adresse hier ein.
Gehen Sie zu Config→Network →E-Mail.



Sender Adresse: E-Mail-Adresse des Absenders.
Benutzername und Passwort: Benutzername und Passwort des Absenders (Sie müssen den Benutzernamen und das Passwort nicht eingeben, wenn "Anonyme Anmeldung" aktiviert ist).
Server-Adresse: Die SMTP-IP-Adresse oder der Hostname.
Wählen Sie den sicheren Verbindungstyp in der Pulldown-Liste "Sichere Verbindung" entsprechend den Anforderungen aus.
SMTP-Anschluss: Der SMTP-Port.
Sendeintervall(e): Das Zeitintervall für das Senden von E-Mails. Wenn sie beispielsweise auf 60 Sekunden eingestellt ist und innerhalb von 60 Sekunden mehrere Bewegungserkennungs-Alarme ausgelöst werden, werden sie nur als ein Alarmereignis betrachtet und es wird nur eine E-Mail gesendet. Wenn ein Bewegungsalarmereignis ausgelöst wird und dann nach 60 Sekunden ein weiteres Bewegungserkennungsalarmereignis ausgelöst wird, werden zwei E-Mails gesendet. Wenn verschiedene Alarme gleichzeitig ausgelöst werden, werden mehrere E-Mails separat gesendet.
Klicken Sie auf die Taste "Testen", um die Verbindung des Kontos zu testen.
Adresse des Empfängers: E-Mail-Adresse des Empfängers.

4.5.11 FTP

Nachdem ein FTP-Server eingerichtet wurde, werden die aufgenommenen Bilder von Ereignissen auf den FTP-Server hochgeladen.
1. Gehen Sie zu Config→Network →FTP.



2. Klicken Sie auf "Hinzufügen", um die FTP-Informationen hinzuzufügen. Klicken Sie anschließend auf "Speichern", um die Einstellungen zu speichern.

Name des Servers: Der Name des FTP-Servers.

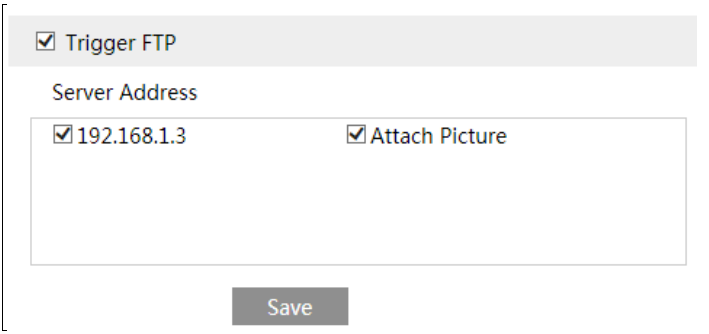
Server-Adresse: Die IP-Adresse oder der Domänenname des FTP.

Upload-Pfad: Das Verzeichnis, in das Dateien hochgeladen werden.

Anschluss: Der Port des FTP-Servers.

User Name and Password: Der Benutzername und das Passwort, die für die Anmeldung beim FTP-Server verwendet werden.

3. Geben Sie in der Ereigniseinstellungsschnittstelle (z. B. Eindringen, Überschreiten von Linien usw.) FTP wie unten gezeigt aus.



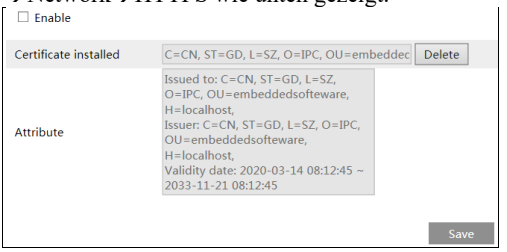
Regel für den FTP-Speicherpfad: /Geräte-MAC-Adresse/Ereignistyp/Datum/Uhrzeit/
Zum Beispiel: Es tritt ein Bewegungsalarm auf
FTP-Dateipfad： \00-18-ae-a8-da-2a\MOTION\2021-01-09\14\
Tabelle mit Ereignisnamen:

Dateiname	Typ des Ereignisses
IP	Änderung der IP-Adresse
BEWEGUNG	Bewegungserkennung
AVD	Video-Ausnahme
STOLPERDRAHT	Erkennung Linienüberquerungen
UMFANG	Erkennung von Eindringlingen in Region
OSC	Objekt verlassen/vermisst

