Leitfaden zur Netzwerksicherheit für die Smart Line-Serie

Inhaltsübersicht

Anwendbare Produkte: Smart Line-Kameras und NVRs
Zielgruppen: Endnutzer, Integratoren

1. Einleitung

Um die Netzwerksicherheit von Benutzergeräten zu verbessern und illegalen Zugriff, böswillige Angriffe oder Datenlecks zu verhindern, empfehlen wir, dass Benutzer vor der Bereitstellung von Geräten eine umfassende Sicherheitskonfiguration durchführen. In diesem Leitfaden werden empfohlene Konfigurationselemente für Konten, Kennwörter, Dienste, Fernzugriff usw. vorgestellt, die Ihnen helfen, die Sicherheitsrisiken im Netzwerk zu verringern.

2. Erstzugang und Geräteaktivierung

Wenn das Gerät zum ersten Mal eingeschaltet oder auf die Werkseinstellungen zurückgesetzt wird, muss der Benutzer das Gerät aktivieren und ein Administratorpasswort festlegen. Vor der Aktivierung kann das Gerät keine Funktionen ausführen.

2.1 Einstellung eines sicheren Passworts

Passwörter sind der wichtigste Sicherheitsfaktor für Netzwerkgeräte. Bitte verwenden Sie starke Passwörter, die schwer vorhersehbar sind, und bewahren Sie sie sicher auf, damit sie nicht ausspioniert werden können.
Empfohlene Passwortstärke: nicht weniger als 8 Zeichen, einschließlich einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

- **Empfohlener Aktualisierungszyklus:** einmal alle 6 Monate für normale Geschäftsszenarien und einmal pro Monat oder Woche für Hochsicherheitsszenarien.
- **Vermeiden Sie die Verwendung von:** Standardpasswörtern, Benutzernamen mit dem selben Benutzernamen, aufeinanderfolgenden Zeichen (z. B. "123", "321"), sich wiederholenden Zeichen (z. B. "aaa", "555") und schwachen Passwörtern (z. B. admin123).
- **Mindestanforderung an die Passwortstärke:** mindestens 8 Zeichen, einschließlich einer beliebigen Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen

✅ Beispiel: Gd3se!A9

2.2 Sicherheitsfragen und GUID-Datei

- **Zertifikatsdatei:** Es wird empfohlen, die Zertifikatsdatei sofort nach der Aktivierung zu exportieren, damit das Passwort wiederhergestellt werden kann, wenn es vergessen wurde.
- **Sicherheitsfragen:** Es wird empfohlen, 3 Fragen als Backup-Überprüfungsmethode zu konfigurieren. Die Antworten müssen ordnungsgemäß aufbewahrt werden und können nicht mit häufig verwendeten Informationen wiederholt werden.

2.3 Optionen zum Zurücksetzen des Passworts

Wenn der Administrator das Passwort vergisst, kann er es auf folgende Weise zurücksetzen:

Reset-Methode	**Voraussetzungen**	**Empfohlenes Niveau**
Importieren von Zertifikatsdateien	Bei Aktivierung exportiert	✅ empfohlen.
Sicherheitsfragen beantworten	Konfigurierte Ausgaben	✅ empfohlen.
Lokales Zurücksetzen auf Werkseinstellungen	Physischen Zugang haben	⚠ letztes Mittel

2.4 Konfiguration der automatischen Abmeldung

Für die Benutzeroberfläche des Geräts wird empfohlen, die Funktion "Automatische Sperre" zu aktivieren, die den aktuellen Benutzer nach einer gewissen Zeit der Inaktivität automatisch aus dem System ausloggt und so das Risiko verhindert, dass die Konsole weiter benutzt wird.
Empfohlene Dauer: 5 Minuten
Pfad: **System > Allgemein > Automatische Sperre**

Bei WEB-Browsern wird empfohlen, die Funktion "Web Session Timeout" zu aktivieren, die den aktuellen Benutzer automatisch abmeldet, wenn er eine bestimmte Zeit lang nicht mehr im Einstellungsmenü gearbeitet hat.

