Netzwerkvideorekorder

Kurzanleitung

V1.0.0

Vorwort

Allgemein

Diese Kurzanleitung (im Folgenden „Handbuch“ genannt) stellt die Funktionen und Bedienvorgänge der NVR-Geräte (im Folgenden „Gerät“ genannt) vor.

Sicherheitshinweise

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

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

Änderungsverlauf

Nr.	Version	Inhaltliche Überarbeitung	Veröffentlichungsdatum
1	V1.0.0	Erste Veröffentlichung.	Juli 2019

Datenschutzhinweis

Als Gerätebenutzer oder veranwortliche Stelle erfassen Sie möglicherweise personenbezogene Daten anderer Personen wie das Gesicht, die Fingerabdrücke, das Autokennzeichen, die E-Mail-Adresse, die Telefonnummer, GPS-Daten usw.
Sie müssen die örtlichen Datenschutzgesetze und Verordnungen einhalten, um die legitimen Rechte und Interessen anderer Personen durch die Umsetzung von Maßnahmen zu schützen, einschließlich, jedoch ohne Beschränkung auf: Bereitstellung einer eindeutigen und sichtbaren Hinweises zur Information der betroffenen Person über das Vorhandensein eines Überwachungsbereichs und Bereitstellung entsprechender Kontaktangaben.

Über das Handbuch

- Das Handbuch dient nur der Veranschaulichung. Bei Unstimmigkeiten zwischen Handbuch und dem jeweiligen Produkt hat das jeweilige Produkt Vorrang.
- Wir haften nicht für Verluste durch den Betrieb verursacht werden, der nicht den Anweisungen im Handbuch entspricht.
- Das Handbuch wird gemäß den neuesten Gesetzen und Vorschriften des jeweiligen Lands aktualisiert. Weitere Informationen finden Sie in der gedruckten Anleitung, auf der beiliegenden CD-ROM, über den QR-Code oder auf unserer offiziellen Website.
  Bei Widersprüchen zwischen dem gedruckten Handbuch und der elektronischen Version hat die elektronische Version Vorrang.
- Änderungen des Designs und der Software vorbehalten. Produktaktualisierungen können zu Abweichungen zwischen dem jeweiligen Produkt selbst und dem Handbuch führen. Wenden Sie sich für neueste Programm und zusätzliche Unterlagen und den Kundendienst.
- Es können immer noch Abweichungen in den technischen Daten, Funktionen und der Beschreibung der Inbetriebnahme oder Druckfehler vorhanden sein. Bei Unklarheiten oder Streitigkeiten nehmen Sie Bezug auf unsere endgültige Erläuterung.
- Aktualisieren Sie die Reader-Software oder probieren Sie eine andere Mainstream-Readersoftware aus, wenn das Handbuch (im PDF-Format) nicht geöffnet werden kann.
- Alle eingetragenen Warenzeichen und Firmennamen im Handbuch sind Eigentum ihrer jeweiligen Besitzer.
- Wenn beim Einsatz des Geräts Probleme aufgetreten, besuchen Sie unsere Website oder wenden Sie sich und den Lieferanten bzw. Kundendienst.
- Bei Unklarheiten oder Widersprüchen konsultieren Sie unsere endgültige Erläuterung.

Wichtige Sicherheits- und Warnhinweise

Verwenden Sie das Gerät nur wie beschrieben. Lesen Sie das Handbuch vor dem Gebrauch des Geräts sorgfältig durch, um Gefahren und Sachschäden zu vermeiden. Halten Sie sich während des Gebrauchs strikt an das Handbuch und bewahren Sie es für späteres Nachschlagen auf.

Betriebsanforderungen

- Installieren Sie das PoE-Frontendgerät im Innenbereich.
- Installieren Sie das Gerät nicht an einem Ort, der direkter Sonneneinstrahlung ausgesetzt ist, oder in unmittelbarer Nähe von Wärme erzeugenden Geräten.
- Installieren Sie das Gerät nicht in einem feuchten, staubigen oder verrauchten Bereich.
- Halten Sie das Gerät waagerecht oder stellen Sie es an einem stabilen Ort auf und verhindern Sie, dass es herunterfällt.
- Lassen Sie keine Flüssigkeiten auf das Gerät tropfen oder spritzen und stellen Sie keine mit Flüssigkeiten gefüllten Gegenstände auf das Gerät, um ein Eindringen von Flüssigkeiten zu verhindern.
- Installieren Sie das Gerät an einem gut belüfteten Ort und blockieren Sie nicht die Lüftungsöffnung.
- Verwenden Sie das Gerät nur innerhalb des Nenneingangs- und -ausgangsbereichs.
- Demontieren Sie das Gerät nicht.
- Transportieren, verwenden und lagern Sie das Gerät innerhalb des zulässigen Luftfeuchtigkeits- und Temperaturbereichs.

Anforderungen an die Stromversorgung

- Achten Sie darauf, den angegebenen Batterietyp zu verwenden. Andernfalls besteht Explosionsgefahr.
- Achten Sie darauf, geeignete Batterien zu verwenden. Andernfalls können die Batterien unter Umständen explodieren oder in Brand geraten!
- Bei Batteriewechsel darf nur der gleiche Batterietyp verwendet werden!
- Entsorgen Sie verbrauchte Batterien gemäß den Anweisungen.
- Das Produkt muss die empfohlenen elektrischen Kabel verwenden, wie in den Technischen Daten beschrieben!
- Verwenden Sie ein Standard-Netzteil, das mit diesem Gerät kompatibel ist. Anderenfalls gehen die daraus resultierenden Verletzungen und Schäden am Gerät auf Ihr Konto.
- Verwenden Sie ein Netzteil, das den SELV-Anforderungen (Safety Extra Low Voltage) entspricht, und schließen Sie es an einer Nennspannung gemäß IEC60950-1 an. Spezifische Anforderungen an die Stromversorgung entnehmen Sie den Geräteetiketten.
- Produkte der Kategorie I werden an einer geerdeten Steckdose angeschlossen.
- Der Gerätestecker dient als Trennvorrichtung. Der Stecker muss während des Betriebs jederzeit frei zugänglich sein.

Inhaltsverzeichnis

1 Lieferumfang

Die Installation muss den örtlichen Vorschriften für Elektroinstallationen entsprechen.
Das Gerät kann nicht mit nach unten gerichteter Frontplatte an der Wand montiert werden.

Wenn Sie das Gerät erhalten, überprüfen Sie bitte anhand der folgenden Checkliste.
Wenn eines der Teile fehlt oder beschädigt ist, wenden Sie sich sofort an Ihren örtlichen Fachhändler oder Kundendiensttechniker.

Reihenfolge	Überprüfen		Anforderungen
1	Verpackung	Erscheinungsbild	Keine offensichtlichen Schäden.
		Verpackungsmaterialien	Keine gebrochenen oder verbogenen Teile, die durch einen Stoß verursacht wurden.
		Zubehör	Vollständig.
2	Etiketten	Etiketten auf dem Gerät	● Das Gerätemodell entspricht der Bestellung. ● Nicht abgelöst. Die Etiketten dürfen nicht zerrissen oder weggeworfen werden, da sonst die Garantieleistungen nicht gewährleistet sind. Sie müssen die Seriennummer des Produkts angeben, wenn Sie den Kundendienst anrufen.
3	Gerät	Erscheinungsbild	Keine offensichtlichen Schäden.
		Datenkabel, Stromkabel, Lüfterkabel, Hauptplatine etc.	Keine Verbindung gelöst. Sollte eine Verbindung lose sein, wenden Sie sich bitte zeitnah an den Kundendienst des Unternehmens.