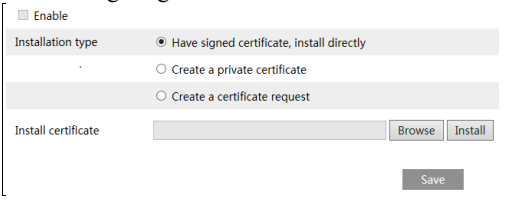
Inhalt der TXT-Datei:
Gerätename: xxx Mac: MAC-Adresse des Geräts Ereignistyp Uhrzeit:
Zum Beispiel:
Gerätename: IPC mac: 00-18-ae-a8-da-2a MOTION Zeit: 2021-03-16 12:20:07

4.5.12 HTTPS

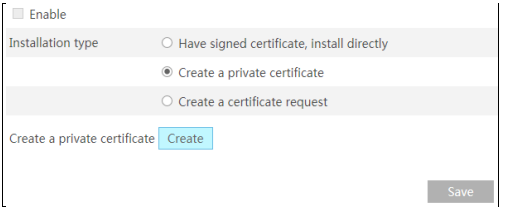
HTTPs ermöglicht die Authentifizierung der Website und schützt die Privatsphäre der Benutzer. Gehen Sie zu Config →Network→HTTPS wie unten gezeigt.



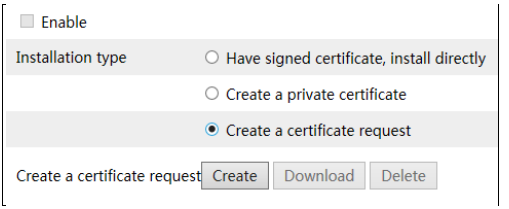
Standardmäßig ist ein Zertifikat installiert, wie oben gezeigt. Aktivieren Sie diese Funktion und speichern Sie sie. Dann kann auf die Kamera zugegriffen werden, indem Sie Folgendes eingeben: https://IP: https-Port über den Webbrowser (z.B. https://192.168.226.201:443).
Ein privates Zertifikat kann erstellt werden, wenn Benutzer das Standardzertifikat nicht verwenden möchten. Klicken Sie auf "Löschen", um das Standardzertifikat zu löschen. Dann wird die folgende Oberfläche angezeigt.



* Wenn ein signiertes Zertifikat vorhanden ist, klicken Sie auf "Durchsuchen", um es auszuwählen, und klicken Sie dann auf "Installieren", um es zu installieren.
* Klicken Sie auf "Privates Zertifikat erstellen", um die folgende Erstellungsschnittstelle aufzurufen.



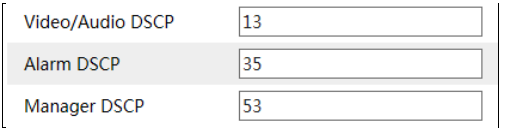
Klicken Sie auf die Taste "Erstellen", um ein privates Zertifikat zu erstellen. Geben Sie das Land (nur zwei Buchstaben verfügbar), die Domäne (IP-Adresse/Domain der Kamera), das Gültigkeitsdatum, das Passwort, die Provinz/das Bundesland, die Region usw. ein. Klicken Sie dann auf "OK", um die Einstellungen zu speichern.
* Klicken Sie auf "Zertifikatsanforderung erstellen", um die folgende Schnittstelle aufzurufen.



Klicken Sie auf "Erstellen", um die Zertifikatsanforderung zu erstellen. Laden Sie dann die Zertifikatsanforderung herunter, und senden Sie sie zur Signatur an die vertrauenswürdige Zertifizierungsstelle. Nachdem Sie das signierte Zertifikat erhalten haben, importieren Sie das Zertifikat auf das Gerät.

4.5.13 QoS

Die QoS-Funktion (Quality of Service) wird verwendet, um unterschiedliche Servicequalitäten für verschiedene Netzwerkanwendungen bereitzustellen. Bei mangelnder Bandbreite sortiert der Router oder Switch die Datenströme und überträgt sie nach ihrer Priorität, um die Netzwerkverzögerung und Netzwerküberlastung mithilfe dieser Funktion zu beheben.
Gehen Sie zu Config→Network→QoS.