Wenn Sie das Kontrollkästchen Zeitüberschreitung der Vorschausitzung nicht aktivieren, behält das System die Sitzung bei, wenn sich ein Stream auf der Vorschau- und der Wiedergabeseite befindet, und die automatische Abmeldefunktion ist während dieses Zeitraums ungültig . Wenn diese Option aktiviert ist, wird das System nach Ablauf des Zeitlimits automatisch abgemeldet, auch wenn der Benutzer den Stream auf der Vorschauseite anschaut, ohne die Maus zu betätigen.

IPC verfügt derzeit nicht über eine offene Einstellungsseite, und standardmäßig wird nach 5 Minuten automatisch ein Timeout und eine Abmeldung vorgenommen.

3. Benutzerkonto & Berechtigungsverwaltung

Um Risiken wie Kontomissbrauch und unbefugten Zugriff zu vermeiden, wird empfohlen, Konten- und Berechtigungsstufen entsprechend den Nutzungsszenarien der Benutzer zu konfigurieren.

3.1 Benutzerrollen

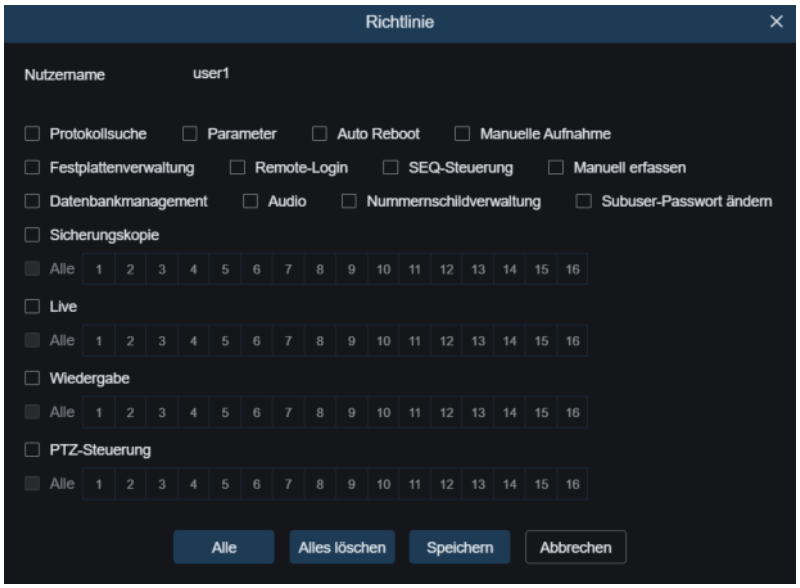
Das System unterstützt standardmäßig die folgenden zwei Arten von Benutzern:

Benutzertyp	**Erlaubnisstufen**	**Typische Verwendungszwecke**
Verwalter	Volle Berechtigungen	Installation, Konfiguration und Upgrade
Gewöhnlicher Benutzer (User)	Mittlere Genehmigungen	Ansicht und Portionskontrolle

3.2 Berechtigungskonfiguration und lokale Vorschaueinstellungen

Administratoren können verfeinerte Betriebsberechtigungen und Vorschaureihen für verschiedene Benutzer festlegen, um zu verhindern, dass nicht relevante Personen auf wichtige Bildschirme zugreifen.

Empfohlener Bedienungspfad:
System > Multi-User > Richtlinie

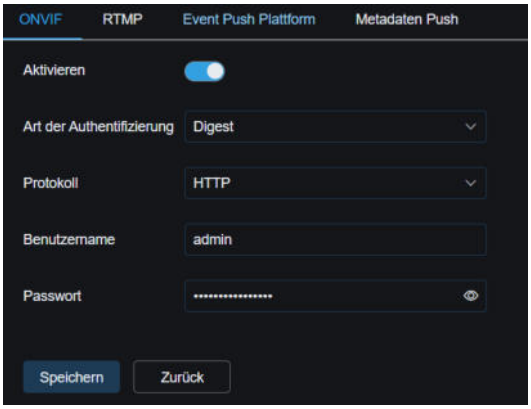


3.3 Leere oder nicht verwendete Konten löschen

Es wird empfohlen, Benutzerkonten, die lange Zeit nicht angemeldet oder ungültig sind, regelmäßig zu bereinigen, um die potenzielle Angriffsfläche zu verringern.