2 Festplatte installieren

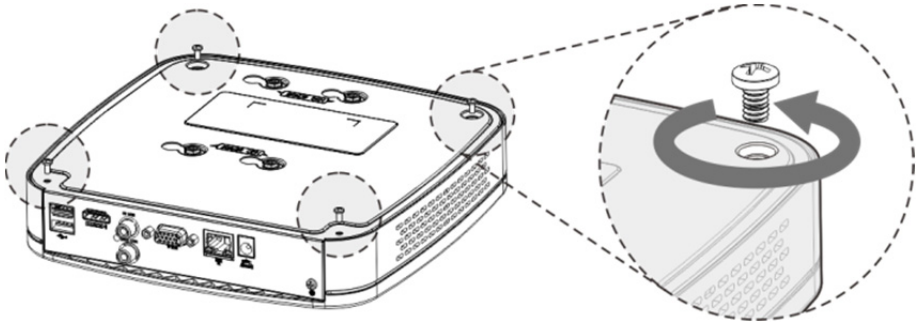
Die folgenden Abbildungen dienen lediglich zur Veranschaulichung.
Maßgeblich ist das Produkt.

Schalten Sie das Gerät aus, bevor Sie die Festplatte austauschen.

2.1 SMART 1U

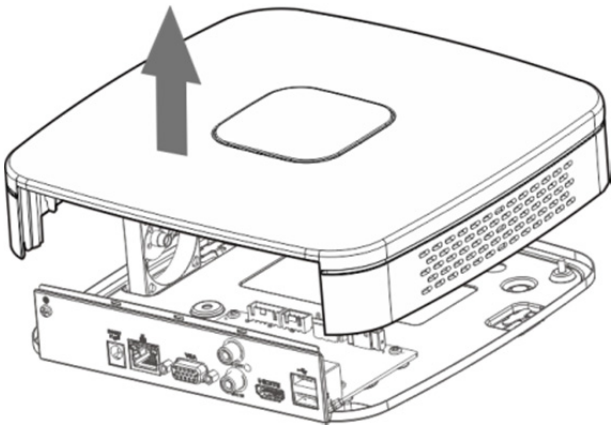
Prüfen Sie bei der ersten Installation, ob eine Festplatte installiert ist. Es ist empfehlenswert, eine Festplatte der Unternehmens- oder Überwachungsklasse zu verwenden. Es ist nicht empfehlenswert, eine PC-Festplatte zu verwenden.
Schritt 1: Drehen Sie das Gerät um und entfernen Sie die vier Befestigungsschrauben an der Grundplatte des Geräts.

Abbildung 2–1 Installation der Festplatte (1)



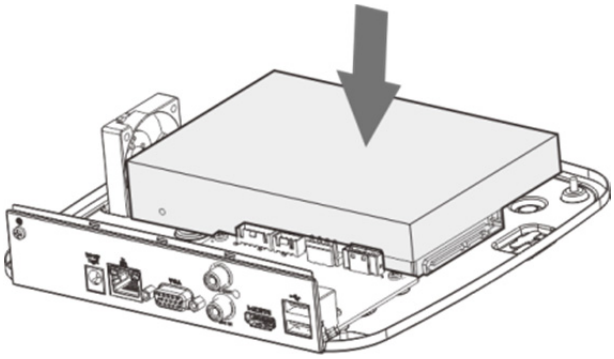
Schritt 2: Entfernen Sie den Gehäusedeckel in Pfeilrichtung, wie in der folgenden Abbildung dargestellt.

Abbildung 2–2 Installation der Festplatte (2)



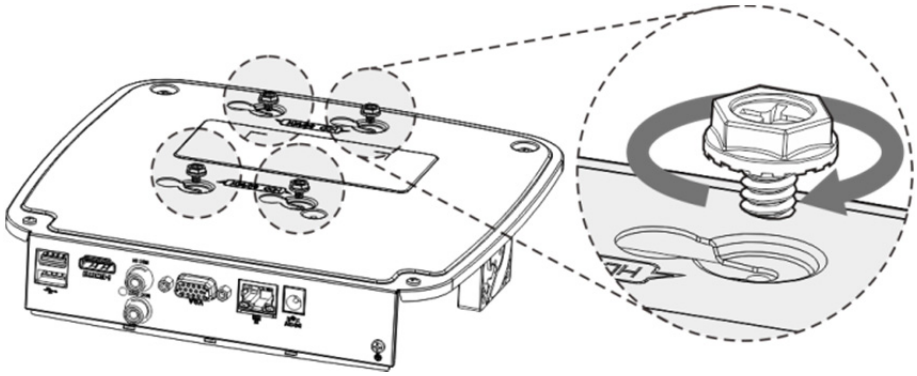
Schritt 3: Richten Sie die Festplatte an den vier Bohrungen in der Grundplatte für den Einbau aus.

Abbildung 2–3 Installation der Festplatte (3)



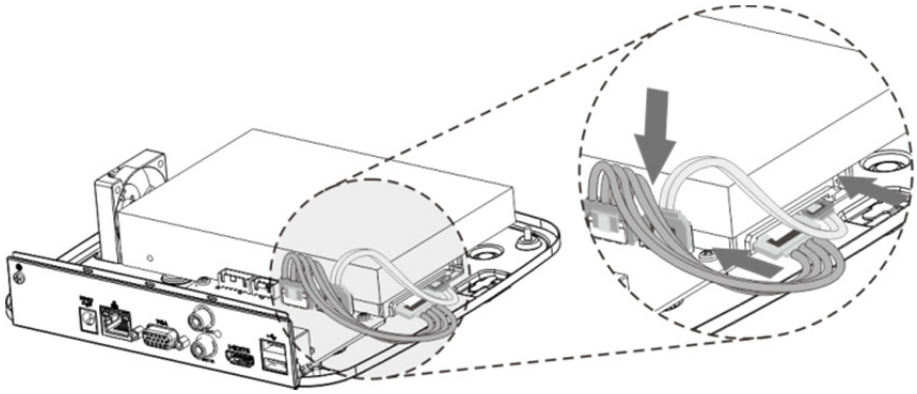
Schritt 4: Drehen Sie das Gerät auf den Kopf, setzen Sie die Schrauben in die Bohrungen von Gehäuse und Festplatte ein und ziehen Sie sie fest. Die Festplatte ist nun an der Grundplatte befestigt.

Abbildung 2–4 Installation der Festplatte (4)



Schritt 5: Schließen Sie das Festplattenkabel und das Stromkabel an.

Abbildung 2–5 Installation der Festplatte (5)



Schritt 6: Setzen Sie den Gehäusedeckel wieder ein und ziehen Sie zum Abschluss der Installation die vier Schrauben an der Grundplatte wieder fest.

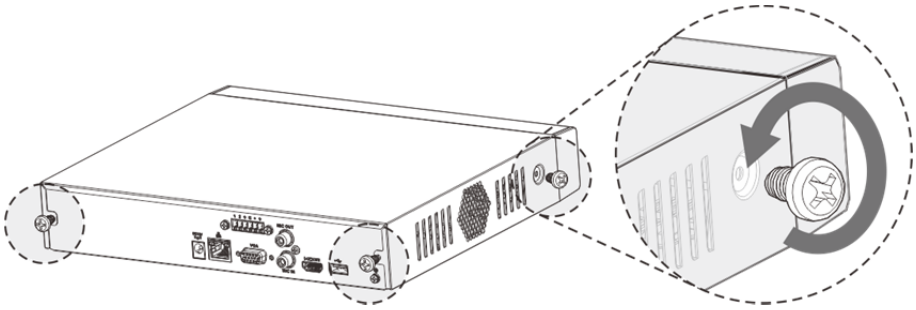
Abbildung 2–6 Installation der Festplatte (6)

2.2 MINI 1U, KOMPAKT 1U, 1U

Prüfen Sie bei der ersten Installation, ob eine Festplatte installiert ist. Es ist empfehlenswert, eine Festplatte der Unternehmens- oder Überwachungsklasse zu verwenden. Es ist nicht empfehlenswert, eine PC-Festplatte zu verwenden.