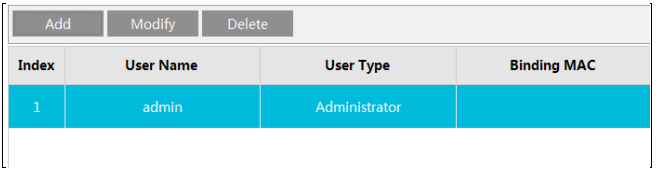


Video/Audio DSCP: Der Bereich reicht von 0 bis 63.
Alarm DSCP: Der Bereich reicht von 0 bis 63.
Manager DSCP: Der Bereich liegt zwischen 0 und 63.
Im Allgemeinen gilt: Je größer die Zahl, desto höher ist die Priorität.

4.6 Sicherheitskonfiguration

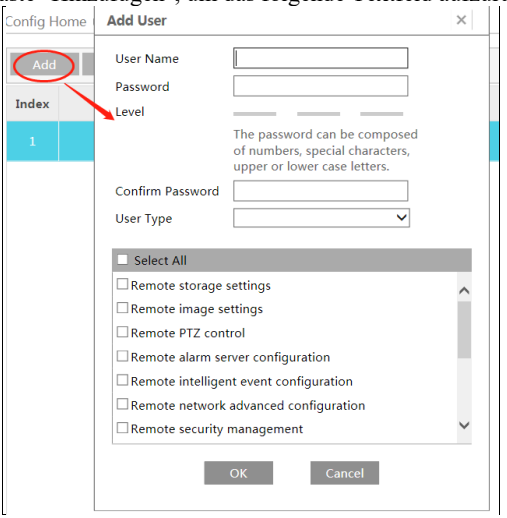
4.6.1 Benutzerkonfiguration

Gehen Sie zu Config→Security→Benutzer-Schnittstelle wie unten gezeigt.



Benutzer addieren:

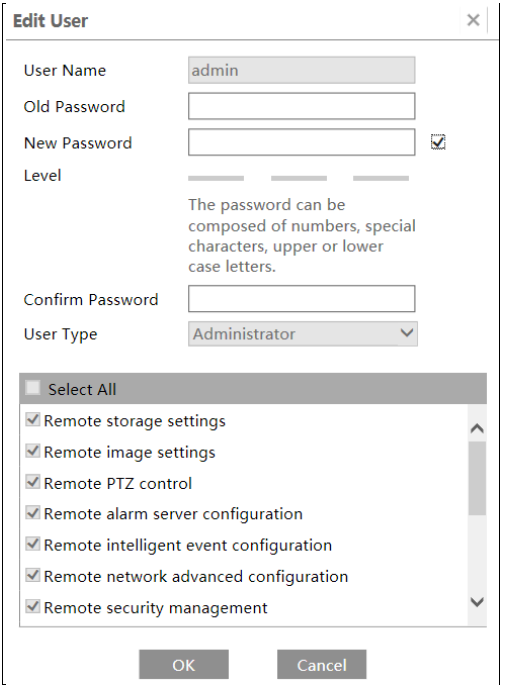
1. Klicken Sie auf die Taste "Hinzufügen", um das folgende Textfeld aufzurufen.



2. Geben Sie den Benutzernamen in das Textfeld "Benutzername" ein.
3. Geben Sie das Passwort in das Textfeld "Passwort" und "Passwort bestätigen" ein. Bitte stellen Sie das Passwort entsprechend den Anforderungen der Passwortsicherheitsstufe ein (Gehen Sie zu Config→Security→Sicherheit Management→Password Security-Schnittstelle zum Festlegen der Sicherheitsstufe).
4. Wählen Sie den Benutzertyp und wählen Sie die gewünschten Benutzerberechtigungen aus.
5. Klicken Sie auf die Taste "OK" und dann wird der neu hinzugefügte Benutzer in der Benutzerliste angezeigt.

Benutzer ändern:

1. Wählen Sie einen Benutzer aus, um das Passwort bei Bedarf im Listenfeld für die Benutzerkonfiguration zu ändern.
2. Das Dialogfeld "Benutzer bearbeiten" wird angezeigt, wenn Sie auf Taste "Ändern" klicken.