3.4 ONVIF Benutzerverwaltung für den Zugang Dritter

Wenn Sie das ONVIF-Protokoll für die Verbindung mit einer Drittanbieter-Plattform verwenden müssen, empfiehlt es sich, ein spezielles Konto mit eingeschränkten Berechtigungen zu erstellen und das Passwort regelmäßig zu ändern. Derzeit gibt es ein separates Konto für das ONVIF-Protokoll auf dem NVR.
Empfohlener Bedienungspfad:
Netzwerk > Plattformzugang > ONVIF



IP-Kameras haben nicht die Funktion eines separaten ONVIF-Kontos.

4. Fernzugriffskontrolle

Der Fernzugriff ist eines der Hauptziele von Netzwerkangriffen, und es wird empfohlen, mehrere Methoden anzuwenden, um nicht autorisierte Fernverbindungen einzuschränken.

4.1 Sperre bei Login-Fehlern

Um Brute-Force-Angriffe zu verhindern, verfügt das Gerät standardmäßig über eine "Login-Failure-Lock"-Funktion.

Maximale Anzahl von Ausfällen	**Zeit sperren**
5 Mal	5 Minuten

Derzeit gibt es keine UI-Seite für Benutzereinstellungen.

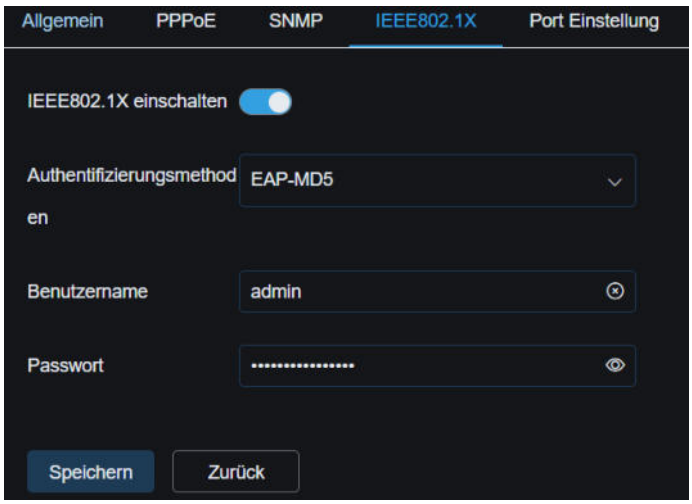
4.2 Ungenutzte Remote-Dienste deaktivieren

Wenn der Cloud-Zugang, der mobile Zugang und andere Funktionen nicht aktiviert sind, empfiehlt es sich, die entsprechenden Protokolle zu deaktivieren:

- **UPnP automatische Portzuordnung** (es wird dringend empfohlen, diese Funktion zu deaktivieren)

4.3 IEEE 802.1x

Die Aufgabe des IEEE 802.1X-Netzwerkauthentifizierungsdienstes besteht darin, die Netzwerkzugriffsrechte von Benutzern oder Geräten durch einen portbasierten Zugriffskontrollmechanismus streng zu überprüfen, um sicherzustellen, dass nur legitime Identitäten nach bestandener Authentifizierung auf Netzwerkressourcen zugreifen können, den Zugriff illegaler Geräte zu kontrollieren und die allgemeine Sicherheitsleistung des Netzwerks zu verbessern.
Die Kamera unterstützt den Standard IEEE 802.1X. Nach der Aktivierung dieser Funktion ist eine Benutzerauthentifizierung erforderlich, wenn die Kamera an ein durch IEEE 802.1X geschütztes Netzwerk angeschlossen wird. Benutzer können 802.1X-Einstellungen konfigurieren, einschließlich Authentifizierungsmethode, EAPOL-Version, Benutzername, Kennwort usw. Einige Authentifizierungsmethoden erfordern den Import von Client-Zertifikaten und Root-Zertifikaten.
Wenn Sie mit der Netzwerkumgebung nicht vertraut sind, empfiehlt es sich, nicht EAP-MD5 und EAP-MSCHAPv2 zu wählen, da diese beiden Authentifizierungsmethoden Sicherheitsrisiken bergen.
Empfohlener Bedienungspfad:
Netzwerk > Allgemein > IEEE802.1X



5. Absicherung von Netzwerkdiensten

Netzwerkdienste sind das Fenster, durch das Geräte mit der Außenwelt interagieren können, und sie sind auch der Einstiegspunkt für Angriffe. Es wird empfohlen, nur die notwendigen Dienste zu aktivieren und ihre Authentifizierungsmethoden und den Zugriffsbereich zu begrenzen.