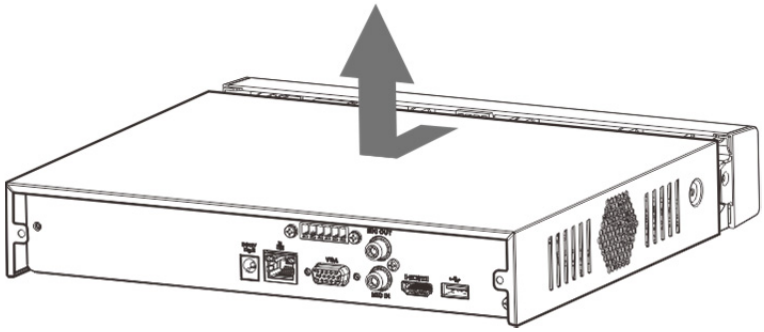
Schritt 1: Entfernen Sie die Befestigungsschrauben des Gehäusedeckels (einschließlich der beiden Schrauben an der Rückseite und der beiden Schrauben an der linken und rechten Seite).

Abbildung 2–7 Installation der Festplatte (1)



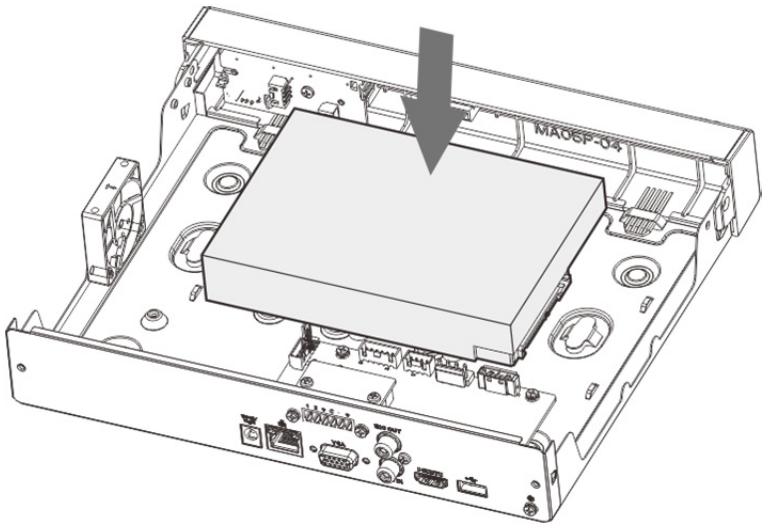
Schritt 2: Entfernen Sie den Gehäusedeckel in Pfeilrichtung, wie in der folgenden Abbildung dargestellt.

Abbildung 2–8 Installation der Festplatte (2)



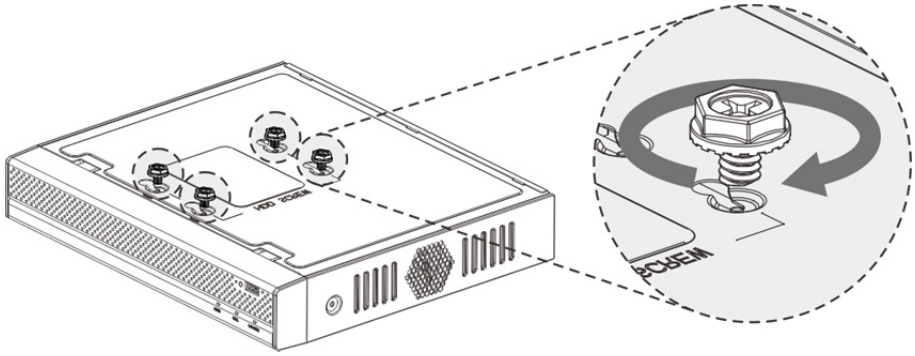
Schritt 3: Richten Sie die Festplatte an den vier Bohrungen in der Grundplatte für den Einbau aus.

Abbildung 2–9 Installation der Festplatte (3)



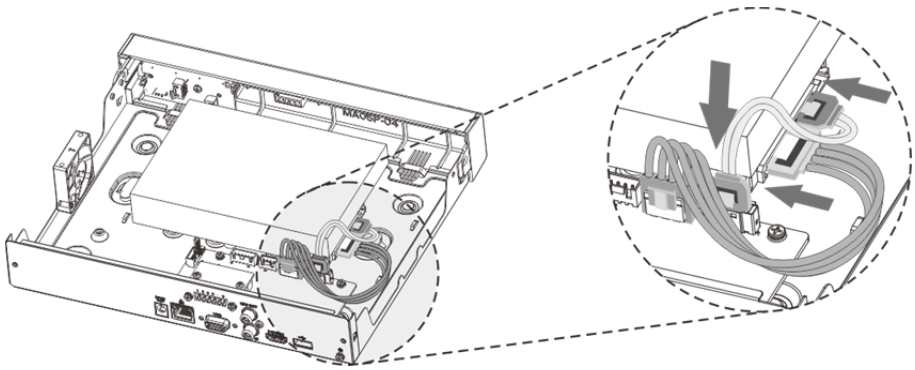
Schritt 4: Drehen Sie das Gerät auf den Kopf, setzen Sie die Schrauben in die Bohrungen von Gehäuse und Festplatte ein und ziehen Sie sie fest. Die Festplatte ist nun an der Grundplatte befestigt.

Abbildung 2–10 Installation der Festplatte (4)



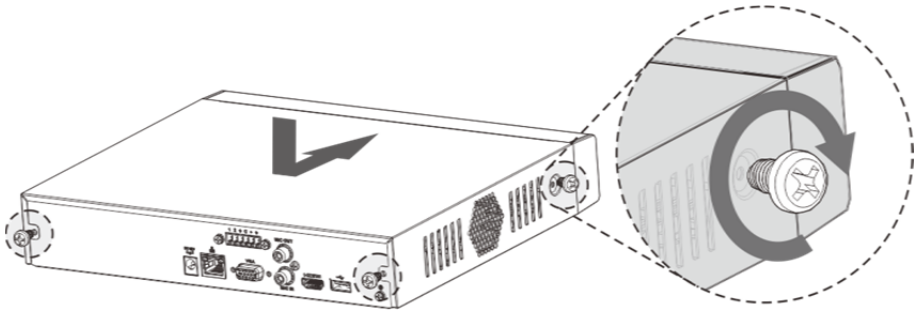
Schritt 5: Schließen Sie das Festplattenkabel und das Stromkabel an.

Abbildung 2–11 Installation der Festplatte (5)



Schritt 6: Setzen Sie den Gehäusedeckel wieder ein und ziehen Sie zum Abschluss der Installation die vier Schrauben an der Rückseite und an den Seiten wieder fest.

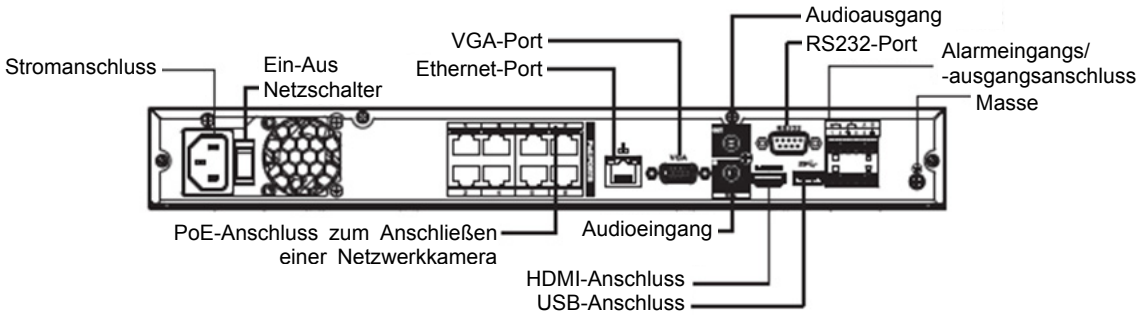
Abbildung 2–12 Installation der Festplatte (6)



3 Verbindung

Die folgenden Abbildungen dienen lediglich zur Veranschaulichung. Maßgeblich ist das Produkt.

Abbildung 3–1 Anschluss der 1U-Serie



- Sehen Sie sich die Symbole auf der Rückseite des Geräts genau an. Ausführliche Informationen finden Sie in Verbindung mit Ihrem konkreten Gerät.
- Bei Symbol DC 12V beträgt die Eingangsspannung DC 12 V. Bei Symbol DC48V beträgt die Eingangsspannung DC 48 V.