3. Geben Sie das alte Passwort des Benutzers in das Textfeld "Altes Passwort" ein.
4. Geben Sie das neue Passwort in Textfelder "Neues Passwort" und "Passwort bestätigen" ein.
5. Wählen Sie die Benutzerberechtigungen für erweiterte oder normale Benutzer aus.
6. Klicken Sie auf die Taste "OK", um die Einstellungen zu speichern.

Benutzer löschen:
1. Wählen Sie den zu löschenden Benutzer im Listenfeld für die Benutzerkonfiguration aus.
2. Klicken Sie auf die Taste "Löschen", um den Benutzer zu löschen.
Notiz: Das Standardadministratorkonto kann nicht gelöscht werden.

Einstellungen für Sicherheitsfragen: Setzen Sie die Fragen und Antworten für den Administrator fest, um das Passwort zurückzusetzen, nachdem Sie das Paswort vergessen haben.

4.6.2 Online-User

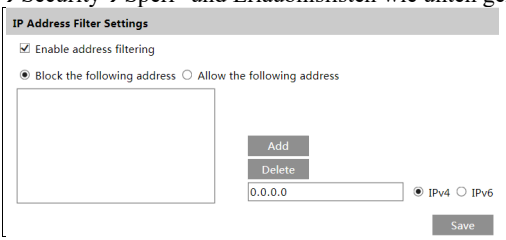
Gehe Sie zu Config→Security→Online-Benutzer, um den Benutzer anzuzeigen, der das Live-Video anzeigt.



Ein Administratorbenutzer kann alle anderen Benutzer (einschließlich anderer Administratoren) rausschmeißen.

4.6.3 Sperr- und Erlaubnislisten

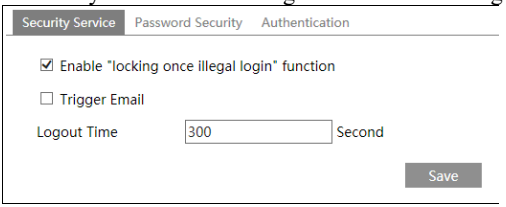
Gehen Sie zu Config→Security→Sperr- und Erlaubnislisten wie unten gezeigt.



Die Einrichtungsschritte sind wie folgt:
Aktivieren Sie das Feld "Adressfilterung aktivieren".
Wählen Sie "Folgende Adresse blockieren / zulassen", IPv4 / IPv6 und geben Sie dann die IP-Adresse in das Adressfeld ein und klicken Sie auf die Taste "Addieren".

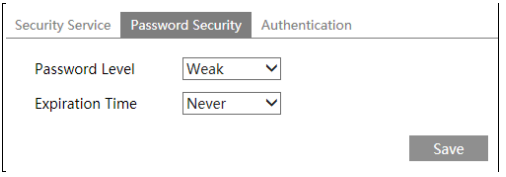
4.6.4 Sicherheitsmanagement

Gehen Sie zu Config→Security→Sicherheitsmanagement wie unten dargestellt.



Um das bösartige Entsperren von Passwörtern zu verhindern, kann hier die Funktion "Sperren nach illegaler Anmeldung" aktiviert werden. Wenn diese Funktion aktiviert ist, wird die Anmeldeschnittstelle nach fünf Fehlversuchen gesperrt. Die Kamera kann nach einer halben Stunde oder nach einem Neustart der Kamera wieder angemeldet werden.
E-Mail aktivieren: Wenn diese Option aktiviert ist, wird eine E-Mail gesendet, wenn Sie sich an- und abmelden oder eine illegale Anmeldesperre auftritt.

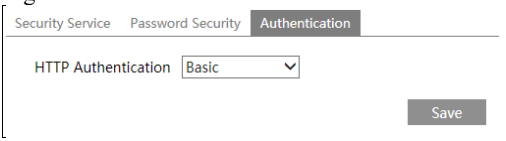
- **Passwort-Sicherheit**



Bitte setzen Sie die Passwortstufe und die Ablaufzeit nach Bedarf ein.
Passwort-Level: Schwach, Mittel oder Stark.
Schwacher-Level: Es können Zahlen, Sonderzeichen, Groß- oder Kleinbuchstaben verwendet werden. Sie können eine davon oder eine beliebige Kombination davon auswählen, wenn Sie das Passwort festlegen.