5.1 Ungenutzte Dienste deaktivieren

Die folgenden Dienste sollten standardmäßig deaktiviert werden, es sei denn, sie sind für das Geschäftsszenario wirklich erforderlich:

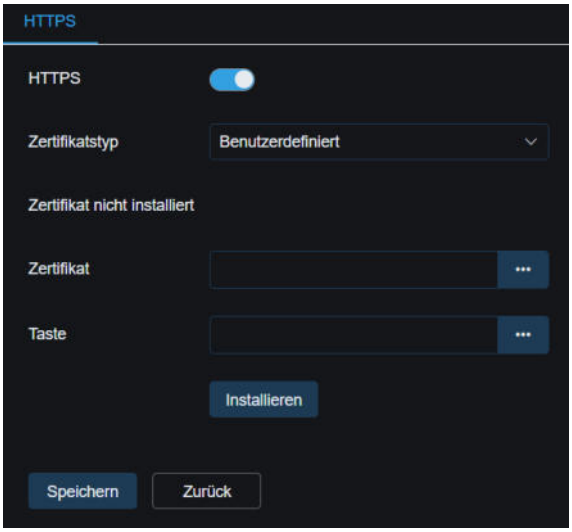
Dienst Name	**beschreiben**	**Empfehlung Status**
Telnet	Klartext-Protokoll für die Fernanmeldung	⚠ Wenn Sie die Zugriffszeit begrenzen müssen, schließen Sie sie rechtzeitig
SSH	Sicheres Terminal-Fernanmeldeprotokoll	⚠ Wenn Sie die Zugriffszeit begrenzen müssen, schließen Sie sie rechtzeitig
UPnP	Automatische Portzuordnung, leicht zu kapern	✖ Deaktivieren Sie

5.2 Aktivieren von HTTPS und Verwalten von Zertifikaten

Es wird empfohlen, den HTTPS-Dienst zu aktivieren und ein vertrauenswürdiges Zertifikat zu konfigurieren. Wir werden https und http standardmäßig aktivieren, aber es wird trotzdem empfohlen, dass Sie https für den Zugriff auf das Gerät verwenden.
Das Gerät ist standardmäßig mit einem selbstsignierten Stammzertifikat und einem Serverzertifikat konfiguriert, und das Zertifikat wird automatisch aktualisiert, wenn es abläuft. Allerdings wird der Browser ein Sicherheitsrisiko anzeigen. **Es wird empfohlen, das Stammzertifikat nach der ersten Anmeldung beim Gerät zu exportieren (es gibt keine Möglichkeit, es jetzt zu exportieren)** und dann das Stammzertifikat über den Browser bei einer vertrauenswürdigen Stammzertifizierungsstelle zu installieren. Wenn Sie sich erneut beim Gerät anmelden, wird der

Browser kein Sicherheitsrisiko anzeigen.

Wenn Sie dem selbstsignierten Zertifikat nicht vertrauen, empfiehlt es sich, ein von einer Zertifizierungsstelle ausgestelltes Zertifikat zu importieren, um die Vertrauenswürdigkeit zu erhöhen. Das Gerät ist nicht mit einem Domänennamen konfiguriert. Wenn Sie eine CSR-Zertifikat-Anwendungsdatei erstellen, wird empfohlen, die IP des aktuellen Geräts im SAN zu konfigurieren.
Empfohlener Operationspfad:
Netzwerk > HTTPS > HTTPS



5.3 Einstellen der Authentifizierungsmethode

Für Dienste wie HTTP, HTTPS, RTSP und ONVIF muss eine sichere Authentifizierungsmethode festgelegt werden.
Zu den gängigen Authentifizierungsmethoden gehören Basic, Digest, Digest-md5, Digest-sha256 usw., und die onvif-Dienste verfügen auch über WSSE-Authentifizierung. Die Basis-Authentifizierung ist die einfachste Authentifizierungsmethode, die Klartext zur Übertragung von Benutzernamen und Kennwörtern verwendet. In unserem System ist die Verwendung der Basic-Authentifizierung streng verboten. Wenn es eine Digest-sha256-Option gibt, wird dringend empfohlen, Digest-sha256 zu wählen.