4 Bedienung der Benutzeroberfläche

Die Schnittstellen der verschiedenen Modelle können sich geringfügig unterscheiden. Die folgenden Abbildungen dienen lediglich zur Veranschaulichung. Maßgeblich ist das Produkt.

4.1 Systems hochfahren

Achten Sie vor dem Einschalten auf Folgendes:

- Die Nenneingangsspannung muss mit der Leistungsaufnahme des Geräts übereinstimmen. Stellen Sie sicher, dass das Netzkabel angeschlossen ist, und schalten Sie dann den Ein/Aus-Schalter ein.
- Verbinden Sie zum Schutz des Geräts zuerst das Netzteil mit dem Gerät und verbinden Sie das Netzteil dann mit der Steckdose.
- Verwenden Sie stets eine stabile Stromversorgung. Es ist empfehlenswert, eine USV zu verwenden.
- Geräte bestimmter Baureihen haben keinen Ein/Aus-Schalter. Sie können das Gerät hochfahren, wenn die Stromversorgung angeschlossen ist.

Verbinden Sie das Gerät mit dem Monitor, schließen Sie es an die Steckdose an und drücken Sie die Ein/Aus-Taste, um es hochzufahren.

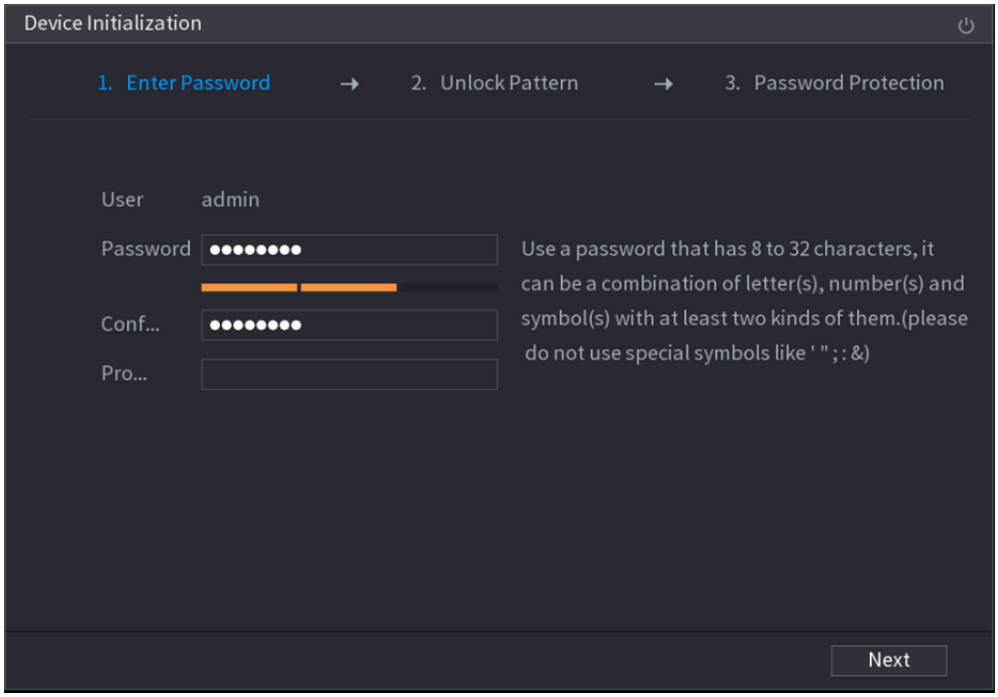
4.2 Initialisierung des Geräts

Beim ersten Hochfahren müssen Sie die Passwortinformationen für **admin** konfigurieren (standardmäßig). Um die Sicherheit des Geräts zu gewährleisten, bewahren Sie das Admin-Passwort gut auf und ändern Sie es regelmäßig.

Schritt 1: Schalten Sie das Gerät ein.

Das Fenster **Geräteinitialisierung** (Device initialization) wird angezeigt. Siehe Abbildung 4–1.

Abbildung 4–1 Passwort eingeben



Schritt 2: Konfigurieren Sie die Passwortinformationen für admin. Details siehe Tabelle 4–1.

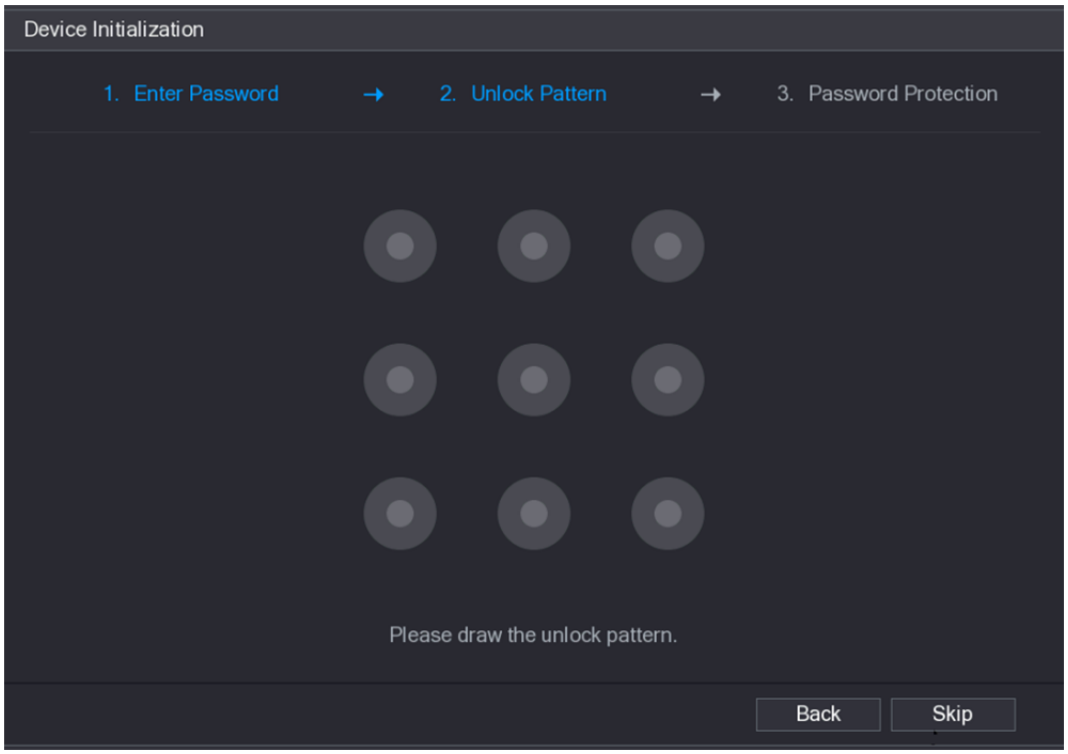
Tabelle 4–1 Informationen zum Passwort

Parameter	Beschreibung
Benutzer	Standardmäßig ist der Benutzer **admin**.
Passwort	Geben Sie im Feld **Passwort** (Password) das Passwort für den Administrator ein. Das neue Passwort kann 8 bis 32 Zeichen und muss mindestens zwei Typen von Zahlen-, Buchstaben- und Sonderzeichen (mit Ausnahme von „‘“, „„“, „““, „.“, „;“, „:“ und „&“) enthalten.
Passwort bestätigen	
Sicherheitsfrage	Geben Sie im Feld **Sicherheitsfrage** (Prompt Question) die Informationen ein, die Sie an das Passwort erinnern können. Klicken Sie im Anmeldemenü auf . Daraufhin wird der Dialog angezeigt, um Ihnen beim Zurücksetzen des Passworts zu helfen.

Schritt 3: Klicken Sie auf **Weiter** (Next).

Das Menü **Entsperrmuster** (Unlock Pattern) wird angezeigt. Siehe Abbildung 4–2.