Mittlere Stufe: 8~16 Zeichen, darunter mindestens zwei der folgenden Kategorien: Zahlen, Sonderzeichen, Groß- und Kleinbuchstaben.
Starkes Level: 8~16 Zeichen. Zahlen, Sonderzeichen, Groß- und Kleinbuchstaben müssen enthalten sein.
Für die Sicherheit Ihres Kontos wird empfohlen, ein sicheres Passwort festzulegen und Ihr Passwort regelmäßig zu ändern.

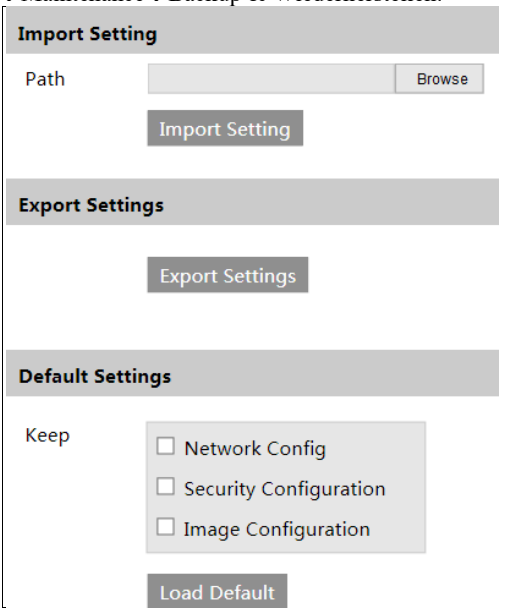
HTTP-Authentifizierung: Basic oder Token ist wählbar.



4.7 Wartungskonfiguration

4.7.1 Backup und Wiederherstellung

Gehen Sie zu Config→Maintenance→Backup & Wiederherstellen.



- **Import- & Exporteinstellungen**

Konfigurationseinstellungen der Kamera können von einer Kamera in eine andere Kamera exportiert werden.
1. Klicken Sie auf "Durchsuchen", um den Speicherpfad für Import- oder Exportinformationen auf dem PC auszuwählen.
2. Klicken Sie auf die Taste "Einstellung importieren" oder "Einstellung exportieren".
Notiz: Das Login-Passwort muss eingegeben werden, nachdem Sie auf die Taste "Einstellungen importieren" geklickt haben.

- **Standardeinstellungen**

Klicken Sie auf die Taste "Standard laden" und überprüfen Sie dann das Passwort, um alle Systemeinstellungen auf die Werkseinstellungen zurückzusetzen, mit Ausnahme derjenigen, die Sie beibehalten möchten.

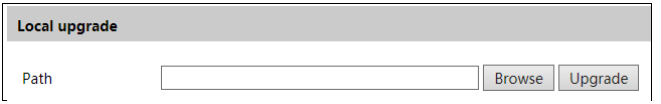
4.7.2 Neustart

Gehen Sie zu Config→Maintenance→Neustart.
Klicken Sie auf die Taste "Neustart" und geben Sie dann das Passwort ein, um das Gerät neu zu starten.

Einstellung für den zeitgesteuerten Neustart:
Falls nötig, kann die Kamera so eingestellt werden, dass sie in einem bestimmten Zeitintervall neu startet. Aktivieren Sie "Zeiteinstellungen", stellen Sie Datum und Uhrzeit ein, klicken Sie auf die Taste "Speichern" und geben Sie dann das Passwort ein, um die Einstellungen zu speichern.

4.7.3 Upgrade

Go to Config→Maintenance→Upgrade. In dieser Schnittstelle kann die Kamera-Firmware aktualisiert werden.

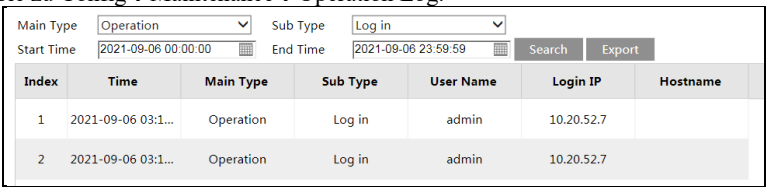


1. Klicken Sie auf die Taster "Durchsuchen", um den Speicherpfad der Upgrade-Datei auszuwählen.
2. Klicken Sie auf die Taste "Upgrade", um das Firmware-Upgrade zu starten.
3. Geben Sie das richtige Passwort ein und das Gerät wird automatisch neu gestartet.