Mit Ausnahme der separaten Konfigurationsseite für ONVIF-Dienste nutzen andere Dienste eine Reihe von Authentifizierungsdiensten, die derzeit auf der Seite nicht aktiviert sind, und die Standard-Authentifizierungsmethode Digest-md5.

5.4 Offene Ports

Die vom Gerät standardmäßig geöffneten Ports sind wie folgt:

Port	Dienst	Beschreibung	Portmerkmale
80	HTTP	HTTP-Dienst-Port	Der Benutzer kann den Anschluss ändern

Port	Dienst	Beschreibung	Portmerkmale
443	HTTPS	HTTPS-Dienst-Port	Der Benutzer kann den Anschluss ändern
554	RTSP	RTSP-Dienst-Port	Der Benutzer kann den Anschluss ändern
3702	Onvif	Onvif-Geräteerkennung WS-Discovery	Unveränderlich
9555	Multicast	Multicast-Anschluss für den Geräteerkennungsdienst	Unveränderlich

Standardmäßig werden nur die erforderlichen Ports geöffnet. Nach der Anwendung des Dienstes sollten sie rechtzeitig geschlossen werden, damit nicht zu viele Ports offengelegt werden. Gleichzeitig ist es notwendig, die häufig verwendeten Ports wie 80 rechtzeitig in ungewöhnliche Ports zu ändern, um zu verhindern, dass andere die Ports erschöpfend auflisten.

5.5 IP-Filterfunktion

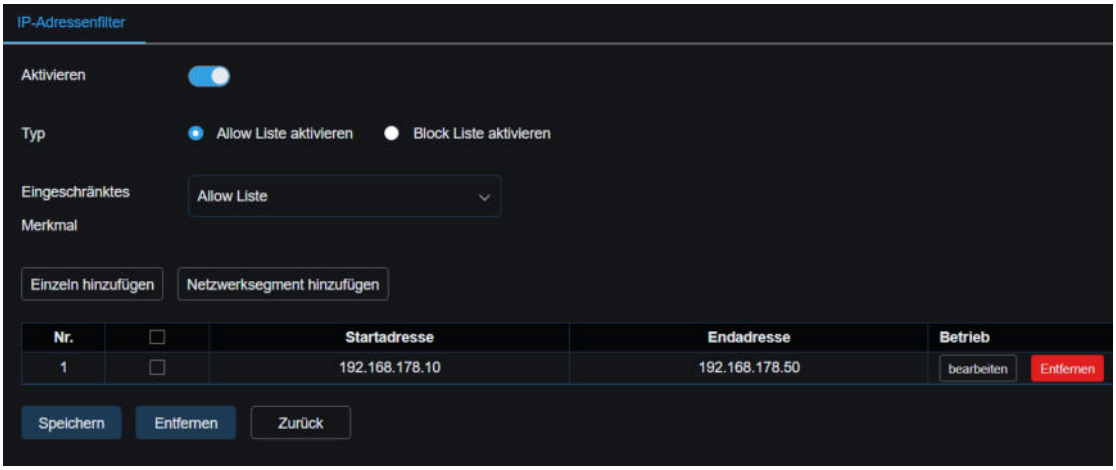
Die Whitelist und die Blacklist in der IP-Filterfunktion sind häufig verwendete Zugangskontrollmechanismen in der Netzsicherheit.

Typ	Zulassungslogik	anwendbare Szenarien
Whitelist	Nur bestimmten IP-Adressen den Zugriff erlauben und allen anderen verweigern	Wird verwendet, wenn Zugriffsquellen (z. B. interne Systeme, API-Schnittstellen) streng eingeschränkt werden müssen oder wenn unbekannte Bedrohungen abgewehrt werden sollen.
Blocklist	Blockieren des Zugriffs von bestimmten IP-Adressen und Zulassen des Zugriffs für alle anderen	Verwenden Sie diese Funktion, wenn Sie bekannte bösartige IP-Adressen (z. B. Quellen für DDoS-Angriffe und Crawler) blockieren oder das Risiko von Fehlblockierungen verringern müssen.