Abbildung 4–2 Entsperrmuster

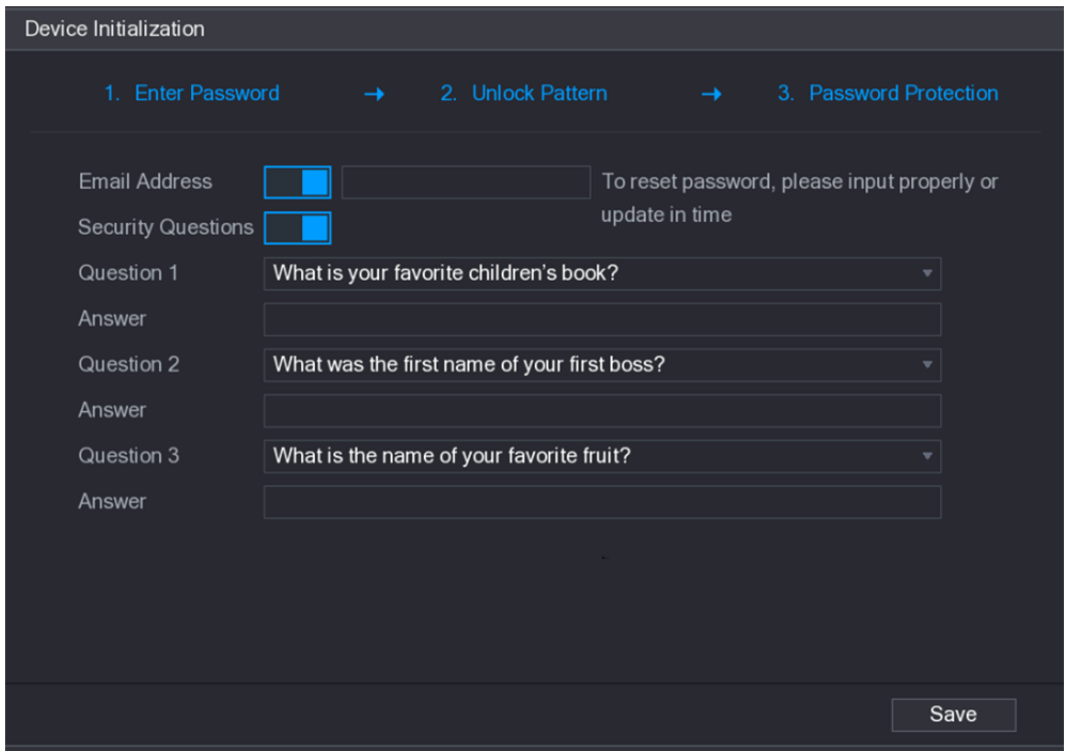


Schritt 4: Zeichnen Sie ein Entsperrmuster.

Nach dem Einstellen des Entsperrmusters wird das Menü Passwortschutz (Password Protection) angezeigt. Siehe Abbildung 4–3.

- Sobald Sie das Entsperrmuster konfiguriert haben, benötigt das System das Entsperrmuster als Standard-Anmeldung. Wenn Sie diese Einstellung überspringen, geben Sie das Passwort zur Anmeldung ein.
- Wenn Sie kein Entsperrmuster konfigurieren möchten, klicken Sie auf **Überspringen** (Skip).

Abbildung 4–3 Passwortschutz



Schritt 5: Konfigurieren Sie die Schutzparameter für das Passwort. Details siehe Tabelle 4–2.

- Wenn Sie nach der Konfiguration das Passwort für den Admin-Benutzer vergessen haben, können Sie das Passwort über die reservierte E-Mail-Adresse oder Sicherheitsfragen zurücksetzen. Nähere Einzelheiten zum Zurücksetzen des Passworts finden Sie in der *Bedienungsanleitung*.
- Wenn Sie die Einstellungen nicht konfigurieren möchten, deaktivieren Sie die Funktionen E-Mail-Adresse und Sicherheitsfragen im Menü.

Tabelle 4–2 Beschreibung der Parameter für den Passwortschutz

Passwortschutz-Modus	**Beschreibung**
E-Mail-Adresse	Geben Sie die reservierte E-Mail-Adresse ein. Geben Sie im Feld **E-Mail-Adresse** (Email Address) eine E-Mail-Adresse zum Zurücksetzen des Passworts ein. Falls Sie das Passwort vergessen haben, geben Sie den Sicherheitscode ein, den Sie von dieser reservierten E-Mail-Adresse erhalten, um das Passwort des Administrators zurückzusetzen.
Sicherheitsfragen	Konfigurieren Sie die Sicherheitsfragen und -antworten. Falls Sie das Passwort vergessen haben, geben Sie die Antworten auf die Fragen ein, um das Passwort zurückzusetzen.
Wenn Sie die Funktion E-Mail oder Sicherheitsfragen später konfigurieren oder die Einstellungen ändern möchten, wählen Sie **Hauptmenü > KONTO > BENUTZER** (Main Menu > ACCOUNT > USER).	

Schritt 6: Klicken Sie auf **OK**, um die Einstellungen zu beenden.

Der **Startassistent** (Startup Wizard) wird angezeigt. Nähere Einzelheiten zu Schnelleinstellungen während des Startens finden Sie in der *Bedienungsanleitung.*

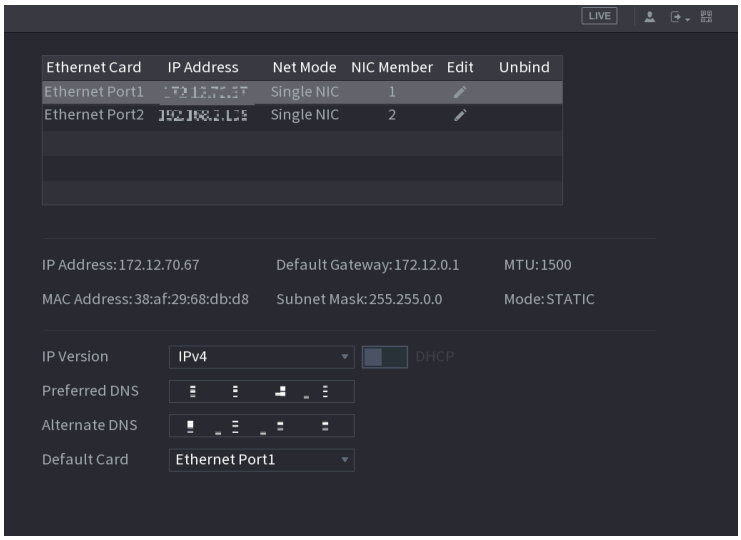
4.3 IP-Adresse ändern

Wählen Sie **Hauptmenü > NETZWERK > TCP/IP** (Main Menu > NETWORK > TCP/IP).

Das Menü TCP/IP wird angezeigt. Siehe Abbildung 4–4. Klicken Sie auf  ,

um die IP-Adresse entsprechend dem aktuellen Netzwerkadressen-Schema zu ändern (die Standard-IP-Adresse lautet 192.168.1.108).