Vorsicht! Schließen Sie während des Upgrades nicht den Browser und trennen Sie die Kamera nicht vom Netzwerk.

4.7.4 Operation Log

So fragen Sie das Protokoll ab und exportieren es:
1. Gehen Sie zu Config→Maintenance→Operation Log.



2. Wählen Sie den Haupt-Typ, den Unter-Typ, die Start- und Endzeit aus.
3. Klicken Sie auf "Suchen", um das Protokoll Log anzuzeigen.
4. Klicken Sie auf "Exportieren", um das Protokoll Log zu exportieren.

5.1 Bildersuche

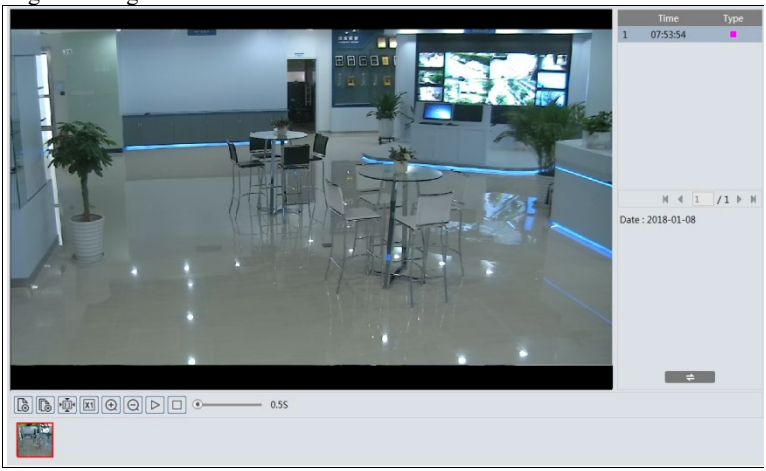
Klicken Sie auf **Suchen**, um zur unten gezeigten Benutzeroberfläche zu gelangen. Bilder, die auf der lokalen PC-Karte gespeichert sind, finden Sie hier.

Notiz: Bei Verwendung des Plug-in-freien Browsers können die lokalen Bilder nicht durchsucht werden.



- **Lokale Bildersuche**

1. Wählen Sie "Bild" – "Lokal".
2. Uhrzeit einstellen: Wählen Sie das Datum aus und wählen Sie die Start- und Endzeit.
3. Klicken Sie hier , um die Bilder zu durchsuchen.
4. Doppelklicken Sie auf einen Dateinamen in der Liste, um die aufgenommenen Fotos wie gezeigt anzuzeigen.



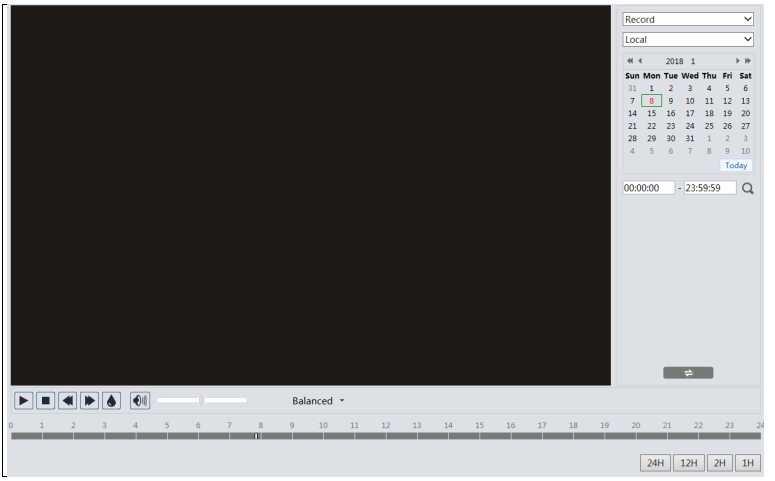
Klicken Sie hier , um zur vorherigen Schnittstelle zurückzukehren.