Wenn die IP-Filterung aktiviert ist, wird jeder IP-Adresse oder jedem IP-Bereich, der der Whitelist "allow list" oder der Blacklist "deny list" hinzugefügt wurde, der Zugriff auf das Gerät erlaubt bzw. verweigert.

Empfohlener Bedienungspfad:

Netzwerk > IP-Filter > IP-Filter



5.5 Sicherheit des Dienstes

Standardmäßig sind nur grundlegende Dienste auf dem Gerät aktiviert, darunter: WEB-Dienst, RTSP-Dienst, ONVIF-Dienst, Gerätesuchdienst und P2P-Dienst.

In der Tat unterstützen wir viele Dienste und bieten den Nutzern mehr Auswahlmöglichkeiten. Es wird empfohlen, dass die Benutzer eine sichere Konfiguration bevorzugen, um den Verlust von Informationen zu verhindern.

5.5.1 FTP-Client-Dienst

Wenn Sie die FTP-Client-Funktion starten, können Sie die Alarmbilder und -videos des Geräts auf einen externen FTP-Server übertragen. Die FTP-Kommunikation ist nicht verschlüsselt und birgt Risiken bei der Verwendung. Wenn eine SFTP-Option vorhanden ist, wird empfohlen, SFTP zu verwenden. Andernfalls sollten Sie die FTP-Funktion nach der Verwendung rechtzeitig schließen, um Datendiebstahl zu verhindern.

5.5.2 E-Mail-Dienst

Aktivieren Sie den E-Mail-Dienst, um die Alarmmeldungen und Alarmbilder des Geräts per E-Mail zu versenden. Bei E-Mail-Servern, die keine Verschlüsselung unterstützen, besteht die Gefahr, dass Informationen während der Nutzung verloren gehen. Es wird empfohlen, einen E-Mail-Server zu wählen, der SSL/TLS-Verschlüsselung unterstützt, und dann SSL- oder TLS-Verschlüsselung in der E-Mail-Client-Konfiguration auszuwählen.

5.5.3 SNMP-Dienst

Wenn Sie den SNMP-Dienst aktivieren, können Sie Geräteinformationen abrufen und eine

einheitliche Geräteverwaltung durchführen. Es wird empfohlen, den V3-Dienst anstelle des V1/V2-Dienstes zu wählen, da bei V1/V2 die Daten nicht verschlüsselt sind und die Datenpakete abgehört und manipuliert werden können. Der SNMP V3-Dienst verfügt über Verschlüsselungs- und Manipulationssicherheitsfunktionen.

5.5.4 HTTPS-Dienst

Standardmäßig sind die Dienste http und https aktiviert. Es wird empfohlen, dass Benutzer https für den Zugriff auf das Gerät verwenden.

5.5.5 RTSP OVER HTTPS-Dienst

RTSP-Streams sind nicht verschlüsselt, so dass Benutzerinformationen und Streamdaten in RTSP manipuliert werden können. Es wird empfohlen, RTSP über HTTPS für den Zugriff auf RTSP-Streams zu verwenden, wenn der HTTPS-Dienst aktiviert ist.
Die spezifischen Zugriffsmethoden sind wie folgt:
https://ip:port/rtsp/streaming?channel=1&subtype=A
A: 0(Hauptstrom), 1(Nebenstrom), 2(mobiler Strom)

5.5.6 DDNS-Dienst

Der DDNS-Dienst kann einen Domänennamen für das Gerät beantragen und dann über den Domänennamen auf das Gerät zugreifen, unabhängig davon, wie sich die IP ändert. Der Dienst wird aus Sicherheitsgründen aufgerüstet, und den Benutzern wird empfohlen, ihn nur bei Bedarf zu aktivieren.

5.5.7 RTMP-Dienst

Es handelt sich um einen Streaming-Dienst. Wenn dieser Dienst aktiviert ist, können die Audio- und Videodaten an den RTMP-Streaming-Server des Benutzers übertragen werden. Der Benutzer kann den RTMP-Stream in Echtzeit anzeigen. Dieser Dienst wird derzeit sicherheitstechnisch aufgerüstet, und den Benutzern wird empfohlen, ihn nur bei Bedarf zu aktivieren.