Abbildung 4–4 TCP/IP



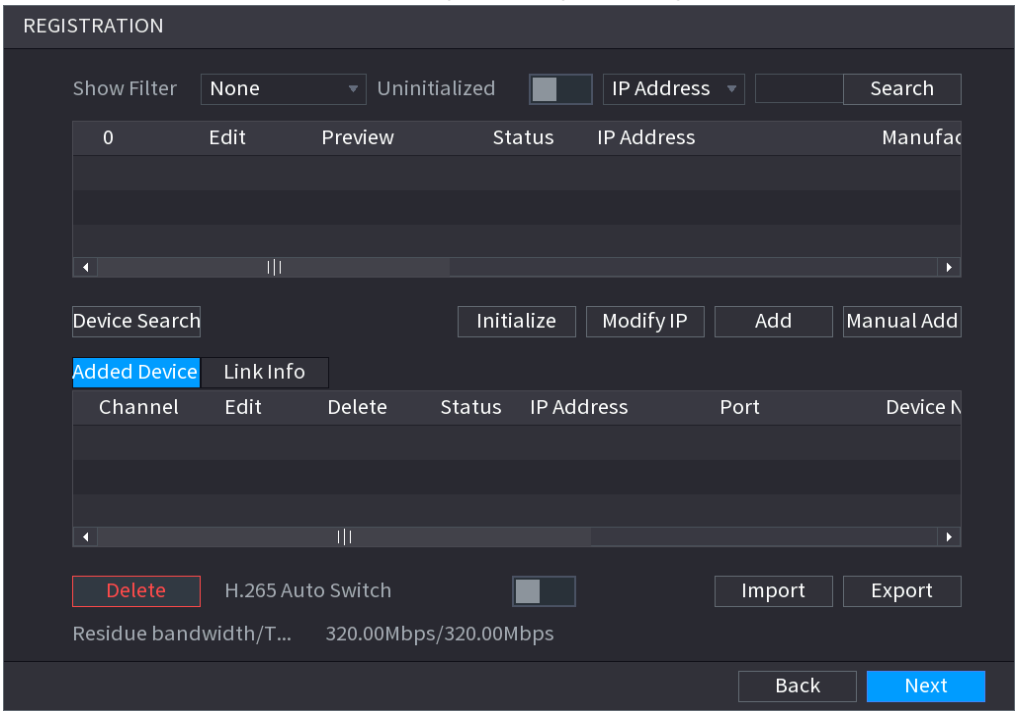
4.4 Registrierung

Wählen Sie **Hauptmenü > KAMERA > Registrierung** (Main Menu > CAMERA > Registration). Das Registrierungsmenü wird angezeigt. Siehe Abbildung 4–5.

Sie können Remote-Geräte auf folgende Weisen registrieren:

- Klicken Sie auf **Gerätesuche** (Device Search). Führen Sie in der Ergebnisliste einen Doppelklick auf das Remote-Gerät aus oder aktivieren Sie das Kontrollkästchen vor dem Gerät. Klicken Sie dann auf **Hinzufügen** (Add), um das Remote-Gerät zu registrieren.
- Klicken Sie auf **Manuell hinzufügen** (Manual Add) und geben Sie die IP-Adresse des Remote-Geräts ein, um es zu registrieren.

Abbildung 4–5 Registrierung



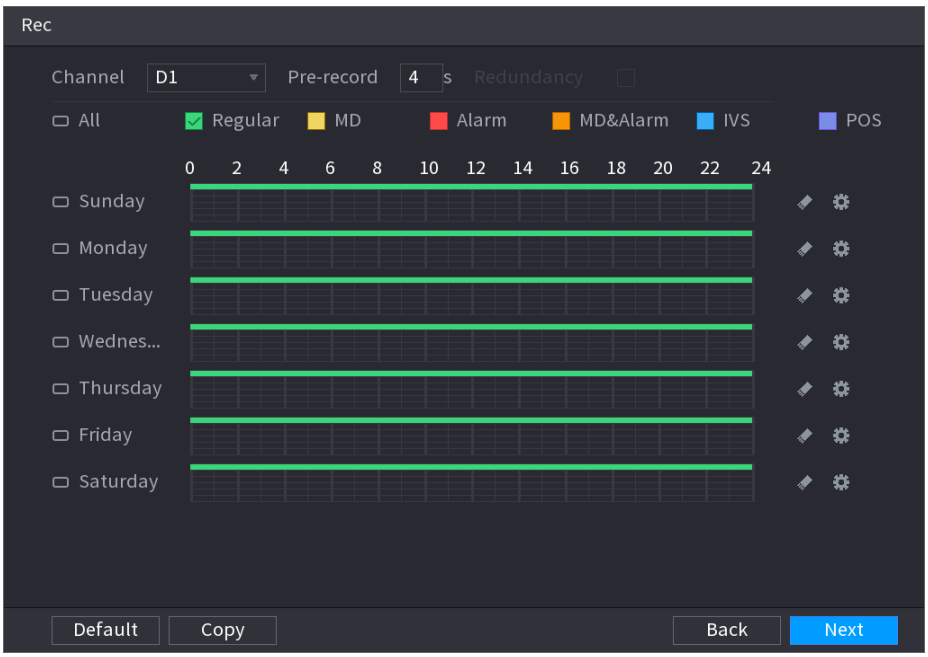
4.5 Planung

Per Werkseinstellung werden alle Kanäle rund um die Uhr kontinuierlich aufgezeichnet. Sie können den Aufnahmezeitraum und den Aufnahmetyp anpassen.

Schritt 1: Wählen Sie **Hauptmenü > Speicher > ZEITPLAN > Aufnehmen** (Main Menu > STORAGE > SCHEDULE > Rec).

Das Menü **Aufnahme** (Rec) wird angezeigt. Siehe Abbildung 4–6.

Abbildung 4–6 Zeitplan



Schritt 2: Konfigurieren Sie Parameter wie Kanal, Voraufnahme, ANR und Aufnahmetyp.

- Nachdem Sie eine Festplatte als redundante Festplatte festgelegt haben, aktivieren Sie das Kontrollkästchen **Redundanz** (Redundancy), um Sicherungskopien von Videodateien zu erstellen. Dies dient dazu, Videodateien auf verschiedenen Festplatten gleichzeitig zu speichern. Falls eine der Festplatten beschädigt ist, befindet sich noch eine Sicherungsdatei auf einer anderen Festplatte, um Datenzuverlässigkeit zu gewährleisten.
- Aktivieren Sie das Kontrollkästchen ANR, um diese Funktion zu aktivieren. Wenn die IPC keinen Netzwerkzugriff hat, nimmt sie weiter auf und speichert die Aufnahmen auf der SD-Karte. Wenn der Netzwerkzugriff wiederhergestellt ist, überträgt die IPC die während des Netzwerkausfalls erstellten Aufnahmen auf den NVR, um die Aufnahmeintegrität zu gewährleisten.

Schritt 3: Legen Sie den Planungszeitraum fest. Dazu müssen Sie zeichnen und bearbeiten.

- Zeichnen: Drücken Sie die linke Maustaste und ziehen Sie die Maus über die Zeitachse, um den Zeitraum zu zeichnen.
- Bearbeiten: Klicken Sie auf  , um den Zeitraum zu konfigurieren, und klicken Sie auf **OK**.

Schritt 4: Klicken Sie auf **Übernehmen** (Apply) oder auf **OK**, um die Einstellungen zu speichern.

Der konfigurierte Aufnahmeplan kann nur übernommen werden, wenn die automatische Aufnahmefunktion aktiviert ist. Nähere Einzelheiten zur Aktivierung der automatischen Aufnahme finden Sie in der *Bedienungsanleitung.*

4.6 Wiedergabe

Wählen Sie **Hauptmenü > WIEDERGABE** (Main Menu > PLAYBACK) oder klicken Sie mit der rechten Maustaste auf das Vorschaumenü und wählen Sie **Suchen** (Search). Das Menü zur Aufnahmesuche (record search) wird angezeigt. Siehe Abbildung 4–7.

Sie können Aufnahmen gemäß dem konfigurierten Aufnahmetyp, der Aufnahmezeit und dem Kanal wiedergeben. Ausführliche Informationen hierzu finden Sie in der *Bedienungsanleitung.*

Abbildung 4–7 Aufnahmesuche

4.7 Ausschalten

Klicken Sie oben rechts auf  und wählen Sie **Herunterfahren** (Shutdown).

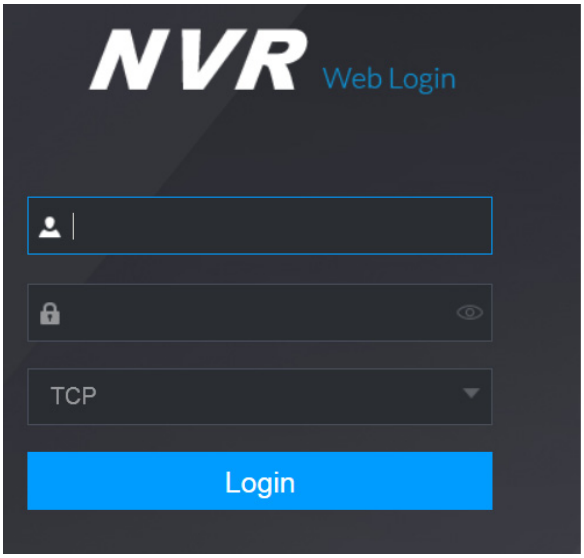
5 Web-Betrieb

Wenn Sie sich zum ersten Mal am Gerät anmelden, müssen Sie es zuerst initialisieren. Ausführliche Informationen hierzu finden Sie in der *Bedienungsanleitung.*

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

Das **Anmelde** (Login)-Fenster wird angezeigt. Siehe Abbildung 5–1.