Die Beschreibungen der Tasten werden wie folgt angezeigt:

Ikone	Beschreibung	Ikone	Beschreibung
	Schließen: Wählen Sie ein Bild aus und klicken Sie auf diese Taste, um das Bild zu schließen.		Alle schließen: Klicken Sie auf diese Taste, um alle Bilder zu schließen.
	Größe anpassen: Klicken Sie hier, um das Bild auf dem Bildschirm anpassen.		Tatsächliche Größe: Klicken Sie auf diese Taste, um die tatsächliche Größe des Bildes anzuzeigen.
	Vergrößern: Klicken Sie auf diese Taste, um die Ansicht digital zu vergrößern.		Auszoomen: Klicken Sie auf diese Taste, um die Ansicht zu verkleinern.
	Abspielen der Diashow: Klicken Sie auf diese Taste, um den Diashow-Modus zu starten.		Stoppen: Klicken Sie auf diese Taste, um die Diashow zu beenden.
5.5S	Abspielgeschwindigkeit: Abspielgeschwindigkeit der Diashow.		

5.2 Video Search

Klicken Sie auf Suchen, um zur unten gezeigten Benutzeroberfläche zu gelangen. Videos, die lokal auf dem PC aufgezeichnet wurden, können über diese Schnittstelle abgespielt werden.
Notiz: Bei Verwendung des Plug-in-freien Browsers können die lokalen Videos nicht durchsucht werden.



1. Wählen Sie "Aufzeichnen" – "Lokal".
2. Suchzeit festlegen: Wählen Sie das Datum aus und wählen Sie die Start- und Endzeit.
3. Klicken Sie hier , um die Bilder zu durchsuchen.
4. Doppelklicken Sie auf einen Dateinamen in der Liste, um die Wiedergabe zu starten.



Ikone	Beschreibung	Ikone	Beschreibung
	Play-Taste. Nachdem Sie das Video angehalten haben, klicken Sie diese Taste, um die Wiedergabe fortzusetzen.		Pause-Taste
	Stopp-Taste		Geschwindigkeit runter
	Geschwindigkeit erhöhen		Anzeige von Wasserzeichen
	Audio aktivieren / deaktivieren; Ziehen Sie den Schieberegler, um die Lautstärke nach dem Aktivieren von Audio anzupassen.		

Appendix 1 Troubleshooting

Wie finden Sie das Passwort?

A: Das Passwort für den ***„admin“*** kann über die Funktion "Sicherheitsfrage bearbeiten" zurückgesetzt werden.

Klicken Sie auf der Anmeldetaste auf "Passwort vergessen" und geben Sie dann die entsprechende Antwort der ausgewählten Frage in das Popup-Fenster ein. Nachdem Sie alle Fragen richtig beantwortet haben, können Sie das Passwort für ***„admin“*** zurücksetzen. Wenn Sie die Antwort auf die Frage vergessen haben, ist dieser Weg ungültig, wenden Sie sich bitte an Ihren Händler, um Hilfe zu erhalten.

B: Die Passwörter anderer Benutzer können vom „***admin***“ zurückgesetzt werden.

Fehler beim Verbinden von Geräten über den IE-Browser.

A: Das Netzwerk ist nicht gut verbunden. Überprüfen Sie die Verbindung und stellen Sie sicher, dass sie richtig angeschlossen ist.

B: Die IP-Adresse ist nicht verfügbar. Setzen Sie die IP-Adresse zurück.

C: Die Webportnummer wurde geändert: Wenden Sie sich an den Administrator, um die richtige Portnummer zu bekommen.

D: Schließen Sie die oben genannten Gründe aus. Wiederherstellung der Standardeinstellung durch IP-Tool.

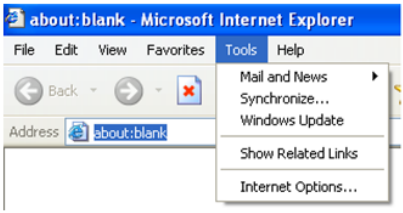
IP-Tool kann Geräte nicht durchsuchen.

Dieses kann durch die Antivirensoftware auf Ihrem Computer verursacht werden. Bitte beenden Sie es und versuchen Sie erneut, das Gerät zu suchen.

IE kann das ActiveX-Steuerelement nicht herunterladen.