5.5.8 Ereignis-Push-Dienst

Es handelt sich um einen Ereignis-Push-Dienst. Wenn dieser Dienst aktiviert ist, können verschiedene Alarmmeldungen und Bilder an den Server des Benutzers gesendet werden. Dieser Dienst wird derzeit sicherheitstechnisch aufgerüstet, und den Benutzern wird empfohlen, ihn nur bei Bedarf zu aktivieren.

6. Protokolle und Audit-Empfehlungen

Audit-Protokolle sind ein wichtiges Mittel zur Aufdeckung von Anomalien und zum Erhalt von Sicherheitsnachweisen. Audit-Protokolle können die Systemsicherheit verbessern, die Systemstabilität erhöhen und die Sicherheits- und Compliance-Anforderungen der Geräte erfüllen. Bei Sicherheitsgeräten ist der Speicherplatz für die Protokolle begrenzt, daher empfiehlt es sich, sie regelmäßig zu exportieren und zu speichern.

6.1 Protokolltyp

Das Gerät zeichnet die folgenden Arten von Protokollen auf:

Typ	**beschreiben**
System-Protokoll	Systemstart, Herunterfahren, Upgrade, Zeitkalibrierung und andere Systemprotokolle
Konfigurieren der Protokollierung	Das Betriebsprotokoll jeder vom Benutzer auf der Konfigurationsseite vorgenommenen Konfiguration
Alarm-Logbuch	verschiedene Einsatzereignisse, Zugriffsanomalien usw.
Benutzerprotokolle	verschiedene An- und Abmeldungen, Benutzersperren und Änderungen von Benutzerinformationen
Video-Logbuch	Protokolle für Suche, Wiedergabe, Sicherung und andere Vorgänge
AI-Protokoll	Aufzeichnungen über verschiedene AI-Einsatzereignisse auslösen
Speicherprotokolle	Festplatten- und SD-Karten-bezogene Protokolle

6.2 Logsuche und Export

Es wird empfohlen, die Protokolldateien einmal im Monat zu exportieren und sie ordnungsgemäß aufzubewahren:

- Unterstützung der Filterung nach Zeit/Typ;
- Unterstützung für den Export in eine csv-Datei;
- Unterstützt die lokale Anzeige oder das Herunterladen aus der Ferne.

7. Systemwiederherstellung und Upgrade-Vorschläge

Um einen langfristig sicheren und stabilen Betrieb des Systems zu gewährleisten, wird empfohlen, regelmäßig die Firmware-Version zu überprüfen, Sicherheits-Upgrades durchzuführen und den Systemwiederherstellungsmechanismus zu verstehen.

7.1 Werksrückstellung und Parameterlöschung

Das Gerät bietet verschiedene Verfahren zum Zurücksetzen auf die Werkseinstellungen, wie in der folgenden Tabelle dargestellt. Wählen Sie die entsprechende Rücksetzmethode.

Funktion	**Wirkung**
Standardeinstellungen wiederherstellen	Netzwerk-/Benutzerkonfiguration beibehalten und nur Geräte-einstellungen wiederherstellen
Werkseinstellungen	Alle Parameter löschen, einschließlich Netzwerk/IP/Benutzer usw.
In den inaktiven Zustand zurückversetzen	Administrator-Passwort-Wiederherstellung, Passwort zurücksetzen

7.2 Hinweise zur Firmware-Aktualisierung

Um die Sicherheit der Benutzergeräte zu schützen, verschlüsseln und signieren wir das Firmware-Paket. Nachdem das Gerät das Firmware-Paket erhalten hat, prüft es die Signatur und entschlüsselt sie, was wirksam verhindern kann, dass das Firmware-Paket manipuliert wird.