Abbildung 5–1 Anmeldung



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

- Der Standardbenutzername ist „admin“, und das Anmeldepasswort ist dasjenige, das Sie bei der Initialisierung des Geräts festgelegt haben. Um die Sicherheit des Geräts zu gewährleisten, sollten Sie das Admin-Passwort regelmäßig ändern und gut aufbewahren.
- Wenn Sie das Admin-Passwort vergessen haben, klicken Sie auf **Passwort vergessen** (Forgot Passwort), um es zurückzusetzen. Ausführliche Informationen hierzu finden Sie in der *Bedienungsanleitung.*

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

Das Menü **Vorschau** (Preview) wird angezeigt. Auf der Weboberfläche können Sie Systemeinstellungen konfigurieren, Geräte verwalten und Netzwerkeinstellungen konfigurieren. Einzelheiten hierzu finden Sie in der *Bedienungsanleitung.*

- Wenn Sie sich zum ersten Mal an der Weboberfläche anmelden, installieren Sie das Steuerelement gemäß den Systemanweisungen.

6 P2P

Schritt 1: Scannen Sie den QR-Code mit dem Mobiltelefon, um die Mobilanwendung herunterzuladen und zu installieren.

Sie können den QR-Code der Mobilanwendung und den QR-Code der SN des Geräts auf die folgenden zwei Weisen erhalten:

- Melden Sie sich an der lokalen Oberfläche an und wählen Sie **Hauptmenü > NETZWERK > P2P** (Main Menu > NETWORK > P2P).
- Melden Sie sich an der Weboberfläche an und wählen Sie **Hauptmenü > NETZWERK > TCP/IP > P2P** (Main Menu > NETWORK > TCP/IP > P2P).

Abbildung 6–1 QR-Code der Mobilanwendung

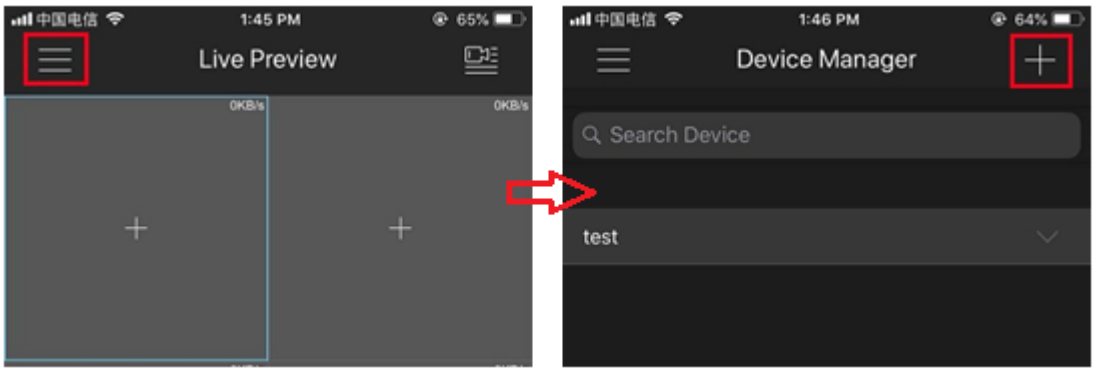
Schritt 2: Registrieren Sie das Gerät in der Mobilanwendung.

Nachdem Sie das Gerät erfolgreich registriert haben, können Sie den Überwachungsbildschirm in der Mobilanwendung anzeigen.

Die folgenden Abbildungen dienen lediglich zur Veranschaulichung. Maßgeblich ist das Produkt. Ausführliche Informationen hierzu finden Sie in der *Bedienungsanleitung*.

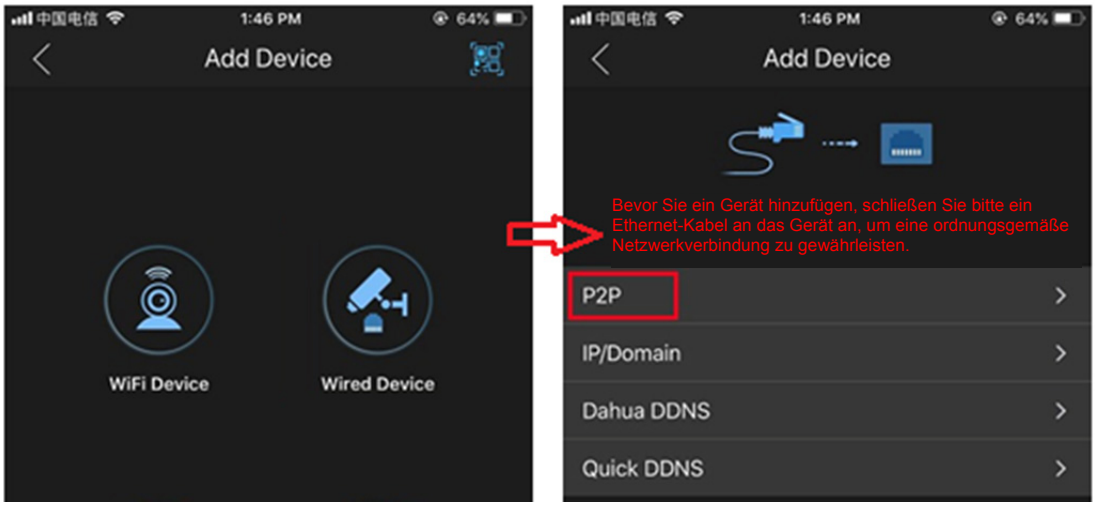
1) Tippen Sie auf , wählen Sie **Geräteverwaltung** (Device Manager), und tippen Sie dann auf . Siehe Abbildung 6–2.

Abbildung 6–2 P2P (1)



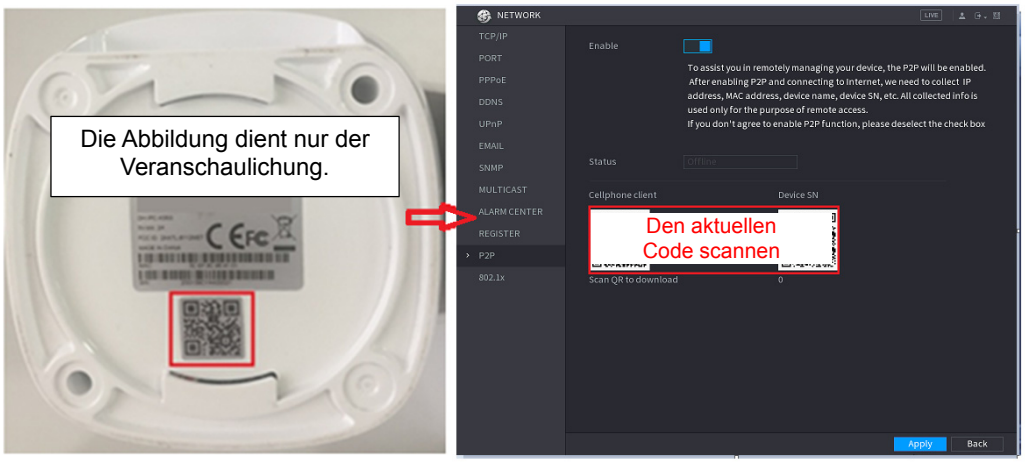
2) Tippen Sie auf den entsprechenden Gerätetyp (**WLAN-Gerät** (WIFI Device) oder **kabelgebundenes Gerät** (Wired Device)) und dann auf **P2P**, um das Gerät zu registrieren. Siehe Abbildung 6–3.

Abbildung 6–3 P2P (2)



3) Scannen Sie den Geräteaufkleber oder die Geräte-SN auf der lokalen Oberfläche (**NETZWERK > P2P** (NETWORK > P2P)), um das Gerät zu registrieren. Siehe Abbildung 6–4.