A. Der IE-Browser kann so eingerichtet sein, dass ActiveX blockiert wird. Führen Sie die folgenden Schritte aus:

① Öffnen Sie den IE-Browser, und klicken Sie dann auf Extras-----Internetoptionen.

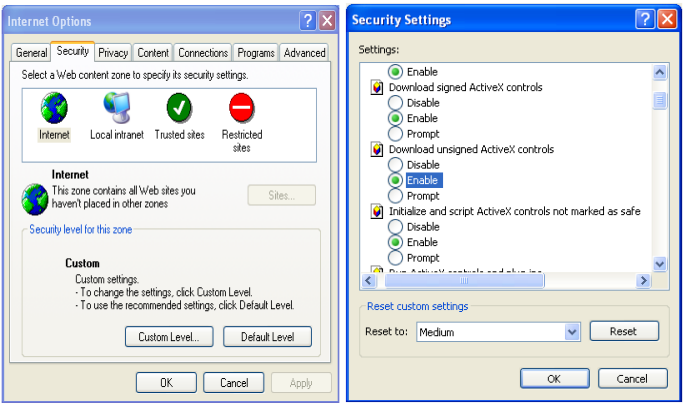


② Wählen Sie Sicherheit------Benutzerdefinierte Stufe....

③ Aktivieren Sie alle Optionen unter "ActiveX-Steuerelemente und Plug-Ins".

④ Klicken Sie auf OK, um die Einrichtung abzuschließen.

B. Andere Plug-ins oder Antivirenprogramme blockieren ActiveX. Bitte deinstallieren oder schließen Sie sie.



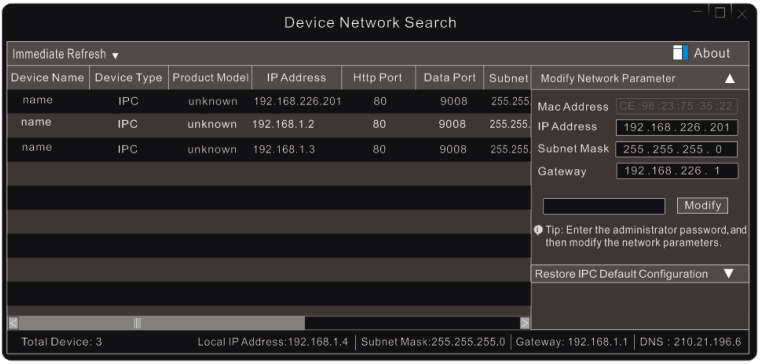
Kein Ton ist zu hören.

A： Das Audioeingabegerät ist nicht angeschlossen. Bitte stellen Sie eine Verbindung her und versuchen Sie es erneut.

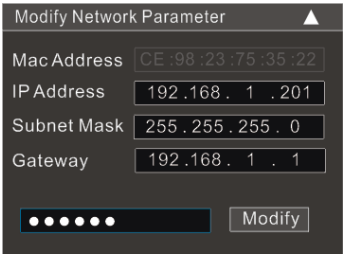
B: Die Audiofunktion ist auf dem entsprechenden Kanal nicht aktiviert. Bitte aktivieren Sie diese Funktion.

Wie ändern Sie die IP-Adresse mit dem IP-Tool?

A: Nachdem Sie das IP-Tool installiert haben, führen Sie es wie unten gezeigt aus.



Die Standard-IP-Adresse dieser Kamera lautet 192.168.1.64. Klicken Sie auf die Informationen der Kamera, die in der obigen Tabelle aufgeführt sind, um die Netzwerkinformationen auf der rechten Seite anzuzeigen. Ändern Sie die IP-Adresse und das Gateway der Kamera und stellen Sie sicher, dass sich die Netzwerkadresse im selben lokalen Netzwerksegment wie die des Computers befindet. Bitte ändern Sie die IP-Adresse Ihres Geräts entsprechend der praktischen Situation.



Zum Beispiel, die IP-Adresse Ihres Computers ist 192.168.1.4. Die IP-Adresse der Kamera muss also auf 192.168.1.X geändert werden. Nach der Änderung geben Sie bitte das Passwort "***admin***" ein, das zuvor in der Schnittstelle zur Geräteaktivierung festgelegt wurde, und klicken dann auf die Taste "Ändern", um die Netzwerkparameter zu ändern.


safire
SMART