- **Prüfen Sie regelmäßig die offiziellen Firmware-Versionen** und geben Sie den Sicherheits-Update-Versionen den Vorrang;
- **Laden Sie die OTA-Firmware nur von der offiziellen Website herunter** und verwenden Sie keine inoffiziellen Aktualisierungspakete;
- **Sichern Sie wichtige Konfigurationen vor dem Upgrade;**
- **Der Upgrade-Prozess darf nicht durch Strom- oder Netzausfälle unterbrochen werden.**

8. Sicherheit von Cloud-Diensten

8.1 2FA Zwei-Faktor-Authentifizierung

Nachdem Sie die 2FA-Zwei-Faktor-Authentifizierung aktiviert haben, müssen Sie sich bei der Fernanmeldung bei Ihrem Konto erneut mit dem E-Mail-Verifizierungscode verifizieren. Diese Funktion ist standardmäßig aktiviert und kann vom Benutzer manuell ausgeschaltet werden.
Es wird empfohlen, die Liste der vertrauenswürdigen Geräte regelmäßig zu überprüfen und alle nicht mehr vertrauenswürdigen Geräte zu löschen.
Es wird empfohlen, die Gesichts-/Fingerabdruckverifizierung zu aktivieren, um die App zu schützen.

9. Empfohlene Konfigurations-Checkliste

Im Folgenden finden Sie eine Liste der empfohlenen Netzwerksicherheitskonfigurationen ✅ . Es wird empfohlen, jeden Punkt bei der Einrichtung des Geräts und bei jährlichen Inspektionen zu überprüfen:

Projekt	Empfehlung Status	Aktuelle Konfiguration
Ändern Sie das Standardpasswort	✅ Starke Passwörter sind aktiviert	□ Ja / □ Nein
Automatische Abmeldung nach Zeitüberschreitung (≤ 5 Minuten) einschalten	✅ Öffnen Sie	□ Ja / □ Nein
Sicherheitsfragen für das Zurücksetzen von Passwörtern und den Export von Zertifikaten konfigurieren	✅ Bereits eingestellt	□ Ja / □ Nein
Löschen von Idle-Benutzerkonten	✅ Gereinigt	□ Ja / □ Nein
Korrekte Konfiguration der Zugriffsrechte für normale Benutzer	✅ Bei Bedarf konfigurieren	□ Ja / □ Nein
Aktivieren Sie HTTPS und installieren Sie das Zertifikat	✅ CA-Zertifikat oder selbstsigniertes Zertifikat	□ Ja / □ Nein
Aktivieren der RTSP/HTTP-Digest-Authentifizierung	✅ Aktivieren Sie	□ Ja / □ Nein
Deaktivieren Sie Protokolle wie UPnP/Telnet/Control4 usw.	✅ Deaktivieren Sie	□ Ja / □ Nein
Konfigurieren der IP-Whitelist	✅ Begrenzung des externen Zugriffs	□ Ja / □ Nein
Deaktivieren Sie nicht benötigte Dienste (HTTP/SNMP/FTP, usw.)	✅ Verschluss	□ Ja / □ Nein
Sperrmechanismus für anormale Anmeldung aktivieren	✅ Aktiviert	□ Ja / □ Nein
Protokolle werden ≥ 30 Tage lang gespeichert und können exportiert werden	✅ Kann kontrolliert und geführt werden	□ Ja / □ Nein
Die Firmware-Version ist die neueste Sicherheitsversion	✅ Aktualisiert	□ Ja / □ Nein
Aktivieren Sie die 2FA-Zwei-Faktor-Authentifizierung	✅ Geöffnet	□ Ja / □ Nein

Anmerkungen:

- Die oben genannten Konfigurationsoptionen können je nach den spezifischen Produktfunktionen leicht variieren. Die tatsächlich unterstützten Elemente entnehmen Sie bitte dem Produkthandbuch.
- Wenn das Gerät mit der Cloud-Plattform verbunden wurde, überprüfen Sie bitte gleichzeitig die Cloud-Kontobindung und den Alarmmechanismus.

Schlussfolgerung des Dokuments:

Dieser Leitfaden soll Anwendern dabei helfen, das Sicherheitsniveau von Gerätenetzwerken auf standardisierte und operative Weise zu verbessern. Wir werden die Version auf der Grundlage neuer Bedrohungen, branchenspezifischer Compliance-Anforderungen und Produktfunktionen ständig aktualisieren. Wenn Sie weitere technische Unterstützung benötigen, wenden Sie sich bitte an den technischen Vertreter oder die Serviceplattform in Ihrer Region.