Abbildung 6–4 P2P (3)



4) Nach dem Scannen können Sie die Geräte-SN anzeigen. Klicken Sie auf **Live-Vorschau starten** (Start Live Preview) und Sie können das Livebild auf dem Mobiltelefon sehen.

Anhang 1 Empfehlungen zur Cybersicherheit

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

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

1. **Verwenden Sie sichere Passwörter**
   Sehen Sie sich die folgenden Vorschläge an, um Passwörter festzulegen:
   - Die Länge darf nicht weniger als 8 Zeichen betragen;
   - Schließen Sie mindestens zwei Arten von Zeichen ein: Groß- und Kleinbuchstaben, Zahlen und Symbole;
   - Fügen Sie nicht den Kontonamen oder den Kontonamen in umgekehrter Reihenfolge ein;
   - Verwenden Sie keine fortlaufenden Zeichen, wie z.B. 123, abc usw;
   - Verwenden Sie keine Mehrfachzeichen, wie z.B. 111, aaa, usw;
2. **Aktualisieren Sie Firmware und Client-Software rechtzeitig.**
   - Gemäß dem in der Tech-Industrie üblichen Verfahren empfehlen wir, die Firmware Ihrer Geräte (wie NVR, DVR, IP-Kamera usw.) auf dem neuesten Stand zu halten, um zu gewährleisten, dass das System mit den neuesten Sicherheitspatches und -fixes ausgestattet ist. Wenn das Gerät mit dem öffentliche Netzwerk verbunden ist, empfehlen wir, die Funktion „Automatische Überprüfung auf Aktualisierungen“ (Auto-Check for Updates) zu aktivieren, um aktuelle Informationen über vom Hersteller freigegebene Firmware-Aktualisierungen zu erhalten.
   - Wir empfehlen, die neueste Version der Client-Software herunterzuladen und zu verwenden.

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

1. **Physischer Schutz**
   Wir empfehlen, dass Sie Geräte, insbesondere Speichergeräte, physisch schützen. Stellen Sie die Geräte beispielsweise in einen speziellen Computerraum und -schrank und implementieren Sie eine gut durchdachte Zutrittskontrollberechtigung und Schlüsselverwaltung, um unbefugte Mitarbeiter davon abzuhalten, physische Kontakte wie beschädigte Hardware, unbefugten Anschluss von Wechseldatenträgern (z.B. USB-Stick, serielle Schnittstelle) usw. durchzuführen.
2. **Passwörter regelmäßig ändern**
   Wir empfehlen, die Passwörter regelmäßig zu ändern, um das Risiko zu verringern, erraten oder geknackt zu werden.
3. **Passwörter einstellen und rechtzeitig aktualisieren**
   Das Gerät unterstützt die Funktion Passwortrücksetzung. Konfigurieren Sie zeitnah die entsprechenden Informationen zum Zurücksetzen des Passworts, einschließlich der E-Mail-Adresse und der Sicherheitsfragen des Endbenutzers. Wenn sich die Daten ändern,

ändern Sie diese bitte rechtzeitig. Bei der Einstellung von Fragen zum Passwortschutz empfehlen wir, keine Fragen zu verwenden, die leicht zu erraten sind.

4. **Kontosperre aktivieren**
   Die Kontosperrfunktion ist standardmäßig aktiviert und wir empfehlen, sie eingeschaltet zu lassen, um die Kontosicherheit zu gewährleisten. Versucht sich ein Angreifer mehrmals mit dem falschen Passwort anzumelden, wird das entsprechende Konto und die Quell-IP-Adresse gesperrt.
5. **Standard HTTP und andere Dienstports ändern**
   Wir empfehlen, die Standard-HTTP- und andere Dienstports in einen beliebigen Zahlensatz zwischen 1024 - 65535 zu ändern, um das Risiko zu verringern, dass Außenstehende erraten können, welche Ports Sie verwenden.
6. **HTTPS aktivieren**
   Wir empfehlen, HTTPS zu aktivieren, damit Sie den Webdienst über einen sicheren Kommunikationskanal besuchen können.
7. **Weißliste aktivieren**
   Wir empfehlen, die Weißlistenfunktion so zu aktivieren, dass jeder, mit Ausnahme derjenigen mit den angegebenen IP-Adressen, vom Zugriff auf das System ausgeschlossen wird. Nehmen Sie daher die IP-Adresse Ihres Computers und die IP-Adresse des Begleitgeräts in die Whitelist auf.
8. **MAC-Adressenverknüpfung**
   Wir empfehlen, die IP- und MAC-Adresse des Gateways mit dem Gerät zu verknüpfen, um das Risiko von ARP-Spoofing zu reduzieren.
9. **Konten und Privilegien sinnvoll zuordnen**
   Gemäß den Geschäfts- und Verwaltungsanforderungen sollten Sie Benutzer sinnvoll hinzufügen und ihnen ein Minimum an Berechtigungen zuweisen.
10. **Unnötige Dienste deaktivieren und sichere Modi wählen**
    Falls nicht erforderlich, empfehlen wir, einige Dienste wie SNMP, SMTP, UPnP usw. zu deaktivieren, um Risiken zu reduzieren.
    Falls erforderlich, wird dringend empfohlen, dass Sie sichere Modi verwenden, einschließlich, aber nicht darauf beschränkt, die folgenden Dienste:
    - SNMP: Wählen Sie SNMP v3 und richten Sie starke Verschlüsselungs- und Authentifizierungspasswörter ein.
    - SMTP: Wählen Sie TLS, um auf den Mailbox-Server zuzugreifen.
    - FTP: Wählen Sie SFTP, und richten Sie starke Passwörter ein.
    - AP-Hotspot: Wählen Sie den Verschlüsselungsmodus WPA2-PSK und richten Sie starke Passwörter ein.
11. **Audio- und Video-verschlüsselte Übertragung**
    Wenn Ihre Audio- und Videodateninhalte sehr wichtig oder sensibel sind, empfehlen wir, eine verschlüsselte Übertragungsfunktion zu verwenden, um das Risiko zu verringern, dass Audio- und Videodaten während der Übertragung gestohlen werden.
    Zur Erinnerung: Die verschlüsselte Übertragung führt zu einem Verlust der Übertragungseffizienz.
12. **Sichere Auditierung**
    - Online-Benutzer überprüfen: Wir empfehlen, die Online-Benutzer regelmäßig zu überprüfen, um zu sehen, ob ein Gerät ohne Berechtigung angemeldet ist.

- Geräteprotokoll prüfen: Durch die Anzeige der Protokolle können Sie die IP-Adressen, mit denen Sie sich bei Ihren Geräten angemeldet haben und deren wichtigste Funktionen erkennen.

13. **Netzwerkprotokoll**
    Aufgrund der begrenzten Speicherkapazität der Geräte sind gespeicherte Protokolle begrenzt. Wenn Sie das Protokoll über einen längeren Zeitraum speichern müssen, empfehlen wir, die Netzwerkprotokollfunktion zu aktivieren, um zu gewährleisten, dass die kritischen Protokolle mit dem Netzwerkprotokollserver für die Rückverfolgung synchronisiert werden.
14. **Aufbau einer sicheren Netzwerkumgebung**
    Um die Sicherheit der Geräte besser zu gewährleisten und mögliche Cyberrisiken zu reduzieren, empfehlen wir:
    - Deaktivieren Sie die Port-Mapping-Funktion des Routers, um einen direkten Zugriff auf die Intranet-Geräte aus dem externen Netzwerk zu vermeiden.
    - Das Netzwerk muss entsprechend dem tatsächlichen Netzwerkbedarf partitioniert und isoliert werden. Wenn es keine Kommunikationsanforderungen zwischen zwei Subnetzwerken gibt, empfehlen wir, VLAN, Netzwerk-GAP und andere Technologien zur Partitionierung des Netzwerks zu verwenden, um den Netzwerkisolationseffekt zu erreichen.
    - Einrichtung des 802.1x Zugangsauthentifizierungssystems, um das Risiko eines unbefugten Zugriffs auf private Netzwerke zu reduzieren.